CHAPTER I: INTRODUCTION

Information security is the main concern of current scenario, which has a number of approaches to preserve data via cryptography, watermarking, steganography techniques. One such approach may always create a negative impact on all the process, which involves with vulnerable activities such as malicious and harmful content spreading by embedding. To identify such content, steganalysis has been performed. The counter technique of image steganography is called as image steganalysis, which begins by recognizing the object that exists in the embedded source file.

Steganography is the practice of concealing a file, message, image, or video within another file, message, image, or video. The word steganography comes from New Latin steganographic, which combines the Greek words steganós. Steganalysis is the study of detecting messages hidden using steganography. Steganalysis applications are identify suspected packages, determine whether or not suspected have a payload encoded into them if possible recover that payload. Steganalysis can be done on image files, video files or even on audio files. Steganalysis is an important part in investigation of digital documents including image files, audio files, video files etc. Various types of steganalysis tools are used to perform steganalysis to extract the hidden data from image files, audio files, video files etc.

Image steganography is defined as the covert embedding of data into digital pictures. Though steganography hides information in any one of the digital Medias, digital images are the most popular as carrier due to their frequency usage on the internet.[2] Because the size of the image file is huge in size, it can cover large amount of information. The Human Visual System cannot differentiate the normal image and the image with hidden data easily. The digital images are usually contains large amount of redundant bits in nature, where images are became the most popular cover objects for steganography. So every research uses image as cover file with different image formats such as JPEG, BMP, TIFF, PNG or GIF files can be used as cover objects to deploy steganography. A bitmap or BMP format is a simple image file format. Data is easy to manipulate, since it is uncompressed. But the uncompressed data leads to larger file size than the compressed image. JPEG (Joint Photographic Expert Group) is the most commonly used image file format. It uses lossy compression technique; the quality of the image is excellent. The size of the file is also smaller. TIFF format uses lossless compression. The file is reduced without

affecting the image quality. GIF (Graphics Interchange format) has colour palette to provide an indexed colour image. It uses lossless compression and it can store only 256 different colours, it is not suitable for representing complex photography with continuous tones, PNG (Portable Network Graphics) file format provides better colours support, best compression, and gamma correction in brightness control and image transparency. PNG format can be used as an alternative to GIF to represent web images.

Steganography is a strong technique to hide a secure message, however, it also vulnerable when the technique used to spread malicious and harmful content by embedding. To identify such content, staganalysis has been performed. The counter technique of image steganography is known as image steganalysis, which begins by recognizing the object that exists in the embedded source file. The aim of this process is not to advocate the removal or disabling of valid hidden information such as copyrights, but to point out approaches that are vulnerable and may be exploited to investigate illegal and dishonest hidden information.[3] Security threats analysis on hidden information may take several forms like detecting, extracting, and disabling or destroying hidden information.[4]An attacker may also embed contradict information over the existing hidden data.

Secret data sharing and secure communication is the major research area, which linked with several security applications. This type of secret data sharing is popular with the help of steganography approaches to deliver safely over computer networks without interference. Steganography is a technique that hides data among the bits of a cover file such as audio, video and image files. [1] In steganography the existence of a message is often unknown. Both data embedding and extraction need a digital image processing technique to deploy. The application such as medical safety, terrorism and hacking types of application need steganalysis. Steganalysis provides a way of detecting the presence of hidden information from the embedded content. This paper provides an overview and comparative analysis of different Steganalysis approaches.

Invisible secrets 4: is software created to protect personal data on your computer. It totally hides them in places that no one can notice that some of your important files can be found there. It encrypts your data and files to secure their transfer via internet.

While Invisible Secrets this software, you may encrypt and hide files directly from Windows Explorer and automatically transfer them via Email or via internet. It features strong encryption algorithms (AES-Rijndale), a password, a shredder which helps you to destroy recovery files, folders and internet traces and a locker that allows you to protect some application.

Moreover, Invisible Secrets provide a wizard that guides you through all the necessary steps needed to protect all your data.

Image Steganography: is also a free software for hiding your information in image files. You can hide text message or files inside an image file just select the source file in which you want to hide the secret message and then select the file to hide or write the text message to hide. Select the output image location and then click on START button to start encoding the file. Encoded image will have the secret message inside the image. You can use the decode option of the same tool to decode the hidden file or message from the image.

In the past studies only single tool was used for extraction of data from image file, audio file, video file etc. In the present study comparison of two steganalysis tools are done.

CHAPTER II: LITERATURE REVIEW

Yong Yang et.al (2019) studied on Steganalysis on Internet images via domain adaptive classifier- In recent years, various steganalysis algorithms have been proposed and achieved satisfactory performance. However, these conventional methods are not effective for mismatched steganalysis. In real world, there are millions of images captured by different cameras and users transmitted on the Internet every day. The steganalysis on Internet images will encounter steganographic algorithm mismatch (SAM) and cover source mismatch (CSM). Therefore, the steganalysis on the Internet is essentially to solve the mismatch problem. This paper proposes a method to solve the mismatched steganalysis on the Internet images by domain adaptation classifier. It makes the distribution between training and testing sets more similar to obtain better detection performance. They integrated joint distribution adaptation and geometric structure as regularization terms to a standard supervised classifier. Specifically, joint distribution adaptation contains marginal and conditional distributions. And considering the characteristics of steganalysis on the Internet images, they added the conditional regularization in the geometric structure to the existing algorithms. Experimental results (include SAM and CSM) on Internet images show that our method has a better performance than state-of-the-art-methods.

