3rd National Conference on Green Technology and Science for Sustainable Development
© 2020 IJSRST | Volume 5 | Issue 6 | Print ISSN: 2395-6011 | Online ISSN: 2395-602X
International Journal of Scientific Research in Science and Technology

A Review on Image Steganography

Sarita T. Sawale*[1], Shweta J. Patil[2], Anju S. Sharma[3]
*[1]Department of Information Technology, Anuradha Engineering College, Chikhali, Maharashtra, India
[2]Department of Information Technology, Anuradha Engineering College, Chikhali, Maharashtra, India
[3]Department of Information Technology, Anuradha Engineering College, Chikhali, Maharashtra, India

ABSTRACT

There is a lot of progress in the Internet technology, there was huge text as well as multimedia data internet transfer. With this data, security is vital need. Steganography and cryptography are data security techniques. Cryptography is defined as a method of concealing information by encrypting plain texts to encrypt texts or cipher text and later transferring it to the intended recipient using an unknown key, on the other hand, Steganography provides or says that security raises to a high level; encrypted text by hiding text, image or other formats. Watermark tags and fingerprints are: the other two technologies used in parallel with steganography; in the field of data hiding. Steganography can be integrated to increase the security of encrypted data. These paper present different techniques of image steganography in spatial and frequency domain. LSB modification techniques and DCT coefficients techniques are covered along with its application.

Keywords : Image, Steganography, Cryptography, Encryption, Data hiding, LSB, DCT, Security.

I. INTRODUCTION

There is large development in the communication field recently, hence the protection and confidentiality of information has become very important need for communication. Internet science and multimedia more rapidly improved and enhanced at your own expense, as well as using alternatives, images, videos, services. Huge information can be transferred through a network of computers and mobile devices. However, the security and privacy of data on the Internet does not depend on the mark, and the data may be captured by an unauthorized user. Therefore, ensuring the security and confidentiality of data transmission is a very important and current need. This requirement can be achieved by various methods such as Steganography and Cryptography [1].

Cryptography alone was not enough to provide different types of information over the Internet. This weakness of cryptography is becoming a source for extensively studying steganography to make information more secure. The literal meaning of the Greek word “stegos + graphics” means “cover + write” [2]. Steganography involves different types of different methods to hide information behind some of the data. Coverage data can be text, images that hide information, such as text and images. Hiding data, taking the object of the cover as an image, is referred to as image steganography. In digital steganography, images are widely used as a cover object because of the binary representation of pixel intensity, whose excess bits are used to hide information. Almost any media that can be encoded in a small stream can be hidden in a digital image. Steganalysis is a study of methods for extracting or removing the secret data which is hidden in some stego-media. Cryptanalysis is a set of method for finding the meaningful secret data from the cipher data. The work done in this paper is

on the methodology for combing together Steganography and Cryptography for images.

Watermark and fingerprints, among steganography-related technologies, are mainly used for intellectual property protection [3]. A digital watermark is a permanently built-in signal in digital data (audio, images, video, and text) that can be detected or extracted subsequently to confirm the accuracy of the data. The watermark is hidden in the host data so that it cannot be removed without clearing the host environment. Although this method keeps data available, it is always noted [4]. Information hidden in a watermark property is a signature that relates to the origin or ownership of the data to ensure copyright protection. In the case of fingerprints, different and special signs are embedded in the examples of work that are supposed to be received by different clients. In this case, it is clear to the owner of the intellectual property of clients who are entitled to breach their license agreement when they are unlawfully transferring the property to other groups [5].
In general steganography is classified into the following four types [6].

A. Image steganography
It is the process of hiding a secret image inside the cover image to make the cover image disappear and the cover image to be original [7-9].

B. Audio steganography
Digital audio files are used to hide a secret message, endlessly changing the binary sequence of an audio file known as audio steganography.

