WWJMRD 2018; 4(1): 215-218
www.wwjmrd.com
International Journal
Peer Reviewed Journal
Refereed Journal
Indexed Journal
UGC Approved Journal
Impact Factor MJIF: 4.25
e-ISSN: 2454-6615

Rasmi.A
Research Scholar, Computer Science and Engineering
Karpagam University
Tamilnadu, India

Correspondence:
Rasmi.A
Research Scholar, Computer Science and Engineering
Karpagam University
Tamilnadu, India

Recent Analysis of Secret Communication Using Image Steganographic Techniques

Rasmi.A

Abstract
In the electronic era because of the extensive use of network technology, security measures play, a vital role for data transmission between sender and receiver. Steganography is the science of masking data bits in a secure manner using cover file, for various purposes. This paper explores and analyses some of the existing steganographic methods from its earliest instances through potential future application

Keywords: Steganography, Data embedding, Cover image, Stego file, Spatial domain

Introduction

Steganography is the art and science of clandestine communication by hiding information into a digital file in a statistically untraceable way. Steganography was first experienced and recorded by Greek people in their golden era for conveying secret information between intended clients. Steganography means covered writing which is originated from the greek words “steganos” and “graphia” and can be applied to perform hidden exchanges in a secure mode. This technique employs the features of human visual system in a promising manner to ensure the secrecy of data communication. Some of the existing data hiding techniques are watermarking, cryptography and Steganography [1, 2].

In ancient days Egyptians used a secret code known as hieroglyphic language which provides furtive communication between users. Similarly during the second world war period , spying agents exploited photographically generated microdots to exchange data. In this masking method the sender embeds the secret data to be sent into the digital media where only the particular customer can extract it. The main components of steganographic techniques are cover image, embedding algorithm, message, extraction algorithm and stego Image [3, 4, 5].A general steganography model is shown in figure.1

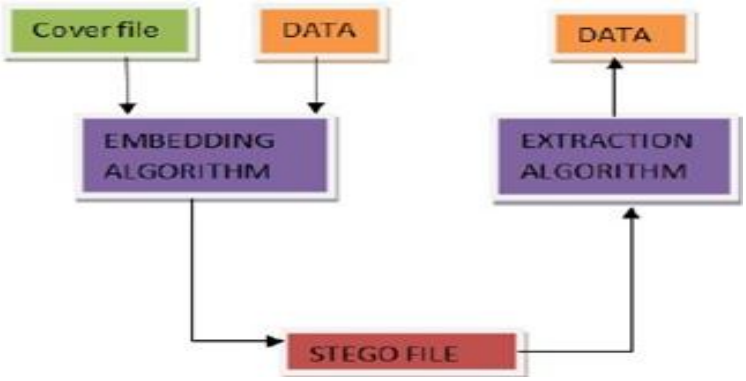

Fig.1: A general Steganography model

The original data file which is used as a carrier is known as cover file. It may be image, text, video or audio. The secret data that the sender wants to be kept confidential is the message, it

it may be image ,text, video or audio .Message is also termed as payload. After embedding payload into cover file the resultant one is stego file. Because of the disguising features of steganographic technique the data is only visible to the intended recipient but to all others it is invisible. It is somewhat similar to the postal system, sending a letter from one place to another,here the envelope without letter acts as cover, so after inserting letter into envelope it becomes stego. Here the letter acts as the payload. [6, 7,8]

Generally Steganography can be stated as the camouflaged making of a stego file and extracting the secret message from it in a protected manner without modifying the cover file. Based on the nature of cover file used for data hiding, different categories are derived they are network steganography, text steganography, image steganography, video steganography and audio steganography. In image steganography the cover file is in image format. If considering cover medium as network protocol it is called network steganography. Video steganography and audio steganography are the methods of hiding secret data inside a video file and audio file respectively. But the most commonly used steganography is image steganography, and the available image formats are graphics interchange format(GIF), joint photographic experts group(JPEG),bit map format(BMP),and portable network graphics (PNG). [9,10]

