IOSR Journal of VLSI and Signal Processing (IOSR-JVSP)
Volume 4, Issue 4, Ver. I (Jul-Aug. 2014), PP 29-31
e-ISSN: 2319 – 4200, p-ISSN No. : 2319 – 4197
www.iosrjournals.org

A Survey of Recent Embedding Techniques and Security Measures in Steganography

Gudapati Sri Kali
Department of ECE,Assistant Professor,
Saveetha School of Engineering,Saveetha University

***Abstract*:** *Steganography is an act of hiding a message, image or file in another message, image or file such that only the intendant sender and receiver know the existence of the secret message. Steganography takes the advantage of the redundancy of data in the cover media to insert the secret data. The steganography requires sufficient embedding capacity as well as security. This paper revises different embedding techniques most popularly used and the security measures to enhance the goal of steganography.*
***Index Terms*:** *Steganography, Cryptography, Payload*

I. Introduction

Security is an important aspect to concentrate while transferring the data or files through internet because of the rapid growth of the multimedia and network. There are four specific security requirements,

- Authentication: The process of validating one's identity.
- Privacy/confidentiality: Protecting the concealment of the message.
- Integrity: Assuring the loyalty of the receiver that the message has not been altered after the secret data is received
- Non-repudiation: A conformation that the sender has sent the message.

The two main technologies used in recent days to enhance the communication security are data hiding and cryptography. Data hiding is a technique that conceals data into a carrier for conveying secret messages confidentially [1],[2]. Steganography is one of method of data hiding. The purpose of both cryptography and steganography is to send secret data, the only difference is the way the data is been transmitted. Secured data transmission has started with cryptography. Cryptography is a form of data sharing where the data is kept secret (fig i) . Cryptography provides authentication and integrity.

Steganography deals with hiding information in an image, audio file or in a video file into another digital media (text, image, audio or video streams). The media used to hide the secret data is called the cover. Recently, images have been a very popular choice as a cover medium primarily in many applications in daily life because of its redundancy[3] .

If a digital image is used as cover then it is called cover image. The cover image that has secret message concealed in it is called a stego-image (or stego-media) (Fig 1)

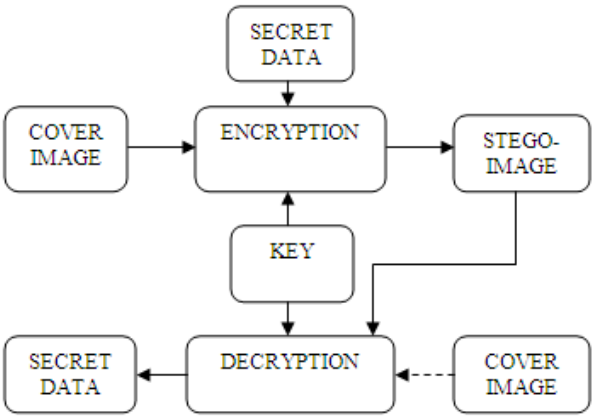

Fig 1. Steganography block diagram

The major concerns of data hiding are payload and invisibility. The payload of a data hiding scheme refers to the amount of the secret data that can be embedded into the cover image and the term invisibility

indicates how covert the fact is to illegal users when the cover image has been manipulated and turned to be a stego-image. In order to maintain the imperceptibility, the data hiding techniques usually alters the most insignificant bits of the cover image. It attempts to establish covert communication between intendment recipients and prevent malicious intruders or attackers from discovering the existence of the hidden message in the stego-image.

II. Embedding Techniques

The least significant bit (LSB) substitution method proposed by is a famous data hiding technique. This method is easy to implement and also costs less. Thereby it has become one of the popular methods for embedding technique. However, LSB embedding method is prone to steganalysis, as the pixels are modified according to their values. The pixels with even values are incremented by one else they remain unmodified and the pixels with odd values are decremented by one else they remain unmodified.

The LSB method uses a single bit for embedding purpose. Usually the right most bit is used for embedding the data. The data-hiding methods which employs two pixels as an embedding unit for hiding a message digit SB in a B-ary notational system is termed as pixel pair matching (PPM). The OPAP scheme proposed by Chi-Kwon Chan and L.M Cheng [4,5], was developed scheme modifies the embedded bits in order to improve the overall visibility of the stego image. This scheme is an improvement over the LSB based algorithm

In exploiting modification direction (EMD) method proposed by X.Zhang and S.Wang et al. [6] in 2006 , only a single pixel is changed in a pixel pair one gray-scale unit at a maximum and a message digit can be embedded in a 5-ary notational system. Therefore, the payload is (1/2)log25=1.161 bpp. LSB matching and EMD increases the image quality with the same payload. These two methods are not suitable for applications requiring high payload since the maximum payloads of LSB matching and EMD are only 1 and 1.161 bpp, respectively.

The embedding method of LSB matching and EMD does not increase the payload. In 2009, Chao et al.[7] proposed a diamond encoding (DE) method to increase the payload. Instead of increasing the payload, Wang et al [8] in 2010 proposed a method to increase the image quality of the stego image. Wein Hong et al.[9] in 2012 proposed APPM for increasing the embedding capacity and also the image quality.

III. Security Measures

Steganography finds its applications in essential banking communication, electronic data transfer, electronic health record, police services and military. The main factor that attracts steganography for these applications is security. The steganographic method is secure enough

(i) If the embedding technique is adventitious and the secret data is autonomous from both the cover and the stego object. Detectability is the ability of the attacker to detect the embedding operation with the knowledge of the cover and the stego image.