C. Video steganography
Video files can be defined as a collection of images and sounds, so most of the imported images and audio can be used and applied to digital video files. In fact, a large amount of confidential data that can be embedded within video files, as the video file is a moving stream of images and sounds.

D. Text steganography

Text spelling mainly refers to information that is hidden in text files. Text steganography involves everything from manipulating and modifying text formatting, changing words within text, generating and generating random sequences, or using contextual linguistic grammar to create readable texts.

II. IMAGE STEGANOGRAPHY

An image is picture that is created or taken from any source and stored electronically of any kind. The image can be described with images of vector graphics or other variants. An image stored in a disaster is sometimes called a bitmap. Image map files containing confidential information that are combined at different locations with hypertext links to the specified image. An image is defined as a set of multiple numbers, which is another form of light intensity in different areas of the image. Such digital pixels, gray scale images that use 8 bits for each pixel and allow to display 256 different colors or shades of gray. Digital color images are usually stored in 24-bit files and use the RGB color model, also known as real color. All colors have different fluctuations for the 24-bit pixels in the primary colors: red, green and blue. And each primary color represented by 8 bits. Thus, in one given pixel there can be 256 different quantities of primary color: red, green and blue.

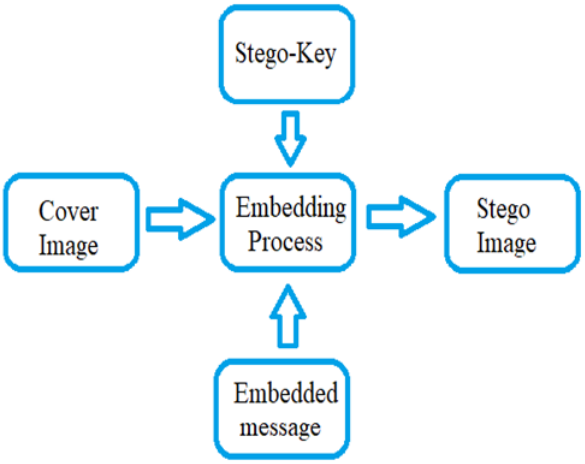

Fig.1 Basic Model of Image Steganography

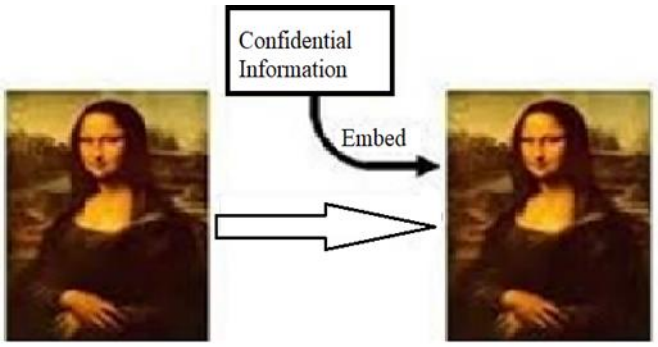

Fig. 2 Example of Image Steganography

III. IMAGE FORMATS

Image file formats are standardized means of organizing and storing digital images. There are 4 main formats in which to store images.

A. TIFF

TIFF stands for Tagged Image File Format.TIFF images are uncompressed and thus contain a lot of complete image data.

B. JPEG

JPEG stands for Joint Photographic Experts Group, which created this standard for this category of image format. JPEG files are the images that have been compressed to store a lot of material in a small-size file.

C. GIF

GIF is Graphic Interchange Format. This format compresses images but as dissimilar from JPEG, the compression is lossless.

D. PNG

PNG stands for Portable Network Graphics. It was formed as an open format to exchange GIF, because the patent for GIF was owned by one company and nobody else wanted to wage licensing fees. It also permits for a full range of color and better compression.