S.Hemalatha et.al (2015)studied on Wavelet Transform Based Steganography Technique to Hide Audio Signals in Image. Information security is one of the most important factors to be considered when secret information has to be communicated between two parties. Cryptography and steganography are the two techniques used for this purpose. Cryptography scrambles the information, but it reveals the existence of the information. Steganography hides the actual existence of the information so that anyone else other than the sender and the recipient cannot recognize the transmission. In steganography the secret information to be communicated is hidden in some other carrier in such a way that the secret information is invisible. In this paper an image steganography technique is proposed to hide audio signal in image in the transform domain using wavelet transform. The audio signal in any format (MP3 or WAV or any other type) is encrypted and carried by the image without revealing the existence to anybody. When the secret information is hidden in the carrier the result is the stego signal. In this work, the results show good quality stego signal and the stego signal is analyzed for different attacks. It is found that the technique is robust and it can withstand the attacks. The quality of the stego image is measured by Peak Signal

to Noise Ratio (PSNR), Structural Similarity Index Metric (SSIM), Universal Image Quality Index (UIQI). The quality of extracted secret audio signal is measured by Signal to Noise Ratio (SNR), Squared Pearson Correlation Coefficient (SPCC). The results show good values for these metrics.

Hedieh Sajedi (2016) studied on Steganalysis based on steganography pattern discovery- The goal of steganalysis algorithms is detection of stego images from clean images. Each steganography method based on its embedding mechanism puts a special pattern on the stego images. Finding this pattern in the images leads us to employ a classifier to be constructed specially for detecting stego images which are the results of a special steganography algorithm. In this paper, to have high detection accuracy, they proposed an approach for Steganography Pattern Discovery (SPD). Our proposed approach employs an evolutionary method to extract the signature of stego images against clean images via fuzzy if–then rules. Based on the discovered knowledge, suitable trained models for steganalysis can be employed and stego images will be detected with high accuracy. Using SPD, they could predict the type of steganography method from a stego image. Employing SPD can enhance the approaches, which assume that a special steganography method is used. The effect of SPD before applying steganalysis methods has been investigated by some steganography and steganalysis techniques and it has been validated using some image databases. The results indicate that the pattern of a steganography method is extracted well and the type of steganography method used to make a stego image can be predicted with high accuracy.

Divya Jennifer D'Souza and Minu P.Abraham(2016) studied on A Multilayered Secure Scheme for Transmission of Sensitive Information based on Steganalysis- Thet proposed a multilayered secure scheme to transfer sensitive text over an unreliable network. The secret text is first encrypted using the AES algorithm. The cipher text produced is hidden in an audio file. The audio file is in turn encrypted in parallel using the concept of Shamir's technique based on CRT to maximize resource utilization. These, audio shares are sent over different channels in the network for security. Experimental results show that, even if certain shares got lost over network, audio files could be recovered at the receiver with the remaining shares without sender needing to resend the file. LSB technique was used.

Yuntao Wang et.al.(2019) studied on MP3 steganalysis based on joint point-wise and block-wise correlations- With the growing attention on multimedia security, various MP3 steganographic and steganalytic algorithms have been proposed increasingly. However, the existing MP3 steganalysis is lack of good universality and detection performance. To address this problem, they devised an effective MP3 steganalytic algorithm based on joint point-wise and block-wise correlations of quantified modified discrete cosine transfer coefficients matrix. On the one hand, a universal rich

high pass filtering module for MP3 steganalysis is deployed to boost the sensitiveness of the algorithm to the subtle signal brought by the data hiding. On the other hand, based on the principle of MP3 encoding and the characteristics of MP3 steganography, multi-scale correlations measure module is introduced, which is used to measure the changes of point-wise, 2×2 block-wise, and 4×4 block-wise correlations due to steganography separately. Additionally, customized feature optimization, including truncated threshold selection and high pass filters measure, is performed based on the properties of MP3 steganography. Experimental results illustrate that our proposed algorithm can be applied to various MP3 steganographic algorithms, bitrates, duration, and relative payloads. Detection accuracies are promoted by more than 20% averagely.

Zhenyu Li and Adrian G. Bors (2017) studied on Steganalysis of 3D objects using statistics of local feature sets- 3D steganalysis aims to identify subtle invisible changes produced in graphical objects through digital watermarking or steganography. Sets of statistical representations of 3D features, extracted from both cover and stego 3D mesh objects, are used as inputs into machine learning classifiers in order to decide whether any information was hidden in the given graphical object. The features proposed in this paper include those representing the local object curvature, vertex normals, the local geometry representation in the spherical coordinate system. The effectiveness of these features is tested in various combinations with other features used for 3D steganalysis. The relevance of each feature for 3D steganalysis is assessed using the Pearson correlation coefficient. Six different 3D watermarking and steganographic methods are used for creating the stego-objects used in the evaluation study.

F. Ghareh Mohammadi and H. Sajedi (2017) studied on Region based Image Steganalysis using Artificial Bee Colony- Steganalysis is the art and skill of discriminating stego images from cover images. Image steganalysis algorithms can be divided into two broad categories, specific and universal. In this paper, a novel universal image steganalysis algorithm is proposed which is called RISAB, Region based Image Steganalysis using Artificial Bee colony. The goal of the proposed method is to realize a sub-image from stego and cover images through ABC with respect to density according to the cover, stego and difference images. In their method, they looked for the best sub-image, which contains the highest density with respect to the changed embedding pixels. Furthermore, after selecting the best sub image, they extracted the features, which have been selected by IFAB, Image steganalysis based on Feature selection using Artificial Bee colony. At the end, both selected features by IFAB and extracted features by RISAB are combined. As a result, a feature vector is generated which improves accuracy of steganalysis. Experimental results show that our proposed method outperforms other approaches.