The equation for detectability is given as

$$D(Pc||Ps) = \int Pc \log(\frac{Pc}{Ps}) \quad \ldots\ldots(1)$$

Where

Pc is the probability distribution of the cover image

Ps is the probability distribution of the stego image.

The stego system is said to be fully secure if D=0.

(ii) If there are no statistical differences between the cover and the stego-image.The quality between the cover and the stego image is calculated using the peak signal to noise ratio(PSNR). PSNR is given by

$$PSNR(db) = 10 * \log(\frac{255^2}{MSE}) \quad \ldots\ldots (2)$$

The mean square error is given by

$$\text{MSE}= \frac{1}{mn}\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}[I(i,j) - K(i,j)] \quad \ldots\ldots(3)$$

Where I is the cover image

K is the stego image

m and n are the number of rows and columns of the image respectively.

(iii) If the relative entropy of the stego image and the cover image is zero. Entropy is the measure of the uncertainty of the random variables.

IV. Security Analysis Tools

The main aim of the steganography is to deceive statistical detection. There are many methods available like MSE calculation, Subtractive Pixel Adjacency Matrix(SPAM) proposed by Pevny et al.[10] and HVDH scheme proposed by Zhao et al.[11]. The MSE calculation method fails in the case of LSB Matching techniques with low MSE also, is easily detectable. The SPAM and HVDH are discussed in this section.

A. Subtractive Pixel Adjacency Matrix(SPAM)

The SPAM analysis is used to detect the stego image. SPAM the the transition probabilities along eight directions are calculated the features of images are obtained. SPAM order and the range of difference determines the number of features . the steganalyzer is implemented using a soft-margin support vector machine (SVM) with Gaussian kernel is employed. The error rate (eq) is used to evaluate the security of the data hiding method against the detection of SPAM.

PErr=1/2 (PFp+PFn)

Where

PFp, PFn is the probability of false positive and negative respectively. The lower error rate implies the detectability of the stego image is higher.

B. Horizontal and Vertical Difference Histogram (HVDH)

HVDH is also one of the recent steganalysis technique used to detect the stego image based on the histogram differences. In this method the distance between the horizontal difference histogram H'h and vertical difference histogram H'v is calculated. The distance D is calculated by

$$D = \left(\sum_{i=-2T}^{2T} (H'h\,(i) - H'v(i)) \right)$$

Where T is the predefined threshold. From the equation it can be noticed that if the H'h and H'v increases the D value also increases. The larger D value indicates the image is embedded with messages.

V. Conclusion

In this paper, different techniques are discussed for embedding data in an image. Later various security measures are outlined. SPAM and HVDH methods are presented to perform the security analysis. The content in this paper will be a source of inspiration for future research directions. The increase in security leads to compromise in the capacity to same extent. This information can be used to develop a solution for relating the security and the capacity.

References

[1]. J. Fridrich, Steganography in Digital Media: Principles, Algorithms, and Applications. Cambridge, U.K.: Cambridge Univ. Press, 2009.

[2]. N. Provos and P. Honeyman, "Hide and seek: An introduction to steganography," IEEE Security Privacy, vol. 3, no. 3, pp. 32–44, May/Jun. 2003.

[3]. Bin Li, Junhui He, Jiwu Huang, Yun Qing Shi, "A Survey on Image Steganography and Steganalysis", Journal of Information Hiding and Multimedia Signal Processing, Vol.2, Issue 2, pp. 142-172, April 2011.

[4]. Chi-Kwong Chan, L.M. Cheng, "Improved hiding data in images by optimal moderately signifcant-bit replacement", IEE Electron Lett. 37 (16) (2001) 1017–1018.

[5]. Chi-Kwong Chan, L.M. Cheng, "Hiding data in images by simple LSB substitution", Pattern Recognition, Vol.37, pp. 469-474, 2010.

[6]. X. Zhang and S. Wang, "Efficient steganographic embedding by exploiting modification direction," IEEE Commun. Lett., vol. 10, no. 11,pp. 781–783, Nov. 2006.

[7]. R.M. Chao, H. C. Wu, C. C. Lee, and Y. P. Chu, "A novel image data hiding scheme with diamond encoding," EURASIP J. Inf. Security, vol. 2009, 2009, DOI: 10.1155/2009/658047, Article ID 658047.

[8]. J. Wang, Y. Sun, H. Xu, K. Chen, H. J. Kim, and S. H. Joo, "An improved section-wise exploiting modification direction method," Signal Process., vol. 90, no. 11, pp. 2954–2964, 2010.

[9]. Wein Hong and Tung-Shou Chen, "A Novel Data Embedding Method Using Adaptive Pixel Pair Matching,"IEEE Trans,Inf. Forensics Security,vol.7,no. 1,February 2012

[10]. T. Pevný, P. Bas, and J. Fridrich, "Steganalysis by subtractive pixeladjacency matrix," IEEE Trans. Inf.Forensics Security, vol. 5, no. 2, pp. 215–224, Jun. 2010.

[11]. H. Zhao, H. Wang, and M. K. Khan, "Statistical analysis of several reversible data hiding algorithms," in Proc.Multimedia Tools and Applications,2009, DOI: 10.1007/s11042-009-0380-y.