IV. IMAGE COMPRESSION

Image compression is the method of encoding or converting an image file in such a way that it consumes less space than the original file. The image has two kinds of compression: lossy compression and Lossless compression [10]. Lossless compression reduces a file's size with no loss of quality or excellence. The most common image has formats, such that the lossless compression is in GIF (abbreviated as graphic Interchange formats). Lossy file compression results in loss of data and quality from the original form. A lossy compression reduces the file by deleting some information, especially redundant information. When the file is compressed, only a fraction of the original information that is still available. In this case, the resulting image is expected to look like the original message. But not the same as the original. An example of an image format that uses such compression techniques as JPEG (abbreviated as a group of collaborative graphics experts) [11].

V. ATTACKS ON IMAGE STEGANOGRAPHY

While the purpose of Steganography is to hide messages, there exist several attacks that one may execute to test for Stenographic data. The power of a stenographic algorithm depends on its ability to successfully withstand attacks. Attacks and analysis of hidden data may take several forms: detecting, extracting, and disabling or destroying hidden data. An attack approach is dependent on what information is available to the steganalyst. A large number of attacks are implemented in steganography to evaluate see if digital media contains hidden data. Attacking stenographic algorithm is very similar to attacking cryptographic algorithms and similar techniques apply. As Fabien A.P. Petitcolas points out that there are six general protocols used to attack the use of Steganography

Classification of attacks based on information available to the attacker [12]

A. Stego-only attack

Only the steganography medium/object is available for analysis.

B. Known-carrier attack

The carrier, that is, the original cover, and steganography media/object are both available for analysis or are known.

C. Known-message attack

In this case, the hidden message is known and can be compared with the stego object/medium.

D. Chosen-stego attack

The steganography medium/object and tool (algorithm) are both available for analysis.

E. Chosen-message attack

Here a chosen message and steganography tool (or algorithm) is used to create steganography media for future analysis and comparison. The goal in this attack is to determine corresponding patterns in the steganography medium.

F. Known-steganography attack

The secret message, steganography medium/object and the steganography tool (algorithm) are known and available for analysis. Steganography elimination techniques is involved with steganalysis that try to eliminate or destroying the hidden information as the purpose is to break the cover communication, but not to render the legitimate channel unusable. The most common attacks based on this factor are [13]:

1) Destroy everything attack: This type of attack aims in destroying the message completely and the attacker might not even try to retrieve the message.

2) Random tweaking attacks: Here small changes in the files are added so that the message will be unreadable.

3) Add new Information: In some cases, the attackers might use the same technique of data hiding to embed a new message into the stego-file. The original message might be overwritten.

4) Reformat attack: A common way to destroy the information hidden in a file is by changing the file format. This type of attack can produce a lot of damages to the hidden message.

5) Compression attack: The attacker might compress the file which might result in the total loss of the secret message embedded in the file, because the compression algorithms tend to remove extra in-formation during compression. From the above, it is clear that if an attacker wants only to destroy the hidden message, he can do that very easily by combining some of the methods of attack presented above.

VI. EVALUATION CRITERIA FOR IMAGE STEGANOGRAPHY

All the above-mentioned algorithms for image steganography have different powerful and weak points and it is important to ensure that one uses the most suitable algorithm for an application. All steganographic algorithms have to follow with a few basic requirements. The most important requirement is that a steganographic algorithm has to be undetectable. The authors suggest a set of criteria to further define the imperceptibility of an algorithm. The requirements are given as follows:

A. Invisibility

The invisibility of a steganographic algorithm is the first and prime necessity, since the strength of steganography lies in its ability to be unobserved by the human eye. The moment that one can see that an image has been interfered with, the algorithm is negotiated.

B. Payload capacity

Unlike watermarking, which wants to insert only a small amount of copyright information, steganography aims at secreted communication and therefore requires enough inserting capacity.

C. Robustness against statistical attacks

Arithmetic steganalysis is the practice of detecting hidden information through applying statistical tests on image data. Many steganographic processes leave a 'signature' when embedding information that can be easily detected through statistical study. To be able to pass by a keeper without being detected, a steganographic algorithm must not leave such a mark in the image as be statistically important.