The ultimate goal of steganography is to enhance the security of covered communication by modifying the redundant bits of an image in an innocuous manner, thus Ensuring that the foe should not suspect the existence of data in the cover file. In general while designing an algorithm to embed data it should meet high payload capacity, robustness, good imperceptibility and less image distortion then only it ensures secure data transfer. The main objective of steganography is to minimize the noticeability of the embedded data by using some protecting techniques in an effective style. A digital image can be denoted as I(p, q), where p=1….n, and q=1….m, is a set of n×m matrix of pixels, where each pixel is an element of the digital image. An image can be defined as a group of pixels. Pixel depth of an image is represented as the total number of bits in an image. Each pixel can be represented either as a group of 8 bits or 24 bits, while considering gray scale image, it uses 8 bits per pixel, where as in colour image each pixel is a collection of 24 bits. Gray scale image is capable of representing 28 combinations, so it can represent 256 different shades of gray, which ranges from 0 to 255. Colour image is capable of representing 224 colour combinations. In colour image each byte is a collection of red, green and blue colours in a predefined order. The value of each byte ranges from 0 to 255. Image steganography techniques can be partitioned into two broad categories namely spatial domain techniques and transform domain techniques.[11,12,13]

In spatial domain pixels are customized directly, where as in transform domain modifications are taken place indirectly. Spatial domain is also known as image domain, in which the secret message is embedded directly into the cover file without modifying the pixel value. In transform domain technique images are first altered and the secret data is inserted into the image. Transform domain is also termed as frequency domain.

Spatial domain schemes are much simpler and computationally fast compared to frequency domain, so most favored one is spatial domain. In spatial domain the most prominent technique is least significant bit (LSB) substitution method which replaces the least significant bit of the cover file with the secret data bit, so get the resultant stego bits. While choosing cover file certain factors have to be monitored, data size should be less than cover size, otherwise will create artifacts, so proper size of data has to be selected for accurate embedding process. The quality of the stego image can be examined by applying the peak signal to noise ratio, which is denoted as PSNR. It is expressed in dB. PSNR is expressed as follows:

$$PSNR = 10 \cdot \log_{10}\left(\frac{MAX_I^2}{MSE}\right)$$
$$20 \cdot \log_{10}\left(\frac{MAX_I}{\sqrt{MSE}}\right)$$
$$20 \cdot \log_{10}(MAX_I) - 10 \cdot \log_{10}(MSE)$$

In the above expression MAXI is 255 for gray scale image and MSE stands for the mean squared error. MSE find out the difference between the cover file and the stego image, it is calculated by the following equation.[14,15,16]

$$MSE = \frac{1}{m\,n}\sum_{i\ 0}^{m-1}\sum_{j\ 0}^{n-1}[I(i,j) - K(i,j)]^2$$

Where I (i,j) stands for the cover image, K(i,j) is the stego image, ‘m’ denotes the height and ‘n’denotes the width of the image. The binary bit of a cover file is represented as given below:

10011011 01101010 10110100
01001010 10001101 11101100

And we want to embed 6 bits of data: 101101 into the cover, so after applying LSB technique the resultant stego is as follows:

10011011 01101011 10110100
01001010 10001101 11101101

Least bit significant bit substitution only replaces the last bit of cover image with the data bits so we get the stego, the bold and underlined bit is the newly added bit. It is simple and easily detectable one and less number of secret information can be hidden in this using LSB technique. [17, 18]

