Scientific Journal of Impact Factor (SJIF): 5.71

e-ISSN (O): 2348-4470
p-ISSN (P): 2348-6406

International Journal of Advance Engineering and Research Development

A National Conference On Spectrum Of Opportunities In Science & Engineering Technology
Volume 5, Special Issue 06, April-2018 (UGC Approved)

IMAGE STEGANOGRAPHY

Ruchi Iche1, Ankita Satao2, Ashwini Ingle3,Chayya Wanare 4

[1,2,3,4] Computer Science & Engg, STC, Khamgaon

Abstract — *Steganography is the art of hiding information in other information. It is one of the methods used for the hidden exchange of information and it can be defined as the study of invisible communication that usually deals with the ways of hiding the existence of the communicated message. Steganography is the process of hiding a secret message within a larger one in such a way that someone cannot know the presence or contents of the hidden message. There is a key object that will 'carry' the hidden message. Many different carrier file formats can be used, but digital images are the most popular because of their frequency on the internet. Many carrier can be referred to a digital image, an mp3, even a paintings and among and etc. A key is used to decode/discover the hidden message. For hiding secret information in jpg format, there exists large variety of steganography techniques some are more complex than others and all of have both strong and weak points. In this way, if successfully steganography is achieved, the message does not attract attention from attackers and hackers. Using steganography, information can be hidden in different embedding mediums, known as carriers. These carriers can be images, audio files, video files, and text files. The focus in this paper is on the use of an image file as a carrier, and hence, the taxonomy of current steganographyc techniques for image files has been presented. These all techniques are referred and used and far discussed not only in terms of their ability to providing security to information in image files but also according to how much information can be hidden, and the robustness or toughness to different image processing attacks. This paper is present to give an overview of image steganography, and know its uses and techniques.*

Keywords- *cryptography,steganography, image steganography.*

I. INTRODUCTION

The word steganography means" covered in hidden writing". The basic need of every growing area in today's world is communication, computers and internet are major communication media that connect with whole world.. Everyone wants to keep the inside information of work to be secret and safe. But the safety and security of long-distance communication is an issue.We use many insecure pathways in our daily life for transferring and sharing information using internet or telephonically, but at a certain level it's not safe. The need to solve this problem is developed steganography schemes. Steganography is a powerful tool that provides high level of security, particularly when it is combined with encryption [1]. Steganography differs from cryptography , we will see this in detail view section.In some cases, sending encrypted information may catch attention, while invisible information will not. Accordingly, cryptography is not the best solution for secure communication; it is only part of the solution. Both sciences can be used together to better protect information. In such case, message cannot be recover even if steganography fails, because a cryptography technique is use here [2]. Watermarking and fingerprinting are also technologies related to steganography, are basically used for intellectual property protection [3]. The message firstly be encoded by sender into graphic file, then receiver needs to decode this file with secret keyword. The watermark is hidden in the host data and removed only with demeaning host medium. This method keeps the data accessible, but permanently marked [4]. In this case, it becomes easy for the property owner to identify such customers who give themselves the right to violate their licensing agreement when they illegally transmit the property to other groups [5].The performance of a steganographic system can be measured using several properties which are in evaluation section.steganographic capacity means how many information can safely hide in statistically detectable objects [6]. Image and audio files satisfy this requirement particularly well [3]. This paper is organized as follows. Section 1abstract. Section 2 introduction .Section 3 presents Requirement analysis. Section 4 Detail view. Section 5 describes stapes for encoding and decoding. Section 6 describes advantages, application and evalualuation. Section 7future scope of steganography. Section 8arrived at conclusions.

