Image Steganography - Fundamentals and Literature Survey

[1]Aswathy Chandran B S,[2]Smitha Vas
[1]M.Tech Student,[2]Assistant Professor
[1]Department of Computer Science and Engineering,
[1]LBSITW, Poojappura, Trivandrum, Kerala, India

Abstract— ***In today's modern world, the number of computer users and the rate of information exchange is growing exponentially. Hence the need for secure transmission of this information is also a relevant research topic. Two common approaches found in the literature so far for the secure transmission of information are cryptography and steganography. In steganography, no one except the sender and receiver knows the existence of communication. But in cryptography, encrypted messages can attract unwanted attention from third parties. The advanced versions for secure information exchange are derived from these basic types, either as a combination or a more powerful version of the basic type. This paper aims at exploring the various steganographic methods found in the literature with a brief description of their advantages and disadvantages.***

Index Terms— ***image hiding, Least significant bit (LSB), discrete cosine transform (DCT), discrete wavelet transform (DWT), pixel value differencing (PVD), distortion, masking and filtering, image mosaic.***

I. INTRODUCTION

The invisible communication by means of concealing message existence is called steganography. The literal meaning of word 'steganography' is "covered writing". It is derived from two Greek words "steganos" and "graptos" which mean "covered" and "writing" respectively. In steganographic methods the communication between two parties is hidden and hence no one apart from the sender and receiver can identify the very existence of communication. So the chances of attracting the attacker's attention are les. But in cryptography the existence of communication is visible to outside world. Because the encrypted file is meaningless and can be a noise file. Hence chances of attack are more in cryptography. Encryption usually makes use of the natural properties of images, such as strong spatial correlation and high redundancy and we obtain an encrypted image which is based on Shannon's confusion and diffusion properties [1]. To prevent the direct attention of attackers, steganography is preferred over cryptography.

This paper is organized as follows. Section 2 overviews the applications of steganography. Section 3 discusses the system modules, related basic terminologies and the different types of steganography. Section 4 describes the existing steganographic methods and section 5 presents the related works. In section 6, a summary of steganographic approaches is presented. Finally, Section 7 summarizes conclusions of steganographic methods.

II. APPLICATIONS OF STEGANOGRAPHY

The applications of steganography were found from the 5th century BC onwards. The first marked instance was that Histaiacus shaved a slave's head and tattooed a message on his skull and the slave was dispatched with the message after his hair grew back [2]. Steganography can be used for the secure transmission of information. It finds application in many different areas in which cryptography is not suitable also. For example in some countries cryptography is prohibited. In such cases steganography can be used as a substitute for cryptography. Steganography can be used for the effective synchronization of audio and video. Steganography provides good authentication guarantee also. It can be used to identify traffic congestion in network paths by incorporating suitable packets to messages. Steganography can be used for the safe communication of secret data between the organizations. Steganography finds greater applications in medical imaging systems where the privacy of patient data is very much important. Steganography can also be incorporated to the printing processes. Fujitsu [3], a Japanese organization developed a technology to embed data to a picture in such a way that it is invisible to human eye. The decoding of data is made possible by using a mobile phone with a camera with a minimum charge fee. This application finds much use in food wrappers, business cards, bill boards etc.

III.OVERVIEW OF BASIC IDEA BEHIND STEGANOGRAPHY

A. Terminologies

i. Cover Object: - An object that is used to embed messages. It can be of different types such as images, audio, video, html pages etc.
ii. Stego Object: - An object which carries a hidden message.
iii. Message: - Message is something like plain text or image which is the original information to be hidden.
iv. Stego key: - A key is used to embed message into cover object and extract message from stego object

B. System Modules

An overview of the steganographic system is shown in figure 1. In general, steganography is the method of hiding information to a cover object to form the stego object by means of some embedding algorithm using a stego key. Then this stego object is send to the intended receiver through any medium by hiding the message existence. Hence third party attackers cannot detect the existence of hidden message. Then the receiver with the correct stego key can extract the message back. Without the correct key, even if existence is detected by some means, message cannot be retrieved back.

