A Review on Image Steganography

[1]Savita, [2] Mamta Juneja

[1]ME, Computer Science and Engineering, University Institute of Engineering and Technology, Panjab University, Chandigarh, Savitabadhan23@gmail.com

[2]Assistant Professor, Department of Computer Science and Engineering, University Institute of Engineering and Technology, Panjab University, Chandigarh, er_mamta@gmail.com

Abstract— Steganography is a form of information hiding. Today there is a very large demand of applications which require data to be transmitted in a safe and secure manner. Steganography is one of the methods used for the hidden exchange of information and it can be defined as the study of invisible communication that does not attract attention from eavesdroppers and attackers. The main requirements of any steganography system are undetectability, robustness and capacity to hide data. This paper includes the important steganography methods and the main focus is on the review of steganography in digital images. Terms used in the paper are M message, C cover image, Z stego image, E_m embedded message, E_x extracted message.

Index Terms— Adaptive steganography, Cryptography, Information hiding, Steganography, spatial domain and transform domain steganography, PSNR, MSE.

1 Introduction

Information hiding plays a very important role in today's world. For many years Information Hiding has captured the attraction of researchers. Digital watermarking and steganography techniques are used for hiding information in a secure and secret manner. These are being used to address copyright management, protect information, and conceal secrets. Information hiding techniques provide an interesting platform for forensic sciences. Information can easily traverse through firewalls undetected .Researches have been made to aid in discovering the steganalysis techniques for percepting the hidden data and hence has lead to the research of improved methods for hiding data. Many techniques have been proposed to hide data in an image [4]. Steganography and digital watermarking are the forms of information hiding.

Steganography [1] comes from the Greek and literally means, "secret writing". It does not attempt to alter the structure of the message to be hidden, but makes use of a cover image to hide it so that no one even knows the existence of the message. In other word, steganography prevents unwanted recipients from even suspecting the existence of data .It aims at transmitting a message on a channel where some other information is already being transmitted. The goal of steganography is to hide messages inside other harmless messages in a way that does not allow any enemy to even detect that there is a second secret message present. Steganography has developed a lot in recent years because of advancements in the digital techniques being used to hide data. Another application of steganography is the copyright protection. Various techniques are also available to detect steganography [3]. Also, main requirements of steganography are security, robustness and payload. In modern world, depending on the nature of cover object, steganography can be divided into these types: Text Steganography, Image Steganography, Audio Steganography, and Video Steganography. Hiding data inside the plain text can be done in many ways .Image steganography use many techniques [2] like LSB insertion, masking and filtering , redundant pattern encoding , encrypt and scatter, algorithms and transformations. So, many steganographic techniques have been developed and are being developed which works with the above concerned objects.

2 Image Steganography Model

A basic steganographic model is shown in figure 1.
The process of embedding can be explained as:

Let C represents the cover object, and Z the stego-image. Let K be a stego-key, and let M be the message that the sender wishes to send. Then, E_m represents an embedded message and E_x represents the extracted message. Therefore,

$$E_m: C \oplus K \oplus M \rightarrow Z;$$
$$E_m: (Em(c,k,m)) \approx m, \forall c \in C, k \in K, m \in M$$

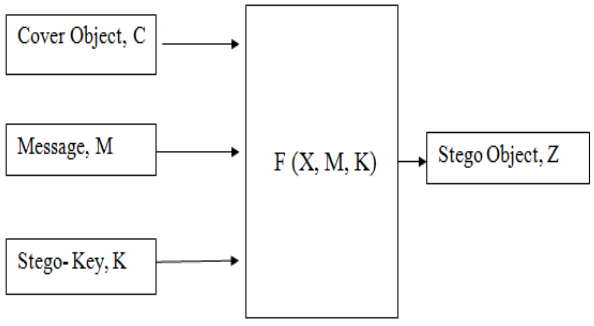

Figure1. Basic Model of Steganography [22]

3 Image Steganography in Spatial Domain

Spatial domain steganographic technique is a relatively simple technique that creates a covert channel in those parts of the cover image in which changes are likely to be imperceptible. The Spatial domain technique

embeds information in the intensity of the pixels directly. . One of the spatial domain technique based method is LSB insertion. This method is basically based on the fact that the least significant bits in an image can be thought of as random noise, and consequently they become not responsive to any changes on the image. Consider an 8-bit grayscale bitmap image where each pixel is stored as a byte representing a grayscale value. Suppose the first eight pixels of the original image have the following grayscale values: (11010010 01001010 10010111 10001100 00010101 01010111 00100110 01000011). To hide the letter A whose binary value is 10000001, we would replace the LSBs of these pixels to have the following new grayscale values: (11010011 01001010 10010110 10001100 00010100 01010110 00100110 01000011).