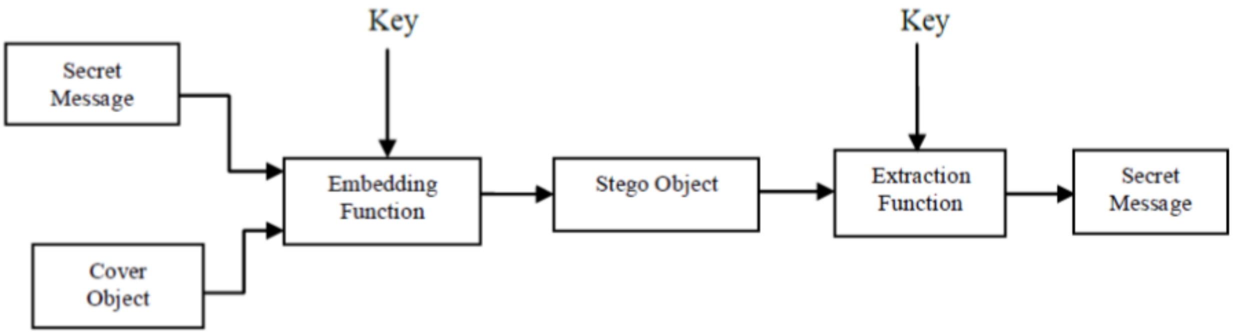
II. Requirement Analysis

2.1.1 Sender

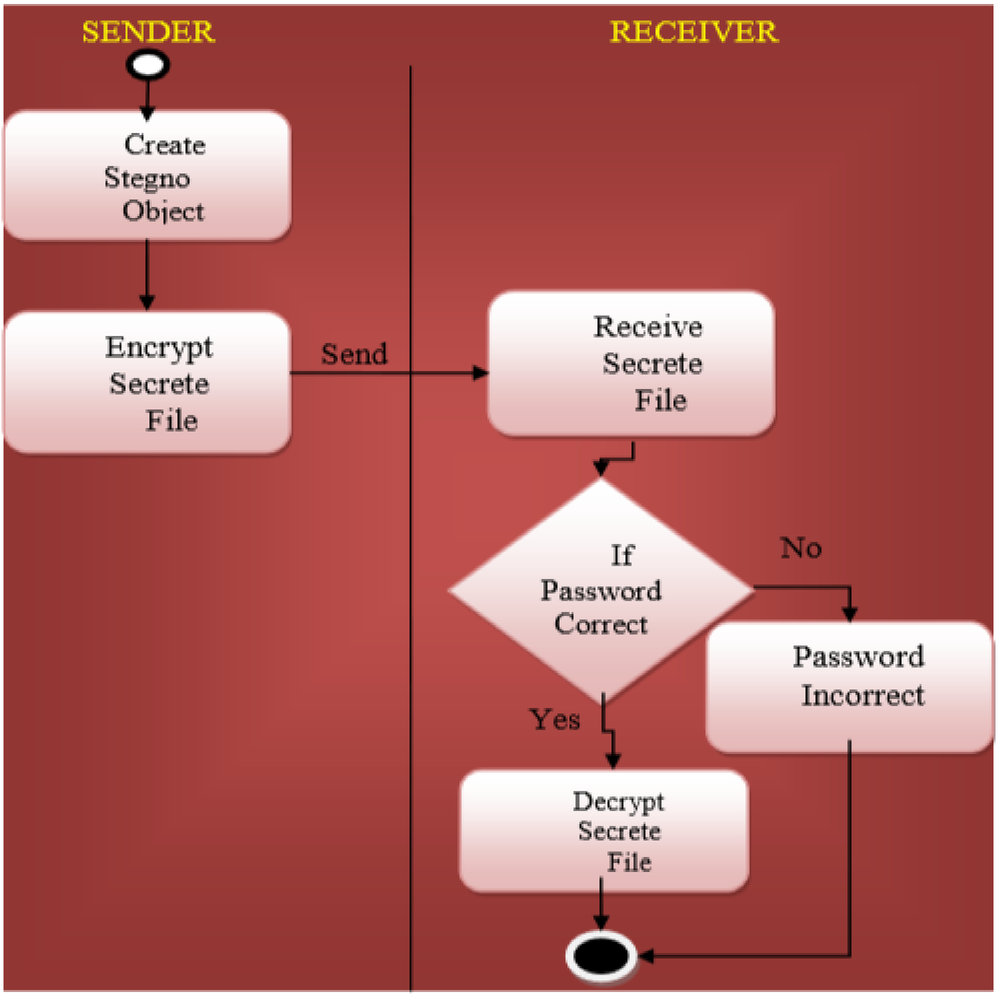
Sender is an authorized person who hide the secret message with the help of stegano image and he has ahas authority to send important information to the receiver with the help of stegano image.