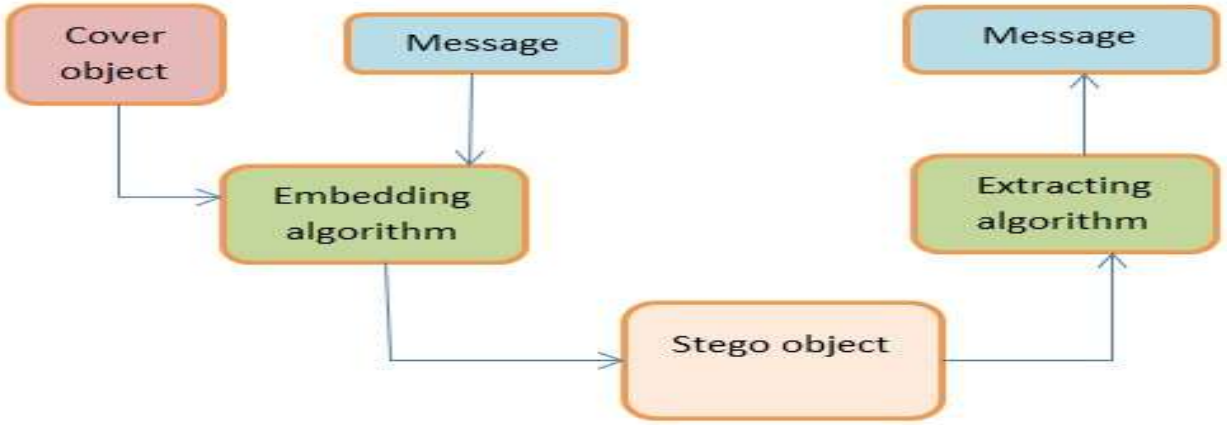

Fig.1. Steganography System

C. Types of Steganography

Steganography can be classified to many different types based on the digital medium used to achieve steganography. Depending on the cover object used to hide message, steganography can be classified as follows

- Image steganography
- Text steganography
- Audio Steganography
- Video Steganography
- Network protocol steganography

A brief description of each of them is given below

Image Steganography: - Images are used as cover objects and pixel intensities are used to hide information

Text Steganography: - In text steganography, count of white spaces, tabs, uppercase letters etc. are used to hide information

Audio Steganography: - audio is carrier of message. Different audio formats such as AVI MPEG, MIDI etc. are used for audio steganography.

Video Steganography: - Video is used as cover object. Generally video consists of a sequence of images and these images are used to hide information. Due to the large size of videos, steganography in videos is not noticeable to human eyes and both the audio and video streams in videos can be used for information hiding. The common video formats used for steganography are Audio Video Interleave (AVI), MPEG, MP4, H.264 etc.

Network protocol Steganography: - In network protocol steganography, the cover object used is anyone of the protocols like Transmission Control Protocol (TCP), Used Datagram protocol (UDP), ICMP, IP etc.

In this paper, various techniques for image steganography and important works in this field are discussed.

IV.IMAGE STEGANOGRAPHY TECHNIQUES

Several domains exist for image steganography. Important steganographic domains are listed below.

i. Spatial Domain Techniques
ii. Temporal domain Techniques
iii. Distortion techniques
iv. Masking and Filtering
v. Spread Spectrum
vi. Image Mosaics

A.Spatial Domain Techniques

The techniques which make direct changes to some pixel value bits to hide information are called spatial domain techniques. We can classify spatial domain techniques to the following types.

- Least Significant Bit (LSB)
- Pixel Value Differencing (PVD)
- Edges Based Data Embedding method (EBE)

In LSB [4] method, information is hidden in the least significant bits of pixels in the image. It is based on the fact that, changing the LSB of pixels does not make noticeable difference to images. The resulting stego image looks identical to cover image for eyes of human beings.

In Pixel Value Differencing [5] method, difference between two consecutive pixels is used to determine whether to embed information to those pixels or not. Large difference indicates that, pixels belongs to an edge area and hence more data can be embedded whereas small difference indicates that pixels belongs to smooth area and only small amount of information can be embedded.