The other most well known technique in spatial domain is the masking and filtering. Masking and filtering techniques are mostly used on 24 bit and grey scale images. Sometimes they are used as digital watermarks also. Performing masking on an image results in the changed luminance of the masked area. The smaller the luminance change, the less chance of it being detected. Masking is more robust than LSB insertion with respect to compression, cropping, and some other image processing functions. Masking techniques embed information in significant areas than just hiding it in the "noise" level and this makes it more suitable than LSB for lossy JPEG images

The Multi Bit Plane Image Steganography (MBPIS) was proposed by Nguyen, Yoon and Lee [10]. They just extended the simple LSB substitution to the multiple bit planes.

Zhang and Wang [8] also presented an adaptive steganographic scheme with the Multiple-Based Notational System (MBNS) based on human visual system (HVS). In this secret data is converted into symbols represented by variable bases in a notational system. But in this, the stego image quality degradation is almost invisible to the human eye.

Another spatial image steganography technique proposed by B. Chen and Wornell is Quantization image modulation [9]. QIM is a commonly used data embedding technique in digital watermarking. It quantizes the input signal x to the output y with a set of quantizer. The quantizer for quantization is determined by the message bit m. Iuon-Chang Lin [11] proposed a Data hiding scheme with distortion tolerance which uses spatial domain for hiding data. This method provides distortion tolerance and gives better quality of processed image. This scheme provides effective results than other schemes in terms of distortion tolerance. From the above, we conclude that the resulting stego-image using LSB techniques are very difficult to be recognized by the human eye due. Moreover, such techniques are simple to implement and popular. The disadvantage of this technique is that it uses each pixel in the image. As a result, if lossy compression is used, some of the hidden information might be lost.

4 Image Steganography in Transform Domain

The Transform domain technique embeds information in frequency domain of the transformed image. Most of the strong steganographic systems today operate within the transform domain. The main advantage of transform domain technique over the spatial domain is that these hide the image in the area that is less exposed to the compression, cropping and image processing. This technique runs on both lossy and lossless image formats .The widely used transformation functions include Discrete Cosine Transformation (DCT), Discrete Fourier Transform (DFT), and Wavelet Transformation.

As for steganography in DCT domain, JSteg [12] is the classical JPEG steganographic tools utilizing the LSB embedding technique. JSteg embeds secret data into a cover image by successively replacing the LSBs of non-zero quantized DCT coefficients with secret message bits. Various JPEG steganography based methods have been developed. JPHide is another classical JPEG steganographic tool utilizing the LSB embedding technique. Unlike JSteg, the quantized DCT coefficients that will be used to hide secret message bits in JPHide are selected at random by a pseudo-random number generator, which may be controlled by a key. Westfeld [6] introduced F5 algorithm. In this, the absolute value of the coefficient is decreased by one if it is needed to be modified instead of re-placing the LSBs of quantized DCT coefficients with the message bits. The advantage of F5 algorithm is that it minimizes the necessary number of changes to hide a message of certain length. OutGuess proposed a better technique which includes the ability to preserve statistical properties. It used pseudo random generator to select the DCT coefficients. Yet Another Steganographic Scheme (YASS) [7] belongs to JPEG steganography but it does not embed data in JPEG DCT coefficients directly. Another technique is perturbed quantization (PQ) [13], which aims to achieve high efficiency, with minimal distortion, rather than a large capacity. Each coefficient in the DCT block is assigned a scalar value that corresponds to how much impact it would make to the carrier image. In the recent year DWT based algorithm for image data hiding has been proposed that uses CH band of cover image for hiding the secret message.

Wavelets transform (WT) transforms the spatial domain data to the frequency domain data. Wavelets are used in the image steganographic model because the wavelet transform clearly partitions the high-frequency and low-frequency information on a pixel by pixel basis.

5 Adaptive Image Steganography

Adaptive image steganography is a form of improved image steganography. Adaptive steganography is a special case of the two former methods. It is also known as ''Statistics-aware embedding'', ''Masking'' or ''Model-Based'' Adaptive steganography considers statistical global features of an image before interacting with its LSB/DCT coefficients. The statistics decides where to make the changes. It is characterized by a random adaptive selection of pixels depending on the cover image and the selection of pixels in a block with large local STD (standard deviation).

