ISSN No:-2456-2165

Analysis of Stenography

Udit Kalra
[1]B.Tech Scholar, Department of IT, Maharaja Agrasen Institute Of Technology, Delhi

Abstract:- Ransacking for just the right article is the foremost preferred and is sort of challenging to look out supported the current requirements. With the advancement in technology day by day, the occurrence of hacking is increasing very often. In these modern times, the area of cybersecurity is in desperate need of prevention from hacking. Gone are those days when firewalls were handy to protect your data. We require to try to do this individually to prevent cybercrime. In keeping with Kaspersky Labs, the standard cost of a cyber-breach is $1.23 million. This paper is on the brink to give the simplest possible ways to assist and helping to secure data by concealing. Security of data has become a vital challenge because of common vulnerabilities and day-to-day hacking. Data Hiding/ Encapsulation can be done in many ways. Some methods to protect your data are cryptography and steganography. Once you know that your data is safe and cannot be misused by someone, I think when might be less accentuated. Steganography, a non-orthographic and syllabic-ideographic orthography, maybe a model to research different hemispheric reading processes in Western subjects. I have thoroughly researched the most general stenographic methods and created a live environment to hide your message using an image. During this paper, I have discussed in detail what steganography is. What are its advantages? Its types and finally discussed about the environment which I created.

Keywords:- *Hacking, Cyber Security, Data Hiding, Application Security, Encapsulation, Cryptography, Steganography.*

I. INTRODUCTION

In this world of digitalization, several businesses and corporations are often the victims of malicious attacks by hackers who wish to steal customer data. Several companies understand the use of the word protection and as a result, they use various cryptographic techniques to encrypt their data and decrypt it in future when required to be used. A minute change or a minute error can cause colossal damage [16]. Therefore handled carefully to allow the best possible results. Many researchers try to search for a praiseworthy solution to unravel these problems.

The growing use of the web must store, send and receive personal information in an exceedingly secured manner. For this, we may adopt an approach that may transfer the data into different forms through encryption and then convert it into the original format using decryption [4], [6], [9]. However, this method has a disadvantage. The disadvantage is that if someone gives sufficient time, then the person can easily decrypt the encrypted text.

To overcome this issue data is embedded within some digital media in such a way that nobody can easily extract it. This better solution is stenography.

Steganography is the practice of hiding a message, an image, a file or any significant data within another message, image, or file to make sure it is safe.

Unlike cryptography, stenography's goal is to thoroughly hide the presence of any data rather than hiding its content. Imperceptibility, embedding dimensions and robustness are the major problems with image steganography.

The main objective of this project is to classify the different types of stenographic methods, their advantages and their implementation [16]. This paper has been divide into many sections. The previous one was abstract. Section I is that the introduction of the subject. Section II is about Related Work. It contains information about the topic and some work related to this paper. In, Section III there is a comparison between stenography and cryptography. Section IV is about the methodology of stenography is performed. Section V is about the implementation and result. It contains snapshots of how encryption and decryption were done. Section VI is all that says the conclusion and future scope on my research. In the end, there are some References to some other research papers.

II. RELATED WORK

Stenography's first use has been traced back to 440 BC when ancient Greece people wrote messages on wood and coated it with wax, which acted as the means of covering [9]. Also, Romans used various types of Invisible In1ks. And to decipher these hidden messages, light or heat were the means used. During World War II, the Germans introduced microdots. Here, they reduced the size of every file to the size of a dot and attached it with the paperwork. Now, we have many modern stenographic techniques and tools to make sure that our data remains secret [14]. The most suitable cover media for stenography is image stenography. Other types of stenographic methods are text, video, audio and network stenography.

Types of Stenography

1. Text Stenography

Text Steganography, as the name suggests, means hiding information inside the text files [2], [17]. It involves

process like changing the form of existing text, changing terms within a text, creating random character sequences, or making use of context-free grammars to come up with readable texts [7]. Different methods accustomed to covering the data within the text are Format Based Method, Random and Statistical Generation, and Linguistic Method.

2. Audio Stenography

In audio steganography, the information is hidden inside an audio signal which modifies the binary sequence of the analogous audio file [17]. Hiding a secret message inside the audio is a way tougher process than compared with others like Image or Text Steganography [7]. Different methods accustomed to covering the data with audio include Least Significant Bit Encoding, Parity Encoding, Phase Coding and Spread Spectrum. In this method, the data is hidden with WAV, AU, and MP3 type sound files.