Steganography Techniques

Steganographic techniques can be broadly classified into spatial domain and transform domain. Different available spatial domain techniques are least significant bit substitution, pixel value differencing, edge based data embedding, random based embedding and gray level modification method. Frequency domain can be classified as discrete Fourier transformation, discrete cosine transformation, and discrete wavelet transformation. In [19] Atallah, and AL. presented a method, which hides the data into cover image only after checking the identical bits existing between the cover file and secret data. If it finds similarity it uses the corresponding bits to hide the secret data, otherwise it uses the least significant bts of the cover file. The hiding locations are identified by using a binary table. In this way the proposed algorithm generates a new stego image. In [20] Ko, chieu et.al. Proposed a novel data

embedding Scheme to improve the capacity of hidden data using tri-way pixel value differencing. In this method it utilizes three different directional edges for data hiding, whereas in the original pixel value differencing it uses only one direction. It also reduces the quality distortion of stego image and thus ensures secure data transfer of confidential information. Tri- way pixel value differencing uses three pairs of pixel values to embed the secret message. N [21] Linjie, Yun et.al. Introduced a minimal distortion embedding method known as uniform embedding distortions function. It is mainly applicable to side informed and non-side informed JPEG steganography. In uniform embedding it attempts to extend modifications uniformly to all the components of quantized discrete cosine transform coefficients. Thus it ensures less statistical detectability of the embedded data and also adds favorable secure embedding capacity. This proposed frame work aids to increase the safety measures and performance of steganography in an effective way. This scheme applies both syndrome trellis coding and uniform embedding approach for secure embedding of payload. In [22] Weixuan Jiwu et.al. Proposed a technique based on adaptive steganalytic scheme, which provides much stronger security than the non-adaptive techniques. The suggested model assigns different weights to different pixels, whereas the existing one offers same weight to each pixel so pixels located in high embedding probability region gains much higher weights than the pixels located in low embedding probability region. The main idea behind this adaptive steganalysis is that pixels located in textural regions have much more masking capacity compared to lighter regions. In the nearby future the proposed work can be extended to detect adaptive JPEG steganography by combining some other features. In [23] Bin ming et.al. Developed a technique called clustering modification directions in spatial steganography. In this the cover image is divided into several sub images, in which the secret data is embedded using additive distortion functions. The proposed system overcomes the statistical detectability faced by present steganalyzers with high dimensional features. After decomposing the cover image, it computes the initial cost for each pixel, then embed the first segment of data into the first portion of image, then update the costs according to the modified pixel directions, afterward embed the next data portion into the next segment of image and continue this till the last data segment. In this manner it generates the stego image. This improves the imperceptibility as well as the robustness by clustering both the directions and location of embedding modifications.

In [24] Prasanthi,et.al introduced a new method based on LSB spatial domain technique. It uses a truth table known as #table, which generates pseudo random numbers, so depending on the random numbers generated secret data is hidden at different positions of cover image. Thus the novel method provides good safety and robustness because without getting the #table details the trespasser cannot extract the secret data. The quality degradation of stego can be enhanced by using randomization method of data embedding. In [25] Linjie Yun et.al. Presented a refined model of uniform embedding. In this method the number of bits to be embedded must be proportional to the coefficient of variation of DCT components. It also employs all DCT coefficients such as the DC,zero, and non-zero AC coefficients as cover. When compared to existing uniform embedding method the proposed uniform embedding revisited distortion tries to homogeneously spread the relative modifications of statistics in such a manner that they are proportional to their DCT coefficient of variations. It ensures secure data embedding and high capacity when compared to the conventional methods. In [26] Lu Jie et.al. Described a technique for masking binary images into the gradient domain of a colour image, by altering the gradient vectors of colour file. It utilizes one pair of pixels to hide one binary bit, similarly applying multiple embedding vectors several binary images can be inserted in one image concurrently, thus ensures high embedding capacity than the traditional methods. It uses the features of human visual system to embed the message in a secure manner. It presumes that if nearby pixels in the host file have allied colour so it is capable of changing a gradient vector to the given direction, otherwise it chooses appropriate pixel pair for embedding of secret data.

In [27] Savita, shilpaet. al proposed a novel data hiding method to embed the data on the least significant bit value of a cover file using different progression techniques. The suggested method embeds a message into an image using modified spatial domain method, thus the experimental results summarized that the proposed one is more efficient and speedy compared to the existing least significant bit. It is only stipulated to gray scale images, so in the nearby future it can be extended to colour images.