2.1.2 Receiver

Receiver is also an authorized person who have authority to access important information which is provided by sender in a secure manner. Receiver require a security code to access the provided data. A model of the steganography process with cryptography is illustrated in Fig. 1



2.2 Activity Diagram



III. Detail view

3.1 Cryptography

The field of cryptography has a rich and important history, ranging from pen and paper methods, to specially built machines, to the mathematical functions that are used today. In this paper only brief discussion that is essential for knowledge transfer has been presented. Cryptology is the science of coding and decoding secret messages [8]. It is usually divided into cryptography, which concerns designing cryptosystems for coding and decoding messages. It states that the term cryptography generally refers to the collection of cryptographic mechanisms that include:

- Encryption and decryption algorithms
- Integrity check functions
- Digital signature schemes

3.2 Steganography

Steganography is a technique used to transmit a secret message from a sender to a receiver in this way such that an unauthorized person does not able to access the secret message. Generally this can be done by encoding the secret message within another digital medium such as text, image, audio or video. [9]. The word steganography is of Greek word that means “concealed writing” from the Greek words steganos meaning “covered or protected”, and graphie meaning “writing” [2]. The first recorded use of this term is by Johannes Trithemius in his Stegano-graphia. It is a high security technique for long data transmission. There are various methods of steganography:

- Least significant bit (LSB) method
- Transform domain techniques
- Statistical methods
- Distortion techniques

3.3 image steganography

The most popular file formats used insteganography are images. They are known as non-causal medium, because the possibility is that toaccess any pixel of the image at randomly. This supports to hidden information could remain invisible to the eye. The image steganography techniques will exploit "holes" in theHuman Visual System (HVS).

3.4 Image Files

An image is defined as an arrangement of numbers and such numbers usually stand for different light intensities in different parts of the image [7]. The numeric description takes the form of a lattice where the individual points given the name 'pixels'. Pixels are displayed horizontally, rowby row. In a color scheme, the number of bits is known as the bit depth and this basically refers tothe number of bits assigned to each pixel [3]The most prominentimage formats, exclusively on the internet, are the graphics interchange format (GIF), jointphotographic experts group (JPEG) format, and to a lesser degree, the portable network graphics(PNG) format. The important issue to touch here is that most of the steganographic techniquesattempt to exploit the structure of these formats. However, some literary contributions use thebitmap format (BMP) simply because of its simple and uncomplicated data structure [8, 9].

IV. STEPS

4.1 Steps For Encoding

Step 1: For Encryption select Encrypt Image tab option.

Step 2: For load image click on button “File” that is next to the Load cover Image. The file open dialog box will displays, select the Image file, which you want to use hide information and click on Open button.

Step 3: Again the file open dialog box will appear, select any type of text or file whatever you want to hide with the image and click on ok button.

Step 4: After this process the password window will be appear for encoding, user has to give minimum 8 character length of password which is also encoded/hided in image.

Step 5: Now click on “Encrypt” button, it will open the save dialog box which ask you to select the path to save the image. The default format of image file is any extension of image.

4.2 STEPS FOR DECODING:

Step 1: Select the Decryption Image tab option.
Step 2: The decrypted image file display.
Step 3: Then the Same password window will be appear .The password must be given by user at decoding code if password is correct then encrypted text is display else the password is not valid it display the invalid password.
Step 4: Now click on Decrypt button, it will decrypt the image, the hidden data and text is saved into selected folder. The message for successful decryption is displayed.

V. ADVANTAGES

- Fast and easy way to send a secure stuff.
- Easy process to encrypt text on image
- Can be added on any images that it is like other images only.
- Difficult to detect and only receiver can detect.
- Provides better security for sharing data in LAN,MAN & VAN

VI. APPLICTION

- Confidential communication and secret data storing.
- Protection of data alteration.
- Access control system for digital content distribution.
- Media database system.