3. Video Stenography

In Video stenography, the information is hidden inside a video type format [17]. The advantage of this type of stenography is that a lot of data can be hidden, and the reason is the size and the fact that it is a moving stream of images and audios. One can say that this is the combination of Image Steganography and Audio Steganography [7]. Two main categories of Video Steganography comprise: Embedding data in uncompressed raw video and compressing it later or Embedding data directly into the compressed data stream.

4. Network Stenography (Protocol Stenography)

In this stenography, the information is embedded within network control protocols utilized in data transmission like TCP, UDP, ICMP and more. One can use this steganography in some covert channels that, can be easily found within the OSI model [7]. An example, one can hide information within the header of a TCP/IP packet in some optional fields.

5. Image Stenography

Image Steganography means hiding information inside the image files [5]. In the digital type of steganography, image stenography is a widely used cover source because there are a large number of bits present in the digital description of an image. Different methods accustomed to covering information with images include Substitution, Masking and Filtering, Transform Technique, and Least Significant Bit Technique [10], [11].

The substitution method commonly doesn't expand the scale of the file [4], [6]. Depending on the scale of that hidden image, it eventually causes a coherent change from the unmodified variant of the image. The Least Significant Bit (LSB) insertion technique is an approach for securing data in a very cover image. When operating a 24-bit image, one tiny bit of each of the first color components is used for LSB [12], [18]. The masking and filtering techniques start with the interpretation of the image. Subsequent, we discover the various places where the hidden message is combined to hide the image, and lastly, we embed the information in a particular area. In addition, to the above three techniques for message hiding, the transform technique has been employed in embedding the message by changing coefficients during a transform domain.

After going through these five types of stenography, I created an environment that works on Image stenography. Here one can store a message in an image, maintain more security and use comparatively less space.

III. STENOGRAPHY AND CRYPTOGRAPHY

Stenography and cryptography are closely related. Cryptography jumbles messages in such an order that one cannot understand them [3]. Whereas in steganography, the message is hidden so that there is no awareness of the existence of a message. In cryptography, the structure of data can be altered, whereas, in stenography, the structure of data remains the same. Stenography supports only Confidentiality and Authentication whereas, Cryptography supports all Confidentiality, Authentication, Data Integrity and Non-repudiation [15]. The message in stenography may or might not be encrypted. If it's encrypted, then a cryptanalysis technique is applied to extract the message. Sometimes, sending an encrypted message can arouse suspicion while an invisible message will not do so. But, both methods combined can provide better protection of a message. In case one method fails the message can be detected. But, it will be of still of no use because it is also encrypted using the second method.

IV. METHODOLOGY

In this section, we discuss a method for image hiding where we store our message in an image file. The primary objective is to use the steganography technique to provide more security and simultaneously using less storage [1].

The tool creates a canvas with an image uploaded and an identically sized canvas with the text entered by the user. It then searches through every pixel of the text canvas and if it sees black, it knows the pixel its viewing is also a component of the message. It'll find the pixel at the same point in your image canvas and ensure that the green value of the RGB ends in an exceedingly very 7. If it sees white or transparent, it knows that it is not on the text entered and can confirm the identically located pixel on your image canvas's green value doesn't end in 7. After this has been performed on the whole image, we now have a picture where every pixel's green value doesn't end during a 7, except where it'll spell a message. The decode function reverses the above process by using the pixels of the uploaded image as it hides any pixel where it does not find any green value ending at 7.

The working of this model is quite simple. In the first step, the user has to enter a message in a text area. After entering that message, the user has to upload an image from his system. Once that image is uploaded, the text and the image overlap, and we can only see the image. Dimensions of both text and image are the same, which means their width and height are the same so that only the image is visible. This phase is called the encryption phase.

After this, the user has to download this image. Once downloaded, the user can decrypt to get the hidden message. For decryption, the user has to upload the downloaded image, and once it is done, the entered message is displayed as the output.

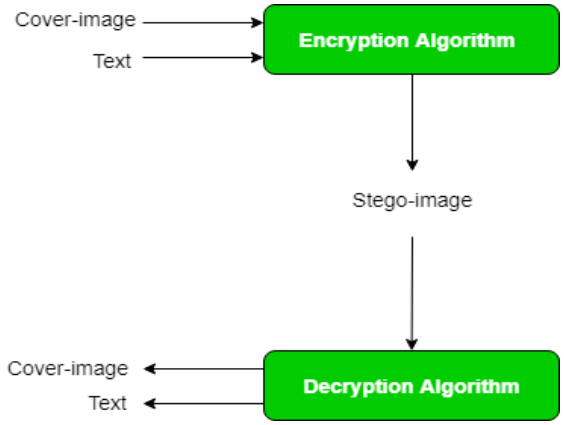

Fig 1. Process of Image Stenography [19]

