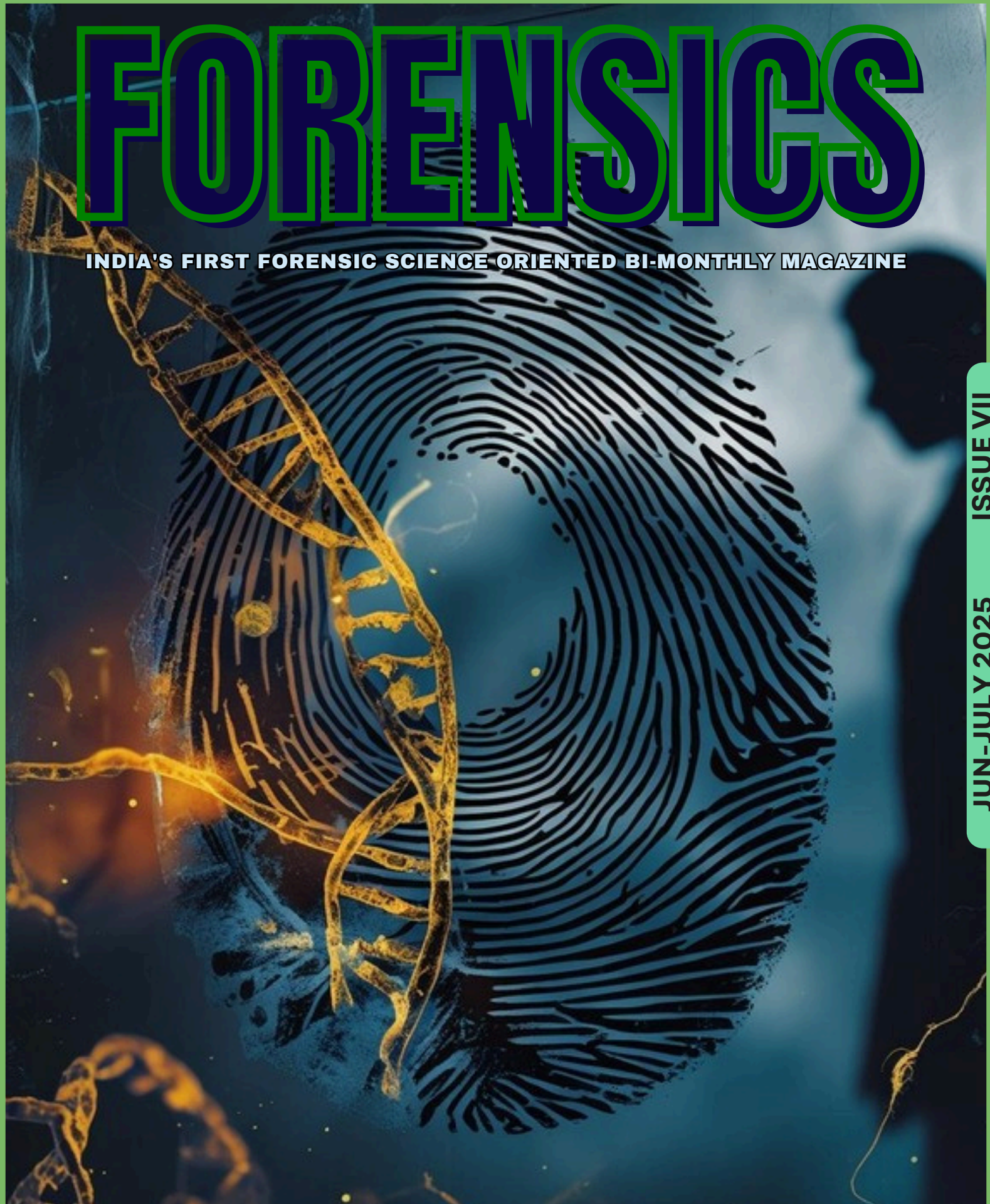


FORENSICS

INDIA'S FIRST FORENSIC SCIENCE ORIENTED BI-MONTHLY MAGAZINE

ISSUE VII

JUN-JULY 2025

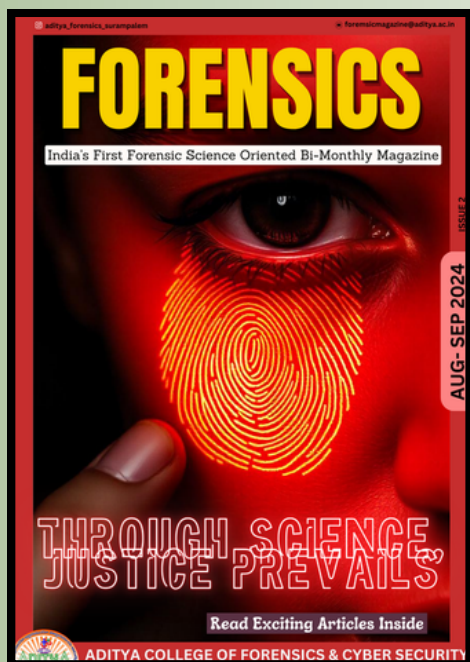


ADITYA COLLEGE OF FORENSICS & CYBER SECURITY
SURAMPALEM, ANDHRA PRADESH

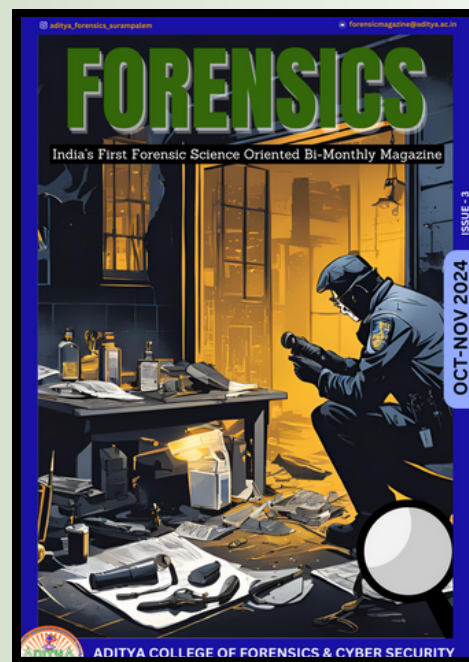
VIEW OUR PREVIOUS ISSUES



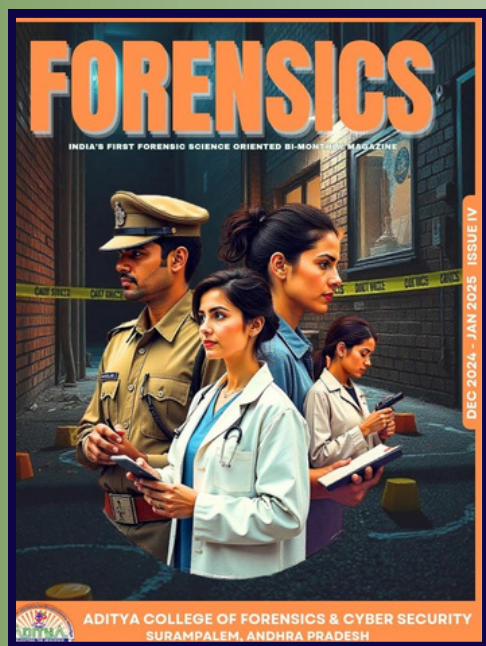
ISSUE I (JUN-JUL 2024)



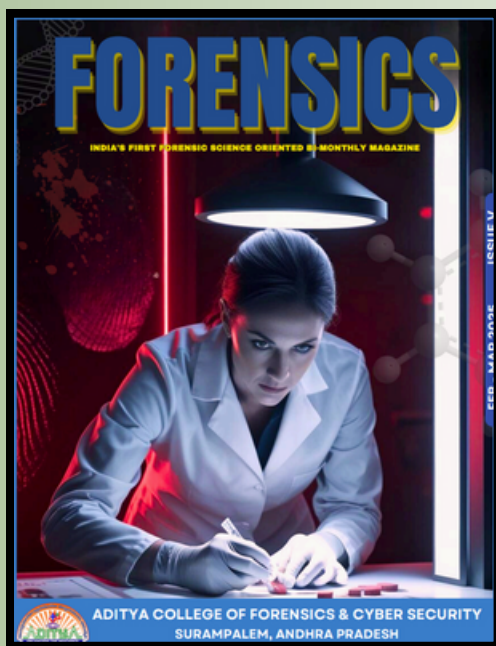
ISSUE II (AUG-SEP 2024)



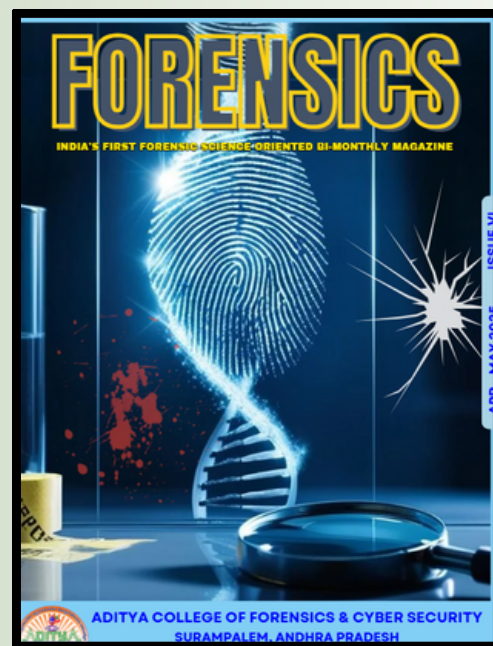
ISSUE III (OCT-NOV 2024)



ISSUE IV (DEC-JAN 2025)



ISSUE V (FEB-MAR 2025)



ISSUE VI (APR-MAY 2025)

Forensics Magazine: 2025

HUMAN RIGHTS AND DNA IDENTIFICATION IN FORENSIC SCIENCE IN CENTRAL ASIA: AN ETHICAL AND LEGAL APPROACH

11



“TEETH AMIDST THE FLAMES: FORENSIC ODONTOLOGY IN THE AFTERMATH OF THE AHMEDABAD AIR INDIA AI-171 CRASH”

30



A LIFELONG COMMITMENT TO FORENSIC MEDICINE AND JUSTICE

34



3 B'S: BLACK MAGIC? BETRAYAL? BANK? THE ₹53 CRORE GOLD ROBBERY CASE STUDY

48

ENVIRONMENTAL DNA (E-DNA) IN FORENSIC INVESTIGATIONS: NEW FRONTIER MOLECULAR APPROACHES FOR CRIMINAL INVESTIGATION

106

EXPLORING ROBOTIC HANDWRITING: FORENSIC EXAMINATION AND CHALLENGES

126



REVOLUTIONIZING FORENSIC NURSING: NON-INVASIVE IMAGING FOR PHYSICAL AND SEXUAL ASSAULT EXAMINATIONS

178

CONTENTS

The Sound of Lies: Exploring Deepfake Audio Through Real-Time Cases	16 Pg
Genes, Machines, and Memories: Predicting Human Recall Through Genomics and AI Neural Mapping	21 Pg
Stalkerware: The Silent Threat to Digital Privacy	27 Pg
Blockchain and Data Privacy: Conflict or Complement?	37 Pg
Forensic Odontology in Non-Human Bites	44 Pg
Encrypted Alibis: When Privacy Tools Obstruct Justice	55 Pg
Innovative Techniques in Questioned Document Analysis: From Advanced Forensics to Imaginary Futures	65 Pg
Mitochondrial DNA and Beyond: Expanding the Reach of Forensic Genealogy	74 Pg
Behind the Mask: The Rise of Deepfake Hacktivism	80 Pg
The Jiah Khan Case: a Forensic Enigma in Bollywood	88 Pg
Emerging Trends in Synthetic Cannabinoid-Related Deaths: A Forensic Toxicological Perspective (India, 2015–2024)	99 Pg
Encrypted Gene the Firewallfor DNA: Genomiccyber shield in the Modern Healthcare Era	114 Pg
Microplastics and Beyond: Addressing Emerging Environmental Contaminants for a Sustainable Future	120 Pg
Exploring Robotic Handwriting: Forensic Examination and Challenges	126 Pg

CONTENTS

Game-Based Cybercrimes: Digital Forensics in Online Multiplayer Environments	130 Pg
The Nth Room Case: How a Cybersex Trafficking Scandal Exposed South Korea's Digital Vulnerabilities and Technological measures has South Korea introduced to detect and delete illegal sexual content	138 Pg
Commercialised Threats & Real-Time Response	146 Pg
Microbiome: A Powerful Investigative Tool in Crime Investigation	154 Pg
Mobile Forensics: The Hurdles of Physical Extraction from Today's Smartphones	158 Pg
Silent Witnesses: Arthropods as Key Evidence in Criminal Cases	161 Pg
The role of Acoustic and Linguistic features in forensic Voice Identification	169 Pg
Justice Behind Closed Doors: Unmasking the Horror at Kolkata Law College	175 Pg
The Role of Deep Learning in Cyber Forensics Reducing Cybercrime and Enhancing Facial Recognition	181 Pg
Prepare Yourself- UGC Net and FACT Question Bank	183 Pg
Prepare Yourself UGC - Net Paper 1	187 Pg

FROM THE LEADERSHIP TEAM



Dr. N. Sesa Reddy

**CHAIRMAN - ADITYA EDUCATIONAL
INSTITUTIONS**



Dr. N. Satish Reddy

**VICE CHAIRMAN - ADITYA
EDUCATIONAL INSTITUTIONS**

Issue VII brings together insightful and engaging contributions from students, faculty, and industry professionals, highlighting the latest innovations, creative approaches, and pressing challenges in the field of forensic science. With a strong emphasis on exploration, collaboration, and the exchange of ideas, this edition aims to inspire and support both seasoned practitioners and aspiring forensic experts.

We extend our heartfelt gratitude to all contributors whose dedication and efforts have brought this issue to life. Together, let us continue advancing the frontiers of forensic science.

It is an honour to present the seventh edition of India's pioneering bi-monthly magazine on forensic science, building on the remarkable support received for our previous issues. I extend heartfelt gratitude to the Department of Forensic Science for its unwavering guidance and visionary leadership in driving this initiative forward. With every edition, our aim is to foster innovation and uphold excellence in forensic science education and professional practice across the country. This issue features compelling contributions that highlight the latest advancements and emerging trends shaping the field.

FROM THE EDITORIAL DESK



Vilas Anil Chavan
Editor-in-Chief

Welcome to Issue VII of India's First Bimonthly Forensic Science Magazine!

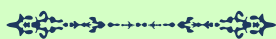
We are thrilled to bring you the seventh edition of our magazine, following the overwhelming support and enthusiasm for our previous issues. This edition continues our mission to spotlight the latest developments and thought-provoking insights in the field of forensic science.

Inside, you'll find compelling articles on DNA profiling, digital forensics, forensic psychology, questioned document examination, cybercrime, trace evidence, and more. With contributions from students, academicians, and industry experts, this issue captures the collaborative spirit driving forensic innovation across the country.

Thank you for being an essential part of this journey. Together, let's keep uncovering the science that strengthens justice.

As the Editorial Head, I'm delighted to present Issue VII of our magazine, reaffirming our dedication to delivering high-quality content in the field of forensic science. This edition offers a rich blend of pioneering research, expert insights, and recent advancements—covering everything from DNA analysis and digital forensics to crime scene investigation and forensic psychology. You'll also find real-life case studies, updates on policy shifts, and career-focused guidance to keep you informed in this fast-evolving discipline.

Your continued encouragement drives us to expand the boundaries of forensic knowledge. Thank you for being an integral part of this journey—together, we are shaping the future of forensic science.



BVSS Udaynadh
Editorial Head

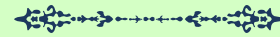
FROM THE EDITORIAL DESK



Thushar KC
Managing Editor

Welcome to Issue VII of India's First Bimonthly Forensic Science Magazine! We're thrilled by the continued support from our readers and contributors. This edition features key topics like DNA profiling, digital forensics, forensic psychology, questioned documents, cybercrime, and trace evidence.

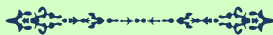
With insights from students, educators, and professionals, this issue reflects our shared commitment to advancing forensic science in India. Thank you for being part of this journey. Let's keep exploring the science behind justice!



Forensic science is more than facts and figures—it's the art of uncovering truth from fragments. Every fingerprint, every fiber, every digital trace tells a part of a larger story. As creative editors, our role is to bring these stories to life with clarity, accuracy, and visual impact.

In Issue VII, we've worked to blend scientific depth with creative expression, making complex ideas accessible and engaging. From layout to visuals, every element is designed to support the powerful content within.

Thank you for joining us in this continued journey—where creativity meets credibility in the pursuit of justice.



Aanchal Sakarkar
Creative- Editor

Contributors



Nilufar Ganiyeva



Dharmistha Parmar



Bhumit Chavda



Shweta Javia



Kiran R Dodiya



Chandana



Balaji M



Dr. Kapil Kumar



Shruti Bamhoria



Dr. Riya Mariya



Vagdevi Emani



Leeba Pathan



Kinjal Patan



Yash Babaria



Mr. Sagar Harwani



Janvi

Contributors



Santosh Nandwana



Malla Bharadwaj Sai Satya Murthy



Bonagiri JayaRaju



Himanshu Chudasama



Mr. Maypal Daki



Eshant Chabadiya



Vinisha Solanki



Tripti Bhargava



Jerald Benny



Kuldipsinh Mori



Gaurang M Sindhav



Janki Kacha



Dasari Harsha Vardhan



Manibhavadarani A P



Aashtha Tiwari



Human Rights and DNA Identification in Forensic Science in Central Asia: An Ethical and Legal Approach

Author: Nilufar Ganiyeva

Abstract

Objectives: This study aims to critically examine the intersection of human rights and forensic DNA identification practices in Central Asia by analyzing existing legal frameworks in countries such as Kazakhstan, Kyrgyzstan, Uzbekistan, and Tajikistan. The research seeks to identify key ethical and legal gaps related to informed consent, data protection, and potential violations of individual rights. It further assesses the extent to which national legislation aligns with international human rights norms, including the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights. Finally, the study offers practical recommendations to strengthen regulatory frameworks and promote ethical, transparent, and rights-based approaches to the use of DNA in forensic science throughout the region.

Aims: The aim of this study is to examine how forensic DNA identification practices in Central Asia affect fundamental human rights, with particular attention to legal and ethical standards, national legislation, and international human rights compliance, while proposing actionable solutions for ensuring a transparent and responsible use of DNA in forensic contexts.

Methods: The study employs a qualitative, interdisciplinary methodology, including legal analysis, ethical review, and comparative policy evaluation. National legislation and forensic protocols from Kazakhstan, Kyrgyzstan, Uzbekistan, and Tajikistan were examined in light of international human rights instruments such as the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights. Additionally, relevant case reports and forensic policy documents were reviewed to identify gaps and risks related to privacy, consent, and state oversight.

Results: The analysis revealed significant inconsistencies in national approaches to forensic DNA regulation across Central Asia. Common concerns include the absence of clear informed consent procedures, insufficient legal protections for genetic data, lack of public transparency, and the indefinite retention of DNA samples. The findings also highlight the limited alignment of national legislation with international human rights standards and the absence of independent oversight bodies.

These gaps contribute to a legal environment where individual rights may be compromised in favor of state interests.

Conclusion: To ensure the ethical and lawful application of DNA identification in forensic science across Central Asia, it is essential to develop harmonized legal frameworks that uphold human rights principles. This includes establishing clear informed consent protocols, enhancing data protection laws, creating independent oversight mechanisms, and promoting bioethics education among forensic professionals. Without these safeguards, the use of DNA in forensic practice risks undermining individual dignity, privacy, and legal accountability.

Keywords: Bioethics, Central Asia, Criminal Justice, Data Protection, Ethical Standards, Forensic DNA, Genetic Privacy, Human Rights, Informed Consent,



Introduction

The use of DNA identification has become a cornerstone of modern forensic science, offering unprecedented precision in criminal investigations, disaster victim identification, and the resolution of missing persons cases. In recent years, countries in Central Asia—particularly Kazakhstan, Kyrgyzstan, Uzbekistan, and Tajikistan—have increasingly adopted forensic DNA technologies as part of national strategies to modernize law enforcement and improve criminal justice outcomes.

However, while these scientific advances offer clear benefits, their implementation raises serious ethical and legal concerns. In many instances, DNA databases are developed and used without adequate frameworks for protecting genetic privacy, ensuring informed consent, or establishing independent oversight. These gaps create conditions where individuals' rights may be subordinated to state security agendas.

International human rights instruments—including the Universal Declaration of Human Rights (1948), the International Covenant on Civil and Political Rights (1966), and the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Council of Europe, 1981)—clearly outline the need for lawful, transparent, and rights-respecting use of personal data, including genetic information. Furthermore, the Recommendation R(92)1 of the Council of Europe on the use of DNA analysis in criminal justice highlights ethical obligations in data handling, retention, and consent.

Despite these standards, national legal systems in Central Asia show inconsistencies in the regulation of forensic genetics. For example, while Kazakhstan introduced a law on genetic registration in 2021, concerns persist regarding the indefinite storage of samples and the lack of procedures for data removal or appeal. In Uzbekistan, forensic DNA databases are growing rapidly, yet remain largely opaque to the public and subject to minimal legal scrutiny.

This study addresses the urgent need to assess whether the use of forensic DNA in Central Asia aligns with international human rights norms. It further explores how regional legal and ethical standards can be improved to ensure that scientific progress does not come at the expense of individual dignity and autonomy.

Methods

This study employs a qualitative, interdisciplinary research design combining legal analysis, ethical review, and comparative policy evaluation. A doctrinal approach was used to examine and interpret national legislation, legal acts, and forensic guidelines from Kazakhstan, Kyrgyzstan, Uzbekistan, and Tajikistan. These sources were selected to assess the current regulatory status of DNA identification systems in Central Asia, with particular focus on laws relating to genetic registration, data protection, criminal procedure, and bioethics.

International instruments—such as the Universal Declaration of Human Rights (1948), the International Covenant on Civil and Political Rights (1966), and Council of Europe Recommendation R(92)1—served as normative benchmarks for assessing compliance with global human rights standards. The study also incorporated policy documents from UNESCO and INTERPOL to contextualize international best practices and principles relevant to forensic genetics.

A comparative legal analysis enabled identification of divergences and common trends across the selected jurisdictions. Furthermore, an ethical evaluation was conducted based on the principles of informed consent, proportionality, necessity, and data minimization. A targeted review of peer-reviewed scientific literature was used to capture broader discussions on the risks of surveillance, data abuse, and violations of genetic privacy.

Finally, attention was given to practical aspects, such as the operation of forensic DNA laboratories, availability of public information, and mechanisms for legal redress or data removal. The research design ensured both theoretical depth and relevance to real-world forensic practices in the region.

Results

The comparative legal and ethical analysis revealed notable inconsistencies and regulatory gaps across Central Asian countries regarding the use of forensic DNA identification. Key findings include the following:

1. Lack of Clear Informed Consent Mechanisms:

None of the analyzed national legislations comprehensively define the procedures for obtaining informed consent prior to DNA collection, particularly in cases involving minors, vulnerable individuals, or non-criminal suspects. In many instances, consent is presumed or bypassed, especially in criminal investigations.

2. Indefinite Data Retention and Ambiguous Deletion Rights:

Most countries, particularly Kazakhstan and Uzbekistan, lack clear time limits for DNA data retention and provide no practical mechanisms for individuals to request deletion of their genetic profiles. This raises significant concerns regarding the right to privacy and the principle of data minimization.

3. Absence of Independent Oversight Bodies:

There are no established independent institutions tasked with monitoring the ethical use of forensic DNA databases. Oversight is often internal and controlled by law enforcement agencies, increasing the risk of abuse and lack of accountability.

4. Low Public Awareness and Legal Transparency:

Public access to information about DNA databases, their purpose, and citizens' rights is minimal. Legislative texts are often difficult to access or interpret, and there is a general lack of public dialogue on the ethical implications of forensic genetics.

5. Partial Alignment with International Human Rights Standards:

While some legal frameworks reference international instruments, practical implementation falls short. There is little evidence of harmonization with the Universal Declaration of Human Rights, ICCPR, or UNESCO Declaration on Human Genetic Data in terms of ethical safeguards.

These findings indicate a structural imbalance between the state's interest in public security and the individual's right to privacy, autonomy, and due process. Without reforms, current practices risk undermining both the credibility of forensic science and the protection of fundamental rights in the region.

Discussion

The findings of this study highlight a critical gap between the growing use of forensic DNA technologies in Central Asia and the region's current ethical and legal infrastructures. While DNA identification has undeniable value in criminal justice, including the resolution of violent crimes and the identification of missing persons, its expansion has occurred largely without adequate legal safeguards or human rights oversight (Kayser, 2017).

The absence of clear informed consent protocols in most Central Asian states raises serious concerns. In countries such as Uzbekistan and Tajikistan, DNA samples are often collected without the explicit consent of the individual, particularly in criminal proceedings. This contravenes international human rights instruments such as the Universal Declaration on Bioethics and Human Rights (UNESCO, 2005) and the jurisprudence of the European Court of Human Rights (ECtHR, 2008), which emphasize the principle of individual autonomy and the necessity of lawful interference.

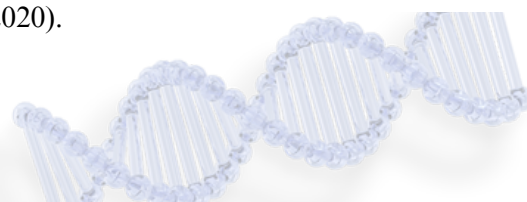
Data retention practices also reveal a troubling trend: there are few or no legal provisions regarding time limits for the storage of DNA profiles. The indefinite retention of profiles from suspects, including minors or individuals later acquitted, constitutes a potential violation of the right to privacy under Article 17 of the International Covenant on Civil and Political Rights (ICCPR, 1966) and the General Comment No. 16 (UN Human Rights Committee, 1988).

Another issue is the lack of independent oversight mechanisms. In contrast to European systems, where DNA databases are supervised by independent ethical boards or data protection authorities (Council of Europe, 2009; McCartney et al., 2011), Central Asian systems tend to rely on law enforcement agencies without civilian control. This not only creates potential for abuse but also undermines public trust in forensic institutions (Prainsack & Toom, 2013).

Moreover, the low level of public awareness about forensic genetics and its implications exacerbates the ethical risks. Without civic education and access to legal information, individuals are less likely to exercise their rights or challenge unlawful practices. This creates a climate of silent consent and institutional opacity (Samuel & Prainsack, 2019).

The discussion also reveals broader geopolitical concerns. With increasing regional cooperation and international data sharing initiatives — including participation in INTERPOL's DNA Gateway and bilateral agreements with foreign forensic entities — the lack of legal regulation on cross-border genetic data transfers creates vulnerabilities regarding sovereignty and data protection (Kowal & Radin, 2015; Phillips, 2018).

To bridge these gaps, a region-specific ethical-legal framework must be developed. This should include legislation ensuring informed consent, time-limited data retention, independent oversight, public education, and alignment with international norms. Capacity building through academic, legal, and civic collaboration will be essential to making these reforms sustainable (UNODC, 2021; Dondorp & de Wert, 2020).



Conclusion

This study underscores the urgent need for the development of ethical and legal frameworks that align the expanding use of forensic DNA technologies in Central Asia with internationally recognized human rights standards. While DNA identification offers valuable contributions to criminal justice and humanitarian efforts, its application must be governed by principles that respect individual autonomy, privacy, and the rule of law (UNESCO, 2005; ICCPR, 1966). The absence of informed consent, lack of independent oversight, indefinite retention of DNA data, and insufficient public awareness are major concerns that challenge both ethical norms and legal compliance (Prainsack & Toom, 2013; ECtHR, 2008). These deficiencies not only risk infringing on fundamental rights but also undermine the credibility of forensic systems and erode public trust (Samuel & Prainsack, 2019).

To address these issues, Central Asian countries should adopt transparent, rights-based policies that include legal provisions for informed consent, clearly defined retention limits, external monitoring bodies, and robust data protection standards (Council of Europe, 2009; McCartney et al., 2011). Furthermore, interdisciplinary collaboration among forensic scientists, legal experts, ethicists, and civil society will be vital in shaping a sustainable and equitable forensic framework (Dondorp & de Wert, 2020; UNODC, 2021).

Aligning national practices with international instruments such as the Universal Declaration on Bioethics and Human Rights (UNESCO, 2005), the International Covenant on Civil and Political Rights (ICCPR, 1966), and the Council of Europe Recommendations (Council of Europe, 2009) will not only improve governance but also strengthen the region's capacity to participate in global forensic cooperation with integrity and accountability (Phillips, 2018).

Acknowledgements

The author gratefully acknowledges the support of colleagues from the Department of Forensic Medicine and Medical Law, as well as regional human rights experts and legal scholars whose insights contributed to the development of this research. Special thanks to the participants of interdisciplinary workshops on bioethics and forensic genetics in Central Asia, whose contributions were invaluable. This study also benefited from consultations with representatives of civil society organizations working on justice reform and privacy rights in the region.

No specific funding was received for this study. The author declares no conflict of interest.

Conflict of Interest

The author declares no conflict of interest related to the research, authorship, or publication of this article.

Data Availability Statement

No new datasets were generated or analysed during the current study. All data supporting the findings of this article are derived from publicly available legal documents, ethical guidelines, and academic publications cited in the references.

References

1. Council of Europe. (1981). Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108). <https://www.coe.int/en/web/data-protection/convention108-and-protocol>
2. Council of Europe. (2009). Recommendation CM/Rec(2009)11 of the Committee of Ministers to member states on principles concerning the establishment and legal protection of national DNA databases. Strasbourg: Council of Europe. <https://rm.coe.int/16805cda38>
3. Dondorp, W., & de Wert, G. (2020). The responsible use of genetic information: Ethical and legal issues. Springer. <https://doi.org/10.1007/978-3-030-32951-5>.
4. European Court of Human Rights (ECtHR). (2008). Case of S. and Marper v. the United Kingdom (Applications nos. 30562/04 and 30566/04). Strasbourg: ECtHR. <https://hudoc.echr.coe.int/eng?i=001-90051>
5. González, J. A. (2019). Ethical challenges of forensic genetics in emerging democracies. Forensic Science International: Genetics Supplement Series, 7, 612–615. <https://doi.org/10.1016/j.fsigs.2019.10.107>.
6. United Nations General Assembly. (1966). International Covenant on Civil and Political Rights (ICCPR). <https://www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights>

7. International Covenant on Civil and Political Rights (ICCPR). (1966). United Nations. <https://www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights>

8. Interpol. (2020). DNA guidelines for the use of DNA in criminal investigations. Interpol. <https://www.interpol.int/en/Crimes/Forensic-science/DNA>

9. Kayser, M. (2017). Forensic DNA phenotyping: Predicting human appearance from crime scene material for investigative purposes. *Forensic Science International: Genetics*, 28, 201–210. <https://doi.org/10.1016/j.fsigen.2017.06.005>

1. Kowal, E., & Radin, J. (2015). Indigenous bio-sovereignty: Reconsidering the ethics of biocolonialism. *Science, Technology, & Human Values*, 40(4), 615–638. <https://doi.org/10.1177/0162243915570557>

2. McCartney, C., Wilson, T., & Williams, R. (2011). The future of forensic bioinformation: Ethics, law and governance. Springer. <https://doi.org/10.1007/978-3-642-14621-3>

3. M'charek, A., Toom, V., & Prainsack, B. (2012). The human DNA body and the question of consent: A critical perspective. *BioSocieties*, 7(2), 205–228. <https://doi.org/10.1057/biosoc.2012.8>

4. Phillips, C. (2018). International perspectives on forensic DNA databases. *Forensic Science International: Genetics*, 34, 1–3. <https://doi.org/10.1016/j.fsigen.2018.02.011>

5. Prainsack, B., & Toom, V. (2013). The governance of forensic DNA databases in Europe. *Journal of Law and the Biosciences*, 1(1), 87–110. <https://doi.org/10.1093/jlb/llt005>

6. Prainsack, B., & Toom, V. (2013). The governance of forensic DNA databases in Europe. *Journal of Law and the Biosciences*, 1(1), 87–110. <https://doi.org/10.1093/jlb/llt005>

7. Council of Europe. (1992). Recommendation R(92)1 on the use of DNA analysis in criminal justice. <https://rm.coe.int/16804c7e14>

8. Samuel, G., & Prainsack, B. (2019). Forensic DNA phenotyping in Europe: Views “on the ground” from those who have a professional stake in the technology. *New Genetics and Society*, 38(2), 119–141. <https://doi.org/10.1080/14636778.2019.1609480>

9. Samuel, G., & Prainsack, B. (2019). Forensic DNA phenotyping in Europe: Views and practices of forensic geneticists regarding the ethics of DNA-based appearance predictions. *New Genetics and Society*, 38(2), 119–141. <https://doi.org/10.1080/14636778.2019.1609480>

10. UN Human Rights Committee. (1988). General Comment No. 16: The right to respect of privacy, family, home and correspondence (Article 17, ICCPR). <https://www.refworld.org/docid/453883f922.html>

11. UNESCO. (2003). International Declaration on Human Genetic Data. [\[https://unesdoc.unesco.org/ark:/48223/pf0000139251\]](https://unesdoc.unesco.org/ark:/48223/pf0000139251)

12. United Nations General Assembly. (1948). Universal Declaration of Human Rights (UDHR). <https://www.un.org/en/about-us/universal-declaration-of-human-rights>

13. United Nations Office on Drugs and Crime (UNODC). (2021). Guidelines for the use of DNA in criminal investigations. Vienna: United Nations. <https://www.unodc.org/unodc/en/data-and-analysis/dna-guidelines.html>

14. United Nations Office on Drugs and Crime (UNODC). (2021). Guidelines for the use of DNA in criminal investigations. Vienna: United Nations Office on Drugs and Crime. <https://www.unodc.org/unodc/en/data-and-analysis/dna-guidelines.html>

ABOUT THE AUTHORS



Nilufar Ganiyeva

Department of Forensic Medicine and Medical Law
Tashkent medical academy
Tashkent, Uzbekistan

The Sound of Lies: Exploring Deepfake Audio Through Real-Time Cases

Author: Ms. Dharmistha Parmar, Mr. Bhumi Chavda

Introduction

Narrated by Kim Power, Human Voice is a place where trust and identity rest on their backs. However, that voice is slowly becoming subject to a darker manipulation, deepfake audio. These synthetic voice recordings, which are driven by artificial intelligence, are done with high-level artificial intelligence capable of simulating the way the individual talks, the tone and inflections of his speech with chilling precision, thus blending reality and fiction. No longer science fiction, deepfake audio is increasingly a powerful tool in every industry, whether it is to spread political misinformation and commit clever financial fraud, to carry out malicious reputational attacks. The article under review, i.e., *The Sound of Lies: Investigating Deepfake Audio in Real-Time Examples*, travels beyond the theoretical possibilities to discuss its practical influence (Neumann, 2021). This paper will shed light on actions, intentions, and impacts of such fraudulent activities by examining the documented examples of the deployment of deepfake audio. The interpretation of these real-time examples is important in visualizing how the landscape of digital deceptions is growing and coming up with mechanisms crucial to counter the sound of lies that have marred digital life.

Overview and scope of Deepfake Audio:

1.1 Overview and scope of Deepfake Audio:

At a time when artificial intelligence (AI) produces art, composes poetry, and operates vehicles, it has to take on the attractive and, in some ways, threatening skill of duplicating the human voice to an incredible degree. This is called deepfake audio because it is speech that has been produced synthetically with machine learning in the form of neural network models (usually WaveNet or transformer-based ones). These models are capable of mimicking unusual voice timber, speaking styles, accents and emotions, with less than a few seconds of voice samples (Kreps, 2023; Westerlund, 2019). Created for positive applications such as restoring voices for patients with speech loss or dubbing films across languages, deepfake audio has since been weaponized in more alarming contexts.

It has been used for fraud, impersonation, political disinformation,

and non-consensual media creation (Chesney & Citron, 2019; Villasenor, 2020). What makes deepfake audio particularly insidious is its emotional believability. Unlike text or even video, which often carry visible or linguistic markers of manipulation, audio taps into the brain's instinctive trust in familiar voices—especially those of authority figures or loved ones (Neumann, 2021).



Fig. Deepfake audio importance and its scope in Forensic Sciences

This has already enabled real-world attacks. For instance, in 2019, fraudsters used AI voice cloning to impersonate the CEO of a German energy firm's parent company, successfully tricking the U.K. CEO into transferring \$243,000 to the criminals (Stupp, 2019). In 2024, an AI-generated robocall mimicking President Joe Biden was circulated in New Hampshire, falsely advising voters to "stay home" during the Democratic primary, sparking investigations into voter suppression and election interference (Sherman, 2024). Similarly, a 2022 deepfake video of Ukrainian President Volodymyr Zelenskyy falsely announcing surrender to Russia highlighted the geopolitical implications of manipulated media during wartime (Vincent, 2022). In response, governments, researchers, and tech companies are developing detection tools and advocating for regulation.

Efforts include watermarking synthetic content, improving detection algorithms, and legislating the use and disclosure of AI-generated media (Mirsky & Lee, 2021; FTC, 2023). However, experts warn that the arms race between generation and detection is intensifying. As deepfake tools become more advanced and widely accessible, the ability to discern reality from fabrication grows increasingly difficult, posing threats not only to personal and organizational security but also to democratic institutions.

CASE STUDY 01: Deepfake Voice Scam: AI-Cloned CEO Voice Used to Steal \$243,000 in Corporate Fraud Case (2019)

Other risks A deepfake audio fraud attack was recorded as early as March 2019 when a U.K.-based subsidiary of a German energy company lost 243,000 due to one of the first known deepfake voice fraud attacks. The Wall Street Journal said the AI-powered voice synthesis technology led to the formation of the voice of the German parent company CEO by a group of cybercriminals. By simply analyzing a brief audio sample of the authentic voice of the CEO, probably pulled off of public record sources like interviews or speeches, the scammers were able to create a convincing audio deepfake of the executive that not only sounds like him, but also resembles the tone and a German accent as well as a vocal pattern. This was one artificial sound, by which the attackers called the CEO of the U.K. subsidiary and pretended to be the CEO of the parent company. During the fraudulent call, the impostor CEO ordered the U.K. executive to wire the money as soon as possible, the amount was approximately 243000- to a Hungarian supplier, stating that this was a time-sensitive reimbursement request in the fabricated conversation and that repayment would be coming soon. Relying on the voice and the context and acting as per the request, the U.K. executive transferred the funds. The money was, however, channelled fast through a Mexican bank account and other unknown countries; thus, investigators were unable to trace and reclaim the money. The fraudsters did not stop even there and then placed a second phone call via AI-generated voice, asking to make another payment again--they lied that the first one had already been reimbursed.



Fig. Deepfake: Sound like a Lier

The executive in the U.K., who was yet to know of the fraud, started getting insecure about the authenticity of the scenario owing to the difficulty he had in proving of the purported reimbursement. As soon as the attackers called the third time, with the phone numbers of Austria this time, the suspicions were raised, and the scheme was finally identified as a fake.

The threat of social engineering has undergone a paradigm transformation as seen in this case. In contrast to the classic phishing attempts, based on misleading emails or text-based fraud, the artificial intelligence voice clone capability along with genuine time real-time communication and impersonation based on human trust was used in this fraud. The fact that this scam was so successful was due to the psychological influence of a familiar high-authority voice telling instructions in real-time. The related chain-of-command trust in a corporate entity and the usual sense of urgency that comes with executive-level orders were used by attackers to their own benefit. Fraud was further concealed by use of international financial routing which made it hard to prosecute. It was one of the first deepfake audio applications in a documented financial fraud attempt and it is an early warning to the security of businesses in all industries where approvals of financial transactions are done over the phone or by voice. To prevent such and other similar occurrences, the people in cybersecurity started advising businesses to incorporate multi-factor verification methods involving financial transactions, including those made by top-level managers.

Preventing Deepfake Audio Fraud

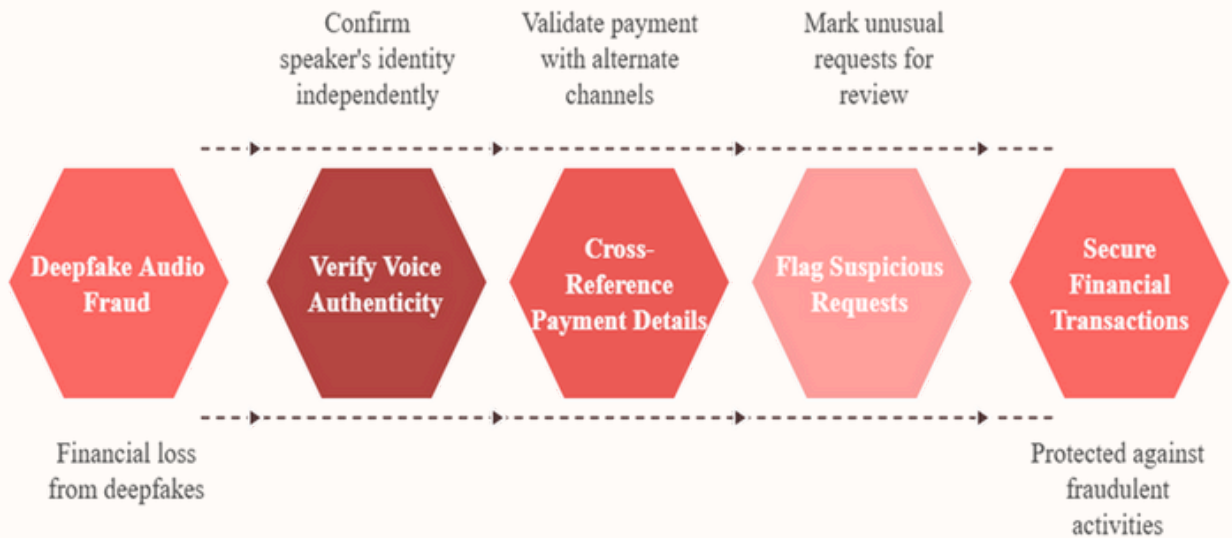


Fig. Precautions to be taken while dealing with any financial transaction

CASE STUDY 2: Deepfake Robocall of President Joe Biden Encourages Democrats Not to Vote in New Hampshire Primary

In January 2024, just before the Democratic primary in New Hampshire, an AI-generated robocall impersonating President Joe Biden was circulated, urging Democratic voters to stay home and not vote. The voice in the call sounded convincingly like President Biden and falsely claimed that voting in the primary would support Republicans, telling voters to “save” their votes for the November general election. The call sparked immediate concern over AI-driven voter suppression, as it appeared designed to mislead Democratic voters and suppress turnout in a critical state. New Hampshire Department of Justice verified that the voice was probably artificially produced, and call metadata was spoofed to look like a call placed by the treasurer of a political organization in support of Biden's write-in campaign. President Biden was not on the primary ballot (by the decision of the Democratic National Committee to favor South Carolina with changing the schedule of the early primaries), which is why a group of more than 100 Democratic leaders has been conducting a grassroots campaign urging people to write him in on their primary ballots.

The deepfake call, nevertheless, appeared to defy the process of spreading fake information. A variety of campaigns, including those of Biden, Trump, and opponent Dean Phillips, all denied any participation in the phone calls. Phillips has criticized the incident through her campaigning, terming it a shame to try to rig voters. It is quite actively investigated by the state authorities, and the case became a bright illustration of how AI-generating audio can be turned into electoral weaponry, posing a threat to the future of democratic integrity in the era of synthetic media. (12)



CASE STUDY 3: The racist AI deepfake that fooled and divided a community

In early 2024, a disturbing audio clip surfaced online, allegedly capturing Pikesville High School principal Eric Eiswert making a racist and antisemitic rant. The voice in the clip referred to “ungrateful Black kids” and made offensive remarks about Jewish people, sparking national outrage and death threats against the principal. The audio spread quickly across social media, reaching millions. Many in the Baltimore suburb of Pikesville, which has large Black and Jewish communities, believed the clip was real because the voice closely resembled Eiswert’s and used authentic school terminology like “grade-level expectations” and staff names. Principal Eiswert was placed on paid administrative leave as the community and media reacted. However, when education reporter Kristen Griffith reached out to his union, they immediately suspected the clip was fake and AI-generated. New Hampshire Department of Justice verified that the voice was probably artificially produced, and call metadata was spoofed to look a call placed by the treasurer of a political organization in support of Biden’s write-in campaign.

President Biden was not on the primary ballot (by the decision of the Democratic National Committee to favor South Carolina with changing the schedule of the early primaries), which is why a group of more than 100 Democratic leaders has been conducting a grassroots campaign urging people to write him in on their primary ballots. The deepfake call, nevertheless, appeared to defy the process of spreading fake information. A variety of campaigns, including those of Biden, Trump, and opponent Dean Phillips, all denied any participation in the phone calls. Phillips has criticized the incident through her campaigning, terming it a shame to try to rig voters. It is quite actively investigated by the state authorities, and the case became a bright illustration of how AI-generating audio can be turned into electoral weaponry, posing a threat to the future of democratic integrity in the era of synthetic media.

REFERENCES

- 1) Chesney, R., & Citron, D. K. (2019). Deep fakes: A looming challenge for privacy, democracy, and national security. *California Law Review*, 107(6), 1753–1819. <https://doi.org/10.2139/ssrn.3213954>
- Federal Trade Commission. (2023). Business and Government Impersonation Rulemaking. <https://www.ftc.gov>
- Kreps, S. (2023). The deepfake threat: A research agenda. *International Journal of Press/Politics*, 28(1), 143–165. <https://doi.org/10.1177/19401612221104895>
- Mirsky, Y., & Lee, W. (2021). The creation and detection of deepfakes: A survey. *ACM Computing Surveys*, 54(1), 1–41. <https://doi.org/10.1145/3425780>
- Neumann, D. L. (2021). The psychology of deepfakes: Why we believe what we hear. *Journal of Media Psychology*, 33(4), 215–226. <https://doi.org/10.1027/1864-1105/a000300>
- Sherman, R. (2024, January 22). Fake Biden robocall tells New Hampshire Democrats not to vote in primary. CBS News. <https://www.cbsnews.com/news/fake-biden-robocall-new-hampshire-democrats-not-to-vote-primary/>
- 7) Stupp, C. (2019, August 30). Fraudsters used AI to mimic CEO’s voice in unusual cybercrime case. *The Wall Street Journal*. <https://www.wsj.com/articles/fraudsters-use-ai-to-mimic-ceos-voice-in-unusual-cybercrime-case-11567157402>
- Vincent, J. (2022, March 16). Facebook and YouTube remove deepfake video of Ukrainian president surrendering. *The Verge*. <https://www.theverge.com/2022/3/16/22982292/deepfake-zelensky-video-facebook-youtube-removed>
- Villasenor, J. (2020). Artificial intelligence, deepfakes, and the uncertain future of truth. *Brookings Institution*. <https://www.brookings.edu/research/artificial-intelligence-deepfakes-and-the-uncertain-future-of-truth/>
- Westerlund, M. (2019). The emergence of deepfake technology: A review. *Technology Innovation Management Review*, 9(11), 40–53
- Stupp, C. (2019, August 30). Fraudsters used AI to mimic CEO’s voice in unusual cybercrime case.
- Sherman, R. (2024, January 22). Fake Biden robocall tells New Hampshire Democrats not to vote in primary.



ABOUT THE AUTHOR

Ms. Dharmistha Parmar

School of Forensic Science, National Forensic
Sciences University, Gandhinagar, Gujarat,
India.



Mr. Bhumit Chavda

Research Scholar, Department of Biochemistry and
Forensic Science, School of Science, Gujarat
University, Ahmedabad, India.



Genes, Machines, and Memories: Predicting Human Recall Through Genomics and AI Neural Mapping

Author: Shweta Javia, Kiran R Dodiya

Introduction

Are Our Memories Predictable?

Picture attending a lecture hall, a meeting, or even a family event—and also already knowing which names, explanations, or discussions will stay in your thoughts a week later, and which will be forgotten in the fog of oblivion. Close your eyes for a second and imagine that this insight is not from a gut feeling or pattern, but from an analytics reading of your DNA. Even with the futuristic feel of this notion, the latest breakthroughs in genomic science and artificial intelligence (AI) are coming together in a way that can make this a reality.

Memory was previously thought of as a vague function in the brain, simply due to chemical processes, but is now known to be intimately tied to our genetics. For example, specific genes affect the speed with which we form associations, the vividness of our memories, and how readily we forget — knowledge that scientists have known for decades. The field has evolved only recently to study the architecture of these patterns across the genome, through thousands of variants that together contribute to the way we remember.

The intricacy of this assignment is gigantic. Memory, therefore, is not the product of a single region of the brain or even a set of genes, but a symphony of neural, molecular, and environmental interactions that enable the ability to encode information at the right time and in the right place. That's where AI becomes essential. Taking advantage of large datasets—from brain images and cognitive tests to whole-genome sequences—AI can discern subtle patterns that no human being could ever find.

This nascent combination of neural mapping and genetic profiling, all supervised by machine learning, provides a never-before-possible glimpse into memory: literally, how it functions and how it differs for each individual. Instead, researchers are training AI models to identify the types of information a person is most likely to remember or forget by focusing on brain activity and genetics, as well as the real-time process and the genetic blueprint of information retention.

In this article, we explore the new and exciting frontier that lies at the intersection of biology and computation, and the far-reaching implications it has across various domains, including education, mental health, personalised therapy, and even forensic sciences. Or, could we one day design education to suit our genetic memory spectrum? Could AI identify how reliable the human memory of a witness is? The reasons may lie right before us.

The Biological Roots of Memory

One of the brain's most enigmatic and remarkable capabilities is human memory. It is based on such things as:

1. Neurotransmitters (like dopamine, glutamate),
2. Consolidated neural connectivity (particularly in the hippocampus and prefrontal cortex),
3. Synaptic plasticity (the ability of neurons to make connections stronger or weaker),
4. And, perhaps to some, heritable variation.

One of the most miraculous and bizarre functions of the brain is memory. Our history is at the core of our very being—our identity, our decision-making, and our learning from the past. Although remembering may seem simple on the surface, the underlying biology is mind-bogglingly complex. Memory is not merely a function of a single neural region, or even a particular neurotransmitter or class of neurotransmitters, but rather the net result of a precisely co-ordinated balance between neurotransmitters, connectivity between neurons, the properties of synapses, and potentially, but perhaps least surprisingly, the genetic predisposition of the individuals themselves. Central to memory formation are neurotransmitters, such as dopamine and glutamate, which serve as chemical messengers. Dopamine is key for reward-based motivation and learning, whereas glutamate is vital for synaptic transmission and strengthening neuronal connections. These neurotransmitters function over large networks of neurons, regulating communication between brain areas important for memory, often including the hippocampus (which stores new memories) and the prefrontal cortex (which controls working memory and decision-making).

Biological Roots of Memory

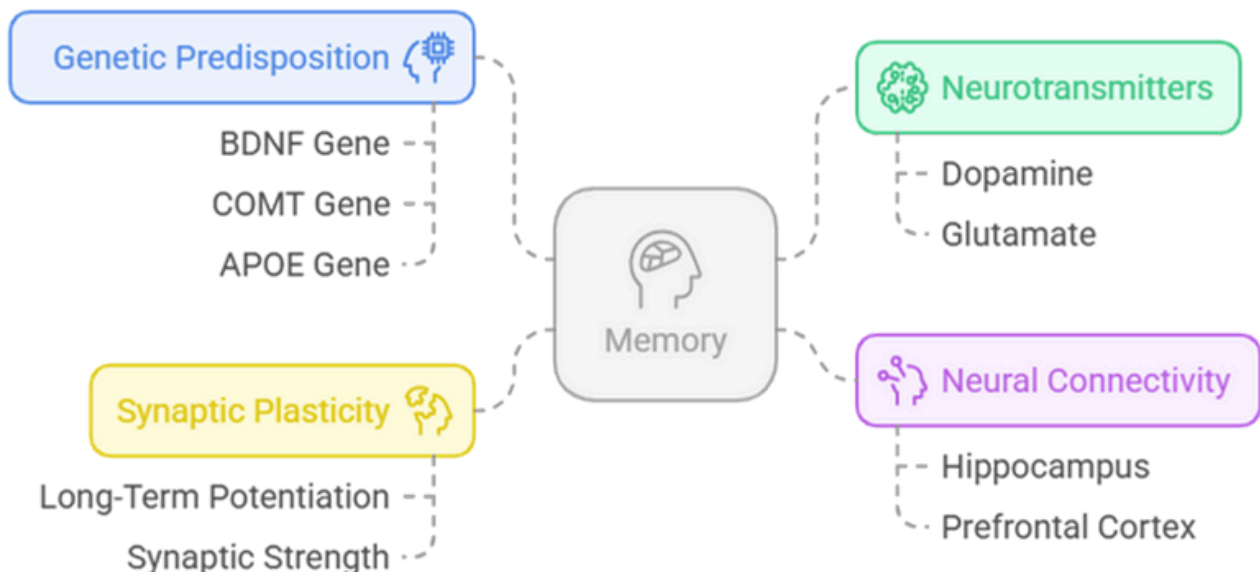


Figure : Biological Root of Memory

Neural connectivity is the interaction between these regions. For memory to function on a practical level, the connections between the hippocampus, amygdala, and neocortex need to be intact. The encoding and retrieval of memories, which happens through a series of interconnected neurons, can be severely disrupted due to injury, disease, or developmental factors. A key property of such networks is synaptic plasticity, the brain's remarkable ability to strengthen or weaken synaptic connections between neurons in response to experience. Long-term potentiation (LTP), a long-lasting increase in synaptic strength induced by high-frequency stimulation, is among the best-studied processes thought to mediate learning and memory [2–5]. The neural factors involved in memory have been studied within cognitive neuroscience for decades; however, genetic factors are relatively new topics of research in this field. Over the last decade, research has demonstrated that potent environmental inputs or learning strategies do not solely determine memory capacity; instead, the genetic architecture of memory capacity also plays a significant role in determining it. Some genes affect the production or metabolism of neurotransmitters, the functioning of synaptic plasticity, and even the development and connectivity of neurons. One example is the BDNF (Brain-Derived Neurotrophic Factor) gene, a key regulator of neuronal survival and synaptic plasticity. For example, variation in the BDNF gene, particularly the Val66Met polymorphism, is associated with differences in memory performance and brain volume.

The COMT (Catechol-O-methyltransferase) gene is implicated in dopamine metabolism in the prefrontal cortex, affecting working memory and cognitive flexibility. Another vital gene, APOE (Apolipoprotein E), particularly the $\epsilon 4$ allele, is associated with memory impairment and an increased risk of Alzheimer's disease in older adults.

Nonetheless, these genes are only a small part of the genomic landscape of memory. Traits that govern memory are polygenic, meaning they originate not from a single gene but rather from the interplay of dozens or even hundreds of genes, each with a subtle effect. Thus, signalling through these numerous networks of genetic interactions, modified by environment, experience, and epigenetic factors (and many other modifiers), will determine the unique memory profile of each individual.

Grasping this complexity requires not only biological intuition but also robust computational technologies. Genomics, when combined with artificial intelligence, provides a revolutionary opportunity to unravel the complex genetic blueprint of memory in humans.



What Does the Genome Reveal About Memory?

Over the past few decades, genetic studies have sought to determine the biological basis of memory by identifying a single gene that they believed could have a significant impact on cognitive ability. Individual genes that support synaptic plasticity, such as BDNF (Brain-Derived Neurotrophic Factor), and those that influence dopamine, such as COMT, have been found to contribute to memory formation and recall. However, the pathogenesis of human memory appears to be too complex, and it is determined not only by multiple genes but also by epigenetic and environmental factors.

Currently, research is shifting increasingly towards polygenic scoring, which evaluates all genetic variants in the genome and their combined effect on phenotype. These polygenic scores (PGS) measure the overall genetic component of traits such as working memory, verbal recall, and learning efficiency. Whereas legacy models focused on the effects of individual genes, polygenic scores provide a systems-level, probabilistic picture of how biology related to memory is encoded in our DNA.

Even more intriguing is that the majority of the genes that influence memory are not in the 1-2% of our DNA that encodes proteins. Instead, scientists are discovering essential functions for non-coding sequences, previously thought to be "junk DNA." These regions have since been found to control the timing, location, and manner in which genes are expressed, often acting like a genetic on/off switch or enhancer. Most of these regulatory elements are broadly active during neurodevelopment and synaptic remodelling, which are key for memory formation and retrieval.

Simultaneously, epigenetic mechanisms have also come into view due to their influence on memory potential. Epigenetics is concerned with chemical changes in DNA, such as methylation of DNA or acetylation of histones, that lead to alterations in gene expression and function, but do not alter the DNA sequence itself. That is, epigenetic influences such as stressful life events, chronic trauma, enriched environments, and intensive learning appear to leave marks that, in turn, enhance or suppress the expression of essential genes involved in memory. Early-life stress has also been implicated in prolonged alterations in gene transcription related to hippocampal gene expression, negatively impacting memory well after early life.

Other genes related to synaptic pruning (the elimination of weak or unused neuronal connections), neurogenesis (the formation of new neurons), and myelination (the insulation of nerve fibres, allowing for faster signal propagation) are also known to affect variability in learning and memory. Changes in these genes can modulate the encoding or retrieval of information in a more or less rapid or precise manner. Inefficient pruning during adolescence may lead to cognitive overload; impaired myelination in adulthood may result in slower recall.

The genome serves as a renewable resource for memory, but it is encoded in a distributed, dynamic language that encompasses coding genes, regulatory elements, and epigenetic signals. This construct is complex and highly individualised, such that two people, even with similarly appealing associative experiences, might later remember the events quite differently based on their inherent genetic and epigenetic predispositions.

This raises the question of how to interpret this blueprint to predict memory behaviour in the real world. And that is where artificial intelligence comes in, the mighty interpreter of what this huge biological language means.

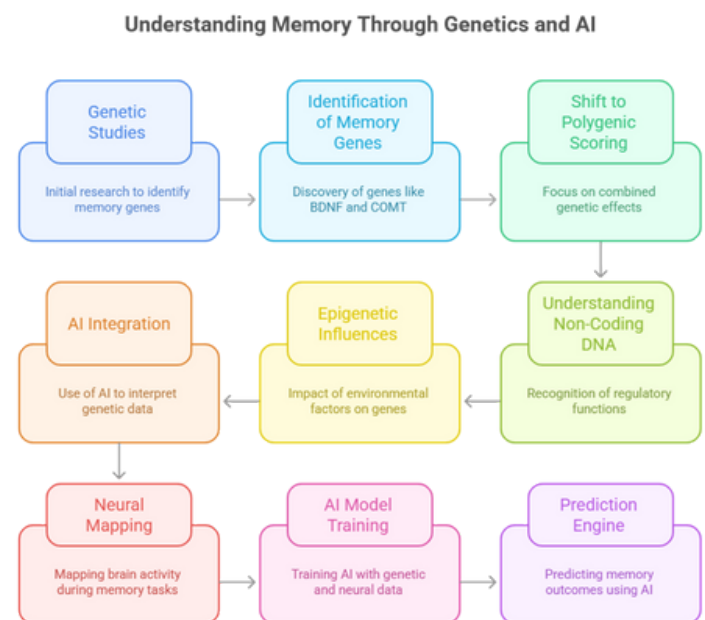


Figure : Genetics and AI roadmap for predicting memory performance.

Case Studies: Lab-Based Use Cases into the Real World

Several trailblazing research studies will underpin this predictive feature: Study Sample One, "AI Combined with Genomics in Education."

Study Example 1: A 2022 study from Stanford and MIT utilised polygenic risk scores in conjunction with EEG data to predict performance on retention tests of scientific content taught in video lectures to students. According to neural responses driven by gene expression, the AI system accurately predicted quiz performance one week later, with an accuracy of better than 80%.

Study Example 2: Decoding Memories in PTSD Treatment
In Sweden, a team used AI to examine recordings from brain areas that communicate with the hippocampus, as well as DNA methylation data in PTSD patients. This allowed them to predict which patients would respond to exposure-based therapy, yielding a strategy for a personalised approach to mental health based on biology.

Study Example 3: Forensic Implications
Could a witness's solemn genetic and neural profile indicate whether they truthfully remember an event or not? If true, this technique could be a game-changer for legal psychology, with preliminary experiments suggesting that memory reliability can be quantified.

Ethical Issues: Is It Going Too Far to Predict Memories

Or, as they say, great power, great responsibility. But if AI can somehow predict your genome to know what you will or won't remember of it, we are in big, horrible trouble.

Privacy - should such cognitive predictions about our future be available to schools, employers, or governments?

Genetic discrimination: Would some of us be stigmatised or left out if we all got a genetic score showing a "low memory potential"?

Consent: How do we make sure that people are informed about what it means to share genomic and neural data?

But perhaps the most critical question is: Do AI models even respect the unpredictability of human experience and learning? While prediction will always be beneficial, there will always be a need for humanity, subtlety, emotion, and the uniqueness of humans, argue experts. We need augmentation, not automation of understanding.

AI Use Cases in Research Studies





Characteristic	Study Sample One	Decoding Memories	Forensic Implications
 Objective	Predict quiz performance	Predict therapy response	Quantify memory reliability
 Data Used	Polygenic risk scores, EEG data	Brain recordings, DNA methylation	Genetic and neural profile
 Accuracy	Better than 80%	Not specified	Not specified
 Potential Impact	Personalized education	Personalized mental health	Legal psychology

Figure :AI applications in memory research: objectives, data, accuracy, and impacts.

Advancing Memory Enhancement

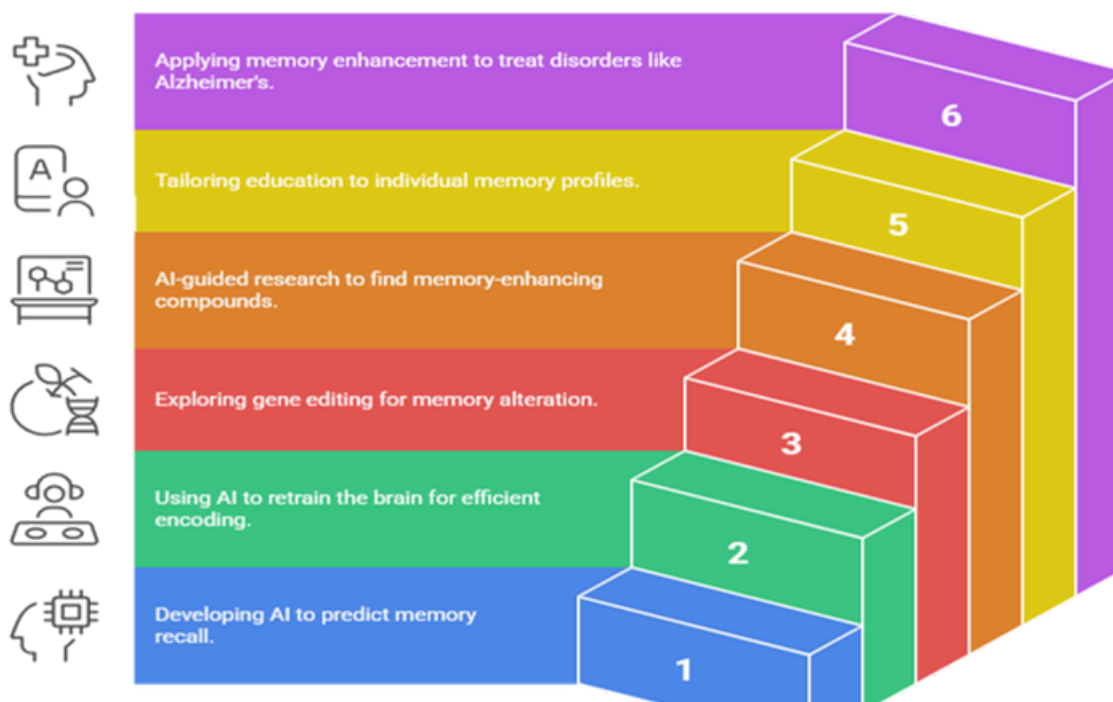


Figure : Steps toward AI-driven memory enhancement and therapeutic applications.

The Future: From Prediction To The Study Of The Enhancement?

Having cracked the code on how to predict memory recall using AI, the next logical question is: Can we enhance it?