JuJia et.al(2019) studied on Transferable heterogeneous feature subspace learning for JPEG mismatched steganalysis - Steganalysis is a technique that detects the presence of secret information in multimedia data. Many steganalysis algorithms have been proposed with high detection accuracy; however, the difference in statistical distribution between training and testing sets can cause mismatch problems, which will degrade the performance of traditional steganalysis algorithms. To solve this problem, we propose a transferable heterogeneous feature subspace learning (THFSL) algorithm for JPEG mismatched steganalysis. Our approach considers the feature space in each domain as a combination of the domain-independent features and the domain-related features. They used the transformation matrix to transfer both the domain-independent and domain-related features from the source and target domains to a common feature subspace, where each target sample can be better represented by a combination of source samples. By imposing low-rank constraints on the domain-independent features, the structures of data can be preserved, which can capture the intrinsic structures for discriminating cover and stego images. The method can avoid a potentially negative transfer by using a sparse matrix to model the domain-related features and, thus, is more robust to different domain changes in mismatched steganalysis. Extensive experiments on various mismatched steganalysis tasks show the superiority of the proposed method over the state-of-the art methods.

Saman Shojae and Chaeikar Ali Ahmadi (2018) studied on Ensemble SW image steganalysis: A low dimension method for LSBR- Blind steganalysis examines digital media for the likely existence of hidden messages, without prior knowledge of the steganographic algorithm that may have been used to hide such messages. This paper puts forward a novel learning-based blind image steganalysis method for tackling spatial domainleast significant bit (LSB) flipping. Its key steganalytic feature is the correlation between message length and the regression of the quantity of intensity-identical pixels and channels. A specially designed support vector machine (SVM) kernel is trained to analyze each pixel as an individual analysis unit, with the combined results of the analysis determining the ultimate steganalysis decision. This method makes a number of innovative contributions to the field of blind steganalysis. First, it offers a novel steganalytic feature for measuring similarity between the weight of pixels and channels. Second, it involves pixels in the steganalytic process according to the degree of their detected membership, thus avoiding neutral pixels influencing the process. Third, it extracts reference statistical behavior from cover and stego pixels, thereby enhancing the sensitivity of the steganalyzer. Fourth, its SVM kernel enhances sensitivity using statistical functions combined with trapezoidal fuzzy membership. Finally, with all these innovations it is capable of achieving a sensitivity of 99.626% for 0.25 bpp stego images through only two analysis dimensions.

Abdelhamid et.al (2017) studied on Data hiding inside JPEG images with high resistance to steganalysis using a novel technique: DCT-M3- Information security relies mainly upon encryption, and in some cases, steganography for an extra layer of security. Steganography is the science and art of secret communication between two sides that attempts to conceal the existence of the message. Many steganographic techniques have been proposed, all of them make statistically noticeable changes in the properties of the cover carrier particularly when the message payload is high. In this paper, they proposed a new methodology of transform domain JPEG image steganography technique that provides high embedding performance while introducing minimal changes in the cover carrier image. The algorithm, named DCT-M3, uses modulus 3 of the difference between two DCT coefficients to embed two bits of the compressed form of the secret message. The proposed algorithm reduces significantly the number of changes in the cover image; the embedding capacity has been improved by 16.7% approximately while maintaining minimum detectability against blind steganalysis schemes.

CHAPTER III: AIMS AND OBJECTIVE

AIM:

To compare extraction method of two different steganalysis tools

OBJECTIVE:

- To extract the hidden data from a image file using two different steganalysis tools.

CHAPTER IV: MATERIALS AND METHODOLOGY

MATERIALS:

Apparatus

1. A laptop
2. A good internet connection
3. Setup files of the tools

Tools

1. Invisible secrets 4
2. Image steganography

METHODOLOGY:

In the analysis, two steganalysis tools were used–"Invisible secrets 4" and "Image steganography". Samples were collected and the above mentioned two tools were used to extract the hidden data.

FIRST TOOL: INVISIBLE SECRETS 4

ENCODING

Step1: Select the particular file which should be hidden. Here I choose a text document-"ashik.txt" which contain the following data-"hiiiiiiiiiiiiiiiiiiiiii my name is ashik"

Figure.1: Creating a text document named as "ashik.txt"

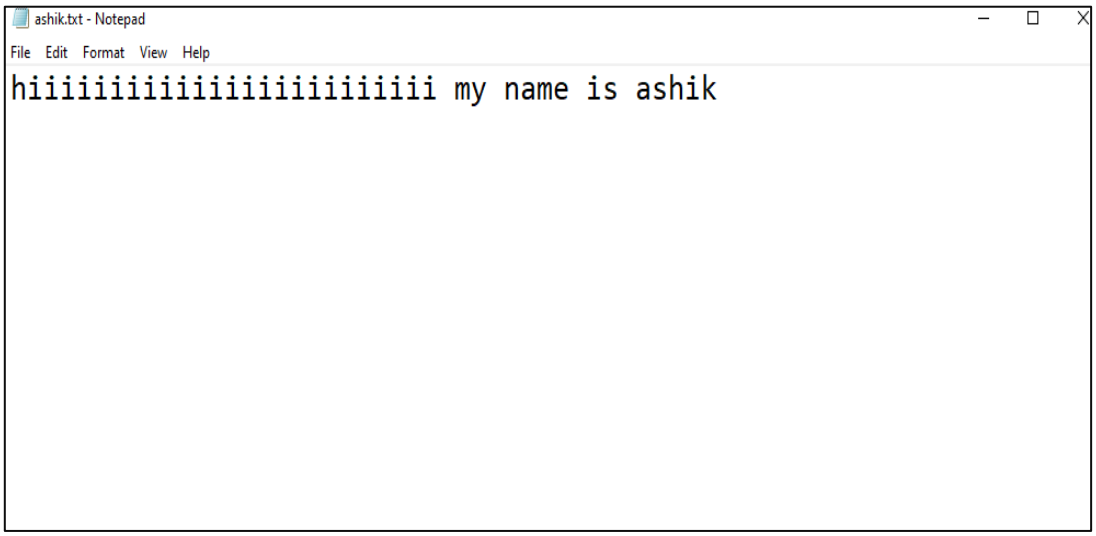

Figure.2: Entering data into the text document

Figure.3: Opening the text document to be hidden inside the steganalysis tool-"Invisible secrets 4"

Figure.4: Text file is added

Step 2: Select a file to which the sample should be hidden.