V. IMPLEMENTATION AND RESULT

[13] The following diagram makes easier to grasp how we proceeded:-

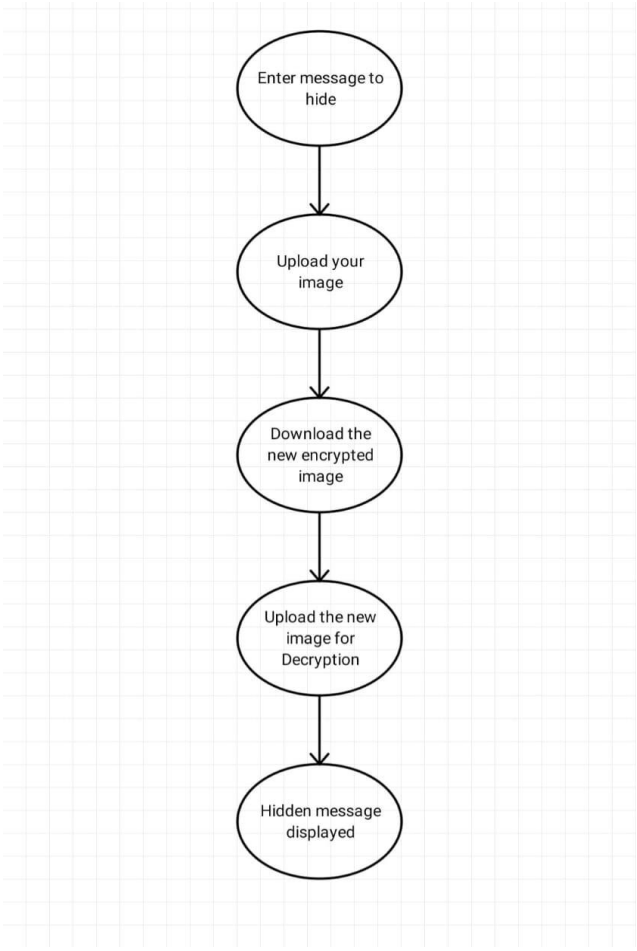

Fig 1. Working of the project

These are the steps one needs to follow:-

1. Enter your message :-

A text area is displayed, and the user has to enter the message which he/she wants to hide.

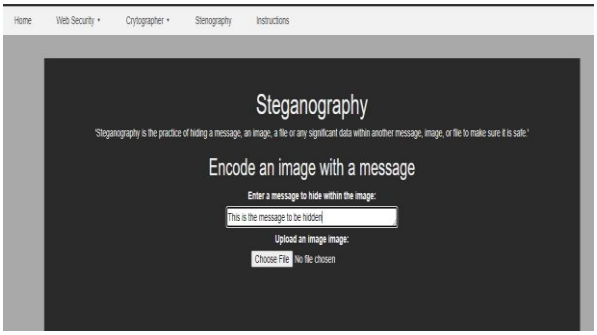

Fig 2. Entered a message in the text area- "This is the message to be hidden"

1. **Upload your image:-**

After entering the text, the next step is to upload an image to perform encryption.

Fig 3. Uploaded image- "my image.jpeg"

2. **Download the encrypted image:-**

Once the image is uploaded, the text and the image overlap, both having equal dimensions in terms of height and width. After this, the user has to download the encrypted image.

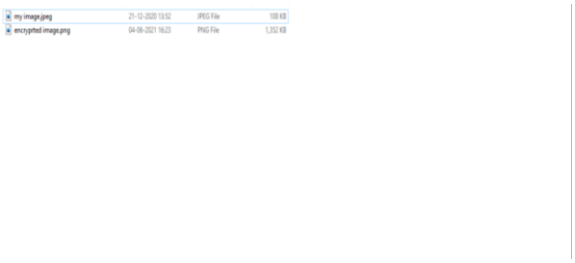

Fig 4. Downloaded the image and saved as- "encrypted image.png"

3. **Upload the new image for decryption:-**

Once downloaded, the user can decrypt the image to get the hidden message. For decryption, the user has to upload the downloaded image.