D. Robustness against image manipulation

In the communication of a stego image by trusted systems, the image may undertake changes by an active keeper in an attempt to remove hidden information. Image management, such as collecting or rotating, can be performed on the image before it reaches its destination. Depending on the manner in which the message is fixed, these manipulations may destroy the hidden message. It is desirable for steganographic algorithms to be strong against either mean or unintentional changes to the image.

E. Independent of file format

With many dissimilar image file formats used on the Internet, it might seem doubtful that only one type of file format is continuously communicated between two parties. The most powerful steganographic algorithms thus own the ability to embed information in any type of file. This also solves the problem of not always being able to find a correct image at the right moment, in the right format to use as a cover image.

F. Unsuspicious files

This requirement includes all characteristics of a steganographic algorithm that may affect in images that are not used normally and may cause suspicion. Abnormal file size, for example, is one property of an image that can result in further investigation of the image by a warden.

VII. TECHNIQUES USED IN IMAGE STEGANOGRAPHY

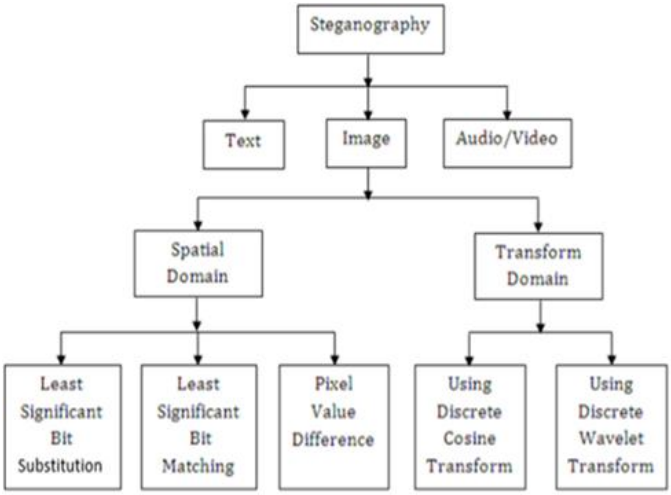

Fig.3 Image steganography techniques

There are two different methods for image steganography:

A. Spatial methods

The spatial domain steganography technique [14] used the pixel gray levels and colour values of the cover image directly for hiding and encoding the message bits, in such a manner that they are not visible by human vision system. These are the various techniques used till now in which pixel embedding has been done directly on the pixels, the methods usually varies in selecting the criteria of order of pixels. In spatial technique, the most common method used is LSB substitution method.

1) Least significant bit (LSB):

This method is a common, simple method to embedding information in a cover file.

In steganography, LSB substitution method is used. I.e. since every image has three mechanisms (RGB). This pixel data is stored in encoded format in one byte. The first bits containing this information for every pixel

can be changed to store the hidden text. For this, the initial condition is that the text to be stored has to be smaller or of equal size to the image used to hide the text.

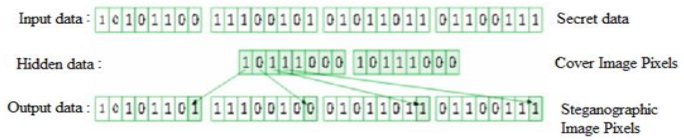

Fig. 4 Example of LSB

LSB based method is a spatial domain technique. But this is weak to collecting and noise. In this method, the MSB (most significant bits) of the message image to be secreted are stored in the LSB (least significant bits) of the image used as the cover image.

It is known that the pixels in an image are kept in the form of bits. In a gray scale image, the intensity of separate pixel is stored in 8 bits (1byte). Similarly, for a colour (RGB-red, green, blue) image, each pixel wants 24 bits (8bits for each layer).

The Human visual system (HVS) cannot detect changes in the colour or strength of a pixel when the LSB bit is changed. This is psycho-visual redundancy since this can be used as an advantage to store information in these bits and yet notice no major change in the image.