Table 1: Summary of review

Paper Title	Algorithm Used	Merits	Demerits
Uniform embedding for efficient JPEG steganography [21]	Uniform embedding distortion function	less statistical detectability, and hence, more secure steganography	Inappropriate use of DC,AC coefficients may lead to artifacts
Adaptive steganalysis based on embedding probabilities of pixels [22]	Adaptive Steganography	Adaptive methods achieve stronger security	Data extraction is difficult
A strategy of clustering modification directions in spatial image steganography[23]	Clustering modification directions (CMD)	Intruder cannot trace the embedded data	It embeds data in heavily textured region
A new approach for data hiding with LSB steganography[24]	Four states# table LSB method	It ensures higher security,	More LSB bits replacement causes data degradation
Using statistical image for JPEG steganography :Uniform embedding revisited [25]	Uniform embedding steganography	It provides secure embedding capacity	computational complexity exists with wavelet domain.
Gradient domain binary image hiding using color difference metric [26]	Multiple hiding vectors	It preserves the image appearance and has better imperceptibility	If the colour change between adjacent pixel is higher ,this method is not applicable
Image steganography – least significant bit with multiple progressions [27]	Progression techniques of LSB	It is more efficient and fast compared to LSB	It is limited to grey scale images only

Conclusion and Future Trends

In this research frame work it tries to examine the background and future trends of steganographic techniques. Steganography can be applied in areas such as military agencies, cyber-crime and confidential data exchange. The ultimate aim of this paper is to examine the features of different existing steganographic methods in an efficient manner, and its strength depends on factors like imperceptibility, robustness and secret hiding capacity.