ISSN No:-2456-2165

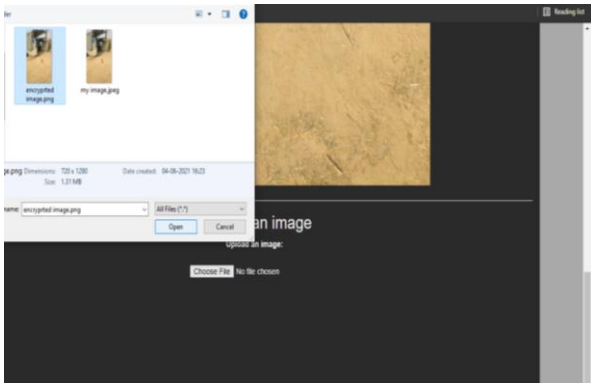

Fig 5. Uploading the encrypted image for decryption.

4. Hidden message displayed:-

Once the encrypted image is uploaded, decryption takes place, and the hidden message is displayed.

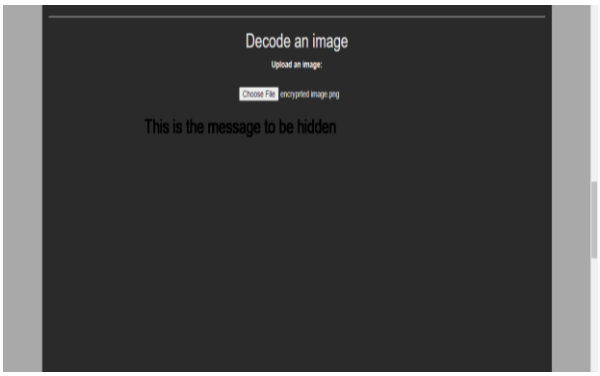

Fig 6. Hidden message displayed

VI. CONCLUSION & FUTURE SCOPE

In this paper, we have discussed five types of different methodologies for image hiding based on steganography [1]. Steganography is beneficial for hiding messages for transmission. Steganography's purpose is to hinder the transmission of malicious data. When properly implemented, steganography is usually very difficult to detect but is not impossible. Digital image stenography and others are constantly growing in both use and application and will continually develop new techniques to provide better protection.

In the future, the principal use of stenographic techniques will presumably be lying within the field of digital watermarking [3]. Content providers are continuously trying to protect their copyrighted works against unauthorized distribution and digital watermarking. Stenography may provide a way of tracking the owners of those who are using these unlawful means. Another possible use of these stenographic techniques in the future can be hiding data on the network in case of a breach, Posting secret communications on the net to avoid transmission, and more.

REFERENCES

[1]. Rajesh Kumar Tiwari, and Gadadhar Sahoo, "Some New Methodologies for Image Hiding using Stenographic Techniques"
[2]. Donovan Artz "Digital Steganography: Hiding Data within Data"
[3]. Arvind Kumar, and Km.Pooja, "Stenography- A Data Hiding Technique"
[4]. M.M Amin, M. Salleh, S. Ibrahim, M.R. Katmin, and M.Z. I. Shamsuddin, "Information hiding using Steganography"
[5]. Mehmood, and Shah, "An overview of image steganography"
[6]. Bret Dunbar, "A Detailed Look at Steganography techniques and their use in an Open Systems Environment"
[7]. Harjit Singh, "Analysis of Different Types of Steganography"
[8]. J. L. Arnott, A. F. Newell and A. C. Downton, "A comparison of plan type and stenograph for use in speech transcription for the deaf"
[9]. Fabien A.P. Petitcolas, R.J. Anderson, and M.G. Khun, "Information Hiding- A Survey"
[10]. Mehdi Hussain, and Mureed Hussain, "A Survey of Image Steganography Techniques"
[11]. S Uma Maheswari, and Jude Hemanth D "Different methodology for image steganography-based data hiding"
[12]. Rajesh Kumar Tiwari, and Gadadhar Sahoo, "Some New Methodologies for Image Hiding using Stenographic Techniques"
[13]. Chin-Chen Chang, Iuan-Chang Lin, and Yaun-Hui YU, "A new Steganographic method for color and gray scale image hiding"
[14]. Venkatraman. S, Ajith Abraham, Marcin Paprzycki "Significance of Steganography on Data Security"
[15]. Hans Delfs, and Helmut Knebl, "Introduction to Cryptography"
[16]. Udit Kalra, "CSRF and XSS Attacks and Defense Mechanisms"
[17]. Navneet Kaur, and Sunny Behal "A Survey on various types of Steganography and analysis of Hiding Techniques"
[18]. K.B. Raja, C.R. Chowdary, Venugopal K R, and L.M. Patnaik " A Secure Image Steganography using LSB, DCT, and Compression Techniques on Raw Images"