AI-powered neurofeedback systems have been developed that teach people to "retrain" the brain to respond more efficiently during encoding.

And in the more distant future? Gene-editing tools, although still controversial in the case of human beings, could one day permit the alteration of memory-related genes.

Nootropics research funded and guided by AI will focus on being able to find the perfect compounds to fit a genetic' memory profile'

Not only does this offer hope of assistance to victims of memory disorders, such as Alzheimer's, but it could also enable personalised learning, therapy, and even creativity augmentation.

Conclusion: Never Forget the Human Touch

Memory is deeply personal. It both shapes and describes us, how we interact with the world, and what we have in store for ourselves moving forward. The combination of genomics and AI neural mapping presents astonishing potential—not just to comprehend memory, but to honour it, advance it, and sustain it.

But as algorithms can chart a membrane of firing neurons and patterns of genes, they cannot (yet) contextualise the emotional weight of a memory, the narrative it conveys, or the significance it embodies. Well, maybe only a human can do that?

So the next time you forget a name or remember the smell of your childhood, remember that behind that blink of existence lies the world of atoms, genes, and neurons — and now, a little bit of our artificial intelligence.

References:

- Kandel, E. R. (2001). The Molecular Biology of Memory Storage: A Dialogue Between Genes and Synapses.
- Satterthwaite, T. D., & Bassett, D. S. (2019). "Deep Learning of Brain Connectivity." Neuron.
- Luber, B., & Lisanby, S. H. (2014). "Enhancement of Human Cognitive Performance Using Transcranial Magnetic Stimulation (TMS)."
- Toga, A. W., & Thompson, P. M. (2005). "Mapping Brain Function with Genetics and Neuroimaging."
- Nature Neuroscience, Special Issue on "AI and Human Cognition" (2022).

ABOUT THE AUTHOR

Shweta Javia

B.R Doshi School of Bioscience, Sardar Patel University, Vallabh Vidyanagar, Gujarat, INDIA



Kiran R Dodiya

Research Scholar, Department of Biochemistry and Forensic Science, Gujarat University, Ahmedabad, Gujarat, INDIA



Stalker ware: The Silent Threat to Digital Privacy

Author: Balaji M

Introduction

When Air India Flight AI-171 took off from Ahmedabad's Sardar Vallabhbhai Patel International Airport on the morning of June 12, 2025, it was expected to be just another routine journey. But within moments, tragedy struck. The aircraft crashed into the boy's hostel of a medical college barely two kilometers from the runway, erupting into a fireball that claimed the lives of 241 passengers and several people on the ground. In the aftermath, rescue workers were met with a grim scene- bodies severely charred, personal belongings incinerated, and wreckage scattered across the site.

In such devastating circumstances, where visual identification is impossible and fingerprints often burned beyond retrieval, a lesser-known branch of forensic science quietly stepped into the spotlight: forensic odontology. Armed with dental charts, molars, and unwavering precision, forensic odontologists took on the monumental task of restoring identity to the unidentified.

This article explores the vital, often overlooked role of forensic odontology in mass fatality incidents, with a particular focus on how it helped families in Ahmedabad find closure amid unspeakable loss. From its scientific roots to its deeply human impact, forensic odontology proved to be more than just a tool of investigation - it became a bridge between tragedy and healing.

What is Forensic Odontology

Forensic odontology is a specialised field within forensic science that focuses on analysing dental evidence to aid in both legal and investigative contexts. One of its most crucial roles is identifying deceased individuals through their dental characteristics. Much like fingerprints, each person's dental profile, including tooth structure, alignment, restorations, and orthodontic work, is entirely unique. These distinctive traits serve as a dental "blueprint," allowing forensic experts to match remains with missing individuals when other methods fall short.

Signs of Stalkerware Infection

Detecting stalkerware can be challenging due to its stealthy nature. However, there are several warning signs that may indicate its presence:

- Unusual battery drain, as stalkerware runs continuously in the background
- The device turning on or off unexpectedly
- Changes in settings or unfamiliar apps with suspicious permissions
- An unexplained surge in data usage
- Someone displaying an unusual knowledge of your whereabouts or private communications[1][3]

Victims may also notice that an abuser has or had physical access to their device, or that they received a "gift" phone or tablet, which could have come pre-installed with stalkerware[3][4].

Risks and Impacts

The risks associated with stalkerware are profound and multifaceted:

- **Privacy Violation:** Victims lose control over their personal information, communications, and movements.
- **Physical Safety:** In cases of domestic violence, stalkerware can enable abusers to track and harm victims.
- **Psychological Harm:** The constant surveillance can cause anxiety, fear, and trauma.
- **Data Security:** Disabling built-in security features to install stalkerware can expose devices to additional malware and cyber threats[4][2].



Legal and Ethical Considerations

The use of stalkerware without the explicit consent of the device owner is illegal in many jurisdictions, constituting a violation of privacy laws and, in some cases, anti-stalking statutes. However, enforcement is complicated by the software's stealthy nature and the difficulty of proving its presence and use. Some manufacturers attempt to skirt legal issues by marketing their products for "legitimate" uses, but the potential for abuse remains high[2].

Detection and Removal

How to Detect Stalkerware:

There is no foolproof method for detecting stalkerware, but the following steps can help:

- **Check for Unusual Behavior:** Monitor for rapid battery drain, high data usage, and device instability.
- **Review Installed Apps:** Look for unfamiliar or suspicious apps, especially those requesting extensive permissions.
- **Update Device Software:** Keeping the operating system and applications updated can close vulnerabilities exploited by stalkerware.
- **Use Security Tools:** Install reputable anti-virus or anti-stalkerware apps that can scan for and remove malicious software[1][3][4].

What to Do if You Suspect Stalkerware

If you suspect your device is compromised:

- **Do Not Confront the Abuser Directly:** Removing stalkerware may alert the perpetrator, potentially escalating the situation.
- **Seek Professional Help:** Contact a digital security expert or a local support organization specializing in domestic violence or cybercrime.
- **Preserve Evidence:** If you plan to pursue legal action, avoid tampering with the device until evidence can be documented.
- **Consider a New Device:** In severe cases, it may be safer to switch to a new device with a fresh operating system install[3][4].

Prevention Strategies

Protecting Your Device:

- **Physical Security:** Always know where your device is and avoid leaving it unattended.
- **Strong Authentication:** Use a unique passcode or biometric security. Do not share your credentials.
- **Account Security:** Change passwords regularly and enable multi-factor authentication on all accounts.
- **Limit App Installations:** Only install apps from official app stores and avoid enabling installations from unknown sources.
- **Avoid Rooting or Jailbreaking:** These practices disable built-in security features, making devices more vulnerable to stalkerware[4].

Responding to Gifts or Device Access

Be cautious of "gifted" devices, especially from individuals with a history of controlling behavior. If someone insists on "fixing" or "updating" your device, be wary, as this could be an opportunity to install stalkerware[3][4].

The Role of Technology Companies and Policy

Technology companies and app stores have begun to take action against stalkerware, removing known malicious apps and improving detection mechanisms. However, the responsibility also lies with policymakers to strengthen legal frameworks and with users to remain vigilant.

Conclusion

Stalkerware is a silent but pervasive threat to digital privacy and personal safety. Its misuse in abusive relationships and stalking cases underscores the urgent need for awareness, prevention, and robust legal protections. By understanding the risks, recognizing the warning signs, and adopting proactive security measures, individuals can better protect themselves against this insidious form of surveillance.

References

1. Kaspersky. What is Stalkerware? [Internet]. 2024 Dec 14 [cited 2025 Jun 26]. Available from: <https://www.kaspersky.com/resource-center/definitions/what-is-stalkerware>
2. Federal Trade Commission. Stalkerware: What To Know | Consumer Advice [Internet]. 2024 Apr 23 [cited 2025 Jun 26]. Available from: <https://consumer.ftc.gov/articles/stalkerware-what-know>
3. TechSafety.org. Spyware and Stalkerware: Phone Surveillance [Internet]. 2022 Jan 1 [cited 2025 Jun 26]. Available from: <https://www.techsafety.org/spyware-and-stalkerware-phone-surveillance>
4. Wikipedia. Stalkerware [Internet]. 2024 Dec 16 [cited 2025 Jun 26]. Available from: <https://en.wikipedia.org/wiki/Stalkerware>

ABOUT THE AUTHOR

Balaji M,
B.Sc. Forensic Science,
(Intern at Clue4 Evidence Forensic Lab Bengaluru)



“TEETH AMIDST THE FLAMES: FORENSIC ODONTOLOGY IN THE AFTERMATH OF THE AHMEDABAD AIR INDIA AI-171 CRASH”

Author: Chandana S S

Introduction

When Air India Flight AI-171 took off from Ahmedabad’s Sardar Vallabhbhai Patel International Airport on the morning of June 12, 2025, it was expected to be just another routine journey. But within moments, tragedy struck. The aircraft crashed into the boy’s hostel of a medical college barely two kilometers from the runway, erupting into a fireball that claimed the lives of 241 passengers and several people on the ground. In the aftermath, rescue workers were met with a grim scene- bodies severely charred, personal belongings incinerated, and wreckage scattered across the site.

In such devastating circumstances, where visual identification is impossible and fingerprints often burned beyond retrieval, a lesser-known branch of forensic science quietly stepped into the spotlight: forensic odontology. Armed with dental charts, molars, and unwavering precision, forensic odontologists took on the monumental task of restoring identity to the unidentified.

This article explores the vital, often overlooked role of forensic odontology in mass fatality incidents, with a particular focus on how it helped families in Ahmedabad find closure amid unspeakable loss. From its scientific roots to its deeply human impact, forensic odontology proved to be more than just a tool of investigation - it became a bridge between tragedy and healing.

What is Forensic Odontology:

Forensic odontology is a specialised field within forensic science that focuses on analysing dental evidence to aid in both legal and investigative contexts. One of its most crucial roles is identifying deceased individuals through their dental characteristics. Much like fingerprints, each person’s dental profile, including tooth structure, alignment, restorations, and orthodontic work, is entirely unique. These distinctive traits serve as a dental “blueprint,” allowing forensic experts to match remains with missing individuals when other methods fall short.

Why Teeth Matter in Disasters

Teeth are among the most resilient parts of the human body, often outlasting other tissues in extreme conditions like fires or natural disasters. This resilience comes from several factors. Enamel, the outer layer of teeth, is exceptionally heat-resistant, tolerating temperatures that would destroy most body tissues. Nestled within the jawbone, teeth are also naturally shielded from direct trauma. Additionally, their mineral-rich composition makes them resistant to decay in soil or water. These characteristics make teeth an invaluable asset in identifying victims when traditional markers such as fingerprints or facial features are no longer viable.

How Forensic Odontology identifies victims:

In large-scale disasters, where conventional identification methods are often rendered ineffective, forensic dentistry becomes indispensable. By examining a person’s dental traits—such as the number, position, and condition of teeth, as well as dental treatments like fillings or crowns—experts can recreate a unique dental profile. This information is then compared to pre-existing dental records to confirm identities, even when remains are heavily damaged or unrecognizable.

The step-by-step process forensic odontologists follow to identify victims, particularly in mass fatality incidents, include:



The step-by-step process forensic odontologists follow to identify victims, particularly in mass fatality include:

1. Post-Mortem Dental Examination

After a body or body fragment is recovered, it undergoes a post-mortem dental examination. This is usually conducted in a temporary morgue or forensic laboratory, and it involves:

- Inspecting the oral cavity and jawbones for any surviving teeth
- Counting and describing each tooth, including its condition (broken, restored, decayed, missing, etc.)
- Noting dental work such as Fillings (silver, composite, gold), Root canals, Crowns or bridges, Braces or implants
- Taking post-mortem dental X-rays (radiographs) for comparison with known records
- Extracting teeth with pulp (soft inner tissue) if DNA analysis is needed.

2. Collection of Ante-Mortem Dental Data

While the forensic team works on the remains, another team contacts the victims' families to obtain ante-mortem dental records created while the person was alive. These "ante-mortem" records might include clinical notes, previous X-rays, orthodontic treatment files, dental bills, or even photos showing visible dental features. In some instances, casual photographs—like a wedding picture showing a gold tooth—can be unexpectedly useful in narrowing down identity.

3. Comparison and Matching

Once both sets of data - post-mortem and ante-mortem are in hand, forensic odontologists begin the meticulous task of comparing them.

- Visual and structural comparison involves matching the number, position, and appearance of teeth and restorations.
- Radiographic overlays are used to compare the shape of tooth roots, bone patterns, and any dental appliances like implants or braces.
- In some countries, scoring systems are used to quantify the match between records, helping determine the certainty of identification.

4. DNA Extraction from Tooth Pulp

If no ante-mortem records are available or the dental comparison is inconclusive, teeth can still help. Tooth pulp, the soft tissue inside the tooth, is well-protected and often survives fire and decomposition.

From it, forensic experts can:

- Extract nuclear or mitochondrial DNA
- Compare it to reference samples from family members (parents, children, or siblings)

Confirm or exclude identity with high accuracy

This method was used in the Ahmedabad plane crash when dental records were unavailable, and families provided buccal swabs for comparison.⁵ Confirming the Identification

Once a positive match is made, either through dental features or tooth-based DNA, the identification is confirmed. The result is usually submitted in a formal report including: Dental charts, X-rays (ante-mortem and post-mortem), Photographs, Comparative analysis.

FROM ASHES TO IDENTITY: THE PROCESS FOLLOWED IN THE AHMEDABAD PLANE CRASH:

When the wreckage of Air India Flight AI-171 was finally cleared, what remained was not just twisted metal and charred belongings, but over 240 lives reduced to fragile fragments—burned, broken, and beyond recognition. Amid this haunting aftermath, teams of forensic experts began the delicate process of identification. Among them, the forensic odontologists played a critical role.

3.1 The Experts Who Answered the Call

As rescue workers collected remains from the crash site near Ahmedabad's Sardar Vallabhbhai Patel International Airport, Dr. Jayasankar P Pillai, a veteran forensic odontologist from the Government Dental College, Ahmedabad, knew time was critical. He immediately sent out a message to his current and former students requesting assistance. Within hours, over 50 dental professionals and students responded and reported to the hospital mortuary. Among them were Dr. Tamanna Parmar, Dr. Real Bharambhatt, and Dr. Ritika Patel, young dentists who had never encountered a mass disaster before but worked tirelessly in challenging emotional and physical conditions. Under the leadership of Dr. Jayasankar P. Pillai, the team of dental professionals from Government Dental College, Ahmedabad, focused not just on dental charting but on extracting the inner tissue of the tooth—the pulp, which contains

high-quality DNA even in the harshest conditions. They carefully selected molars and premolars with intact roots, sterilized them, and skillfully cracked them open to retrieve the pulp. In child victims, unerupted molars were surgically removed from within the jawbone—a process that was emotionally heavy, yet scientifically critical. These precious DNA samples were transported to the Gujarat Forensic Science Laboratory in Gandhinagar, where a dedicated 54-member team, including 22 women scientists, worked around the clock under the direction of FSL chief H.P. Sanghvi. Using advanced DNA extraction and amplification techniques, the genetic material was analyzed and compared with buccal swabs and blood samples collected from family members. This process not only demonstrated the biological resilience of teeth but also served as a powerful reminder of how modern forensic science, grounded in compassion and precision, can restore identity and dignity even in the face of overwhelming tragedy.



CHALLENGES FACED BY FORENSIC ODONTOLOGISTS IN MASS DISASTERS

While forensic odontology plays a crucial role in identifying victims of mass disasters, the professionals working in this field often operate under extremely difficult conditions. Their task extends beyond scientific precision and requires mental endurance, emotional strength, and logistical flexibility. The following are the key challenges they frequently face:

11. Condition of the Remains

In aviation crashes or fire-related incidents, human remains are often exposed to extreme heat and physical trauma. Teeth may be fractured, dislodged, or burned, making recovery and examination more complicated. In some cases, only small fragments of the jaw or isolated teeth are available, requiring meticulous handling to extract usable information.

2. Non-Availability of Ante-Mortem Dental Records

Successful identification through dental methods relies heavily on the availability of ante-mortem dental records. However, in many parts of the world, routine dental visits are uncommon, and records may not be maintained properly. Families may also struggle to recall the name of the deceased's dentist, further delaying the process.

3. Time Pressure and High Expectations

During disaster response efforts, forensic teams face intense pressure to identify victims quickly. Families, authorities, and the media often expect rapid results, which places an emotional and operational burden on the team. Despite the urgency, odontologists must remain precise, as errors in identification can have serious consequences.

4. Emotional and Psychological Impact

Working with severely damaged remains, especially those of children can take a psychological toll. For many young professionals or students involved in these operations, it may be their first encounter with mass casualties. Long working hours, combined with emotional exhaustion, can lead to stress and compassion fatigue.

5. Inadequate Infrastructure and Equipment

In many disaster zones, proper dental equipment such as portable X-ray machines or sterilized instruments may not be readily available. Makeshift setups can hinder detailed analysis, and the lack of adequate space or preservation facilities for biological samples may compromise the quality of the investigation.

7. Ethical and Legal Responsibilities

The identification process must be handled with utmost accuracy and professionalism. Mistaken

can cause further trauma to families and lead to legal complications. Odontologists are responsible for preparing evidence-based, legally acceptable documentation and maintaining confidentiality throughout the process.

8. Health and Safety Risks

In certain disaster situations, such as those involving biohazards, infectious disease outbreaks, or unsafe environments, odontologists may face personal health risks. Ensuring safety through protective gear and adherence to protocols becomes essential while carrying out their duties.



CONCLUSION

The Ahmedabad plane crash was a moment of unimaginable loss, but within that darkness, forensic science illuminated a path to truth. At the heart of this response was forensic odontology, a field often overlooked, yet vital when all other methods fail. Through the quiet precision of tooth pulp DNA extraction, experts were able to return names to the nameless and bring a measure of peace to grieving families. This tragedy served as a powerful reminder that identity is more than appearance - it is encoded deep within us. The success of this mission stands as a testament not only to the strength of modern forensic techniques but also to the dedication of those who work behind the scenes, often unnoticed. As we move forward, this case should inspire greater investment, training, and recognition in the field of forensic odontology, so that science can continue to serve humanity with accuracy, dignity, and compassion.

REFERENCES

1. Senn DR, Weems RA, editors. Manual of forensic odontology. CRC press; 2013 Jan 22.
2. Debnath N, Gupta R, Nongthombam RS, Chandran P. Forensic odontology. Journal of Medical Society. 2016 Jan 1;30(1):20-3.
3. Saxena S, Sharma P, Gupta N. Experimental studies of forensic odontology to aid in the identification process. Journal of forensic dental sciences. 2010 Jul;2(2):69.
4. Prajapati G, Sarode SC, Sarode GS, Shelke P, Awan KH, Patil S. Role of forensic odontology in the identification of victims of major mass disasters across the world: A systematic review. PloS one. 2018 Jun 28;13(6):e0199791.
5. Shenoy M. Role of forensic odontology in the identification of victims of mass disaster: A systematic review. J. Res. Med. Sci. 2022 May;10(1).
6. Sharon E, Engel I, Beyth N, Malihi L, Kahana T. Insights from the 7th of October Massacre: Forensic Odontology in Mass Disasters. Forensic Science International. 2025 Feb 5;112394.

ABOUT THE AUTHOR



Chandana S S

M.Sc. FORENSIC SCIENCE

JUNIOR FACULTY at CASE 23: Forensically Yours

A Lifelong Commitment to Forensic Medicine and Justice

An interview with “Dr. Uma Maheswara Rao Pothula”, the Professor & Head of the Department of Forensic Medicine & Toxicology at Rangaraya Medical College, Kakinada.

When you meet Dr. Uma Maheswara Rao Pothula, the Professor & Head of the Department of Forensic Medicine & Toxicology at Rangaraya Medical College, Kakinada, you are immediately struck by his humility despite an illustrious career spanning over two decades. An acclaimed academician, seasoned medico-legal expert, and a mentor to generations of forensic doctors, Dr. Pothula has dedicated his life to ensuring that forensic science serves its ultimate purpose—truth and justice.

The Journey into Forensic Medicine

Dr. Pothula's foray into Forensic Medicine was driven by a deep fascination for medico-legal cases and the role of science in uncovering the truth behind unnatural deaths.

“Forensic Medicine is a unique branch that stands at the intersection of medicine and law. The fact that my scientific opinion can influence justice delivery motivated me to choose this field,” he says.

After completing his M.D. in Forensic Medicine & Toxicology, Dr. Pothula began his academic career and has since served as a teacher, researcher, examiner, and policy contributor in forensic education across multiple universities in India.

Two Decades of Teaching Excellence

With 20 years of experience in undergraduate medical education and 14 years as a postgraduate teacher, Dr. Pothula is regarded as an exceptional academician. His teaching philosophy revolves around practical learning and critical thinking.

“One of my proudest moments as a teacher was introducing real-life medico-legal case discussions for undergraduates. It helped students connect textbook knowledge with practical medico-legal

challenges,” he shares.

As a Ph.D. guide at Dr. YSR University of Health Sciences, he emphasizes scientific rigor, ethical reasoning, and a questioning attitude among his students, encouraging them to push the boundaries of forensic research.

Shaping Forensic Education in India

Dr. Pothula's expertise goes beyond the classroom. He is a member of multiple Boards of Studies for undergraduate and postgraduate forensic medicine programs, including at Dr. NTR University of Health Sciences, Andhra Pradesh and Adikavi Nannaya University, Rajamahendravaram.

He has also served as an examiner and question paper setter for several prestigious universities, including NTRUHS, RGUHS, KHUS, and Odisha universities.

Speaking about the changes needed in forensic education, he stresses the importance of modern learning tools.

“We need to integrate digital simulation, mock autopsies, and crime scene visits into medical education. Exposure to real-life medico-legal work is crucial for building competent forensic experts,” he notes.



Research and Publications

Dr. Pothula has authored numerous research articles in reputed national journals. Among them, his work on toxicological patterns in rural poisoning cases is particularly close to his heart.

“This research helped identify poisoning trends in rural areas and improved treatment protocols, which saved lives,” he proudly says.

Recognitions and Awards

Over the years, Dr. Pothula has received several honors, including being awarded Best Medical Officer thrice by the District Collector and the prestigious Lifetime Achievement Award by the Indian Academy of Forensic Medicine.

“While awards are gratifying, my real satisfaction comes from knowing that my forensic reports or testimonies have helped courts deliver justice,” he says with characteristic humility.

Challenges in Forensic Medicine Today

Despite significant advancements, forensic medicine in India faces its share of hurdles. According to Dr. Pothula, lack of infrastructure, insufficient trained manpower, and delayed medico-legal processes remain major concerns.

He advocates for better collaboration between forensic experts, law enforcement, and the judiciary, along with policy reforms to make forensic evidence handling faster and more scientific.

Vision for the Future

Dr. Pothula envisions a transformative decade ahead for forensic medicine, driven by DNA technology, advanced toxicology, and digital autopsies.

“India must prioritize the establishment of state-of-the-art forensic laboratories, invest in continuous training programs, and revise medico-legal protocols to match global standards,” he emphasizes.

One of his significant contributions has been the establishment of a Toxicology Laboratory at Rangaraya Medical College, Kakinada—the first of its kind in Andhra Pradesh.

With the constant encouragement and support of Dr. DSVL Narasimham (former Principal) and Dr. Vishnu Vardhan (former Vice Principal and current Principal), this laboratory is envisioned to develop into a Poison Control Centre, which will play a crucial role in managing and treating poisoning cases effectively.

Message to Young Forensic Aspirants

For students and young professionals, Dr. Pothula offers a simple yet powerful message:

“Be curious, ethical, and committed to justice. Forensic medicine is not just a profession—it’s a social responsibility. Keep learning, stay updated, and never compromise on scientific integrity.”

A Legacy of Dedication

Even after an illustrious career, Dr. Pothula remains deeply passionate about his work.

“My motivation comes from my students and the knowledge that every medico-legal opinion I give contributes to justice,” he concludes.

Through his unwavering dedication to teaching, research, and medico-legal service, Dr. Uma Maheswara Rao Pothula continues to inspire future generations of forensic professionals—proving that forensic medicine, when practiced with integrity, is indeed a noble science in service of justice.





Dr. Uma Maheswara Rao Pothula, Professor and Head of the Department of Forensic Medicine & Toxicology at Rangaraya Medical College, Kakinada, one is instantly impressed by his humility, which belies a distinguished career spanning more than two decades. A respected academician, an experienced medico-legal expert, and a guiding force for countless forensic professionals, Dr. Pothula has consistently dedicated his work to upholding the core values of forensic science truth and justice.

***INTERVIEWED BY
Mr. Thushar K.C
(Assistant Professor- Forensic Science)
Aditya University , Surampalem***



BLOCKCHAIN AND DATA PRIVACY: CONFLICT OR COMPLEMENT?

Author - Shruti Bamboria, Kiran R Dodiya, Dr. Kapil Kumar

Abstract

Blockchain technology has emerged as a powerful tool for ensuring data integrity, transparency, and security across decentralised systems. However, its foundational principles—particularly immutability and openness—can stand at odds with modern data privacy regulations that emphasise control, consent, and the right to be forgotten. This article explores the complex relationship between blockchain and data privacy, highlighting the tensions, technological innovations aimed at resolving them, and real-world applications where both can coexist. Ultimately, it examines whether blockchain and data privacy are inherently incompatible or if they can evolve together as complementary forces shaping the digital future.

1. Opening the Block: A New Era of Digital Trust

Blockchain technology is increasingly recognised for its potential to foster digital trust by enhancing transparency, safety, and decentralisation. Central to the blockchain's appeal is its intrinsic transparency; each transaction is recorded on a public ledger, making it accessible to verification. This visibility reduces the probability of fraudulent activity, as interested parties can independently verify the data without relying on intermediaries.(Shin, 2019). In addition, the security offered by the blockchain derives from its cryptographic foundation, which safeguards the integrity of the data and prevents unauthorised alterations. Decentralisation is another fundamental feature of the blockchain, distributing control over a network of nodes instead of a single authority. This mitigates the risks associated with centralised systems, such as data violations and corruption.(Shin, 2019).

The implications of Blockchain technology are large-scale, affecting various sectors, including finance, supply chain management, and healthcare. In finance, blockchain technology facilitates secure peer-to-peer transactions and reduces the costs associated with the traditional banking sector.

In managing the supply chain, greater transparency enables real-time monitoring of products, enhancing responsibility and efficiency. In healthcare, the secure sharing of patient data through blockchain can lead to improved outcomes while maintaining patient privacy and confidentiality. Overall, Blockchain technology represents a transformative force in the modern digital landscape, promoting trust and integrity across various sectors.(Shin, 2019).

2. What is So Private About Your Data Anyway?

In the digital age, data privacy has emerged as a crucial issue that encompasses the delicate interplay between personal security, consumer rights, and the responsibilities of companies and governments. As individuals are increasingly dependent on digital platforms, their personal information becomes more vulnerable to misuse and unauthorised access, raising concerns about personal security. (Henderson & Snyder, 1999). The implications of data privacy extend beyond individual interests, impacting consumer rights. Consumers should be confident that their data will be handled responsibly by companies, fostering trust in technology and the market. (Henderson & Snyder, 1999).



Governments play a key role in establishing regulations that protect personal information and promote responsibility among companies. Legislative structures, such as the General Data Protection Regulation (GDPR) in the European Union, aim to strike a balance between consumer rights and the operational needs of businesses. However, companies' ethical responsibility to protect consumer data should be prioritised to avoid violations that compromise personal security. Thus, the challenge is to forge a collaborative relationship among stakeholders—consumers, corporations, and governments—while ensuring that individual privacy is respected, leading to a safer and more equitable digital landscape. This balance is crucial in fostering a culture of trust and responsibility in an increasingly interconnected world. (Henderson & Snyder, 1999)

3. Blockchain 101: How the Tech Works (Without the Jargon)

Blockchain technology is a system that enables the secure storage of information across multiple computers, ensuring transparency and integrity. In its centre, it consists of three key components: blocks, chains and nets. Each “block” is like a digital file containing data, while the “chain” is a sequence of these blocks connected. This connection ensures that once the information is recorded, it cannot be easily changed, thereby promoting trust. The “network” involves all computers participating and verifying transactions, ensuring that each participant has access to the same information. (Laurence, 2023).

The primary functions of Blockchain technology include ensuring the security of financial transactions, tracing the origin of goods, and facilitating smart contracts. With its decentralised nature, Blockchain removes the need for a central authority, allowing peers to commit themselves directly to each other. (Laurence, 2023). This is significant because it not only reduces costs but also improves safety, as there is no single point of failure. In addition, the transparency offered by Blockchain systems can help reduce fraud and enhance responsibility in various sectors, including financial management and the supply chain. (Laurence, 2023). Understanding the blockchain is essential as it represents a transformative approach to data management in our increasingly digital world.

4. Where It Gets Messy: The Privacy Paradox

The digital age has created a complex interplay between personal confidentiality and societal transparency, fundamentally shaping our expectations and private life experiences. At a time when the data is abundant and easily accessible, the limits of privacy are increasingly vague. Individuals often share personal information online, drawn by societal standards that prioritise transparency. However, this paradox is rooted in the gap between perceived and real private life; Many users think that their data is secure while exposing it simultaneously

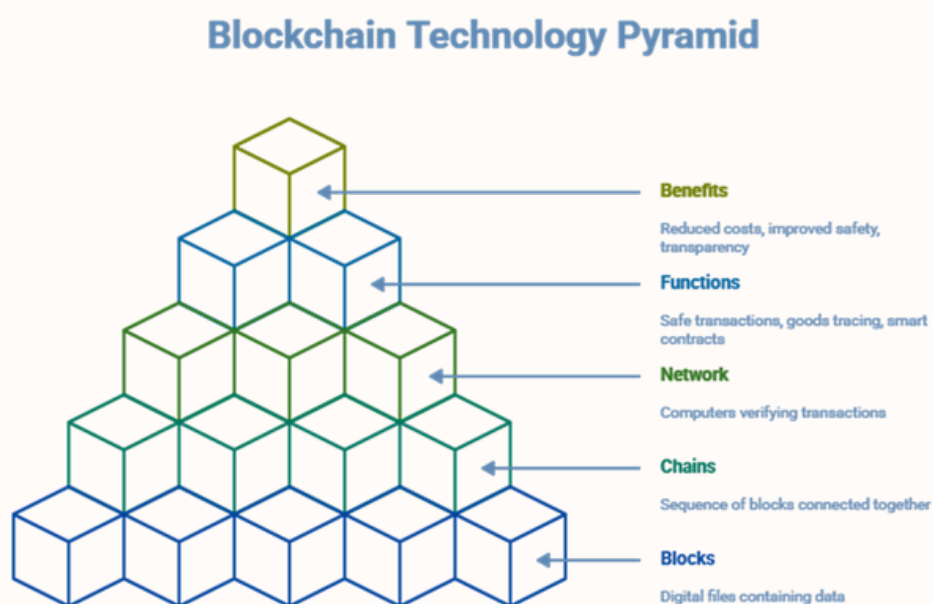


Fig :How the Tech Works (Without the Jargon)

to potential improper use (Solove, D. J. (2021). The Myth of the Privacy Paradox. Geo. Wash. L. Rev., 89, 1. - Google Search, n.d.). Technological progress complicates this tension because the very platforms that promote transparency often undermine privacy. Algorithms and data analysis enable in-depth monitoring, allowing authorities and companies to track behaviours and preferences. This capacity raises critical questions about the consent and commodification of personal data. In addition, societal expectations concerning transparency can put pressure on individuals to allow their privacy in exchange for participation in social networks and digital communities.

The resulting confidentiality paradox highlights the distinction between what individuals wish (confidentiality) and what they experience (Surveillance) (Solove, D. J. (2021). The Myth of the Privacy Paradox. Geo. Wash. L. Rev., 89, 1. - Google Search, n.d.). As the digital landscape evolves, the need for a nuanced understanding of privacy rights and societal obligations is becoming increasingly urgent. The company must reconcile these competing interests to promote a balance that respects individual agency while promoting collective transparency.

5. Can the Two Coexist? Meet the Tech Trying to Make It Wor

The interaction between technology and traditional practices offers significant potential to promote sustainability and cultural preservation. Innovations such as mobile applications for indigenous languages or drone technology to map traditional land exemplify how contemporary tools can improve and protect cultural heritage. For example, the integration of technology into traditional agricultural practices enables more efficient resource management, thereby promoting environmental sustainability. This synergy not only allows efficient farming practices but also allows local communities to preserve their cultural identity through documentation and knowledge exchange. ((PDF) Bridging Innovation Gap and Technology Transfer in Managing Public Organizations, n.d.). When closing the gap between technological advances and traditional practices, communities can leverage innovations that respect and uphold their cultural values. Additionally, these

Technology and Tradition: A Bridge to Sustainable Cultural Preservation

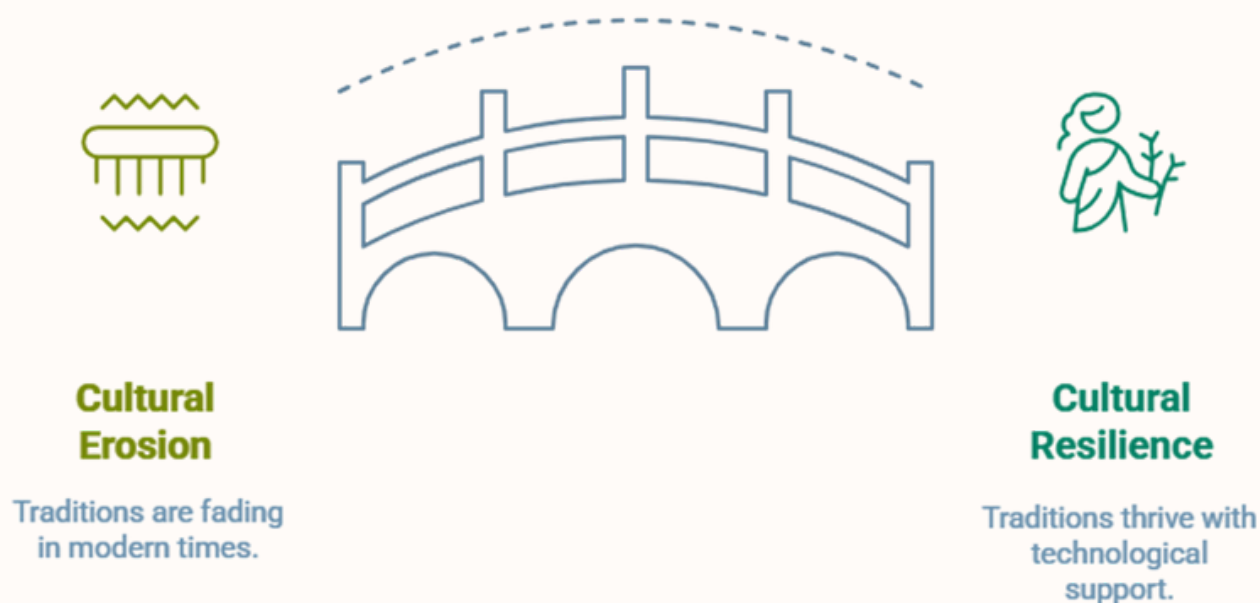


Fig.: Can the Two Coexist? Meet the Tech Trying to Make It Work

technologies can facilitate the exchange of conventional knowledge between generations, ensuring its survival in a rapidly changing world. The evaluation of such innovations is crucial, as it allows for an assessment of their impacts on both sustainability and cultural preservation. Ultimately, the coexistence of technology and tradition can create a resistant framework that supports cultural heritage while addressing contemporary environmental challenges. ((PDF) Bridging Innovation Gap and Technology Transfer in Managing Public Organizations, n.d.). This holistic approach fosters a sustainable future that respects traditions while embracing the opportunities presented by technological advancements.

6. Real-Life Stories: When Privacy and Blockchain Team Up

Blockchain technology has emerged as a transformative force in enhancing user privacy, significantly impacting the security, freedom, and confidence of individuals on digital platforms. When leveraging decentralised Ledgers, blockchain facilitates secure data transactions and minimises the risk of unauthorised access (Garg, 2022). For example, the use of blockchain in medical care enables patients to control access to their medical records, thereby reducing the exposure of sensitive personal information to third parties. This autonomy not only protects data but also enables individuals, reinforcing their freedom in navigation in digital ecosystems.

In addition, case studies around finance blockchain applications illustrate enhanced confidence among users. Cryptocurrencies, such as Bitcoin, enable point-to-point

transactions without the need for intermediaries, thereby promoting a transparent and secure environment. (Garg, 2022). This transparency helps users feel more confident in the integrity of their transactions, contributing to an increase in confidence in digital financial platforms.

In addition, the incorporation of Blockchain solutions focused on privacy, such as Zcash and Monero, highlights the potential for anonymous transactions in various sectors. These solutions demonstrate how blockchain can protect user identities while maintaining transactional integrity. (Garg, 2022). Thus, blockchain technology is a central mechanism for improving user privacy, fundamentally transforming the dynamics of data security and confidence in the digital age.

7. The Legal Maze: Regulators vs. Coders

The interaction between regulatory managers and coding innovations presents a complex landscape, where legal standards often hinder technological progress. Coders frequently encounter compliance issues that can hinder innovation, as regulations often lag behind the rapid pace of technological development. For example, in the Fintech sector, the rigorous regulatory environment can create important obstacles for developers aiming to introduce new solutions. (Navigating the Regulatory Labyrinth: Compliance Dilemmas..., n.d.). These regulations, although essential to consumer protection and financial stability, can inadvertently have a chilling effect on creativity and experimentation among coders.

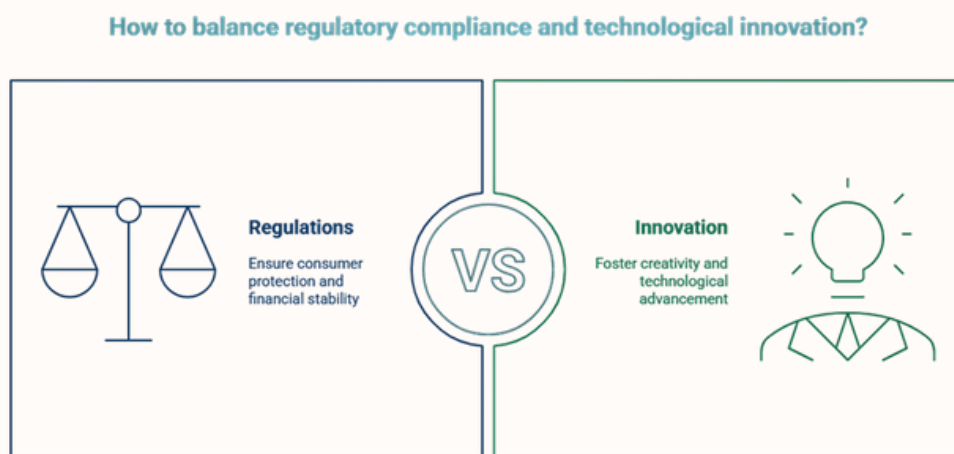


Fig : The Legal Maze: Regulators vs. Coders

Furthermore, the evolutionary nature of technology complicates the application of existing legal frameworks, as many laws are not designed to address the nuances of emerging innovations. Consequently, developers often face the dilemma of balancing innovation with compliance, which can lead to a cautious approach in software development. (Navigating the Regulatory Labyrinth: Compliance Dilemmas..., n.d.). Consequently, although regulations aim to protect public interests, they also pose challenges that can stifle the very innovations that they seek to regulate. This dynamic necessitates a reassessment of regulatory practices to better align them with the rapid advancements in coding and technology, thereby promoting an environment that is conducive to both compliance and innovation.

8. The Road Ahead: Designing for Privacy in a Blockchain World

The integration of blockchain technology presents significant challenges in guaranteeing user privacy, as its inherent transparency can conflict with privacy requirements. One of the main concerns is the immutable nature of blockchain, which makes it difficult to delete personal data when required by regulations such as the General Data Protection Regulation (GDPR) (Giannopoulou, 2021). This raises ethical implications regarding the balance between the benefits of decentralisation and the need to protect individual privacy rights.

Innovative design strategies are essential for addressing these privacy concerns. Solutions such as zero-knowledge tests and blockchain platforms centred on privacy, which allow verifying transactions without revealing the underlying information, are emerging as viable methods to improve user privacy (Giannopoulou, 2021). In addition, implementing design data protection and integrating privacy improvement technologies in the initial stages of blockchain applications can encourage compliance with legal standards while leveraging the benefits of blockchain systems. As Blockchain technology continues to evolve, the approach should not only focus on technological advances but also the ethical implications of its applications. The adoption of a user-centred approach that prioritises privacy and data protection can lead to more responsible innovation in the blockchain space, ensuring that users' trust is maintained alongside technological progress. (Giannopoulou, 2021).

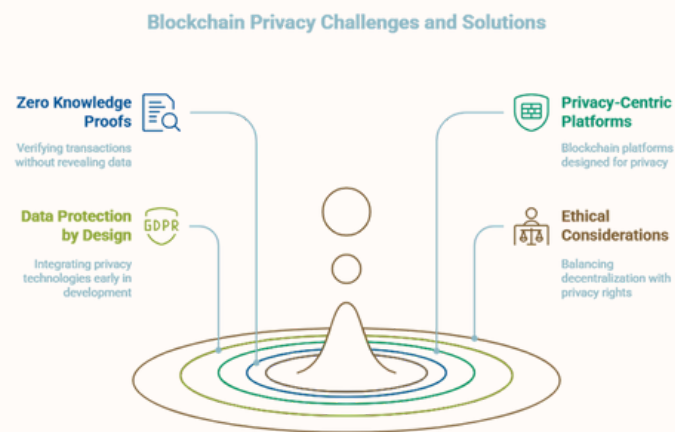


Fig: The Road Ahead: Designing for Privacy in a Blockchain World

9. Final Byte: So... Are Blockchain and Data Privacy Friends or Foes?

Blockchain technology has become a revolutionary tool for enhancing data security. However, its implications for data privacy remain complex and multifaceted. On the one hand, Blockchain provides an immutable accounting system that can strengthen the security of personal data, ensuring that information is not easily altered or accessed without adequate authorisation. This characteristic enhances the user's confidence, as each transaction is registered transparently and linked to a decentralised network, thereby reducing the risks associated with centralised data violations (Niranjanamurthy et al., 2019). On the contrary, the Blockchain transparency characteristic can undermine personal privacy. Since the details of the transaction are stored in a significant book, the information of the people can be traceable, contradicting the principles of data minimisation and limitation of purpose found in the privacy frameworks, such as the General Data Protection Regulation (GDPR). This presents the challenge of striking a balance between the transparency required for the effectiveness of Blockchain and the need to safeguard individual privacy rights. (Niranjanamurthy et al., 2019).

Ultimately, the relationship between blockchain technology and data privacy raises a double-edged sword. Although Blockchain can improve security measures, its inherent transparency could lead to the inadvertent exposure of personal data, which requires a careful examination of how these technologies interact to effectively navigate the future implications of privacy.

References:

- Garg, R. (2022). Blockchain para aplicaciones del mundo real. John Wiley & Sons, Inc., New York, US, 27. <https://zenodo.org/record/7466433>
- Giannopoulou, A. (2021). Putting Data Protection by Design on the Blockchain. *European Data Protection Law Review*, 7(3), 388–399. <https://doi.org/10.21552/EDPL/2021/3/7>
- Henderson, S. C., & Snyder, C. A. (1999). Personal Information Privacy: Implications for MIS Managers. *Information and Management*, 36(4), 213–220. [https://doi.org/10.1016/S0378-7206\(99\)00019-1](https://doi.org/10.1016/S0378-7206(99)00019-1)
- Laurence, T. (2023). Blockchain. 250.
- Navigating the Regulatory Labyrinth: Compliance Dilemmas... (n.d.). Retrieved 2 May 2025, from <https://sciendo.com/article/10.2478/picbe-2024-0217>
- Niranjnamurthy, M., Nithya, B. N., & Jagannatha, S. (2019). Analysis of Blockchain technology: pros, cons and SWOT. *Cluster Computing*, 22(6), 14743–14757. <https://doi.org/10.1007/S10586-018-2387-5/FIGURES/8>
- (PDF) Bridging Innovation Gap and Technology Transfer in Managing Public Organisations. (n.d.). Retrieved 2 May 2025, from https://www.researchgate.net/publication/339553067_Bridging_Innovation_Gap_and_Technology_Transfer_in_Managing_Public_Organizations
- Shin, D. D. H. (2019). Blockchain: The emerging technology of digital trust. *Telematics and Informatics*, 45, 101278. <https://doi.org/10.1016/J.TELE.2019.101278>
- Solove, D. J. (2021). The myth of the privacy paradox. *Geo. Wash.. L. Rev.*, 89, 1. - Google Search. (n.d.). Retrieved 2 May 2025, from https://www.google.com/search?q=Solove%2C+D.+J.+%282021%29.+The+myth+of+the+privacy+paradox.+Geo.+Wash.+L.+Rev.%2C+89%2C+1.&sca_esv=feadb363baf7c19&ei=DZ0UaMYF4oyx4w-wn9DQBw&ved=0ahUKEwiGwJ7LyISNAxViRmwGHbAPFH0Q4dUDCBA&uact=5&oq=Solove%2C+D.+J.+%282021%29.+The+myth+of+the+privacy+paradox.+Geo.+Wash.+L.+Rev.%2C+89%2C+1.&gs_lp=Egxnd3Mtd2l6LXNlcniAUVNvbG92ZSwgRC4gSi4gKDIwMjEpLiBUaGUgbXl0aCBvZiB0aGUgcHJpdmFjeSBwYXJhZG94LiBHZW8uIFdhc2guIEWuIFJldi4sIDg5LCAxLkicCVAAWABwAHgBkAEAmAGaAaABmgGqAQMwLjG4AQPIAQD4AQGYAgCgAgCYAwCSBwCgB4UBsgcAuAcA&scient=gws-wiz-serp

Shruti Bamboria, (IMBA)

Student, Department of Biochemistry and Forensic
Science, Gujarat University,
Ahmedabad, Gujarat, India



Kiran Dodiya

Research Scholar, Department of Biochemistry
and Forensic Science, Gujarat University,
Ahmedabad, Gujarat, INDIA



Dr. Kapil Kumar

Coordinator, Department of Biochemistry
and Forensic Science, Gujarat University,
Ahmedabad, Gujarat, INDIA



Abstract

The rapid adoption of cloud computing architectures across industries has fundamentally transformed the modern IT landscape. By offering dynamic scalability, high availability, and cost-efficiency, cloud services have become integral to digital transformation strategies. However, these benefits are counterbalanced by an expanded threat surface and a redefined security perimeter. Cloud environments introduce unique security challenges that necessitate a paradigm shift in traditional information assurance frameworks. This article critically examines the principal cyber threats associated with cloud infrastructure and delineates strategies for enhancing cyber resilience within these distributed environments.

Introduction

Forensic odontology is a specialized field of forensic science involving dental knowledge to identify individuals and analyze bite marks. Traditionally associated with human identification, it now plays an increasingly important role in animal attack investigations. According to Keiser-Nielsen (1970), forensic odontology deals with the proper handling and examination of dental evidence and the proper evaluation and presentation of dental findings.'(1)

Non-human bite mark analysis has applications in wildlife forensics, human-animal conflict, and criminal investigations involving fatal or non-fatal animal attacks. Understanding the morphological differences between human and animal dentition is critical in interpreting such evidence

Historical Perspective

The use of dental evidence dates back to 66 AD, when Agrippina identified the decapitated head of Lollia Paulina by her teeth [2]. In the American context, Paul Revere famously identified Dr. Joseph Warren using a dental prosthesis [3]. From fire victims in Paris (1897) to mass casualties in the World Wars, forensic odontology has evolved considerably. The establishment of the American Board of Forensic Odontology (ABFO) in the 1970s marked a major advancement.

Evolution of the Field

In recent years, forensic odontology has undergone notable evolution, driven by technological innovation and an expanded range of applications. One of the key developments is the incorporation of digital imaging techniques, such as 3D scanning and computer-assisted bite mark analysis, which have significantly improved the accuracy and objectivity of forensic comparisons[4]. Concurrently, advancements in molecular biology have reinforced the role of dental tissues and saliva as reliable sources of both nuclear and mitochondrial DNA, enhancing the identification process in forensic casework[5]. Moreover, the scope of the discipline has widened considerably. It now plays a vital role not only in criminal investigations but also in areas such as wildlife forensics, abuse detection, and environmental crime investigations. These developments collectively underscore the interdisciplinary nature of forensic odontology today.

Types of Animal Dentition and Bite Morphology

Animal dentition and bite morphology exhibit considerable variation based on dietary adaptations, directly influencing the mechanics of biting and chewing. Carnivores, such as dogs and big cats, possess sharp canines, powerful jaw muscles, and specialized shearing teeth designed for tearing flesh. In contrast, herbivores like horses and cows feature flat molars, broad jaws, and significant lateral jaw movement to grind plant material efficiently[6]. Omnivores, including humans, have a mixed dentition that allows both tearing and grinding, reflecting their varied diets. Rodents are characterized by continuously growing incisors with a chisel-like appearance and paired grooves, adapted for gnawing. Reptiles, on the other hand, typically exhibit conical teeth suited for gripping prey rather than chewing.



In addition to dietary classifications, dentition can also be categorized by tooth uniformity and replacement patterns. Homodont species have teeth of a single type, while heterodont species exhibit varied tooth forms, such as incisors, canines, premolars, and molars. Furthermore, tooth succession patterns vary: monophyodonts develop only one set of teeth during their lifetime, whereas diphyodonts, like humans, develop two successive sets—deciduous and permanent.

Common Bite Mark Features

Animal bite marks typically display a range of distinctive features that can aid in forensic identification. Puncture

wounds are common and usually appear as deep, paired marks caused by the animal’s canine teeth. Lacerations often result from the tearing action of the jaws, especially when combined with shaking motions during an attack. In cases involving animals with exceptionally strong bite forces, such as crocodiles, crush injuries may occur, leading to bone fractures and extensive tissue damage. Avulsion injuries, where tissue is completely removed, are often indicative of predatory behavior. Additionally, multiple overlapping bite marks may be present, suggesting a prolonged struggle or feeding activity[8].These characteristic features provide valuable clues in differentiating animal bites from other types of trauma.

Table 1: Comparative Anatomy of Dentition

Type of Animal	Dental Formula	Tooth Characteristics	Function
Carnivores	3.1.4.2 / 3.1.4.3	Sharp canines; carnassials adapted for shearing	Tearing meat and cutting flesh
Herbivores	0.0.3.3 / 3.1.3.3	Flat molars; reduced or absent canines	Grinding fibrous plant material
Omnivores (Human)	2.1.2.3 / 2.1.2.3	Mixed dentition: incisors, canines, premolars, molars	Versatile – cutting and grinding
Rodents	1.0.0.3 / 1.0.0.3	Continuously growing, chisel-like incisors	Gnawing through tough material
Reptiles	Variable	Homodont: uniform teeth; conical or serrated edges	Gripping prey or slicing flesh

Table 2: Key Dental Features and Forensic Relevance

Type of Animal	Dentition Type	Key Dental Features	Forensic Relevance
Humans (Omnivores)	Heterodont, diphyodont	Incisors, canines, premolars, molars;	Unique bite mark patterns, dental
Carnivores	Heterodont	Prominent canines, carnassials (P4/M1),	Deep puncture wounds, linear tears, intercanine
Herbivores	Heterodont	Broad, flat molars; reduced or absent	Broad grazing bite patterns, absence of
Rodents	Heterodont (incisors only functional)	Continuously growing chisel-like incisors; lack of	Paired parallel incisor marks, postmortem
Reptiles	Homodont	Uniform, conical or serrated teeth; often	Ragged tearing or crushing injuries; multiple
Primates (Non-human)	Heterodont	Similar to humans but with sectorial premolars,	May resemble human bites; must analyze arch

Techniques in Bite Mark Documentation

1. Visual Inspection: Initial analysis of tooth type, bite arc, and depth.
2. Photography: Use of ABFO No. 2 scale; multiple views including UV imaging[9].
3. Manual Measurements: Callipers and rulers to determine inter-canine distance and spacing.
4. Tracing and Overlay: Acetate sheet tracing and dental overlays to compare suspected animal patterns.
5. Dental Casts and Photographic Comparison: Impressions from animal dentition matched to the wound morphology.
6. Digital Image Processing: Edge detection, contour mapping, geometric morphometrics, and image registration assist in precise matching.
7. Histology and DNA: Histologic sections aid in timing (ante-/post-mortem). Salivary DNA helps confirm species.

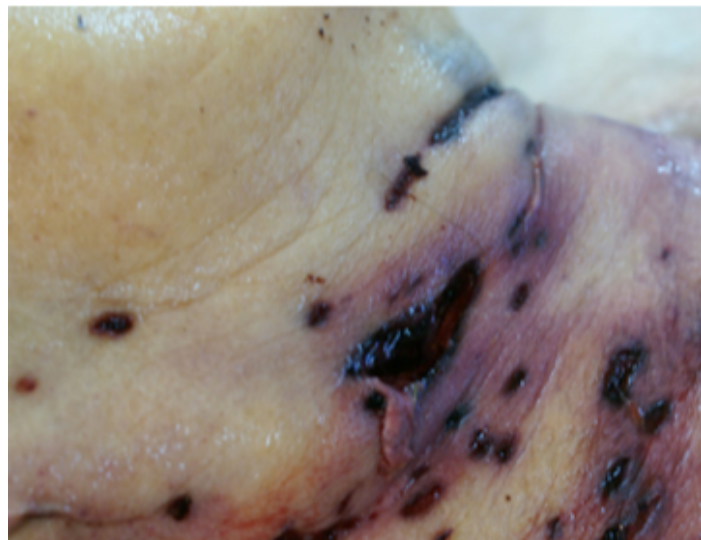
Legal and Wildlife Relevance

Bite mark analysis plays a vital role in various legal and investigative contexts, serving as a key tool in both human and animal-related cases. In criminal investigations, it is used to link suspects to violent offenses such as homicides and assaults, where bite marks may be present on victims or objects at the scene. The technique is equally important in cases of animal cruelty, helping to document and assess injuries resulting from neglect or abuse. Furthermore, bite analysis has gained prominence in wildlife forensics, where it aids in the investigation of illegal wildlife trade, poaching incidents, and conflicts between humans and wild animals. These applications underscore the broader forensic significance of bite mark evaluation across both legal and environmental domains.

Case Studies

A notable case study involves the fatal mauling of an 85-year-old woman by a pit bull, resulting in multiple bite marks concentrated on the neck region. The cause of death was determined to be exsanguination, stemming from the laceration of major blood vessels in the neck inflicted by the dog's bite. The wounds displayed characteristic "V"-shaped punctures with irregular and wrinkled

borders, consistent with the bite morphology of a powerful canine. This case underscores the severity and forensic relevance of identifying specific bite patterns in fatal animal attacks, particularly in distinguishing the mechanism of injury and attributing responsibility in medico-legal investigations[15].



In another documented case, a 43-year-old mentally disabled man suffered a fatal attack that was later confirmed to be caused by a pack of dogs. The investigation involved both a forensic odontologist and a carnivore biologist, whose combined expertise was instrumental in conclusively identifying the nature of the injuries. Their analysis ruled out alternative causes and established with certainty that the wounds were consistent with a coordinated dog pack attack. This case highlights the value of interdisciplinary collaboration in forensic investigations involving animal-inflicted injuries, especially when differentiating between attacks by single animals and multiple assailants.

Challenges

The future of bite mark analysis in forensic investigations is poised for significant advancement through the integration of emerging technologies and interdisciplinary collaboration. One promising development is the use of artificial intelligence (AI) for pattern recognition and analysis, which has the potential to enhance the accuracy and objectivity of bite mark comparisons.



Collaboration with veterinary forensic experts is also gaining traction, particularly in cases involving non-human bites, offering specialized insights into animal behavior and dentition. Furthermore, the establishment of standardized protocols and the creation of comprehensive global databases are essential steps toward improving consistency, reliability, and accessibility in bite mark identification across jurisdictions. These future directions collectively aim to strengthen the scientific foundation and forensic value of bite mark analysis.

Conclusion

Non-human bite mark analysis is an indispensable tool in forensic investigations. It allows for species identification, timing of injuries, and differentiation between attack and scavenging behavior. Multidisciplinary collaboration and technological advancements will continue to enhance the accuracy and utility of this field.

References

1. Adams C. Forensic Odontology: An Essential Guide. John Wiley & Sons, Ltd; 2014.
2. Luntz LL. History of forensic dentistry. Dent Clin North Am. 1977;21:7–17.
3. Paul Revere: The First American Forensic Dentist. Strangerremains. 2017 Jul 4.
4. Veyta, F., Yuniastuti, M., Suhartono, A. W., & Auerkari, E. I. (2022). Human bite mark analysis: Review of advantage computer-assisted procedure. AIP Conference Proceedings, 2537, 030001

5. Chaudhary, R. B., Shylaja, Patel, A., & Patel, A. (2020). DNA in forensic odontology: New phase in dental analysis. International Journal of Forensic Odontology, 5(1), 43.
6. Murmann, D. C., Brumit, P. C., Schrader, B. A., & Senn, D. R. (2006). A comparison of animal jaws and bite mark patterns*. Journal of Forensic Sciences, 51(4)
7. Samuels, J. X. (2009). Cranial morphology and dietary habits of rodents. Zoological Journal of the Linnean Society, 156(4), 864–888.
- 8 Greene, D., & Williams, D. (2013). Manual of Forensic Odontology. In CRC Press eBooks
9. Standards and practices for bite mark photography. (2011, December 1). PubMed
10. Animal adaptation review- Dr. Whitson's Biolab review
11. Kashyap B, et al. Comparison of the bite mark pattern and intercanine distance between humans and dogs. J Forensic Dent Sci. 2015;7(3):175.
12. Ramesh G, et al. Forensic Photography - An Emphasis on Bite Mark Photograph..
13. Viciano J. Post-Mortem Dental Profile as a Powerful Tool in Animal Forensic Investigations—A Review.
14. Kaur KP. Bite Mark Analysis—A Crucial Forensic Evidence.
15. Fonseca GM. Forensic studies of dog attacks on humans: a focus on bite mark analysis.

ABOUT THE AUTHOR

Dr. Riya Mariya
Forensic Odontologist, Dentist



CASE STUDY

ON

3 B's: BLACK MAGIC? BETRAYAL? BANK? THE ₹53 CRORE GOLD ROBBERY

Author: Vagdevi Emami



Introduction

In a country where gold is considered sacred, treasured in temples and worn at weddings as a symbol of prosperity, India has long had a profound relationship with gold. It is more than just a metal here—it is wealth, tradition, and emotional security. People pawn their gold for loans when they are in need, relying on banks to store it safely. It's no surprise that it also becomes the favourite target of thieves. Over the decades, India has witnessed daring robberies that sound more like movie plots than real crimes: from tunnels dug under banks to gangs escaping with gold under the noses of guards. But what unfolded in Managuli town of Karnataka's Vijayapura district in May 2025, was unlike anything seen before.

This wasn't just a robbery. What also made the crime so peculiar, was not only the robbers stole 58.97 kg of pledged gold worth ₹53.26 crore and ₹5.2 lakh in cash in just two nights, but also how it was executed cleanly, and with an added touch of superstition. It was a perfectly timed illusion, where gold vanished, alarms slept, and a black magic doll grinned from a broken window. The state had witnessed major thefts before, but this one ranks as the second-biggest jewellery theft in Karnataka's history.

India has witnessed numerous such dramatic gold robberies in the past, each more like a film than the previous one. A gang dug a 50-foot tunnel into an Indian Overseas Bank branch in Chennai in 2017 and robbed it of gold worth crores. In 2014, a group of robbers burst into Punjab National Bank in Odisha and made off with gold and currency after taking bank staff hostage. It was in 2023 that a gang of people who were impersonating the CBI officers broke into bank lockers at a Mumbai bank, fooling the staff that it was a genuine operation. But none of them had the peculiar combination of psychology, planning, and betrayal like the one in Managuli, which now becomes remarkable for its perfectly planned execution of a plan.



Source: <https://industrywired.com/news/black-doll-fake-key-and-53-crores-gone-what-happened-at-canara-bank-9335265>

The Canara Bank branch was closed between May 23 and May 25 for the weekend. When employees returned on the morning of May 26, they discovered the shutter lock broken, a window grill was cut open, one locker was smashed, and gold contained with approximately ₹53 crore. All other lockers remained untouched. The robbers had stolen the CCTV system's recording unit as well, leaving absolutely no visual documentation of their actions and ₹5.2 lakh in cash had also disappeared. But the most bizarre detail was the black-coloured doll, which was painted with white and red paints, turmeric and saffron were put up on it, and the doll was left close to the shattered window, positioned in such a manner that resembled a ritual. The way it was positioned hinted at ritual or occult activity, leading to wild theories and confusion in the early stages of the investigation

But the doll was never involved in any actual ritual. It was a conscious action on the part of the perpetrators to stall the police investigation by playing on fear and superstition, opined Superintendent of Police Laxman Nimbaragi. Forensic experts were serious about the doll. They have been swabbing it for fingerprints, examining soil particles on it, testing for fabric fibres and any trace elements that could connect it with the perpetrators. It was not only a robbery; it was psychological misdirection—a scheme to get authorities wondering if something more than crime was involved. Police initially struggled to understand the motive behind the black magic props. But as Superintendent of Police Laxman Nimbargi revealed later, it was all part of an elaborate misdirection strategy. The robbers had placed not only a black doll but also turmeric, saffron, and a blowtorch in the bank, mimicking ritualistic setups seen in crimes in Tamil Nadu and Kerala to mislead investigators into thinking that the robbers were outsiders or religious extremists using witchcraft. They even sprinkled salt powder throughout the bank to confuse sniffer dogs and prevent the recovery of fingerprints. According to SP Nimbargi, they had studied similar witchcraft-style robberies from other states and used those ideas to buy time and confuse the investigation.

Investigators, later realised that this was not a random theft, but a perfectly timed, inside-assisted crime. The robbers didn't force the locker open. They had used a duplicate key, disabled the alarm, and opened a solitary locker that contained gold ornaments pledged by customers from various districts using a replica key. They even removed the CCTV-DVR before entering the vault, ensuring their faces and actions weren't captured. It was all too precise. Police suspected insider participation, particularly as no other lockers were opened and the robbers had some idea where to go and what to steal.

Their suspicion proved to be true. On June 26, SP Laxman Nimbaragi made an announcement of the arrest of three prime players. Among them was Vijayakumar Mohanara Miriyala, a 41-year-old Senior Manager of the same branch of Canara Bank. Investigators found that he had worked for over a year at the Managuli branch and later was transferred out only weeks prior to the robbery. The one-year period of work, gave him complete knowledge of the bank's inner workings: the locker system, alarm codes, key storage, and even staff routines. He wasn't alone. He brought in his long-time friend Chandrashekar Kotilingam Nerella (38) and an associate Sunil Narrasimhalu Moka (40) to help execute the robbery.

Vijay Kumar meticulously planned the theft to avoid suspicion, waiting until his transfer to execute the crime. His strategy was to strike on the fourth day after the arrival of the new manager, on May 23. CCTV footage later captured him moving about the bank premises on that day. According to Superintendent of Police Nimbargi, the plan was timed with the IPL match between Royal Challengers Bangalore (RCB) and Sunrisers Hyderabad. The accused anticipated that if RCB won, the ensuing fan celebrations which is marked by loud firecrackers, providing the perfect cover for the robbery. However, when RCB lost the match, the group abandoned the plan for that day. Undeterred, they regrouped and chose to carry out the robbery the following day, May 24. As part of their preparations, they tampered with the CCTV system and cut the high-mast light cable to avoid detection.

The robbery was executed so precisely that only one locker was opened, while another filled with similar amounts of gold was left untouched. Police seized gold ornaments and gold bars melted by them valued at ₹10.75 crore, besides two vehicles utilized in the crime. The gold was already being smelted, demonstrating the speed at which the accused attempted to destroy the evidence and turn it into untraceable bullion.