An adaptive least-significant bit (LSB) steganographic method was proposed. This method includes pixel value differencing (PVD) which uses the difference value of two consecutive pixels to estimate the total number of secret bits that can be embedded into the two pixels. This approach helps to differentiate the smooth and edge areas. A k-bit LSB substitution method is used for hiding data in the pixels located in the edge areas. The range of difference values is adaptively divided into three different levels that are lower level, middle level, and higher level. This method results in larger payload capacity and high image quality.

Another method proposed under adaptive image steganography is LSB Matching. The LSB matching scheme was introduced by A. Ker et al., [14]. LSB matching randomly increases or decreases the pixels. BPCS (bit plane complexity segmentation) [15] was introduced by J. Spaulding et al to compensate for the drawback of the traditional LSB manipulation techniques of data hiding

Chin-Chen et al. [21], propose an adaptive technique for index- based images using codeword grouping applied to the LSB substitution method. Their idea is to exploit the correlation between neighboring pixels to estimate the degree of smoothness. The resulting embedding capacity was high.

Yang et al. [16] proposed an adaptive LSB steganographic method using PVD and LSB replacement. In their scheme, the difference value of two consecutive pixels is used to estimate the hiding capacity into the two pixels. Pixels located in the edge areas are embedded by a *k*-bit LSB substitution method. The scheme embeds more secret data into edged areas than smooth areas in the host image. In [17], a GA-based algorithm is presented which generates a stego-image to break the detection of the spatial domain and the frequency-domain steganalysis systems by artificially counterfeiting statistical features.

A new method which makes use of more surrounding pixels around a target pixel to find the most appropriate capacity value in order to improve imperceptibility was introduced [20]. As compare to other steganographic techniques which use either three or four adjacent pixels around a target pixel, this technique is able to utilize all eight adjacent neighbors, which improves the imperceptibility value.

6 STEGANOGRAPHY AND CRYPTOGRAPHY

Steganography is different from cryptography[5]. Steganography is a type of cryptography in an obscure manner [19]. In cryptography, the message is altered to a form which is impossible to detect unless the key to decrypt it is available. While, the goal of steganography is to hide messages inside other harmless messages in a way that does not allow any enemy to even detect that there is a second secret message present. Even though both methods provide security, to add multiple layers of security it is always a good practice to use Cryptography and Steganography together. The combination of these two methods will enhance the security of the data embedded. This combined chemistry will satisfy the requirements such as capacity, security and robustness for secure data transmission over an open channel. The steganography and cryptography differ in the way they are evaluated: steganography fails when the "enemy" is able to access the secret key used, while cryptography fails when the "enemy" detects that there is a secret message present in the steganographic medium. An optical cryptosystem with adaptive steganography is proposed for video sequence encryption and decryption. The optical cryptosystem employs a double random phase encoding algorithm to encrypt and decrypt video sequences. The video signal is first transferred to RGB model and then separated into three channels: red, green, and blue. For higher security, an asymmetric method is applied to cipher session keys. Kavitha et al [18] applied both cryptography and steganography to the colored images and the resulting system was more robust than that with either cryptography or steganography.

7 ANALYSIS

So as to analyze the performance of any steganographic system its main requirements, security, capacity, and imperceptibility, may be used to rate its performance.

As a performance measure for image distortion due to embedding, the well-known peak-signal-to noise ratio (PSNR), which is categorized under difference distortion metrics, can be applied to stego images as:

$$PSNR = 10 \log\left(\frac{C_{max}^2}{MSE}\right)$$

Where MSE denotes the mean square error, which is given as:

$$MSE = \frac{1}{MN} \sum_{x=1}^{M} \sum_{y=1}^{N} (S_{xy} - C_{xy})^2$$

Where x and y are the image coordinates, M and N are the dimensions of the image, S_{xy} is the generated stego-image and C_{xy} is the cover image. Also C^2_{max} represents the maximum value in the image.

8 CONCLUSION

This paper presented a discussion on the major algorithms of steganography deployed in digital imaging. Both transform domain and spatial domain have their own benefits and flaws. One can deduce that while one technique may lack in payload capacity, another may lack in robustness. Generally transform domain methods have a lower payload compared to spatial domain algorithms. Also spatial domain techniques are easy to implement as compared to those in transform domain. Spatial domain technique Adaptive LSB steganography has benefit of high payload capacity and not too prone to attacks, especially when the secret data is short in size. Steganography when combined with cryptography results in a more secure and robust system. So we conclude by saying that there are large number techniques for implementing image steganography. As steganography requires that the cover image must be carefully selected. Thus, for a person to send secret data using steganographic techniques he or she must select a suitable steganographic technique in a particular domain and suitable cover image as well .In short, one has to compromise on some characteristics to ensure the high performance of other characteristics.

