SURVEY ON DIFFERENT METHODS OF IMAGE STEGANOGRAPHY

B.Deekshitha[1], Gnanamanjari.S[2], Chaithanya.S[3]

[1,2] *6th Sem, Dept of ECE, Rajarajeswari College of Engineering, Bangalore, India*
[3] *Asst. Professor, Dept of ECE, Rajarajeswari College of Engineering, Bangalore, India*

ABSTRACT

Today major part of communication goes through internet and this communication needs to be secret and protected against malicious attack, therefore security problems become an essential issue. Image steganography is also defined as the study of invisible communication that usually deals with the ways of hiding the existence of the communicated message. The Objective of steganography are Un detectability, robustness and capacity of the concealed data, these key factors that separate it from related techniques like cryptography and watermarking. A survey of image steganography is done here and the different techniques to hide a secrete data behind a cover image are described. It is very useful technique in information security domain. In this study we analyse how image steganography is done, where it is used and the advantages and disadvantages of each technique.

Keywords: *Image steganography, information security, robustness, cryptography, watermarking*

---

1. INTRODUCTION

Steganography word is originated from Greek words steganos (Covered), and Graptos (Writing) which literally means "cover writing". Generally steganography is known as "invisible" communication. Image steganography is the idea of hiding private or sensitive data or information within something that appears to be nothing out of normal. Image steganography is one of the popular technique in encoding the data because the digital images are most popular for hiding information because of their frequency on interest. Steganography means is not to alter the structure of the secret message, but hides it inside a cover-object (carrier object). After hiding process cover object and stegao-object (carrying hidden information object) are similar. So, steganography (hiding information) and cryptography (protecting information) are totally different from one another. Image Steganography is mostly used in modern printers. HP and Xerox brand laser printers uses Image Steganography. This printer adds tiny yellow dots to each page. The dots are not easily visible and contain encoded printer serial numbers as well as date and time stamps.

2. IMAGE STEGANOGRAPHY METHODS

Steganography for binary images is mainly concentrated on hiding data in gray-scale images and colour images. The luminance component of a colour image is equivalent to a gray-scale image. It is commonly considered that gray-scale images are more appropriate than colour images for hiding data because the disturbance of correlations between colour components may simply reveal the trace of embedding data. In this section we give an overview of the most important and popular steganographic techniques in digital images.

2.1. Image Steganography Terminologies

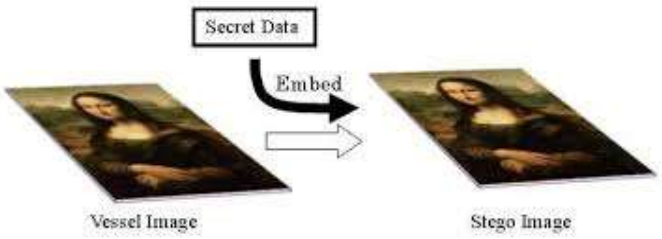

Fig-1: Image Steganography

Image steganography terminologies are as follows:
- Vessel-Image : Original image which is used as a carrier for hidden information.
- Secrete Data : Actual information which is used to hide into images. Message could be a plain text or some other Image.
- Stego-Image : After embedding message into cover image is known as stego-image.
- Stego-Key : A key is used for embedding or extracting the messages from cover- images and stego-images.

Generally image steganography is method of information hiding into cover-image and generates a stego-image. This stego-image then sent to the other party by known medium, where the third party does not know that this stego-image has hidden message. After receiving stego-image hidden message can simply be extracted with or without stego-key (depending on embedding algorithm) by the receiving end [21]. Basic diagram of image steganography is shown in Figure 2 without stego-key, where embedding algorithm required a cover image with message for embedding procedure. Output of embedding algorithm is a stego-image which simply sent to extracting algorithm, where extracted algorithm un hides the message from stego-image.

2.2. Image Steganography Classifications

Generally image steganography is categorized in following aspects and Table-1 shows the best steganographic measures.

High Capacity : Maximum size of information can be embedded into image.

Perceptual Transparency : After hiding process into cover image, perceptual quality will be degraded into stego- image as compare to cover

Robustness : After embedding, data should stay intact if stego-image goes into some transformation such as cropping, scaling, filtering and addition of noise.

Temper Resistance : It should be difficult to alter the message once it has been embedded into Stego - image.

Computation Complexity : How much expensive it is computationally for embedding and extracting a hidden message?

Table-1: Image Steganography Algorithm Measures

Measures	Advantage	Disadvantage
High Capacity	High	Low
Perceptual Transparency	High	Low
Robustness	High	Low
Temper Resistance	High	Low
Computation complexity	Low	High

2.3 Image Steganographic Techniques

Image steganography techniques can be divided into following domains.