Steps used in LSB steganography:

a. Steps for hiding message image:
1. Read the image to be used as protection image. Noise is added to make it easier to cover changes due to embedding the message image.
2. Read the image to be used as message image.
3. Separate the bit planes of each image.
As it is known that the LSB (least significant bit) plane contains the least data linked with any image, and the MSB (most significant bit) plane contains most of the shape, colour information of an image.

It is generally ideal to replace up to 4 least bit planes of the cover image, with the upper 4-bit planes without revealing variations in the resultant image. Lesser number of bit planes from the message image could be used, but the regained image would become partial and loses information.
4. Replace the least 4-bit planes of cover image with the 4 most significant bit planes from message image.
5. Get the resultant Steganographic image by recombining these bit planes.

b. Recovering message image:
1. Read the Steganographic image.
2. Extract the essential number of bit planes of the image.
3. Recombining the lower four-bit planes would give the retrieved message image.

2) Least Significant Bit Matching:
LSBM pays a minor modification to LSB. If the secret bit does not match the LSB of the cover image, then +1 or -1 is casually added to the corresponding pixel value. Statistically, the probability of increasing or decreasing for each altered pixel value is the same and so the noticeable asymmetry objects introduced by LSB replacement can be simply avoided. Therefore, the common methods used to detect LSB replacement are totally unsuccessful at detecting the LSBM.
3) Pixel Value Difference:
The PVD-based methods [15] enhanced the embedding capacity without introducing obvious visual artifacts into stego images. The method involves, finding the number of embedded bits from the difference between the pixel and its neighbor. The larger the difference, the more secret bits can be embedded. PVD Technique is more imperceptible than LSB-Technique (when having same embedding capacity.

B. Transform Domain
The transform-based techniques instead of embedding the data into the bits of the pixel's intensities directly,

image first get transformed using domain like frequency domain (DCT, DFT), wavelet domain (DWT)etc. and then data is hidden behind the transformed image and then the image is retransformed. Since it is a complex way of hiding secret information behind image, image manipulation becomes harder for the warden. The various transform domain techniques are:

1) Using Discrete Cosine Transform:

DCT [16] is a general orthogonal transform for digital image processing and signal processing. Important features include high compression ratio, small bit error rate, good information integration ability and good synthetic effect of calculation complexity. DCT allows an image to be broken up into different frequency bands namely the high, middle and low frequency bands to embed some watermarks. Mostly the middle frequency bands are chosen because it does not scatter the watermark information.

2) Using Discrete Wavelet Transform:

A wavelet is a small wave which oscillates and declines in the time domain. The Discrete Wavelet Transform (DWT) [17] is a relatively recent and computationally efficient technique in computer science. Wavelet analysis is advantageous as it performs local analysis and multiresolution analysis. To analyze a signal at different frequencies with different resolutions is called multiresolution analysis (MRA). This technique transforms the object in wavelet domain, processes the coefficients and then performs inverse wavelet transform to represent the original format of the stego object.

VIII. APPLICATION

Steganography is applicable to, but not limited to following areas.

- Confidential communication and s;;ecret data storing.
- Protection of data alteration.
- Access control system for digital content distribution media database systems.
- Media database system.
- Protects copyrights, to maintain confidentiality.

A. Fields of application

- Defense and intelligence
- Medical
- On-line banking
- On-line transaction
- To stop music piracy
- Other financial and commercial purposes

IX. ADVANTAGES

- It supports all image format and sizes.
- It provides a high performance.
- It creates java-based tools called IMStego to embedded a secret message into images using 1-LSB and 2-LSB.
- Difficult to detect. Only receiver can detect.
- It is used in way of hiding not the information but the password to reach that information.
- It can be done faster with the large no of software.
- It is used in the way of hiding not the information but the password to reach that information.

