ISSN: 2348 9510
International Journal Of Core Engineering & Management (IJCEM)
Volume 1, Issue 10, January 2015

Image Steganography: Classification, Application and Algorithms

Shikha Mohan[1] and Satnam Singh[2]
[1]M.Tech Scholar, ECE Department, SSCET,Badhani,Punjab, India
[2]AP, ECE Department, SSCET, Badhani, Punjab, India
Email: shikha.mohan@yahoo.com , jeevanjot1999@gmail.com

***Abstract* — Steganography is the technique/science of hiding information inside some innocent looking canvas like images. The growth of internet and communication technology has enabled the demand to send a message as safely and as securely as possible. In the last few years, we have seen that new and powerful steganography techniques reported in the literature. This paper intends to give an overview of image steganography, its applications and techniques. The paper gives the description of various techniques used in steganography and attempts to identify the requirements of a good steganography algorithm.**

***Index Terms* –Least Significant Bits (LSB), Peak Signal-to-Noise Rate (PSNR), Mean Square Error (MSE), Steganalysis**.

I. INTRODUCTION

Steganography literally means covered/hidden writing i.e., writing known to casual observer and is derived from Greek words 'steganos' meaning covered or secret and 'graphy' meaning writing or drawing. Information is the wealth of any organization therefore security issues are top priority to an organization dealing with confidential data. Steganography is the science that involves communicating secret data in an appropriate multimedia carrier, e.g., image, audio, and video files.

Image Steganography is the technique for hiding information by embedding messages within image. It is widely used in military, diplomatic, personal and intellectual property applications. Steganography is the term applied to any number of processes that will hide a message within an object particularly an image, where the hidden message will not be apparent to an observer. Typically, the message is embedded within another object (image) known as a cover object, by tweaking its properties. The resulting output, known as a stego object or stegogramme is engineered such that it is a near identical perceptual model of the cover object, but it will also contain the hidden message. If anybody intercepts the communication, they will obtain the stegogramme, but as it is so similar to the cover, it is a difficult task for them to tell that the stegogramme is anything but innocent. It is therefore the duty of steganography method to ensure that the adversary regards the stegogramme - and thus, the communication - as innocuous [1, 2].

Steganography differs from cryptography because the latter does not attempt to hide the fact that a message exists. Instead, cryptography merely obscures the integrity of the information so that it does not make sense to anyone but the creator and the recipient. The adversary will be able to see that a message exists, and the inverse process of cryptanalysis involves trying to turn the meaningless information into its original form. Steganography in the modern day sense of the word usually refers to information or a file that has been concealed inside a digital Picture, Video or Audio file. What Steganography essentially does is exploit human perception; human senses are not trained to look for files that have information hidden inside of them. Steganography is employed in various useful applications, e.g., for human rights organizations, as encryption is prohibited in some countries copyright control of materials, enhancing robustness of image search engines and smart identity cards, where details of every person are embedded in their photographs [3]. Other applications are video-audio synchronization, companies' safe circulation of secret data, TV broadcasting, TCP/IP packets, for instance a unique ID can be embedded into an image to analyze the network traffic of particular users, and also checksum embedding [4]. Carrier is also known as cover-object, in which message is embedded and serves to hide the presence of the message. The data can be any type of data (plain text, cipher text or

ISSN: 2348 9510
International Journal Of Core Engineering & Management (IJCEM)
Volume 1, Issue 10, January 2015

other image) that the sender wishes to remain confidential. Password is known as stego-key, which ensures that only recipient who knows the corresponding decoding key will be able to extract the message from a cover-object. The cover-object with the secretly embedded message is then called the stego-object.

II. Steganography Classification

Almost all digital file formats can be used for steganography, but the formats that are more suitable are those with a high degree of redundancy. Redundancy can be defined as the bits of an object that provide accuracy far greater than necessary for the object's use and display. The redundant bits of an object are those bits that can be altered without the alteration being detected easily. Image and audio files especially comply with this requirement, while research has also uncovered other file formats that can be used for information hiding. There are four main categories of file formats that can be used for steganography shown in "Figure 1". Since, images are quite popular cover or carrier objects used for steganography. In the domain of digital images many different image file formats exist, most of them for specific applications. For these different image file formats, different steganographic algorithms exist. Here, in this paper, we will discuss about the image domain steganography methods. In Image Domain methods secret messages are embedded using the intensity of the pixels values directly. The image domain methods are relatively simple compared to the other methods and are sometimes characterized as the "simple systems". However, they are generally more sensitive to small changes on the image such as filtering, resizing and squeezing.