VII. EVALUATION OF DIFFERENT TECHNIQUES

All the above mentioned algorithms with respect to image steganography is depend on three parameters are as follows :Undetectability (imperceptibility): this parameter is the first and the primary requirement; itrepresents the ability to avoid detection, where the human eye fail to notice it.alter the image in a way that it is detectable by the statisticaltests. Truly secure steganographic techniques should be undetectable neither by the human eye nor by the statistical attacks.Robustness: it is the second parameter that measures the ability of the steganographic technique to survive the attempts of removing the hidden information. Such attempts include, image manipulation, data compression, and image filtering.Hiding information via steganographic techniques that modify the elements in the visual image results in a stegoimage that will survive rotation, scaling and much lossy compression like JPEG.

VIII. FUTURE SCOPE

In the present world, the data transfers using internet is rapidly growingbecause it is so easy as well as fast to transfer the data to long distance destination. So,many individuals usersand business people use to transfer business documents,important information using internet via gmail, whatsapp or any transferring application. Security is anvery important issue while transferring the data using internetbecause any unauthorized individual can hack the data and make it uselessor obtain information un- intended to him. The future work on this project is to improve the compression ratio of theimage to the text. This project can be extended to a level such that it can beused for the different types of image formats like .bmp, .jpeg, .gif etc., in thefuture. The security using Least Significant Bit Algorithm is good but we canimprove the level to a certain extent by varying the carriers as well as usingdifferent keys for encryption and decryption.

IX. CONCLUSION

As all of the methods evaluated required either color reduction of the original images palette or color substitution in the stegeno image, they all had their own weaknesses as the steganoed image inevitably suffered some distortion from the steganography process.Steganography is a fascinating and effective method of hiding data that has been used throughout history. Methods that can be apply to encode and decode stegano file, but the first step are awareness that such methods even exist. There are many good reasons as well to use this type of data hiding, including watermarking or a more secure central storage method for such things as passwords, or key processes. Regardless, the technology is easy to use and difficult to detect. The more that you know about its features and functionality, the more ahead you will be in the game.

X. References

[1] S.A. Halim and M.F.A Sani. "Embedding using spread spectrum image steganography with GF ( )," in Proc. IMT-GT-ICMSA, 2010, pp. 659-666.

[2] N.N. El-Emam. (2007). "Hiding a large amount of data with high security using steganography algorithm." Computer Science. [On-line]. 3(4), pp. 223-232.

[3] T. Morkel, J.H.P. Eloff, and M.S. Oliver. "An overview of image steganography." in Proc. ISSA, 2005, pp. 1-11.

[4] L. Chun-Shien. Multimedia security: steganography and digital watermarking techniques for protection of intellectual property. USA: Idea Group Publishing, 2005, pp. 1-253.

[5] R.J. Anderson and F.A.P. Petitcolas. (1998, May). "On the limits of steganography." IEEE Journal of Selected Area in Communications. [On line]. 16(4), pp. 474-481. Available: http://www.cl.cam.ac.uk/~rja14/Papers/jsac98-limsteg.pdf [Jun., 2011].

[6] I.J. Cox, M.L. Bloom, J.A. Fridrich, and T. Kalkert. Digital watermarking and steganography. USA: Morgan Kaufman Publishers, 2008, pp. 1-591.

[7] N.F. Johnson and S. Jajodia. (1998, Feb.). "Exploring steganography: seeing the unseen." IEEE Computer Journal. [On line]. 31(2), pp. 26-34. Available: http://www.jjtc.com/pub/r2026.pdf [Jun. 2011].

[8] A. Cheddad, J. Condell, K. Curran and P.M. Kevitt. (2010). "Digital image steganography: survey and analysis of current methods." Signal Processing Journal. [On line]. 90(3), pp. 727-752. Available: http://www.abbascheddad.net/Survey.pdf [Aug. 2011].

[9] M. Fortrini. "Steganography and digital watermarking: A global view." University of California, Davis. Available: http://lia.deis.unibo.it/Courses/RetiDiCalcolatori/Progetti00/fortini/project.pdf . [June 2011].