Spatial Domain Methods

Least significant bit

The most basic and important image Steganographic Technique is Least Significant Bit [6, 7] embedding technique. In this technique data can be hidden in the least significant bits of the cover image and the human eye would be unable to notice the hidden image in the cover file. There are 256 possible intensities of each primary colour, so, changing the LSB of a pixel results in small changes in the intensity of the colours. These changes cannot be perceived by the human eye, thus the message is successfully hidden. But this approach is very easy to detect.

Pixel Value differencing (PVD)

In this method, the image is divided into non-overlapping blocks of two consecutive pixels and then the difference value is calculated for each block in similar way as in [9]. On the basis of the difference value, each block is identified either as a part of smooth region or edge region. This method embeds the secret data bits into the smooth regions by simple LSB substitution method and for edge area [8] is used. Thus, it increases the data hiding capacity to a great extent without disturbing the image quality much.

Pixel Mapping Method

In this technique, the embedding pixels are selected based on some mathematical function which depends on the pixel intensity value of the seed pixel and its 8 neighbours are selected in counter clockwise direction. Before embedding a checking has been done to find out whether the selected embedding pixels or its neighbours lies at the boundary of the image or not [10]. Data embedding are done by mapping each two or four bits of the secret message in each of the neighbour pixel based on some features of that pixel.

MSB bit difference method

This technique uses the difference of two pixel's bits of the cover image. Bit No. 5 and 6 of a pixel are targeted for embedding. The difference between bit 5 and 6 is set according to the incoming secret information bit. If the difference between bit 5 and 6 is equal to the incoming secret bit then no change is required in bit 5. If the difference between bit 5 and 6 does not match with the incoming bit then bit 5 is changed to make the difference and incoming bit equal[14]. The advantage of this method is, MSB bits makes the system more secure and shows that it has greater PSNR and better Payload capacity which can be used to hide more data in a single cover image.

Histogram mapping method

In histogram based data hiding technique [2] the crucial information is embedded into the image histogram. Pairs of peak points and zero points are used to achieve low embedding distortion with respect to providing low data hiding capacity.

Transform Domain Technique

This is a more complex way of hiding information in an image. The process of embedding data in the frequency domain of a signal is much stronger than embedding principles that operate in the time domain. Transform domain techniques are broadly classified as follows

Discrete Cosine Transformation technique (DCT)

DCT is a general orthogonal transform for digital image processing and signal processing with advantages such as 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 thus making it easier to choose the band in which the watermark is to be inserted [13]. Mostly the middle frequency bands are chosen because embedding the information in a middle frequency band does not scatter the watermark information to most visual important parts of the image i.e. the low frequencies and also it do not overexpose them to removal through compression and noise attacks where high frequency components are targeted.

Discrete Fourier Transform(DFT)

The DFT based technique is similar to the DCT based technique but it utilizes the Fourier transform instead of cosine which makes it lack resistance to strong geometric distortions[15] . Although it increases the overall complexity of the process.

Discrete Wavelet Transformation technique (DWT)

This technique [5] is used to transform the image from its spatial domain into its frequency domain. We use DWT in the process of steganography so that we can clearly identify the high frequency and low frequency information of each pixel of the image. To obtain the DWT of the cover image, a filter pair called the Analysis Filter pair is used. First, the low pass filter is applied to each row of data in order to get the low frequency components of the row. Since the LPF is a half band filter, the Output data needs to be sub-sampled by two, so that the output Data now contains only half the original number of samples. Next, the high pass filter is applied for the same row of data, and similarly the high pass components are separated, and placed by the side of the low pass components. This procedure is done for all rows [5]. Again filtering is done for each column of the intermediate data. The resulting two-dimensional array of coefficients contains four bands of data, each labelled as LL (Low-Low), HL (High-Low), LH (Low High) and HH (High-High). The LL band can decomposed once again in the same manner, thereby producing even more sub-bands.

Spread Spectrum

In spread spectrum techniques, The message is spread over a wide frequency bandwidth than the minimum required bandwidth to send the information. This can be accomplished by adjusting the narrowband waveform with a wideband waveform, such as white noise. After spreading, the energy of the narrowband signal in any one frequency band is low and therefore difficult to detect [12]. In spread spectrum image steganography the message is embedded in noise and then combined with the cover image to produce the stego image. Since

the power of the embedded signal is much lower than the power of the cover image, the embedded image is not perceptible to the human eye or by computer analysis without access to the original image [12].

Distortion Techniques

Distortion techniques need knowledge of the original cover image during the decoding process where the decoder functions to check for differences between the original cover image and the distorted cover image in order to restore the secret message. The encoder adds a sequence of changes to the cover image. So, information is described as being stored by signal distortion. Using this technique, a stego object is created by applying a sequence of modifications to the cover image. This sequence of modifications is use to match the secret message required to transmit. The message is encoded at pseudo-randomly chosen pixels. If the stego-image is different from the cover image at the given message pixel, the message bit is a "1." otherwise, the message bit is a "0." The encoder can modify the "1" value pixels in such a manner that the statistical properties of the image are not affected. However, the need for sending the cover image limits the benefits of this technique. In any steganographic technique, the cover image should never be used more than once. If an attacker tampers with the stego-image by cropping, scaling or rotating, the receiver can easily detect it[1]. In some cases, if the message is encoded with error correcting information, the change can even be reversed and the original message can be recovered.