In edge based data embedding [6] method, data is hidden in those regions which are least like their neighbors, such as edges, lines, corners etc. It is based on the fact that, the chances of detecting hidden messages by the attackers at the edges is less. Edges are detected using some edge detection algorithms.

Advantages of Spatial domain techniques are:

- Chances of original image degradation is less
- More data can be embedded to a single image

Disadvantages of Spatial domain techniques:

- Less robustness
- Data is destroyed by even smaller attacks also.

B.*Transform domain techniques*

Transform domain techniques used to hide data in those portions of the image that are less used to compression. Here data is embedded to the frequency domain of signals. Embedding data in frequency domain is stronger than embedding procedures that operate on time domain. We can classify transform domain techniques to the following categories.

- Discrete cosine transformation technique (DCT).
- Discrete wavelet transformation Technique (DWT).

In Discrete cosine transformation based steganography [7], images are separated to parts of varying importance such as high, middle and low frequency components. The low frequency sub-band contains the important visible parts of the image, whereas high frequency sub-band contains high frequency components which are removed usually through compression. Hence message embedding is done by modifying components in the middle frequency sub-band.

In wavelet transformation [8] methods also, image is first transformed from spatial domain to frequency domain. Wavelet transform partition images to low frequency and high frequency components on a pixel by pixel manner, and hence it provides better resolution than DCT method. Mathematical functions that are used to divide data to varying frequency components are called wavelets. One of the simplest DWT is Haar- DWT [9]. The secret data is then embedded in the high frequency components and it provides maximum robustness also.

Advantages of transform domain techniques are;

- Hide data in those areas of image that are less exposed to image processing
- Embedding in transform domain is stronger than embedding in time domain.

Disadvantage of transform domain technique:

- More complex method of embedding.

C.Distortion Technique

In distortion techniques [9], encoder alters the cover image by adding some changes. Thus the information is stored into the cover image by means of some distortion to the original cover image. The decoder on the other end needs the original cover image to compare he difference between cover image and distorted image. The message will be encoded to those pixels which are selected randomly. At the receiver, those pixels in the stego image which are different from the cover image are marked as 1. Then, the '1' value pixels are modified, in such a way that it does not affect the overall statistical properties of image. The disadvantage with this method is that, it needs to send the original cover image together with the stego image. Hence there is greater possibility of attack.

D.Masking and Filtering Techniques

Masking and filtering techniques [2], are commonly used for grey scale images and 24-bit images. Here embedding of two signals is done in such a way that, only one among them is perceptible to human eye. Masking involves, change of the luminance of area that is to be masked.

Advantages of masking and filtering:

- Highly robust.
- Better resistance to image manipulation.

Disadvantages of masking and filtering:

- This method is usually restricted to grey scale and 24-bit images.

E.Spread Spectrum

In Spread spectrum techniques [10], a narrow band signal is spread to a wide band of frequencies. By this process, the original signal can be converted to a larger bandwidth than the original signal. At the receiver end, original signal is retrieved by the correlation of spread signal using a synchronized copy of the spreading signal. Modulation techniques are used for the spreading of narrow band signal to wide band. Thus, this method offers better resistance to image processing such as cropping, rotation etc. also. Commonly used spread spectrum techniques are direct sequence spread spectrum and frequency hopping spread spectrum [11].

Advantages of spread spectrum:

- Highly robust
- Spread spectrum techniques uses DCT lossy compression, hence high color quality of embedding is offered.
- Since message is both encrypted and scattered, only the correct recipient will be able to decode message.

Disadvantage:

- It is based on frequency domain techniques and hence more complex way of embedding.
- There will be more distortion to the image because of spreading the signal throughout the entire image.

F.Image Mosaic

A latest trend of image steganography, using a type of mosaic image called secret fragment visible mosaic image is proposed in [12]. The secret image is divided to blocks and embedded into the similar blocks of a selected target image. This method offers a compression less method of steganography. The user is free to select target image of their choice.