Figure.5: Enter the file name of the carrier in which you want to encrypt and hide the text file

Figure.6: Choosing a carrier file

Figure.7: After selecting the carrier file click next.

Step 3: Choose a password to encrypt it.

Figure.8: Setting a password

Step 4: Choose a destination for the output file and give a name.

Figure 9: Enter the new name for the encrypted file

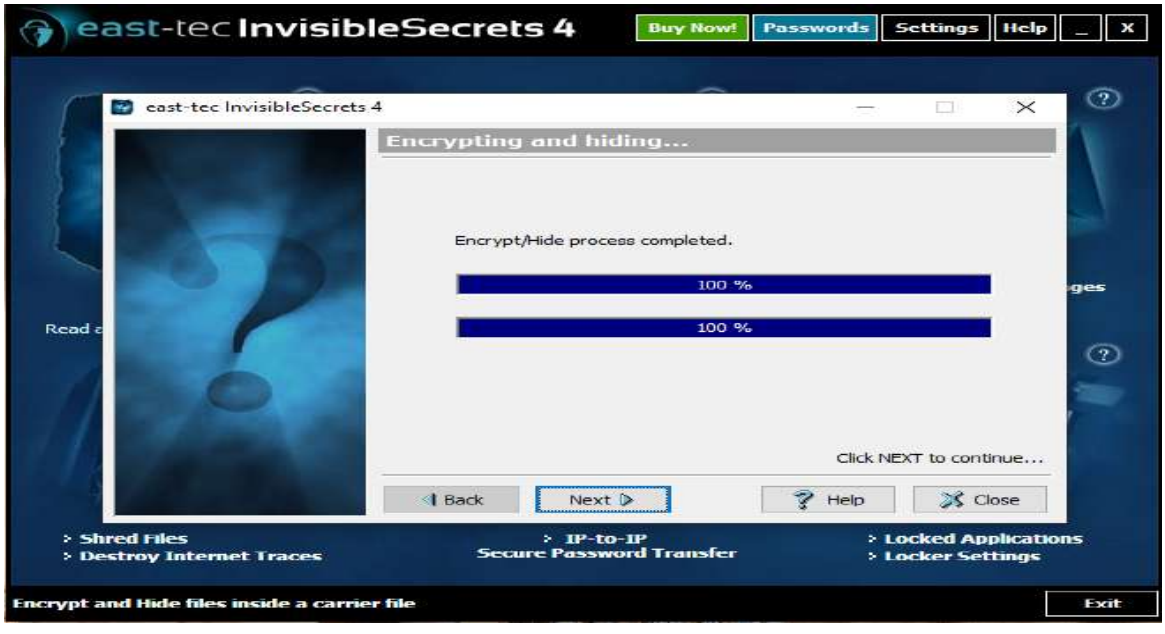

Figure 10: Encrypting and hiding process completed.

Figure 11: Click on finish and explore the output folder

Step 6: The output file named “HIDDEN”, which is shown in the image.

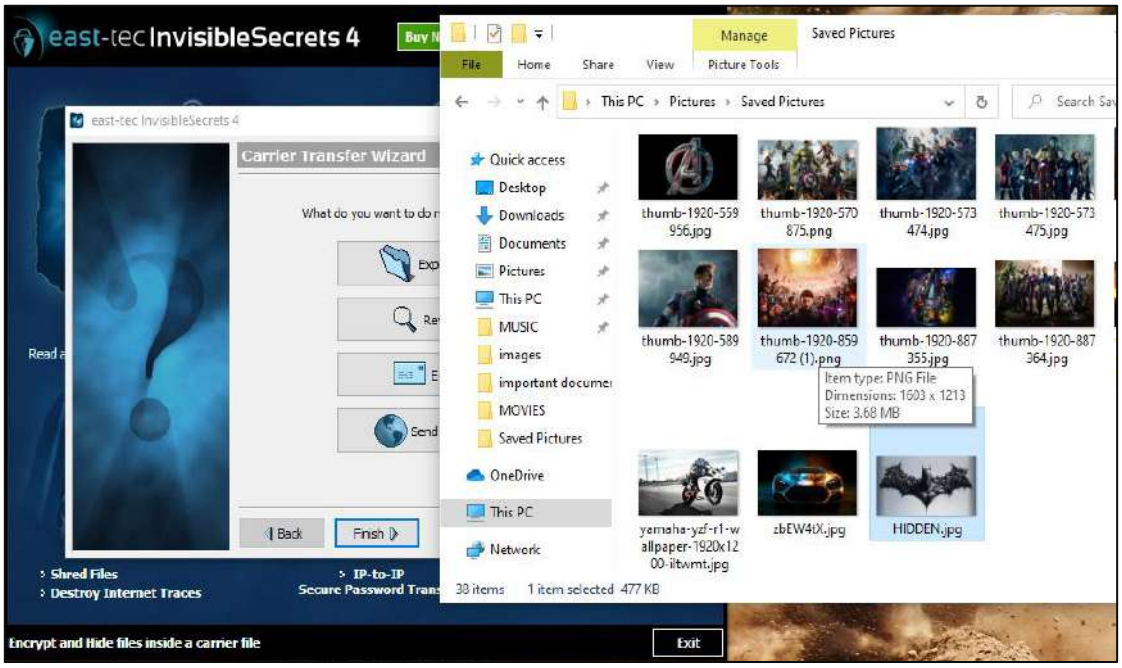

Figure 12: Image where the text is hidden

DECODING

Step 7: Select the particular file which should be decoded.