9 ACKNOWLEDGEMENT

Many thanks to Ms. Mamta Juneja, Assistant Professor in UIET, Panjab University Chandigarh, for doing this literature review.

10 REFERENCES

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

[2] Nagham Hamid, Abid Yahya, R. Badlishah Ahmad & Osamah M. Al-Qershi "Image Steganography Techniques: An Overview" International Journal of Computer Science and Security (IJCSS), Volume (6): Issue (3):2012.

[3] Robert Krenn, "Steganography and steganalysis", An Article, January 2004.

[4] Yang You, Yu Ping, Xu Jiangfeng "An improved LSB algorithm based on multi-transformation" In Proc. 2008 International Symposium on Information Science and Engineering (ISISE'08). Shanghai (China), Dec. 20-22, 2008, vol. 1, p. 487-491.

[5] Cryptography – Wikipedia, http://en.wikipidea.org/wiki/Cryptography

[6] Andrew Westfeld, F5-a steganographic algorithm: high capacity despite better steganalysis, Proc.of the 4th Information Hiding Workshop, vol. 2137, pp. 289-302, Springer, 2001

[7] K. Solanki, A. Sarkar, and B. S. Manjunath, Yass: Yet another steganographic scheme that resists blind steganalysis,Proc. of the 9th Information Hiding Workshop, Springer, vol. 4567, pp. 16-31, 2007.

[8] Xinpeng Zhang and Shuozhong Wang, Steganography using multiple-base notational system and human vision sensitivity, IEEE Signal Processing Letters, vol. 12, no. 1, pp. 67-70, 2005.

[9] B. Chen and G. W. Wornell, Quantization index modulation: A class of provably good methods for digital watermarking and information embedding, IEEE Trans. Information Theory, vol. 47, no. 4, pp. 1423-1443, 2001.

[10] B.C. Nguyen, S.M. Yoon et H.-K. Lee: Multi bit plane image steganography. Proc. Digital Watermarking, 5th International Workshop, IWDW 2006, volume 4283 de Lecture Notes in Computer Science, pages 61–70, Jeju Island, Korea, November 2006. Springer

[11] I.-C. Lin et al , "Hiding data in spatial domain images with distortion tolerance", Computer Standards & Interfaces 31 (2009) 458–464.

[12] Derek Upham. Jsteg, http://zooid.org/~paul/crypto/jsteg.

[13] J. Fridrich, M. Goljan, D. Soukal, Perturbed quantization steganography, ACM Multimedia and Security Journal 11 (2) (2005) 98–107.

[14] A. Ker, "Steganalysis of LSB Matching in Grayscale Images." IEEE Signal Processing Letters, vol. 12(6), pp. 441–444, 2005

[15] J. Spaulding, H. Noda, M.N. Shirazi, E. Kawaguchi, BPCS steganography using EZW lossy compressed images, Pattern Recognition Letters 23 (13) (2002) 1579–1587.

[16] Cheng-Hsing Yang, Chi-Yao Weng, Shiuh-Jeng Wang, Hung-Min Sun Adaptive data hiding in edge areas of images with spatial LSB domain systems. *IEEE Transactions on Information Forensics and Security*, 2008, vol. 3, no. 3, p. 488-497.

[17] Y.T.Wu, F.Y.Shih, Genetic algorithm based methodology for breaking the steganalytic systems, IEEE Transactions on Systems, Man, and Cybernetics—part B: cybernetics36 (1)(2006) 24–31.

[18] Mrs. Kavitha, Kavita Kadam, Ashwini Koshti, Priya Dunghav / International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 Vol. 2, Issue 3, May-Jun 2012, pp. 338-341.

[19] I. Venkata Sai Manoj, "Cryptography and Steganography", International Journal of Computer Applications (0975 – 8887), Volume 1 – No.12.

[20] Masoud Afrakhteh and Subariah Ibrahim, "Adaptive Steganography Scheme Using More Surrounding Pixels", IEEE International Conference On Computer Design And Applications (2010).

[21] C.C. Chang, P. Tsai, M.H. Lin, An adaptive steganography for index- based images using codeword grouping, Advances in Multimedia Information Processing-PCM, Springer, vol. 3333, 2004, pp. 731–738.

[22] Information hiding using steganography by Muhalim bin Mohamed Amin,Puan Subariah Ibrahim, Puan Mazleena Salleh, Mohd Rozi Katmin, Vote No: 71847, Universiti Teknologi Malayasia