X. LIMITATION

- Huge number of data, huge files size, so someone can suspect about it.
- If this technique is gone in the wrong hands like hackers, terrorist, criminals than this can be very much dangerous for all.
- It does not distribute a shareable key in secure manner.
- Limited to image size 256*256 which is easy to recover the embedded message.
- It provides a weak robustness because it is based on LSB1 and LSB2 methods.
- It does not provide an encryption.

- • Limited to only BMP and PNG image formats.

XI. FUTURE SCOPE

In today's world, we frequently listen a popular term "Hacking". Hacking is nothing but an illegal access of data which can be collected at the time of data transmission. With respect to steganography this problem is frequently taken as Steganalysis.

Steganalysis is a process in which a steganalyzer crashes the cover object to get the hidden data. So, whatever be the technique will be established in future, degree of security related with that has to be kept in mind. It is hoped that Dual Steganography, Steganography along with Cryptography may be some of the future result for this above-mentioned problem.

XII. CONCLUSION

There exist various methods for hiding secret information behind the cover image. Every detail about what type of image format is best suitable and depending upon what type of requirement can decide that a particular steganographic algorithm is good or not. On the other hand, three different levels are used to tell the strong point and weakness of a stenographic algorithm in particular parameter or requirement. Different techniques to insert data inside the cover image have also been explained to the reader. The paper emerges with the idea to think about what types of issues should be kept in mind in order to come up with a new stenographic algorithm. The study shows that the transform domain techniques are best for the attack strong system with relatively lower data capacity and higher complexity while the spatial domain is best for limited complexity systems and also provides greater options for techniques selection for the systems with incomplete computational power.

XIII. REFERENCES

[1] Shahzad Alam, S M Zakariya, M Q Rafiq, "Analysis of Modified LSB Approaches of Hiding Information in Digital Images", 2013 5th International Conference on Computational Intelligence and Communication Networks, @ 2013 IEEE.

[2] Moerland, T., Steganography and Steganalysis, Leiden Institute of Advanced Computing Science, www.liacs.nl /home/ tmoerl/privtech.

[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.

[6] S. Kurane, H. Harke, and S. Kulkarni, "TEXT AND AUDIO DATA HIDING USING LSB AND DCT A REVIEW APPROACH," Natl. Conf. "Internet Things To war. a Smart Future. "Recent Trends Electron. Common., 2016.

[7] . E. R. Harold, "What is an Image," 2006.

[8] B. N. Chary and B. Sreenivas, "Processing of satellite image using digital image processing," 2011.

[9] S. shica and D. K. Gupta, "Various Raster and Vector Image File Formats," Ijarcce, vol. 4, no. 3, pp. 268–271, 2015acs.nl /home/ tmoerl/privtech.

[10] Moerland, T., "Lossy and lossless", Leiden Institute of Advanced Computing Science, www.liacs.nl/home/ tmoerl/privtech.pdf.

[11] Johnson, N.F. & Jajodia, S., "Exploring Steganography: Seeing the Unseen", Computer Journal, February 1998.

[12] . S. Katzenbeisser and F. A.P. Petitcolas, Information hiding techniques for steganography and digital watermarking. Vol.

[13] . P. Wayner, disappearing cryptography: information hiding: steganography & watermarking. Morgan Kaufmann, 2009. 316. Norwood: Artech house, 2000.

[14] Kamaldeep, Image steganography techniques in spatial domain, their parameters and analytical techniques: a review article, IJAIR, vol.2, no.5, pp.85-92, 2013.

[15] Wu, C., Tsai, W.H., A steganographic method for images by pixel-value differencing, Pattern Recognition Letters, vol.24, pp.1613-1626, 2003.

[16] Kaur, B., Kaur, A., Singh, J., Steganographic approach for hiding Image in DCT domain, International Journal of Advances in Engineering & Technology, July 2011.

[17] Kumar, V. and Kumar, D., Performance evaluation of DWT based image steganography, Advance computing conference (IACC), IEEE 2nd International.2010