Figure 13: Select the carrier file

Figure 14: Opening the carrier file

Figure 15: After selecting the carrier file click on next

Step 8: Enter the password.

Figure16: Enter the password

Step 9: Click on unhide.

Figure 17: Click on unhide

Step 10: Click on finish.

Figure 18: Unhiding

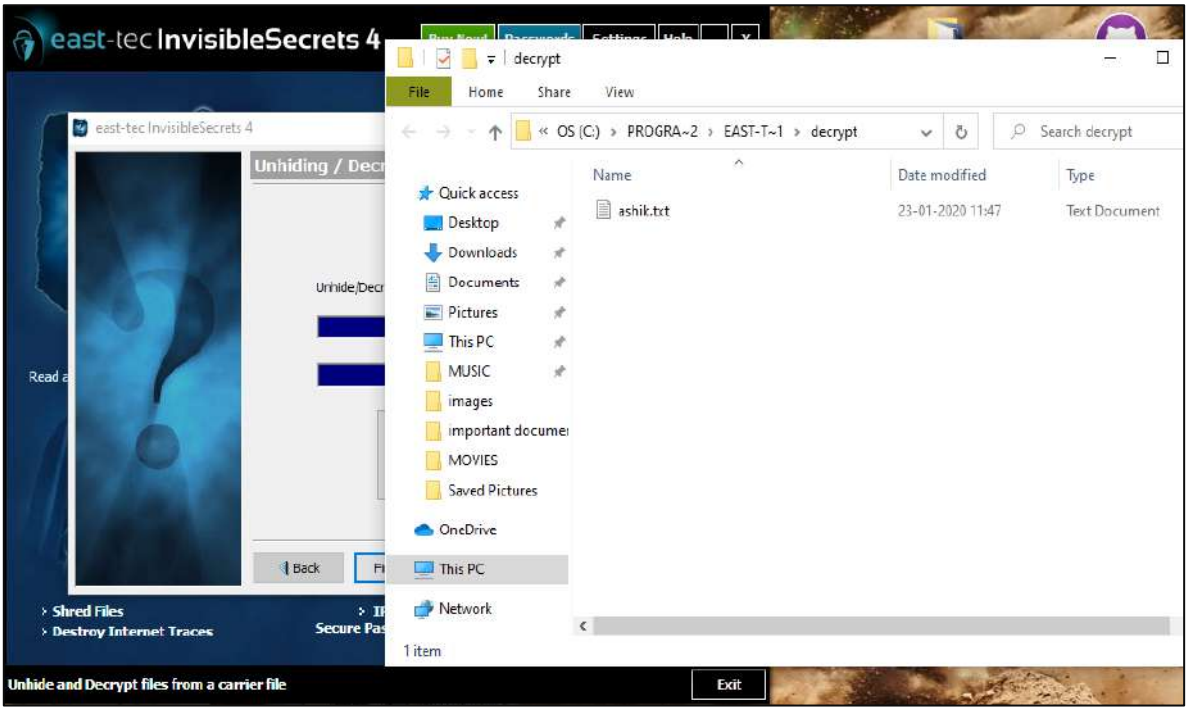

Figure 19: Opening the unhidden text document

Figure 20: Data inside the text document

SECOND TOOL: IMAGE STEGANOGRAPHY

ENCODING

Step 1: Type the text to be encoded into the image.

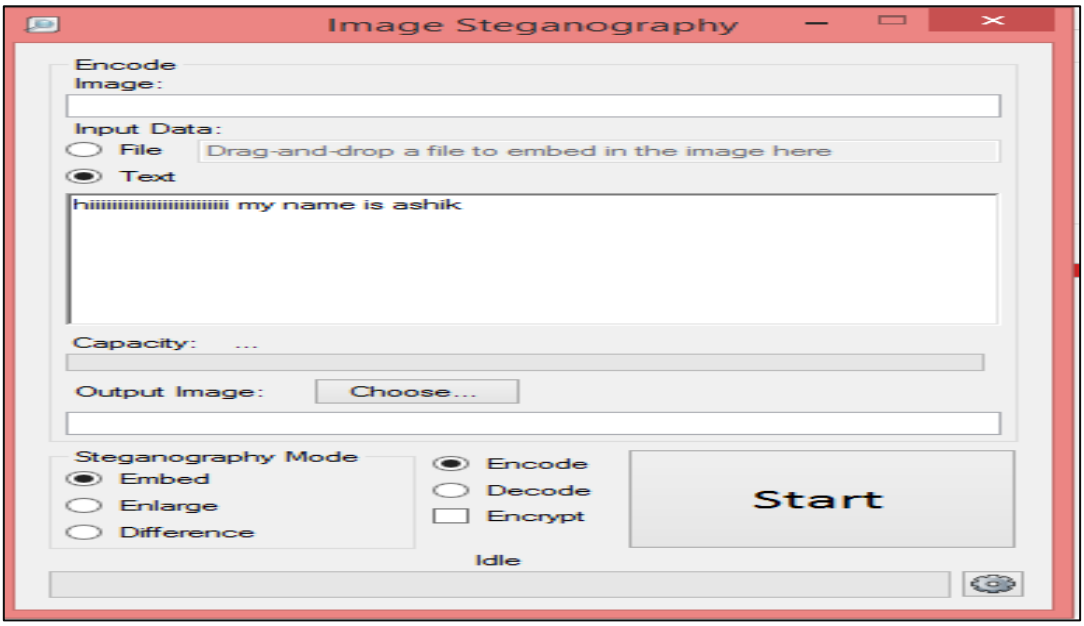

Figure 21: Type the text to be hidden

Step 2: Select the image where the text should be hidden and click on START. Encoding is completed.

