Volume 8, No. 5, May-June 2017
ISSN No. 0976-5697
International Journal of Advanced Research in Computer Science
REVIEW ARTICLE
Available Online at www.ijarcs.info

A Review of Image Steganography Techniques: Development Trends to Enhance Performance

Aditi Sharma, Monika Poriye and Vinod Kumar
Dept. of Computer Science and Applications
Kurukshetra University, Kurukshetra, India

Abstract: Steganography deals with the study of invisible information. It is the art and science of hiding the existence of message being sent so that except sender and receiver no one knows about the sent message. Secret message is hidden inside mediums like text, images, network and protocol. These are used as carrier to hide the secret message without any significant change in the carrier which is visible to human eye. This doesn't cause any suspicion about the secret message. This paper presents the review of different security and data hiding techniques available that are used to implement the image steganography.

Keywords: Compression, Data hiding, LSB, Steganography, Stego-image and Visual Cryptography.

I. INTRODUCTION

With increased use of computers and web in every field like banking, medical and industries, the way of communication has undergone a revolution. In daily life, emails or telephones are used for sharing information. But due to increasing attacks like eavesdropping and phishing, it is not safe at all for the exchange of confidential information. This has increased the need of security while communication. Cryptography was used in classic methods of securing communication, which encrypts plaintext to generate cipher text using encryption key which is agreed upon by sender and receiver [**1**]. The encrypted message cannot be read by anyone without knowing the key. However, when encrypted message is transmitted, it can draw others attention towards the encrypted message that may thus be intercepted and decrypted. A solution to this problem is steganography. It is a Greek word and combination of two words – Steganos meaning covered and Graptos means writing, which means hidden communication. In this technique, the main idea is not only to hide the message but the fact of the existence of message is also hidden. Its main advantage is that it does not draw any unwanted attention towards the secret message. Information is hidden inside multimedia content like image, audio, video and text. The stego-image looks like the original image. For increasing the confidentiality of communicating data, the combination of both techniques can be used. The steganography involves three components: the "carrier", "the message", and "the key". The carrier carries the hidden message and it can be a painting, a picture, an audio file or a TCP/IP packet. A key is used as decoding mechanism for the hidden message.

The history of steganography can be traced back to 440 BC. Physical techniques of steganography were used that time. For example sending a message on the scalp of a person, invisible ink and wax tablets crunched into tiny balls .Nowadays, digital techniques are used for hiding information. The stego-image is compared with the cover image to evaluate the effectiveness of any steganographic technique. There are some factors that determine the efficiency of technique like Imperceptibility, Robustness, High Capacity, Accurate Extraction, PSNR (Peak Signal to Noise Ratio). Whenever a new steganographic algorithm is proposed, its performance is evaluated mainly on the basis of the three parameters which are hiding capacity, distortion measure, and security [**2**]. A tradeoff is to be maintained between these parameters to achieve better results as it is not possible to have all parameters perfectly in one algorithm. Although it is used in military communication and many other government organizations for secure communication but improvements are necessary for additional strengthening of the techniques against increasing threats against information exchange [**3**].

There is a branch called steganalysis involved with the detection of the presence of any hidden information. It uses feature extraction and classification methods of pixels in images or other mediums. The techniques used in steganalysis are based on identifying statistical features like mean and variance, calculating variation in gradient-energy, histogram methods to find differences between original and stego-medium. The applications of steganography are cyber warfare, computer forensics,
access control system for digital content distribution, tracking internet criminal activities [**4**]. It is also used to evaluate the weaknesses of the existing steganographic algorithms and improve their security. So, to design good algorithm for steganography, it is essential to know the concepts and techniques of steganalysis as well.

The rest of the paper is organized in following sections. Section II presents the basic model of Steganography followed by types of steganography in Section III. Section IV describes the steganography techniques available using image as cover to hide data. Section V gives performance evaluation parameters followed by conclusion in section VI.