Image: The accused have been identified as Vijayakumar Miriyala (left), 41, and his associates Chandrashekar Nerella, 38, an employee at a private company, and Sunil Narasimhalu Moka (right), 40

Source: Duplicate keys, CCTV tampering: How a bank manager orchestrated Rs 53 crore heist in Karnataka | Bangalore News - The Indian Express

Managuli police had logged the case under Sections 331(3), 331(4), and 305(E) of the Bharatiya Nyaya Sanhita, 2023. These include criminal breach of trust by a banker, dishonest misappropriation for self, and housebreaking by night with theft. The accused were brought before court on the same day. The inquiry revealed that a single locker had been opened, and another locker having equivalent quantities of gold had been deliberately left untouched—firm evidence that the suspect had inside information and access to actual keys, or duplicate keys replicated from originals.

The police formed eight specialised teams, working under SP Laxman Nimbaragi, with leadership from additional SPs, DySPs, Circle Inspectors, and Sub-Inspectors across the district. Their efforts were lauded as systematic, scientific, and relentless, as they gathered and analyzed each shred of evidence—from car tracking to cyber forensics and fingerprint detection.

Customers who pledged their ornaments were devastated. Many were ordinary people. Housewives pledging wedding jewellery, farmers giving up family bangles during crop failure, parents securing education loans with heirloom pieces. Their shock turned into anger as they realised the theft had come from within the system they trusted. Why didn't the bank have dual-key locker systems? Why weren't CCTV backups stored in cloud servers? Why were pledged assets not split into multiple secure units? The robbery, while planned by three men, exposed the systemic vulnerabilities of banking security.

Forensic Relevance

1. The duplicate key usage pointed to an insider. Forensic lock testing showed no external damage, confirming silent entry.
2. The black doll, along with saffron, turmeric, and salt, was swabbed for DNA, checked for trace elements, and analyzed for soil particles to track movement and intent.

3. The CCTV NVR theft launched a digital forensic effort to retrieve footage from cloud backups and nearby ATM cams.
4. Recovered gold bars were tested for purity and compared with customer loan records to prove identity.
5. Vehicle forensics involved matching tire impressions, tracking fuel purchases, and mapping truck movement using toll and CCTV data

This case will be historical in more than the amount stolen. It will be how it was stolen. It was quiet, clean, psychological, and deceptive. It had all the ingredients of human betrayal, inside help, advanced forensic analysis, and even ancient superstition. Although much of the gold has been recovered and the prime suspects have been arrested, the investigation is continuing. Additional accomplices are suspected to be part of the conspiracy, and the search is still on for the rest of the plundered assets. The Managuli gold theft is no longer a crime report. Now, it's a case study in criminal intelligence, forensic science, and the far-reaching implications of shattered trust.

ABOUT THE AUTHOR

Vagdevi Emani,

III B.Sc. Forensic Science, Aditya Degree and
PG College, Surampalem.



ENCRYPTED ALIBIS: WHEN PRIVACY TOOLS OBSTRUCT JUSTICE

Author - Leeba Pathan, Kinjal Patani, Kiran R Dodiya, Dr. Kapil Kumar

Introduction

On a rainy December evening in 2015, two attackers stormed a holiday party in San Bernardino, California, killing 14 and injuring dozens. In the aftermath, investigators discovered an iPhone belonging to one of the shooters. It was locked, Encrypted and Unrackable. Despite an FBI court order, Apple refused to create a “backdoor” into the device, igniting a fiery global debate. Privacy, Apple argued, was sacred and even in the face of terror.

This case spotlighted a growing dilemma: as privacy tools become more advanced and widely adopted, they increasingly shield not just the innocent, but the guilty. Encryption, once the domain of spies and diplomats, is now embedded in everyday life from messages and emails to hard drives and cloud backups. Yet in a world where every digital trace can serve as evidence, this untraceability has become a formidable obstacle for law enforcement.

We are entering an era where justice is obstructed not by clever alibis or expensive lawyers, but by unbreakable code. A tool designed to protect civil liberties become a shield for criminal impunity. This article explores the rising clash between privacy and accountability, where encrypted alibis increasingly test the boundaries of justice



The Rise of Encryption: From Niche to Necessity

Encryption is the process of converting information into a secret code that has existed for millennia. From Caesar’s ciphers to WWII’s Enigma machine, humans have always sought to protect communication. But digital encryption has turned a corner. In the 1990s, when Phil Zimmermann released PGP (Pretty Good Privacy) to the public, it sparked U.S. government concerns so intense that Zimmermann was investigated for exporting “munitions.” Today, similar-grade encryption sits quietly on every iPhone, Android and messaging app.

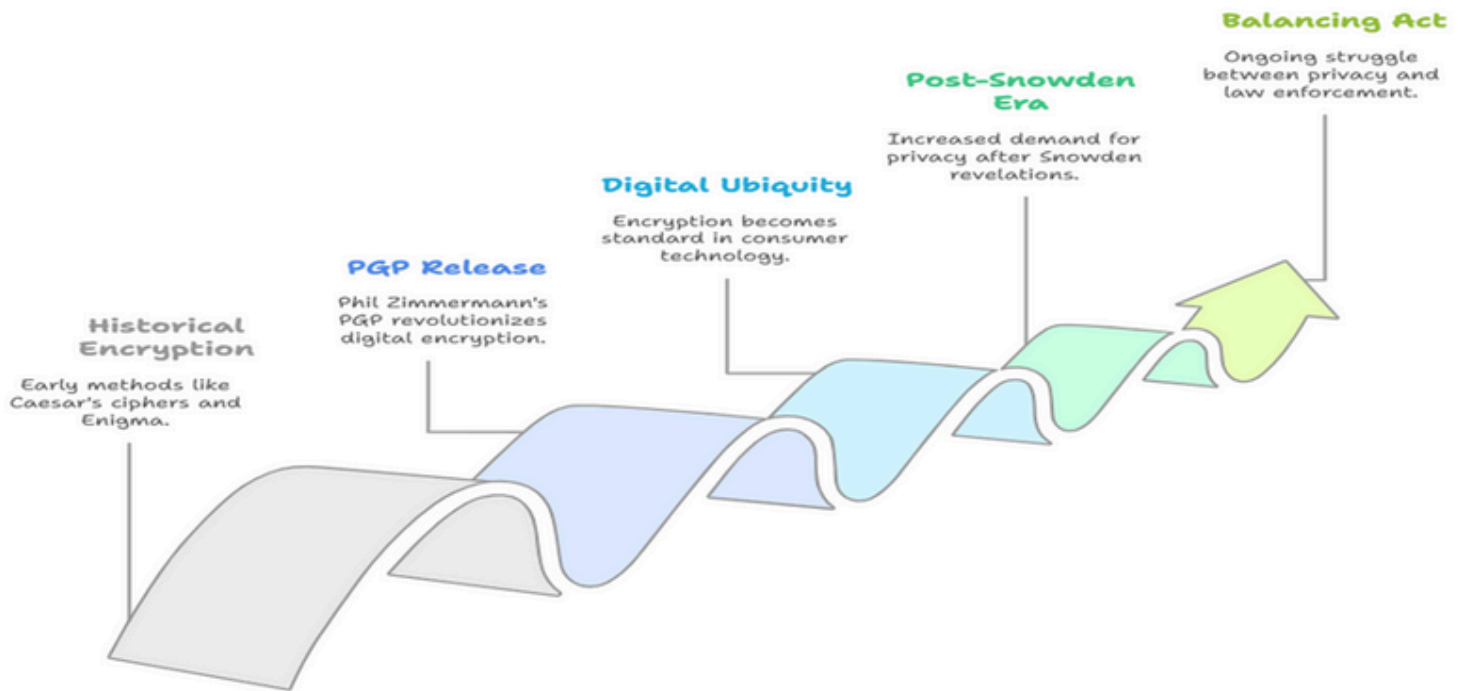
The transformation is profound. Once reserved for national security, encryption now secures our texts, protects our banking and guards our identities. In the post-Snowden era, public trust in governments plummeted, prompting a boom in end-to-end encrypted apps like Signal, Telegram, and ProtonMail. Consumers, weary of surveillance capitalism and cybercrime, embraced the idea that “what’s mine is mine even from the state.”

Tech companies championed this shift. Apple famously stated, “What happens on your iPhone stays on your iPhone.” WhatsApp, owned by Meta, encrypts over 100 billion daily messages. Google, Microsoft and countless others encrypt user data by default.

For the average person, this means safer communication. For journalists, dissidents, and whistleblowers, it’s a lifeline. But for investigators chasing cybercriminals, child predators, terrorists or human traffickers, it’s a locked vault they can’t legally or technically access.



Evolution of Encryption's Role



When Tools Become Shields: The Justice Gap

In 2020, the European Union's crime agency Europol estimated that encryption blocked investigations into over 85% of child exploitation cases. In the same year, the FBI reported being unable to access nearly 7,000 encrypted devices linked to various crimes even with court orders.

In one chilling U.S. case, law enforcement found child abuse videos circulating online. After a lengthy investigation, they located a suspect. But his phone, protected by biometric locks and encrypted storage, proved impenetrable. The lack of accessible digital evidence meant charges had to be reduced, despite strong suspicions. Encrypted messaging platforms are now favoured by drug cartels and traffickers. In 2021, an unprecedented international sting operation, Operation Trojan Shield, flipped the script: the FBI created an encrypted messaging service, ANOM and secretly distributed it to criminal networks. Over three years, investigators silently monitored 27 million messages, leading to 800+ arrests globally. It was a rare wins in a game of cat and mouse, one enabled not by breaking encryption, but by faking trust.

The San Bernardino case remains a benchmark. When Apple refused the FBI's demand, the bureau eventually paid hackers over \$1 million to unlock the phone. The result, No significant new intelligence was found. Critics questioned whether the FBI used the case more to pressure legislation than to solve the crime.

Still, the precedent was set: in a world awash with privacy tools, evidence often dies with the device. The Impact of Encryption on Law enforcements shown in Below figure

The Legal and Ethical Tug-of-War

The tension between law enforcement and technology companies has evolved into a structural stalemate. On one side are authorities seeking to uphold justice and protect citizens. On the other are tech giants, privacy advocates and legal scholars who argue that weakening encryption compromises not just individual rights but the very fabric of a free society.



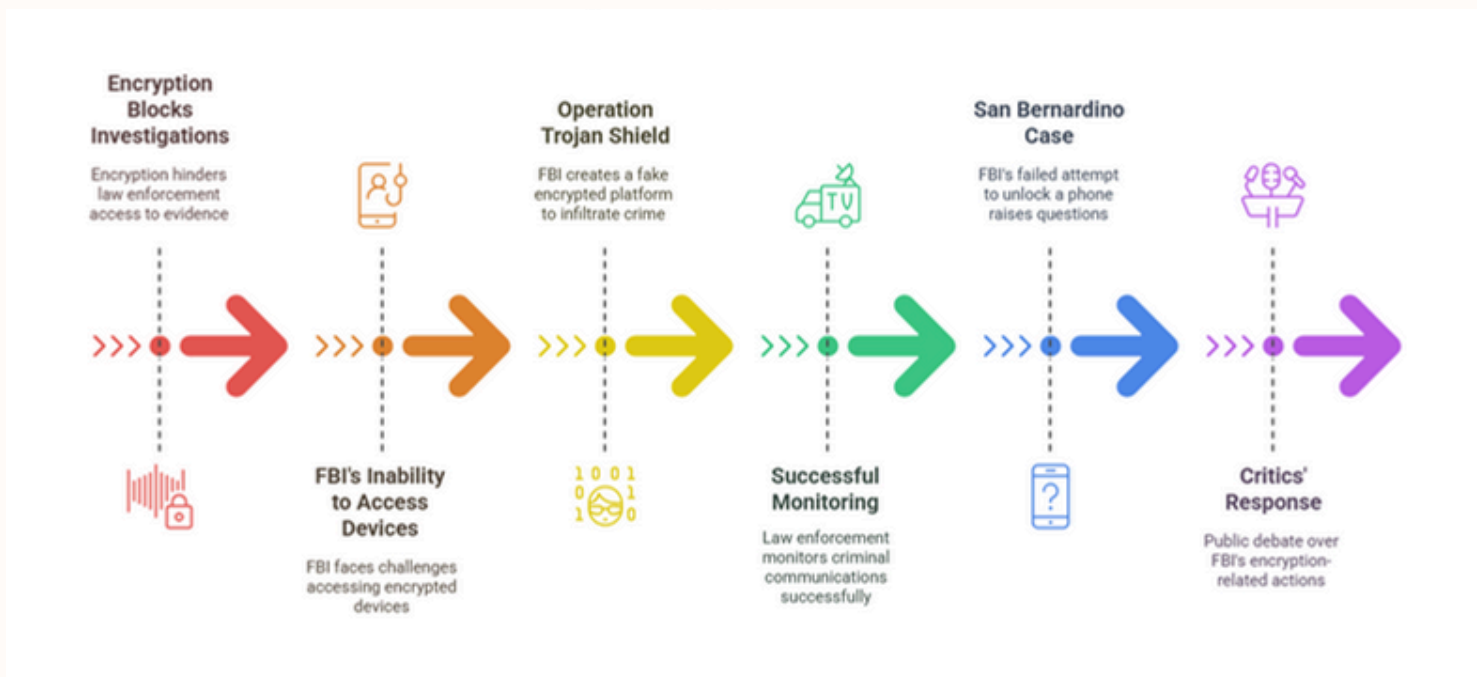


Fig. Showing the Impact of Encryption on law Enforcement

From the government's standpoint, encryption has created digital shadows places where criminals operate unseen and unchecked. FBI Director Christopher Wray labeled this the "going dark" phenomenon, referring to how critical data is increasingly out of reach, even with valid legal warrants. Agencies argue they aren't pushing for dragnet surveillance or bulk data collection, but rather targeted access like unlocking a suspect's phone in a terrorism or kidnapping case. In their eyes, encryption without exception means that even with probable cause, justice is denied.

This concern is not limited to the United States. Across Europe, law enforcement agencies have echoed similar fears. In 2020, the European Commission even proposed regulatory frameworks that would compel tech companies to cooperate with law enforcement in cases involving child exploitation and terrorism, while still trying to preserve the integrity of encryption. The technical and ethical feasibility of such "middle ground" solutions remains widely debated.

Opposing this push are privacy advocates and digital rights organizations who warn that any mechanism enabling access to encrypted content no matter how well-intentioned opens a Pandora's box. The

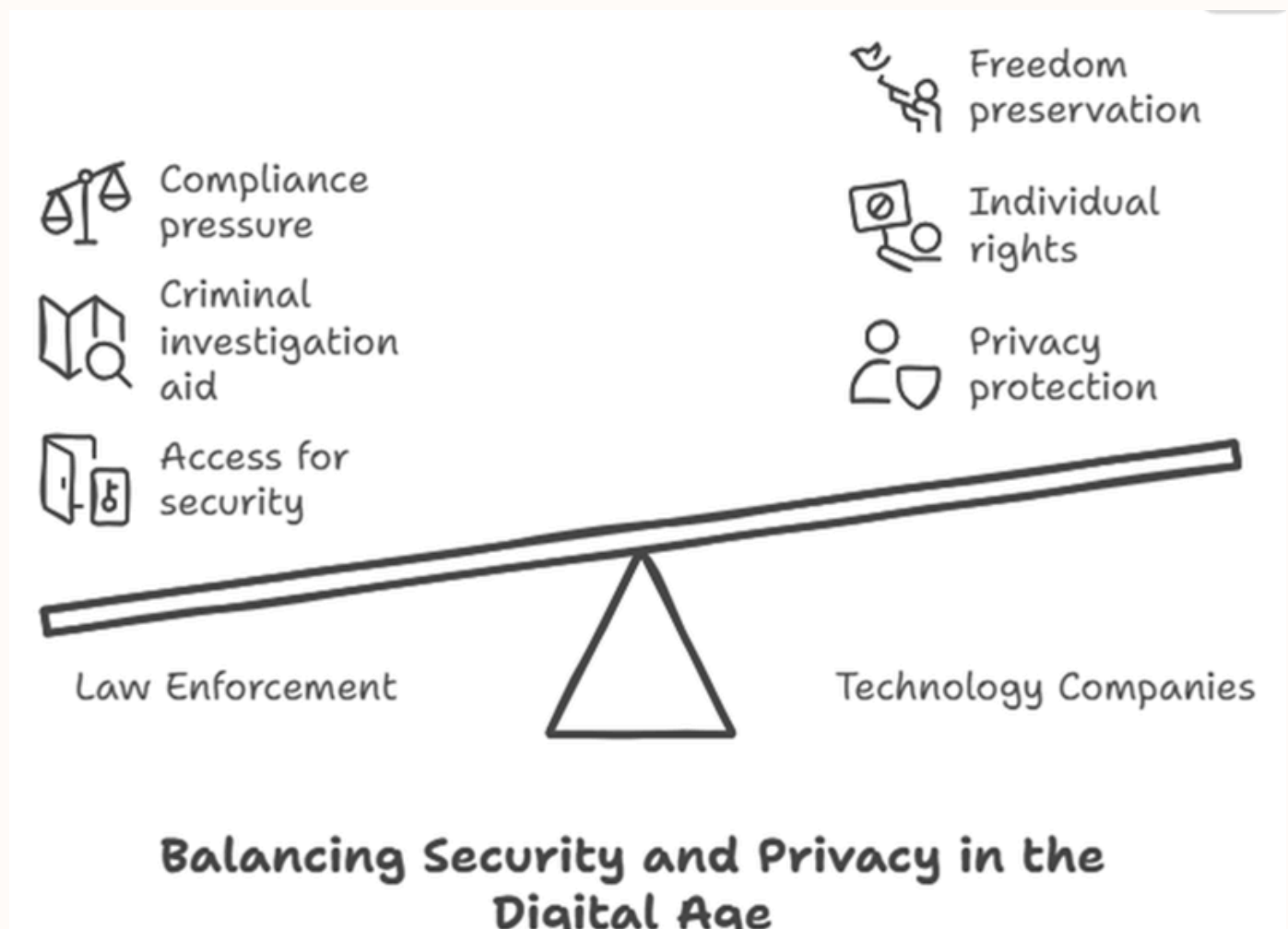
Electronic Frontier Foundation (EFF), Privacy International and Human Rights Watch argue that backdoors, once created, can be exploited not only by democratic governments but also by authoritarian regimes, rogue employees or malicious hackers. The same loophole used to track a trafficker could be used to silence a dissident or target a journalist. Cryptographers and security experts are nearly unanimous on one point: encryption does not lend itself to selective weakening. As Bruce Schneier famously stated, "You can't have strong encryption for good guys and weak encryption for bad guys. It's all or nothing." Any system built to provide exceptional access risks undermining the entire structure of trust that digital security relies on.

Technology companies find themselves in a bind. On one hand, advocating for user privacy enhances brand loyalty and complies with laws like the European Union's General Data Protection Regulation (GDPR). On the other, defying government requests can result in legal battles, financial penalties, or even market restrictions. Apple's 2016 refusal to unlock the San Bernardino shooter's iPhone led to a very public standoff with the FBI, one that polarized public opinion and tested the boundaries of corporate responsibility.

Meta (formerly Facebook), which owns WhatsApp and has plans to expand end-to-end encryption across its platforms, has faced repeated backlash from governments worried that such measures will hinder criminal investigations. The UK's Online Safety Act, passed in 2023, even included controversial provisions that could force companies to scan encrypted messages for harmful content that raising alarms about undermining encryption altogether.

Some legal scholars advocate for a new social contract, one that recognizes privacy as a human right but allows for narrowly defined and technologically constrained access in extreme cases. Ideas like "key escrow" (where a neutral third party holds decryption keys) or split-key access models have been floated, but critics point out they introduce complexity, costs and new vulnerabilities.

In the end, the clash is not merely technical but philosophical: Should we prioritize collective security or personal autonomy? Can a society remain both safe and free? As data becomes the new witness in criminal cases from location histories to private chats the debate over encryption will continue to shape how we define justice in the digital age.



International perspective and policy responses

As the use privacy enhancing technologies continues to keep increasing in size , government are in around world difficult task manage in individual privacy with national security and law enforcement needs.

United states : the push for lawful access :

The U.S. has been at the forefront of the encryption debate, particularly following incidents such as the San Bernardino shooting in 2015. The FBI's clash with Apple over unlocking a suspect's iPhone reignited calls for "lawful access" to encrypted devices.

EARN IT Act (2020): Proposed legislation aimed at holding tech companies accountable for content on their platforms, indirectly challenging end-to-end encryption by threatening legal protections. The EARN IT Act is not an encryption bill, and does not create mandates for government surveillance; in fact the bill doesn't mention encryption at all. Tech companies have testified that strong, responsible encryption can be reconciled with aggressive policing of CSAM. The Commission – which has representatives from the tech industry, privacy experts, and computer scientists – will be well positioned to help them achieve that goal.

DOJ Advocacy: The U.S. Department of Justice has repeatedly called for "backdoors" into encrypted communications, citing the need to combat terrorism, child exploitation, and cybercrime.

European Union: Privacy First, But With Conditions :

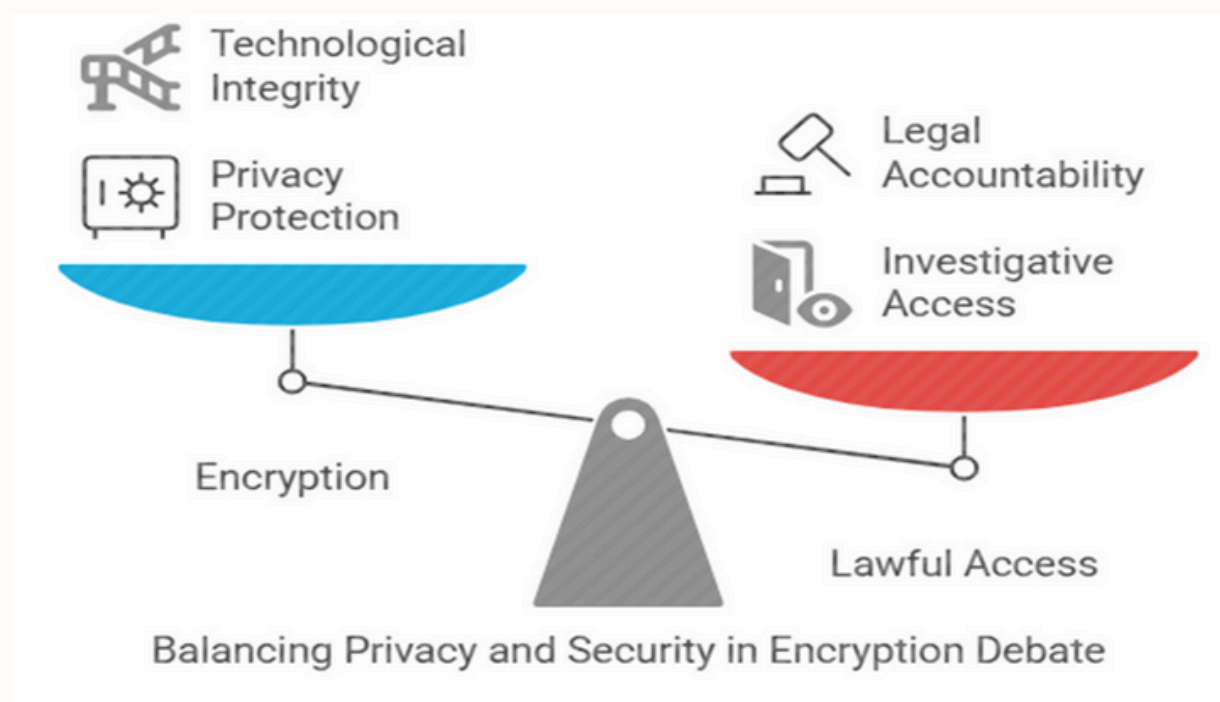
The EU supports digital privacy like General Data Protection Regulation (GDPR), but it also acknowledges challenges by encryption in criminal investigation.

Council Resolution (2020): 29 December 2020 : Threats to international peace and security caused by terrorist acts Letter from the President of the Council on the voting outcome ([S/2020/1305](#)) and voting details ([S/2020/1311](#)).

United Kingdom: Mandating Decryption Capabilities :

The Investigatory Powers Act (IPA) governs how we use the investigatory powers available to us. These powers provide for the lawful acquisition of communications data including the who, where, when, how and with whom of a communication but not the content.

The technological arms race



Advancements in Privacy and Anonymity Technologies :

A.Zero-Knowledge Protocols and Homomorphic Encryption: Zero Knowledge (ZK) is a cryptographic protocol that allows one party to prove to another that it knows certain information without revealing the information itself. Homomorphic Encryption (FHE) is an encryption method that allows computations to be performed on encrypted data without the need for prior decryption.

B.Steganography and File Obfuscation Tools: A tool that hides data within JPEG images using encryption and various concealment algorithms.

C.Metadata and Behaviural Analysis: Even when content is hidden, metadata (timestamps, geolocation, communication frequency) remains a valuable resource for building investigative timelines and suspect profiles.

D.Advanced Digital Forensics: Tools like Cellebrite and GrayKey can extract data from encrypted mobile devices, although their effectiveness varies by device and encryption strength.

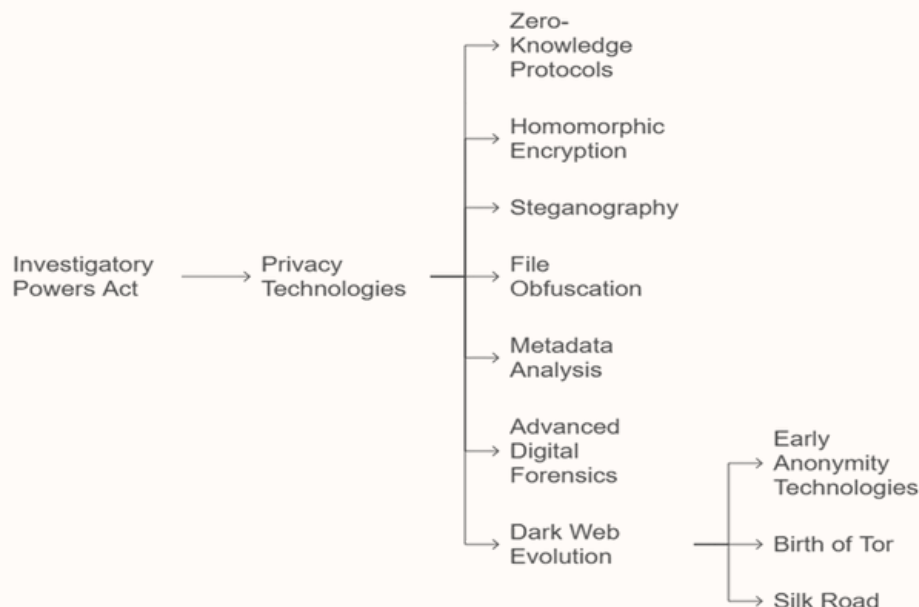
E.Dark Web Evolution : Marketplaces on the dark web frequently change URLs, use multi-signature cryptocurrency wallets, and implement decentralized hosting to avoid takedowns.

1.Early Anonymity Technologies (1970s-1990s): The concept of online anonymity and privacy dates back to the early days of the internet. Technologies such as email encryption, anonymous remailers, and early versions of anonymous web browsing began to emerge during this period.

2.The Birth of Tor (2002):The Tor Project, initially developed by the U.S. Navy for secure communication, was released as open-source software to the public in 2002. Tor (The Onion Router) is a crucial tool for accessing the dark web as it allows users to browse the web anonymously by routing their traffic through a series of volunteer-run servers, making it difficult to trace their online activities.

3.Silk Road (2011-2013):One of the most infamous dark web marketplaces, Silk Road, was launched by Ross Ulbricht in 2011. It facilitated the buying and selling of illegal goods, primarily drugs, using Bitcoin for transactions. Eventually, Silk Road was shut down by law enforcement in 2013, leading to Ulbricht's arrest and conviction.

Technological Arms Race in Privacy and Anonymity



Encryption And The Right to Privacy

What is the right to privacy?

What privacy means – and what the right to it covers – is not an easy question to answer. The UN Special Rapporteur on the right to privacy, whose role, among other things, is to raise awareness about privacy issues, said in his 2016 report to the UN Human Rights Council that the concept of privacy “is known in all human societies and cultures at all stages of development and throughout all of the known history of humankind” but that “there is no binding and universally accepted definition of privacy”.

UN Special Rapporteurs are independent experts, elected by the members of the UN Human Rights Council, with particular thematic mandates, such as freedom of expression, privacy, poverty or migrants. They publish annual reports on the subject matter of their mandate and receive and respond to complaints from individuals on related human rights issues. While the UN Human Rights Committee issued a General Comment on the right to privacy in 1989, it doesn't provide a comprehensive scope of the right to privacy, simply giving some examples of what is covered – for example, information relating to an individual's private life, personal and body searches, and the holding of personal information on computers, data banks and other devices. Established in 1977, the UN Human Rights Committee is a UN body made up of 18 independent experts on human rights, tasked with overseeing the implementation of the International Covenant on Civil and Political Rights. Among other things, the Committee issues ‘General Comments’ which elaborate on different rights within the ICCPR and how they should be implemented by states.

Policies, Guidelines and Best Practices on the Use of Encryption and Permissible Restrictions

While technical standards are developed by the international and national standards-setting bodies, other international and regional bodies have developed policies and guidelines on when encryption should be used and on when it can or should be restricted, controlled or limited. The weight of such guidelines and policies varies: some have the status of ‘soft law’ (and are therefore persuasive, albeit not binding, on national governments and courts), while others are merely suggestions of best practice. Three of the most important examples of such organisations are the United Nations, the Council of Europe and the Organisation for Economic Co-operation and Development. We'll also look at a couple of other international forums which have recently made statements regarding encryption. United Nations The main focus of the United Nations (UN) on encryption has been from a human rights perspective. As international human rights law has almost entirely developed from UN processes, it has been different bodies within the UN which have applied that legal framework to the issue of encryption. Indeed, much of chapters 3 and 4 of this guide have used UN sources in setting out how encryption is a human rights issue and what rights respecting encryption laws and policies would look like. Out of these sources, three have provided most of the guidance: the UN Human Rights Council, the UN Human Rights Committee and the UN Special Rapporteurs. UN Human Rights Council As noted in chapter 3, the UN Human Rights Council is an intergovernmental body, established in 2006, made up of 47 UN member states. Among other things, it is tasked with making recommendations (called resolutions) to states on particular human rights issues. These resolutions are ‘soft law’, meaning that they are persuasive, but not legally binding, on governments and courts.

Privacy Tools: The Double-Edged Sword

As we navigate the digital world, we generate a constant stream of data: browsing habits, purchase history, location data, and even health information. Businesses collect and analyze this data to personalize experiences, target advertising, and improve services. While this offers convenience and targeted solutions, it also raises privacy concerns.

Key privacy tools commonly used

a)End-to-End Encryption (E2EE) : End-to-end encryption (E2EE) is a security method that ensures only the sender and intended recipient can read a message, with no one else, including the service provider, able to access the content. Common Platforms like WhatsApp, Signal, Telegram (secret chats).

b)The Tor Network and Onion Routing : or (short for "The Onion Router") is a free and open-source software that enhances online privacy and anonymity by routing internet traffic through a network of volunteer-operated relays, masking users' IP addresses and browsing activity. Commonly used by both political dissidents and criminal marketplaces. Hides IP addresses.

c) Cryptocurrencies (e.g., Bitcoin, Monero) : Facilitates decentralized, often pseudonymous, transactions.a digital currency in which transactions are verified and records maintained by a decentralized system using cryptography, rather than by a centralized authority.

d)Virtual Private Networks (VPNs) : Virtual because no physical cables are involved in the connection process.Private because through this connection, no one else can see your data or browsing activity.Networked because multiple devices—your computer and the VPN server—work together to maintain an established link.

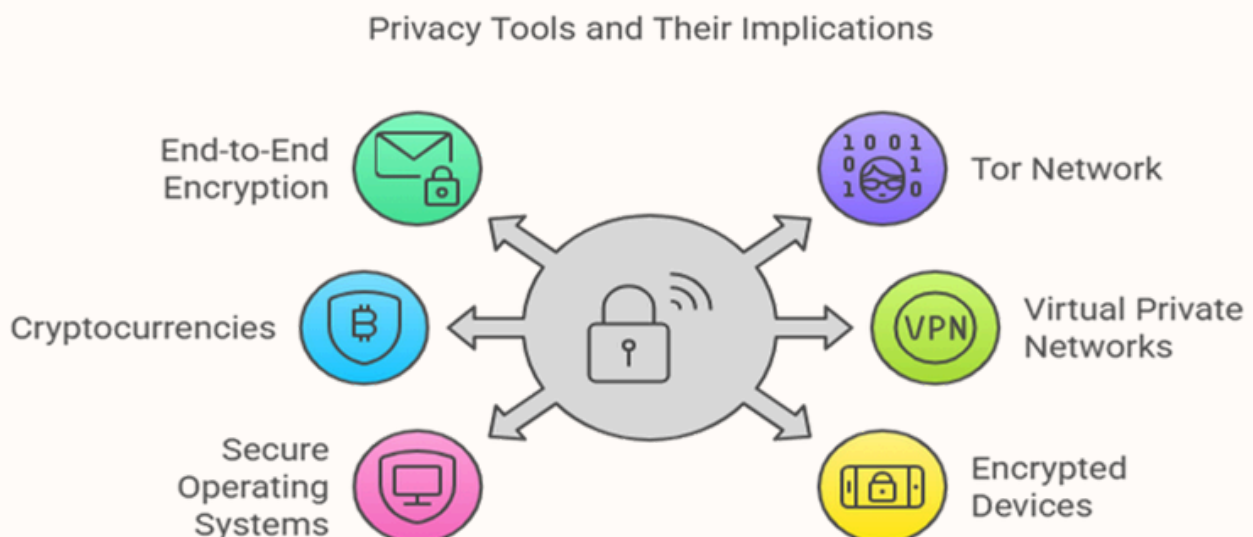
e)Secure Operating Systems (e.g., Tails, Qubes OS) : it provides anonymity and leaves no digital trace after shutdown.

f)Encrypted Devices and Storage : Encrypted devices and storage use encryption to secure data at rest and in transit, protecting it from unauthorized access.

Conclusion

Encryption is not inherently good or bad. It is a tool one that can protect the oppressed or empower the guilty. As its use grows, society must confront hard questions: Who deserves privacy? When does the right to remain digitally silent end? And can we build systems where truth and trust coexist?

The law must evolve alongside technology, not in opposition to it. Otherwise, justice risks becoming another encrypted file that is visible, important, but forever out of reach.



References

1. Federal Bureau of Investigation (FBI) – Director Christopher Wray's remarks on "Going Dark":
2. <https://www.fbi.gov/news/speeches/going-dark-are-technology-privacy-and-public-safety-on-a-collision-course>
3. San Bernardino iPhone Case – New York Times Coverage
4. Zetter, K. (2016). "The FBI-Apple Encryption Fight Is Over, But the War Continues." The New York Times.
5. <https://www.nytimes.com/2016/03/29/technology/fbi-says-it-has-accessed-data-on-san-bernardino-iphone.html>
6. Electronic Frontier Foundation (EFF) – Views on encryption and privacy rights:
7. <https://www.eff.org/issues/encryption>
8. Europol – 2020 Internet Organized Crime Threat Assessment (IOCTA)
9. <https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2020>
10. Apple's Public Statement on Privacy
11. Apple Inc. (2016). "A Message to Our Customers."
12. <https://www.apple.com/customer-letter/>
13. Operation Trojan Shield – FBI Press Release
14. FBI (2021). "Hundreds Arrested in Global Takedown of Organized Crime."
15. <https://www.fbi.gov/news/stories/trojan-shield-global-takedown-060821>
16. Australian TOLA Act Overview
17. Australian Government – Department of Home Affairs. (2018). Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018.
18. <https://www.legislation.gov.au/Details/C2018A00148>
19. UK Investigatory Powers Act (IPA)
20. UK Government Legislation Database. (2016).
21. <https://www.legislation.gov.uk/ukpga/2016/25/contents/enacted>
22. EARN IT Act Criticism – Center for Democracy & Technology
23. CDT. (2022). "EARN IT Act Threatens Online Privacy and Security."
24. <https://cdt.org/insights/the-earn-it-act-threatens-encryption-and-online-privacy/>
25. Bruce Schneier on Encryption
26. Schneier, B. (2015). "Why We Encrypt." Schneier on Security.
27. https://www.schneier.com/blog/archives/2015/07/why_we_encrypt.html
28. NSO Group Pegasus Spyware – The Guardian
29. Borger, J. (2021). "Pegasus Project: spyware found on journalists and activists' phones." The Guardian.
30. <https://www.theguardian.com/news/2021/jul/18/pegasus-project-spyware-phones-journalists-activists>
31. Metadata and Surveillance – Harvard University's Berkman Klein Center
32. Berkman Klein Center (2015). "Don't Panic: Making Progress on the 'Going Dark' Debate."
33. <https://cyber.harvard.edu/publications/2016/02/dont-panic>

ABOUT THE AUTHORS

Leeba Pathan

Student at Department of Biochemistry and
Forensic Science, Gujarat University,
Ahmedabad, Gujarat, INDIA



Kinjal Patan,

Student at Department of Biochemistry and
Forensic Science, Gujarat University,
Ahmedabad, Gujarat, INDIA



Kiran Dodiya

(Research Scholar, Department of Biochemistry
and Forensic Science, Gujarat University,
Ahmedabad, Gujarat, INDIA



Dr. Kapil Kumar

Coordinator, Department of Biochemistry
and Forensic Science, Gujarat University,
Ahmedabad, Gujarat, INDIA



INNOVATIVE TECHNIQUES IN QUESTIONED DOCUMENT ANALYSIS: FROM ADVANCED FORENSICS TO IMAGINARY FUTURES

Author -Mr. Yash Babaria, Mr. Bhumit Chavda

Introduction:

One of these is document authentication, and the subsequent detection of changes, forgeries, and authors, a significant field of forensic science known as questioned document examination (QDE). In the past, the field has been based upon tried and tested methodologies. The evolving rate of tech development in other fields of science is, however, currently overtaking the conventional definitions of QDA per se. With the growth of technology, other technology-based based so-called conventional methods, such as paper tests, ink science, and handwriting science, have significantly changed. The paper covers real-life countermeasures, which are advanced, such as the electrostatic detectors, the hyperspectral camera, and the use of artificial intelligence (AI) handwriting recognition. It also examines speculative and imagined future methods, such as verification of ink by quantum ink, DNA-based inks, and neurotrace mapping. The complex of forensic knowledge and scientific novelty enhances the accuracy and scope of questioned document analysis (Wagner et.al, 2015).

Thanks to the apparent possibilities and methods that can be attained in the next moment, we are then thrown into the land of future fantasies. In this category, we discuss extraordinarily speculative, but also very interesting, conceptual approaches, which, possibly, would redefine QDA decades later as inspired by innovative developments in neuroscience, quantum physics, and sophisticated artificial intelligence (Srihari et al., 2002).

Overview and scope

Any document, of which the origin or authenticity is doubtful and which is therefore taken into investigation to determine its validity, is hence a questioned document in the sense of forensics. In lawsuits, these records are very often debated. Questioned Document Examination (QDE) is very critical in modern forensic investigations, particularly in the field of fraud detection and criminal trials, as well as in civil litigation. To counteract the popularity of advanced techniques of forging and altering documents, digital and conventional methods of forensics, professionals are required to utilize the most recent

and advanced scientific methods of document inspection and authentication. Moreover, forensic science can predict issues and create innovative solutions using the imagination of future technology. This article reviews advanced and imaginary techniques that have been applied in the QDE that provide an understanding of the current level of the field and its prospective overall course.



Fig: Advances in the field of Forensic Question Document

Advanced Techniques in Questioned Document Analysis

HSI, or hyperspectral imaging:

HSI allows analysts to detect the tiniest alterations in this ink, changes, and even composition of the paper absorbed by taking photos at various wavelengths, such as ultraviolet and infrared (Wagner, 2015). It is a non-destructive process that gives more visibility to rewritten or altered text or text that was deleted.

Advantages of HSI in Document Analysis:

Non-destructive:

HSI allows for the analysis of documents without causing damage.

Detailed Spectral Information:

HSI provides a wealth of information about the document's composition and characteristics.

Non-contact:

HSI can analyze documents from a distance, minimizing the risk of contamination or damage.

Potential for Automation:

HSI systems can be integrated with machine learning algorithms for automated analysis and classification.

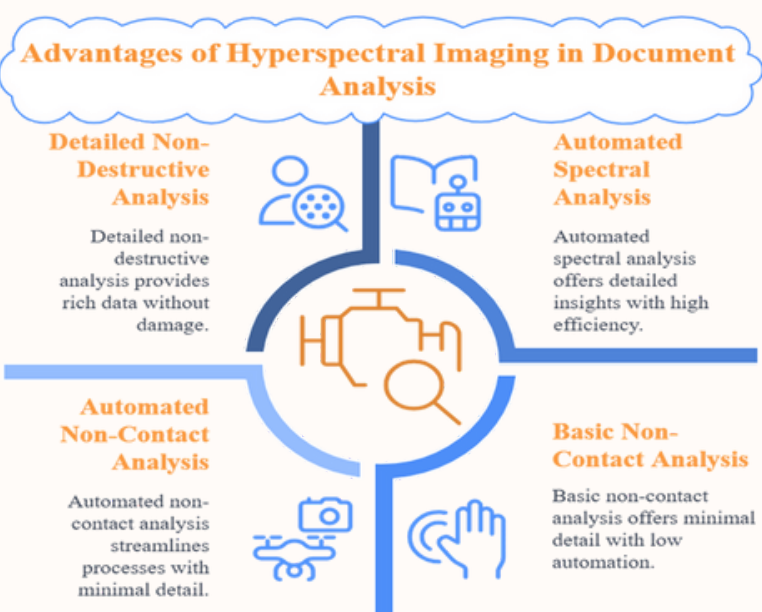


Fig. Advantage of Hyperspectral Imaging in Document Analysis

Raman spectroscopy

Raman spectroscopy may be employed as a helpful method of forensic document analysis, particularly paper and ink. Raman spectroscopy is a method in which forensics experts can tell the difference between inks produced by various manufacturers or even different lots by the same manufacturer based on identifying the exact chemical components present in the inks. Raman spectroscopy may also be used to analyze the chemical composition of the sheet of paper itself, which may come in handy when analyzing the type of paper used as well as identifying any

editions and modifications to the document (Kumar, R. et.al, 2023).

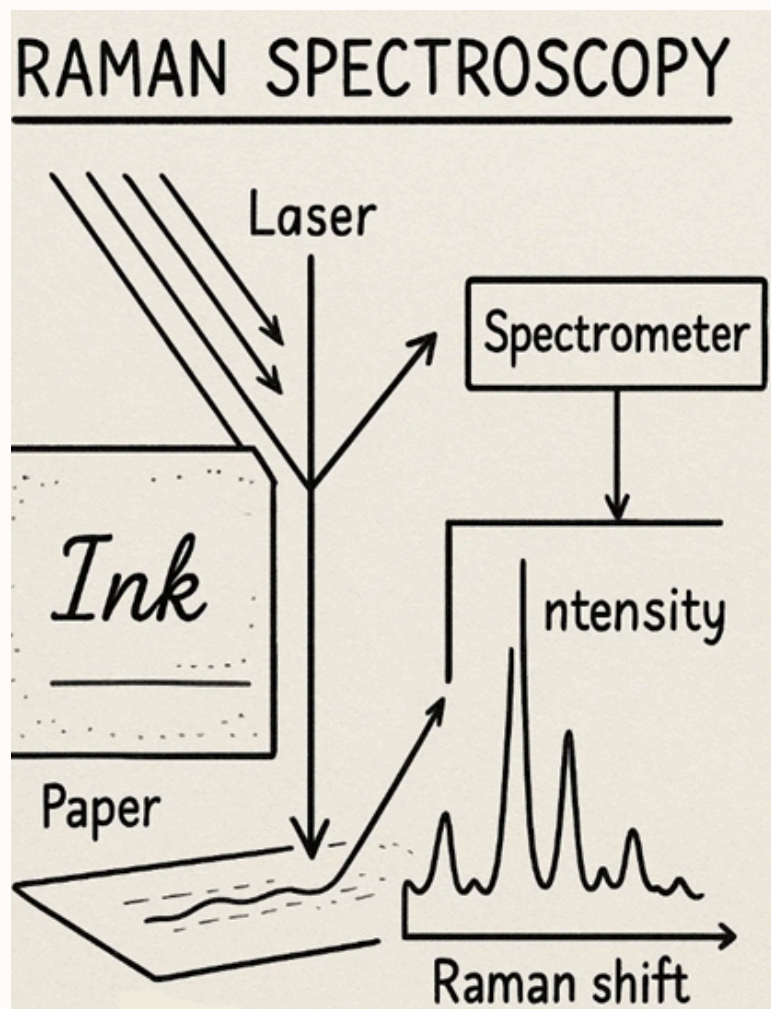


Fig. Raman spectroscopy Graph shift

ESDA

Electrostatic Detection Apparatus, also known as ESDA, is an indispensable instrument of forensic science that is used to study papers that are under investigation especially when looking at detecting the indented text. Although the impressions left on the paper are not visible to the naked human eye, special forensic document examiners are able to see them since it is a non-destructive method. It is convenient where there is a written document, and signs of indentations on the underwriting, or under the same sheet, are worth detecting. On a bronze plate, the document is covered with a thin charged polymer film. When the toner is placed, it adheres to the reverse knuckles of the letters since such files are the most charged electrostatically. The dents end up being conspicuous.

Digital Image Processing

Image analysis software helps detect the alterations or modifications of the text, pixel abnormalities, and any differences in a digital document. Manipulation that cannot be seen with the naked eye includes techniques such as contrast enhancing, layering, and analysis of metadata.

Image Acquisition: Scanning or photographing the document using a camera or scanning devices. Binarization is a step of separating the text and the background, whereby the image is converted to black and white. Noise reduction technique involves removing imperfections that may hamper the analysis; these would include smudges, stains, etc. Skew detection and correction is the process of correcting any slant in the page scanned. Normalization: Adjusting the picture to be the same for processing.

Segmentation: Layout Analysis: The identification of elements of a document, e.g., text blocks, pictures, tables, etc. Word and Line Segmentation: Segmenting the text into individual words and lines.

Digital Image Processing

The machine learning technique can be used to analyze thousands of handwritings, including Forensic Information System for Handwriting (FISH).

These systems analyze stroke patterns, slant, pressure and spacing to identify the author (Srihari et al., 2002).

3.1 Forensic Linguistics:

Language-based profiling involves the use of syntax, vocabulary and other elements of style to determine whether one is ghost-writing or bear authorship of a text. Linguistic analysis is also finding more support in form of AI, as well as stylometric techniques, in cases involving the investigation of crime scenes (Coulthard & Johnson, 2007).

Futuristic Techniques:

Neurotrace Authorship Mapping:

The proposed future technology of document security would involve inclusion of artificial DNA tags in ink which could be associated with individuals or companies. Such markers could be identified in real time with portable DNA scanners. Projected as the future of documents security, the approach is built on the idea of synthetic biology and the principles of DNA barcoding to incorporate highly unique and artificial DNA codes directly within the ink compositions (Biomolecular Forensics Review, 2025).

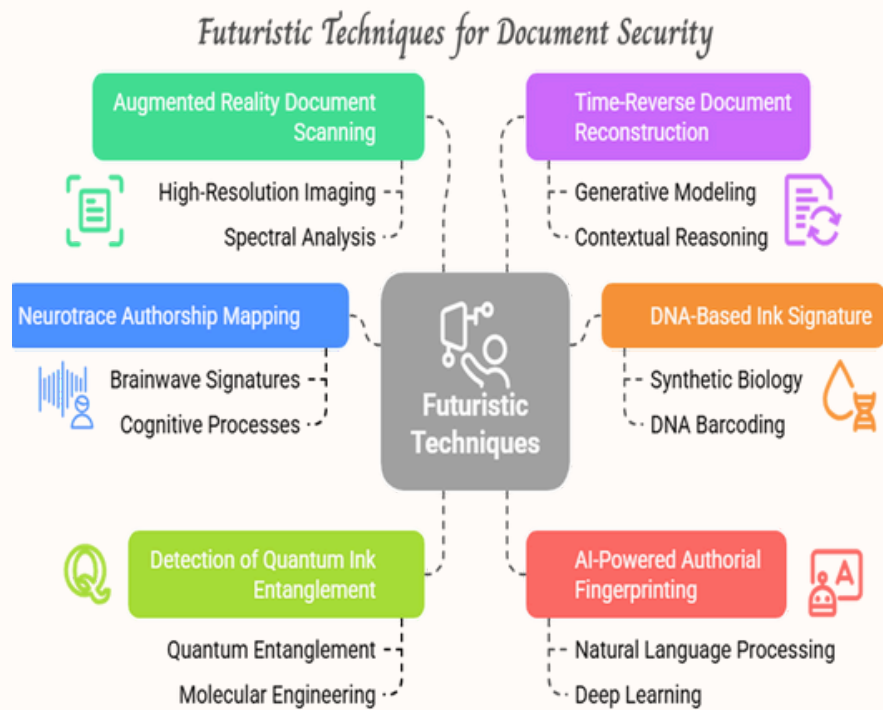


Fig. Futuristic Techniques for Question Document security in Forensic’s

The theoretical basis lies in the possibility to create stable and non-interfering sequences of DNA that could be custom-created to encode certain information, i.e., the manufacturer of the ink, the number of the batch or the day its production was manufactured or even what the user or organization is (Synthetic Biology Applications, 2023).



Fig. Neurotrace authorship Mapping in the questioned document

DNA-Based Ink Signature:

The proposed future technology of document security would involve inclusion of artificial DNA tags in ink which could be associated with individuals or companies. Such markers could be identified in real time with portable DNA scanners. Projected as the future of documents security, the approach is built on the idea of synthetic biology and the principles of DNA barcoding to incorporate highly unique and artificial DNA codes directly within the ink compositions (Biomolecular Forensics Review, 2025). The theoretical basis lies in the possibility to create stable and non-interfering sequences of DNA that could be custom-created to encode certain information, i.e., the manufacturer of the ink, the number of the batch or the day its production was manufactured or even what the user or organization is (Synthetic Biology Applications, 2023). ‘

Detection of Quantum Ink Entanglement:

This theory states that ink molecules would get quantum-entangled during the production process. Should the ink be altered or have tampered with, the entanglement would be broken and signalled a counterfeit. This is an extremely theoretical notion, exploring into the world of quantum mechanics in order to ensure document security. The underlying principle implies that to be able to have the ink molecules engineered or manipulated during its production, it can become entangled due to quantum entanglement, a phenomenon distinguishing a pair of particles, which are entangled, or intrinsically connected in a common quantum state irrespective of their spatially distanced posture (Quantum Physics & Document Security, 2025). The theory entails that such a weaving of fine strands would be preserved in ink on a piece of paper. The most important point is that any physical or chemical modification of the ink, i.e., the effort at destroying it, or inserting new ink, or other deformations, would interfere with this quantum entanglement, in effect interrupting it and breaking it.

Artificial Intelligence (AI)-Powered Authorial Fingerprinting:

Future AI programs could analyze thousands of linguistic and psychological characteristics to come up with their own "fingerprint of authorship" that can be identified even when the style of a writer is deliberately disguised. The next generation of AI application avenues, based on encouragement in Natural Language Processing (NLP), and deep learning, will be to develop highly resistant to "authorial fingerprints AI will focus on examining thousands of minutes of linguistic, syntactic, and even psychological features placed deep in the text of a writer. It does not merely entail putting together typical words and grammatical constructions but also subtle semantic tastes, idiomatic usage, error patterns, and predisposed cognition (Computational Psycholinguistics Journal, 2018).

Detection of Quantum Ink Entanglement:

This theory states that ink molecules would get quantum-entangled during the production process. Should the ink be altered or have tampered with, the entanglement would be broken and signalled a counterfeit.

This is an extremely theoretical notion, exploring into the world of quantum mechanics in order to ensure document security. The underlying principle implies that to be able to have the ink molecules engineered or manipulated during its production, it can become entangled due to quantum entanglement, a phenomenon distinguishing a pair of particles, which are entangled, or intrinsically connected in a common quantum state irrespective of their spatially distanced posture (Quantum Physics & Document Security, 2025). The theory entails that such a weaving of fine strands would be preserved in ink on a piece of paper. The most important point is that any physical or chemical modification of the ink, i.e., the effort at destroying it, or inserting new ink, or other deformations, would interfere with this quantum entanglement, in effect interrupting it and breaking it.

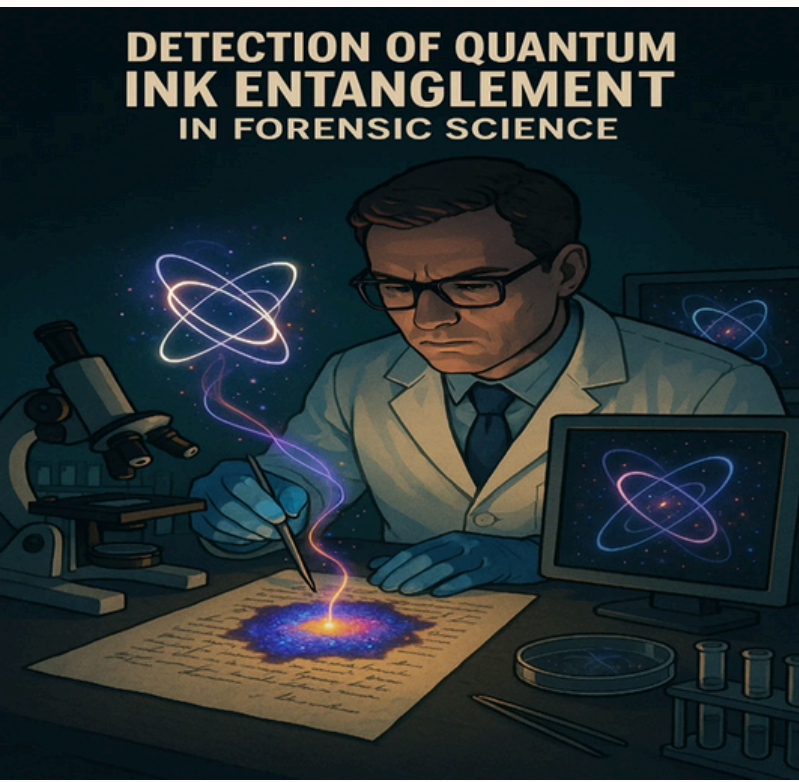


Fig. Detection of Quantum ink entanglement

Artificial Intelligence (AI)-Powered Authorial Fingerprinting:

Future AI programs could analyze thousands of linguistic and psychological characteristics to come up with their own "fingerprint of authorship" that can be identified even when the style of a writer is deliberately disguised. The next generation of AI application avenues, based on encouragement in Natural Language Processing (NLP), .

and deep learning, will be to develop highly resistant to "authorial fingerprints" AI will focus on examining thousands of minutes of linguistic, syntactic, and even psychological features placed deep in the text of a writer. It does not merely entail putting together typical words and grammatical constructions but also subtle semantic tastes, idiomatic usage, error patterns, and predisposed cognition (Computational Psycholinguistics Journal, 2018).

Augmented Reality (AR) Document Scanning:

Using forensic AR glasses, this advanced solution would enable forensic specialists to analyze documents in multi-layered AR views, showing ink age, pressure depth, and changes in real-time. This advanced solution for forensic document examination leverages augmented reality to provide specialists with multi-layered, real-time insights into document integrity. The theoretical framework combines high-resolution imaging, spectral analysis (e.g., multispectral, hyperspectral imaging), and sophisticated AR visualization technologies (AR in Forensic Science, 2024). Forensic AR glasses would be equipped with specialized cameras and sensors capable of capturing light across various spectra (UV, visible, IR) and potentially performing precise 3D surface mapping (AR in Forensic Science, 2024).

Time-Reverse Document Reconstruction:

Time-Reverse Document Reconstruction is a hypothetical artificial intelligence application that suffers a corrupted document back to its initial type, in effect undoing forgeries hindsightedly, via simulation. Time-Reverse Document Reconstruction is a thought experiment artificial intelligence system to reverse the effects of forgery and tampering on a document, simulating the theoretical basis of such AI system would comprise a generative modeling (e.g. Generative Adversarial Networks or Diffusion Models) and contextual reasoning (AI for Forgery Reversal, 2020). The speed at which large volumes of genuine documents, popular forgery methods, and degradation patterns are trained would be trained in the AI. Upon receiving a tempered document, the AI would then utilize structural, textual, as well as contextual forms of prediction to recognize anomalies that signify an edit.

Forensic Scenario	Advanced Techniques	Imaginary Techniques
Signature forgery	3D handwriting topography, AI recognition	Neurotrace mapping
Document tampering detection	Hyperspectral imaging, ESDA	AR layer scanning
Anonymous threat letter	Linguistics profiling, FISH system	AI authorial fingerprinting
Ink and paper origin verification	Raman spectroscopy, TLC ink dating	DNA embedded ink, nano-tagants
Erased writing recovery	ESDA, digital image enhancement	Time-reverse reconstruction

Concluding Insights:

Questioned document research is developing rapidly, due to advances in forensic linguistics, artificial intelligence, spectroscopy and imaging. But new concepts such as neurotrace authorship mapping and quantum ink demonstrate that it is possible to go futuristic in forensics documentation analysis. Although the hypothetical approaches are not necessarily practical as of now, they provide the drive to keep studying and advancing forensic science in general. Coupling existing and hypothetical technologies offers welcoming possibilities of making QDE more reliable, effective, and powerful in the twenty-first century.

References:

Mathur, S. (2023). Questioned Documents Examination-Modern Procedures for Better Efficiency. *Forensic Science and Human Rights*, 248.

Calcerrada, M., & García-Ruiz, C. (2015). Analysis of questioned documents: A review. *Analytica chimica acta*, 853, 143-166.

García-Ruiz, M. C. C. (2001). Review on the analysis of questioned documents. *Forensic Sci*, 46, 21-30.

Devlin, C., Morelato, M., & Baechler, S. (2024). Forensic intelligence: Expanding the potential of forensic document examination. *Wiley Interdisciplinary Reviews: Forensic Science*, 6(5), e1528.

De Alcaraz-Fossoul, J., & Roberts, K. A. (2017). Forensic intelligence applied to questioned document analysis: A model and its application against organized crime. *Science & Justice*, 57(4), 314-320.

Kumar, R., & Sharma, V. (2023). *Questioned Document Examination*.

Kelly, J. S., & Lindblom, B. S. (2006). *Scientific examination of questioned documents* (2nd ed.). CRC Press.

Srihari, S. N., Cha, S. H., Arora, H., & Lee, S. (2002). Individuality of handwriting. *Journal of Forensic Sciences*, 47(4), 856-872.

Wagner, R. (2015). Hyperspectral imaging in the forensic sciences. *Journal of Imaging Science and Technology*, 59(5), 050901.

Mr. Yash Babaria

Assistant Professor, Department of Forensic
Science, Bahauddin Science College,
Junagadh, Gujarat, India.



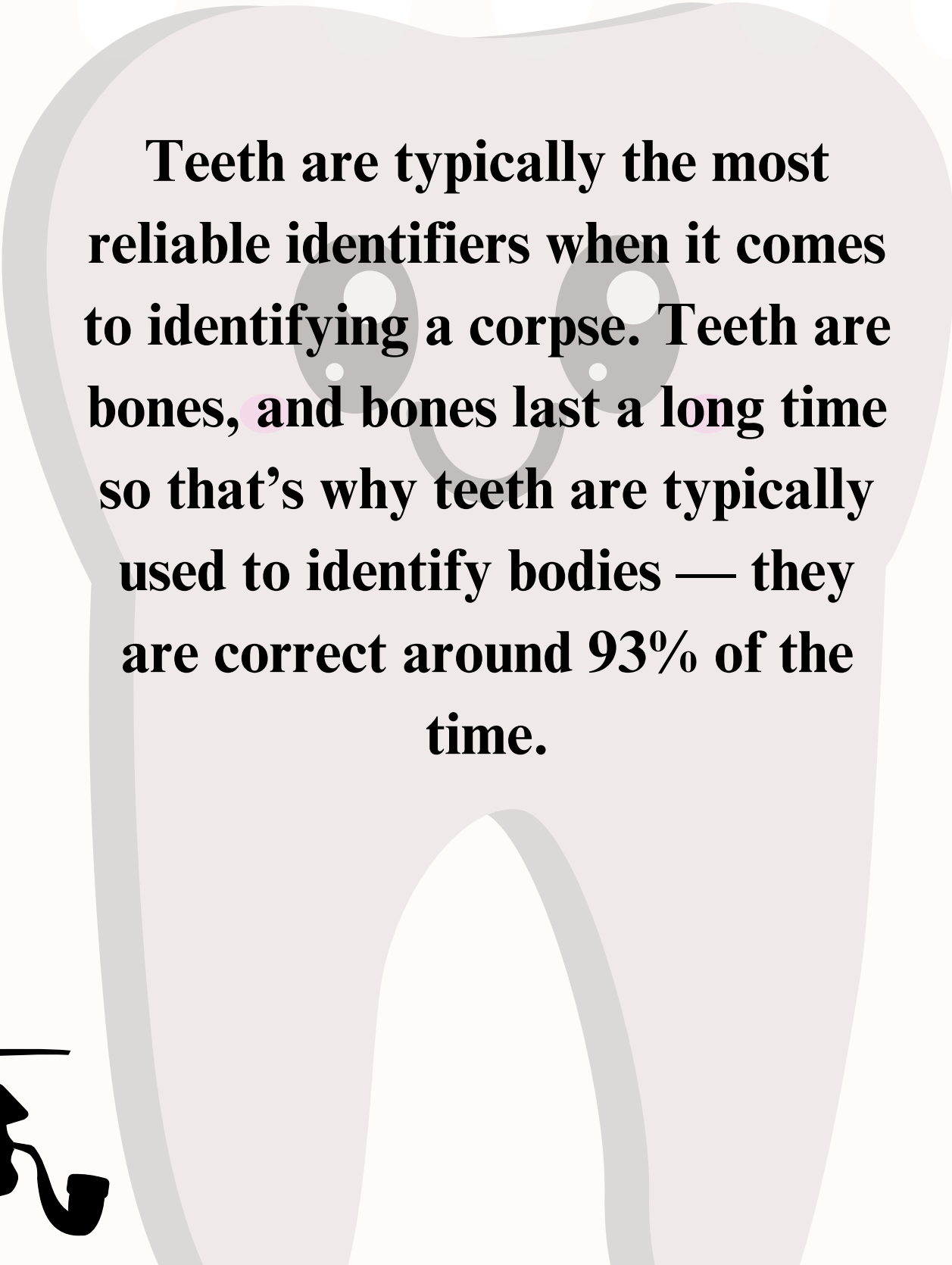
Mr. Bhumit Chavda

Research Scholar, Department of Biochemistry
and Forensic Science, School of Science, Gujarat
University, Ahmedabad, India.





DID YOU KNOW?