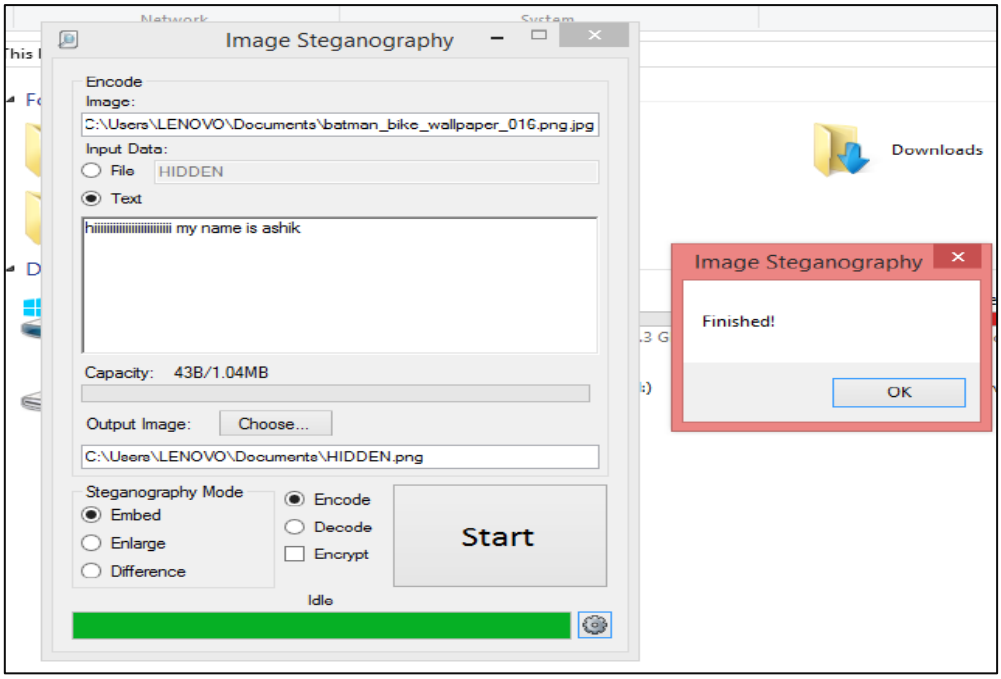

Figure 22: Select the image where the text should be hidden and encoded

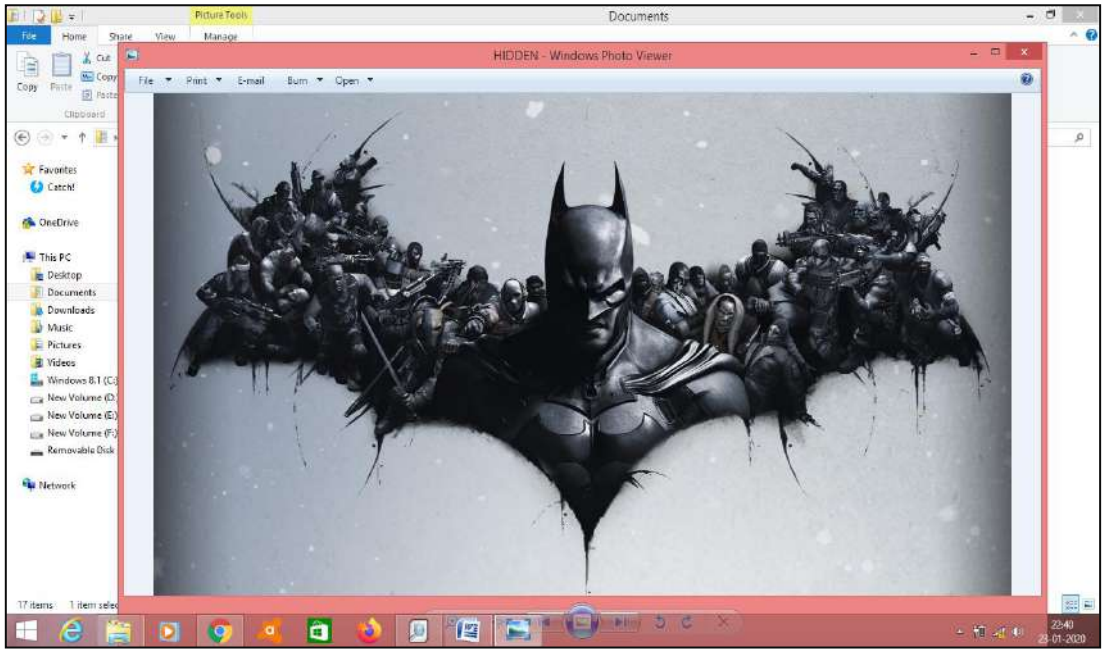

Figure 23: The hidden file

DECODING

Step 3: Select the image file from where the text should be decoded.