Masking and Filtering

These techniques hide information by marking an image, in the same way as to paper watermarks. These techniques embed the information in the more significant areas than just hiding it into the noise level. The hidden message is more integral to the cover image. The advantage of this method is much more robust than LSB replacement with respect to compression since the information is hidden in the visible parts of the image. The disadvantage of this technique is it can be applied only to gray scale images and restricted to 24 bits.

Adaptive Steganography

Adaptive steganography is special case of two former methods. It is also known as "Statistics aware embedding" and "Masking". This method takes statistical global features of the image before attempting to embed secret data in DCT or DWT coefficients. The statistics will dictate where to make changes.

3. APPLICATIONS

- Secure private files and documents.
- Hide passwords and encryption keys.
- Transmit message or data without revealing the existence of available message.
- Smart id's
- Copywrite protection
- Printers

4. CONCLUSION AND FUTURE WORK

We have done survey of image steganography, its techniques, classifications, and the advantages and disadvantages of main image steganography techniques. We came to know that all these techniques have few advantages and disadvantages .We have to choose a technique which is most suitable for the application of the problem statement. The next plan is to develop a steganography technique that is robust to different types of attacks and also work can be enhanced for other data files like audio, video, and text. By these methods we can achieve best completeness, correctness, quality and accuracy.

5. ACKNOWLEDGEMENT

We are delighted to present the report on "Survey on different methods of image steganography". We take this opportunity to express our sincere thanks towards the staff of electronics and communication department, RRCE and special thanks to Chaithanya. S madam for providing technical guidelines and giving certain suggestion regarding line of this work.

6. REFERENCES

[1] N.Johnson and s.Jajodia, exploring steganography:"seeing the unseen,IEEE computer, ppt 26-34, February 1998.

[2] YildirayYalman 1 , FeyziAkar 2 and Ismail Erturk "Contemporary Approaches to the Histogram Modification
[3] JagvinderKaur and Sanjeev Kumar, " Study and Analysis of Various Image Steganography Techniques" IJCST Vol.2, Issue 3, September 2011.
[4] Ks. Mrs.Kavitha, KavitaKadam and P. Dunghav, "Steganography using least signicantbit algorithm," International Journal of Engineering Research and Applications(IJERA), vol. 2, pp. 338–341, May-June sssss2012.
[5] International journal of innovative research in computer and communication engineering "survey on different methods of image steganography", vol.2, issue 12, December 2014
[6] Deshpande N, Snehal K., "Implementation of LSB Steganography and Its Evaluation for Various Bits" K.K.Wagh Institute of Engineering Education & Research, Nashik India
[7] Morkel, T., Eloff, J.H.P & Olivier, M.S., (2005) "An overview of Image Steganography", Proceedings of Information Security South Africa (ISSA) Conference
[8] Wu D. C and Tsai W. H. (2003), "A steganographic method for images by pixel-value differencing", Pattern Recognition Letters, vol. 24, no. 9-10, pp. 1613-1626.
[9] Wu H.C., et al. (2005), "Image Steganographic scheme based on pixel-value differencing and LSB replacement methods", VISP (152), No.
[10] International Journal of Engineering and Innovative Technology (IJEIT) Volume 3, Issue 7, January 2014 "A Review on Different Image Steganography Techniques" Anjali Tiwari, Seema Rani Yadav, N.K. Mittal
[11] W. Zhang, S. Wang, and X. Zhang, "Improving embedding efficiency of covering codes for applications in steganography," IEEE Communications Letters, vol. 11, pp. 680–682, August 2007.
[12] Marvel, L.M., Boncelet Jr., C.G. & Retter, C.,"Spread Spectrum Steganography", IEEE Transactions on image processing, 8:08, 1999
[13] Blossom Kaur, Amandeep Kaur, Jasdeep Singh "STEGANOGRAPHIC APPROACH FOR HIDING IMAGE IN DCT DOMAIN", International Journal of Advances in Engineering & Technology, July 2011.
[14] Ammad Ul Islam1 , Faiza Khali **"**An Improved Image Steganography Technique based on MSB using Bit Differencing**",**Innovative Computing Technology (INTECH), 2016 Sixth International Conference on,978-1-5090, IEEE,2016
[15] Nadiya, P.V.; Imran, B.M., "Image steganography in DWT domain using double-stegging with RSA encryption," Signal Processing Image Processing & Pattern Recognition (ICSIPR), 2013 International Conference on , vol.7, no. 8, pp.283,287, Feb. 2013.