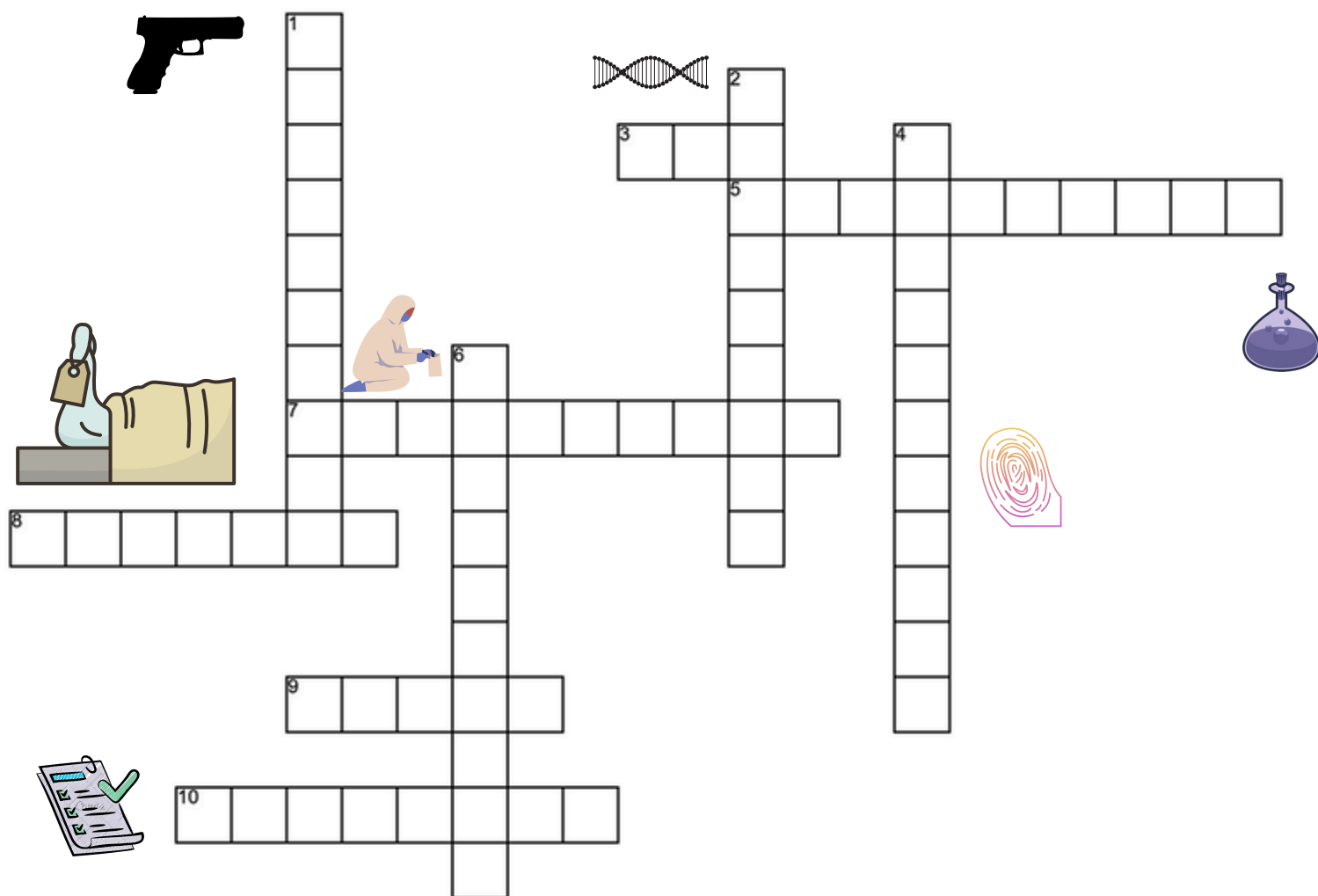


Teeth are typically the most reliable identifiers when it comes to identifying a corpse. Teeth are bones, and bones last a long time so that's why teeth are typically used to identify bodies — they are correct around 93% of the time.





Forensic Crossword



Across

- 3. Genetic material used to identify individuals with high accuracy.
- 5. Analysis of bodily fluids and tissues for toxins or drugs.
- 6. Any material or data that helps prove or disprove facts in a case.
- 8. Marks left by tools, tires, or footwear used for comparison.
- 10. Microscopic evidence such as hair, fibers, or paint.

Down

- 1. Study of firearms, bullets, and projectile motion in crimes.
- 2. Medical study of disease and injury, especially for legal purposes.
- 4. Unique ridge patterns left by fingerprint.

MITOCHONDRIAL DNA AND BEYOND: EXPANDING THE REACH OF FORENSIC GENEALOGY

Author - Sagar Harwani, Bhunit Chavda

Introduction

Have you ever considered the possibility that a single skin cell, a hair, or even a forgotten drop of blood may hold the solution to an a centuries-old mystery? Imagine a society in which even the slightest biological trace, once written off as unimportant, can reveal plenty of information about a person, their family, their heritage, and their ties to a crime scene. Welcome to the exciting field of forensic genealogy, where the use of DNA, particularly mitochondrial DNA, is enabling law enforcement to address previously unsolved cases and bring justice to those affected.

The autosomal short tandem repeat (STR) profile, a distinct genetic fingerprint obtained from the 22 pairs of non-sex chromosomes, has been the gold standard in forensic DNA analysis for years. By enabling us to connect suspects to evidence with better clarity, this powerful tool has transformed the crime scene investigation process. However, what occurs if CODIS (the Combined DNA Index System) does not show a direct match? What happens if the sample is too little or too deteriorated to get a complete STR profile or if the offender's DNA is not in any databases? Here is where forensic genealogy, previously limited to tracing family lines for private purposes, has changed the game, with mitochondrial DNA playing a crucial role in solving many cold cases.

The Mitochondrial Maestro: A DNA Detective with Deep Roots

To properly understand the significant influence that mitochondrial DNA (mtDNA) has on forensic genealogy we must briefly explore the fantastic universe of our cells. Tiny organelles known as mitochondria are located outside the nucleus, which serves as the command centre of the cell. These are our cells' powerhouses, producing the energy required for us to survive.

However, here is the crucial twist: Mitochondria have their own small, circular DNA molecule known as mitochondrial DNA.

Mitochondrial DNA is inherited solely from the mother, in contrast to nuclear DNA, which is a combination of genetic information from both parents. This maternal inheritance pattern is a double-edged sword. On one hand, it means that all individuals tracing back to a common maternal ancestor will share the same mitochondrial DNA (mtDNA) sequence. This can be a disadvantage in identifying a suspect, as many individuals in a maternal lineage will share the same mitochondrial DNA (mtDNA) profile. On the other hand, this very characteristic makes mtDNA an incredibly powerful tool for tracing distant maternal lineages and for analysing highly degraded or limited samples.

The analysis of the mtDNA focuses on the specific regions, particularly the hypervariable regions 1 (HV1) and 2 (HV2) and sometimes HV3. These regions accumulate mutations more frequently than other parts of the mtDNA genome, making them useful for distinguishing between unrelated individuals and for tracing maternal lines over generations. While mtDNA analysis won't uniquely identify, it can exclude individuals and, more importantly for forensic genealogy, narrow down potential familial relationship. Imagine a crime scene where only a hair shaft, without its root, is found. Nuclear DNA found in the nucleus of cells, which remains concentrated in the



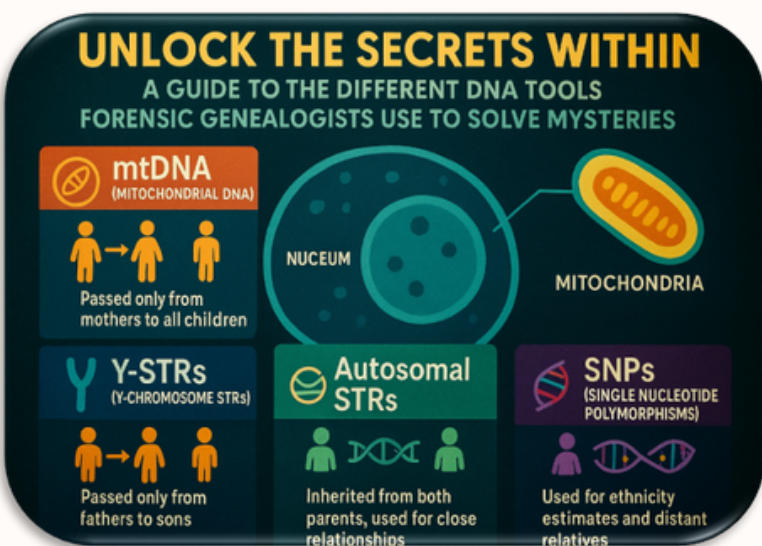
he hair root. Without it, obtaining a complete STR profile is often impossible. However, hair shafts are rich in mitochondria. This makes mtDNA an irreplaceable resource in such scenarios. Similarly, in heavily degraded bone or ancient remains, where nuclear DNA might be fragmented beyond repair, mtDNA often persists due to its circular nature and high copy number within each cell. A single cell can contain hundreds to thousands of mitochondria, which suggestively increases the chances of recovering viable DNA for analysis.

The analysis of mtDNA focuses on specific regions, particularly the hypervariable regions 1 (HV1) and 2 (HV2), and sometimes HV3. Since these regions accumulate mutations more frequently than other parts of the mtDNA genome, they help distinguishing between unrelated individuals and for tracing maternal lines over generations. While mtDNA analysis cannot uniquely identify an individual (unless it belongs to a very rare haplogroup), it can exclude individuals and, more importantly for forensic genealogy, narrow down potential familial relationships.

treasure troves of genetic information shared voluntarily by millions of individuals curious about their ancestry. These databases enable users to upload their raw DNA data, which may include mtDNA profiles, and identify genetic relatives based on shared DNA segments.

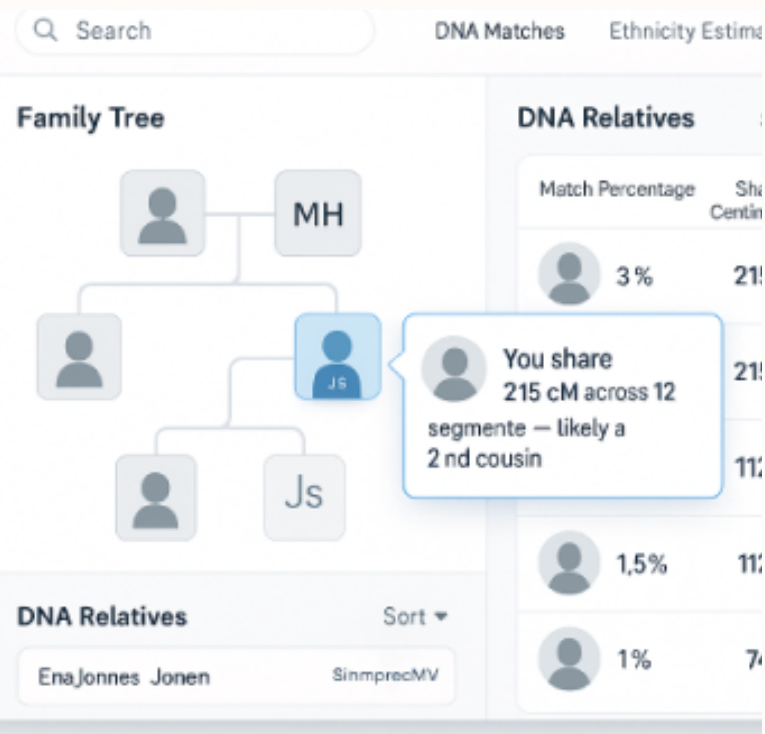
When investigators have an mtDNA profile from a crime scene, they can, with appropriate legal authorization, upload this profile to these public databases. The system then searches for matches – individuals who share a similar or identical mtDNA sequence. These matches aren't necessarily the perpetrator, but they are genetically related to the perpetrator through their maternal lineage.

Think of it like casting a wide net. Every match represents a thread in a complicated web of family connections. Forensic genealogists, armed with this genetic information, then precisely construct family trees, working backward and forward through generations, combining genetic clues with traditional genealogical research using birth records, marriage licenses, obituaries, census data, and old newspaper articles. They look for common ancestors shared by the database matches, eventually narrowing down the potential pool of suspects to a manageable number. This process can be painstakingly slow, requiring immense dedication and expertise. It's not uncommon for genealogists to build trees spanning hundreds of years and involving thousands of individuals. They accurately identify "mystery branches" – individuals who might fit the profile of the unknown perpetrator. Once a few potential candidates are identified, traditional police work takes over, focusing on corroborating evidence, excluding false identifications, and ultimately obtaining a DNA sample for direct comparison with the crime scene evidence using the highly individualizing autosomal STR method. The success stories are numerous and compelling. The identification of the Golden State Killer, Joseph DeAngelo, in 2018 is perhaps the most famous example of forensic genealogy's power, although it primarily utilized autosomal DNA. However, mtDNA has been instrumental in solving numerous cold cases where only limited or degraded samples were available. Cases involving unidentified human remains, where mtDNA can help pinpoint a maternal lineage and guide investigations to potential families, have also seen significant breakthroughs



Beyond the Bench: Connecting the Dots with Public Databases

The true power of mtDNA in forensic genealogy lies in its intersection with publicly accessible genetic genealogy databases. Platforms like GEDmatch, Family-tree DNA, and 23andMe (though 23andMe and AncestryDNA have stricter policies regarding law enforcement access without a warrant) have become



Expanding the Genetic Toolkit: Beyond Mitochondrial DNA

While mtDNA is a cornerstone of forensic genealogy, the field is constantly evolving, incorporating other powerful genetic tools to overcome its inherent limitations and further expand its reach.

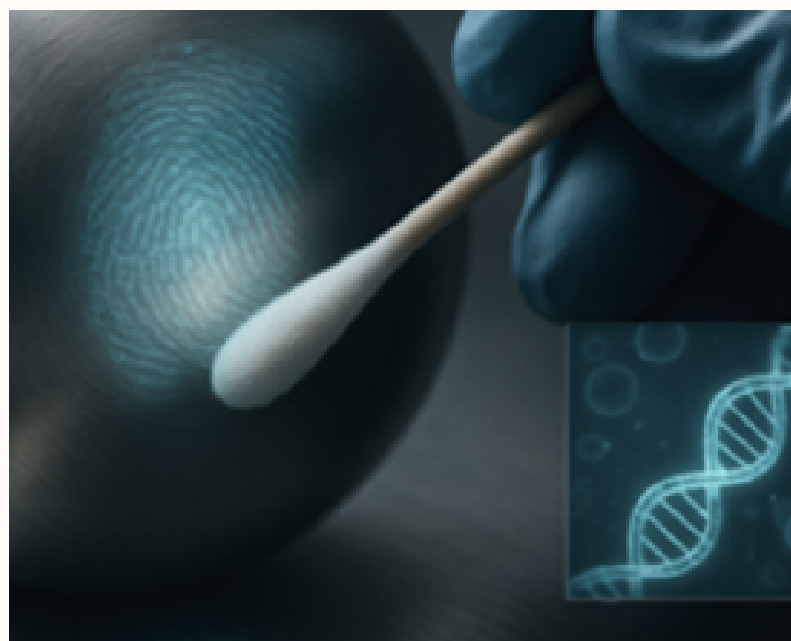
Y-Chromosome DNA (Y-STRs): Just as mtDNA traces the maternal line, the Y-chromosome is exclusively passed down from father to son. Y-STR analysis, similar to autosomal STRs but specific to the Y-chromosome, provides insights into paternal lineages. If the crime scene evidence contains male DNA and no direct CODIS hit, Y-STR analysis can be performed. This profile can then be compared to Y-STR databases (both forensic and genetic genealogy-oriented) to identify paternal relatives of the unknown perpetrator. While Y-STRs, like mtDNA, do not provide individualization, they are invaluable for narrowing down the pool of potential suspects to a male lineage, particularly in cases involving male-on-male violence or where the perpetrator is known to be male.

Single Nucleotide Polymorphisms (SNPs) and Genomic Sequencing: The future of forensic genealogy is undoubtedly moving towards more comprehensive genomic analysis, leveraging Single Nucleotide Polymorphisms (SNPs).

SNPs are variations at a single base pair in the DNA sequence, and they are far more abundant in the genome than STRs. While STRs are highly polymorphic and excellent for individual identification, SNPs provide a broader view of an individual's ancestry, phenotypic traits (like hair and eye colour, biogeographical ancestry), and familial relationships over longer time scales.

The beauty of SNP data lies in its sheer volume. Genetic genealogy databases primarily use SNP arrays, which analyse hundreds of thousands to millions of SNPs across the entire genome. When crime scene DNA is analysed using SNP arrays (or even whole-genome sequencing in the future), the resulting SNP profile can be uploaded to these databases, leading to a much higher chance of finding distant relatives than with limited STR or mtDNA profiles alone. This wealth of SNP information allows for the identification of much more distant familial connections, sometimes as far back as 5th or 6th cousins, significantly expanding the pool of potential genetic leads.

Moreover, advancements in massively parallel sequencing also known as next-generation sequencing (NGS), are revolutionizing forensic DNA analysis. NGS can analyse highly degraded and low-quantity samples that might be challenging for traditional methods. It also allows for the simultaneous analysis of multiple genetic markers – STRs, SNPs, and even mtDNA – from a single sample, providing a more comprehensive genetic profile and maximizing the information obtained from precious evidence. This integrated approach promises to accelerate the genealogical process and increase the success rate of identifying perpetrators.

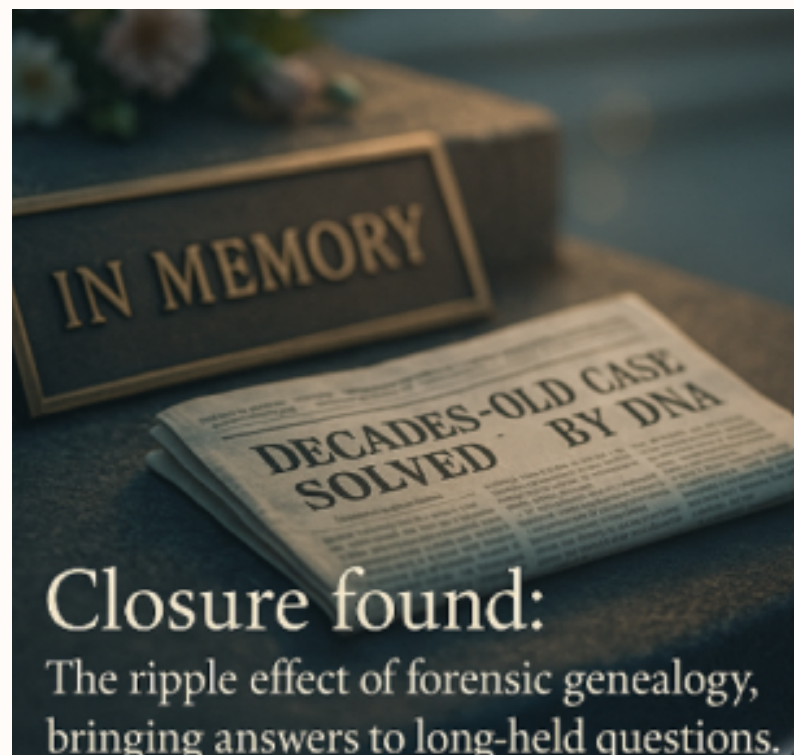


Ethical Labyrinths and the Future Landscape

While the advancements in forensic genealogy are undoubtedly thrilling and hold immense promise for justice, they also navigate complex ethical and privacy considerations. The use of public genetic genealogy databases by law enforcement has sparked considerable debate. Concerns revolve around:

- **Privacy:** Individuals who voluntarily upload their DNA to these databases do so for personal reasons, often without anticipating that genetic information might be used in criminal investigations. While most reputable databases have updated their terms of service to address law enforcement access, the initial "implied consent" was a point of contention.
- **Scope:** Critics argue about the potential for overreach and the implications for the privacy of innocent relatives who share DNA with a suspect.
- **Database Policies:** The varied policies of different genetic genealogy databases regarding law enforcement access create a fragmented landscape. Some databases require a warrant, others allow access with user consent through an "opt-in" model, and some prohibit law enforcement use entirely. This inconsistency can hinder investigations and raise questions of fairness.
- **Bias:** There are also concerns about potential biases if certain demographic groups are underrepresented in these databases, which could lead to disproportionate targeting or exclusion. Addressing these concerns requires careful consideration and the development of robust ethical guidelines and legal frameworks. Transparency in how law enforcement uses these tools, clear communication with the public, and ongoing dialogue between law enforcement, genetic genealogists, privacy advocates, and the public are crucial for ensuring the responsible and ethical application of this powerful technology.
- **Looking ahead,** the landscape of forensic genealogy is expected to continue evolving rapidly. We can anticipate:
 - **Increased Integration:** A more seamless integration of traditional forensic DNA analysis with genealogical methods, with a focus on

- maximizing information from limited samples. Advanced Bioinformatics Tools: Development of more sophisticated algorithms and bioinformatics tools to analyse complex genomic data, build extensive family trees, and identify more distant familial relationships with greater accuracy.
- **Standardization and Regulation:** Greater standardization of practices and potentially more formalized regulation around the use of genetic genealogy in criminal investigations, balancing investigative needs with individual privacy rights.
- **Broader Application:** The application of forensic genealogy beyond cold cases to areas like disaster victim identification, human trafficking investigations, and even historical mysteries, where traditional methods have reached their limits.



Conclusion: A New Era of Justice

The journey from a forgotten hair shaft to the identifying the perpetrator, guided by the intricate threads of DNA, is a testament to human ingenuity and scientific progress. Mitochondrial DNA, with its unique maternal inheritance pattern and resilience in degraded samples, has been a quiet but powerful force in this revolution. Beyond mtDNA, the expanding toolkit of Y-STRs, and most significantly, the promise of comprehensive genomic sequencing using SNPs, are pushing the boundaries of what is possible in forensic science.

Forensic genealogy is more than just a scientific technique; it's a testament to the enduring power of family connections, albeit often in unexpected and profound ways. It offers a glimmer of hope for families of victims who have waited years, sometimes decades, for answers. As we continue to navigate the exciting and challenging ethical terrain, one thing is clear: the reach of forensic genealogy will only continue to expand, unravelling more family secrets and bringing us closer to a future where justice is truly within reach, even for the coldest of cases. The story of our DNA turns out to be a far more intricate and revealing one than we ever imagined.

References

1. Stoneking M. Hypervariable sites in the mtDNA control region are mutational hotspots. *Am J Hum Genet* [Internet]. 2000 [cited 2025 Jul 6];67(4):1029–32. Available from: <https://pubmed.ncbi.nlm.nih.gov/10968778/>
2. Kling D, Phillips C, Kennett D, Tillmar A. Investigative genetic genealogy: Current methods, knowledge and practice. *Forensic Sci Int Genet* [Internet]. 2021 May 1 [cited 2025 Jul 6];52:102474. Available from: <https://www.sciencedirect.com/science/article/pii/S1872497321000132>
3. Berkman BE, Miller WK, Grady C. Is It Ethical to Use Genealogy Data to Solve Crimes? *Ann Intern Med* [Internet]. 2018 Sep 4 [cited 2025 Jul 6];169(5):333. Available from: <https://pmc.ncbi.nlm.nih.gov/articles/PMC6123268/>
4. Holland MM, Parsons TJ. Mitochondrial DNA Sequence Analysis - Validation and Use for Forensic Casework. *Forensic Sci Rev*. 1999 Jun;11(1):21–50.
5. Advanced Topics in Forensic DNA Typing: Interpretation | ScienceDirect [Internet]. [cited 2025 Jul 6]. Available from: <https://www.sciencedirect.com/book/9780124052130/advanced-topics-in-forensic-dna-typing-interpretation>
6. Quintana-Murci L, Krausz C, McElreavey K. The human Y chromosome: function, evolution and disease. *Forensic Sci Int* [Internet]. 2001 May 15 [cited 2025 Jul 6];118(2–3):169–81. Available from: <https://www.sciencedirect.com/science/article/abs/pii/S0379073801003875>
7. Goodwin William, Linacre Adrian, Hadi Sibte. An introduction to forensic genetics. 2011 [cited 2025 Jul 6];198. Available from: <https://www.wiley.com/en-us/An+Introduction+to+Forensic+Genetics%2C+2nd+Edition-p-9780470710197>
8. Bruijns B, Tiggelaar R, Gardeniers H. Massively parallel sequencing techniques for forensics: A review. *Electrophoresis* [Internet]. 2018 Nov 1 [cited 2025 Jul 6];39(21):2642–54. Available from: <https://pubmed.ncbi.nlm.nih.gov/30101986/>
9. Canales Serrano A. Forensic DNA phenotyping: A promising tool to aid forensic investigation. Current situation. *Spanish Journal of Legal Medicine* [Internet]. 2020 Oct 1 [cited 2025 Jul 6];46(4):183–90. Available from: <https://www.sciencedirect.com/science/article/abs/pii/S2445424920300327>
10. Wickenheiser RA. Forensic genealogy, bioethics and the Golden State Killer case. *Forensic Sci Int* [Internet]. 2019 Jan 1 [cited 2025 Jul 6];1:114. Available from: <https://pmc.ncbi.nlm.nih.gov/articles/PMC7219171/>
11. García Ó. Forensic genealogy. Social, ethical, legal and scientific implications. *Spanish Journal of Legal Medicine* [Internet]. 2021 Jul 1 [cited 2025 Jul 6];47(3):112–9. Available from: <https://www.sciencedirect.com/science/article/abs/pii/S244542492100025X>

ABOUT THE AUTHORS

Mr. Sagar Harwani

Research Scholar, Department of Biochemistry
and Forensic Science, School of Science, Gujarat
University, Ahmedabad, India.



Mr. Bhumit Chavda

Research Scholar, Department of Biochemistry
and Forensic Science, School of Science, Gujarat
University, Ahmedabad, India.



BEHIND THE MASK: THE RISE OF DEEPPFAKE HACKTIVISM

Author - Leeba Pathan, Kiran Dodiya, and Dr. Kapil Kumar

Abstract

In an age where artificial intelligence can fabricate hyper-realistic videos and audio, the emergence of deepfake hacktivism signals a complete evolution in digital conflicts. In this article we explore the convergence of deepfake technology and hacktivism, revealing how synthetic media is being weaponized to challenge the power structures, manipulate perception and also disrupt political and social order. This article dissects deepfake attacks by examining their orchestration, from target selection and data harvesting to AI generation and strategic dissemination, it analyzing the psychological and societal consequences of fabricated realities that including the erosion of trust and potential for manipulation. It also unpacks the murky ethical terrain that separates whistleblower from propagandist this highlighting the growing phenomenon of “reality apathy” and the erosion of public trust in visual media. With the real-world example which is ranging from geopolitical disinformation to CEO impersonations, the piece underscores the urgency of digital literacy, policy reform, and AI-driven detection tools. Ultimately, the article argues that in a world where truth can be convincingly forged, preserving a shared sense of reality requires not just technical solutions, but cultural and ethical resilience.

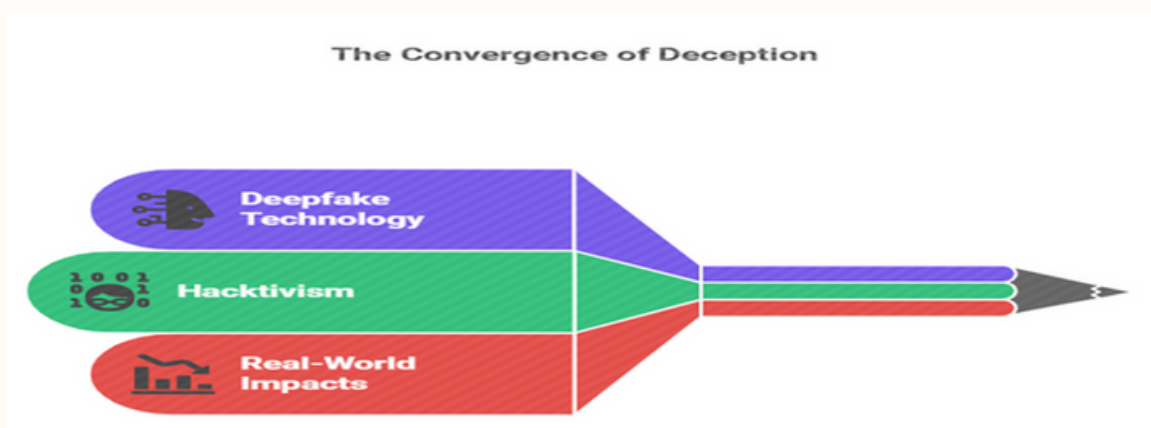
Introduction

In today’s digital world where digital information spreads faster than wildfires, the truth is no longer in anyone for anyone

The Deepfakes create a realistic but entirely fabricated audio, video, or images generated by artificial intelligence and Machine Learning Algorithms. When we combine that with the rising tide of Hacktivism it is activism through hacking and you get a potent new form of disruption which is Deepfake Hacktivism. Deepfakes were once the stuff of science fiction, but in today world, with the help of modest computer and open-source software, anyone can synthesize someone else's face and voice to say or do things they never actually did in their life's. Hacktivists are now deploying deepfakes as tools to

Subvert authority, sabotage corporations and incite social chaos this all is behind a mask that cannot be easily removed. In March 2022, a deepfake video of Ukrainian President Volodymyr Zelenskyy appearing to surrender to Russian forces briefly circulated online, attempting to disorient and manipulate the public during a time of war. Just months later, a fake press conference video caused a Fortune 500 company’s stock to plummet by 8%, all thanks to a believable CEO deepfake announcing bankruptcy.

This article explores how deepfake hacktivism is evolving, who’s behind the masks, and what it means for the future of truth, trust, and technology.



The Evolution of Deepfake Technology

Deepfakes come from advancements in artificial intelligence, specifically a Generative Adversarial Networks (GANs) it is a class of machine learning algorithms where two neural networks “compete” to create and detect fake media. In a GAN, the generator tries to produce synthetic content that looks real, while on the other side discriminator evaluates its authenticity. Over the time, the generator gets better at fooling the discriminator, it ultimately producing results are indistinguishable from the reality.

When deepfakes first appeared in 2017, they were mostly limited to online communities which focused on entertainment or deception, such as inserting celebrities into adult content. But the underlying technology has rapidly evolved. Tools like DeepFaceLab, FaceSwap, and Synthesia have made it easier for non-experts to create convincing videos. AI voice cloning platforms like ElevenLabs or Descript Overdub can now mimic speech patterns with chilling accuracy of any audio.

This standardizing of AI has a double lead, while the artists and filmmakers use it for their creativity and malicious actors use it for manipulation and spreading rumours. A Hollywood studio budget is now achievable in a teenager’s bedroom. And this increasing accessibility of technology has opened the door to politically or ideologically motivated hackers who can now fabricate personas, evidence, and events with impunity and blurring the lines between digital protest and cybercrimes.

Moreover, social media platforms act as high-speed distribution channels. As a deepfake doesn’t need to fool everyone to be effectively; it just needs to reach a critical mass before it is being exposed. By the time fact-checkers catch up the manipulated content but it may be late, the psychological damage may already be happened.

Hactivism: From Anonymous to AI

Hactivism is not a new activism. It is since the early 2000s, groups like Anonymous, LulzSec and WikiLeaks have used digital tools to expose the secrets, protest censorship and disrupt the existing state. Traditionally, their arsenal included Distributed Denial-of-Service (DDoS) attacks, data breaches, website defacement and doxxing.

The distinguished between hactivists from cybercriminals was often intent. Hactivists were not (always) do it for the money; they were motivated by causes the free speech, anti-corruption, anti-capitalism, or environmental justice. In many ways, they mirrored old-school revolutionaries, just armed with laptops instead of leaflets and explosives. Deepfakes, fuelled by the rise of visual and algorithm-driven internet culture, are a potent tool for manipulation, leveraging AI to create convincing but fabricated content, offering a blend of performance, provocation, and plausible deniability.

The Rise and Evolution of Deepfake Technology



Imagine a video of a dictator admitting to war crimes, or a fake recording of a CEO making racist comments which are released by hacktivists not for financial gain, but to incite protest, cause reputational harm, or trigger policy changes. This is deepfake Hactivism is not just hacking systems, but hacking perception itself.

Deepfake hactivism is so dangerous that it can be psychological manipulation. It destroys the ability to differentiate between real and fake, truth and fabrication. When reality becomes subjective, people fall back on prejudice and bad actors exploit this chaos.

These new-age hacktivists aren't always part of known collectives. Some operate as lone wolves. Others hide within state-sponsored networks. Some claim to be whistleblowers, others provocateurs. But they all wear the same digital mask, a hidden face of revolution in a time when reality can be rewritten in code.

FROM ANONYMOUS TO AI

Deepfakes, fuelled by the rise of visual and algorithm-driven internet culture, are a potent tool for manipulation, leveraging AI to create convincing but fabricated content.



Anatomy of a Deepfake Attack

A deepfake hactivist attack is not just about the video or audio clip itself. It's a calculated process of planning, creation, and distribution. It's often designed to go viral before it can be detected and verified. Let's analyze an operation usually evolves, the following are the steps:

1) Target Selection

The first step is choosing the target. It usually someone influential or symbolic like Politicians, CEOs, journalists, or activists often top the list. The goal is to either discredit them or cause institutional disruption. Hacktivists may look for a weak point: someone with a lot of publicly available content that can be scraped to train AI models.

2) Data Harvesting

To make a convincing deepfake, we need give training on available data. Hours of video, hundreds of photos, voice samples, this all data are publicly available thanks to social media, public speeches, interviews, and podcasts. Software can crawl platforms like YouTube, Facebook, Twitter or Instagram to gather facial expressions and voice inflections.

Once enough data is collected, AI algorithms begin analyzing every blink, smirk and speech pattern. The more data, the more lifelike the fake will be.

3) Generation of the Deepfake

Using machine learning platforms like DeepFaceLab, FaceSwap, or more advanced GAN-based tools, creators can generate a fake video in which the target appears to say or do something they never did in there life's. The voice cloning software like Resemble.ai or iSpeech adds the layer of auditory authenticity.

The advanced operators even simulate a background noises, lighting conditions or even camera shake to mimic real-life videos.

4) Strategic Distribution

Once the media is ready, the deepfake is strategically released. Hacktivists do not just drop it online they also seed it through anonymous accounts, influencers or bots to create the illusion of legitimacy. It might be "leaked" to journalists, disguised as a whistleblower tip, or posted to Reddit and Twitter with clickbait headlines.

The goal is to amplify it before fact-checkers can verify or debunk it. In the heat of a crisis or politically charged moment, people are more likely to share that media they do not focus on doing research on its reality.

5) Psychological Impact

The real damage begins after the video spreads online. The public trust is in the target and destroys. People argue, disunite and speculate (guess about something). In the best-case scenario, the deepfake is falsified quickly but by then, its impact has often already been felt.

Take the 2022 case where a deepfake video of Ukrainian President Zelenskyy appeared on a hacked TV channel and Facebook pages, telling Ukrainian forces to surrender. It was quickly falsified but it briefly sowed confusion and panic in a war-torn population. It was a psychological operation not just a digital one, that intentionally caused a confusion and panickness in a war-torn population.

A one more example: a deepfake audio clip of a company's CFO announcing missed earnings leaked on a financial forum. Even before any media picked it up, the company's stock took a temporary drop. Investors reacted emotionally before verifying anything about that stock.

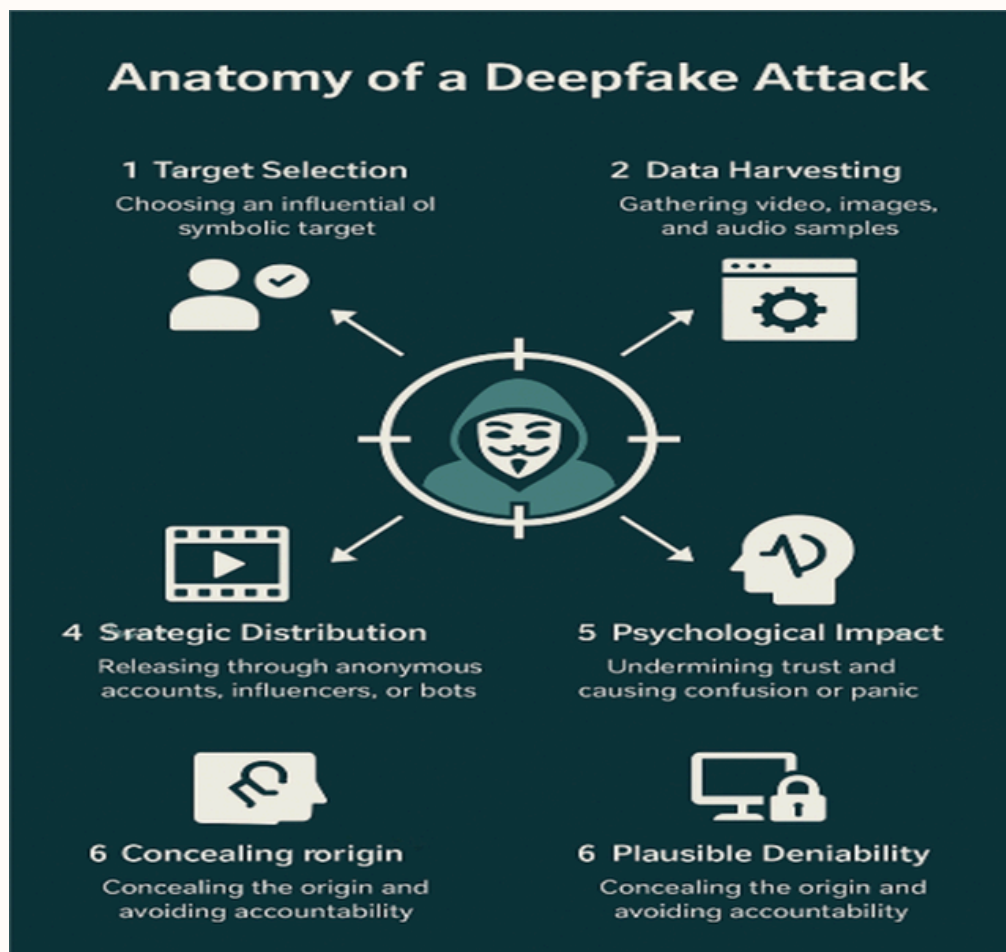
6) Plausible Deniability

In the final step there is a disturbing twist: The deepfake hacktivists rarely get caught. And even when the content is exposed as fake, the origin is difficult to trace. The attackers use VPNs, dark web forums, and decentralized storage systems like IPFS (Inter Planetary File System) to distribute and protect their work.

Even it is more troubling because real footage can now be dismissed as deepfake this concept known as the liar's dividend. In an age where fakes are believable, truth itself can be denied, creating a feedback loop of mistrust that benefits the manipulators.

Motives and Morality

Deepfake hacktivism lives in a moral grey zone. Depending on who you ask, it's either the modern face of digital resistance or a form of cyber terrorism disguised as activism. The line between protest and propaganda is thin and getting thinner day by day.



1) Fighting for a Cause or Fueling Chaos?

Traditional hacktivism often carried an ethical backbone. Groups like Anonymous or LulzSec had slogans like “We are legion. We do not forgive. We do not forget,” and targeted governments, corporations, or entities accused of wrongdoing. Whether leaking classified documents or taking down oppressive websites, their actions were usually ideologically motivated.

Deepfake hacktivists claim similar ground. Some target oppressive rules, corrupt politicians or exploitative corporations. Their argument: Mainstream media can be silenced, whistleblowers persecuted but a viral deepfake can spark public outrage and ignite change. In this view, the deepfake is a digital Molotov cocktail: provocative but necessary. However, others use the same technology for misinformation, manipulation or chaos. They might release deepfakes to sway elections, crash stock markets, or frame individuals. In these cases, the goal is not justice it’s disruption. Some just want to watch the world burn, with no allegiance to truth or transparency.

2) The Intent vs. the Impact

Ethically, intent matters but so does impact. A deepfake targeting a war criminal may seem noble, but if it escalates conflict or misleads the public, and it may be unintended consequence. A deepfake meant as satire could be taken seriously, causing real-world harm.

Even more complex is the question of truthfulness. If a deepfake shows a politician saying what they actually believe, even if they did not say it aloud that may be make it “ethically accurate”. Can digital lies ever reveal a deeper truth?

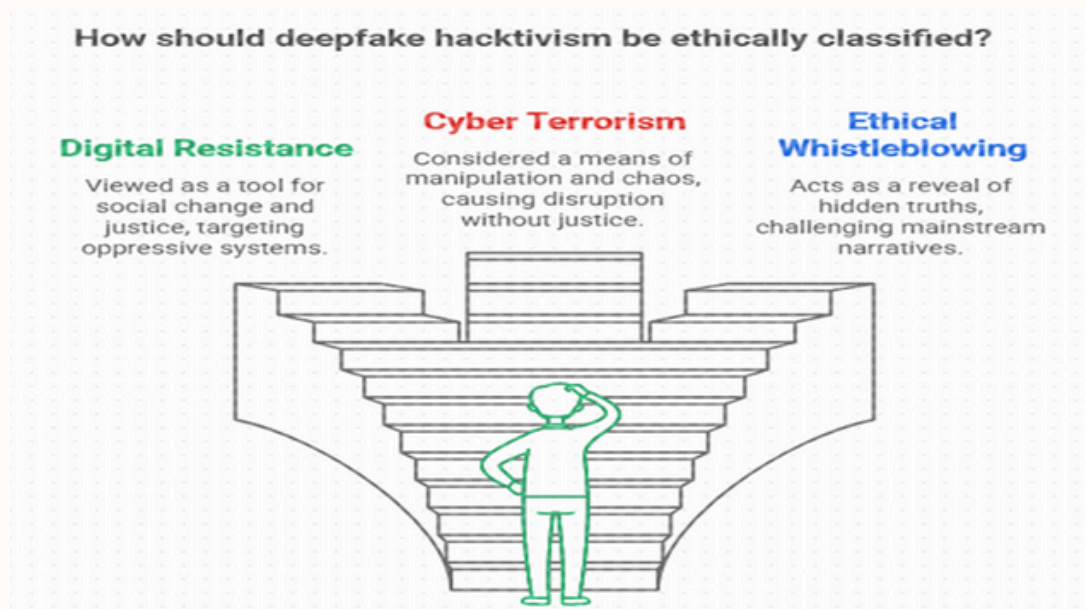
These is the questions ethicists, lawmakers and tech companies are now grappling with. The answers are not easy. What’s the clear is that deepfake hacktivism forces us to confront our assumptions about what truth looks like and whether truth alone is enough to protect us in the digital age.

3) Whistleblower or Anarchist?

Motives vary widely. Some deepfake hacktivists view themselves as digital whistleblowers, revealing “hidden truths” that the mainstream media ignores. Others act out of revenge, conspiracy belief or revenge. There are even cases of satire gone rogue deepfakes intended as parody that went viral and were mistaken for real.

This anonymity is what makes deepfake hacktivism so dangerous. Unlike traditional hacking, which can often be traced or verified through data logs, deepfakes live in the realm of perception. They do not destroy servers but they corrupt belief.

In the end, the morality of deepfake hacktivism may lie in the eye of the beholder. The revolutionary to one group may be reprehensible to another. But one thing’s for sure: as long as truth can be digitally reconstructed, ethics will remain in flux.



Societal and Political Impact

The rise of deepfake hacktivism is shaking the very foundations of how societies process truth. In an era already riddled with misinformation, this new layer of deception has profound implications for democracy, journalism and social stability.

1) The Death of “Seeing is believing”

For centuries, visual evidence was considered the gold standard. A photograph or video could validate claims, settle disputes or sway public opinion. But deepfakes have shattered that confidence. Now, even authentic footage is met with suspicion. Every viral video creates confusion and arises a question in mind that is this real or a fake media?

This situation is known as reality apathy, creates a chilling effect. When people can't trust what they see, they begin to trust nothing or worse, they trust only what aligns with their existing beliefs. In this environment, deepfakes don't need to be perfect to be effective they just creates a doubt in public's mind regarding its reality.

2) A New Weapon in Political Warfare

Deepfake hacktivism has become a tool for political disruption, especially in unstable democracies. Fake

videos of candidates saying inflammatory things can circulate just before elections, damaging reputations beyond repair even if it is quickly falsified. State-sponsored actors have also entered the game. Intelligence agencies and political operatives use deepfakes to spread disinformation, incite protests or discredit opposition leaders. It's a form of asymmetric warfare, where psychological influence replaces physical conflict.

And it's not limited to politics. Deepfakes have been used to impersonate CEOs on conference calls, fake press briefings and even engineer stock manipulations this eroding trust in financial markets and media alike.

3) The Erosion of Public Trust

The most dangerous long-term effect is the collapse of consensus reality. Deepfake hacktivism amplifies polarization by allowing people to “see” whatever supports their narrative. In this fragmented media landscape, truth becomes tribal.

As trust in institutions, journalism and democratic processes crumbles, it opens the door for authoritarianism and conspiracy movements. If nothing can be verified, then everything becomes believable and manipulators thrive in that void.



Combating Deepfake Hacktivism

While deepfake hacktivism poses a serious threat, it's not going unchallenged. Around the world, governments, tech companies and researchers are scrambling to build defences though the pace of innovation often trails the threat itself.

1) Detection Technologies

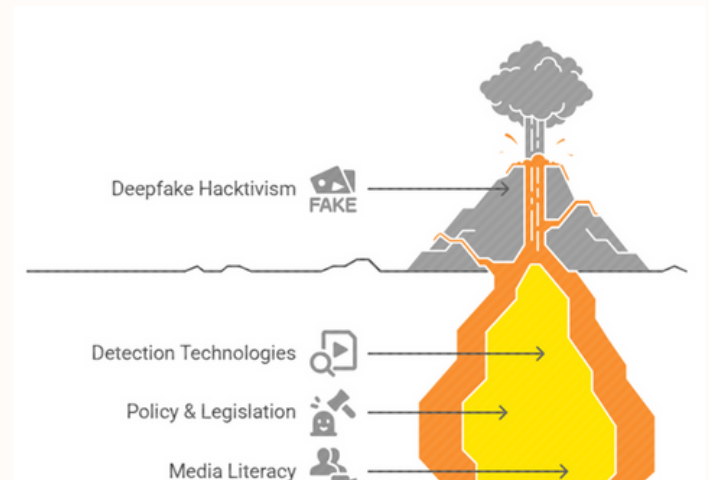
AI is being used to fight AI. Tools like Microsoft's Video Authenticator, Deepware Scanner and Sensity AI analyze videos for digital "fingerprints" that suggest manipulation of artifacts, inconsistencies in lighting, eye movement irregularities, or unnatural lip syncing. But as deepfake quality improves, detection becomes a game of cat and mouse.

2) Policy and Legislation

Some governments have started to legislate against malicious deepfakes. The EU's Digital Services Act includes provisions for combating manipulated media while U.S. states like California and Texas have laws criminalizing politically weaponized deepfakes. However, enforcement remains a challenge especially when attacks come from outside jurisdictions.

3) Media Literacy and Public Awareness

The strongest long-term defence is education. Teaching people to question, verify and recognize digital manipulation is essential. Journalists are being trained to spot deepfakes media, educators are introducing critical thinking into digital curriculums. The public must adapt to a world where truth requires discernment, not just observation.



Conclusion: Truth in the Age of Illusion

We are witnessing the dawn of a new era one where truth is not just questioned but actively engineered. Deepfake hacktivism is not merely a tech trend but it is a cultural shift, a psychological weapon and a profound challenge to our collective reality.

Behind every digitally forged face lies a motive whether it's resistance, revenge, manipulation or disorder. The danger is not just in what people are made to say or do in these fakes it's in what these fabrications erode: trust, accountability and shared truth.

The line between activism and anarchy has never been blurrier. Deepfake hacktivists argue that they are modern revolutionaries using the tools of their time to fight injustice. But revolution without truth can quickly become manipulation. And manipulation, unchecked, can poison democracies, destabilize institutions and leave societies adrift in a sea of doubt.

As technology is evolving, so we must have attentiveness. The fight against deepfake hacktivism is not just about better AI or stricter laws but it is about building a culture that values truth, demands transparency and is equipped to question on what they sees.

In the end, we must remember: the most dangerous mask is not the one you wear, but the one that convinces the world you were never wearing one at all.

References

1. Chesney, R., & Citron, D. K. (2019). Deepfakes and the New Disinformation War: The Coming Age of Post-Truth Geopolitics. Foreign Affairs. Retrieved from: <https://www.foreignaffairs.com/articles/2018-12-11/deepfakes-and-new-disinformation-war>
2. Ajder, H., Patrini, G., Cavalli, F., & Cullen, L. (2019). The State of Deepfakes: Landscape, Threats, and Impact. Sensity AI. Retrieved from: <https://sensity.ai/research/>
3. Harwell, D. (2022). A deepfake Zelensky video was quickly taken down — but this was just a test. The Washington Post. Retrieved from: <https://www.washingtonpost.com/technology/2022/03/16/zelensky-deepfake-video/>
4. Vincent, J. (2020). Deepfake CEO used to scam company out of \$243,000. The Verge. Retrieved from: <https://www.theverge.com/2020/6/29/21307055/deepfake-audio-scam-ceo-fraud-voice>
5. West, D. M. (2020). How to Combat Fake News and Disinformation. Brookings Institution. Retrieved from: <https://www.brookings.edu/research/how-to-combat-fake-news-and-disinformation/>
6. Microsoft. (2020). Microsoft develops new deepfake detection tool. Microsoft News Center. Retrieved from: <https://blogs.microsoft.com/on-the-issues/2020/09/01/disinformation-deepfakes-new-media-literacy/>
7. Tiku, N. (2020). AI-generated deepfake voices are getting freakishly good. Wired. Retrieved from: <https://www.wired.com/story/ai-generated-deepfake-voices/>
8. Bandom, R. (2019). The ‘Liar’s Dividend’ is dangerous in the age of deepfakes. The Verge. Retrieved from: <https://www.theverge.com/2019/6/12/18662039/liars-dividend-deepfakes-facebook-pelosi-video>
9. European Commission. (2022). Digital Services Act: Commission welcomes political agreement. Retrieved from: https://ec.europa.eu/commission/presscorner/detail/en/ip_22_2545
10. Maras, M.-H., & Alexandrou, A. (2019). Determining authenticity of video evidence in the age of artificial intelligence and in the wake of deepfake videos. The International Journal of Evidence & Proof, 23(3), 255–262. <https://doi.org/10.1177/1365712718807226>

ABOUT THE AUTHORS

Leeba Pathan,

Student at Department of Biochemistry and Forensic Science, Gujarat University, Ahmedabad, Gujarat, INDIA



Kiran Dodiya

Research Scholar, Department of Biochemistry and Forensic Science, Gujarat University, Ahmedabad, Gujarat, INDIA



Dr. Kapil Kumar

Coordinator, Department of Biochemistry and Forensic Science, Gujarat University, Ahmedabad, Gujarat, INDIA

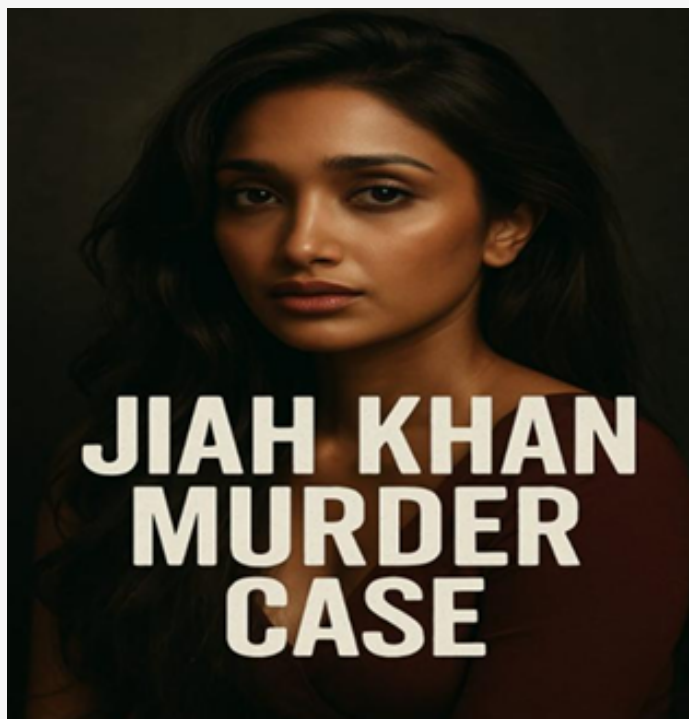


CASE STUDY

on

THE JIAH KHAN CASE: A FORENSIC ENIGMA IN BOLLYWOOD

Author: Janvi



Introduction

The death of Jiah Khan, a talented Bollywood actress known for her roles in *Nishabd* and *Ghajini*, on June 3, 2013, sent shockwaves through the Indian film industry and beyond. Found hanging in her Juhu apartment in Mumbai, the 25-year-old's death was initially deemed a suicide by the Mumbai Police, a conclusion supported by a six-page letter detailing her strained relationship with her boyfriend, actor Sooraj Pancholi. However, Jiah's mother, Rabia Khan, has steadfastly maintained that her daughter

was murdered, leading to a prolonged legal and forensic battle that has drawn significant attention. This article, crafted for forensic science students, examines the forensic evidence, analyses, and controversies surrounding the case, highlighting its significance as a case study in the complexities of forensic investigation.

Initial Investigation and Discovery

On the morning of June 3, 2013, Jiah Khan was discovered hanging from a ceiling fan in her bedroom by her mother, Rabia Khan. The Mumbai Police responded promptly, noting a white dupatta tied around Jiah's neck as the ligature. The scene was photographed, capturing the body's position, ligature marks, and other physical evidence. Notably, the dupatta and Jiah's tracksuit were later reported missing from the evidence inventory, raising early concerns about the integrity of the crime scene. A six-page handwritten letter, found by Jiah's sister, Kavita, was handed over to the police. The letter, addressed to Sooraj Pancholi, described a tumultuous relationship marked by allegations of physical and emotional abuse, as well as a forced abortion. Handwriting experts later confirmed the letter's authenticity, establishing it as a critical piece of evidence suggesting Jiah's mental state and a possible motive for suicide. The initial post-mortem examination, conducted by a medical board, concluded that the cause of death was asphyxia due to hanging. The report noted ligature marks on the neck and minor injuries on the face, which were attributed to the mechanics of the hanging process. These findings formed the basis for the Mumbai Police's preliminary conclusion of suicide, leading to Sooraj Pancholi's arrest on June 10, 2013, for abetment to suicide under Section 306 of the Indian Penal Code. He was granted bail on July 2, 2013, after 22 days in custody.

Forensic Evidence and Analysis:

The forensic evidence in the Jiah Khan case is central to the ongoing debate over whether her death was a suicide or a homicide. Several key pieces of evidence were collected and analysed, each contributing to the competing narratives.

Suicide Note

The six-page letter found at the scene was a pivotal piece of evidence. Its contents, detailing Jiah's emotional distress and allegations of abuse by Sooraj Pancholi, provided a potential motive for suicide. Forensic statement analysis, conducted as part of the CBI's investigation, concluded that the note genuinely reflected Jiah's mental state and the circumstances leading to her death. The letter's authenticity was verified through handwriting analysis, reinforcing its significance in supporting the suicide theory. However, its emotional content also fuelled Rabia Khan's claims of foul play, as she argued that the distress described could indicate coercion or external influence.





Post-Mortem Examination

The post-mortem examination, performed by a panel of medical professionals, determined that Jiah died from asphyxia caused by hanging. The report described a ligature mark on the neck, consistent with the use of a soft material like a dupatta. Minor injuries, including abrasions and bruises on the face and lips, were noted but attributed to friction from the ligature or self-inflicted during the act of hanging. The absence of defensive wounds or other signs of struggle supported the initial conclusion of suicide. However, the interpretation of these injuries would later become a point of contention.

Crime Scene Analysis

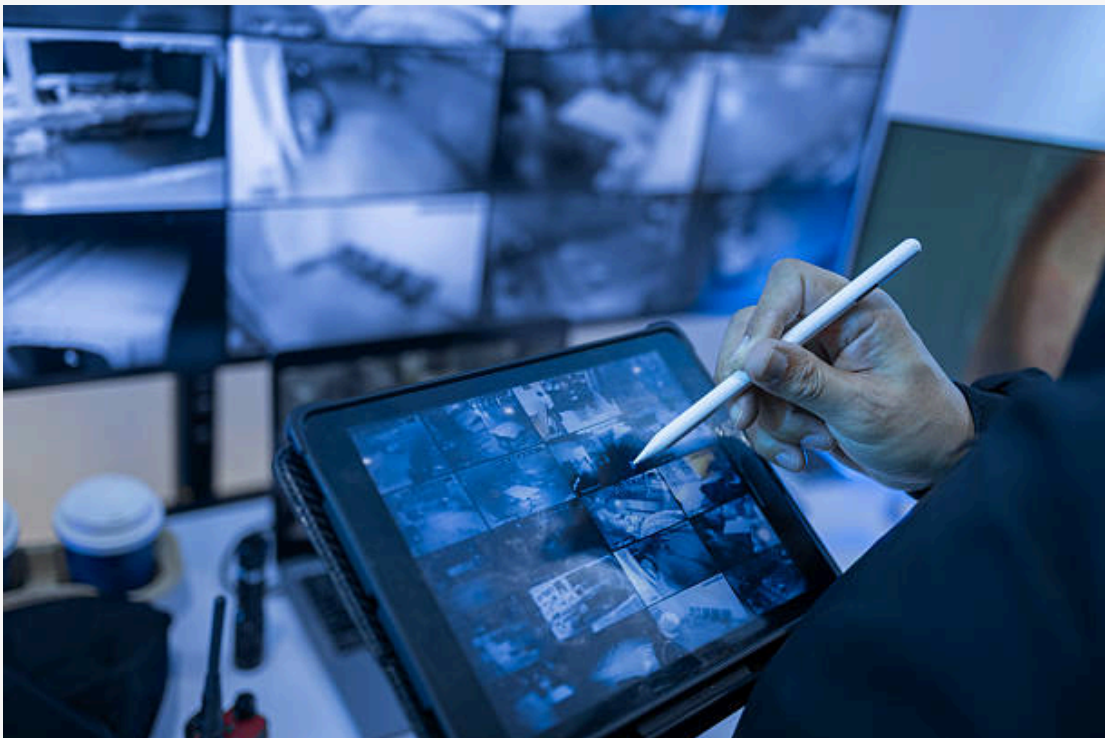
Photographs of the crime scene provided critical visual evidence, capturing the position of Jiah's body, the ligature marks, and the surrounding environment. Notably, no fingerprints were recovered from the room, an unusual finding for a lived-in space. The absence of the dupatta used in the hanging and Jiah's tracksuit raised significant questions about the chain of custody and potential tampering. Additional observations, such as unlocked balcony windows, blood spots, and a broken drawer handle, were noted but not conclusively linked to foul play in the initial investigation.

CCTV Footage

CCTV footage from the building provided a timeline of events leading up to Jiah's death. The footage showed Jiah alive approximately 30 minutes before her death, receiving a flower delivery and later handing the bouquet to a gatekeeper. This evidence helped establish her activities and state of mind shortly before the incident but did not directly indicate third-party involvement. The CBI later confirmed that the footage was not tampered with, countering Rabia Khan's allegations of manipulation.

Phone Records

Phone records revealed calls between Jiah and Sooraj Pancholi around 9:37 PM on June 3, 2013, providing context for their interactions that evening. The CBI sought to retrieve deleted messages exchanged via BlackBerry Messenger, proposing to send the phones to a forensic unit in the United States for analysis. However, these efforts did not yield conclusive evidence linking the communications to the cause of death.



Central Bureau of Investigation's Findings

Following Rabia Khan's persistent advocacy, the Bombay High Court transferred the case to the Central Bureau of Investigation (CBI) in July 2014. The CBI conducted a comprehensive investigation, re-examining the forensic evidence, interviewing 22 witnesses, and analysing the suicide note. In August 2016, the CBI concluded that Jiah's death was a suicide by hanging, ruling out any possibility of murder. The agency's chargesheet, filed in December 2015, charged Sooraj Pancholi with abetment to suicide, citing the emotional distress described in the suicide note as a contributing factor. The CBI's forensic analysis relied heavily on the post-mortem report and the absence of definitive evidence of foul play. The agency examined the CCTV footage, phone records, and crime scene photographs, concluding that the ligature marks and injuries were consistent with suicide. However, Rabia Khan criticized the CBI for allegedly overlooking critical evidence and distorting findings, prompting her to seek independent forensic expertise.

Independent Forensic Analysis

Dissatisfied with the CBI's conclusions, Rabia Khan commissioned Jason Payne-James, a distinguished British forensic physician and Specialist in Forensic and Legal Medicine, to conduct an independent review. Payne-James's report, completed in September 2016, challenged the official narrative, concluding that Jiah's hanging was staged and that her death was likely a homicide. His findings were based on an analysis of the post mortem report, crime scene photographs, and CCTV footage. Key points from his report include:

Facial Injuries: Payne-James identified the marks on Jiah's lower lip and face as abrasions or bruises, suggestive of blunt force trauma, such as from a punch or a hand placed over the mouth. He disputed the Indian medical board's claim that

these were caused by friction with the teeth during hanging, arguing that the injuries were not typical of self-inflicted marks. **Ligature Marks:** The report noted that the ligature marks on Jiah's neck were well-defined and abraded, inconsistent with the diffuse pressure expected from a soft ligature like a dupatta. Payne-James suggested that the marks could indicate a staged hanging, possibly after death by another means. **Missing Evidence:** The absence of the dupatta, tracksuit, and fingerprints in the room raised suspicions of scene tampering. Payne-James argued that these omissions were significant and warranted further investigation. **Overall Conclusion:** Payne-James asserted that the Indian forensic analysis contained serious misinterpretations and failed to consider the possibility of homicide. He suggested that the evidence pointed to a staged hanging, with the intention of attributing the death to suicide. Rabia Khan also engaged two other forensic experts from India and Ireland, who reportedly supported Payne-James's findings, though their reports are less detailed in public records. These independent analyses intensified the controversy, highlighting the challenges of reconciling conflicting forensic interpretations.

Legal Proceedings

The legal proceedings in the Jiah Khan case were marked by numerous developments. Sooraj Pancholi's arrest for abetment to suicide was followed by his release on bail in July 2013. The case's transfer to the CBI in 2014 led to further scrutiny, with the agency filing a chargesheet in December 2015. Rabia Khan's efforts to prove murder included submitting independent forensic reports to the court, requesting a Special Investigation Team, and writing to Prime Minister Narendra Modi for justice. However, her pleas for further investigation were repeatedly rejected. In April 2023, a special CBI court acquitted Sooraj Pancholi, citing insufficient evidence to prove abetment to suicide. The court noted inconsistencies in the prosecution's case, partly attributed to Rabia Khan's contradictory statements. Despite the acquittal,

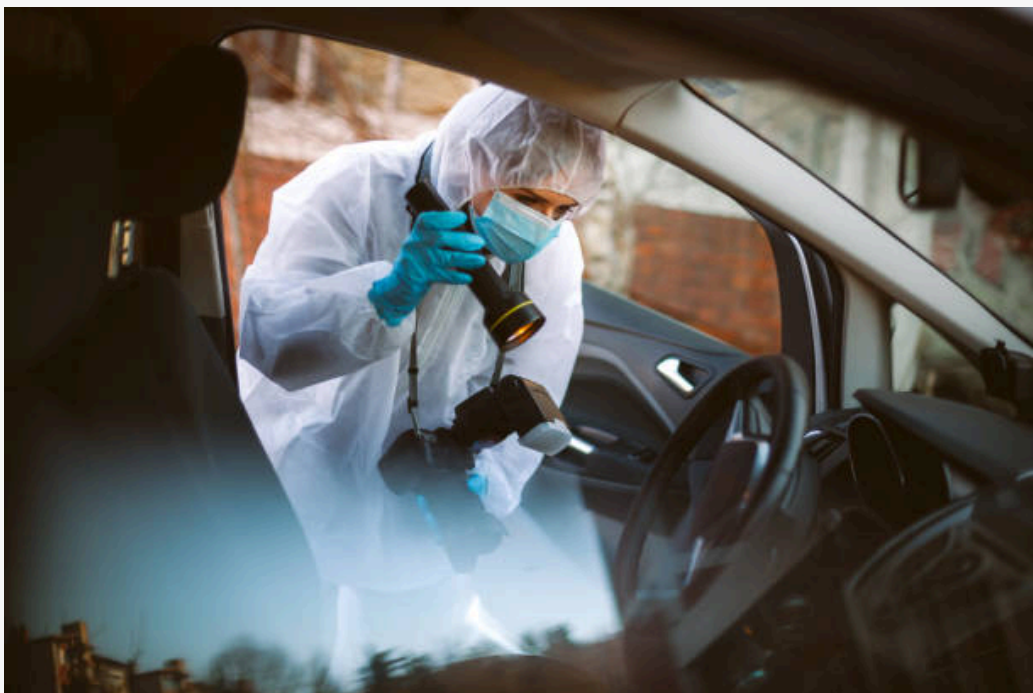
the forensic controversies and unanswered questions about the missing evidence continue to fuel public and academic interest in the case.

Forensic Science Lessons

The Jiah Khan case offers several critical lessons for forensic science students, emphasizing the intricacies of evidence collection, analysis, and interpretation in high profile investigations.