References

1. Tseng, Y.C., Chen Y.Y. Pan H.K.:'A secure data hiding scheme for binary images', IEEE Trans. Commun., 2002, 50,pp. 1227-1231.
2. Pawan R Sharma, Jitendra Mishra"A Comprehensive Survey on Data Hiding Technique" IRJET e-ISSN: 2395 -0056 Volume: 02 Issue: 04 July-2015.
3. Gurpreet Kaur, Kamaljeet Kaur "Digital Watermarking and Other Data Hiding Techniques" IJITEE ISSN: 2278-3075, Volume-2, Issue-5, April 2013, 181.
4. Provos, N. & Honeyman, P., "Hide and Seek: An introduction to steganography", IEEE Security and Privacy Journal, 2003.
5. Y.K. Lee, L.H. Chen, "High capacity image steganographic model", IEEE Proceedings on Vision, Image and Signal processing, Vol. 147, No.3,pp. 288-294, 2000.
6. X. Liao, Q. Wen and J. Zhang, "A steganographic method for digital images with four-pixel differencing and modified LSB substitution", Journal of Visual Communication and Image Representation, vol 22, no 1, pp. 18, 2011.
7. A. Rashid and M. K. R. Rashid, "Stego-Scheme for Secret Communication in Grayscale and Color Images", British Journal of Mathematics and Computer Sciences, vol. 10, no, 1 (2015), pp. 1-9.
8. Sandeep Kaur,Arunjot Kaur & Kulwinder Singh" A Survey of Image Steganography" IJRECE, Volume 2-Issue 3 June 2014, e- ISSN 2321-3159 p-ISSN 2321-3159.
9. Yambern Jina Chanu, Themrichon Tuithung, Kh. Manglem Singh "A Short Survey on Image Steganography and Steganalysis Techniques" IEEE-2012
10. Ge Huayong, Huang,"Steganography and Steganalysis Based on Digital Image", International conference & signal Processing-2011 IEEE.
11. Vijay KumarSharma, Vishalshrivastava, "A Steganography Algorithm for Hiding Images by improved LSB substitution by minizedetection."Journal of Theoretical and Applied Information Technology, Vol. 36 No.1, ISSN: 1992-8645, 15th February 2012.
12. Amitava Nag, Sushanta Biswas,"A Novel Techniques for image steganography based on DWT and Huffman Encoading", IJCSS, Vol(4):issue(6)
13. Hniels Provos & Peter Honeyman,"Hide & Seek: An Introduction to Steganography" IEEE Computer Society Pub- 2003.
14. M. Nosrati, R. Karimi, H. Nosrati, and A. Nosrati, "Embedding stego-text in cover images using linked list concepts and LSB technique", Journal of American Science, Vol. 7, No. 6, 2011, pp. 97-100.
15. Abbas Cheddad, Joan Condell, Kevin Curran, Paul Mc Kevitt, "Digital image steganography: Survey and analysis of current methods", Journal of Signal Processing, Elsevier, Volume 90, Issue 3, March 2010, pp.727-752.
16. M. Naseem, Ibrahim M. Hussain, M. Kamran Khan, Aisha Ajmal, "An Optimum Modified Bit Plane Splicing LSB Algorithm for Secret Data Hiding", International Journal of Computer Applications, Vol. 29, No. 12, 2011. Foundation of Computer Science, New York, USA, pp. 36-43.
17. Ming Sun Fu and O.C. Au, "Data hiding watermarking for halftone images", IEEE Transactions on Image Processing, Vol.11, No. 4, Apr. 2002, pp.477-484.
18. Soo-Chang Pei and J.M. Guo, "Hybrid pixel-based data hiding and block-based watermarking for error-diffused halftone images", IEEE Transactions on Circuits and Systems for Video Technology, Vol.13, No. 8, Aug. 2003, pp. 867- 884.
19. Atallah M. Al-Shatnawi, "A new method in image steganography with improved image quality", Applied Mathematical sciences, Vol.6, 2012, No. 79, pp 3907-3915.
20. Ko-Chin Changa, Chien-Ping Changa, Ping S. Huangb, and Te- Ming Tua " A novel image steganographic method using Tri- way pixel value differencing" Vol.3,No.2,2008,pp.37-44.
21. Linjie Guo, Jiangqun Ni,and Yun Qing Shi, "Uniform Embedding for Efficient JPEG Steganography "IEEE Transactions on information forensics and security, VOL. 9, NO. 5, MAY 2014, pp.814-825
22. Weixuan Tang, Haodong Li, Weiqi Luo,and Jiwu Huang, "Adaptive Steganalysis Based on Embedding Probabilities of Pixels" IEEE Transactions on Information Forensics and Security, 2015, DOI 10.1109/TIFS.2015.2507159
23. Bin Li,Ming Wang, Xiaolong Li, Shunquan Tan, and Jiwu Huang "A Strategy of Clustering Modification Directions in Spatial Image Steganography" IEEE Transactions on Information Forensics and Security, 2015, DOI:10.1109/TIFS.2015.2434600,
24. G. Prashanti and K. Sandhyarani, "A New Approach for Data Hiding with LSB Steganography", Springer International Publishing Switzerland 2015, Volume 2,DOI:10.1007/978-3-319-13731-5_46,pp.423-430.
25. Linjie Guo, Jiangqun Ni, Wenkang Su,Chengpei Tang, and Yun- Qing Shi, "Using Statistical Image Model for JPEG Steganography: Uniform Embedding Revisited" IEEE Transactions on Information Forensics and Security, VOL. 10, NO. 12, DECEMBER 2015,pp.2669-2680
26. Lu Hao, Jie Feng,and Bingfeng Zhou "Gradient Domain Binary Image Hiding Using Color Difference Metric", 2015 ACM. ISBN 978-1-4503-3930-8/15/11
27. Savita Goel, Shilpi Gupta, and Nisha Kaushik "Image Steganography – Least Significant Bit with Multiple Progressions", Springer International Publishing Switzerland 2015, DOI: 10.1007/978-3-319-12012-6_12.