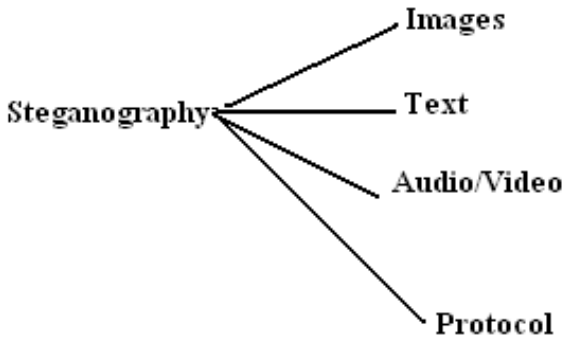

Fig 1: The four main categories of file formats that can be used for steganography

To hide information in audio files similar techniques are used as for image files. One different technique unique to audio steganography is masking, which exploits the properties of the human ear to hide information unnoticeably. A faint, but audible, sound becomes inaudible in presence of another louder audible sound. This property creates a channel in which to hide information. Although nearly equal to images in steganography potential, the larger size of meaningful audio files makes them less popular to use than images.

III. Various Image Steganography Techniques

Image steganography techniques can be classified into two broad categories: Spatial-domain based steganography and Transform-domain based steganography.

A. Spatial Domain Method

In spatial domain scheme, the secret messages are embedded directly. Here, the most common and simplest steganography method is the least significant bits (LSB) insertion method. In the LSB technique, the least significant bits of the pixels are replaced by the message bits which are permuted before embedding. Most steganography software hide information by replacing only the least-significant bits (LSB) of an image with bits from the file that is to be hidden. This technique is generally called LSB encoding. One of the most common techniques used in steganography. The

ISSN: 2348 9510
International Journal Of Core Engineering & Management (IJCEM)
Volume 1, Issue 10, January 2015

following example shows how the letter A can be hidden in the first eight bytes of three pixels in a 24-bit image.

Pixels: (10101111 11101001 10101000)
(10100111 01011000 11101001)
(11011000 10000111 01011001)

Secret message: 01000001

Result: (10101110 11101001 10101000)
(10100110 01011000 11101000)
(11011000 10000111 01011001)

The three bold bits are the only three bits that were actually altered. Since the 8-bit letter A only requires eight bytes to hide it in, the ninth byte of the three pixels can be used to begin hiding the next character of the hidden message. A slight variation of this technique allows for embedding the message in two or more of the least significant bits per byte. This increases the hidden information capacity of the cover-object, but the cover-object is degraded more, and therefore it is more detectable.

Spatial LSB embedding is widely used for its high hiding quality and simplicity to realize. However, the robustness of this method is weak and the message length can be estimated by statistical scheme [5]. In order to solve this problem, some researcher's proposed various methods which are advanced version of LSB techniques. A reversible histogram transformation function-based

LSB steganographic method is proposed by Der-Chyuan Lou and Chen-Hao Huto resists statistical steganalysis [6]. The experimental results show that the proposed method resists not only Regular-Singular (RS) attack but also Chi-Square (χ 2) detection methods. Chia-Chun Wu et al. proposed a novel secret image sharing scheme by applying optimal pixel adjustment process to enhance the image quality under different payload capacity and various authentication bits conditions [7]. The experimental result of proposed scheme shows the improvement of image quality of stego images. He also provides several experiments to demonstrate the efficacy of authentication capability of the proposed scheme and therefore maintains the secret image sharing and authentication ability while enhances the image quality.
Xin Liao et. al. improve the embedding capacity and provide an imperceptible visual quality, by give a novel steganographic method based on four-pixel differencing and modified Least Significant Bit (LSB) substitution [8]. The experimental result of proposed method gives not only an acceptable image quality but also provides a large embedding capacity.

As vast channels for communication such as the Internet are becoming popular, the security of digital media becomes a greater concern. The hiding of a message will reduce the probability of detecting this message. This method hides a gray image in one another. The cover is divided into blocks of equal sizes. Each block size equals the size of the embedding image. Edge Based Steganography is in which only the sharper edge regions are used for hiding the message while keeping the other smoother regions as they are. It is more difficult to observe changes at the sharper edges than those in smoother regions. In this method Enhanced Least Significant Bit algorithm is used which can reduce the rate of pixel modification thereby increasing the security both visually and statistically.

Grey Level Modification Steganography Method steganography method is based on image layers. This method divides the host image into blocks and embeds the corresponding secret message bits into each block using the layers which are made by the binary representation of pixel values. It then performs a search on the rows and columns of the layers for finding the most similar row or column. The location of row/column and its differences from the secret message is then marked by modifying minimum number of bits in the least significant bits of the blocks.

B. TRANSFORM DOMAIN METHOD

Here we can embed information in DCT, DFT, FFT domains etc. The main strength offered by transform domain techniques is that they can take advantage of properties of alternate domains to address the limitations of pixel-based methods or to support additional features.

A possible disadvantage of spatial techniques is that they are not very robust against attacks. In addition to this, adaptive steganography techniques are a bit more difficult in the spatial domain. Both the robustness and quality of the watermark could be improved if the properties of the cover image could similarly be exploited. For instance, it is generally preferable to hide watermarking information in noisy regions and edges of images, rather than in smoother

ISSN: 2348 9510
International Journal Of Core Engineering & Management (IJCEM)
Volume 1, Issue 10, January 2015

regions. The benefit is two-fold; Degradation in smoother regions of an image is more noticeable to the HVS, and becomes a prime target for lossy compression schemes.