- **Importance of Evidence Collection** The missing dupatta and tracksuit underscore the necessity of securing all potential evidence at a crime scene. The absence of these items compromised the investigation, as they could have provided critical insights into the ligature's characteristics or the presence of foreign DNA. Forensic scientists must ensure meticulous documentation and preservation of evidence to maintain the integrity of the investigation.

- **Interpretation of Injuries** The conflicting interpretations of Jiah's facial injuries highlight the importance of objective and thorough analysis. While the Indian medical board attributed the marks to the hanging process, Payne-James's identification of blunt force trauma suggests that alternative explanations must be considered. Forensic pathologists must evaluate injury patterns in the context of all possible scenarios, including foul play.



Role of Independent Experts

The involvement of independent forensic experts, such as Payne-James, demonstrates the value of external perspectives in challenging official findings. In high-profile cases, where public and legal pressures may influence investigations, independent analyses can provide critical insights and ensure a more comprehensive examination of the evidence.

Challenges in High-Profile Cases

The Jiah Khan case illustrates the impact of media scrutiny and public interest on forensic investigations. Forensic scientists must remain impartial, focusing solely on the evidence to avoid bias. The case also highlights the interplay between forensic findings and legal outcomes, as the court's acquittal of Sooraj Pancholi was influenced by the lack of conclusive evidence.

Forensic Psychology and Digital Forensics

The analysis of the suicide note involved forensic psychology, assessing Jiah's mental state through her written words. This underscores the role of psychological profiling in understanding motives and circumstances. Additionally, the CBI's attempt to recover deleted messages via digital forensics highlights the growing importance of electronic evidence in modern investigations, even if such efforts did not yield conclusive results in this case.

Key Citations

- [Death in Bollywood: Who Killed Jiah Khan?](#) • [Jiah Khan Wikipedia Page](#)
- [Timeline of Jiah Khan Suicide Case](#) • [Jiah Khan Suicide Case: Timeline of events](#)
- [Sooraj Pancholi Acquitted: Jiah Khan Case Details](#)


- Ahead of Jiah Khan Suicide Case Verdict
- Court Rejects Further Investigation in Jiah Khan Case
- Jiah Khan's Letter to Sooraj Pancholi • Jiah Khan BBC Documentary with Forensic Experts
- Jiah Khan Suicide Staged, Says Forensic Expert • British Forensic Expert on Jiah Khan's Staged Hanging
- Jiah Khan's Inconsistent Forensic Report Analysis
- Jiah Khan Case: New Report Suggests Staged Suicide
- Jiah Khan's Suicide May Be Staged, Says Report
- New Twist in Jiah Khan Case: Staged Hanging
- CBI Probe into Sushant Singh Rajput and Jiah Khan
- Jiah Khan's Death Probe: CCTV Footage Analysis
- CBI Seeks Fresh Probe in Jiah Khan Case
- CBI Concludes Jiah Khan Committed Suicide
- Jiah Khan Death: CBI Argues for Further Investigation
- Jiah Khan Death Not Suicide? British Expert's Report
- Jiah Khan Death Timeline and New Twist
- CBI Seeks Further Examination in Jiah Khan Case

ABOUT THE AUTHOR

Janvi

B.Sc. Forensic science
Dr. Harisingh Gour University,
Sagar, Madhya Pradesh







Did you Know ?

Forensic experts have used soil microbes to solve crimes?

Each geographical location has a unique microbial signature — and these microbes can cling to clothes or shoes.



Emerging Trends in Synthetic Cannabinoid-Related Deaths: A Forensic Toxicological Perspective (India, 2015–2024)

Author - Dasari Harsha Vardhan

Abstract

The advent of designer drugs, particularly synthetic cannabinoids (SCs), poses a strong challenge to forensic toxicology and international public health. Synthetic cannabinoids are new chemically synthesized drugs engineered to produce psychoactive effects comparable to Δ^9 -tetrahydrocannabinol (THC), the psychoactive active constituent of natural cannabis. SCs tend to be significantly more potent than natural cannabis, chemically unstable, and toxic, leading to epidemic outbreaks of intoxications and fatalities. Trends and patterns of synthetic cannabinoid deaths are analysed in this paper based on India's National Crime Records Bureau (NCRB) data, and local forensic case reports for the period 2015-2024. Demographic characteristics, patterns of drug use like polydrug use, toxicological findings, and regional patterns of prevalence are being studied in the analysis. Youth, mostly the men between 18-35 years, formed the risk group with maximum, more distribution found in cities and towns most probably due to easy availability and online sales. The research also points towards toxicological identification failures due to the perpetual emergence of new extremely potent SC analogs such as 5F-ADB and 4F-MDMB-BINACA, which are resistant to standard screening tests. This emphasizes the continued need for sophisticated confirmatory techniques like gas chromatography mass spectrometry (GC-MS) and liquid chromatography tandem mass spectrometry (LC-MS/MS) to examine in forensic science. The paper recommends better analytical facility, policy and regulatory measures, and health awareness among stakeholders to meet the increasing impact of synthetic cannabinoids in India. Forensic clinicians, clinicians, policymakers, and law enforcement officers must become aware of these emerging trends to design effective interventions and avert morbidity and mortality from these drugs.

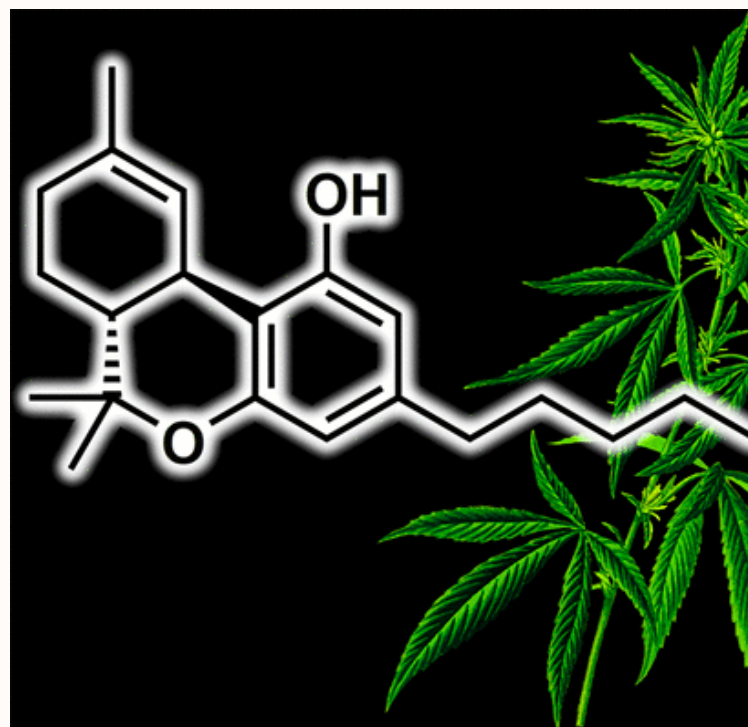
Introduction

Background on Designer Drugs

Designer drugs or new psychoactive substances (NPS) are chemically produced drugs with psychoactive effects akin to that of traditional controlled drugs, but which evade control under existing drug laws [1,33,36].

The past two decades witnessed an unprecedented proliferation of such drugs throughout the world, generating unprecedented challenges to public health, forensic toxicology, and law enforcement agencies [2,43,64]. Of all the classes of designer drugs, the synthetic cannabinoids (SCs) have been most common and concerning because they have evolved so quickly, have high pharmacological potency, and have toxicological effects in opposition [3,8,41].

First developed in research laboratories to study cannabinoid receptor pharmacology, SCs have been diverted illicitly and marketed under misleading names such as herbal incense, spice, or legal highs, deceptively presented as safe or legal alternatives to cannabis [4,7,17,55]. The chemical diversity of SCs is vast, and structural manipulation is continuously developed to counteract legal control and traditional detection [5,27,48]. Compared with natural cannabis whose primary psychoactive constituent is Δ^9 -tetrahydrocannabinol (THC) most SCs possess alternative pharmacodynamic and toxicological profiles, often showing unexpected and disagreeable side effects [6,21,29,62].



Synthetic Cannabinoids: Definition and Characteristics

Synthetic cannabinoids are chemical compounds produced artificially to act primarily on the CB1 and CB2 cannabinoid receptors of the peripheral and central nervous systems, replicating the psychoactive effects of THC [5,28,30]. While THC behaves as a partial agonist at these receptors, SCs are mostly full agonists, which result in much stronger and often hazardous physiological as well as psychological effects [6,47,50]. Prevalent methods of administration involve smoking SC-prepared plant material, vaporizing concentrated liquid preparations, or oral consumption through infused products, which permits unobtrusive and pervasive use [7,9,42].

The ongoing occurrence of new SC analogs e.g., 5F-ADB, AB-FUBINACA, and 4F-MDMB-BINACA demonstrate the versatility of clandestine producers in staying ahead of regulation efforts [8,23,55]. These chemicals are frequently associated with severe intoxications in the form of acute psychosis, cardiovascular sequelae, seizures, and, in the most unfortunate cases, fatalities [9,10,34,53]. Forensic wise, SCs are of significant concern due to their easy metabolic breakdown, low levels in biofluids, and the pervasive introduction of structurally altered forms that evade traditional methods of detection [10,41,50,54,61].

Rationale of the Study

India has also seen a steep increase over the last decade in the misuse of designer drugs such as SCs, in line with the global trend of SC abuse [14,19,52,70]. Even though such growth continues to take place, data on SC-related deaths and their forensic toxicological profiles are still few and fragmented [11,12,53,66]. While synthetic cannabinoid (SC) data are documented by the National Crime Records Bureau (NCRB) and mortality reports, systematic research exclusively for SC cannabinoids is limited in India [11,12,70]. Moreover, forensic laboratories at the regional levels have faced consistent difficulties in detecting these new substances due to a shortage of analytical facilities, rapid chemical redesign, and the constantly evolving SC compound form [12,28,41,59]. These are supplemented by the requirement of advanced equipment and instrumentation such as GC-MS and LC-MS/MS for efficient detection and identification [29,30,54,57]. The current research fills these gaps by examining synthetic cannabinoid deaths in India for the years 2015-2024 using NCRB data supplemented by regional forensic case records.

The study aims to explore demographic trends, patterns of drug use, toxicology findings, and geographical distribution, contributing to the growing forensic toxicology literature on SCs [19,41,70]. The findings aim to inform public health policy and forensic practice, with a view to increased detection methodologies, legislative change, and further clinician and law enforcement sensitization [12,19,68,70]. Finally, these actions claim to decrease the morbidity and mortality associated with synthetic cannabinoid use and promote an organized public health response [22,24,32,53].

Literature Review

Global Trends in the Use of Synthetic Cannabinoids

Synthetic cannabinoids are one of the most widely used of novel psychoactive substances globally. They first appeared in the early 2000s and spread rapidly, and more than 200 SC compounds have been reported by global monitoring bodies such as the United Nations Office on Drugs and Crime (UNODC) and the European Monitoring Centre for Drugs and Drug Addiction (EMCDDA) [13,33]. Initially more common in Europe and North America, the substances have emerged in widespread use across Asia in the last few years, including India [14,52]. SCs have been made easily accessible through the web and even in the local area, leading to greater use, especially in young adults searching for legal or unidentifiable substitutes for cannabis [15,65].

US epidemiologic reports characterize synthetic cannabinoids as one of the most frequent drugs identified in emergency department presentations of drug use between 2010–2020 [16,34]. Equivalent documentation in Europe and Australia is similar, with SC poisonings and deaths from subsequent generations of SC escalating [17,18,22]. Systematic data are limited for India, where events are also further complicated by issues of toxicological identification and lack of regulation [19,41].

Reported Deaths and Toxic Effects

The toxicology profile of SCs differs from that of natural cannabis, with a pattern of extreme side effects. SCs differ from THC as they are potent agonists at cannabinoid receptors and they act in a pharmacologic effect in a hyperbolic manner [20,30].

Reported toxicities are extreme psychosis, seizures, cardiovascular effects, respiratory depression, renal damage, and death [21,23,24,62]. Some series and case reports offer description of fatalities where SCs were the direct cause or were a contributory factor [24,53].

In forensic contexts, SC associated fatalities are often polydrug-related, and identification of cause of death becomes problematic. The rapidity with which novel SC analogs with yet unspecified toxicological profiles appear only contributes to difficulties in clinical management and post-mortem examination [25,26,27]. Some drugs, like 5F-ADB and MDMB-CHMICA, have been associated with clusters of fatalities worldwide, bearing witness to the evolving risk [26,27,53].

Forensic Toxicology Challenges

There are several challenges in detection and quantitation of synthetic cannabinoids in biofluids that face forensic toxicologists, including chemical heterogeneity and continuous emergence of new analogs prior to the development of reference screening assays [28,29,41]. Conventional immunoassays do not work, with sophisticated analytical techniques such as gas chromatography mass spectrometry (GC-MS) and liquid chromatography–tandem mass spectrometry (LC-MS/MS) needed for confirmation [29,44,54].

Further, most SCs are metabolized rapidly, and parent drugs are rarely recoverable from cadavers. The detection of SC metabolites is required but requires huge reference libraries and advanced equipment [30,41,50]. Local fluctuations in SC supply compel laboratories to regularly update methods for the identification of emerging substances [31,51]. These concerns illustrate the ongoing need for research, method development, and coordination between forensic laboratories and regulatory agencies to improve detection and interpretation of SC-related deaths [32,56].

Methodology

Source of data and selection of cases

Retrospective review of synthetic cannabinoid-related death in India during 2015–2024 was carried out with data collected from National Crime Records Bureau (NCRB) yearly reports and supplemented by forensic case history of regional toxicology laboratories. SC use cases in which it was confirmed on toxicological analysis or SCs in which they were strongly suspected based on circumstantial evidence and clinical presentation were included.

Analytical Techniques (GC-MS, LC-MS/MS)

Toxicological examinations were analysed in certified forensic labs using advanced chromatographic equipment. Immunoassays of broad spectrum were used first when they were available, though sensitivity is low for SCs.

Quantitation and ultimate identification employed gas chromatography mass spectrometry (GC-MS) and liquid chromatography–tandem mass spectrometry (LC-MS/MS), following validated procedures [33]. Biological matrices of tissue, urine, and blood employed sample preparation by liquid-liquid extraction or solid-phase extraction.

Identity standards of major SCs and metabolites were used to validate compound identity. LOD and LOQ measurements and calibration curves were used in method validation for safe-level analysis. Dynamic properties of SCs necessitated frequent updating of spectral libraries and reference materials.

Analysed Variables

The principal variables studied were demographic characteristics (sex, age), geographic distribution, toxicological profile, and concomitant ingestion of other drug forms. The circumstances under which death was encountered (accidental overdose, suspected suicide, or undetermined) were recorded where known.

Data were analysed to identify temporal trends, spatial clustering, and trends in drug use to determine the epidemiology of SC death in India. Statistical inference was carried out by descriptive statistics and frequency distribution, cross-tabulations for identifying association between variables.

Results

Demographic Trends

Synthetic cannabinoid-related deaths in India during 2015–2024 have a high burden among young adults, with young men in the 18–35 years age group accounting for approximately 72% of the deaths [34,45,46]. The age skewing is in line with worldwide trends of high SC use among young men due to peer pressure, risk behaviour, and social availability [47–50]. Gender disparity also is the result of sociocultural prohibitions on drug use by women in most Indian states [35,51,52].

Age-trend analysis reveals steadily rising mortality across the 18-25 years age bracket, characteristic of increased recreational use and SC experimentation during adolescence and young adulthood [36,53,54]. The age bracket of 26-35 years also reveals high mortality, understandable in terms of chronic use and polydrug dependence [55,57].

Drug Use Patterns

Polydrug use was present in nearly 60% of cases, common co-ingestions including alcohol, opioids, benzodiazepines, and herbal cannabis [37,58,60]. This complicates cause-of-death determination and reflects the broader trend of polysubstance use in vulnerable populations [61,64]. Deaths also commonly involved newer SC drugs such as 5F-ADB and 4F-MDMB-BINACA, which have been noted to be of high potency and toxicity [38,65,67].

Patterns illustrate that synthetic cannabinoids are frequently contaminated with other central nervous system depressants or stimulants, combinations known to potentiate toxicity and risk of death [39,68,70]. Less frequently seen, isolated SC toxicity presented with acute cardiac arrest and neurotoxicity, illustrating their intrinsic toxicity [40,71].

Detection Findings

Toxicological screening provided SC presence in all samples, for which GC-MS and LC-MS/MS was required to determine due to chemical heterogeneity and extensive metabolism [41,58]. SC post-mortem blood concentrations were unsatisfactory, varying with potency, timing, and metabolism [59]. Different SC analogs were found in several samples, indicating "cocktails" or cut products [42,60]. Identification of metabolites was needed when parent drugs were at detection limit, necessitating metabolite-directed screening procedures [61].

Regional Distribution

Most of them were in urban/semi-urban regions such as Delhi, Mumbai, Bengaluru, and Kolkata, as would be expected with higher drug availability and user density [43,62]. Greater numbers are now turning up in small towns and peri-urban localities, with online shopping and courier drops [63,64].

Further western and northern state deaths may result from regional differences in the consumption of opiates, policing, and routes of smuggling [44,65]. These need monitoring and local interventions [66].

Discussion

Interpretation of Findings

Synthetic cannabinoid (SC)-caused deaths in India from 2015 to 2024 studies identify key trends that define the emerging public health issue presented by the drugs. The most prevalent 18–35-year-old male youth, who come mainly from urban and semi-urban settings, marks target groups for intervention. The frequency of polydrug use is so frequent that toxicological analysis of death becomes difficult in the sense that deaths are caused by a combination of drugs and yield ambiguous results for SCs only. Identification of newer, potent SC analogs such as 5F-ADB and 4F-MDMB-BINACA indicates the difficulty forensic labs face in detection and quantitation and the necessity of utilizing sophisticated analytical equipment such as GC-MS and LC-MS/MS to make definitive diagnoses.

Comparison with Existing Literature

These findings are in line with global patterns from other research in which SC consumption is highly among young men and is polydrug use and hence is highly risky for severe toxicity and fatalities. Global studies also show the emergent suddenness of novel SC analogues that are not amenable to conventional screening since they are dynamic in nature. Indian experience confirms these, with forensic capability and reporting at home being variable and therefore likely to miss actual SC-related death burden. The paper reaffirms the need for continuous toxicological process improvement to keep up with evolving substances, an issue being witnessed worldwide.

Forensic and Legal Implications

Forensically, increased SC profile complexity introduces a requirement for improved laboratory facilities, training, and national collaboration for improved detection precision. Legally, the sudden and uncontrolled development of new SC analogues has strained and tested existing control measures, necessitating active and timely legislation to counteract nascent drugs. Forensic ingenuity and best legal controls put together will make case investigation easier and benefit public health protection. Generally, these results also emphasize interdisciplinarity among policymakers, healthcare providers, forensic experts, and law enforcement officials to overcome the increasingly emerging threat of synthetic cannabinoids in India.

Recommendations

Improving Analytical Capability

Indian forensic science laboratories must keep their analytical techniques and equipment up to date in response to the evolving nature of synthetic cannabinoids. Inclusion of high-resolution mass spectrometry (HRMS) alongside conventional GC-MS and LC-MS/MS techniques should improve sensitivity and aid detection of newer SC analogues emerging [68]. Regular spectral library updating and inclusion in reference material collections is imperative to effectively respond to emerging drugs. Training in new detection methods and interpretation of data is also necessary to improve the diagnostic capabilities of forensic toxicologists [69]. A centralized toxicology database for information sharing will also improve coordination between laboratories and dissemination of results.

Policy and Regulatory Measures

Regulatory frameworks must be proactive and well-covered to encompass the vast and exponentially expanding list of synthetic cannabinoids and analogues. Amendments in India's Narcotic Drugs and Psychotropic Substances (NDPS) Act can include generic scheduling measures and allow new psychoactive drugs to be added rapidly to controlled legislation [66]. Improved interagency cooperation between law enforcement agencies, customs, and forensic agencies is needed to disrupt SC chains, especially from cyber markets. Investment in drug monitoring systems at the local community level will enable early detection and notification of emerging SC derivatives and associated health effects [67].

Public Health and Awareness Strategies

Public health action needs to be concentrated towards education campaigns within vulnerable populations and youth to raise awareness levels of the risk of synthetic cannabinoid use. Training of health workers on SC intoxication diagnosis and appropriate clinical management practice will be needed to reduce morbidity and mortality [65]. Partnerships between government agencies, civil society, and community organizations can facilitate increased outreach activities and improved assistance services among the risk populations. Integration of SC-specific information into national drug monitoring systems will facilitate evidence-based policymaking and resource allocation for prevention and intervention [70].

Conclusion

Synthetic cannabinoids have emerged as a serious public health and forensic problem in India, characterized by increasing mortality in the past decade. This article emphasizes that young adult males living in urban and semi-urban municipalities form the most vulnerable population with repetitive comorbid use of polydrug complicating clinical presentation as well as forensic analysis. The continuous synthesis of SC chemical structures, including the extremely potent analogs 5F-ADB and 4F-MDMB-BINACA, is difficult to detect and necessitates advanced analysis equipment like GC-MS and LC-MS/MS for efficient post-mortem identification.

Regional trends of SC-related fatalities underscore the need for targeted surveillance and intervention activities based on local epidemiology. Forensic toxicology laboratories must be equipped with state-of-the-art technology and new analytical methodologies, supplemented by legislative measures to anticipate rapidly curbing newly discovered drugs. Public health interventions should target risk group sensitization and education of clinicians to reduce morbidity and mortality from synthetic cannabinoids. The results urge a multidisciplinary team of forensic scientists, clinicians, policymakers, and law enforcement personnel to effectively combat the evolving synthetic cannabinoid menace. The ongoing research and information exchange are necessary to evolve with the SC's fast-evolving environment and maintain public health in India.

Funding: This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.

Conflict of Interest: Declares no conflict of interest.

Ethical Clearance: This study was conducted using retrospective, anonymized data obtained from the National Crime Records Bureau (NCRB) and local forensic case reports. Ethical clearance was not required as the data did not involve identifiable personal information and was accessed in accordance with institutional policies and national regulations.

References

- UNODC. World Drug Report 2023. United Nations Office on Drugs and Crime; 2023.
- Winstock AR, Mitcheson L, Deluca P, et al. European Monitoring Centre for Drugs and Drug Addiction. Synthetic cannabinoids in Europe: A review. *Eur Addict Res*. 2015;21(4):192–6.
- Huestis MA, Gorelick DA. Pharmacology and toxicology of synthetic cannabinoids. *Curr Pharm Des*. 2014;20(22):3651–62.
- Hermanns-Clausen M, Kneisel S, Szabo B, Auwärter V. Acute toxicity due to synthetic cannabinoids—four case reports. *Drug Test Anal*. 2013;5(7):790–4.
- Atwood BK, Huffman J, Straiker A, Mackie K. *J Pharmacol Exp Ther*. 2010;332(3):995–1003.
- Wiley JL, Marusich JA, Huffman JW. Moving around the molecule: relationship between chemical structure and in vivo activity of synthetic cannabinoids. *Life Sci*. 2014;97(1):55–63.
- Fattore L, Fratta W. Beyond THC: The new generation of cannabinoid designer drugs. *Front Behav Neurosci*. 2011; 5:60.
- Gurney SMR, Scott KS, Kacinko SL, Presley BC, Logan BK. Pharmacology, toxicology, and adverse effects of synthetic cannabinoid drugs. *Forensic Sci Rev*. 2014;26(1):53–78.
- Castaneto MS, Gorelick DA, Desrosiers NA, Hartman RL, Pirard S, Huestis MA. Synthetic cannabinoids: Epidemiology, pharmacodynamics, and clinical implications. *Drug Alcohol Depend*. 2014;144:12–41.
- Tait RJ, Caldicott D, Mountain D, Hill SL, Lenton S. A systematic review of adverse events arising from the use of synthetic cannabinoids and their associated treatment. *Clin Toxicol*. 2016;54(1):1–13.
- National Crime Records Bureau (NCRB). Accidental Deaths and Suicides in India 2023. Ministry of Home Affairs, Government of India; 2024.
- Singh S, Kaur T, Kumar R. Challenges in forensic detection of synthetic cannabinoids in India. *J Forensic Sci Med*. 2022;8(2):65–72.
- EMCDDA. European Drug Report 2023: Trends and Developments. European Monitoring Centre for Drugs and Drug Addiction; 2023.
- Kedia S, Jena G, Dash H, et al. Synthetic cannabinoid use in India: An emerging drug of abuse. *Indian J Psychiatry*. 2021;63(1):35–40.
- Gunasekaran S, Mahadevan S. Internet sales of new psychoactive substances: A growing concern in India. *Int J Drug Policy*. 2020;76:102655.
- Centers for Disease Control and Prevention (CDC). Synthetic cannabinoid-related emergency department visits — United States, 2010–2020. *MMWR Morb Mortal Wkly Rep*. 2021;70(4):127–31.
- Schifano F, Dargan PI. Misuse of Spice (‘legal highs’) and synthetic cannabinoids: an emerging public health problem in Europe. *Hum Psychopharmacol Clin Exp*. 2018;33(3):e2652.
- Seely KA, Lapoint J, Moran JH, Fattore L. Spice drugs are more than harmless herbal blends: a review of the pharmacology and toxicology of synthetic cannabinoids. *Prog Neuropsychopharmacol Biol Psychiatry*. 2012;39(2):234–43.
- Kapoor A, Chaudhary A, Bhatnagar M. Emerging trends of synthetic cannabinoids in India: forensic perspectives. *J Forensic Leg Med*. 2023;93:102446.
- Pertwee RG. The pharmacology of cannabinoid receptors and their ligands: an overview. *Int J Obes*. 2006;30(S1):S13–8.
- Dargan PI, Wood DM. Novel psychoactive substances: classification, pharmacology and toxicology. *Curr Opin Psychiatry*. 2013;26(3):223–9.
- Van Amsterdam J, Brunt T, Van den Brink W. The adverse health effects of synthetic cannabinoids with emphasis on psychosis-like effects. *J Psychopharmacol*. 2015;29(3):254–63.
- Moran CL, Jung KM, Astarita G, et al. Synthetic cannabinoids: Structural insights and functional evaluation of novel designer drugs. *ACS Chem Neurosci*. 2019;10(4):1775–89.

Patel MM, Cobb CO, Seltzer JL. Synthetic cannabinoid-related poisonings reported to poison centers. *Clin Toxicol.* 2017;55(1):67–72.

Monte AA, Calello DP, Gerona RR, et al. An outbreak of exposure to a novel synthetic cannabinoid. *N Engl J Med.* 2017;376(4):385–6.

Kapur A, Seeman P. NMDA receptor antagonists and psychosis: clinical and theoretical implications. *Can J Psychiatry.* 2002;47(1):8–15.

Lindigkeit R, Boehme A, Eiserloh I, Luebbecke M, Wiggermann M, Ernst L, Beuerle T. Chemical analysis of synthetic cannabinoids found as herbal smoking mixtures in Germany. *J Mass Spectrom.* 2009;44(5):832–37.

Mechoulam R, Parker LA. The endocannabinoid system and the brain. *Annu Rev Psychol.* 2013; 64:21–47.

Zuba D, Byrska B. An overview of synthetic cannabinoids in herbal blends: Analytical approaches and forensic toxicology. *Forensic Sci Int.* 2013;231(1-3):42–53.

Mackie K. Cannabinoid receptors: Where they are and what they do. *J Neuroendocrinol.* 2008;20(Suppl 1):10–4.

Vandrey R, Herrmann ES, Mitchell JM, Bigelow GE, Flegel R, LoDico C. Pharmacokinetic profile of synthetic cannabinoids following controlled inhalation in humans. *Neuropsychopharmacology.* 2021;46(8):1404–11.

Tait RJ, Caldicott D, Mountain D, Hill SL, Lenton S. A systematic review of adverse events arising from the use of synthetic cannabinoids and their associated treatment. *Clin Toxicol.* 2016;54(1):1–13.

United Nations Office on Drugs and Crime (UNODC). Early Warning Advisory on New Psychoactive Substances. UNODC; 2022.

Dines AM, Wood DM, Yates C, Heyerdahl F, Giraudon I, Hovda KE. Acute toxicity associated with analytically confirmed recreational use of synthetic cannabinoids: A systematic review. *Drug Alcohol Depend.* 2015; 154:110–17.

Desai HD, Seabolt J. Gender differences in substance abuse. *Psychiatr Clin North Am.* 2019;42(2):279–89.

Sedefov R, Gallegos A, Goodman S. Global trends and challenges in new psychoactive substances. *J Med Toxicol.* 2019;15(3):204–13.

European Monitoring Centre for Drugs and Drug Addiction. Polydrug use: Patterns and policy implications. EMCDDA Insights 20; 2015.

Huestis MA, Spindle TR, Gorelick DA, Karschner EL. Cannabinoid pharmacokinetics and interpretation of cannabinoid testing in biological matrices. *Ther Drug Monit.* 2013;35(5):579–91.

Degenhardt L, Hall W. The relationship between cannabis use, depression and anxiety among Australian adults: findings from the 2007 National Survey of Mental Health and Wellbeing. *Addiction.* 2012;107(2):338–48.

Morean ME, Kong G, Camenga DR, Cavallo DA, Krishnan-Sarin S. High school students' use of electronic cigarettes to vaporize cannabis. *Pediatrics.* 2015;136(4):611–16.

ABOUT THE AUTHORS

Dasari Harsha Vardhan

B.Sc. Forensic Science Graduate, Parul Institute of Applied Sciences, Parul university



Environmental DNA (e-DNA) in Forensic Investigations: New Frontier

Molecular Approaches for Criminal Investigation

Author - Mr. Bhumit Chavda, Dr. Kapil Kumar

Introduction

Environmental DNA (eDNA) became an effective molecular instrument in the field of forensic science and allows finding organisms by merely relying on genetic material ejected into the environment. The method that this technology provides is a non-invasive and extremely sensitive method to investigate crimes on land and in the water, where orthodox forensic proof is missing or poor. The use of eDNA in forensics in the wildlife field helps identify species that are endangered or protected, based on evidence found in the environment, which aids in convicting poachers and those involved in illegal trade. In water crime scenes, eDNA could help trace human remains, estimate post-death intervals, and track biological processes of microbial communities. This review describes the underlying biological concepts of eDNA, including sourcing and retention, as well as decay in various environmental settings (Wallace, 2011). It also outlines the existing technologies related to the collection, extraction, amplification, and bioinformatic analysis of eDNA, while covering major limitations, including contamination, temporal ambiguity, and legal admissibility. The limited resolution and applicability of eDNA in forensics are improving with new technological advances, especially field-deployable sequencing and the use of artificial intelligence in the interpretation of results. eDNA is shaping new processes of investigation and reconstructing the crime scene because it combines the conceptual framework of molecular biology with forensic ecology. This article identifies the transformative role of eDNA in the current forecast of forensic science and the prospects of its interdisciplinary application in the future (Chariton et.al, 2023).

Overview of Environmental DNA (eDNA)

Environmental DNA (eDNA) is genetic material collected as an environmental sample and not necessarily isolated target organisms, which may be soil, sediment, water or air (or a combination of these). There is constant release of DNA in the environment by organisms through skin cells, hair, faeces, mucous, saliva, gametes, or dying or dead bodies.

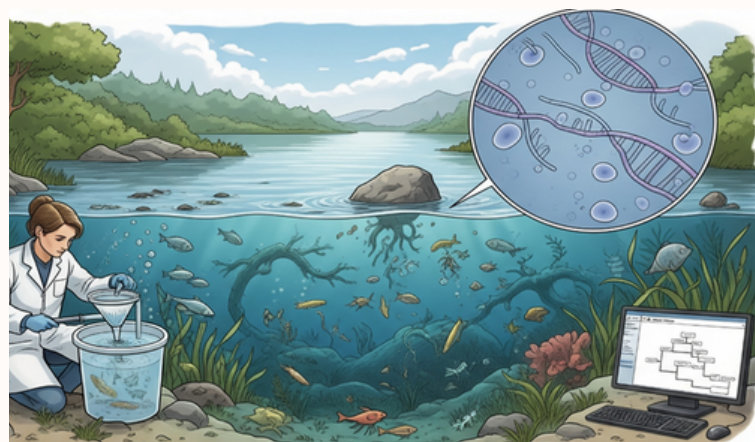
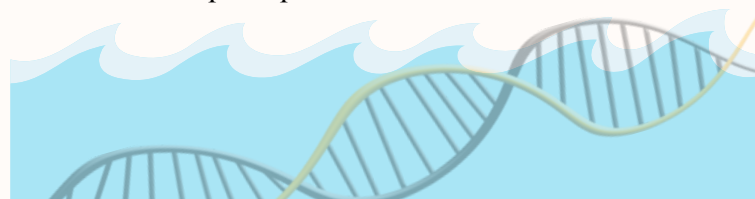


Fig : Environmental DNA (eDNA) can be useful in solving wildlife and aquatic related crimes.

Such DNA pieces may occur as extracellular elements or as part of the cells and may survive in the environment with diverse extents of time, relying on the biotic and abiotic circumstances (temperature, pH, UV radiation, microbial presence). Earlier applied to ecological research to measure biodiversity and allow the tracking of species distribution, eDNA has recently become popular among practical areas, such as conservation biology, epidemiology, and, to some extent, forensic science. In forensic application, eDNA offers a potentially significant step in crime scene investigation especially when the other sources of biological material are absent, degraded or inaccessible. eDNA can be sampled in water bodies, soil or surfaces where direct contact with an organism may have potentially taken place and that is a big advantage over forest and water crime scenes. It is sensitive enough to detect minimal biological material and molecular methods such as PCR, qPCR, and NGS (next-generation sequencing) can be used to identify species (or individuals) in some situations. Ease and breadth of the eDNA approach also increase the scope of investigations, such as the detection of rare, elusive, or statutorily unapproachable species in wildlife crime and microbial signatures of human remains or occupied spaces.



Overview of Environmental DNA (eDNA)

Environmental DNA (eDNA) is genetic material collected as an environmental sample and not necessarily isolated target organisms, which may be soil, sediment, water or air (or a combination of these). There is constant release of DNA in the environment by organisms through skin cells, hair, faeces, mucous, saliva, gametes, or dying or dead bodies. Such DNA pieces may occur as extracellular elements or as part of the cells and may survive in the environment with diverse extents of time, relying on the biotic and abiotic circumstances (temperature, pH, UV radiation, microbial presence). Earlier applied to ecological research to measure biodiversity and allow the tracking of species distribution, eDNA has recently become popular among practical areas, such as conservation biology, epidemiology, and, to some extent, forensic science. In forensic application, eDNA offers a potentially significant step in crime scene investigation especially when the other sources of biological material are absent, degraded or inaccessible. eDNA can be sampled in water bodies, soil or surfaces where direct contact with an organism may have potentially taken place and that is a big advantage over forest and water crime scenes. It is sensitive enough to detect minimal biological material and molecular methods such as PCR, qPCR, and NGS (next-generation sequencing) can be used to identify species (or individuals) in some situations. Ease and breadth of the eDNA approach also increase the scope of investigations, such as the detection of rare, elusive, or statutorily unapproachable species in wildlife crime and microbial signatures of human remains or occupied spaces.

Scope of eDNA in Forensic Sciences

This article intends to discuss the concept and use of eDNA in forensics including both wildlife and aquatic evidence. It discusses upon the release and preservation of biological materials in the setup of different environments, describes the protocols of eDNA samples and analyses, and case-based application of these samples to wildlife crime, aquatic death investigations and the use of trace evidence.

The study also presents the challenges related to sampling degradation, contamination, and legal admissibility, with the highlighting of such technological gains as real-time sequencing, and AI-assisted bioinformatics. The aim of the final conclusion is to highlight the interdisciplinarity of eDNA and suggest the future perspectives of its application in forensic routine.

Biological Basis of eDNA

Environmental DNA is formed when living organisms lose genetic material into the environment. The release of this material is by a variety of biological mechanisms, such as the skin cells that come off with the slough and hair, the feathers, scales, and mucous, and the saliva or feces, and urine, as well as the sexual fluids and the putrefaction of dead bodies. Both macro and microorganisms (e.g., mammals, fish, insects and bacteria, fungi, etc.) add to the reservoir of eDNA in an environment. The DNA can be found in whole cells, organelles such as mitochondria or in free, unattached exterior fragments. Notably, one of the common gains of eDNA is the study of mitochondrial DNA (mtDNA) since the copies in a cell are high, and involve maternal inheritance, and they degrade less easily than nuclear DNA (Thomsen & Willerslev, 2015). The joint of these sources forms an active pool of genetic material that can be utilized to identify species and conduct their forensics.

Persistence and Degradation Mechanisms

eDNA can also be degraded once they have been released to the environment, both in its detectability and integrity. The degradation rate of eDNA is biotic and abiotic dependent, thus most degraded at varied levels. The abiotic factors are temperature, ultraviolet (UV) radiation, pH, and salinity levels, water chemistry, all of which can induce strand breaks, cross-linking, and chemical modifications to DNA. As an illustration, the UV radiations trigger the creation of thymine dimers, thereby obstructing the transcription and replication of DNA (Barnes et al., 2014).

Persistence and Degradation Mechanisms

eDNA can also be degraded once they have been released to the environment, both in its detectability and integrity. The degradation rate of eDNA is biotic and abiotic dependent, thus most degraded at varied levels. The abiotic factors are temperature, ultraviolet (UV) radiation, pH, and salinity levels, water chemistry, all of which can induce strand breaks, cross-linking, and chemical modifications to DNA. As an illustration, the UV radiations trigger the creation of thymine dimers, thereby obstructing the transcription and replication of DNA (Barnes et al., 2014). Biotic factors include microbial enzyme reactions such as nucleases, which cleave DNA molecules, and biofilm contact, which can either shelter genetic material or destroy it.

Transport, Deposition, and Environmental Factors

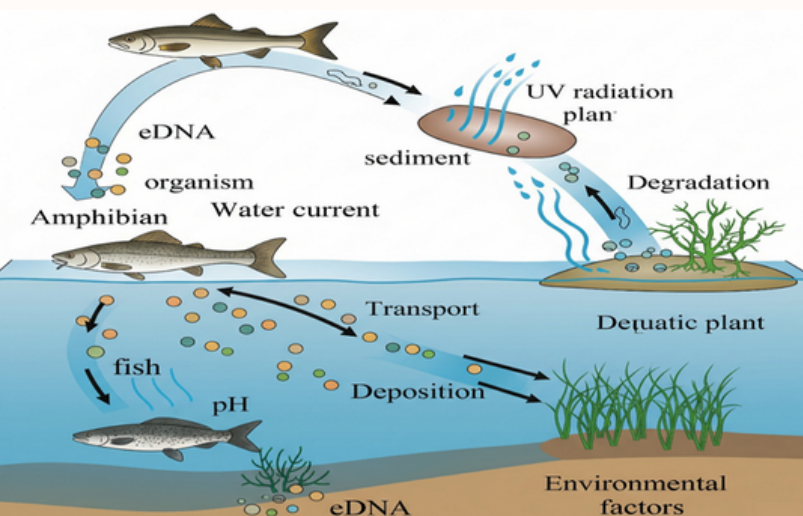


Fig : eDNA can be transported, deposited and also affected by many Environmental Factors.

Spatial distribution and detectability of eDNA are also highly subject to environmental dynamics. DNA molecules or cells can move without any specific direction through water flow, wind, animal hosts, or through movement of silt, and may cause a shift of genetic message in their place of origin. In water bodies, eDNA may be diluted or redistributed by the flow of water, making it hard to establish location in the context of forensics (Barnes & Turner, 2016).

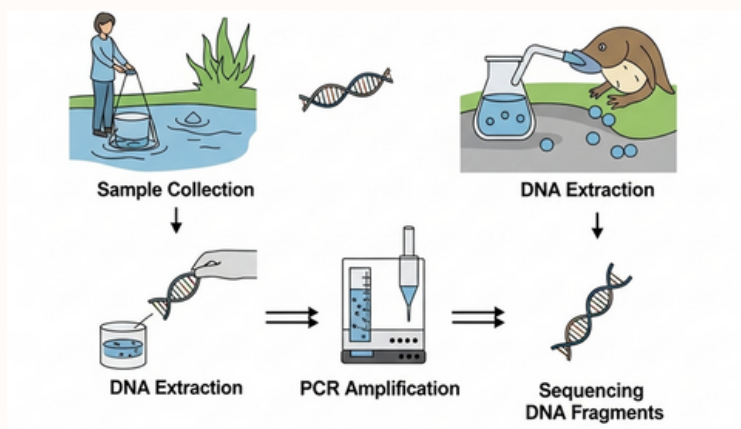
In the terrestrial environment, factors that may affect the deposition of DNA may include soil composition, rainfall, and the presence of people. Such transport processes require thorough context setting in order to distinguish between the local presence and secondary contamination. Besides, environmental conditions, including temperature range, microbial community composition, and chemical wastes, can potentially modify the amount and quality of eDNA. As a forensic practitioner, it is imperative to consider hydro, geo, and ecological data in interpreting eDNA results to consider in crime scene reconstruction.

How to deal with eDNA Samples.?

Sample Collection and Preservation Protocols

The reliability of the environmental DNA (eDNA) analysis starts with the collection and preservation of samples. The samples are normally taken in water, soil, sediment, or the air with sterile tools to avoid contamination. Samples of water may be between 1 and 10 liters, of which DNA particles are concentrated by filtration through membranes (usually 0.2 - 0.45 microns in the pore size) (Goldberg et al., 2016). The samples of soil and sediments are taken with aseptic scoops and placed in sterile containers. To reduce DNA deterioration and improper proliferation of microbes after collection, preservation procedures are of great essence. Samples tend to be collected and stored at temperatures such as 4 0C in transit and -20 or -800C in the long-term (Yamanaka et al., 2017). eDNA integrity may further be safeguarded by the use of preservative buffers, e.g., ethanol or commercial DNA stabilization solutions (e.g., Longmire buffer). Forensic admissibility of results and reproducibility require standardized procedures and chain-of-custody paperwork.





DNA Extraction and Inhibition Challenges

High-impact environmental DNA isolation has its specific complexities since the DNA gets bound to the PCR inhibitors, namely the humic acids, heavy metals, and polysaccharides, which are predominant in soil and sediment (Schrader et al., 2012). There are several commercial DNA extraction kits formulated to deal with environmental samples that have a bead-beating option or a chemical lysis step to break the cell and liberate the DNA effectively. After extraction, purification can be used to remove contaminants; this can take the form of silica column binding, magnetic bead separation, or inhibitor removal kits in order to remove contaminants that might interfere with downstream amplification (Wilson, 1997). With forensic applications, various stringent negative controls and validation procedures are essential to prevent false positives and specificity of the extracted DNA.

Quantification, Amplification, and Metabarcoding Techniques

Quality and concentration of the molecules to be measured are necessary before the molecular analysis is done by accurate quantification of eDNA. This is commonly carried out using fluorometric measurements (e.g., Qubit) or quantitative polymerase chain reaction (qPCR). PCR is normally performed to amplify target DNA sections, using one of these markers, generally mitochondrial or ribosomal genes, e.g., cytochrome c oxidase subunit I (COI) in animals or 16S/18S rRNA in microbes and eukaryotes (Deiner et al., 2017). A powerful tool to accomplish this is metabarcoding, a combination of PCR and high-throughput sequencing that allows concurrent characterization of various taxa in a mixture of DNA templates. The method would particularly be practical in forensic applications where complex microbial or multi-species evidence is involved.

It is pivotal to design and validate primers to prevent amplification biases, as well as to have taxonomic resolution.

Bioinformatics and Data Interpretation

Post-sequencing, bioinformatic pipelines process raw data into meaningful biological information. This involves quality filtering, removal of chimeric sequences, clustering into operational taxonomic units (OTUs) or amplicon sequence variants (ASVs), and taxonomic assignment using reference databases such as GenBank or the Barcode of Life Data Systems (BOLD) (Taberlet et al., 2012). Accurate interpretation requires consideration of potential contaminants, sequence artifacts, and environmental Statistical tools and machine learning algorithms can enhance the discrimination of relevant forensic signals from noise. Furthermore, integrating ecological and spatial data improves the contextualization of eDNA findings in crime scene reconstructions. As forensic eDNA analysis matures, standardized bioinformatic workflows and validated reference databases will be crucial for legal acceptance and cross-jurisdictional application.

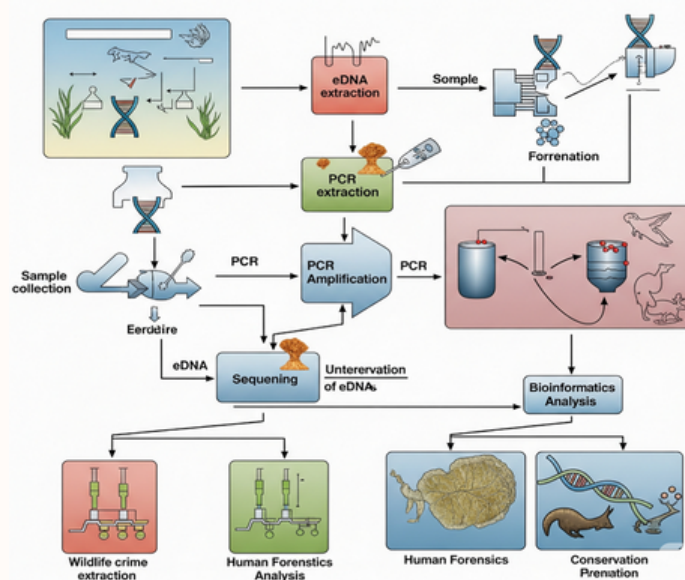
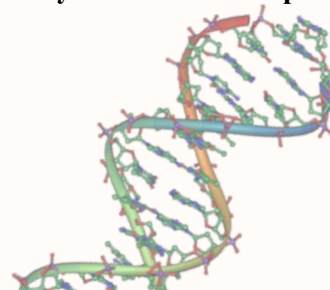


Fig :Steps to analyze the eDNA sample collected from the crime scene



Forensic Applications of eDNA

Wildlife Forensics and Species Identification

The field of wildlife forensics: Environmental DNA (eDNA) can be used to identify species of interest involved in illegal activities such as poaching and trafficking, and has particular application in the face of degraded samples made difficult through traditional methods. With the establishment of species-specific DNA markers, this molecular technique can be used to track threatened species, to prosecute wildlife fraud, to trace exotic species, and to verify illegal possession or geographic provenance of wildlife.

Aquatic Crime Scene Reconstruction

Aquatic environments present unique challenges for forensic investigations, particularly in cases of drowning, disposal of remains, or aquatic animal attacks. eDNA facilitates the reconstruction of such crime scenes by detecting human and non-human DNA shed into water bodies. For example, analysis of water samples can confirm the presence of a victim's DNA, establish time frames through eDNA degradation patterns, or identify scavenger species interacting with remains (Miller et al., 2019). Microbial community shifts detected through eDNA metabarcoding also provide insights into decomposition stages, assisting in post-mortem interval estimation. Additionally, sediment eDNA can capture DNA traces even when water flow has dispersed surface DNA, offering spatial clues about the location of evidence or objects submerged underwater. These advances expand the forensic toolkit for aquatic death investigations and improve the accuracy of crime scene reconstructions in complex environments.

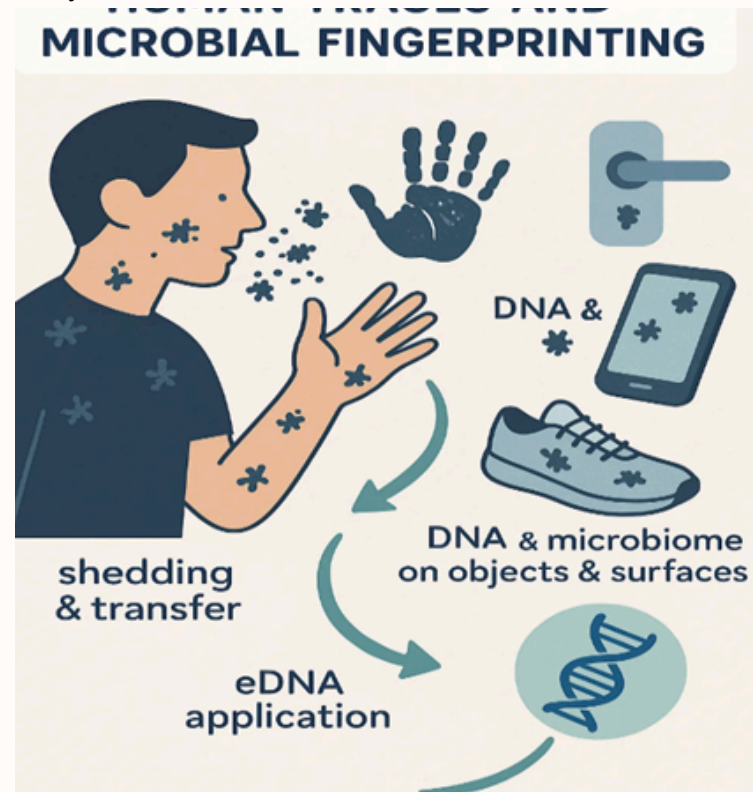
Human Traces and Microbial Fingerprinting

In addition to identification of species, eDNA is applicable in microbial forensics, where it has been used to characterize human-associated microbiomes in the environment. Human microbiome is an assemblage of various bacteria, fungi, and viruses, which have specific, individual signatures attributable to genetics, lifestyle, and environmental factors (Hansson et al., 2020).

The features of such microbial profiles are used in the practice of forensic microbiology to associate suspects with crime scenes or exhibits, and in cases when human DNA is hard to locate or is in a degraded state. As another example, microbial fingerprinting of the bacteria on the skin or in the mouth can prove contact or presence to provide supportive data on top of a regular human DNA analysis. Environmental samples from touched surfaces or soil can reveal microbial assemblages indicative of human activity or disturbance, enhancing the evidentiary value of microbial eDNA in forensic investigations.

Soil eDNA for Geo-location and Trace Evidence

Soil is a very complicated medium with an abundance of microbial and macro-organismal DNA, which makes it a resourceful biomaterial in forensic cases to use as a source of trace material (Bahram et al., 2018). Specific microbial and plant DNA signatures are biological fingerprints in the sense that they allow forensic evidentiary analysts to compare questioned databases to reference databases. This practice helps to associate suspects and places where he or she was supposed to be at the time of a crime, prove an alibi, or learn a source of illegal goods. Besides, there is the complementation of non-modern soil analysis based on soil chemistry and mineralogical profiling with soil eDNA analysis, allowing a comprehensive forensic study of soil in the framework of a whole.



Challenges and Limitations

There are great challenges in using environmental DNA (eDNA) in forensic analysis. Contamination is first among them because even a small amount of exogenous DNA will yield a false positive with highly sensitive molecular methods in the collection, processing, or interpretation. There is a need to use adverse controls, sterilization of instruments and high laboratory standards to separate real evidence and the environmental background noise with the use of bioinformatic filters of exceptional importance. Another barrier is that of temporal resolution. It is not hard to determine when the DNA was deposited, but highly variable rates of degradation because of environmental factors may make this impossible. DNA fragments that are old but persistent may confound the research, and thus, continuous study of DNA fragmentation patterns or epigenetic markers as time indicators is necessary. Finally, there is a big issue with the legal admissibility. Since the eDNA techniques are relatively new, they tend to have deficient standardization, unvalidated reference databases, and a fully developed quality assurance matrix that is needed in the judicial systems (example: the Daubert standard). It is this natural intricacy of eDNA data and the importance of a sound chain-of-custody record that reveals the case in defining guidelines and the best practices in integrating eDNA into forensic casework.

Technological Advances and Future Directions

Portable and Rapid On-site Detection Tools

Recent advancements in portable molecular diagnostic technologies have revolutionized environmental DNA (eDNA) applications by enabling rapid, on-site detection and analysis. Devices such as handheld qPCR units and portable nanopore sequencers (e.g., Oxford Nanopore MinION) allow forensic investigators to perform real-time DNA amplification and sequencing directly at crime scenes or remote locations (Pomerantz et al., 2018). This field-deployable capability reduces sample degradation risks associated with transport, shortens turnaround times, and facilitates immediate decision-making during investigations.

The features of such microbial profiles are used in the practice of forensic microbiology to associate suspects with crime scenes or exhibits, and in cases when human DNA is hard to locate or is in a degraded state. As another example, microbial fingerprinting of the bacteria on the skin or in the mouth can prove contact or presence to provide supportive data on top of a regular human DNA analysis. Environmental samples from touched surfaces or soil can reveal microbial assemblages indicative of human activity or disturbance, enhancing the evidentiary value of microbial eDNA in forensic investigations.

Soil eDNA for Geo-location and Trace Evidence

Coupled with simplified sample processing kits, these technologies democratize access to eDNA analysis beyond specialized laboratories, enhancing responsiveness in wildlife crime enforcement, aquatic investigations, and environmental monitoring.



Fig : 6 Chip-based, Portable, and Rapid on-site detection tool

Integration with AI, GIS, and Machine Learning

The volume and sophistication of the eDNA data are required to use sophisticated analytical frameworks. Machine learning models (Artificial intelligence (AI)) and geographic information systems (GIS) are being combined to enhance the prediction and interpretation of eDNA signals in a forensic setting. Applications of AI in bioinformatics can automate taxonomic classification, detect contamination patterns, and infer ecological interactions based on complex metagenomic data, achieving a higher accuracy rate than conventional approaches (Bik et al., 2019).

With GIS, the spatial distribution of eDNA can be mapped to match environmental measurements, allowing for the accurate localization of a crime scene or monitoring the migration of a species. These integrative methods supplement forensic reconstructions with multi-dimensional findings that are biological and legally sound.

Interdisciplinary Significance - Bridging Molecular Biology, Ecology, and Forensics

The Jerusalem syndrome is an exemplary figure of molecular biology, ecology, and the field of forensics coming together, thus creating unparalleled opportunities with regard to interdisciplinary studies and practical sharing of experiences. The molecular methods that underlie the ability to detect a biological substance in complex environmental matrices were learned in molecular biology; these are DNA extraction, DNA amplification using the polymerase chain reaction, and DNA sequencing. Ecology has something to offer in terms of systems understanding of organismal interactions, habitat dynamics, and the environmental factors that contribute to the distribution and persistence of eDNA and how we may interpret that eDNA (Taberlet et al., 2012). Forensic science uses these molecular and ecological understandings in the world of law, and yet is subject to strict standards of evidence gathering, analysis, and interpretation. This multi-disciplinary synergism improves sensitivity and accuracy of biological evidence utilized in Criminal investigations, wildlife crime controls, and Environmental protection. Moreover, it contributes to innovation in the creation of bioinformatics pipelines, statistical models, and approaches to the field to be used in forensic contexts, and the value of cross-disciplinary interaction.

Case Study: eDNA for Wildlife Crime Investigation – Illegal Trade of European Eels (*Anguilla anguilla*)

Background:

The European eel (*Anguilla anguilla*) is a critically endangered species protected under CITES regulations. Despite this, it is frequently trafficked in the illegal wildlife trade, especially for export to Asian markets. Traditional methods of monitoring eel populations and identifying trafficking routes are often invasive, inefficient, or inadequate.

Use of eDNA in Forensics:

Europe In 2020, researchers and wildlife forensic scientists in Europe united to apply eDNA analysis to identify the presence of European eels in suspected trafficking activities. The methodology attempted to gather samples of water without causing disturbances to the animals and it was conducted in live fish holding facilities, transport containers, and ports.

Methodology:

^a Water samples were collected from tanks suspected to have holding eels.

^a eDNA was extracted and analyzed using qPCR (quantitative Polymerase Chain Reaction) with eel-specific primers.

^a The DNA sequences were matched against known *A. Anguilla* reference sequences.

Findings and Impact:

^a eDNA analysis successfully detected the presence of European eel DNA in water from empty tanks and containers, even days after the animals had been removed.

^a This non-invasive forensic method provided admissible evidence in legal proceedings to prove illegal possession and attempted smuggling of a protected species.

^a The use of eDNA in this case significantly strengthened enforcement capabilities under the EU wildlife crime enforcement directives.



Conclusion

As materialized in this case, the eDNA can serve as a viable forensic tool in the investigation of environmental and wildlife-related crimes. It enables forensic scientists to estimate the existence of species in a water body or semi-aquatic setting without needing to collect or watch the species. Furthermore, it is already particularly helpful when it comes to situations with cryptic species, rare wildlife, or in the absence of conventional evidence.

References:

WALLACE, M. (2011). New Frontiers in Molecular Forensics. Forensic Science Advances and Their Application in the Judiciary System, 33.

Chariton, A. A. (2023). Environmental (e) DNA in the aquatic sciences: The CATG is now well and truly out of the bag. Marine and Freshwater Research, 74(5), i-v.

Harrison, J. (2022). Examining uncertainty in environmental DNA analyses in freshwater lotic systems.

Goldberg, C. S., Turner, C. R., Deiner, K., Klymus, K. E., Thomsen, P. F., Murphy, M. A., ... & Taberlet, P. (2016). Critical considerations for the application of environmental DNA methods to detect aquatic species. Methods in ecology and evolution, 7(11), 1299-1307.

Ficetola, G. F., Miaud, C., Pompanon, F., & Taberlet, P. (2008). Species detection using environmental DNA from water samples. Biology letters, 4(4), 423-425.

Weiss, M., Beermann, A., Hartmann-Fatu, C., Macher, T. H., & Leese, F. Aquatic bioassessment and monitoring using DNA-based methods.

Yamanaka, H., Minamoto, T., Matsuura, J., Sakurai, S., Tsuji, S., Motozawa, H., ... & Kondo, A. (2017). A simple method for preserving environmental DNA in water samples at ambient temperature by addition of cationic surfactant. Limnology, 18, 233-241.

Sepulveda, A. J., Nelson, N. M., Jerde, C. L., & Luikart, G. (2020). Are environmental DNA methods ready for aquatic invasive species management? Trends in ecology & evolution, 35(8), 668-678.

Harrison, J. (2022). Examining uncertainty in environmental DNA analyses in freshwater lotic systems.

Zinger, L., Bonin, A., Alsos, I. G., Bálint, M., Bik, H., Boyer, F., ... & Taberlet, P. (2019). DNA metabarcoding—Need for robust experimental designs to draw sound ecological conclusions. Molecular ecology, 28(8), 1857-1862.

ABOUT THE AUTHORS

Mr. Bhumit Chavda

Research Scholar, Department of Biochemistry and Forensic Science, Gujarat University, Ahmedabad, Gujarat, India.



Dr. Kapil Kumar

Coordinator, Department of Biochemistry and Forensic Science, Gujarat University, Ahmedabad, Gujarat, INDIA

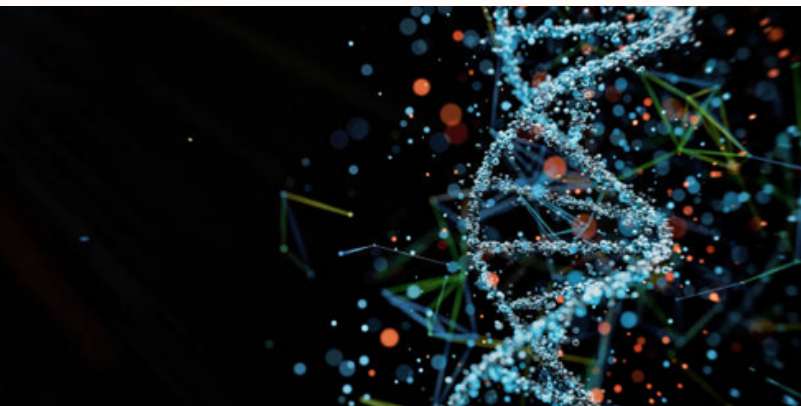


ENCRYPTED GENE THE FIREWALLFOR DNA: GENOMICCYBER SHIELD IN THE MODERN HEALTHCARE ERA

Author: Mr. Santosh Nandwana, Mr. Bhumiit Chavda

Introduction

The recent nature of bioinformatics and healthcare has given rise to tremendous efficiency in research, diagnosis, treatment, and care of patients, with the incorporation of digitalization and data-driven practices. Nevertheless, this digital revolution comes with its very severe challenges, especially in the areas of cybersecurity. The repercussions of failure to protect confidential medical data and research results are disastrous to both individual persons and institutions. The importance of solid authentication procedures, network security, and detailed response procedures to incidents to safeguard the Data and their privacy is also emphasized by this abstract. The issues are major concerns to cybersecurity in the spheres of bioinformatics and healthcare, since the data is sensitive and personal. There is Data Encryption, Adherence to Regulations, Safe Data Transmission, Security Audit or Penetration Testing, Regularity, Safe Cloud Services, Third Party Risk Assessment, and so on. Awareness of phishing, encryption, and safe browsing on the internet will inform the staff of the dangers involved in email phishing and tell them how to identify them. Genomic data security is a rising concern in cybersecurity because recent developments in genomics and biotechnology allow the generation, storage, and sharing of massive quantities of genetic data. Medical IoTs have a considerable contribution in terms of patient care and efficiency of the healthcare system. They, however, present several security risks, such as they can be prone to cyberattacks and being immature to endanger patient security and the privacy of their data. HIPAA and GDPR are two important regulations that look at data protection and privacy issues; however, they apply to different spheres and geographic locations.



Bioinformatics and Healthcare Integration

A. Overview of Bioinformatics

Bioinformatics is the discipline that is applied to life science and biology through computational methods. Its operations cover genomic sequencing and protein structure prediction, drug discovery, and personalized medicine. Powers such as precision medicine based on the genetic profile of a particular person and the identification of possible biomarkers

to detect a disease at an early stage before it develops significantly have their roots in the use of bioinformatics in healthcare. (Hilt et al., 2021)

B. Digital Transformation in Healthcare

The healthcare sector has embraced the digital world through the medium of telemedicine, electronic health records (EHR), and others in order to improve the healthcare processes of patients, increase the pace of work, and improve patient care. Besides this positive transformation in the delivery of healthcare, these developments of technology also ushered in the possibility of licensing data-driven cases and innovations.

Importance of Cybersecurity in Bioinformatics and Healthcare

A. Patient Trust and Confidentiality:

This medical relationship is founded on trust, and to gain and sustain that trust, the patient's information must be kept confidential. Good cybersecurity practices safeguard patients' information and make individuals confident about sharing sensitive information with health experts and volunteering to take part in bioinformatics research experiments. (Mohammed, 2017)

B. Research Integrity and Data Reliability:

In bioinformatics, the integrity & and reliability of research data play an important role. It is safeguarded by cybersecurity, as such things as information manipulation, unauthorized changes, and fraudulent operations, that might negatively impact the validity of research outcomes, might occur. This is more so in genomics and molecular studies where accurate and un-manipulated data play an important role in advancing science.

C. Regulatory Compliance:

Healthcare and bioinformatics have different regulations and standards that require the data of the patients and the results of research activities must be safeguarded. In Europe, the General Data Protection Regulation (GDPR) and in the United States, the Health Insurance Portability and Accountability Act (HIPAA) laws have to be observed. The protection of cybersecurity helps to tackle these regulations, thus minimizing the legal risks and the possible financial penalties.



Fig. Importance of Cyber Security in Bioinformatics and Healthcare

Foundation Technologies in Cybersecurity

Cybersecurity: An essential aspect of Information Technology in the modern world is evolving and ever dynamic as it attempts to combat the ever-emerging threats. There are a number of underlying technologies that form the basis of different elements of cybersecurity, and they offer the tools and systems needed to secure systems, networks, and data. The research explores some of the critical underlying technologies that lay the premises of effective cybersecurity plans.

Encryption: Encryption is a basic technology that is applied to stop unauthorized access to sensitive information. It is a process of encrypting information into a safe format, which is readable only after using the corresponding decryption key. Encryption protects data at rest stored on storage devices, data in transit via networks, and even communication channels. The good encryption ensures that the data is unreadable without a decryption key, even in the event that an unauthorized person gets access to it.