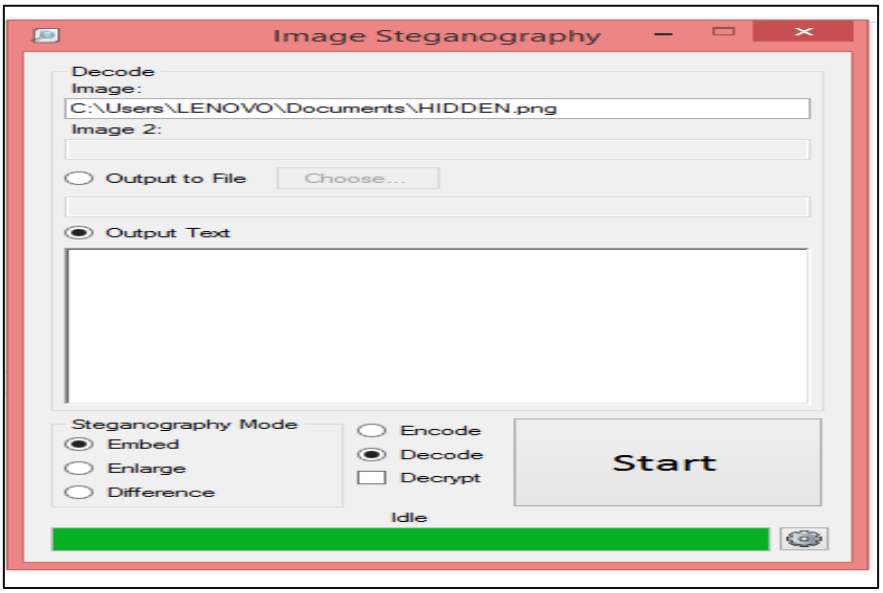

Figure 24: Select the image from where the text should be extracted

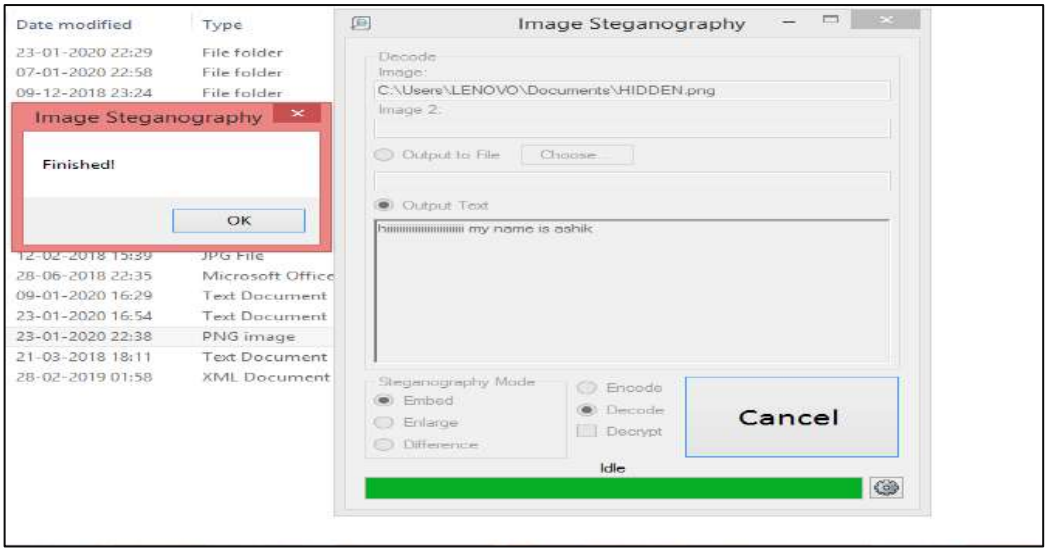

Figure 25: Decoding

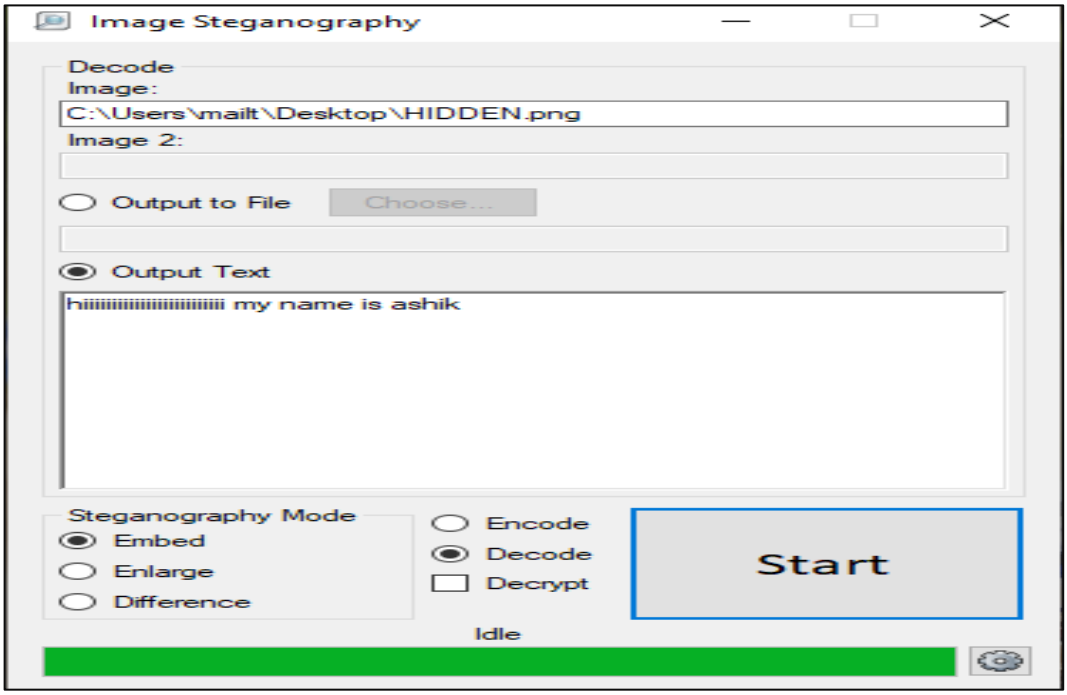

Figure 26: Data extracted

CHAPTER V: RESULT AND CONCLUSION

RESULT:

The hidden text data “hiiiiiiiiiiiiiiiiiiiiiii my name is ashik” successfully extracted from the image where it was hidden.