V. RELATED WORKS

Hemalatha S, U Dinesh Acharya, Renuka A & Priya R Kamath (2013) [13] proposed an image steganographic technique based on integer wavelet transform. They choose a 256x256 color image as the cover image and two 128x128 grey scale images as secret images. Then, for the secret images, integer wavelet transformation is obtained and the sub-bands they obtained are named as LL, LH, HL, and HH. For hiding the secret images, LL sub-band is used. They can hide the two secret images into the single cover image.

Reddy, H.S.M, Sathisha N & Kumari (2012) [14] proposed a secure steganographic model using Hybrid domain technique. At first, cover images of different size and format are resized to dimensions that are powers of 2. Then Daubecchies Lifting wavelet theorem is applied too cover image and four sub-bands namely XA, XH, XV and XD are obtained. The XD sub-band is divided as upper and lower blocks to embed payload. Then the payloads are also resized to power of 2 and divided to four blocks of equal size. To improve payload security, the stego object is further scrambled using Decision Factor based manipulation. Then for the retrieval process, inverse Dubechies Lifting wavelet transform is used.

Ya-Li Lee & Wen-Hsaing Tsai (2014) [12] proposed an image steganographic method using secret fragment visible mosaic images. Their proposed work is a modification of work done by I.J Lai and W. H. Tsai in [15] 2011. In their proposed system, steganography is achieved by means of mosaicking. The user is free to choose any image as cover image and both the secret and target images are divided to blocks of equal sizes. The similar secret and target blocks are mapped to each other and the color characteristics of secret image are transformed to be that of cover image. Similarity is measured on the basis of mean and standard deviations. The tile fitting information is also embedded to random blocks selected using a pseudo random number generator. For optimum results a rotation operation is also performed whenever necessary to reduce the Mean square Error.

Neda Raftari & Amir Masoud (2012)[16] , proposed a digital image steganography based on integer wavelet transform and assignment algorithm. They use Munkres' assignment algorithm in which secret image can be embedded to the frequency domain of cover image with high matching quality. For converting secret and cover images to frequency domain, integer wavelet transformation was used. For finding the best matching blocks, assignment algorithm is used.

V1.SUMMARY OF STEGANOGRAPHIC APPROACHES

In this section, the summary of steganographic approaches, with a brief description of their advantages and disadvantages is given. Table 1 illustrates the steganographic methods and their advantages and disadvantages.

Sl No:	Technique	Method of embedding	Advantages	Disadvantages
1	Least Significant Bit(LSB)	The least significant bits of pixels in cover image are used to hide most significant bits of secret image	Easy to implement, simple way of message embedding	Causes distortion to original image, attacker can change the LSBs and results in modification of original message.
2	Pixel Value Differencing. (PVD)	Difference between adjacent pixels is used to determine edge and smooth areas. More information is hidden into edge areas.	High quality stego image is produced.	Poor in resisting to statistical analysis.
3	Edge based data embedding (EBE)	Data is hidden into those regions which are least like their neighbors, like edges, corners etc.	Hiding capacity is more; good quality stego image is produced.	Easily detected by RS Steganalysis, only limited experimental dataset is available.
4	Discrete Cosine Transform (DCT)	Embeds data by changing the transformed DCT coefficients.	More robust technique; hidden data is distributed over the whole image evenly.	Complex way of embedding.
5	Wavelet Transform	Different wavelets are taken to embed a single image. Wavelets partition image to low and high frequencies in a pixel by pixel manner.	Wavelet coefficients are altered within tolerable level of noise; less distortion. Highly robust.	It is also a complex way oh information hiding.
6	Distortion technique	Information is stored by signal distortion. Deviation from cover image is measured in decoding step.	Information storage is at random bits. But not fully secure and used with text steganography in earlier days only.	Need of original cover image for decoding process.
7	Masking and Filtering	Involves changing the brightness of masked area.	Highly robust, better resistance to image manipulation	Limited to grey scale and 24-bit images.
8	Spread spectrum	Message is spread over wider frequency bandwidth than the minimum required bandwidth.	Secure from image processing attacks	Level of noise is more.
9	Image Mosaic	Works by embedding secret blocks to target blocks.	User is free to choose any image as the cover image.	For extraction purpose, a large amount of recovery information needs to be embedded. This may lead to distortion.