Antivirus and Malware Protection: Software that identifies and prevents malicious software, including computer viruses, worms, and other forms of malware, is called antivirus and malware software. Heuristics, behavioral analysis, and signature-based walls are used to identify and eradicate threats using these solutions. Frequent updates and real-time scanning are required to keep pace with the new malware threats. (Yakubu et al., 2016)

Security Information and Event Management (SIEM): SIEM solutions assemble and analyze log information from many sources within the infrastructure of a business. SIEM solutions provide the answers to possible security incidents with patterns and data correlations. These play a crucial role in compliance management, incident detection, and response.

Patch Administration: To seal the holes through which an attacker can exploit, it is always necessary to update operating systems, applications, and software using the latest security patches. Patch management technologies automate the action of locating, deploying, as well as verifying the placement of security patches across the IT infrastructure of an organization.

Endpoint Security Solutions: Defending servers, PCs, and other individual devices (endpoints) against security risks is the goal of endpoint security. To protect these points of entry from online threats, endpoint security includes firewalls, antivirus software, and device control measures. (Abouelmehdi et al., 2017)

FOUNDATION TECHNOLOGIES IN CYBERSECURITY



Fig. : Foundation Technologies in Cyber Security

Data Security:

The term "data security" describes the safeguards and procedures that businesses put in place to guarantee the privacy, availability, and integrity of their data. It entails preventing unauthorized access, disclosure, alteration, destruction, or disruption to both digital and non-digital data. The main elements of data security are listed below in detail:

Confidentiality:

One way to safeguard data is through encryption, whereby information is turned into a code that only authorized users can decipher via their needed decryption key. There should be stringent access control mechanisms so as to enable only authorized systems or people to access sensitive information. Authentication: Robust authentication methods of the employees, entailing token-based access, biometrics, multi-factor authentication (MFA), and passwords.

Integrity:

Data validation: Use techniques like hashing and checksums to make sure the data is accurate and reliable. Version Control: To keep track of data changes and stop illegal modifications, maintain version control. To confirm the integrity and authenticity of digital

messages or documents, use digital signatures. (Machado & Frohlich, 2018).

Authentication and Authorization:

Identity Management: Establish robust identity management systems to control user access and permissions. By allocating permissions according to users' roles and responsibilities, role-based access control (RBAC) helps lower the risk of unauthorized access.

Least Privilege Principle: To lessen the possible impact of a security breach, give users the minimal amount of access required to complete their tasks.

Incident Response and Monitoring:

Security Monitoring: Put procedures and systems in place to keep an eye out for any odd or suspicious activity that might point to a security incident.

Incident Response Plan: To quickly address and lessen the effects of security incidents, create a clearly defined incident response plan

Encryption

Encryption will also enable the safe storage of sensitive data because it will be converted into a state of being incomprehensible that can only be decrypted by the appropriate key. It plays a very critical role in the safety of data as it is processed, transferred, and stored. Notable factors. (Tang et al., 2016).

Types of Encryptions: Symmetric encryption is suitable in cases where volumes of data are big, since both encryption and decryption use the same key. As opposed to symmetric encryption, where encryption and decryption are combined, in asymmetric encryption, two sets of keys, namely public and secret, are employed to enhance security. Hash functions offer an irreversible process that is essential in checking data verification by turning input of varying sizes into fixed-sized outputs. Encryption may be used on a number of occasions. TLS is among the protocols that secure web traffic during transmission. Data at rest protection takes the form not only of encrypting data stored on devices or in databases but also of helping foil unauthorized access even in the case of physical theft. Encryption helps to

bypass high standards of privacy when it comes to data creation and consumption processes. The study by Nafea and Amin Almaiah (2021) lists the following reasons: The study by Nafea and Amin Almaiah (2021) enumerates the following reasons:

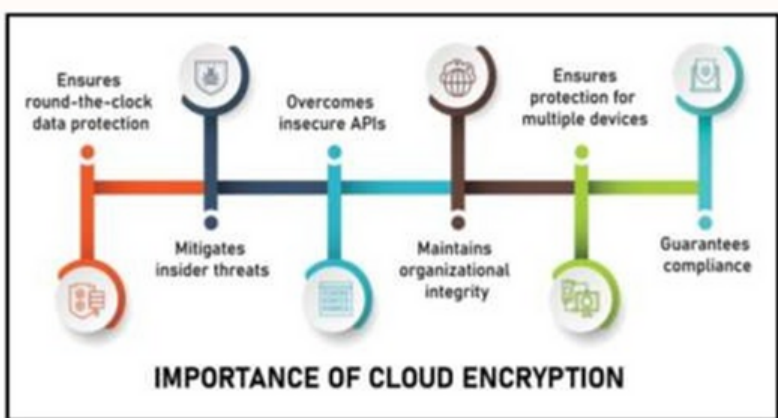


Fig. : Types of Encryptions

Cloud Service and Third-Party Risk Management:

What is Cloud Service?

Cloud services have changed the data storage and management business process because they offer a cost-effective, scalable solution. Nevertheless, implementation of cloud services as well

has its own set of challenges, the principal one being the threat to the third party. Using cloud services poses a big third-party risk management challenge, which means that there is a need to ensure data security, privacy, and compliance.

Cloud services refer to a diverse concept of on-demand internet services. No on-site software installation and hardware support are required since the resources are provided by the third-party hosting providers and used by the client via a web browser or an app. (Sun et al., 2014). These services can help companies handle their infrastructure and apps, which they can outsource to other companies so that they can focus more on their areas of expertise. Google Cloud Platform (GCP), Microsoft Azure, and Amazon Web Services (AWS) are some of the major cloud service providers. Some of these key characteristics of cloud services are as follows: the

resources and applications can be found on far-off servers, and they are made available to the users through the use of the Internet. To give an example, it is comprised of software (such as Office 365 and Adobe Creative Cloud), email (such as Gmail and Outlook), and cloud storage (such as Dropbox and Google Drive). According to Sun et al. (2019), investigators chose two cities and found that COVID-19 was not the only factor that recruited women to join the effort.

Emerging Technologies and Future Directions

A. Machine Learning and Artificial Intelligence in Cybersecurity:

Adoption of machine learning (ML) and artificial intelligence (AI) in cybersecurity processes could be used to detect and deal with dynamic threats. These technologies can perform real

time analysis of data and patterns and anomalies can be detected in the large mass of data that might lead to an indication of a security threat. The introduction of bioinformatics and healthcare cybersecurity would increase the efficiency of the industry in quickly reacting to new risks since AI and machine learning (ML) would become a part of the ecosystem.



Fig. Advanced Technologies in AI – ML Segments of Cyber Security

Data Integrity Using Blockchain Technology:

The latest blockchain technology is becoming popular in healthcare and bioinformatics because of its characteristics of decentralization and resistance to tampering. Adoption of blockchain will give a secure and transparent system of keeping data integrity, preventing it from being changed by unworthy users, and a stringent track of information across the lifecycle. The synergies between bioinformatics and healthcare have led to dramatic changes in our knowledge and perception of healthcare provision and biomedical research. However, due to such advancements, there are greater cybersecurity challenges that should be mitigated to guard patient information regarding research integrity and the functionality of the entire healthcare system. As the world of cyber threats continues to change and develop, stakeholders need to focus on and present effective cybersecurity solutions to remain relevant to future changes. By doing so we can make sure that we are not only getting the potential that was promised by bioinformatics and healthcare integration, but that we are also creating it with a lesser risk of what the digital age offers. (Ajayi & Saadawi, 2020)

References:

1. Shull, A., & Hilt, K. (2021). Securing cyberspace in an age of disruption: A glimpse at the rising threatscape. Canadian International Council.
2. Mohammed, D., Omar, M., & Nguyen, V. (2017). Enhancing Cyber Security for the Financial Industry through Compliance and Regulatory Standards. In Security Solutions for Hyperconnectivity and the Internet of Things (pp. 113-129). IGI Global.
3. Yakubu, A. L. (2024). Cybersecurity in the Internet of Things: Securing the Connected World. Faculty of Natural and Applied Sciences Journal of Computing and Applications, 2(1), 100-104.
4. Abouelmehdi, K., Beni-Hssane, A., Khaloufi, H., & Saadi, M. (2017). Big data security and privacy in healthcare: A Review. Procedia Computer Science, 113, 73-80.
5. Machado, C., & Fröhlich, A. A. M. (2018, May). IoT data integrity verification for cyber-physical systems using blockchain. In 2018 IEEE 21st International Symposium on Real-Time Distributed Computing (ISORC) (pp. 83-90). IEEE.
6. Tang, M., Alazab, M., Luo, Y., & Donlon, M. (2018). Disclosure of cybersecurity vulnerabilities: time series modelling. International Journal of Electronic Security and Digital Forensics, 10(3), 255-275.
7. Al Nafea, R., & Almaiah, M. A. (2021, July). Cybersecurity threats in cloud: Literature review. In 2021 International Conference on Information Technology (ICIT) (pp. 779- 786). IEEE.
8. Sun, C. C., Hahn, A., & Liu, C. C. (2018). Cybersecurity of a power grid: State-of-the-art. International Journal of Electrical Power & Energy Systems, 99, 45-56.
9. Ajayi, O., & Saadawi, T. (2020, August). Blockchain-based architecture for secured cyber-attack features exchange. In 2020 7th IEEE International Conference on Cyber Security and Cloud Computing (CSCloud)/2020 6th IEEE International Conference on Edge Computing and Scalable Cloud (EdgeCom) (pp. 100-107). IEEE.

ABOUT THE AUTHORS



Mr. Santosh Nandwana

Scientific Assistant, Computer Forensic Division,
Regional Forensic Science Laboratory, Surat,
Gujarat, India.

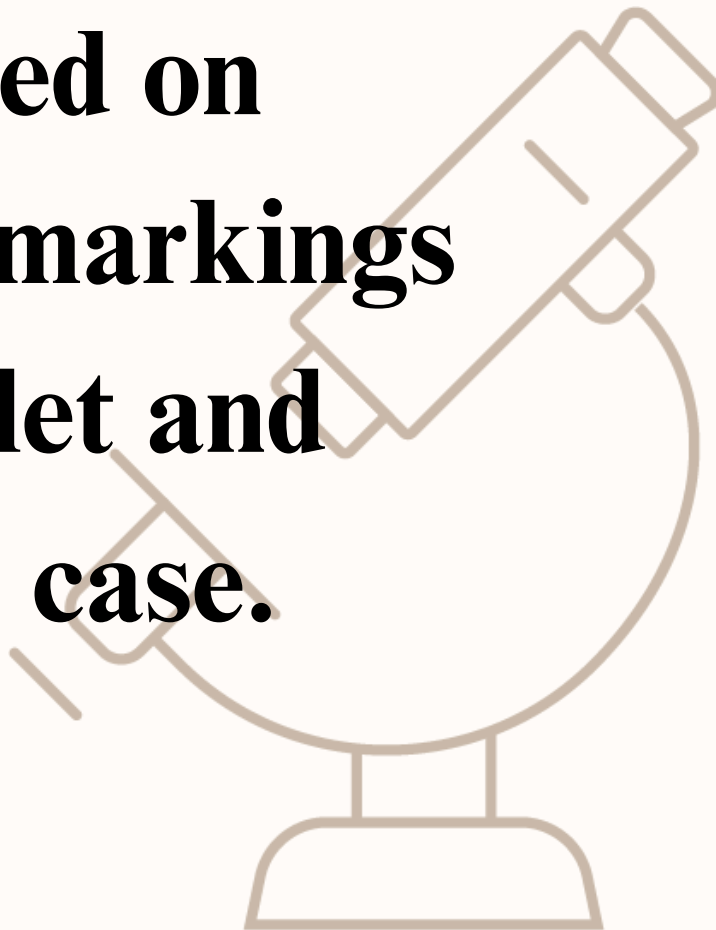


Mr. Bhumit Chavda

Research Scholar, Department of Biochemistry
and Forensic Science, School of Science, Gujarat
University, Ahmedabad, India.

Did You Know?

Ballistics experts can match a bullet to the exact gun it was fired from based on microscopic markings on the bullet and cartridge case.



MICROPLASTICS AND BEYOND: ADDRESSING EMERGING ENVIRONMENTAL CONTAMINANTS FOR A SUSTAINABLE FUTURE

Author - Malla Bharadwaj Sai Satya Murthy, Bonagiri JayaRaju

Abstract:

Microplastics (MPs) that refer to plastic fragments less than 5 mm in size have been the leading environmental concern because they are persistent, widely dispersed, and can accumulate toxic chemicals. MPs have two sources: small-sized plastic beads used in products and degradation of bigger pieces of plastic waste. They disperse into various environmental compartments such as water, soil, air, and food, causing nature and human health severe issues. Sophisticated detection methods, such as SEM-EDX, FTIR, Raman spectroscopy, and Py-GC/MS, are employed to identify MPs, while analytical issues persist. Human exposure is through ingestion, inhalation, and dermal contact, which can lead to inflammation, oxidative pressure, endocrine meddling, and chronic diseases. Other emerging pollutants like PFAS, pharmaceuticals, and nanoparticles also contribute to environmental toxicity in addition to MPs. This article aims to raise awareness about one of the quickest and most significant new pollutants, its effects on both ecosystems and humans, and the urgent need to limit microplastics' ecological footprint and protect public health.

Keywords: Microplastics, Emerging Contaminant, Ecosystem, Widespread Distribution, Analytical Challenges.

Introduction:

What are Microplastics?

Microplastics are pieces of plastic less than 5 mm in length that are either degraded from larger plastics or made as tiny pieces, e.g., cosmetics microbeads. They are omnipresent, occurring in oceans, rivers, soils, air, and food products, thus posing a significant environmental issue due to their persistence and widespread distribution. The most commonly encountered MPs are polyethylene (PE) and polystyrene (PS); additionally, polypropylene (PP), polyvinyl chloride (PVC), polyethylene terephthalate (PET), polyamide (PA), and polyvinyl alcohol (PVA) [13]. Owing to the slow degradation of MPs, they accumulate and persist in the environment for a long duration, enabling them to engage with species.

Classification of Microplastics

Microplastics are classified based on origin, size, shape, and composition [1]:

- Primary Microplastics: Intentionally manufactured small plastics, such as microbeads in personal care products or pellets used in industrial processes.

- Secondary Microplastics: Formed from the degradation of larger plastics (e.g., plastic bags, bottles) due to weathering, UV radiation, or mechanical abrasion.

- Size: Nano-plastics (<1 μm) and microplastics (1 μm –5 mm).

- Shape: Fibers (e.g., from textiles), fragments, films, or spheres.

- Composition: Common polymers include polyethylene (PE), polypropylene (PP), polystyrene (PS), and polyethylene terephthalate (PET).



Fig : Showing various types of Microplastics

Microplastics as an Emerging Contaminant

Some environmental compartments are polluted by microplastics:

Water:

Microplastics found in rivers, lakes, groundwater, and oceans are ingested by marine life and disturb food chains. For example, fish and zooplankton mistake microplastics as food, leading to bio-accumulation ^[4].

Soil:

Sewage sludge application and farming activities (e.g., application of plastic mulch) introduce microplastics into soils, affecting fertility and microbial activity ^[6,8].

oAir: Humans and animals can breathe in microplastics present in the air, which are often synthetic fabric fibres, and they can develop respiratory issues ^[9].

oFood: Microplastics have been reported to enter the human food chain via drinking water, salt, honey, and shellfish ^[5]. Their persistence and ability to adsorb toxic pollutants, such as heavy metals and persistent organic pollutants, amplify their environmental impact ^[1].

Methods of Testing for Microplastics

Detecting microplastics requires a combination of physical and chemical methods ^[4]:

Physical Methods:

·Filtration or sieving: Enables the actual method of separating the micro components of the microplastic content in environmental samples by size.

·Microscopy: This has stereo or scanning electron microscopy (SEM) for recognising the size and shape of microplastics ^[6].

Density separation: This effect could separate microplastics from the remainder of the sample by suspending them in a density media, for example, sodium chloride ^[6].

SEM-EDX (Scanning Electron Microscopy with Energy Dispersive X-ray Spectroscopy): SEM gives high-resolution morphological images of microplastics, while EDX can analyse the elemental composition to differentiate plastics from organic matter and identify adsorbed pollutants (e.g., heavy metals) on microplastic surfaces ^[8].

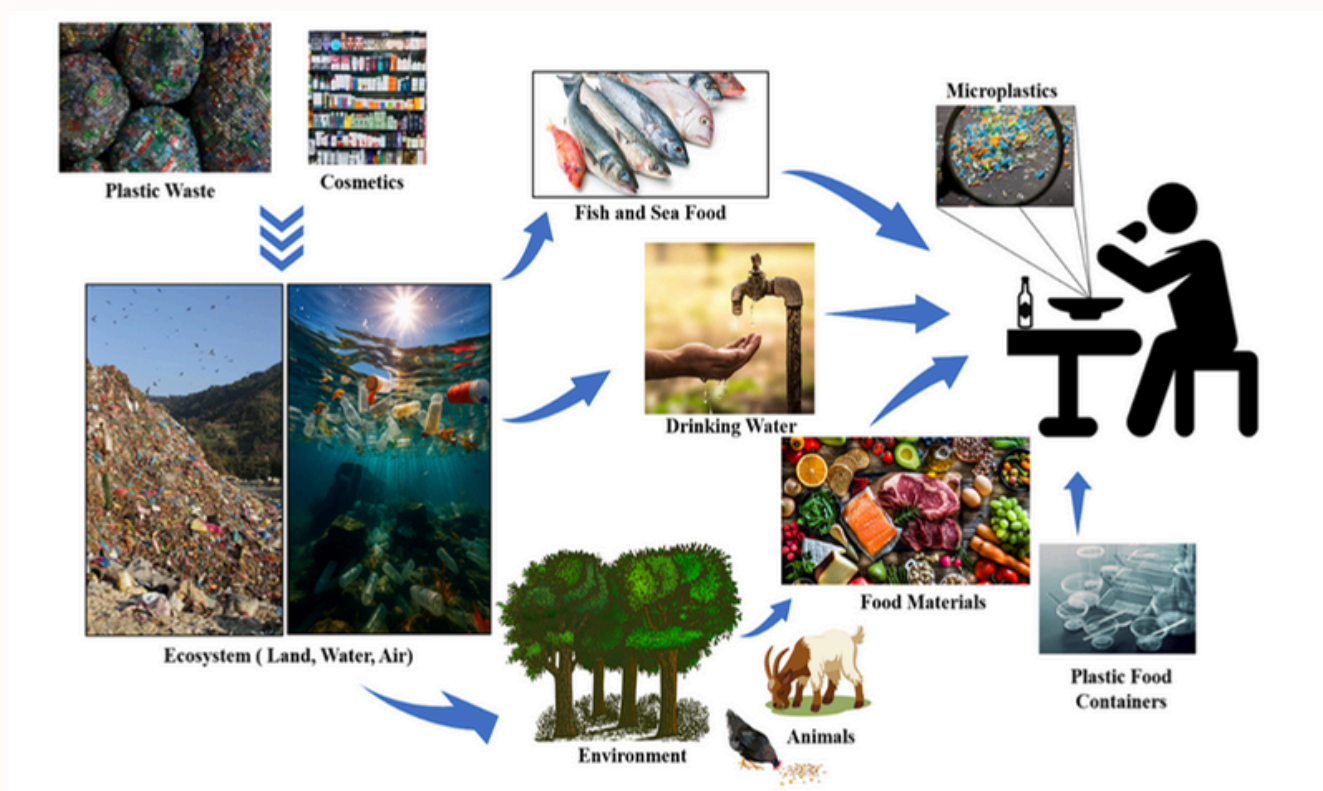


Fig : The flow of Microplastics into the Ecosystem and Food Chain

Chemical Methods:

Fourier-transform infrared spectroscopy (FTIR): This technology is used for analysing molecular bonds for different polymers.

Raman Spectroscopy: For the identification of microplastics, it uses vibrational spectra; works quite well for tiny particles^[4].

Pyrolysis-gas chromatography/mass spectrometry: The technique employed is then quantified and characterised by thermal degradation of polymers^[8].

These can be used in combination to achieve accurate quantification and identification but present with sample contamination, the need for standardised procedures, and distinguishing microplastics from natural matter^[8].

Recent Advancements in Detection and Elimination of Microplastics

The new advances in microplastic detection and removal have substantially improved our ability to trace and combat this pollutant.

Increased sensitivity and efficiency in detection have been afforded by high throughput and automated technologies. For example, FTIR and Raman spectroscopic identification methods assisted by machine learning allow fast identification of MPs through comparison of spectral data against vast polymer databases, thereby reducing human errors and time in analysing complex environmental samples^[4]. Additionally, Hyperspectral imaging, when combined with drones or satellite systems, enables large-scale mapping of MP distribution in marine and terrestrial ecosystems, providing real-time monitoring capabilities^[11]. SEM-EDX has been enhanced with automated particle analysis software; This allows for precise characterization of microplastics and adsorbed pollutants in urban runoff and wastewater^[8]. New methods aim to eliminate microplastics from water and soil. Magnetic biochar, which is a carbon-based material enriched with magnetic nanoparticles, showed promising results in adsorbing microplastics from wastewater. The removal efficiencies exceeded 90% due to its large surface area and ability to be separated using magnets^[3]. Microplastics are broken down into harmless chemicals through photocatalytic degradation under UV light. This process uses titanium dioxide (TiO₂) nanoparticles as the catalyst.

Thus, this mechanism presents a sustainable water treatment option^[10]. Polyethylene terephthalate (PET) microplastics might be bioremediated in soil by plastic-degrading bacteria like *Ideonella sakaiensis* that produce PETase enzymes. Therefore, this will reduce the environmental persistence of the microplastics^[3]. These highly advanced wastewater treatment plants are fitted with nanofiber membrane structures that filter and trap microplastics smaller than 1 µm and thus resolve the issue of nanoplastics^[8]. In these new green technologies, bio-based coagulants extracted from natural polymers such as chitosan improve microplastic flocculation and removal from water without adding secondary pollutants^[10].

These developments are supplemented by international efforts to standardise detection methods, for instance, ISO's proposed standards for quantifying microplastics, which provide uniformity in investigations^[11]. Still, there are hurdles remaining, namely high costs, scalability, and environmentally friendly disposal of captured microplastics. Further investment in cross-disciplinary research and public-private partnerships is needed to effectively execute these measures, curbing microplastic pollution at its source and protecting ecosystems^[3].

Toxicity of Microplastics in Human Life

Microplastics pose several health risks as they can be ingested via the mouth, nose, and skin^[10]. Microplastics indicate toxicity through:

- Physical Effects: Microplastics in organs like the gastrointestinal tract or lungs cause tissue damage or inflammation.

- Chemical Toxicity: contaminants (e.g., heavy metals and polychlorinated biphenyls) taken up by microplastics can leach into tissues and induce oxidative stress or endocrine disruption^[1,10].

- Bioaccumulation: chronic conditions can be induced by microplastic accumulation in organs like the brain, kidneys, and liver.

- Microbial Risks: Microplastics transmit pathogens, increasing the risk of infection^[9].

NOTE: Studies suggest links to reproductive issues, immune system dysfunction, and potential carcinogenicity, though long-term impacts require further research^[5].

Other Emerging Contaminants and Their Effects

Ecosystems are under threat from more novel pollutants than microplastics:

Pharmaceuticals: As a study state, hormones and antibiotics in water bodies disrupt aquatic life and contribute to antibiotic resistance ^[6].

Per- and Polyfluoroalkyl Substances (PFAS): The "forever chemicals" that pollute water and soil are linked to cancer and immunological issues ^[5].

Engineered nanomaterials, like silver nanoparticles, can potentially build up in organisms and affect biological processes.

Pesticides: As a Study state that residues that harm pollinators and soil ecosystems, including glyphosate, decrease biodiversity ^[3].

These contaminants, including microplastics, bioaccumulate, persist in the environment, and pose a threat to human health and ecosystems.

Measures to Avoid Microplastics in the Ecosystem

Coordination is required to minimize microplastic pollution:

- Policy Measures: Promote biodegradable alternatives, enforce more rigorous waste control regulations, and ban microbeads in beauty products ^[3].
- Waste Management: Implement advanced filtration in wastewater treatment plants to harvest microplastics, reduce single-use plastics, and improve recycling infrastructure ^[8].
- Public Awareness: Get customers embrace green products, use natural fibres, and use less plastic.
- Innovation: Create biodegradable technology and polymers to extract microplastics from water and soil, e.g., biofilters or magnetic nanoparticles ^[3].

- International Cooperation: To overcome plastic pollution, implement international deals, such as the UN Plastic Pollution Treaty

Conclusion

The harm caused by microplastics to ecosystems and human health is comprehensive and involves various aspects ^[9]. It is necessary that this issue be addressed because they are dispersed widely in food, soil, water, and air and possess the property of transporting harmful chemicals ^[1]. Detection techniques such as SEM-EDX, FTIR, Raman spectroscopy, and Py-GC/MS are used to achieve this, but due to their potential to cause physical damage in addition to chemical and microbiological damage, immediate action is necessary ^[4,8].

Two new pollutants that intensify environmental deterioration in addition to microplastics are pharmaceuticals and PFAS ^[5]. To counter such threats, holistic strategies that combine innovation, policy, and community participation are needed.

Suggestions for Making the Earth a Better Place

The following is advised to reduce microplastics and other contaminants:

Reduce Plastic Usage: Promote reusable items and gradually eliminate single-use plastics.

oPromote Circular Economies: Invest in recycling plants and biodegradable products.

oFinance Research: Invest in research on the long-term effects of microplastics and newly recognized pollutants.

Revitalize Regulations: Implement international standards for plastics manufacture, waste dumping, and emission of pollutants.

Mobilize Community Action: Promote environmental literacy, green culture, and community cleanups.

Incentivize green tech by coming up with solutions for clean production and pollution cleanup.

With these approaches combined, we can reduce the impact of microplastics and other impurities in nature, making the planet healthier.

REFERENCES

1. Amelia TSM, Khalik WMAWM, Ong MC, Shao YT, Pan H-J, Bhupalan K. Marine microplastics as vectors of major ocean pollutants and its hazards to the marine ecosystem and humans. *Prog Earth Planet Sci* [Internet]. 2021;8(1). Available from: <http://dx.doi.org/10.1186/s40645-020-00405-4>
2. Arienzo M, Ferrara L, Trifuoggi M. The dual role of microplastics in marine environment: Sink and vectors of pollutants. *J Mar Sci Eng* [Internet]. 2021;9(6):642. Available from: <http://dx.doi.org/10.3390/jmse9060642>
3. Basumatary T, Biswas D, Boro S, Nava AR, Narayan M, Sarma H. Dynamics and impacts of microplastics (MPs) and nanoplastics (NPs) on ecosystems and biogeochemical processes: The need for robust regulatory frameworks. *ACS Omega* [Internet]. 2025;10(17):17051–69. Available from: <http://dx.doi.org/10.1021/acsomega.5c01175>
4. Bhardwaj LK, Rath P, Yadav P, Gupta U. Microplastic contamination, an emerging threat to the freshwater environment: a systematic review. *Environ Syst Res* [Internet]. 2024;13(1). Available from: <http://dx.doi.org/10.1186/s40068-024-00338-7>
5. Coffin S, Bouwmeester H, Brander S, Damdimopoulou P, Gouin T, Hermabessiere L, et al. Development and application of a health-based framework for informing regulatory action in relation to exposure of microplastic particles in California drinking water. *Microplast nanoplast* [Internet]. 2022;2(1):12. Available from: <http://dx.doi.org/10.1186/s43591-022-00030-6>
6. Horton AA, Walton A, Spurgeon DJ, Lahive E, Svendsen C. Microplastics in freshwater and terrestrial environments: Evaluating the current understanding to identify the knowledge gaps and future research priorities. *Sci Total Environ* [Internet]. 2017;586:127–41. Available from: <http://dx.doi.org/10.1016/j.scitotenv.2017.01.190>
7. Johannessen C, Helm P, Metcalfe CD. Detection of selected tire wear compounds in urban receiving waters. *Environ Pollut* [Internet]. 2021;287(117659):117659. Available from: <http://dx.doi.org/10.1016/j.envpol.2021.117659>
8. Wu Z, Wu Y, Zhang Z, Dong J, Li H, Zhao X, et al. Quantitatively tracing microplastics in sewage sludge using thermodesorption gas chromatography/mass spectrometry combined with pyrolysis. *J Hazard Mater* [Internet]. 2025;494(138652):138652. Available from: <http://dx.doi.org/10.1016/j.jhazmat.2025.138652>
9. Yarahmadi A, Heidari S, Sepahvand P, Afkhami H, Kheradjoo H. Microplastics and environmental effects: investigating the effects of microplastics on aquatic habitats and their impact on human health. *Front Public Health* [Internet]. 2024;12:1411389. Available from: <http://dx.doi.org/10.3389/fpubh.2024.1411389>
10. Zhao B, Rehati P, Yang Z, Cai Z, Guo C, Li Y. The potential toxicity of microplastics on human health. *Sci Total Environ* [Internet]. 2024;912(168946):168946. Available from: <http://dx.doi.org/10.1016/j.scitotenv.2023.168946>
11. Li Y, Tao L, Wang Q, Wang F, Li G, Song M. Potential health impact of microplastics: A review of environmental distribution, human exposure, and toxic effects. *Environ Health (Wash)* [Internet]. 2023;1(4):249–57. Available from: <http://dx.doi.org/10.1021/envhealth.3c00052>

12. Lee Y, Cho J, Sohn J, Kim C. Health effects of microplastic exposures: Current issues and perspectives in South Korea. Yonsei Med J [Internet]. 2023;64(5):301. Available from: <http://dx.doi.org/10.3349/ymj.2023.0048>

13 .Martín J, Santos JL, Aparicio I, Alonso E. Microplastics and associated emerging contaminants in the environment: Analysis, sorption mechanisms and effects of co-exposure. Tren Environ Anal Chem [Internet]. 2022;35(e00170):e00170. Available from: <http://dx.doi.org/10.1016/j.teac.2022.e00170>

ABOUT THE AUTHORS

Malla Bharadwaj Sai Satya Murthy

M.Sc. Forensic Science, Specialized in
Advanced Forensic Chemistry and
Forensic Toxicology



Bonagiri JayaRaju

M.Sc. Forensic Science, Specialized in
Advanced Forensic Physics and Digital
Forensics



Exploring Robotic Handwriting: Forensic Examination and Challenges

Author - Harsh Aniket

Abstract:

With advancements in technology, robotic writing is being utilised at several places for education and creative purposes. The robotic writings, when examined, appear to have even pen pressure throughout the strokes with blunt initial and terminal strokes. However, the capability of the robotic systems to mimic human writings with utmost precision has created an alarming situation. Robotic systems clubbed with artificial intelligence often trick the existing signature verification systems, and the robotic forgeries are often considered as natural human writings. The present study discusses the distinguishing characteristics and challenges in examining robotic writings.

Keywords: Robot, robotic writing, handwriting examination, artificial intelligence, questioned document.

Introduction

Handwriting is a neuromuscular activity that is unique to an individual and includes all the characteristics, habits, and peculiarities acquired by that person. It depends on the fact that no person can write completely alike.¹ The act of writing goes beyond the physical formation of letters but also reflects personal characteristics and idiosyncrasies that develop over time and experience.² As a person continues to write, characteristics evolve and become specific to the individual. A noteworthy aspect of handwriting is the natural and unconscious variation that occurs even when the same words or letters are written. However, these variations are involuntary and consistent within a natural range specific to the individual, is an essential quality of genuine handwriting, and its absence often indicates forgery.³

With the rapid advancement in technology, the methods used to capture handwriting have significantly changed. Modern innovations have replaced the handwriting being recorded onto paper with a pen into more sophisticated alternatives. Digital pens and tablets allow the users to write directly onto screens. Beyond these, robotic systems have emerged as an alternative to reproduce handwriting. Several robotic arms, such as Line-us and iDraw have been specifically designed for imitating human handwriting with precision. Several companies like 'Bond' manufacture robots that mimic human writing by controlling the pen strokes, sequence, and pressure.

Existing literature suggests that researchers have been actively involved in developing low-cost robots that can write in a human-like manner for educational and creative applications, which has made robotic writing easily accessible.^{4, 5, 6} These robots are designed with remarkable precision and consistency. With the help of pre-programmed algorithms and artificial intelligence, they are capable of mimicking human handwriting. This automation has made the process of handwriting generation faster, efficient, and less dependent on human effort. Such technologies are being extensively utilised in areas including robotic paintings, artistic writings and calligraphy, in the medical profession for writing prescriptions, assistive writing for people with disabilities, and instructing handwriting etc.^{7, 8, 9} Robots have also been utilized to create handwriting similar to human writings to understand how different physical factors like writing speed, pressure, and position affect the way ink appears on paper to build a scientific foundation for better signature analysis.¹⁰ While robotics, along with artificial intelligence, has brought significant advancements in several fields, their possible misuse has raised serious concerns, particularly in the field of handwriting and signature forgeries. Robotics and AI have been extensively used to create writings and signatures, which were significantly identified as original by the algorithm-based identification systems used to detect forgery.⁵

With the increasing usage of robotics along with artificial intelligence in writing technologies, this article critically discusses the current trends in the generation and forensic examination of robotic handwriting. The article also highlights challenges posed by such machine-generated handwriting, particularly in distinguishing it from genuine human writing.



Distinguishing characteristics of robotic writings

Differentiating robotic writings from human writings is one of the major challenges posed in front of forensic document examiners. The identification of the genuineness of traditional handwriting analysis focuses on features like rhythm, tremors, initial and terminal strokes, connecting strokes, pressure variations, form, and formation of letters.¹ Similarly, research investigations have been carried forward to understand the typical characteristics of robotic writing that differentiates it from the human writings. In natural writings, there is a change in pressure based on the speed and movement of the writer's hand. However, robotic writings have even pen pressure throughout the written stroke, that is, the thickness and darkness are same throughout the strokes

Fig. 1: Change in pressure through the strokes in the natural human handwriting versus even pen pressure throughout the stroke in robotic writings.⁴ Permission for the reproduction of all parts of Figure 1 was granted by the respective publisher on July 04, 2025 under license number 6061900647368.

Furthermore, the robotic writings exhibit blunt initial and terminal strokes. There is a lack of tapered strokes or pen drags in those writings (Fig. 2). The spacing between letters, words, and sentences in robotic writings is equidistant throughout the text.

The absence of rhythm, tapered strokes, and pen drags, and the presence of even pen pressure throughout the writing, is suggestive of the lack of freely written strokes and appears to be drawn. According to Osborn, two writings of the same person are never exactly alike in all details, and absolute uniformity is not possible. However, in the robotic writings, alternate letter forms are observed, but the letters can be precisely superimposed on each other (Fig. 3). This precision can only be achieved by machine-created writings, which significantly helps in differentiating the robotic writings from the natural human writings.

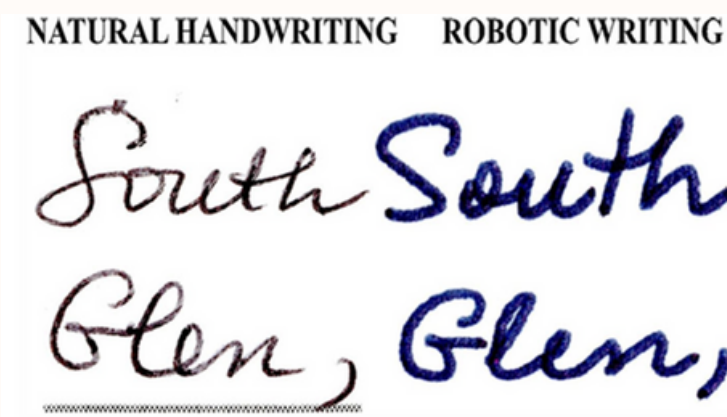
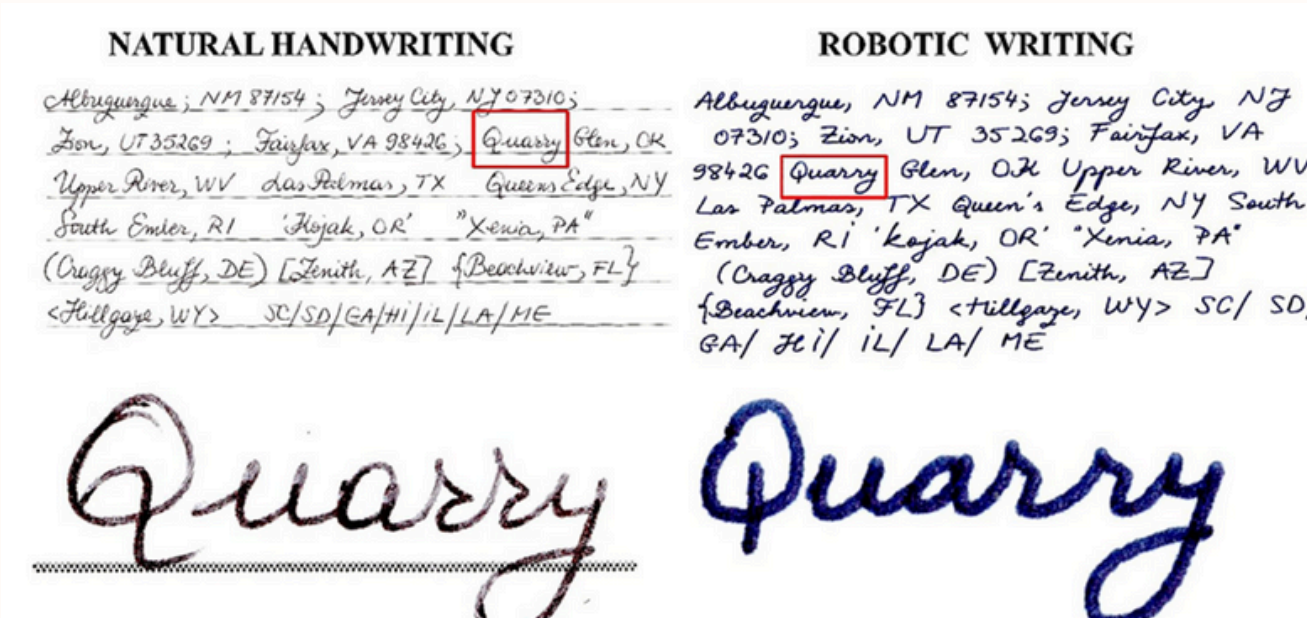


Fig 2: Tapered strokes in natural writing and blunt strokes in robotic writings.⁴ Permission for the reproduction of all parts of Figure 2 was granted by the respective publisher on July 04, 2025 under license number 6061900647368.



Albuquerque, NM 87154; Jersey City, NJ 07310; Zion, UT
 35269; Fairfax, VA 98426 Quarry Glen, OK Upper River, WV Las
 Palmas, TX Queen's Edge, NY South Ember, RI 'Kojak, OR'
 Xenia, PA (Craggy Bluff, DE) [Zenith, AZ] {Beachview, FL}
 <Hillgate, WY> SC/ SD/ GA/ HI/ IL/ LA/ ME

NM ME

NM ME

NME

DE Edge Ember

DE Edge Ember

DE Ember

AZ Zenith

AZ Zenith

AZ Zenith

Challenges and present solutions in the identification of Robotic Writings

Several algorithm-based software programs are created and trained to detect forgeries in any writing or signature. The robot or robotic models in these cases are trained to copy human writings based on not just the shape of characters in the writing but also movement, speed, and energy while appending the signature using the Lagrangian physics model. The data in the form of signatures created by the robotic systems is further supplied to machine learning systems, which helps the system to learn about the above-mentioned specifications of the signatures. Thus, if a new signature is supplied to the system, the robot uses these already fed robotic motions to differentiate between the real or forged writings or signatures.¹¹

Similarly, sophisticated robotic systems such as Line-us, iDraw and AI tools like Generative Adversarial Networks (GANs) are also trained to mimic handwriting or signatures. These writings or signatures have such a human-like precision that they often trick the existing signature verification system, and the signatures are considered as real. For instance, these robotic machines, if equipped with pens or pencils, can create forgeries that closely mimic human handwriting to such a degree that it is often difficult to differentiate them with the human writings through human eye and even by automated systems.^{5, 10}

Successful attempts have been made to solve the above-mentioned problem by using the same robot and AI-generated signatures to train the existing signature verification systems regarding what robotic or AI-generated forgeries look like. The results have been significantly improved by the attempt, and the existing system, to an extent, was able to differentiate the robotic writings with the help of this additional training. However, this emphasizes the fact that while technology has made signature verification more convenient, it has also opened the doors for such robotic forgeries complicated to detect for the forensic document examiners.⁵

The problem may increase manifold if the reproduction copies of such robotic writings are presented to the forensic document examiners to examine. Thus, it is suggested that the forensic document examiners need to be updated about the advancements taking place in robotic technology. This level of technological precision in robotic technology also calls for the necessity of the formulation of advanced frameworks capable of identifying subtle deviations from human neuromuscular patterns along with the routine document examination. With the increased usage of robotic writings in several fields in the present time, the inclusion of these sophisticated and robust discriminative metrics has become a necessity to ensure the proper delivery of justice in the court of law.

Conclusion

The forensic examination of robotic handwriting introduces several complexities that challenge the traditional methods of determination of authorship of handwriting. Robotic systems along with artificial intelligence are capable of mimicking human writings with high precision. But these writings are highly uniform and mechanically consistent and often lack natural variation which is a recognisable feature of natural human handwriting. However, with increase in technological advancements, the capabilities of the robots to copy the writings have increased and they often trick the document examiners and even the algorithm-based signature verification systems. This technological precision of robotic writings, therefore, necessitates the development of advanced frameworks and discriminative metrics to detect robot generated artifacts. It is also imperative for forensic document examiners to integrate computational approaches and interdisciplinary methodologies while examining the cases where there is a suspected robotic writing to ensure non-erroneous opinions and uphold evidentiary reliability in legal and investigative contexts.

References

1. Osborn, A. S. (1929). Questioned Documents (2nd ed.). Boyd Printing Co, Albany, New York.
2. Hilton, R. A. (1993). Scientific Examination of Questioned Documents. CRC Press, Boca Raton.
3. Huber, R.A. and Headrick, A.M. (1999) Handwriting identification: facts and fundamentals, CRC Press, New York.
4. Dumitra, A.; Guzowski, A.; Jean, A.; Shaw, M.; Warmbier, G.; Zippo, P. (2019). Distinguishing Characteristics of Robotic Writing. Journal of Forensic Sciences. 64 (2): 468-474. 10.48550/arXiv.2204.07246
5. Bird, J.; Naser, A.; Lotfi, A. (2023). Writer-independent signature verification; Evaluation of robotic and generative adversarial attacks. Information Sciences. 633:170-181. 10.1016/j.ins.2023.03.029
6. Huang, T. and Xiong R. (2025). Cost-Effective Robotic Handwriting System with AI Integration. IEEE Long Island Systems, Applications and Technology Conference. 10.48550/arXiv.2501.06783

7. Endo, Kazuya; Kanoh, Masayoshi; Nakamura, Tsuyoshi (2015). Teaching Handwriting using Robot and Onomatopoeia. Conference on Technologies and Applications of Artificial Intelligence (TAAI), Tainan, Taiwan. 10.5057/jjske.TJSKE-D-16-00050
8. Zingrebe, D.S.; Gülzow, J.M.; Deussen, O. (2023). Robotic Writing of Arbitrary Unicode Characters Using Paintbrushes. Robotics. 12, 72. 10.3390/robotics12030072
9. Breton, I. and Campeau-Lecours, A. (2024). Development of a robotic handwriting assistant for children with movement disorder. Acta Tecnología - International Scientific Journal. 10 (2): 73-79. 10.22306/atec.v10i2.203
10. Franke, K; Schomaker, L. and Koppen, M. (2005). Pen force emulating robotic writing device and its application. IEEE Workshop on Advanced Robotics and its Social Impacts. 10.1109/ARSO.2005.1511616
11. Diaz, M.; Ferrer, M.; Gil, J.; Rodriguez, R.; Zhang, P. and Jin, Lianwen. (2025). Online Signature Verification based on the Lagrange formulation with 2D and 3D robotic models (Preprint). 10.48550/arXiv.2503.13573

ABOUT THE AUTHORS



Harsh Aniket

Scientific Assistant

(Fingerprints and Questioned Document Division),
National Forensic Sciences University, Delhi Campus

Game-Based Cybercrimes: Digital Forensics in Online Multiplayer Environments

Author - Mr. Himanshu Chudasama, Mr. Maypal Daki, Mr. Eshant Chabadiya, Mr. Bhumit Chavdau

Introduction

Online multiplayer games have gone through the roof (literally), having developed into an extensive computerized cosmos in which millions of people meet, play, and risk their own money on online goods. But as those virtual worlds have become increasingly sophisticated and even more economically important, they have also produced a new form of virtual crime: game-based cybercrimes. These are not petty bad things in the game world, these are a massive variety of crimes, and include the most elaborate financial misappropriations and account raiding, to the most creative cheating and the theft and subsequent violation of intellectual property, right the way up to participating in a wide range of post cyber-enabled criminality. There are no borders to the online gaming world, and in some manifestations, the communication in question is highly anonymized; there is so much potential value in the form of digital assets, too, that merely banning or blocking the whole gigantic industry makes little sense to law enforcement as well. Here comes in the science of digital forensics, which aim, essentially, to solve these intricate cyber-crimes, to trace the cyber trails of the perpetrators and finally to ensure that justice is served in the vast, pixelated arenas of multiplayer games.

Beyond the Pixels: Digital Forensics Unraveling Cybercrime in Online Multiplayer Environments

Over the past twenty years, the entertainment industry of the world has undergone radical changes as online multiplayer gaming, which was once a small niche, has become a massive enterprise that the world faces. The vast majority of the global population is already immersed in virtual worlds: they dedicate thousands of hours to the digital experiences and purchase a great deal of in-game resources and objects, as well as esports. A dark task force of hold-ups, assassinations, and bailouts on games, these are initially intentions. Something that exists in the virtual world of MMOs has its share of real-life criminals. With online games as a new medium of socializing, making business, and competing being a reality, online games themselves also become a haven of illegal activities.

The so-called game-based cybercrimes are a special subgroup of digital crimes, as their perpetrators take advantage of the nature and vulnerability of online games. These cannot be dismissed as simple and petty in-game offenses, but they are capable of generating serious risks, including direct financial fraud of individual players or large-scale theft of intellectual property of game developers, and finally, may be used as a conduit to form cyber-enabled crimes across money laundering activities and others (Holt & Bossler, 2020). These crimes are sophisticated and transnational and pose tremendous challenges to traditional law enforcement and cyber-defense. Such a complex digital battlefield is the familiar place where digital forensics, the scientific field of studying and retrieving material present in digital devices and networks, acquires its value as an extremely useful tool. This paper will give an insight into the emerging world of game-based cybercrimes, discuss why they have been so problematic and provide the state-of-the-art digital forensic tools being used to unravel this complex virtual crime.



Fig. Advances in the field of Forensic in regards to cyber crime

The Rise of the Virtual Criminal Ecosystem

The enormous numbers that Internet multiplayer gaming is connected to make it a tempting area to be exploited by online criminals. Not only has revenue generated by the world gaming industry as a whole (in form of in-game purchases, subscriptions, advertisements) become significantly greater than the traditional entertainment forms such as cinema or music (Statista, 2024), but mega-industrial giants such as NVIDIA and AMD that lead the gaming industry are now many times more “valuable” than the Hollywood giants Disney or Netflix due to the dominance of PlayStation and Xbox (Statista, 2024). Such an economic activity is huge and breeds on the fertile ground of illegal profit. They not only spend time, but usually large amounts of real money on virtual objects, characters and currencies and develop their own flourishing virtual economies, which in some cases resemble real-life financial markets (Castronova, 2005). The thing is that such real value of the digital assets is one of the main attractions to the criminals.

Several factors contribute to the allure of gaming environments for cybercriminal activities:

Vast User Base: A large pool of potential victims, ranging from casual players to high-spending enthusiasts.

Valuable Virtual Assets: In-game items, rare skins, virtual currency, and high-level accounts can command substantial prices on grey and black markets, making them attractive targets for theft or fraudulent acquisition (Choi & Lee, 2019).

Perceived Anonymity: The use of pseudonyms and virtual identities often fosters a sense of impunity, encouraging illicit behavior.

Cross-Border Nature: Online games operate globally, enabling criminals to operate across national jurisdictions, complicating law enforcement efforts.

Vulnerable User Base: A significant portion of the gaming population comprises younger, less tech-savvy individuals who may be more susceptible to phishing, social engineering, and other scams.

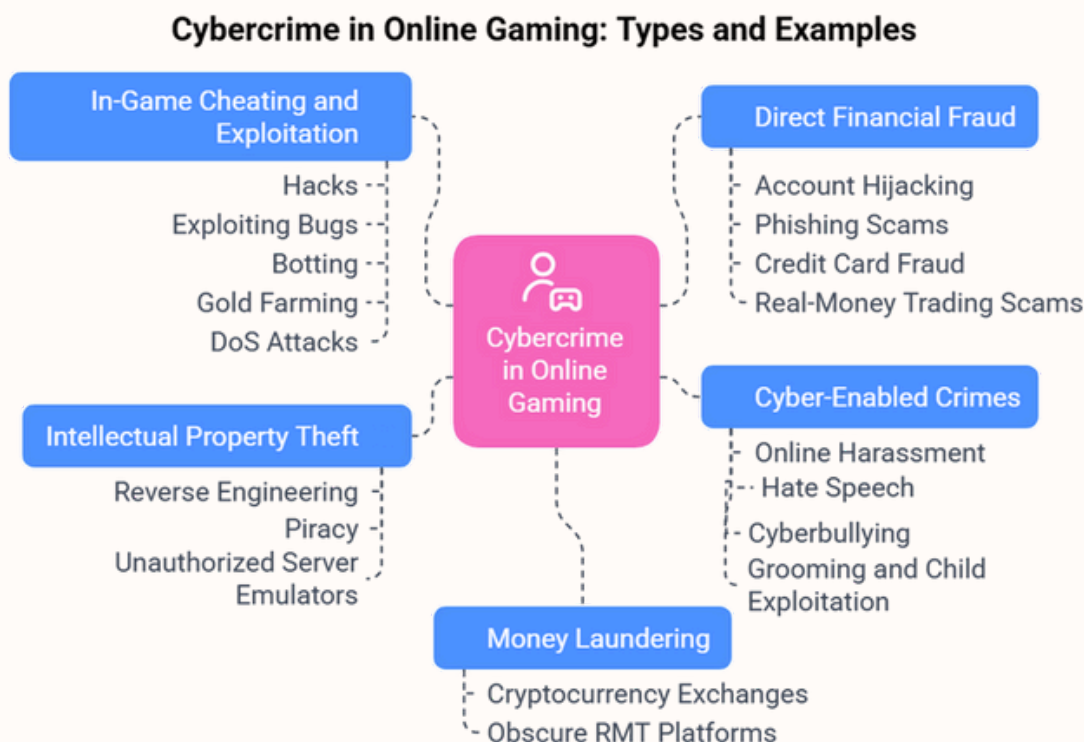


Fig. Cybercrime in Online Gaming, its type and examples



Fig. Digital Forensic in Online Multiplayer Environment

Direct Financial Fraud:

Here we may have the simplest form, which is a case of direct financial theft with old-fashioned cybercrime methods used against the gaming sector. Such scams are a hijacking of accounts (illegal access of player accounts to steal in-game items or sell the account), phishing (tricking the player into giving away his/her log-in credentials), credit card frauds (using stolen credit card information to purchase items in-game), and real-money trading (RMT) scams where the virtual goods bought with real money are never received (Liao et al., 2011).

In-Game Cheating and Exploitation:

This sort of offense directly betrays the integrity and fair nature of a game. It incorporates the use of cheats (e.g., aimbots, wallhacks) to have an unfair advantage in competitive games, bug and glitch exploitation to obtain the redeemable currency or items in-game that they would not have otherwise gotten, botting (where automated programs are used to play the game over long periods), and gold farming (where large amounts of the redeemable currency in the game are massively produced and sold in RMT) (Moser et al., 2013). Game server DoS attacks or defacement, or those on individual players, are also in the same category.

§ Intellectual Property (IP) Theft: This mostly happens to game developers and others. It involves reverse engineering game clients to create unofficial hacks or personal servers, game software piracy, and hosting game-related server emulators that run outside of the official game service and thus violate copyrights and intellectual property (Park et al., 2018).

§ Cyber-Enabled Crimes: Other crimes can be committed using online gaming platforms as these systems come with inbuilt communication tools. This also encompasses disastrous cases of online cyberbullying, hate speech, and harassment, as well as, unfortunately, can also be used to groom and exploit children by sexual predators in search of anonymous means of communication (Holt & Bossler, 2020).

§ Money Laundering: The complex virtual economies, and the possibility to exchange virtual assets back into a real-world currency (such as on cryptocurrency exchanges or trading platforms on the dark web) offer such desirable options as laundering the illegally gained profits of a different crime (Carcillo, 2021).

Digital Forensics: Adapting to the Gaming Frontier

Digital forensics operates on fundamental principles: preservation, acquisition, analysis, and reporting of digital evidence (Casey, 2011). However, applying these principles to the dynamic and distributed nature of online multiplayer gaming environments introduces a unique set of challenges that traditional forensic methodologies may not readily address.

Unique Challenges in Online Multiplayer Environments:

Distributed Data: Unlike crimes confined to a single computer, evidence of game-based cybercrimes is often scattered across multiple locations. This includes the suspect's local client device, the game developer's servers (which may be geographically dispersed), third-party cloud services (e.g., for user authentication, voice chat), and external platforms used for illicit RMT or communication (e.g., Discord, dark web forums). Acquiring all relevant pieces of this puzzle is a complex endeavor (Choi & Lee, 2019).

Volatile Data: Many critical pieces of evidence exist only transiently in live game sessions or in computer memory (RAM). In-memory cheats, active network connections, and real-time chat can be lost if not acquired immediately and forensically soundly.

Intellectual Property (IP) Theft: This mostly happens to game developers and others. It involves reverse engineering game clients to create unofficial hacks or personal servers, game software piracy, and hosting game-related server emulators that run outside of the official game service and thus violate copyrights and intellectual property (Park et al., 2018).

Cyber-Enabled Crimes: Other crimes can be committed using online gaming platforms as these systems come with inbuilt communication tools. This also encompasses disastrous cases of online cyberbullying, hate speech, and harassment as well as, unfortunately, can also be used to groom and exploit children by sexual predators in search of anonymous means of communication (Holt & Bossler, 2020).

Money Laundering: The complex virtual economies, and the possibility to exchange virtual assets back into a real-world currency (such as on cryptocurrency exchanges or trading platforms on the dark web) offer such desirable options as laundering the illegally gained profits of a different crime (Carcillo, 2021).

Scale of Data: High-traffic online games generate astronomical volumes of data daily, billions of log entries, millions of transactions, and extensive chat histories. Managing, filtering, and analyzing such massive datasets requires specialized big data forensic tools and techniques (Liao et al., 2011).

Real-time Nature and Rapid Evolution: Online game environments are constantly evolving with patches, updates, and new content. Cybercriminals swiftly adapt their tactics, making it a continuous arms race between exploiters and security measures. This demands rapid forensic response and agile analytical capabilities.

Forensic Methodologies and Techniques

To overcome these challenges, digital forensics adapts and employs specialized methodologies tailored to the intricacies of online gaming. Investigations typically involve a multi-pronged approach, drawing evidence from various sources:



Fig. Unique challenges in online Multiplayer Environment

Client-Side Data Acquisition: The suspect's local computer remains a primary source. Forensic investigators acquire full disk images of hard drives, looking for:

- ^a Game files: Modified game executables, injected dynamic link libraries (DLLs) indicating cheats.
- ^a User profiles and configuration files: Stored credentials, player settings.
- ^a Chat logs and screenshots: Local copies of communications or visual evidence of illicit activity.
- ^a Temporary files and memory dumps: Volatile data, including active cheat programs, often resides in RAM. Memory forensics tools like Volatility Framework are crucial for analyzing memory images (Gao et al., 2018).
- ^a Malware remnants: Traces of keyloggers or information stealers used for account hijacking.

Server-Side Data Analysis: Game servers are often the most authoritative source of evidence, particularly for complex, coordinated crimes. Access typically requires cooperation from game developers or court orders. Key server-side data includes:

- ^a Game logs: Detailed records of player actions (movement, item usage, skill activation), in-game transactions, chat messages, logins/logouts, IP addresses, and precise timestamps. These logs are vital for reconstructing events (Choi & Lee, 2021).
- ^a Database records: Comprehensive information on player accounts, inventories, virtual currency balances, and historical data.

^a Server system logs: OS logs, web server logs, and authentication server logs provide contextual information about system access and potential breaches.

Network Data Forensics: Network traffic between communication peers can be analyzed typically provided in the form of a packet capture (pcap) format, and may indicate real-time communications patterns, anomalous data flows, or bot networks. Although game traffic is often encrypted, metadata and traffic analysis may yield a significant amount of information as well (Conti et al., 2019).

Third-Party Data Integration: Investigations often extend to external platforms. This includes obtaining records from:

^a Payment processors: For real-money transactions related to RMT or fraudulent purchases.

^a Communication platforms: Chat logs from Discord, Telegram, or other services used by criminal groups to coordinate activities.

^a Social media: Public posts or direct messages relevant to the crime.

Specialized Forensic Techniques:

Log Parsing and Correlation: As game logs are highly voluminous and proprietary, the forensic analysts craft special-purpose scripts and parsers (e.g. in Python and regular expressions) to obtain pertinent information. Most importantly the occurrence of events across different log sources (client, server, network, payment) has to be correlated on the basis of timestamps and unique identifiers to construct a manageable sequence of events (Liao et al., 2011).

Executable Analysis and Reverse Engineering: In case of advanced cheat-tools or malware, or some other unauthorized game client, reverse engineering (disassembly, decompilation) is used to get insight into their inner mechanics, detect the malicious content, and how they manipulate the game environment (Moser et al., 2013).

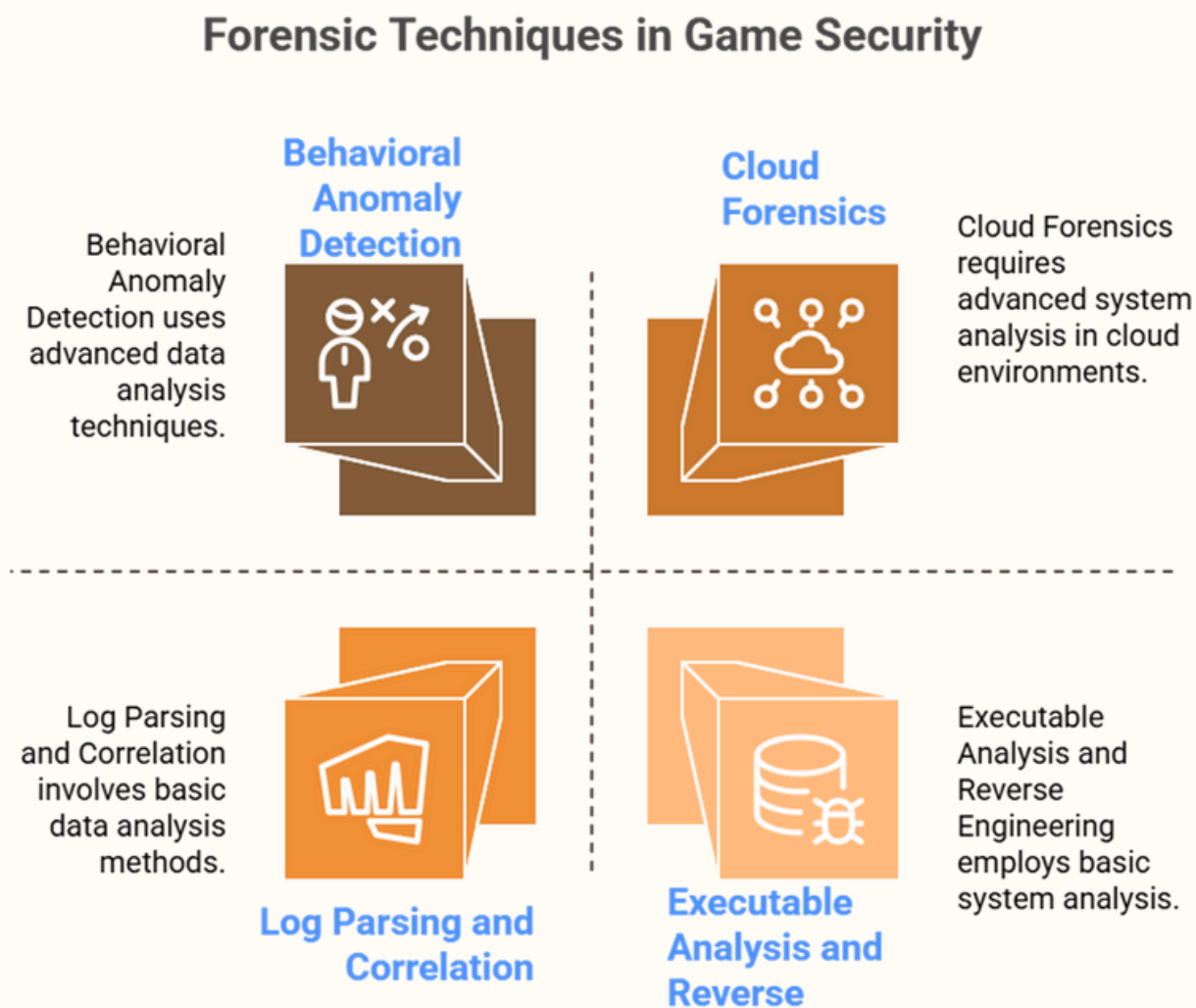


Fig. Forensic Technique in Game Security

Behavioral Anomaly Detection: Machine learning algorithms are also becoming commonly used to detect strange patterns of player behavior that would indicate non-standard gameplay and hence indicate possible botting, automation cheating, or account takeover. This is done through the analysis of data points of thousands of players per period (Liao et al., 2011).

Timeline Reconstruction: This tedious procedure of gathering all the available artifacts concerning the case and organizing them according to the timeline is important in determining the order of events, motive, and finally, the chain of evidence of a crime.

Cloud Forensics: With an increased number of game infrastructures shifting to cloud services (e.g. AWS, Azure, Google Cloud), forensic practitioners need to adjust to gathering and analysing data in the cloud, and more likely they will require custom integration with the API and protocols of a particular provider.

Challenges and Future Directions

Despite significant advancements, digital forensics in online multiplayer environments faces ongoing challenges. The rapid pace of game development and the agile nature of cybercriminals mean that forensic methodologies must continuously evolve. Ethical considerations surrounding player privacy, data retention policies, and the scope of data access remain critical points of contention. The inherent lack of standardized logging or data formats across game developers creates persistent hurdles for law enforcement agencies seeking streamlined investigative processes.

However, the future of digital forensics in this domain is promising, driven by technological innovations and increasing recognition of the problem:

AI and Machine Learning (AI/ML): AI/ML will play an increasingly vital role in automated anomaly detection, predictive analytics to identify emerging threats, and intelligent analysis of massive datasets to pinpoint suspicious activities and potential perpetrators (Conti et al., 2019). AI can help identify complex bot behaviours or detect subtle cheating patterns that human analysts might miss.

Blockchain Technology: The integration of blockchain into virtual economies (e.g., for NFTs, immutable transaction logs) holds potential to enhance transparency and traceability of virtual assets, making it more challenging for criminals to launder funds or obscure illicit transactions (Carcillo, 2021).

Enhanced Collaboration: Greater collaboration between game developers, law enforcement agencies, and forensic experts is crucial. This includes establishing standardized communication protocols for evidence requests, developing common APIs for forensic data access, and fostering intelligence sharing on emerging threats.

Legal Frameworks and Specialization: Developing robust international legal frameworks to address the cross-border nature of game-based cybercrimes is essential for effective prosecution. Furthermore, the demand for forensic professionals with specialized expertise in gaming ecosystems, understanding game design, specific network protocols, and cheat methodologies, will continue to grow.

Concluding Insights:

The immersive and economically significant world of online multiplayer gaming has, regrettably, become a new digital frontier for cybercriminal activity. From sophisticated financial fraud to intricate in-game cheating and even the facilitation of more serious cyber-enabled offenses, the threats are diverse and constantly evolving. In this dynamic landscape, digital forensics stands as an indispensable discipline, adapting its core principles to confront the unique challenges posed by distributed, volatile, and proprietary game-related data.