IV. Results and Discussion

The PSNR represents a measure of the peak error, whereas, MSE represents the cumulative squared error between the resultant image and the original image.

$$MSE = \frac{\sum_{M,N}(T(r,c) - T'(r,c))^2}{M * N}$$

$$PSNR = 10 * log_{10}\left[\frac{R^2}{MSE}\right]$$

Where T (r c,) is the original image and *T '(r, c)* is the resultant stego-image, *r* and *c* are the number of rows and columns in the input images and M and N are the size of the images, respectively. *R* is the maximum fluctuation in the input image data type or we can say that it gives the maximum intensity value of image.
Various image steganography methods have different values of PSNR and MSE.

The results of LSB, DCT and DWT based Steganography is shown in figure 1. The PSNR values of various algorithm is shown in Table 1.

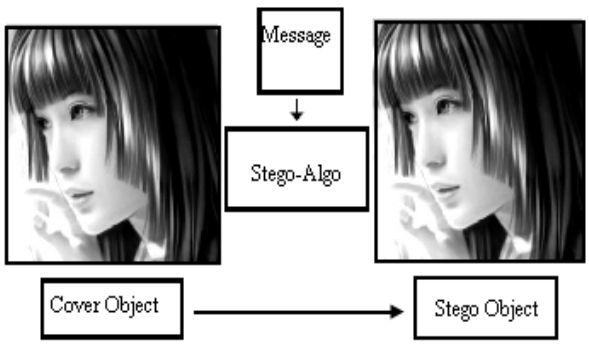

Figure 2: Cover Image and Stego Image.

Table 1: PSNR values of various algorithms

Image	PSNR		
	LSB	DCT	DWT
Lena	64.23	52.53	58.98
Baboon	64.12	53.21	59.34
Girl	63.98	52.89	59.23
House	64.31	52.65	59.10
Nature	63.92	52.97	59.65
Building	64.19	53.10	58.76
Flower	64.02	52.94	59.25

IV. Conclusions

In this paper, Survey, classification and application of various methods of steganography were discussed. Most of the techniques work on the least significant bits of the pixel values. Table 1 shows that LSB based steganography perform better than others. DWT domain shows promising results and outperforms DCT embedding especially in terms of compression survival. Table 2 shows the overall comparative performance analysis of various techniques of image steganography.

Table2. Comparative Performance Analysis

	LSB	DCT	DWT	Spread Spectrum
Invisibility	Low	High	High	High
Payload capacity	High	Medium	Medium	Medium
Robustness against	Low	Medium	High	High

ISSN: 2348 9510
International Journal Of Core Engineering & Management (IJCEM)
Volume 1, Issue 10, January 2015

statistical attacks				
Robustness against image manipulation	Low	Medium	Medium	Medium
Independent of file format	Low	Medium	Medium	Medium
PSNR	High	Medium	Medium	Medium
MSE	Less	Medium	Medium	Medium

REFERENCES

[1] Abbas Cheddad, Joan Condell, Kevin Curran, Paul McKevitt, "Digital image steganography: Survey and analysis of current methods", Journal of Signal Processing, Elsevier, Vol. 90, 2010, pp: 727–752.

[2] Yambern Jina Chanu, ThemrichonTuithung, Kh. Manglem Singh, "A Short Survey on Image Steganography and Steganalysis Techniques", IEEE 3rd conference on Emerging Trends and Applications in Computer Science (NCETACS), Shillong, 30-31 March 2012, pp: 52 – 55.

[3] Alain Brainos, "A Study of Steganography and The Art of Hiding Information"July,2004, http://www.infosecwriters.com/text_resources/pdf/steganographyDTEC6823.pdf

[4] Paunwala, M.C. Patnaik, S., "Sheltered Identification with Hiding Biometrics", International Conference on Signal and Image Processing (ICSIP), IEEE, Surat, 15-17 Dec., 2010, pp: 191-196.

[5] R. Shreelekshmi, M. Wilscy, C.E. Veni Madhavan, "Cover Image Preprocessing for More Reliable LSB Replacement Steganography", Proc. of International Conference on Signal Acquisition and Processing, IEEE, Trivandrum, 9-10 Feb., 2010; pp: 153-156.

[6] Der-Chyuan Lou and Chen-Hao Hu, "LSB steganographic method based on reversible histogram transformation function for resisting statistical steganalysis", Journal of Information Sciences, Elsevier, Vol. 188, 2012, pp: 346–358.

[7] Chia-Chun Wu, Shang-Juh Kao and Min-Shiang Hwang, "A high quality image sharing with steganography and adaptive authentication scheme", Journal of Systems and Software, Elsevier, Vol. 84, 2011, pp: 2196– 2207.

[8] Xin Liao, Qiao-yan Wen and Jie Zhang, "A Steganographic method for Digital Images with Four-pixel Differencing and Modified LSB Substitution", Journal of Visual Communication and Image Representation, Elsevier, Vol. 22, 2011, pp: 1–8.