Table: 1. Summary of steganography approaches

V11.CONCLUSION

Steganography is attaining much importance these days due to the large transfer of multimedia data throughout the internet. One of the important concerns regarding these data is its security. Steganography is gaining wider popularity since the stego message does not attract the attention of attackers while the encrypted message on the other hand, will be like noise and easily attract the attention of attackers. In this paper, a review of steganographic approaches is presented, with a brief description of their advantages and disadvantages.

VIII.ACKNOWLEDGMENT

I am thankful to my guide Mrs.Smitha Vas, Assistant Professor of Computer Science and Engineering LBS ITW, for her guidance and encouragement for this paper work.

REFERENCES

- SJ.Fridrich, "Symmetric ciphers based on two – dimensional chaotic maps," *Int.J.Bifurc. Chaos*, vol.8, pp.1259-1284, 1998.
- N.F. Johnson, S. Jajodia, "Exploring steganography: seeing the unseen", *IEEE Computer* 31 (2) (1998) 26–34..
- S.N.Provos, P. Honeyman, "Hide and Seek: an introduction to Steganography", *IEEE Security and Privacy* 1(3) (2003) 322-44.
- J.R.Krenn," Steganography and Steganalysis", January 2004. Deshpande Neeta, KamalapurSnehal, Daisy Jacobs, "Implementation of LSB Steganography and its Evaluation for carious Bits", 2004.
- Chung-Ming Wang, Nan-I Wu, Chwei-Shyong Tsai Min-Shiang Hwang, "High quality steganographic method with pixel-value differencing and modulus function. "Science Direct The Journal of Systems and software, 24 January 2007.
- K. M Singh, L. S Singh, A. B Singh and K. S Devi, "Hiding secret message in edges of the image, " in *Proc. Int conf. information and communication Technology* pp. 238-241, mar. 2007.
- K. B Shiva Kumar, K.B Raja, R. K Chhotaray, Sabyasachi Pattnaik, " Coherent Steganography using Segmentation and DCT, " IEEE-978-1-4244-5967-4/10/$26.00©2010.
- A.A Abdelwahab and L. A. Hassan, "A discrete wavelet transform based technique for image data hiding, *"Proceedings of 25th National radio Science Conference, NRSC* 2008, Egypt March 18-20 2008, pp. 1-9.
- S.C Katzenbeisser, "Principles of steganography in information hiding techniques for steganography and digital watermarking ", *S. Katzenbeisser and F. Petitcolas, Ed. London* : Artech House ,(2000), pp. 43-78 .
- I. J Cox, F.T Leighton and T. Shamoon, "Secure spread spectrum watermarking for multimedia, " *IEEE Trans. on Image Processing* , vol 6,no. 12, 1997.
- Xu Anuying, Liu Shuwei, Xiong Shan, Huang Juhua, Xu Sisi, "Audio information hiding based on distance metric ", *IEEE, 2010*, 978-14244-6893-5.
- Ya-Lin Lee, Wen-Hsiang Tsai, "A new secure image transmission technique via secret fragment visible mosaic images by nearly reversible color transformations, " *IEEE Transactions on circuits and systems for video technology*, vol. 24, No. 4, April 2014.
- Hemalatha S, U Dinesh Acharya, Renuka A, Priya R Kamath," A secure and high capacity image steganography technique" *Signal and image processing: An international Journal (SIPIJ*) Vol.4, No. 1, February 2013.
- Reddy, H.S.M, Sathisha N, Kumari A, RajaK.B, "Secure steganography using hybrid domain technique, "Computing Communication & Networking Technologies (ICCCNT)2012,Vol no 111 pp -26-28July 2012.
- I. J Lai and W. H Tsai, " secret fragment visible mosaic image- a new computer art and its application to information hiding" IEEE Trans. Information Forensics and security, vol. 6, no.3, pp. 936-945, 2011.
- Raftari, N. Moghadam, "Digital Image Steganography Based on integer wavelet transform and assignment algorithm, " Modeling symposium (AMS), 2012 Sixth Asia, vol..no.pp.87,92,29-31 May 2012.

.