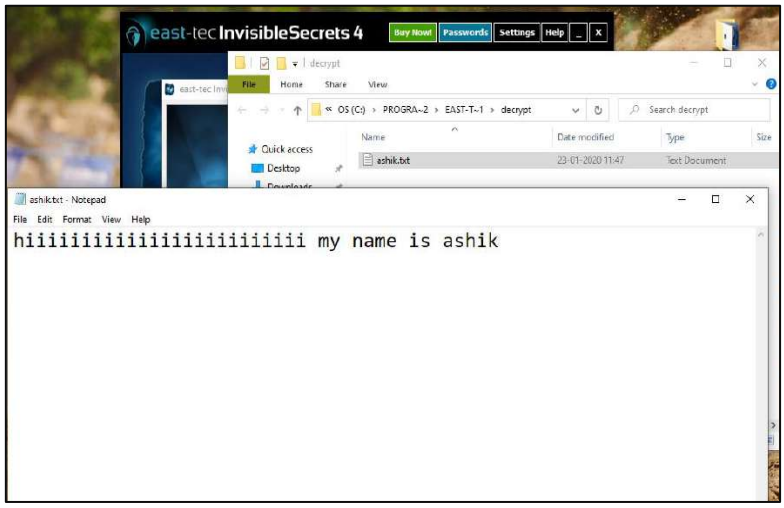

Figure 27: Using Invisible Secrets 4

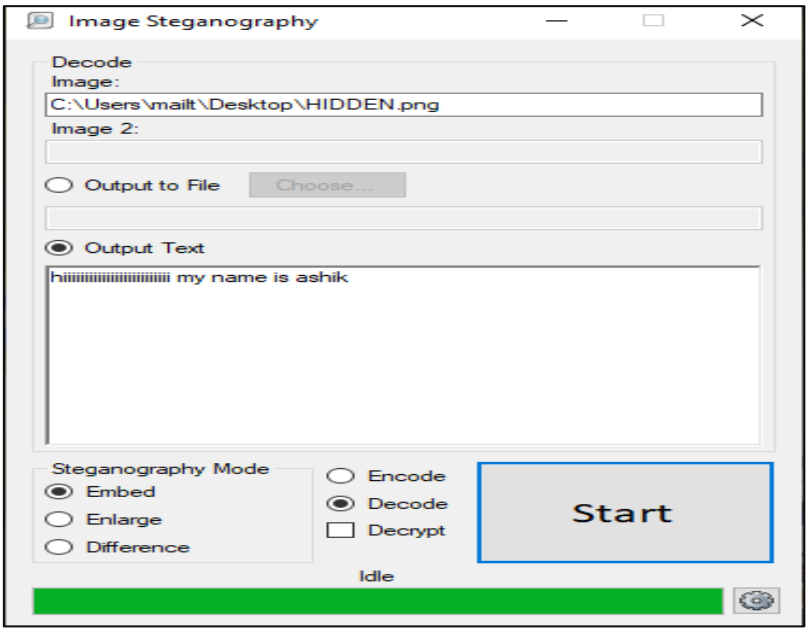

Figure 28: Using Image Steganography

CONCLUSION:

The steganalysis plays an important role in the current trend. Detection and analysis of steganographic images are the most important process in several real-time applications. The lack of training samples for steganalysis make these processes much complicated.

Data extracted by the two tools are same, but the first tool – "Invisible secrets 4" can read and extract the data only from .jpg format images. While the second tool – "Image steganography" can read and extract the data only from .png format image.

So far many steganalysis tools are present for reading and verifying different image format. A forensic examiner requires all tools, at the same time, space should not be wasted. The future scope of this project is invention of a single steganalysis tool which can read and verify all type of image format.

CHAPTER VI: REFERENCE

1. Zoran Duric, Michael Jacobs and Sushil Jajodia (2005) Information Hiding: Steganography and Steganalysis. Handbook of Statistics Volume 24, Pages 171-187
2. Arooj Nissar and A. H. Mir (2010) Classification of steganalysis techniques. Digital Signal Processing Volume 20, Issue 6, Pages 1758-1770
3. Konstantinos Karampidis (2018) A review of image steganalysis techniques for digital forensics. Journal of Information Security and Applications Volume 40, Pages 217-235
4. Abdelhamid Awad Attaby (2018) Data hiding inside JPEG images with high resistance to steganalysis using a novel technique: DCT-M3. Ain Shams Engineering Journal Volume 9, Issue 4, Pages 1965-1974
5. Yong Yang (2019) Steganalysis on Internet images via domain adaptive classifier. Neurocomputing Volume 351, Pages 205-216
6. https://www.sciencedirect.com/search/advanced?qs=steganalysis
7. https://www.geeksforgeeks.org/image-steganography-in-cryptography/
8. https://www.geeksforgeeks.org/image-steganography-using-opencv-in-python/
9. https://www.bing.com/search?q=invisible+secrets+4&form=EDGTCT&qs=PF&cvid=0f073c7a95134534993fbcad8247f568&refig=af01e0ccfafd475ae8ba22a04f84fb4f&cc=IN&setlang=en-US&plvar=0&PC=DCTS
10. https://www.east-tec.com/invisiblesecrets/
11. https://downloads.tomsguide.com/Invisible-Secrets,0301-14404.html
12. https://www.securitywizardry.com/index.php/products/forensic-solutions/anti-forensic-tools/invisible- secrets
13. https://sourceforge.net/projects/image-steg/
14. https://resources.infosecinstitute.com/steganography-and-tools-to-perform-steganography/#gref