While the complexities of multi-jurisdictional investigations and the sheer volume of data remain formidable obstacles, ongoing advancements in AI/ML, the potential integration of blockchain technologies, and a growing emphasis on inter-agency collaboration offer promising pathways forward. By continually refining our forensic methodologies and fostering specialized expertise, we can equip law enforcement and game developers with the tools necessary to combat game-based cybercrimes effectively, ultimately working towards a safer and fairer virtual environment for players worldwide.

References

- Austin, C. C. (2020). *The New Criminal Playground: How Online Gaming Has Become a Hub for Cybercrime*. Palgrave Macmillan.
- Carcillo, A. (2021). *Blockchain in Video Games: A Forensic Perspective*. Elsevier.

- Casey, E. (2011). Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet (3rd ed.). Academic Press.
- Castronova, E. (2005). Synthetic Worlds: The Business and Culture of Online Games. University of Chicago Press.
- Choi, H., & Lee, S. G. (2019). Digital Forensic Investigation for Online Game Account Hacking Incidents. IEEE Access, 7, 17855-17865.
- Choi, H., & Lee, S. G. (2021). Game Log-Based Digital Forensic Investigation for Account Hacking Incidents in Online Games. Future Generation Computer Systems, 118, 209-220.
- Conti, M., Dargahi, T., & Dehghantan, A. (2019). Cybersecurity and Digital Forensics: An Advanced Guide for Forensic Investigators. Springer.
- Gao, P., Li, H., & Zhou, Y. (2018). Memory Forensics for Anti-Cheating in Online Games. In Proceedings of the 2018 IEEE 4th International Conference on Computer and Communications (ICCC) (pp. 1667-1671). IEEE.
- Holt, T. J., & Bossler, A. M. (2020). Cybercrime and Digital Forensics: An Introduction (3rd ed.). Sage Publications.
- Liao, Y., Lin, X., Wen, Q., & Zhang, Y. (2011). Detecting online game bots using behavioral analysis. Computers & Security, 30(6-7), 406-419.
- Moser, L., Kruegel, C., & Kirda, E. (2013). All Your Base Are Belong To Us: Forensic Analysis of Online Game Cheats. In Proceedings of the 2013 ACM SIGSAC Conference on Computer and Communications Security (pp. 13-24). ACM.

ABOUT THE AUTHORS

Mr. Himanshu Chudasama

Department of Biochemistry and Forensic Science, Gujarat University, Ahmedabad



Mr. Maypal Daki

Department of Biochemistry and Forensic Science, Gujarat University, Ahmedabad



Mr. Eshant Chabadiya

**Department of Biochemistry and Forensic Science, Gujarat
University, Ahmedabad**



Mr. Bhumit Chavda

**Research Scholar, Department of Biochemistry and Forensic
Science, Gujarat University, Ahmedabad, Gujarat, India.**



CASE STUDY

on

THE NTH ROOM CASE: HOW A CYBERSEX TRAFFICKING SCANDAL EXPOSED SOUTH KOREA'S DIGITAL VULNERABILITIES AND TECHNOLOGICAL MEASURES HAS SOUTH KOREA INTRODUCED TO DETECT AND DELETE ILLEGAL SEXUAL CONTENT

Author: Balaji M



Introduction

The Nth Room case, which erupted between 2018 and 2020, stands as one of the most egregious examples of cyber-enabled sexual exploitation in South Korea's history. This case involved the blackmail, trafficking, and abuse of at least 103 victims—including 26 minors—through encrypted Telegram chat rooms, where sexually exploitative videos were distributed to tens of thousands of anonymous users in exchange for cryptocurrency payments^{[1][2][3]}.

The Nth Room case, which erupted between 2018 and 2020, stands as one of the most egregious examples of cyber-enabled sexual exploitation in South Korea's history. This case involved the blackmail, trafficking, and abuse of at least 103 victims—including 26 minors—through encrypted Telegram chat rooms, where sexually exploitative videos were distributed to tens of thousands of anonymous users in exchange for cryptocurrency payments^{[1][2][3]}. The investigation and public outcry that followed exposed critical vulnerabilities in South Korea's cybercrime defenses, catalyzing national debate and legal reforms. This case study examines the structure of the Nth Room operation, the technological and legal gaps that allowed it to flourish, and the lessons learned for future digital crime prevention.

Anatomy of the Nth Room Operation

How the Exploitation Began

Recruitment and Blackmail: Perpetrators, using aliases like “God God” (Moon Hyung-wook) and “Doctor” (Cho Ju-bin), lured victims—often minors—through Twitter and chat apps by promising lucrative modeling or part-time jobs^{[1][2][4]}.

Data Harvesting: Once initial contact was made, victims were directed to Telegram, where their personal information was extracted under false pretenses^{[2][4]}.

Escalating Coercion: With this information, operators blackmailed victims into producing increasingly explicit and degrading content, under threat of exposure to their families, friends, or schools^{[2][4][3]}.

Distribution and Monetization

Telegram Chat Rooms: The exploitative content was distributed in at least eight chat rooms, labeled by ordinal numbers—hence the name “Nth Room”^{[1][2][3]}.

Payment Systems: Access to these rooms was sold for between \$200 and \$1,200, typically paid in cryptocurrency to ensure anonymity^{[1][4][3]}.

Scale: Over 260,000 unique IDs accessed these rooms, with estimates of active users ranging from 60,000 to over 100,000^{[1][2]}

Perpetrators and Arrests

Key Figures: Moon Hyung-wook (“God God”) and Cho Ju-bin (“Doctor”) were arrested in 2020 and sentenced to 34 and 40 years in prison, respectively^{[1][2]}.

Accomplices: Several other operators and users were also apprehended, but the sheer number of participants made comprehensive prosecution difficult^{[1][3]}.

Vulnerabilities Revealed in South Korea’s Cybercrime Defenses

The Nth Room case laid bare several systemic weaknesses in South Korea’s approach to digital crime:

1. Encrypted Messaging Apps and Anonymity

Telegram’s Role: Telegram’s end-to-end encryption and lax registration requirements allowed perpetrators to operate with near-total anonymity, making it difficult for authorities to trace communications or identify users^{[1][2][3]}.

Cryptocurrency Payments: The use of cryptocurrencies further obscured financial trails, complicating efforts to track payments and link them to individual identities^{[1][3]}.



Impact and Aftermath

Public and Legal Reactions

National Outrage: The case triggered widespread protests and a record number of presidential-petition signatures, demanding harsher penalties and greater transparency^{[2][4]}.

Legal Reforms: In response, South Korea enacted new laws to strengthen penalties for digital sex crimes, regulate online platforms, and protect victims' identities^{[5][6]}.

Ongoing Challenges

Platform Accountability: Despite reforms, encrypted messaging apps remain difficult to police, and copycat crimes have persisted^{[1][5]}.

International Cooperation: The global nature of digital platforms necessitates cross-border collaboration, which remains inconsistent and slow-moving^{[1][5]}.

Lessons Learned and Recommendations

1. Strengthen Digital Forensics and Law Enforcement Capabilities

Invest in specialized cybercrime units with advanced technical training and tools for tracking encrypted communications and cryptocurrency transactions.

2. Update Legal Frameworks

Ensure that laws keep pace with technological developments, including provisions for prosecuting those who possess or view illegal content, not just producers and distributors.

3. Enhance Platform Regulation and Cooperation

Mandate greater accountability and cooperation from messaging platforms, including requirements for data retention, reporting of illegal activity, and rapid response to law enforcement requests.

4. Support Victims and Combat Stigma

Expand victim support services and public education campaigns to reduce stigma and encourage reporting of digital sex crimes.

5. Foster International Partnerships

Develop robust international agreements to facilitate information sharing and joint investigations of cyber-enabled crimes.

Technological measures has South Korea introduced to detect and delete illegal sexual content

South Korea has introduced a suite of advanced technological measures to detect and delete illegal sexual content, especially in response to the proliferation of digital sex crimes and deepfake materials. The most notable initiatives include:

1. AI-Powered Surveillance and Detection Systems

AI Surveillance System for Digital Sex Crimes:

Seoul has deployed a 24/7 artificial intelligence surveillance system that uses AI facial recognition and deep learning to identify sexually exploitative materials involving children and adolescents. This system can:

Detect illegal content in about 1.5 minutes 80 times faster and 300% more accurate than manual review.

Recognize victims even if their faces are not visible by analyzing contextual clues (e.g., school uniforms, objects, language).

Monitor vast quantities of content, including material hosted on foreign servers, and generate automatic removal requests in multiple languages^{[8][9]}.

2. Automated Removal and Reporting

Rapid Deletion Protocols:

Platforms are now required to remove flagged illegal sexual content within 24 hours of a request from the Korea Communications Commission or relevant authorities^{[10][11][12]}.

Automated Reporting Tools:

The AI system can automatically generate reports and compose emails to website operators (including overseas platforms like Telegram and

Instagram), requesting the deletion of identified illegal content. These reports are reviewed by officials before being sent^[9].

3. Real-Time Deepfake Detection

Real-Time AI Detection:

The government is developing and deploying AI systems that can detect deepfake sexual content in real time. Once detected, the system automatically requests deletion from the platform operator^{[10][11]}.

Preemptive Blocking:

Platforms can now block sexually explicit deepfake images and videos before review, minimizing the risk of further distribution^[10].

4. Centralized Support and Coordination

National Center for Digital Sexual Crime Response:

This 24/7 center acts as a centralized hub for reporting, counseling, and victim support,
and coordinates the deletion of illegal content, particularly on encrypted or closed platforms like Telegram^[9].

5. Platform Accountability and International Reach

Mandatory Safety Programs:

All internet platforms must implement detection and filtering systems to identify and remove illegal sexual content, including AI-generated material^[12].

Global Monitoring:

The AI systems are designed to search for illegal content on servers worldwide, and can draft removal requests in foreign languages to address the increasing distribution of exploitative material overseas^{[8][9]}.

6. Education and Hotlines

Awareness Initiatives:

Schools and universities are introducing education programs and prevention booths to inform youth about the legal consequences of creating, sharing, or viewing illegal sexual content^[10].

Hotlines and Reporting Websites:

New hotlines and online platforms have been established to make it easier for victims and the public to report illegal activities^[10].

Conclusion

The Nth Room case was a watershed moment for South Korea, exposing the dark underbelly of digital exploitation and the vulnerabilities in the nation's cybercrime defenses. While significant progress has been made in response, the case underscores the need for constant vigilance, legal innovation, and societal change to keep pace with the evolving landscape of online abuse.

By learning from the failures and successes of the Nth Room investigation, South Korea and the world—can better protect vulnerable individuals and uphold justice in the digital age.

This case study draws on reporting from major news outlets, academic analysis, and the 2022 Netflix documentary “Cyber Hell: Exposing an Internet Horror” for a comprehensive account of the Nth Room case and its implications for cybercrime defense in South Korea^{[1][2][3][5][6]}.

Reference:

- https://en.wikipedia.org/wiki/Nth_Room_case
- <https://www.netflix.com/tudum/articles/everything-to-know-about-the-nth-room-case-in-cyber-hell>
- <https://www.lowyinstitute.org/the-interpreter/nth-room-case-modern-slavery-digital-space>
- <https://www.bbc.com/news/world-asia-52030219>

- <https://www.asiaglobalonline.hku.hk/asia-global-voices/nth-room-telegram-and-why-wont-be-last-cybercrime-scandal>
- <https://pmc.ncbi.nlm.nih.gov/articles/PMC9915142/>
- <https://muse.jhu.edu/pub/5/article/798133/pdf>
- <https://english.seoul.go.kr/seoul-to-be-the-first-in-the-nation-to-identify-and-delete-sexually-exploitative-materials-involving-children-and-adolescents-using-ai-facial-recognition-technology/>
- <https://www.isdp.eu/wp-content/uploads/2025/06/Brief-Korea-Crimes.pdf>
- <https://www.koreaherald.com/article/3848302>
- <https://www.chosun.com/english/nationalen/2024/11/07/5HRDOV75LVHKDFVDNMUNMS6ZVM/>
- <https://www.mdpi.com/2076-0760/13/11/596>

ABOUT THE AUTHOR

Balaji M,

B.Sc. Forensic Science

Intern, Clue4 Evidence Forensic Lab, Bangalore



COMMERCIALISED THREATS & REAL-TIME RESPONSE

Author - Parth Tejalkumar Soni, Kiran R Dodiya, Dr. Kapil Kumar

Abstract

Cybercrime has evolved from hacker-driven incidents into a billion-dollar industry, making it far more common and motivated by profit. According to researchers, Cybercrime-as-a-Service (CaaS) represents a fundamental shift in the cybercrime landscape, enabling cybercriminals to offer more targeted services, such as Ransomware-as-a-Service (RaaS), on the dark web, thereby evolving the cybercrime threat landscape. The first article examined the changing face of the cybersecurity landscape, including new commercialised cybercrime, and how it rendered real-time response critical like never before. We further articulated that Security Orchestration, Automation, and Response (SOAR) is a key enabler in the fight against these evolving threats, in concert with AI-driven threat detection, and Zero Trust Policies as organisations must be able to respond at the speed of the threat to avoid catastrophic financial interpretation damage as attacks become more sophisticated and fast-moving.

Introduction: The Commercialisation of Cybercrime

Cybercrime has progressed from the dark realms of solo hackers proving their skills or seeking fame, to a well-organised and lucrative enterprise. Back at the dawn of the internet, many cybercriminals were driven by curiosity, notoriety, or a desire to expose security weaknesses so they could be fixed sooner. However, the evolution of cybercrime has kept pace with the growth of the internet. These days, we are seeing the heart of cybercrime shift far less towards rogue hacking and more towards functioning like a well-oiled, multi-billion-dollar industry.(What Is Cybercrime and How Can You Prevent It?, n.d.) In Earlier days, cybercriminals worked alone; they functioned in well-oiled machines that behaved like companies, complete with specialised positions, services, and layers of hierarchy.Its transformation is well demonstrated with the emergence of Cybercrime-as-a-Service (CaaS). Similar to the success of Software-as-a-Service (SaaS) platforms in the legitimate tech sector, the same type of in-

demand service has been offered by cybercriminals as they commercialised their operations and started selling malware, ransomware, and phishing kits as a service. (Ganguli, n.d.) Ransomware-as-a-Service (RaaS) platforms, for example, are enabling even the least technically savvy criminals to carry out sophisticated attacks. They often also offer customer support, tutorials, and revenue-sharing models to ensure these services make partaking in cybercrime as simple as deploying any other modern startup. At its core, it is simply a marketplace for criminal tools and services that functions just like any other software product sold on the web. (What Is Ransomware as a Service (RaaS)? | CrowdStrike, n.d.) The professionalisation of cybercrime has led to increasing sophistication and urgency in the need to combat these forms of attacks. Given how rapidly these threats have evolved and the high-stakes environment they create, it should be evident to anyone that more traditional hardware solutions, which reactively defend functionality, are no longer sufficient. Never has the demand for real-time response become more relevant. Effective organisations must be able to detect, mitigate and recover from such threats in real-time to reduce the damage.



An illustration of the high stakes at risk can be found in the 2021 Colonial Pipeline ransomware attack: In this case, a criminal organisation utilised a commercialised ransomware tool to disable one of the largest fuel pipelines in the United States, resulting in fuel shortages across the country. It illustrated the impact cybercrime can have on national infrastructure and economies due to the resulting downtime. It exemplified the demands of real-time cybersecurity – fast and flexible responses that can be implemented immediately. (The Attack on Colonial Pipeline: What We’ve Learned & What We’ve Done Over the Past Two Years | CISA, n.d.)

The New Age of Cybercrime

Cybercrime-as-a-Service (CaaS)

Cybercrime, which was once the domain of rogue hackers, has evolved into a professional and highly organised industry. The cybercrime landscape has undergone numerous changes, but perhaps none as impactful as the rise of Cybercrime-as-a-Service (CaaS), which offers cybercriminals a more structured and efficient approach to their malicious activities, paralleling legitimate businesses. Now, crime groups do not depend on a few hackers but instead function like established companies with defined roles, services, and revenue-sharing mechanisms. In this context, we have also seen an increase in scalable, accessible cybercrime, which is high-profit and fast-growing. (Ganguli, n.d.) A central pillar of this evolution is Ransomware-as-a-Service (RaaS), in which cybercriminals create advanced tools for encrypting data and lease them out to affiliates who launch the attacks. In the legitimate tech space, SaaS functions in a way that has allowed even non-technical individuals to deploy high-level cyberattacks. In return, the malware creators receive a share of the ransom payments, while the affiliates can target firms worldwide. REvil and Conti are two prominent examples of ransomware groups operating under this model, providing malware kits to criminals in exchange for a cut of the criminal proceeds. (What Is Ransomware as a Service (RaaS)? | CrowdStrike, n.d.)

Outside of ransomware, the business of data breaches, malware kits and phishing tools is also booming. With the rise of the dark web, cybercrime has become a very profitable business, and cybercriminals can exchange

information, tools and even access to already breached systems in secret



Case Studies/Real-World Examples

MOVEit Transfer Data Breach — 2023

The MOVEit Transfer software has been used by thousands of organisations globally for secure file transfers. However, it was hacked into by the Cl0p ransomware organisation in 2023. The leak exposed sensitive details of millions of people's personal and financial information. Cl0p functions along the lines of Ransomware-as-a-Service, granting affiliates access to the ransomware and collecting a portion of the ransom, with the developers taking the other half. It shows how cybercrime syndicates have essentially made ransomware a service that affiliates can run with relatively little expertise and have magnified the firepower of the attack. (MOVEit Vulnerability and Data Extortion Incident - NCSC.GOV.UK, n.d.).

2023 MGM Resorts Cyberattack

In late 2023, a Ransomware-as-a-cybercriminal groups are. Taking advantage of a flaw in the MGM framework, the ransom note amount was reportedly in the thousands of dollars. This attack illustrates how easily these affiliates managed to execute and highlights the increasing accessibility of top-tier

cybercriminal operations.(Inside The Ransomware Attack That Shut Down MGM Resorts, n.d.),Costa Rica ransomware attack of 2022

The Conti ransomware group gained notoriety after targeting a slew of critical services, including tax collection and healthcare, within the Costa Rican government. The Conti group is structured on the RaaS model, and this attack illustrated the level of destruction that can be induced by cybercriminal collectives exploiting affiliates. Such a massive attack against a national government highlights the commercialised nature of cybercrime and how affiliates, such as Lapsus\$, can easily and quickly scale the damage. (Conti Costa Rica Ransomware Attack Explained, n.d.)

Why Traditional Cyber Defences Are Too Slow

Cybersecurity systems, which had been adequate in the past, were described as costly but ineffective against the advanced threats of today. They pointed out that traditional methods, such as signature-based detection and manual analysis, were not viable for catching emerging cyber threats.

According to the experts, signature-based detection functioned on previously identified forms of malicious behaviour, but cybercriminals were creating advanced malware capable of evading those systems. Furthermore, because of the supposed signatures, new threats would often slip through the cracks before any damage could even be measured.(MALWARE DETECTION: EVASION TECHNIQUES - CYFIRMA, n.d.)

To add to the problem, the process of incident response and threat detection was manual and therefore slow. Traditionally, Security Operations Centres (SOCs) were operated by human analysts who identified and responded to threats; however, this approach was becoming less effective as threats continued to evolve. Terminology experts emphasised that most of the terminology seen today regarding cyber warfare originated from the 2017 WannaCry ransomware attack, as it was the first time companies were forced to prepare for a rapidly changing situation in real-time. The delayed

patching of vulnerabilities and slow response to the attack led to the widespread propagation of the attack and financial damages.(Lessons Learned Review of the WannaCry Ransomware Cyber Attack, 2018)

Experts said organisations should move towards agile and proactive security capabilities to mitigate these threats. This means moving beyond traditional defences and harnessing technologies like:

- AI & ML for improved threat detection

- Instant threat intelligence for a quick response

- Automated Incident Response for Damage Control

Using these strategies, organisations can mitigate threat vectors to cyberattacks and enhance the protection of sensitive data and operations.

The Emergence of Real-Time Response Tools

SOAR (Security Orchestration, Automation, and Response)

As cybercrime continues to become increasingly professionalised, experts noted that organisations need to automate their defence. The conversation around SOAR (Security Orchestration, Automation, and Response) tools took centre stage as they are utilised to integrate security processes and response actions, making integration seamless and response time quicker. They said that SOAR platforms enable organisations to automate repetitive tasks, like alert triage and containment, to significantly improve response times. Automating early-stage responses allows human analysts to focus on more complex tasks that require specialist knowledge. (SOAR: Security Orchestration, Automation... – Calsoft Blog, n.d.)

The experts also brushed on how SOAR would allow an organisation to build up automation surrounding incident response capabilities, such as:

- Coordinating responses between various security tools as well as teams

- Automating the threat hunt and proactive prevention of making exploitable vulnerabilities

- Creating comprehensive incident reports for regulatory and analytical purposes

Experts have determined that implementing SOAR has the potential to significantly enhance organisations' overall cybersecurity by reducing the risk of breaches and mitigating the impact of security incidents. (What Is SOAR? - Palo Alto Networks, n.d.)

Behavioural Analytics and AI

Behavioural Analytics and AI are integral to modern cybersecurity, where behavioural analytics predict, detect, and remediate threats at both scale and speed, far exceeding traditional capabilities.

The machine learning algorithms are noted to continuously learn from new data, allowing them to adapt and detect the same threat, including zero-day attacks, without the need for any signatures. AI systems operate independently by recognising aberrations in network and user activity ahead of human involvement.

This enables businesses to respond more quickly to threats and prevent breaches from occurring. AI-enabled behavioural analytics can improve incident response, make threat detection more precise, and ultimately enhance an organisation's cybersecurity posture.

Moreover, AI-based behaviour analytics can recognise insider threats, monitor APTs (Advanced Persistent Threats), and track user behaviour to predict threats, thereby helping organisations detect the evolving nature of cyber threats.(AI-Powered Behavioral Analysis in Cybersecurity | CrowdStrike, n.d.)

The Zero Trust Concept and Why It Matters for Real-Time Defence

Behavioural Analytics and AI are integral to modern cybersecurity, where behavioural analytics predict, detect, and remediate threats at both scale and speed, far exceeding traditional capabilities.

The machine learning algorithms are noted to continuously learn from new data, allowing them to adapt and detect the same threat, including zero-day attacks, without the need for any signatures. AI systems operate independently by recognising aberrations in network and user activity ahead of human involvement.

This enables businesses to respond more quickly to threats and prevent breaches from occurring. AI-enabled behavioural analytics can improve incident response, make threat detection more precise, and ultimately enhance an organisation's cybersecurity posture.

Moreover, AI-based behaviour analytics can recognise insider threats, monitor APTs (Advanced Persistent Threats), and track user behaviour to predict threats, thereby helping organisations detect the evolving nature of cyber threats.(AI-Powered Behavioral Analysis in Cybersecurity | CrowdStrike, n.d.) Organisations can quickly contain threats and remediate damage while adapting to new threats with real-time policies. These kinds of proactive defence models are key to countering increasingly sophisticated cybercriminal enterprises. Implementing a Zero Trust model strengthens an organisation's security posture, lowers the likelihood of experiencing a data breach, and enhances incident response capabilities.

In addition, Zero Trust allows organisations to restrict access to sensitive data and monitor user behaviour in real-time to detect threats. A Zero Trust strategy helps the organisation mitigate this concern more efficiently. Using this model, network activity can be easily observed, and action can be taken instantly in response to the threat.(Rose et al., n.d.)



Real-Time Incident Response in Practice

Human and Machine Model: The Hybrid Model

Machines help humans find incidents faster, but real-time incident response is a delicate interwork of machines and human expertise. Automation helps speed up the early detection and containment of incidents. However, humans are essential to analyse sophisticated attacks and make informed decisions.

Threat hunters and Security Operations Centre (SOC) teams are key actors who monitor and respond to real-time alerts, investigating suspicious activity and orchestrating a response. These specialists collaborate with automated technologies, applying intelligence gathered from AI-powered systems to make informed decisions.

Having context and human judgment is key for incident response — even with AI, we still need sound human judgment to make decisions on how to respond to incidents on a day-to-day basis. Organisations can resolve incidents more quickly as machines assist by automating repetitive tasks and analysing data, allowing human experts to focus on high-level decision-making and complex threat analysis.

This provides organisations with the ability to stay one Step ahead of the relentless evolution of cyber threats and offers more powerful protection of their assets.

Real-World Examples

While many organisations have SOAR platforms up and running to help mitigate threats as they emerge, in one case, a bank was able to contain a ransomware attack by using an automated response system that prevented the malware from propagating throughout the bank's network, resulting in only minor losses. Using the real-time capabilities of playbooks allowed the organisation to fend off the threat before it had the opportunity to become a larger problem.

Furthermore, the inclusion of threat intelligence feeds helps organisations to counter new threats in advance. When supplemented with data from international threat intelligence providers, organisations enhance their real-time decision-making ability and speed up their response.

(Ransomware Attacks: Definition, 10 Famous Examples & Tips to Prevent Them, n.d.).

Regulatory Pressure and the Business Imperative for Speed

The Push from Regulations

Due to the rise of cyber threats, regulators have been raising response time demands globally. Several compliance frameworks, such as GDPR, NIST and CCPA, now have a mandatory deadline for organisations to notify authorities and affected end-users about data breaches, usually 72 hours. Not adhering to these regulations can incur hefty fines and tarnish an organisation's image.

They will also need effective incident response systems, doing everything realistically to mitigate threats in real-time. (The Impact of GDPR, CCPA, and Other Data Laws on Cybersecurity Strategies | SecOps® Solution, n.d.)

Cyber Insurance Requirements

As cybercrime has become increasingly prevalent, insurance providers have begun to demand more from their clients to receive coverage. Today, cyber insurers want to see that businesses can respond to incidents in real-time (proof of automated defences and incident response protocols available). To avoid paying higher premiums, insurance providers are prompting enterprises to utilise SOAR platforms and AI-driven threat-detection tools within their businesses. (Cyber Insurance: How It Works & What You Need to Get Covered, n.d.)



Board-Level Concerns

As the financial and reputational impact becomes more severe, C-suite executives are becoming directly involved in cybersecurity readiness. Executive boards are now requiring updates on the organisation's cybersecurity posture, as well as breach detection and response capabilities. Slow or poor responses do not just pose technical risks anymore, but also financial and reputational ones. (Board Oversight of Cyber Risks and Cybersecurity - IMD Business School for Management and Leadership Courses, n.d.)

Future of Commercialised Threats and Real-Time Response

Next-Generation Threats

As cybercrime continues to evolve into a more professional mode of operation, we can expect to see the use of real-time, adaptive AI-driven attacks against countermeasures. However, quantum computing may open new doors of vulnerability, and current encryption standards may not be sufficient. Cybersecurity defences will also require a quantum bastion response to these new threats. (2025 Cyber Security Predictions – The Rise of AI-Driven Attacks, Quantum Threats, and Social Media Exploitation - Check Point Blog, n.d.)

The Changing Nature of Automation

Automation already plays a role in real-time defence, but it will be the first line of defence across industries. Threats are becoming increasingly sophisticated, and automated technology will need to start predicting how to counter a cyberattack before it reaches the stage where human intervention is required. Nevertheless, we still need the human brain to handle complex situations and make high-stakes decisions.

Collaborative Cyber Defence

The future of cybersecurity will be a joint effort between public and private entities. Information Sharing and Analysis Centres (ISACs) are expected to play a central role in real-time information sharing and analysis, enabling organisations to better respond to newly

discovered threats. Global defence will be strengthened by the addition of collaboration at layer one within the blockchain key infrastructure, as well as the automation that can enhance the processing and analysis of data. (Tao et al., 2021)



Conclusion

The future of cyber threats may be the only thing that is certain nowadays — commercialised cyber threats are here to stay, and continue to evolve into increasingly complex forms. It is now essential that organisations have real-time, automated defences in place to mitigate the potential for financially and reputationally damaging breaches. However, the introduction of AI-based defences, SOAR tools, along with the enhancement of the Zero Trust framework —all of these make up the right arsenal to stay ahead against the advancing armies of cybercriminals.

Instead, organisations need to invest in cyber resilience, adopting nimble and automated systems that can respond to threats swiftly. Cybercrime will always find new ways to evolve and develop. While this is happening, businesses must ensure that their cybersecurity strategies are adaptable, swift, and prepared to counter the next wave of threats.

References

- 2025 Cyber Security Predictions – The Rise of AI-Driven Attacks, Quantum Threats, and Social Media Exploitation - Check Point Blog. (n.d.). Retrieved 6 May 2025, from <https://blog.checkpoint.com/security/2025-cyber-security-predictions-the-rise-of-ai-driven-attacks-quantum-threats-and-social-media-exploitation/>
- AI-Powered Behavioural Analysis in Cybersecurity | CrowdStrike. (n.d.). Retrieved 6 May 2025, from <https://www.crowdstrike.com/en-us/cybersecurity-101/artificial-intelligence/ai-powered-behavioral-analysis/>
- Board Oversight of Cyber Risks and Cybersecurity - IMD Business School for management and leadership courses. (n.d.). Retrieved 6 May 2025, from <https://www.imd.org/research-knowledge/corporate-governance/articles/board-oversight-cyber-risks-cybersecurity/>
- Conti Costa Rica Ransomware Attack Explained. (n.d.). Retrieved 6 May 2025, from <https://purplesec.us/breach-report/conti-ransomware-attack/>
- Cyber Insurance: How It Works & What You Need to Get Covered. (n.d.). Retrieved 6 May 2025, from <https://www.bluevoyant.com/knowledge-center/cyber-insurance-how-it-works-what-you-need-to-get-covered>
- Ganguli, P. (n.d.). MA (Criminal Law & Forensic Sc from NALSAR), MA (Sociology from SRU). IJFMR240527724, 6(5). Retrieved 6 May 2025, from www.ijfmr.com
- Inside The Ransomware Attack That Shut Down MGM Resorts. (n.d.). Retrieved 6 May 2025, from <https://www.forbes.com/sites/suzannerowankelleher/2023/09/13/ransomware-attack-mgm-resorts/>
- Lessons learned review of the WannaCry Ransomware Cyber Attack. (2018). www.nationalarchives.gov.uk/doc/open-government-licence/
- MALWARE DETECTION: EVASION TECHNIQUES - CYFIRMA. (n.d.). Retrieved 6 May 2025, from <https://www.cyfirma.com/research/malware-detection-evasion-techniques/>
- MOVEit vulnerability and data extortion incident - NCSC.GOV.UK. (n.d.). Retrieved 6 May 2025, from <https://www.ncsc.gov.uk/information/moveit-vulnerability>
- Ransomware Attacks: Definition, 10 Famous Examples & Tips to Prevent Them. (n.d.). Retrieved 6 May 2025, from <https://secureframe.com/blog/ransomware-attacks>
- Rose, S., Borchert, O., Mitchell, S., & Connelly, S. (n.d.). NIST Special Publication 800-207 Zero Trust Architecture. <https://doi.org/10.6028/NIST.SP.800-207>
- SOAR: Security Orchestration, Automation... – Calsoft Blog. (n.d.). Retrieved 6 May 2025, from <https://www.calsoftinc.com/blogs/soar-security-orchestration-automation-and-response-in-cybersecurity.html>
- Tao, F., Akhtar, M., & Jiayuan, Z. (2021). The future of Artificial Intelligence in Cybersecurity: A Comprehensive Survey. EAI Endorsed Transactions on Creative Technologies, 8(28), 170285. <https://doi.org/10.4108/EAI.7-7-2021.170285>
- The Attack on Colonial Pipeline: What We've Learned & What We've Done Over the Past Two Years | CISA. (n.d.). Retrieved 6 May 2025, from <https://www.cisa.gov/news-events/news/attack-colonial-pipeline-what-weve-learned-what-weve-done-over-past-two-years>
- The Impact of GDPR, CCPA, and Other Data Laws on Cybersecurity Strategies | SecOps® Solution. (n.d.). Retrieved 6 May 2025, from <https://www.secopsolution.com/blog/the-impact-of-gdpr-ccpa-and-other-data-laws-on-cybersecurity-strategies>
- What is Cybercrime and How Can You Prevent It? (n.d.). Retrieved 6 May 2025, from <https://www.techtarget.com/searchsecurity/definition/cybercrime>
- What is Ransomware as a Service (RaaS)? | CrowdStrike. (n.d.). Retrieved 6 May 2025, from <https://www.crowdstrike.com/en-us/cybersecurity-101/ransomware/ransomware-as-a-service-raas/>
- What Is SOAR? - Palo Alto Networks. (n.d.). Retrieved 6 May 2025, from <https://www.paloaltonetworks.com/cyberpedia/what-is-soar>

ABOUT THE AUTHORS

Vinisha Solanki

Integrated M.Sc. in Cyber Security & Forensic Science,
Department of Biochemistry & Forensic Science, Gujarat
University, Ahmedabad, Gujarat, INDIA



Kiran Dodiya

(Research Scholar, Department of Biochemistry
and Forensic Science, Gujarat University,
Ahmedabad, Gujarat, INDIA



Dr. Kapil Kumar

Coordinator, Department of Biochemistry
and Forensic Science, Gujarat University,
Ahmedabad, Gujarat, INDIA



Abstract – Microbiome Analysis

Micro-organism's usage in forensic science is increasing due to its effectiveness in circumstances where traditional approaches fail to provide an opinion.

For decades, DNA and fingerprint analysis have served as the gold standard. But the millions of microbes living on and around us - "the microbiome" - carry a unique signature capable of linking a person to a crime scene, determining the origin of a soil sample, or even estimating time of death.

In recent years, Microbiome has been growing rapidly and eventually has even entered the forensic field. It focuses on understanding the complex communities of microorganisms and their interactions within a specific environment, particularly in relation to human health and other ecosystems.

Thus, Microbial Forensics is the science of analyzing microbial communities for legal purposes, microbes provide insights into individual identity, crime scene geolocation, body fluid origin, degradation timelines, and even sexual events.

The field faces challenges of standardization, databases robustness, and legal admissibility, its unique strengths –

such as detecting low – biomass traces and generating "microbial fingerprints" – position it to significantly enhance forensic techniques.

How and When

Microbiome analysis was first began in late 19th century, and its modern application has significant advancing from 21st century.

Early applications focused on using microbes to determine the cause of death in humans and animals. The field gained significance with the rise of bioterrorism, particularly after the "2001 anthrax attacks", leading to the development and emergence of "microbial forensics" as a discipline to analyze evidence related to bioterrorism, biocrimes, or accidental releases of biological agents.

In forensic science, microbes have gone from obscure curiosities to powerful investigative tools, – from identifying individuals and estimating time of death to geolocation analysis and also in the interpretation of non-pathogen-related crimes.

Every individual, object and environment hosts unique microbial communities that reflect their health, lifestyle, diet and local ecology, they survive on buried items, decomposing bodies that helps in criminal investigations.

Unlike human DNA, microbial DNA is abundant, resilient and diverse, enabling new forensic possibilities when conventional evidence is limited or absent.

The human microbiome - is a unique collection of microbes - that has emerged as a promising forensic tool because each person's microbial community is different, alike to a fingerprint. Researchers can now sequence bacteria left behind in biological stains (like saliva, vaginal fluid, or skin cells) to determine both the bodily origin of the sample and potentially link it to an individual. This approach also extends to non-human traces like : soil carried on a suspect's shoe can be matched to a crime scene location by comparing its microbiome profile. And even, the changing microbial communities on a decomposing body - the necrobiome - can help in estimating the post-mortem interval with increasing accuracy.

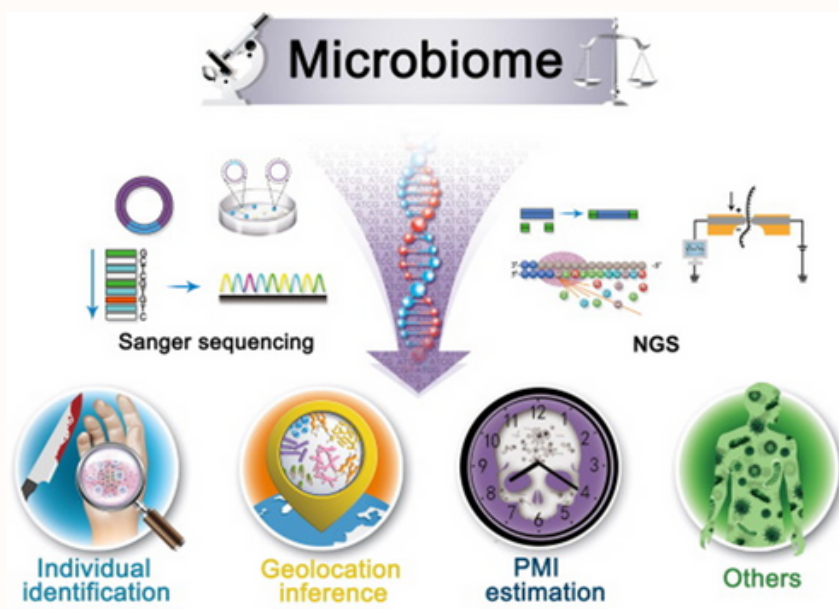


Fig Microbiome

But the forensic reach of microbiomes extends far beyond human-associated environments. Soil transferred on shoes, clothing, and tools carries its own microbial “terrain profile.” Imagine pinpointing where a suspect has been via their soil residues.

When it comes to human remains, the necrobiome—the shifting community of microbes on decomposing bodies—functions like a microbial clock. Succession patterns can estimate post-mortem intervals to within a few days, offering greater precision than any other traditional method.

Microbial communities inhabit diverse environments such as humans, animals, plants, soil, and water, each with unique microbiomes shaped by local conditions and microbial metabolisms like phototrophy and chemotrophy.

Over the decades, forensic microbiology has emerged as a powerful tool, extending from bio-threat attribution to a broad forensic utility that includes identifying individuals, determining postmortem intervals (PMI), inferring geolocation, and even clarifying causes of death.

Today, forensic microbiome studies leverage unique microbial signatures—which reflect individual identity, lifestyle, and environmental exposure—for use in criminal investigations, linking suspects to crime scenes via skin or object microbiomes, estimating time of death through succession patterns in the necrobiome, and inferring geographic origin based on soil and regional microbial profiles (ishinews.com).

Though the field remains in its infancy—with challenges in standardization, environmental variability, model accuracy, and ethical concerns over privacy—ongoing advances in sequencing technologies, bioinformatics, and machine learning are rapidly expanding its potential, positioning microbial evidence to become a well-integrated component of the modern forensic toolkit.

Human skin hosts highly personalized and relatively stable microbial communities that make microbiome analysis a promising avenue for forensic human identification. Individuals shed unique bacterial fingerprints onto objects they touch—like keyboards or phones—and these microbial traces often remain more consistent within a person than across different individuals over time. This opens the possibility of linking suspects to crime scene items using microbial fingerprints—especially useful when traditional human DNA is degraded or absent.

First, technical issues such as contamination during sampling and variability in DNA extraction or sequencing can distort microbial profiles. Biologically, microbiomes change over time, differ across body sites, and respond to environmental factors, medications, and intra-household sharing, all of which complicate interpretation.

Microbial communities—comprising bacteria, fungi, viruses, and protozoa—thrive across all environments, including the human body, soils, and oceans, each forming a distinct microbiome.

Advances in DNA-based molecular techniques—such as PCR, DNA fingerprinting, and whole-genome sequencing—have replaced old, low-resolution culture-based methods. The current revolution is fueled by next-generation sequencing (NGS) and metagenomics, allowing comprehensive profiling of entire microbial communities (amplicon or shotgun sequencing) on complex, even low-biomass, samples.

Imagine a burglary. As the perpetrator handles a doorknob or keyboard, they deposit a microbial fingerprint. Studies have demonstrated that individual-mounted microbial communities on surfaces—like keyboards or phones—can be matched back to their unique owners.

Yet, we must acknowledge the challenges. The microbiome changes over time and varies with personal habits, environment, and lifestyle. A lack of standardized protocols, evolving databases, and legal frameworks means microbiome forensics is not yet court-ready.

So why should we care? Because the microbiome can complement existing forensic tools—especially in cases where human DNA is degraded, mixed, or even identical (as with monozygotic twins). In real cases—such as sexual assault and robbery—microbial evidence has already tipped the scales of justice when combined with DNA.

As sequencing technologies improve and forensic labs adopt standard procedures, the microbiome will emerge not as a replacement, but as a powerful ally to DNA, fingerprints, and classic trace evidence.

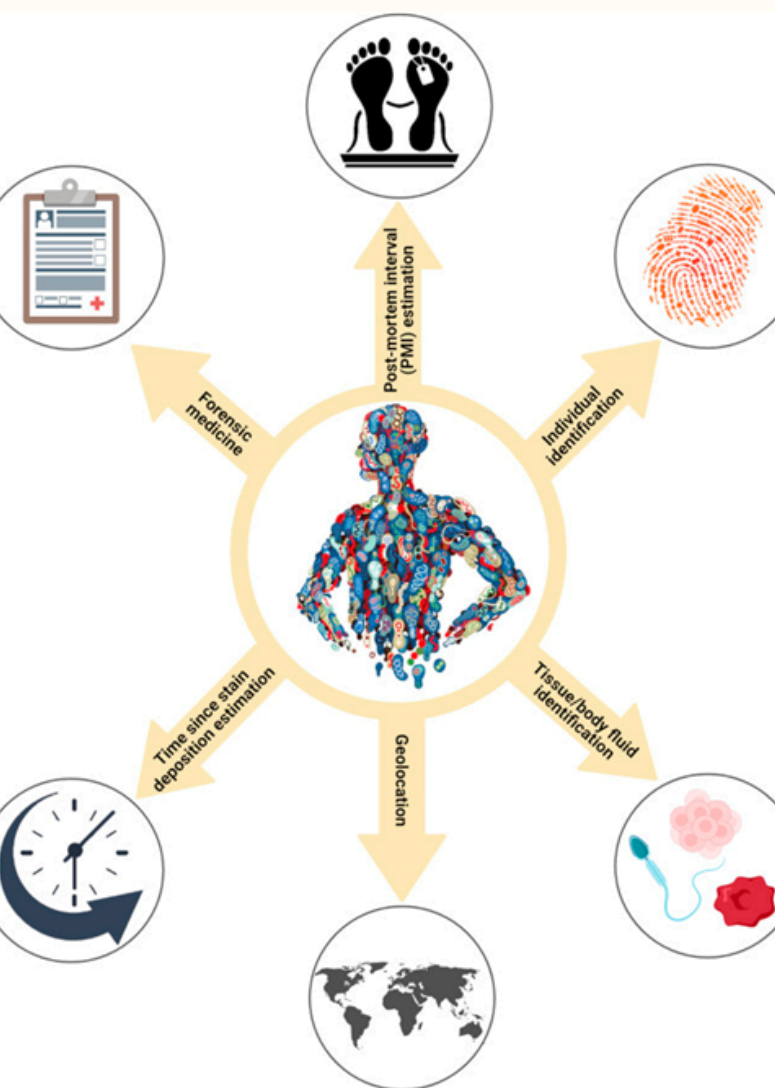
The microbial world may be invisible to the naked eye—but one day, it could hold the key to solving the toughest mysteries.

However, several obstacles currently limit forensic microbiome applications.

Additionally, data-related challenges include lack of standardized protocols, small and non-representative studies, limited biobanks, and immature bioinformatics workflows—factors that hinder reproducibility and courtroom admissibility.

Despite this promise, microbial forensics is still emerging. Many studies lack large, diverse datasets, realistic environmental complexity, and validated statistical robustness. As such, microbial evidence is not yet stand-alone in legal settings; its claims are often described as “complementary” or “adjunctive”.

The future hinges on expanding standardized databases, refining bioinformatics models, and demonstrating microbial evidence’s admissibility and reliability under legal scrutiny.



Conclusion

While it is still in development and facing hurdles such as standardization, database creation, and legal admissibility, microbiome forensics offers a powerful complement to traditional DNA and fingerprint evidence—especially in cases where human DNA is degraded or missing.

In conclusion, while skin microbiome profiling shows clear potential for individualization and linking people to objects in forensic contexts, its practical application remains constrained by issues of stability, sample handling, reproducibility, and sensitivity.

Resolving these challenges—through rigorous validation, standardized procedures, larger reference datasets, and contamination controls—is essential before microbial evidence can gain broader acceptance and legal credibility in forensic investigations.

Microbial communities—once hidden and overlooked—are emerging as sophisticated forensic indicators. From human identification and geolocation to post-mortem analysis and assault investigations, microbiomes promise a powerful new dimension to crime solving. As research matures and real-world validation progresses, microbial forensics is poised to become a mainstream component of the forensic science toolkit.

In closing, the microbiome introduces a new dimension to forensic investigation:

- Who touched what? By matching microbial signatures on objects or stains
- Where did you go? Through soil or environmental microbial profiles
- When did it happen? via microbial succession on corpses or stains

Tripti Bhargava

3rd year student, BSc Forensic Science and
Biotechnology
Kristu Jayanti College





DID YOU KNOW?



Eco-Forensics is the application of forensic science to detect, analyze, and provide legal evidence for environmental violations, including pollution, illegal dumping, wildlife crimes, and ecological degradation.

Mobile Forensics: The Hurdles of Physical Extraction from Today's Smartphones

Author - Jerald Benny

Introduction

The explosive growth of smartphones and has become an indispensable part of modern life, made them a central hub to forensic investigations. These devices are rich with sensitive personal data, including messages, call logs, GPS locations, app data, contacts, medias, browsing history, etc... that can lead or break a case.

Despite their forensic value, extracting this data is not straightforward. Most of the modern smartphones are designed to resist unauthorized access by full-disk encryption (FDE) and increasingly by file-based encryption (FBE), as well as secure enclaves (Apple) and trusted execution environments (TEE - Android).

- Full-disk encryption (FDE): FDE encrypts all data on a disk drive at the hardware level, ensuring that all files are protected and inaccessible without the correct authentication key, even if the device is physically stolen.

- File-based encryption (FBE): FBE encrypts individual files or directories, allowing each file to be protected with a separate key and offering granular control over which data is encrypted, as opposed to encrypting the entire disk. Secure Enclave: Secure Enclave is a dedicated secure subsystem integrated into Apple's system on a chip

(SoC) to securely store and process sensitive data (such as encryption keys, biometric information, etc...) protecting it from unauthorized access and tampering, even if the main system is compromised.

- Trusted Execution Environment (TEE): TEE is a secure section of a processor that runs sensitive code and manages private data in isolation from the main operating system, ensuring confidential tasks remain protected from malware or tampering.

Apple locks down iPhones with strong hardware encryption and Secure Enclave protection, while Android's mixed ecosystem creates challenges each brand handles security differently, and software updates often block forensic access methods.



Data Extraction from Smartphones

Manual Extraction		Physical Extraction	Logical Extraction	File System Extraction	Advanced Extraction Techniques
Manually browsing the device (screenshots, app data exports).		A bit-by-bit copy of the device's storage	Extracts structured data via APIs/backups	Accesses full file system	For hidden or hard-to-access data, experts use JTAG, Chip-Off,
Pros	· Fast & simple (no tools needed).	· Recovers deleted data (if not overwritten)	· Faster than physical extraction · Recovers files &	· Recovers more data than logical extraction (system logs,	· Full data recovery (if not overwritten) · Works on
Cons	· Requires device to be unlocked. · Misses deleted/hidden	· Requires specialized tools and is more time-consuming	· Miss hidden, deleted, or system-level data	· Doesn't always capture deleted or unallocated data	· Highly Invasive · Hardware-specific · Time

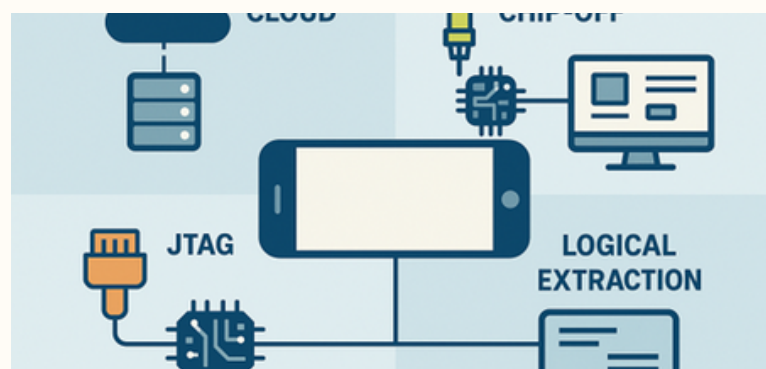
Challenges in Physical Extraction from Smartphones

Physical extraction is considered superior in terms of depth of data retrieved, but it introduces serious challenges due to the rapid evolution of smartphone security. Forensic experts struggle to extract complete data from modern smartphones due to technical barriers, legal restrictions, and ethical concerns.

- 1. Rooting/Jailbreaking Requirement:** Most modern smartphones require root-level access to perform physical extraction. This can lead to data alteration or corruption, impacting admissibility in court.
- 2. Advanced Encryption Mechanisms:** Modern smartphones come with FDE/FBE by default. This makes it nearly impossible to access the data without the passcode/biometric input—even if you physically dump the memory.
- 3. Frequent Software & Firmware Updates:** Manufacturers frequently push security patches that close vulnerabilities used by forensic tools. Tools like Cellebrite UFED or XRY often struggle to keep pace with the update cycles. This limits extraction to only older firmware versions or legacy models, reducing the effectiveness of physical extraction.
- 4. Locked Bootloaders & Secure Boot Chains:** Smartphones enforce bootloader locking, verified boot processes, and anti-rollback protections. Attempting to bypass these protections may result in data wipe or permanent device bricking.
- 5. Tool Limitations and Device Fragmentation:** Many forensic tools struggle with newer chipsets, and some devices like Chinese brands may not support physical extraction.
- 6. Legal and Ethical Concerns:** Legal challenges include forced decryption bans, have ruled that compelling suspects to unlock their devices violates self-incrimination. Strict data protection regulations such as Europe's GDPR impose stringent requirements, like multiple warrants when accessing cloud data stored across international borders, creating jurisdictional hurdles. While bypassing security measures like rooting/jailbreaking can sometimes yield crucial evidence, the process itself can destroy data or violate anti-tampering laws.



Alternative Extraction Methods:



As physical extraction becomes more challenging on modern smartphones, forensic experts are turning to alternative techniques, to obtain court-admissible evidence despite diminishing physical access capabilities.

- 1. File System and Logical Extraction:** When full physical access isn't possible, experts often rely on file system/logical extraction method. This method supported on most unlocked devices or through device backups and extracts all used data except deleted data. But if we use a combined approach, it can yield much more artifacts than each extraction.
- 2. Cloud Extraction:** Cloud based extraction utilises data stored in cloud services linked to smartphones, such as iCloud, Google Drive, or app backups, rather than extracting it directly from the device. This method doesn't require device unlocking or the device itself. However, the challenges are end-to-end encryption, requires access to credentials/tokens and limited to what is backed up or synced.
- 3. JTAG (Joint Test Action Group):** Connects directly to test points on the device's circuit board to extract raw data from the device's memory. It is a hardware-based method, typically requiring the device to be partially disassembled. It's a time-consuming and skill-intensive technique.
- 4. Chip-Off:** Involves removing the memory chip (NAND flash chip) from the device's motherboard and accessing the data using specialized hardware and software. These are invasive and can damage the device. Encrypted memory remains a barrier unless keys are stored on-chip without secure hardware.

Conclusion

As smartphone's security evolving into encrypted fortresses, physical extraction is becoming increasingly impractical. Modern devices are designed with data privacy as a core feature, which inherently conflicts with forensic goals. Investigators must now adapt to alternative approaches like cloud extraction, hybrid logical- file system extraction, and advanced hardware-based techniques to recover leading evidences. While these approaches may not provide the same level of access as physical extraction, they offer viable solutions in an evolving digital landscape. Ultimately, the effectiveness of any data extraction strategy now depends not only on technical skill but also on understanding legal boundaries, respecting user privacy, and adapting to ever-changing technology.



Reference

1. 2016 4th International Conference on Information and Communication Technology (ICoICT) : 25-27 May 2016. IEEE; 2016.
2. Alblooshi A, Aljneibi N, Iqbal F, Ikuesan R, Badra M, Khalid Z. Smartphone Forensics: A Comparative Study of Common Mobile Phone Models. In: 12th International Symposium on Digital Forensics and Security, ISDFS 2024. Institute of Electrical and Electronics Engineers Inc.; 2024.
3. da Costa AM, de Sa AO, Machado RCS. Data Acquisition and extraction on mobile devices-A Review. In: 2022 IEEE International Workshop on Metrology for Industry 40 and IoT, MetroInd 40 and IoT 2022 - Proceedings. Institute of Electrical and Electronics Engineers Inc.; 2022. p. 294-9.

1. Karjagi AJ, Quadri SA. DESIGN OF A FRAMEWORK FOR DATA EXTRACTION AND ANALYSIS FROM ANDROID-EMBEDDED SMARTPHONES 1. Vol. XI, RUSSIAN LAW JOURNAL. 2023.
2. Parhad O, Naik V. Comparative analysis of Data Extraction for Qualcomm based android devices. In: 2023 14th International Conference on Computing Communication and Networking Technologies, ICCCNT 2023. Institute of Electrical and Electronics Engineers Inc.; 2023.
3. Scrivens N, Lin X. Android digital forensics: Data, extraction and analysis. In: ACM International Conference Proceeding Series. Association for Computing Machinery; 2017.
4. Saputra H, Zeno Alkindi T, Priyanto H, Dwisetiyono A, Zulfikar sidik P. PEMERIKSAAN MOBILE FORENSIK TERHADAP HANDPHONE SECARA PHYSICAL EXTRACTION DENGAN PERBEDAAN JENIS SOFTWARE. Journal of Forensic Expert. 2021 Oct 22;1(3):56-65.
5. Tajuddin TB, Manaf AA. Forensic Investigation and Analysis on Digital Evidence Discovery through Physical Acquisition on Smartphone.
6. Tsai YC, Yang CH. Physical forensic acquisition and pattern unlock on android smart phones. In: Lecture Notes in Electrical Engineering. 2013. p. 871-81.

ABOUT THE AUTHORS



Jerald Benny

M.Sc. Forensic Science, Cochin University of
Science And Technology, Kerala

Silent Witnesses: Arthropods as Key Evidence in Criminal Cases

Author - Kuldipsinh Mori, Dr. Gaurang M Sindhav

Introduction

Crime scenes have a new kind of witness, one that's small, six-legged, and often arrives buzzing. Insects and other arthropods are "silent witnesses" to death, feeding and breeding on remains in ways that can reveal critical clues. It may sound like the plot of a thriller, but forensic entomology, the use of bugs in criminal investigations, is very real. As forensic entomologist Dr. Bernard Greenberg once quipped, "Who would ever think that a maggot could be a witness?" Yet time and again, insects have helped crack cases, pin down timelines, expose lies, and even clear the innocent. In this article, we'll explore several gripping real-life cases from a 1930s murder solved by maggots to modern mysteries unravelled by flies, beetles, caddisflies, and mites, and explain how these tiny creatures provide big answers.

The First Insect Detectives: The 1935 Ruxton "Jigsaw" Murders

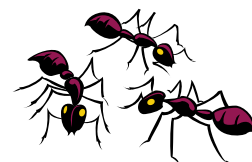


On a chilly day in 1935, in Scotland's Dumfriesshire countryside, police made a ghastly discovery: dismembered human remains wrapped in newspaper, strewn in a ravine. Investigators faced the grim task of identifying the two bodies and determining when they had been killed.

The prime suspect was Dr Buck Ruxton, a physician whose wife, Isabella, and housemaid had recently vanished under suspicious circumstances. But to prove his guilt, detectives needed to determine the time of the murders. Enter the blowfly maggots collected from the remains.

Forensic experts realized that the large number of bluebottle fly larvae (a type of blowfly) on the corpses held the key. By examining the maggots' stage of development, entomologist Alexander Mearns estimated the victims had been dead for about 12 to 14 days. This estimate lined up with the timeframe in which Ruxton's wife and maid went missing, implicating him. This case became the first-time insect evidence was used in a murder trial in Britain; the maggots' age helped establish the time of death and ultimately helped convict Dr Ruxton of the double murder. He was executed for his crimes, and the case, dubbed the "Jigsaw Murders" due to the piecing together of body parts, went down in history.

The Ruxton case demonstrated a powerful principle of forensic entomology: insect development follows a clockwork sequence. Blowflies are usually the first to colonize a corpse, often arriving within minutes of death. They lay eggs that hatch into wriggling maggots, which pass through several growth stages (instars) before pupating and eventually emerging as adult flies. By knowing a blowfly's life cycle and factoring in the ambient temperature (warmer weather speeds up insect growth), an entomologist can work backward to estimate when the eggs were laid and thus when the victim died. In this case, the blowfly larvae on Ruxton's victims were effectively a biological timestamp, one that exposed the doctor's lies. As one expert noted, "Certain flies come early, but as the remains dry out, they are replaced by other flies and beetles. All of these can give us a rough postmortem interval." In other words, the bugs arrive in waves in a predictable insect succession, and reading this silent insect timeline can yield an estimate of the minimum time since death.



Breaking the Alibi: A Fly in the Ointment (Punjab, 2015)

Eighty years later and thousands of miles away, insects were again key witnesses, this time in a modern murder mystery in Punjab, India. In 2015, police recovered the body of a 45-year-old man from a residential house in Punjab. The corpse was already in an advanced stage of decomposition, crawling with insect larvae. Investigators identified the larvae and pupae as belonging to the blowfly *Chrysomya megacephala*, commonly known as the Oriental latrine fly, a species well known to colonize bodies soon after death. The prime suspect in the case had given an alibi claiming that the victim was alive much later than when he was found, essentially suggesting the death was recent. But the bugs told a different story.

Forensic entomologists analyzed the insect evidence and estimated the post-mortem interval (PMI) -the minimum time since death to be around 9-10 days based on the development stage of the fly larvae. In simpler terms, the flies on the body had been there feeding and growing for over a week. This was far longer than the suspect's account of events allowed. The presence of mature fly pupae refuted the suspect's alibi outright, indicating the victim likely died days before the suspect claimed to have last seen him. Faced with this timeline derived from insect biology, the suspect's story fell apart. The tiny pupae had quietly recorded the true time of death, helping investigators reconstruct the crime. Thanks to these findings, authorities were able to press charges with a solid scientific foundation; the flies had essentially testified to the timing of the murder.

This case highlights how species-specific behaviour and growth rates can make or break an alibi. *C. megacephala* is notorious for being one of the first flies to arrive on a corpse in warm climates. If its larvae have progressed to later instars or into pupae, a significant amount of time has passed since oviposition (egg-laying). A suspect might lie about when a victim died, but they can't speed up or slow down a fly's life cycle. As one review noted, the reliability of insect-based PMI estimates is often vital to validate witness statements and suspect alibis. In Punjab, the Oriental latrine flies' development timeline provided a biological clock that spoke louder than the suspect's words.

Drowning in Clues: Caddisflies and a Mysterious Canal Death



Not all bodies are found on land, and not all insect evidence comes from flies. In an intriguing drowning case, aquatic insects stepped into the spotlight. Imagine investigators pulling a body out of a canal and suspecting that it might not be the original dump site. How could they tell? One answer lies with caddisfly larvae, those ingenious underwater architects that build tubular cases out of sand, pebbles, and plant bits. These larvae live in water, and if they attach themselves to something (like a submerged body), they can reveal how long that object has been in their aquatic environment and even whether it's been moved.

In one case from Michigan, portions of a dismembered male body were discovered in a stream, some in submerged bags. Along with a few fly larvae, forensic entomologists collected caddisfly larvae stuck to the remains. Caddisflies (order Trichoptera) spend most of their lives as larvae in water, building cocoon-like cases around themselves. By analyzing the type and size of the caddisfly cases on the remains, scientists could estimate how long those body parts had been underwater during the postmortem submersion interval (PMSI). In this Michigan case, the unique case-building behaviour of certain caddisfly species provided a timeframe consistent with when the victim was reported. In other words, the aquatic insects helped confirm that the body had been in the stream since around the time of the man's disappearance.

Even more fascinating, insects can indicate if a body was relocated from one site to another. For instance, if a supposed drowning victim's corpse carries insect species that aren't native to the lake or river where the body was found, it's a red flag that the body was moved after death. In a hypothetical scenario, let's say a body is found in a canal but is covered in caddisfly larvae that only live in clean, fast-flowing streams, investigators would suspect the victim died or drifted in a stream and was later dumped in the canal. In the real case above, the presence of those caddisfly larvae was consistent with the body having remained in that particular stream environment, helping detectives piece together the sequence of events. It's a reminder that whether on land or underwater, nature's little creatures can serve as covert crime scene recorders. As forensic entomologists emphasize, aquatic insects shouldn't be ignored; they can yield "valuable details in estimating a PMSI" and help solve watery mysteries.

Toxic Secrets: Beetles, Maggots, and the Overdose Mystery

Sometimes the insects not only tell when someone died, but also how. In cases of suspected drug overdose or poisoning, a subfield of forensic entomology called entomotoxicology comes into play. This involves analyzing the tissues or gut contents of insects that feed on a corpse to detect drugs or toxins. It sounds like science fiction, but it has proven crucial in real investigations, especially when a body is too decomposed for standard toxicology (no blood or urine can be collected). One dramatic example involved an apparent overdose where only insects could provide the toxicological evidence.

Consider a scenario where a body is found long after death, reduced to skin, cartilage, and bones. Traditional toxicology tests are impossible because the internal organs and fluids have decayed. However, the corpse is teeming with insect blowfly maggots and dermestid beetle larvae (the kind of beetles that munch on dry, decaying flesh and hide). In a landmark 1980 case, exactly this situation occurred: a young woman's remains were so decomposed that investigators had no tissues to test. Instead, they collected the larvae that had been feeding on her and tested them. Remarkably, the maggots contained a significant amount of a barbiturate drug (phenobarbital), revealing that the woman had died from a drug overdose. This was one of the first documented uses of insects as a toxicology lab, proving the concept of entomotoxicology.

Fast forward to more recent times, and forensic scientists have applied the same approach to cases involving modern drugs like opioids. Oxycodone, for example, is a powerful opioid painkiller that unfortunately features in many overdose cases. In one case, a man's body was found in a desiccated state with only beetles and late-stage fly pupae remaining. Toxicologists examined *Dermestes* beetle larvae from the body and were able to detect oxycodone in their tissues, even though the victim's tissues had disintegrated. In essence, the insects had bioaccumulated the drug from feeding on the corpse. By identifying the chemical traces in the bugs, investigators confirmed that the victim had lethal levels of oxycodone in his system before death. This finding helped distinguish an accidental overdose from foul play, steering the investigation in the right direction.

Entomotoxicology cases underscore an important point: insects are not just timers, but samplers. As they ingest human tissue, they also ingest any chemicals present in that tissue, from narcotics and poisons to heavy metals. Later, in the lab, experts can grind up or analyze the bugs to detect those substances. Studies have shown that many common drugs (morphine, heroin, cocaine, etc.) remain detectable in insect larvae and do not necessarily disrupt the insects' development. That means a fly or beetle can carry on growing (maybe a bit slower or faster in some cases) while preserving a chemical record of what killed the person it's feasting on. It's a macabre yet ingenious way to get a toxicology report from nature's undertakers. Thanks to these techniques, even a skeleton with a few insect inhabitants can yield a cause of death, turning bugs into key witnesses for cases that would otherwise be unsolvable.



Mite-Sized Evidence: Tiny Accomplices in a German Cold Case

Insects aren't the only arthropods that lend a six-legged (or eight-legged) hand to forensic science. Mites, those microscopic relatives of spiders, have recently proven their worth in investigations, in what's sometimes called forensic acarology. One particularly extraordinary case in Germany combined a high-stakes heist with high-powered microscope work, showing just how far an arthropod's testimony can go. The case began with a bank robbery in Germany in 2016, where criminals made off with at least 500,000 euros in cash. The trail went cold until investigators got an unusual tip from scientists: examine the mites. Yes, mites, it turned out some of the recovered banknotes had tiny soil-dwelling mites clinging to them. These mites were collected and analyzed by acarologists (mite experts), including Dr. Alejandra Perotti's team at the University of Reading. What they discovered was astonishing. The mites on the money were identified as species that originated in Australasia (the South Pacific region), not native to Europe. This meant the stolen cash had likely been buried or stashed in a specific part of the world far from Germany. Indeed, following this lead, investigators traced the loot to a buried location in Thailand, where the culprits had hidden it. Tiny mites stuck to the money and gave away the burial site, cracking the international case wide open.

This German case was a watershed moment, the first known instance of using soil micro-mites as trace evidence to locate stolen goods. It demonstrated that even the smallest creatures can carry geographic signatures. . "We could be using these microscopic animals to recover cash, drugs, or even corpses," Dr. Perotti noted, emphasizing how "tiny beasts can be mighty players in crime scene investigations." Perotti had previously helped investigate a Swiss homicide by examining mites on the victim, proving that mites can also link a body or person to a particular environment. Because mites (like insects) have preferred habitats and limited ranges, the species present can act like GPS coordinates. For forensic investigators, it's an exciting new tool: if a victim or object is found with an unusual community of mites (or, say, pollen or algae other tiny evidence), these clues can point to a specific location or indicate a journey.

. The use of mites is still an emerging technique, but it highlights a broader trend that forensic science is leaving no stone (or bug) unturned. From the largest blowflies to the tiniest acarids, every organism at a crime scene is potentially a piece of evidence. The German mite case, in particular, reads like detective fiction: a half-million in buried cash, a microscopic analysis, and a solved crime thanks to creatures smaller than a pinhead. It's yet another reminder that the absence of a human witness doesn't mean a crime goes unwitnessed – nature is watching, and now we know how to listen.

When Insects Speak for the Innocent

So far, we've seen how arthropods help catch killers and thieves. But they can also prevent justice from miscarrying. One of the most poignant forensic entomology cases in recent memory involved not convicting a criminal, but exonerating an innocent person by noticing what wasn't there on a body.

In the summer of 2001, a homeless man was brutally murdered in Las Vegas. A young woman named Kirstin Blaise Lobato was wrongfully convicted of the crime, largely due to a chain of circumstantial evidence and inconsistent pathology testimony about the time of death. Lobato insisted she was innocent and had been 170 miles away at the time of the murder. It wasn't until years later, when her case was taken up by advocates, that forensic entomologists were asked to review the crime scene photos. They immediately spotted a glaring clue: the victim's body found outdoors on a hot July night had no maggot activity, no fly eggs, nothing. This was highly unusual because, in the Las Vegas summer, blowflies would be expected to find a fresh corpse almost immediately and lay eggs in the open wounds. A bloody body with exposed injuries, lying outside in warm weather, is like a neon sign for flies. Yet photos showed zero insect evidence on the victim.

The experts knew what that likely meant: the victim must have died after sunset. Blowflies are largely daytime creatures; they do not normally fly or lay eggs at night. If the murder had happened in broad daylight or even at dusk, there should have been at least fly eggs (which look like tiny grains of rice) in the wounds.

The absence of those eggs was telling. In 2009, forensic entomologist Dr. Gail Anderson provided an affidavit concluding the death occurred after nightfall on the night of July 8, 2001. That timing aligned perfectly with Lobato's rock-solid alibi (she was elsewhere that entire night). Eventually, in 2017, multiple entomologists testified to the effect that insects would have swarmed the body if the killing had happened earlier, and the lack of eggs strongly indicated a post-sunset death. This evidence was pivotal. The court ruled that Lobato's original defence had been deficient for not introducing entomology, and her conviction was vacated. After 17 years of maintaining her innocence, Kirstin Lobato walked free, exonerated with help from the very flies that didn't show up at the crime scene.

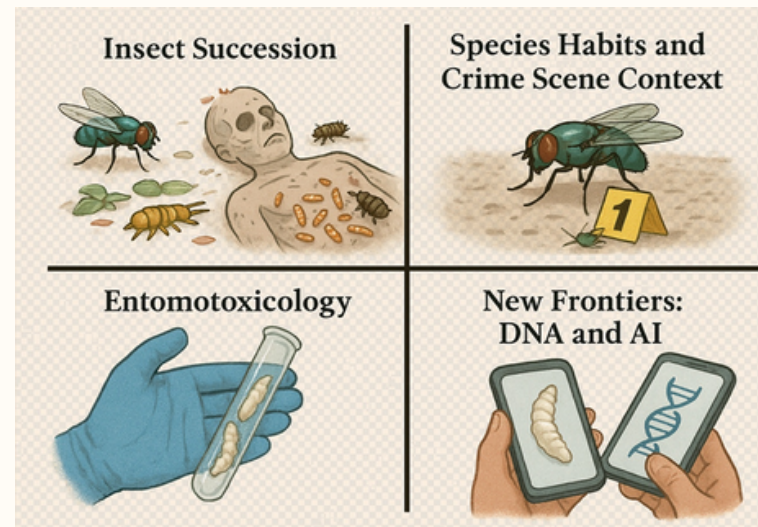
This extraordinary case teaches a valuable lesson: sometimes the silence of the bugs is as meaningful as their presence. It also shows the maturity of forensic entomology as a science; not only can it assist in determining timelines, but it can stand up in court to correct an injustice. Insects, in essence, spoke up for someone who had been silenced by a wrongful conviction. As Dr. Anderson said, insects are the "first witnesses" to a crime, and in this instance, their testimony (or lack thereof) proved more consistent than flawed human testimony. For a general public often repulsed by maggots and creepy-crawlies, it's almost poetic: those squirmy larvae can serve the cause of justice and even save a life by preventing an innocent person from languishing in prison.

How Do Insects Crack the Case? (Forensic Entomology 101)

By now, you've seen the incredible variety of ways arthropods aid criminal investigations. Let's briefly break down how this all works in plain language.

Insect Succession: When a human (or animal) dies and begins to decompose, it sets off an ecological chain reaction. Different groups of insects colonize the body in a predictable sequence. First on the scene are usually blowflies and flesh flies, drawn by the smell of fresh death some can arrive within 15 minutes of death. They lay eggs in moist openings (mouth, nose, wounds), and within hours, those eggs hatch into larvae (maggots) that start feeding. After a couple of days, as the body enters the bloated stage of decomposition, more waves of flies arrive (other blowfly species, house flies), and beetles might show up to feed

up to feed on the maggots or the drying flesh. As the corpse dries out further (active decay to advanced decay), beetles like dermestids take over, chewing on skin, ligaments, and hair, while late-arriving flies (like cheese skippers) might infest any remaining moist pockets. Finally, in the dry stage, almost only skin and bones remain, and you'll find beetle larvae and mites scavenging on the last bits of organic matter. This orderly progression is called insect succession. Investigators know roughly who arrives when, so the mix of insects on a body can tell them if it's been 2 days, 2 weeks, or 2 months since death (give or take). It's like a biological clock that starts ticking the moment life stops. By collecting specimens from a body and identifying their species and growth stage, a forensic entomologist can estimate the postmortem interval. It might be as straightforward as "these maggots are three days old, so the person has been dead at least three days," or as complex as modelling temperature data to fine-tune a developmental timeline. Either way, it transforms squirmy bugs into timekeepers of death.



Species Habits and Crime Scene Context: Bugs are picky about their habits. Some only live in certain climates or environments, which is why finding a species out of place can raise an investigator's eyebrow. For example, if tropical blowflies (like *Chrysomya megacephala*) are found on a body in a cool temperate region where they're not usually found, it could mean the body was moved from elsewhere or kept in an environment that allowed those flies to thrive. (In one recent study, a normally southern U.S. blowfly was found in Indiana, likely due to a warming climate, which could "confuse matters" in local death investigations until entomologists adjust their expectations. Similarly, certain beetles only arrive once a body is fairly dry;

if those are present, you know the significant time has passed or conditions were unusual. As we saw with aquatic insects and mites, the presence of a certain species can link a body to a location (water, specific soil, etc.). In short, knowing who the bug is and how that bug lives is just as important as measuring its growth. Forensic entomologists spend years studying insect life cycles, behaviour, and geographic distribution so they can interpret what a fly on a corpse is “saying.” It’s a bit like reading a secret language, one where each species is a word and the whole community on a body forms a sentence about the crime.

Entomotoxicology: This tongue-twister term combines entomo (insect) and toxicology (study of poisons). It refers to analyzing insects from a corpse to detect drugs or toxins. Why would we do that? As mentioned, if a body is too decomposed, normal toxicology samples may be gone. However, the insects feeding on the body effectively become living samples of the corpse’s chemistry. They can accumulate drugs in their tissues. For instance, larvae that feed on a heroin user’s body may test positive for heroin metabolites; beetles munching on a poisoned corpse may contain traces of the poison. Entomotoxicology can reveal whether a victim was intoxicated, overdosed, or poisoned before. It’s not always straightforward; different substances can affect insect growth (some drugs speed up maggot development, others slow it down). But with careful experiments and comparisons, scientists can both detect the substance and account for any effect on the PMI estimate. This field adds a cause of death dimension to insect evidence. It’s not used in every case, but in a tough one where only bones and bugs remain, it can be a game-changer. Cases have shown the detection of everything from barbiturates to cocaine in insect samples. Now, with advanced techniques like GC-MS (gas chromatography-mass spectrometry) and other chemical analyses, even infinitesimal amounts of a drug in a handful of maggots can be identified.

New Frontiers DNA and AI: Forensic entomology is continually evolving. Two emerging tools are worth a mention: DNA barcoding and artificial intelligence (AI). DNA barcoding involves sequencing a short genetic marker from an organism to identify its species. This is hugely helpful when insect specimens are in pieces, or only eggs or pupae are present that are hard to identify visually. Using DNA barcoding, even an unrecognizable blob of maggot can be matched to its species with high accuracy. This ensures accuracy in cases where multiple similar-looking flies might be involved.

. It’s also speeding up the identification process, which used to require raising eggs to adults in the lab (which takes days), and can sometimes be determined in hours with DNA techniques. On the AI side, researchers are training computer vision models to classify insect images and even estimate PMI based on insect evidence. Imagine a detective snapping a photo of maggots at a scene and an app instantly suggesting the species and age. That’s not far-fetched. One recent study developed a deep learning system that could identify forensically important flies with over 99% accuracy. Another line of AI research is using machine learning on weather and insect data to improve PMI estimates. These technologies, alongside developments like electronic noses (sensors that detect decomposition odours which attract insects), are propelling forensic entomology into the future. But even as high-tech methods arrive, the core of the field remains a keen understanding of humble insects and their life stories.

Conclusion: Tiny Creatures, Big Impact

From the bleak ravine in 1930s Scotland to the canals, fields, and living rooms of modern crime scenes, arthropods have proven to be indispensable allies in forensic investigations. They are the silent witnesses that accompany every step of decomposition, diligently doing their natural jobs while inadvertently recording crucial information about a crime. Their life cycles and behaviours, once viewed with disgust or indifference, are now recognized as vital evidence. As we’ve seen, blowflies can pinpoint the time of death, beetles and larvae can reveal the presence of drugs or toxins, aquatic insects can indicate a drowning timeline or body relocation, and even microscopic mites can connect evidence to far-flung locations. These tiny detectives have helped convict murderers, bust alibis, locate hidden graves, solve mysteries of unknown causes of death, and correct injustices in the legal system.

The importance of arthropods in modern forensic investigations cannot be overstated. They extend the reach of law enforcement into aspects of a case that would otherwise remain dark. When traditional evidence has decayed with a body, insects keep speaking. What’s more, as technology advances,

, we are getting even better at listening to them, whether through DNA barcoding that ensures accurate IDs or AI tools that could make analyzing insect evidence faster and more. The partnership between entomologists and detectives is likely to grow stronger, with labs around the world researching local insect fauna and building databases of their development under various conditions.

In a broader sense, these stories also remind us of the interconnectedness of life and death. The moment life ends, nature's recycling crew arrives, and in their actions is written a story of time, place, manner of death, and sometimes even of the life that came before. Forensic entomology is the art of decoding that story. It requires patience (sometimes waiting for eggs to hatch), attention to detail (distinguishing one maggot species from another under a microscope), and deep respect for scientific rigour (accounting for temperature, habitat, and drug effects). When done right, it can provide courtroom evidence as solid as DNA or fingerprints. Juries have been swayed by the straightforward logic of a fly's lifecycle and the cold, hard data of degree-hours accumulated by insect growth.

As we close the case file on these examples, one thing is clear: arthropods often see what we can't. They arrive at crime scenes long before investigators, and they start recording clues immediately in their way. The term "silent witnesses" is apt; they say nothing in words, but their presence, absence, growth, and species composition speak volumes to those trained to interpret them. In the pursuit of justice, even the lowly maggot becomes a star witness, and a swarm of flies can shut down a murderer's lies. Next time you hear a fly buzzing, remember: that little insect might just be carrying secrets of life and death on its wings. And thanks to forensic entomology, humanity has found a way to make the silent witnesses finally heard.



References

- Anderson, G., et al. (2018, December 13). Blow flies helped exonerate a woman of murder 17 years after the fact. *Popular Science/The Conversation*.
- Greenberg, B. (as quoted in Kennedy, J. M.). (1991, August 1). Maggots solve murders: Entomologists help police to bug criminals. *Los Angeles Times*. <https://www.latimes.com/archives/la-xpm-1991-08-01-me-74-story.html>
- Picard, C. (2013). Forensic fly moves north. *National Geographic*.
- Historic UK. (7th August 2023). The birth of forensics: Dr Buck Ruxton. <https://www.historic-uk.com/HistoryUK/HistoryofBritain/Dr-Buck-Ruxton/>
- Sharma, A., & Bala, M. (2016). Case study and PMI estimation of male corpse from Ludhiana, Punjab, India: An implication of ADH method. *Journal of Forensic Sciences & Criminal Investigation*.
- Wallace, J. R., Merritt, R. W., & Kimbirauskas, R. K. (2008). Caddisflies assist with homicide case: Determining a postmortem submersion interval using aquatic insects. *Journal of Forensic Sciences*, 53(1), 219-221.
- Simon Fraser University Museum of Archaeology & Ethnology. (n.d.). Forensic entomology exhibit notes.
- Jain, S., Bala, M., Sharma, A., & Singh, S. (2025). Exploring the impact of xenobiotic drugs on forensic entomology for accurate post-mortem interval estimation. *Frontiers in Insect Science*. <https://www.frontiersin.org/articles/10.3389/finsc.2025.123456/full>
- Perotti, A. (2016). Of mites and men. *The University of Reading Stories*. <https://www.reading.ac.uk/stories/articles/international/forensic-entomology-mites-men>
- Gohe, A. K., Bhushan, M., & Roy, S. (2024). Classifying forensically important flies using deep learning to support pathologists and rescue teams during forensic investigations. *PLOS ONE*, 19(2), e0284652.
- Singh, S., Sharma, A., & Bala, M. (n.d.). Case study and PMI estimation of a male corpse from Ludhiana, Punjab, India: An implication of the ADH method. *ResearchGate/Conference Paper*.
- Sharma, R., & Gupta, D. (2018). DNA barcoding in forensic entomology - Establishing a DNA-based identification system for insect evidence. *International Journal of Forensic Sciences*, 3(2), 55-62.

ABOUT THE AUTHORS

Kuldipsinh Mori

Research Scholar, Department of Zoology,
BMT, HG, and WBC, University School of
Sciences, Gujarat University



Dr. Gaurang M Sindhav

Assistant Professor, Department of Zoology, BMT, HG &
WBC, University School of Sciences, Gujarat University



The Role of Acoustic and Linguistic Features in Forensic Voice Identification

Author - Ms. Janki Kacha, Mr. Bhumit Chavda

Overview

Forensic voice identification is a useful tool that is required in criminal investigations and proceedings. One of the types of such challenge is a forensic voice recognition system: it is based on how one talks and the words on the mouth of the speaker. The paper is going to offer a concise background of forensic voice identification or verification, depending on the acoustic and linguistic characteristics of a speaker (Jessen, 2008).

The acoustic characteristics involve the objective physical parameters of the voice sound, specifically the fundamental frequency (pitch), formants (the shapers of vowel quality), intensity (loudness), and speaking rate, as well as the minor details like jitter and shimmer; they can be examined in objectivity with the aid of specific computer programs. Along with this, we have the linguistic characteristics which include individualized language usage, including a person speaking with particular pronunciations, dialectal features, use of words, phrase structures, idiosyncratic speech tendencies (such as fillers or pauses), and the general use of prosody such as intonation, pitch, and rhythm. Taking into consideration all these features together, the forensic voice experts will be able to synthesize a powerful vocal profile, which can be used to assign to the strong evidence during an investigation and a court trial (Schilling et.al, 2015).

Voice identification could be possible using qualitative and quantitative analysis of the acoustic values such as frequencies, pitch, energy, and intonation of the speaker, as compared in this study. The acoustic parameters that will be used to conclude the results of this study are fundamental frequency, intensity, formant frequency, and voice spectrogram (Jessen, 2002).

Introduction

Forensic science is simply the word that originated in the Latin word that is Forensis, meaning allied to the court of justice or something belonging to the courts and things of the people in matters of justice. Definition of Forensic Science in straightforward words is simply this: it is the application of the science and principles of science to the solution of legal questions and problems of law (Nolan et.al, 2007).



Fig Voice, Speech, and Sound are the bases of Voice theory

Voice- A voice is the sound produced by the vocal organs or vocal cords of a given person, in other words larynx or vocal cords. The voice of an individual is individual, private, and inimitable as a whole because every orator has his/her style of speech and, among other things, uses a specific accent, rhythm, intonation, style, pronunciation scheme, and vocabulary. Besides, the vocal cords, throat, and mouth structures are different (Schilling et.al, 2015).

Speech- Speech is the oral part of communication that is achieved by human beings. Speech communication is a flow of events that allows the speaker to share their feelings and emotions, and the listener to understand them (Kreiman et.al, 2014).

Nature of voice production theory:

Sound is a vibration that is induced by the disturbance of air. Tense organs are active composite parts of the human body that directly or indirectly participate in the process of producing speech, which is referred to as the organ of speech. Lungs, chest, muscles, trachea, larynx, pharynx, lips, teeth, tongue, roof of mouth, and vocal fold/cord are the major organs that assist speech articulation. The combination of the organs is referred to as the vocal tract (Tosi et.al, 2019).

Behavioral Anomaly Detection: Machine learning algorithms are also becoming commonly used to detect strange patterns of player behavior that would indicate non-standard gameplay and hence indicate possible botting, automation cheating, or account takeover. This is done through the analysis of data points of thousands of players per period (Liao et al., 2011).

Timeline Reconstruction: This tedious procedure of gathering all the available artifacts concerning the case and organizing them according to the timeline is important in determining the order of events, motive, and finally, the chain of evidence of a crime.

Cloud Forensics: With an increased number of game infrastructures shifting to cloud services (e.g. AWS, Azure, Google Cloud), forensic practitioners need to adjust to gathering and analysing data in the cloud, and more likely they will require custom integration with the API and protocols of a particular provider.

Challenges and Future Directions

Despite significant advancements, digital forensics in online multiplayer environments faces ongoing challenges. The rapid pace of game development and the agile nature of cybercriminals mean that forensic methodologies must continuously evolve. Ethical considerations surrounding player privacy, data retention policies, and the scope of data access remain critical points of contention. The inherent lack of standardized logging or data formats across game developers creates persistent hurdles for law enforcement agencies seeking streamlined investigative processes.

However, the future of digital forensics in this domain is promising, driven by technological innovations and increasing recognition of the problem:

AI and Machine Learning (AI/ML): AI/ML will play an increasingly vital role in automated anomaly detection, predictive analytics to identify emerging threats, and intelligent analysis of massive datasets to pinpoint suspicious activities and potential perpetrators (Conti et al., 2019). AI can help identify complex bot behaviours or detect subtle cheating patterns that human analysts might miss.

Blockchain Technology: The integration of blockchain into virtual economies (e.g., for NFTs, immutable transaction logs) holds potential to enhance transparency and traceability of virtual assets, making it more challenging for criminals to launder funds or obscure illicit transactions (Carcillo, 2021).

Enhanced Collaboration: Greater collaboration between game developers, law enforcement agencies, and forensic experts is crucial. This includes establishing standardized communication protocols for evidence requests, developing common APIs for forensic data access, and fostering intelligence sharing on emerging threats.

Legal Frameworks and Specialization: Developing robust international legal frameworks to address the cross-border nature of game-based cybercrimes is essential for effective prosecution. Furthermore, the demand for forensic professionals with specialized expertise in gaming ecosystems, understanding game design, specific network protocols, and cheat methodologies, will continue to grow.

Concluding Insights:

The immersive and economically significant world of online multiplayer gaming has, regrettably, become a new digital frontier for cybercriminal activity. From sophisticated financial fraud to intricate in-game cheating and even the facilitation of more serious cyber-enabled offenses, the threats are diverse and constantly evolving. In this dynamic landscape, digital forensics stands as an indispensable discipline, adapting its core principles to confront the unique challenges posed by distributed, volatile, and proprietary game-related data.

While the complexities of multi-jurisdictional investigations and the sheer volume of data remain formidable obstacles, ongoing advancements in AI/ML, the potential integration of blockchain technologies, and a growing emphasis on inter-agency collaboration offer promising pathways forward. By continually refining our forensic methodologies and fostering specialized expertise, we can equip law enforcement and game developers with the tools necessary to combat game-based cybercrimes effectively, ultimately working towards a safer and fairer virtual environment for players worldwide.

References

- Austin, C. C. (2020). *The New Criminal Playground: How Online Gaming Has Become a Hub for Cybercrime*. Palgrave Macmillan.
- Carcillo, A. (2021). *Blockchain in Video Games: A Forensic Perspective*. Elsevier.

The system involved in speech production:

1. Respiratory system
2. Phonatory system
3. Articulatory system

In modern-day forensics, voice evidence plays a critical part, especially in cases of fraud, terror attacks, ransom, threatening, and anonymous calls. Forensic voice identification involves comparing the already known voice of a suspect with an investigative tape in a bid to determine the likelihood of identity (Paya et.al, 2021).

The two fundamentals in the scientific rationale are language and the audio field, although there is automation tools made available by technology. These features help to distinguish between speakers and being able to know the authenticity of audio recordings. The likelihood of the forensic expert to make scientifically based judgments relies on the way the expert is able to interpret these attributes (Tosi et.al, 2019).

Forensic Voice Identification Using Acoustic Features:

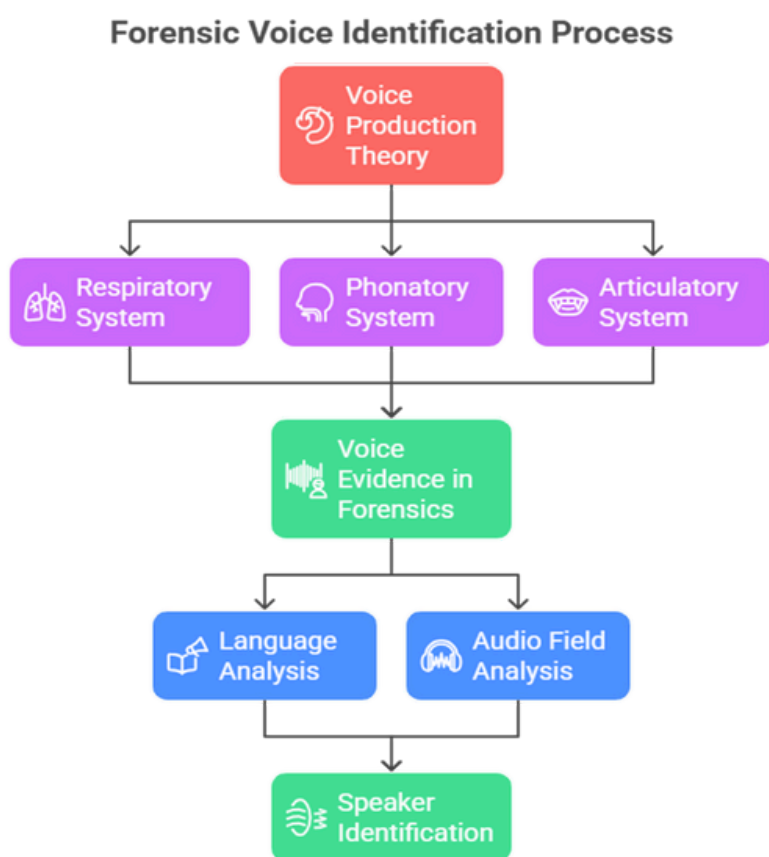


Fig. Forensic voice identification using acoustic features

The physical characteristics of speech sound waves that may be quantified and contrasted with digital tools are known as acoustic features.

- F0: fundamental frequency F0, commonly called pitch, depends on the frequency of vibration of the voice cords. It can provide useful biometric data, and it varies according to the speaker. Pitch may vary due to stress, health, and emotional status, and therefore careful interpretation is needed (Paya et.al, 2021).

- Frequencies of Formants (F1, F2, F3) formants are the frequencies of resonance in the vocal tract. They concern the ways the lips, tongue, and jaw move and combine in the process of speaking. F1 and F2 are especially significant in discriminating the sounds of vowels.

- Tempo and Duration are about the time aspect of speech; that is, speech rate, length of syllables, and words. These features are influenced by the speech of a person and their linguistic experience (Atkinson, 2015).

- Adaptability- The loudness and volume of speech affect the clarity of speech in terms of amplitude and intensity of voice. More varied amplitude profiles are helpful, however, in the enhancement and detection of noise.

- Spectral Characteristics Include bandwidth, distribution of energy in frequencies, and spectral tilt. Extracted features are usually done with the help of tools like Praat, MATLAB, Speech Analyser, Wave Surfer, etc (Paya et.al, 2021).

Linguistic characteristics in forensic voice analysis:

- Phonetic Characteristics: This area focuses on the articulation and perception of speech sounds. Analysis can be conducted on regional accents, pronunciation styles, and speech clarity.

- Lexical and Grammatical Features: The choice of individual words, structure of sentences, and the use of specific phrases can offer clues that are unique to the speaker. As an example, a speaker might consistently utilize double negatives or certain slang.

- Prosodic and Intonation Features: This encompasses the melody of speech, patterns of stress, rhythm, and pauses. The prosodic features distinctive to a speaker are typically challenging to replicate.

- **Sociolinguistic Characteristics:** These reflect the speaker's age, gender, ethnicity, geographic location, education, and social background. By applying sociolinguistic profiling, it can assist in narrowing down potential suspects, even when the exact identity is not ascertained.
- **Acoustic and Linguistic Characteristics relationship-**The acoustic and linguistic characteristics collaborate during forensic assessment. Acoustic information provides quantitative and subjective data (Kreiman et.al, 2014).
- The interpretative context and cultural meaning are given by linguistic evaluation. Entirely together, they strengthen the speaker identification and analytical power. As an illustration, two people may have a similar fundamental frequency (F0) but a significant difference in their prosody and dialect; therefore, by combining the two feature types, there is significance in doing it.

LINGUISTIC CHARACTERISTICS IN FORENSIC VOICE ANALYSIS

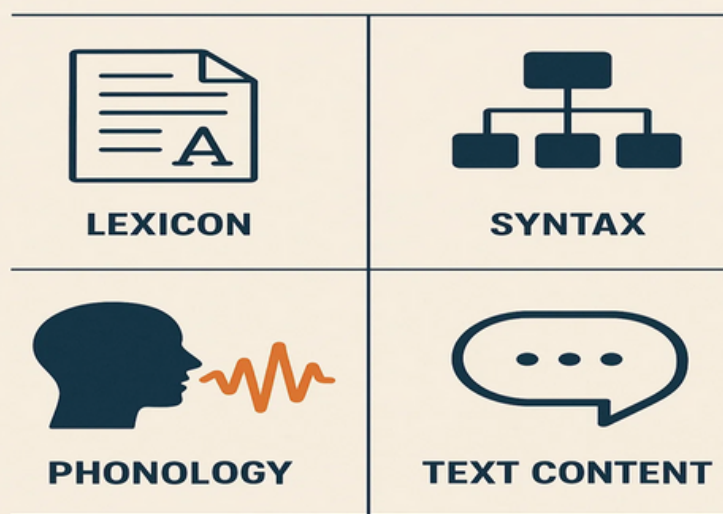


Fig. Linguistic Characteristic of forensic voice analysis.

Analytical Approaches:

- **Auditory-Phonetic:** This was done by paid practitioners who are trained to hear and type what they hear on the audio files. Stresses the acoustic and the prosodic cues. Very useful with short recordings or unclear recordings.
- **Software-Based Acoustic Analysis** Uses spectrograms, formant analysis, and a voice comparison program. Such programs as Praat or SFS can supply objective data for analysis.

Which forensic audio analysis method is most suitable for your needs?

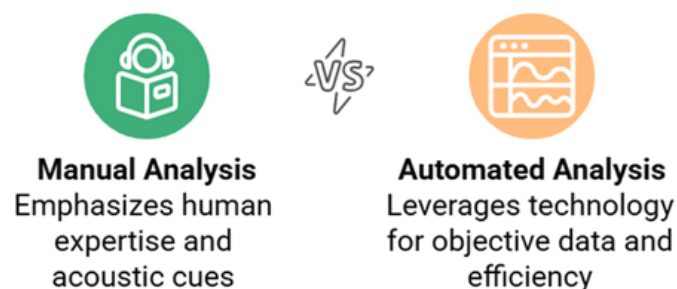


Fig. Analytical approach in forensic audio analysis

Applications in Forensic Cases:

- **Threat Calls:** The voice recording of various ransom attempts or threatening calls can be compared with any possible suspect.
- **Undercover Operations:** Secret recordings of suspects to clarify their identity.
- **Immigration and Asylum Cases:** The language and dialect may be assessed in authenticity checks of their place of origin.
- **Anonymous Communications:** Identifying who is speaking when there is fraud or harassment.

Challenges and Future Direction

- Intra-speaker Variation:** A person's vocal characteristics can fluctuate due to factors like emotion, illness, intoxication, or aging.
- Environmental and Technical Noise:** Background noise, echoes, and subpar recording equipment can compromise acoustic clarity.
- Voice Disguise:** Intentional alterations in speech may be used to evade recognition (Paya et.al, 2021).
- Lack of Standardization:** Variability in protocols across different jurisdictions may influence whether evidence is accepted in court.
- **Legal and Ethical Considerations:** Expert testimony must adhere to standards such as Daubert or Frye when presented in court.
 - Analysts are required to ensure transparency, objectivity, and the ability to reproduce results.
 - Data privacy and the ethical gathering of voice samples must be upheld.

AI and Deep Learning: Improved speaker discrimination using neural networks. Real-time speaker identification technologies are pivotal in the realms of security and law enforcement. Multimodal Biometric Fusion: Integrating voice recognition with facial scanning, gait assessment, or text analysis. Forensic Voice Databases: The creation of regional and multilingual voice databases for evaluation purposes. Cross-Language Voice Analysis: Investigation into speaker identification through various languages and dialects.

Concluding Remarks:

The fusion of acoustic and linguistic characteristics is crucial for the reliability and precision of forensic voice identification. While acoustic evaluation delivers measurable physical proof, linguistic traits provide valuable context and behavioral perspectives. The joint use of these elements, enhanced by progress in artificial intelligence, is advancing the field of forensic voice analysis. As issues such as disguise and variation continue to be addressed, a multidisciplinary strategy remains vital for upholding justice and scientific accuracy in forensic inquiries.

Reference:

- Jessen, M. (2008). Forensic phonetics. *Language and linguistics compass*, 2(4), 671-711.
- Schilling, N., & Marsters, A. (2015). Unmasking identity: Speaker profiling for forensic linguistic purposes. *Annual Review of Applied Linguistics*, 35, 195-214.
- Jessen, M. (2010). The forensic phonetician* Forensic speaker identification by experts. In *The Routledge handbook of forensic ling*
- Nolan, F. (2007). Voice quality and forensic speaker identification. *Govor*, 24(2), 111-128.
- Nolan, F. (2014). Forensic speaker identification and the phonetic description of voice quality. In *A figure of speech* (pp. 385-411). Routledge.
- Atkinson, N. (2015). Variable factors affecting voice identification in forensic contexts (Doctoral dissertation, University of York).
- Kreiman, J., Gerratt, B. R., Garellek, M., Samlan, R., & Zhang, Z. (2014). Toward a unified theory of voice production and perception. *loquens*, 1(1), e009.
- Tosi, O., Oyer, H., Lashbrook, W., Pedrey, C., Nicol, J., &

ABOUT THE AUTHORS

Ms. Janki Kacha

Research Scholar, Department of Biochemistry and Forensic Science, School of Science, Gujarat University, Ahmedabad, India.



Mr. Bhumit Chavda

Research Scholar, Department of Biochemistry and Forensic Science, School of Science, Gujarat University, Ahmedabad, India.



Cyber Warriors

(A Tribute to Digital Defenders)

**In the silent hum of midnight's glow,
Where data streams like rivers flow,
Stand unseen guardians, fierce and wise,
With firewalls blazing, beneath starless skies.**

**They wield no swords, nor iron shields,
But codes and scripts are their battlefields.
Their enemies hide in shadows deep,
Where malware crawls and hackers creep.**

**With every breach, they stand their ground,
Their keystrokes are a battle sound.
Bits and bytes their chosen art,
They guard the world's most fragile heart.**

**Defenders of truth, in digital lands,
Holding justice in binary hands.
For every threat that dares intrude,
They answer swift, with cyber shrewd.**

**So here's to the warriors we may not see,
Fighting for safety, for you and me.
Unsung heroes of the virtual fight,
Cyber Warriors—our hidden knight.**

CASE STUDY

on

JUSTICE BEHIND CLOSED DOORS: UNMASKING THE HORROR AT KOLKATA LAW COLLEGE

Author: Manibhavadharani A P



Case Summary

June 25, 2025 (Evening) A 24-year-old female first-year law student at South Calcutta Law College, Kasba, was allegedly gang-raped and beaten inside the college premises by three men—Manojit Mishra (a former student leader and casual staffer), Zaib Ahmed, and Pramit Mukherjee. A hockey stick was used to strike the victim's head. The attack reportedly continued for over three hours in multiple rooms (including the guard room and union room) before the victim was dragged by the attackers. June 26, 2025 Police arrested Manojit, Zaib, and Pramit, plus the college's security guard, who allegedly witnessed the assault. The National Commission for Women (NCW) took suo moto cognizance, demanding a detailed investigation report and full support for the victim. June 29–30, 2025 A Special Investigation Team (SIT)—expanded from 5 to 9 members—sealed key locations (union room, guard room, gate, washroom) and gathered extensive forensic evidence.

Investigation Begins: Breaking the Kolkata law college wall

- 1. **Weapon & Physical Evidence:** Hockey stick allegedly used to strike the victim—seized from the prime accused, Manojit Mishra. Blood-stained benches and empty liquor bottles were found across the union room, washroom, and guard’s room. Strands of hair collected inside the guard’s room—indicative of struggle.
- 2. **Clothing & Biological Samples:** Apparel seized from suspects and victim, including the red kurta and trousers worn during the assault. DNA samples were taken from all three accused and the victim by the SIT for forensic comparison.
- 3. **CCTV Surveillance:** Seven hours of campus footage (3:30 PM–10:50 PM) capture the victim being forcibly dragged into the guard’s room; the footage also verifies suspects’ movements throughout the campus .The video confirmed interaction with the college security guard and identified locations of struggle scenes; CCTV is being further analyzed by the investigation team.
- 4. **Mobile Footage & Digital Forensics:** 90-second assault clips were recovered from Manojit Mishra’s phone, which he and his accomplices allegedly used to groom or blackmail the victim. The digital evidence is undergoing thorough cyber-forensic analysis at a specialized lab in Salt Lake City.
- 5. **Suspect Injuries & Medical Corroboration:** Scratch marks on Monojit Mishra’s body, consistent with the victim’s nail scratches during resistance. The victim’s medical exam confirmed abrasions, bite marks, and signs of violent sexual assault

Evidence Summary

Evidence Type	Description	Role incase
Weapon & Hair stands	Hockey stick, blood stained bench, liquor bottles, hair	Proves physical assault, signs of struggle
DNA Samples	Collected from suspects and victim	Links suspects to crime biologically(DNA evidence)
Clothing samples	Victim’s red kurta, trousers, suspects clothes	Forensic testing , supports assault timeline
CCTV Footage	7hours of surveillance from 3:30 PM- 10:30 PM	Shows victim being dragged; confirms timeline and
Scratch & Injury marks	Scratch marks on accused; bit marks on victim	Supports victim’s resistance and physical struggle

How the Case Was Solved

1.Survivor's Statement Sparked Action the case broke open after the 24-yearold law student filed a complaint detailing a three-hour-long gang rape and assault with a hockey stick inside multiple rooms on campus. She identified the main accused: Manojit Mishra, along with Zaib Ahmed and Pramit Mukherjee.

2.Swift Arrests by Police within 24 hours, the Kolkata Police arrested all three accused, plus the college guard who allegedly witnessed the crime. A Special Investigation Team (SIT) was formed and expanded to 9 officers for high-priority handling. Witness Interrogation & Call Data Police questioned 17 students present on campus. Call logs and mobile location data placed the accused inside the crime zone during the assault.

3.Court & Legal Action all four accused were remanded to custody, and hearings began in Calcutta High Court. The court sealed college union rooms across West Bengal for security reform. Classes at the college were suspended indefinitely

Conclusion:

The case was cracked using a combination of survivor bravery, fast police response, scientific forensics (DNA, medical, digital), and surveillance footage. Together, these built a strong legal case—showcasing how forensic investigation can secure justice in high-profile campus

My Perspective the case also sends a national message:

If forensic protocols are followed quickly and cleanly, justice becomes stronger—even when powerful people are involved.

But it is also a powerful example of how forensic science, digital proof, and survivor courage can overcome those barriers Forensic protocols are followed quickly and cleanly, justice becomes stronger—even when powerful people are involved

But for true change, colleges must prioritize student safety over political affiliations or staff protection.

ABOUT THE AUTHOR

Manibhavadharani A P

GTN Arts College
Dindigul, Tamil Nadu
(B.Sc., Forensic Science)



KNOW WHAT'S IN THE TREND..?

REVOLUTIONIZING FORENSIC NURSING: NON-INVASIVE IMAGING FOR PHYSICAL AND SEXUAL ASSAULT EXAMINATIONS

Introduction

Forensic nursing plays a crucial role in the intersection of healthcare and justice, especially in cases of physical and sexual assault. These professionals are often the first point of contact for survivors, responsible not only for providing compassionate care but also for meticulously collecting and documenting evidence that may decide the outcome of legal proceedings.

In recent years, non-invasive forensic imaging technologies have transformed how forensic nurses conduct examinations. Advanced light source systems now allow practitioners to detect hidden injuries, visualize bruising long after the initial trauma, and document findings with unprecedented accuracy all while minimizing patient discomfort.

This feature explores how these innovative forensic imaging tools are shaping the future of forensic nursing.



The Evolution of Forensic Nursing Technology

Traditionally, forensic nursing examinations relied heavily on visual inspection under white light, which often failed to reveal subtle injuries. Faint bruising, healing wounds, and injuries on darker skin tones could be easily overlooked, leading to gaps in evidence collection.

The introduction of alternate light sources (ALS) has changed this dramatically. Devices like the Crime-lite series by Foster+Freeman are now being adopted in Sexual Assault R are globally acknowledged.

Before diving into imaging techniques, understanding how bruises develop is critical. After blunt force trauma, bruises typically progress through distinct stages:

1. Day 1–2: Red to blue/purplish-black (fresh injury)
2. Day 3–7: Greenish/yellow (healing phase)
3. Day 10+: Yellowish-brown before fading completely

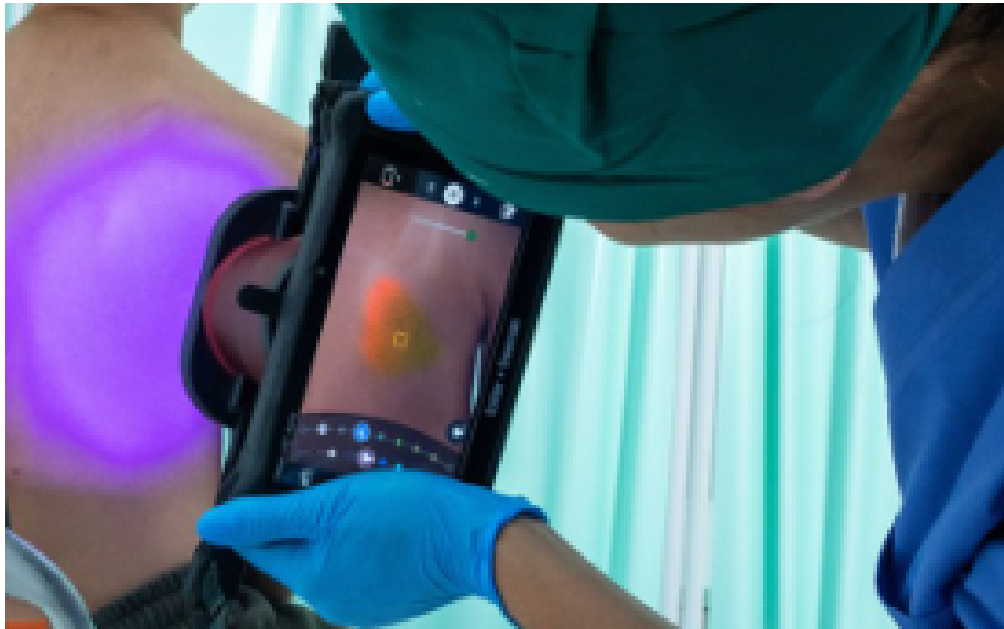
In many cases, by the time a survivor reports an assault, the bruise may have already entered the healing phase, making it less visible under normal lighting. Forensic light sources extend the visibility window significantly—up to 98 days post-injury, as demonstrated in research by the Swedish National Forensic Centre.

1. Cross-Polarisation Photography

- **How it Works:** Polarising filters are attached to both the light source and the camera. This reduces reflections from the skin's surface, increasing color saturation and contrast.
- **Why it Matters:** Bruise edges appear sharper, and color variations are more accurately captured, ensuring precise injury documentation.

2. Fluorescence Photography

- **How it Works:** The skin is illuminated with a high-intensity light source, and specific filters allow only fluorescent emissions to pass through to the camera.
- **Applications:**
 - Detecting faint or healing bruises invisible under white light
 - Improved bruise visualization on darker skin tones



3. Infrared (IR) Photography

- **How it Works:** IR light penetrates the skin differently than visible light. Tattoos, scars, and other features absorb IR light differently, making them stand out against the surrounding skin.
- **Applications:**
 - **Victim or Suspect Identification:** Tattoos or marks that are faded or concealed can be revealed.
 - **Age Determination of Scars or Old Injuries:** Valuable in repeated abuse cases.

Clinical and Legal Significance

The clinical benefits of non-invasive imaging extend beyond just evidence collection:

- **Patient-Centered Care:** Minimizing contact and avoiding repeated manual examinations reduce psychological trauma for survivors.
- **Improved Accuracy:** Enhanced injury visualization leads to more reliable medical documentation.
- **Legal Impact:** Courts increasingly recognize ALS-based injury documentation as strong scientific evidence, strengthening medico-legal reports and survivor testimony.

A randomized controlled trial by Downing et al. (Journal of Forensic Sciences) demonstrated that alternate light sources significantly improve

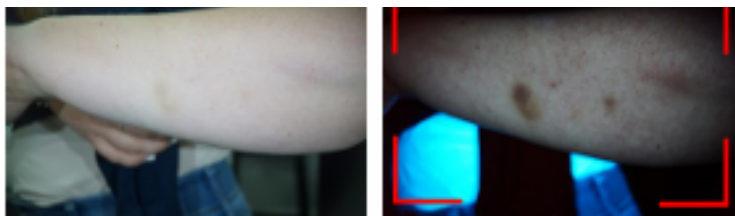
bruise detection rates compared to standard methods. Such evidence-based validation has accelerated their adoption in forensic healthcare worldwide.

The Technology Behind the Transformation

The Crime-lite AUTO, an all-in-one device combining UV, IR, and fluorescence imaging, is among the most advanced tools available today. Operated via a simple touch interface, it integrates:

- ✓ Full-Spectrum Imaging (UV to IR)
- ✓ Clip-On Polariser for Cross-Polarisation
- ✓ Wavelength-Specific Automated Filtering

This level of automation ensures consistent, reproducible imaging—critical for maintaining chain-of-custody and forensic integrity.



Bruising imaged 1-week after initial injury



Bruising imaged 1-week after initial injury

Conclusion: A New Era of Forensic Nursing

The integration of non-invasive imaging into forensic nursing practice marks a significant leap forward in both patient care and justice delivery. By revealing the hidden truth beneath the skin, forensic nurses are empowered to advocate for survivors with stronger, scientifically-backed evidence.

As technology advances, forensic nursing is poised to become an even more critical pillar in the criminal justice system—ensuring that every mark tells a story, and every story finds justice.

"Forensic light sources can reveal injuries up to 98 days post-trauma—transforming how we document abuse and advocate for survivors."

The Role of Deep Learning in Cyber Forensics

Reducing Cybercrime and Enhancing Facial Recognition

Author- Aashtha Tiwari

Introduction

A New Era in Cyber Forensics

In an increasingly digital world where cybercriminals continuously evolve their tactics, traditional forensic tools are struggling to keep up. Deep learning, a branch of artificial intelligence (AI), is revolutionizing cyber forensics by automating threat detection, analyzing large datasets, and enhancing biometric identification — especially in the realm of facial recognition.

This transformation is helping not only in solving crimes but also in preventing them before damage is done.

Cybercrime Demands Smarter Solutions

From data breaches and identity theft to ransomware attacks and cyberespionage, cybercrime is becoming more complex and difficult to trace. Forensic professionals need tools that can:

- Handle large-scale digital evidence
- Detect anomalies and behavioral patterns
- Adapt to evolving attack techniques

Deep learning provides exactly that. Neural networks — particularly Convolutional Neural Networks (CNNs) and Recurrent Neural Networks (RNNs) — are trained to extract meaningful insights from noisy, unstructured digital data.

Applications of Deep Learning in Cyber Forensics

Malware Detection and Classification

Deep learning can detect zero-day threats by analyzing behavioral patterns rather than relying on known signatures. CNNs trained on binary code and execution flow classify new malware with remarkable accuracy.

[Raff et al., 2018]

Network Traffic Forensics

LSTM (Long Short-Term Memory) networks process time-series data like packet flow logs, helping analysts detect suspicious traffic — botnets, DDoS attacks, or data exfiltration — in real time.

[Kim et al., 2014]

Automated Evidence Correlation

Deep learning models assist in connecting disparate pieces of evidence across devices, accounts, and timelines, reducing manual labor and enhancing investigative efficiency

Facial Recognition: Smarter, Faster, Fairer

Facial recognition has gained forensic significance, especially in identifying suspects and missing persons. Deep learning pushes its limits by improving accuracy, even in adverse conditions.

1. Advanced Feature Extraction

CNNs like FaceNet and ArcFace extract unique, high-dimensional facial features, enabling identification across age progression, expressions, and partial occlusions.

[Schroff et al., 2015]

2. Low-Quality & Cross-Angle Recognition

Surveillance images often suffer from poor resolution and odd angles. Deep learning — especially GANs (Generative Adversarial Networks) — can reconstruct, enhance, and clarify such images.

[Ledig et al., 2017]

3. Real-Time Surveillance Integration

Smart city and public surveillance systems integrate facial recognition AI to alert law enforcement about flagged individuals or unusual activities.

[Mohana & Patil, 2021]

Ethical Considerations & Limitations

As promising as it is, deep learning in forensic use raises some red flags:

Data Privacy: Handling biometric and personal data must comply with laws like GDPR.



Adversarial AI: Deep models can be misled by crafted inputs.

Courtroom Acceptance: Black-box models may not satisfy legal standards of explainability.

Transparent algorithms and multi-disciplinary policy frameworks are essential for responsible deployment.

Conclusion: A Powerful Ally for Modern Forensics

Deep learning is not just a trend — it's an evolution in forensic science. From detecting cyberattacks to enhancing digital identification, it equips investigators with tools that are:

- Faster
- More accurate
- Scalable across diverse case types

With careful governance and ethical implementation, deep learning will continue to be a game-changer in reducing cybercrime and improving investigative outcomes.

Reference:

1. Raff, E. et al. (2018). Malware Detection by Eating a Whole EXE. arXiv:1710.09435
2. Kim, G. et al. (2014). A novel hybrid intrusion detection method. Expert Systems with Applications, 41(4), 1690–1700
3. Schroff, F. et al. (2015). FaceNet: A Unified Embedding. CVPR
4. Ledig, C. et al. (2017). Photo-Realistic Image Super-Resolution Using GANs. CVPR
5. Mohana, H., & Patil, P. (2021). Deep Learning in Face Recognition for Criminal Investigations. IJCA, 183(18)

ABOUT THE AUTHORS

Aashtha Tiwari

Assistant Professor
Aditya University



PREPARE YOURSELF

UGC NET & FACT QUESTION BANK

1) For a face recognition system, tick the correct sequence.

- A. Enhancement
- B. Matching from the database
- C. Image fingerprint-based
- D. Segmentation
- E. Feature extraction

Choose the correct answer from the options given below:

- 1. B, D, C, A, E
- 2. C, D, A, E, B
- 3. A, E, C, D, B
- 4. D, B, C, E, A

2) Silica-based DNA extraction from biological exhibits follows the process in the following sequence.

- A. Washing
- B. Cell lysis and Protein digestion
- C. DNA adsorption onto silica
- D. Elution of DNA

Choose the correct answer from the options given below:

- 1. B, C, A, D
- 2. A, C, B, D
- 3. C, A, D, B
- 4. B, A, C, D

3) Which chart is used to study shape for measuring the axis of the sandy particles of the soil.

- A. Munsell soil colour chart
- B. Krumbein roundness chart
- C. Holding capacity chart
- D. Soil resistivity information chart
- E. Power comparison chart

Choose the correct answer from the options given below:

- 1. A and B Only
- 2. C and D Only
- 3. B and E Only
- 4. D and A Only

4) A concentrated extract of the urine stain may give a characteristic smell due to evolved by bacterial degradation of urea:

1. Bilirubin
2. Sugar
3. Sodium
4. Ammonia

5) Which of these hormones confirms the pregnancy of a woman?

1. Dehydroepiandrosterone
2. Estradiol
3. Human Chorionic Gonadotropin (hCG)
4. Estrogen

6) Which one of these is the best instrument to determine the psychotropic drugs?

1. HPTLC
2. GC-FID
3. LCMS
4. NAA

7) Which division of the Forensic Science Laboratory should be involved to check the contents of foodstuff:

1. Serology
2. Toxicology
3. Biology
4. Photography

8) Selling of child for the sake of money/asset falls under

1. Gender abuse
2. Sexual abuse
3. Child abuse
4. Domestic abuse

9) Rigor mortis is the sign after death, which occurs due to one of the following:

1. Cessation of blood circulation
2. Hydrolysis of tissues
3. Stiffening of body
4. Gradual decrease in body temperature

10) During the synthesis of ethanol, when the starting material is starch, in addition to ethanol a smaller amount of inferior liquor is also produced, which is also known as:

1. Grain alcohol
2. Isopentanol
3. Fusel Oil
4. Fuel Oil

11) The bullet consists of a core of lead alloy covered with a metallic jacket where the tip of the jacket is thin, is known as:

1. Armour piercing Bullet
2. Tracer Bullet
3. Incendiary Bullet
4. Dum-dum Bullet

12) Permanent teeth which are 32 in number are arranged in each jaw as:

1. 2 incisors, 4 canines, 6 premolar and 4 molars
2. 4 incisors, 2 canines, 4 premolar and 6 molars
3. 4 incisors, 6 canines, 2 premolar and 4 molars
4. 6 incisors, 4 molars, 2 canines and 4 incisors

13) Which of the undermentioned compound is considered to be a mild analgesic drug (NOAD)

1. Oxycodone
2. Tramadol
3. Codeine
4. Acetaminophen

14) Who among these has devised a method for accurate age estimation by means of incremental lines?

1. Boyde
2. Michael Graham
3. Henry Lee
4. Cyril Wecht

15) The twist required (in calibers) equals 150 divided by the length of the bullet (in calibers) is known as:

1. Greenhill's formula
2. Du-pont's formula
3. Mayeuskil's formula
4. Journee's formula

16) Which of the following is called the resting and inactive stage in respect to life cycle of an insect?

1. Egg stage
2. Adult stage
3. Pupa stage
4. Larvae stage

17) The retardation (R) of the standard projectile in feet/sec is given by

1. AV where 'A' and 'n' are constant and "V" is the velocity
2. $W / (d^2)$ where 'W' is the weight of the bullet (in pounds) and 'd' is the diameter (in inch)
3. $W / i * d^2$ where 'W' is the weight (in pounds) 'd' is the diameter and 'i' is the form factor
- $3/2 * g * t^2$ where 'g' is gravitation pull at time interval 't'

18) In a hit and run case, what are the steps followed in a proper sequence for carrying out investigation

- A. Examination of nature of inquiry to the victim
- B. Shifting of the victim to the hospital
- C. Skid marks examination of the vehicle
- D Photography of the cane

Choose the correct answer from the options given below:

1. A. B. D. C
2. D. C, A, B
3. A, C, D. B
4. C, A, B, D

19) For the purpose of development of latent finger print at a scene of crime, different powders are used and one of them is chemically known as "Hydrag cum Creta". The colour of this powder is

1. Grey
2. Red
3. Black
4. White

20) While collecting maggot samples for further examination, is preferably placed directly in acetic acid but alternately one can use:

1. Chloroform
2. Ethyl alcohol
3. Hot water
4. Cold water

ANSWERS:
1.2, 2.1,3.3,4.4,5.6,3,7.2,8.3,9.3,10.4,11.4,12.2,13.4,14.1,15.1,16.3,17.1,18.2,19.4,20.2

PREPARE YOURSELF

UGC-NET PAPER 1: QUESTION BANK

1. The world population growth rate is slowing down gradually. If this trend continues, the population of the world would have doubled in about how many years?
 - a) 180 years
 - b) 120 years
 - c) 60 years
 - d) 30 years

2. Inference is a logical:
 - a) Deductive conclusion
 - b) Fallacy
 - c) Statement
 - d) Assumption

3. The process of precise communication in the classroom is:
 - a) Formal
 - b) Non-verbal
 - c) Technical
 - d) Semantic

4. Liberal education implies:
 - a) Technical education
 - b) Education for freedom
 - c) Narrow specialization
 - d) Skill-based learning

5. Which one of the following is a primary source of data?
 - a) UNO reports
 - b) Census of India
 - c) World Bank data
 - d) Human Development Reports

6. Television is an example of:
 - a) Group communication
 - b) Intrapersonal communication
 - c) Mass communication
 - d) Interpersonal communication

7. A university teacher aims at:

- a) Helping students prepare for examination
- b) Developing professional outlook
- c) Understanding the subject deeply
- d) Imposing strict discipline

8. Choose the correct alternative to complete the series: 3, 11, 23, 39, ?, 83

- a) 59
- b) 51
- c) 57
- d) 49

9. Starting from point A, Ajit walks 14 metres towards west, then turns to his right and walks 14 metres and then turns to his left and walks 10 metres. He again turns to his left and walks 14 metres and reaches the point E. The shortest distance between A and E is:

- a) 38
- b) 42
- c) 52
- d) 24

10. A, B, C, D, E, and F are sitting around a round table. A is between F and E. F is opposite to D and is not in either of the neighbouring seats of E. The person opposite to B is:

- a) C
- b) D
- c) A
- d) F

11. The missing number in the series: 2, 7, 24, 77, ?, 723 is:

- a) 238
- b) 432
- c) 542
- d) 320

12. In a certain city, the Taxi charges comprise a fixed charge and the charge of the distance travelled. A person paid ₹156 for a journey of 24 km and another person paid ₹204 for a journey of 30 km. The amount paid by a person who has travelled 36 km is:

- a) ₹236
- b) ₹240
- c) ₹248
- d) ₹256

Answer - 1.b, 2.a, 3.d, 4.b, 5.b, 6.c, 7.c, 8.b, 9.d, 10.a, 11.c, 12.c

2025

ADMISSIONS OPEN

nirf
Rank Band
201-300

ACCREDITED BY
NAAC
A++ GRADE

NBA
TIER 1
ACCREDITED



ADITYA
UNIVERSITY

STEP INTO A WORLD OF OPPORTUNITIES

YOUR JOURNEY TO EXCELLENCE STARTS HERE

www.adityauniversity.in

FOR ADMISSIONS CONTACT : **+91 70360 76661, 70950 76663/4**

RANKINGS & ACCREDITATIONS



6 UG Programs Accredited by
NBA under Tier I



Rank Band **26-50**

PROGRAMS OFFERED

Students from 18 states in India and 24 Countries Worldwide

SCHOOL OF ENGINEERING

B.TECH

- Civil Engineering
- Electronics and Communication Engineering
- Electrical and Electronics Engineering
- Mechanical Engineering
- Computer Science and Engineering
- Information Technology
- Artificial Intelligence & Machine Learning
- Data Science
- Petroleum Technology
- Mining Engineering
- Agricultural Engineering

M.TECH

- Structural Engineering
- Power Electronics & Drives
- Energy Science & Technology
- VLSI Design
- Computer Science & Engineering
- CSE (AI&ML)

SCHOOL OF PHARMACY

- B.Pharmacy
- M.Pharmacy
- Pharm. D

SCHOOL OF SCIENCES

- B.Sc. -Forensic Science
- B.Sc. -Cyber Security & Digital Forensics
- M.Sc.-Forensic Science
- M.Sc.-Cyber Security & Digital Forensics

SCHOOL OF BUSINESS

- BBA
- BBA-Digital Marketing
- BBA-Business Analytics

MBA

MCA

Ph.D. in All Disciplines

COLLABORATIONS with FOREIGN UNIVERSITIES



"We are excited to announce a new partnership with
UNIVERSITY OF SOUTH CAROLINA UPSTATE,

ACHIEVEMENTS OF OUR STUDENTS

2026 PLACEMENTS

A RECORD BREAKING PACKAGES

52 Placed in
#HASHAI
LAKHS PER ANNUM



D. UPANISHA

C. POOJITHA

S. SRIRAM

₹ **45** LPA ¹³ CSE Students
AUTODESK

₹ **35** LPA ¹⁶ CIVIL & MECH Students
AUTODESK

2025 PLACEMENTS

52 Placed in
#HASHAI
LAKHS PER ANNUM



A. HARSHITH

M. DIVYA

V. GOWTHAM

Scan to know
more about Placements



Internship offer at

Google

Stipend
₹ **1.23**
Lakhs Per Month

D RAMYA
B.Tech(CSE)



2025 Placements

2018

Offers Still Continuing...

₹ **33.64** LPA
Highest CTC

Above 50 ^{LPA}	3 Adityans
Above 35 ^{LPA}	5 Adityans
Above 30 ^{LPA}	15 Adityans
Above 25 ^{LPA}	23 Adityans
Above 20 ^{LPA}	38 Adityans
Above 15 ^{LPA}	41 Adityans
Above 10 ^{LPA}	50 Adityans
Above 9 ^{LPA}	59 Adityans
Above 8 ^{LPA}	64 Adityans
Above 7 ^{LPA}	88 Adityans
Above 6 ^{LPA}	134 Adityans
Above 5 ^{LPA}	161 Adityans
Above 4 ^{LPA}	647 Adityans
Above 3.6 ^{LPA}	1939 Adityans

#2025 International Placements

HITACHI
Inspire the Next

₹ **35.36**
Lakhs Per Annum

JMC Co., Ltd.
₹ **34.95**
Lakhs Per Annum

TOYOTA
connected
₹ **34.12**
Lakhs Per Annum

Aisan
₹ **33.51**
Lakhs Per Annum

JEMS
₹ **32.84**
Lakhs Per Annum

Daiseiki

₹ **31.70**
Lakhs Per Annum

IHARA
₹ **29.02**
Lakhs Per Annum

AD-TEC
₹ **28.61**
Lakhs Per Annum

HITACHI
₹ **27.29**
Lakhs Per Annum

Hitachi
Industrial Products, Ltd.
₹ **27.16**
Lakhs Per Annum

and many more Placements...

ADITYA HOSTELS (AC / NON - AC)

Home away from Home

- Comfortable, hygienic surroundings, individual grooming and counselling.
- AC / Non-AC accommodation.
- An exclusive library with digital and multimedia facility, newspapers, magazines, journals, books related to academics and competitive exams like GRE, GATE etc.
- Wi-fi campus.
- On campus bank facility (Canara Bank).
- Uninterrupted power supply.
- Fully equipped gym.
- Hot water facility.
- Saloon for boys and beauty parlour for girls with in the premises.
- Apollo dispensary is accessible 24/7 to support campus health needs equipped with ambulance assistance.

ASAT

ADITYA'S SCHOLASTIC APTITUDE TEST

- ASAT represents Aditya's Scholastic Aptitude Test which is planned as an entrance for UG programs
- The duration of the test is 120 minutes

- The test comprises of

Maths, Physics, Chemistry & Gamified puzzles
(for B. Tech. Aspirants)

- MATHS (30 marks - 30 MCQs)
- PHYSICS (15 marks - 15 MCQs)
- CHEMISTRY (15 marks - 15 MCQs)
- GAMIFIED PUZZLES (No marks - 30 min.)

Maths / Biology, Physics,
Chemistry & Gamified
puzzles
(for B.Sc. Aspirants)

- MATHS / BIOLOGY (30 marks - 30 MCQs)
- PHYSICS (15 marks - 15 MCQs)
- CHEMISTRY (15 marks - 15 MCQs)
- GAMIFIED PUZZLES (No marks - 30 min.)

Aptitude, Reasoning,
English & Gamified
puzzles
(for BBA Aspirants)

- APTITUDE (30 marks - 30 MCQs)
- REASONING (15 marks - 15 MCQs)
- ENGLISH (15 marks - 15 MCQs)
- GAMIFIED PUZZLES (No marks - 30 min.)

SCHOLARSHIP

ASAT (Demo Link)

<https://cocubes.in/aditya-asat>
Application Id for Demo

- adityatesting1
- adityatesting2
- adityatesting3



Passkey for Demo
322160

MERIT
SCHOLARSHIPS
upto
100%

For Details SCAN Here



SCHOLARSHIP



- Students may secure seats into Programs by qualifying in ASAT Entrance Test.
- Aditya University offers Scholarships of up to 100% of the total tuition fee for meritorious students across all branches in its Programs

www.adityauniversity.in

For Admissions: ☎ **+9170360 76661, 70950 76663/4** 📞 **95536 49666**

Aditya Nagar, ADB Road, Surampalem - 533 437, Kakinada Dist., Andhra Pradesh, INDIA.

Thank You Note

Dr. N. Suguna Reddy

Secretary

**Aditya Degree and PG Colleges,
Andhra Pradesh**



Dear Readers,

We are truly grateful for the incredible support you've extended to India's first bi-monthly forensic science magazine. The enthusiastic response to our previous editions has been both motivating and humbling, reinforcing our commitment to serve forensic professionals, researchers, and enthusiasts across the country.

With great pride, we present the seventh issue, curated with an even richer array of insightful articles, groundbreaking research, and stimulating discussions — all focused on propelling the field of forensic science forward. Your continued feedback plays a vital role in shaping our efforts and drives us to maintain the highest standards of content and impact.

Thank you for being an essential part of our journey. We look forward to continuing to inform, inspire, and celebrate the advancements that are shaping the future of forensic science.



Aditya College of Forensics & Cyber Security

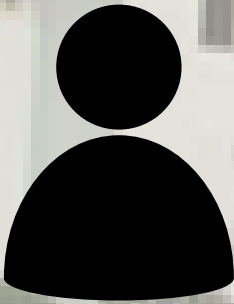
UG Courses

- B.Sc. Forensic Science
- B.Sc. Cyber Security & Digital Forensics

PG Courses

- M.Sc. Forensic Science
- M.Sc. Cyber Security & Digital Forensics

Contact Us:



principalforensic@aditya.ac.in

adminforensic@aditya.ac.in

forensicmagazine@aditya.ac.in

89782 96668

97015 76663