II. BASIC MODEL

The basic model of steganographic system is as shown in figure 1. The sender hides secret information into carrier object by using stego-key without disturbing the quality of cover object. Thus, the basic components of a teganographic system include a message M, cover object C, stego-key K and function F(C,M,K) that gives an output as a stego-object, Z.

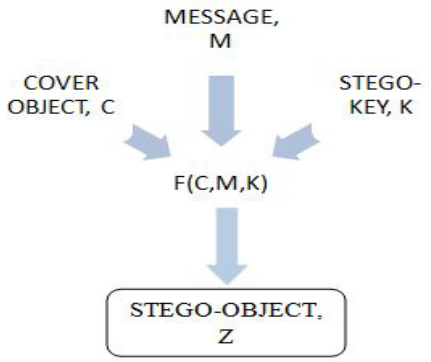

Fig.1: Model of Steganography

III. TYPES OF STEGANOGRAPHY

Steganography techniques are classified depending up on the cover medium used to hide secret data.

1. Text Steganography – It uses text documents to hide secret data inside white spaces, tabs of the document. Text messages have very less redundancy thus used very rarely.
2. Image Steganography – Images are used as cover medium due to the presence of redundancy in pixels of images.
3. Video Steganography- Videos are used as medium to hide information. The discrete fourier transform is calculated and the values are manipulated. The changes in videos are un noticeable to human eye. It can be done in formats such as mp4, MPEG, AVI.
4. Audio Steganography- The Voice over Internet Protocol leads to the familiarity of audio files as a cover medium. Message can be hidden in any audio formats like avi, mpeg, wave, midi by using methods such as Low Bit Encoding, Phase Coding, and Spread Spectrum.
5. Protocol Steganography- Secret message is hidden inside covert channels in OSI reference model. Here, the unused header bits of TCP/IP fields are used. TCP packet header has 6 unused bits and IP packet header has two reserved bits.

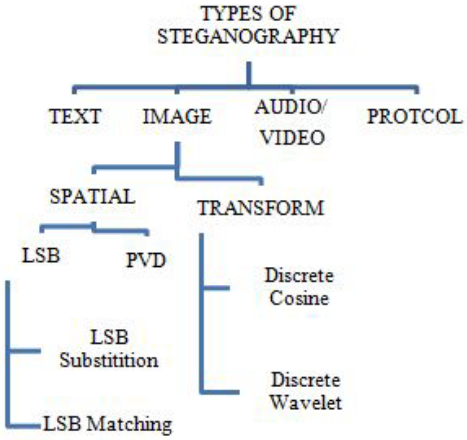

Fig. 2 Classification of steganographic techniques

IV. RELATED WORK

Steganography techniques have been used for ages to avoid suspicion for the secret messages. Work on image steganography is being done almost from decades. There is a high degree of redundancy available in images and millions of images are used
over internet especially by social media sites like facebook which make images as widely used medium for hiding information. Image steganography can be performed either in spatial domain or transform domain. In spatial domain methods, the secret data is embedded in the spatial domain where manipulations are made in the least significant bits (LSBs) of pixels [4]. In transform domain, the image is converted into transform domain of the cover image. It is a more advanced way of hiding message in an image. There are different types of frequency domain methods that include i) Discrete Fourier transformation technique (DFT) ii) Discrete cosine transformation technique (DCT) iii) Discrete Wavelet transformation technique (DWT).
LSB is the most commonly used method by many researchers to conceal message in cover file [**5**]. The constant efforts were made to increase the strength of the LSB algorithm to make it more robust. A LSB based image steganography approach was introduced in [**6**] where pixels of red matrix are X-ORed with secret key and based on the criteria for x-or value hidden information is placed in either LSB of blue or green channel. This method provides good security and less distortion as compared to earlier methods.
Another proposed method Signature Hiding Standard [**7**], an enhancement to LSB technique with a consideration of more secure data transfer technique takes binary image as input and embed it into RGB image. In this method, 1^{st} and 2^{nd} bits of current pixel decide the color of next pixel where data is to be embedded. Then, 4^{th} and 5^{th} bit decide the difference between current and next stego-pixel and number of bits of hidden data will be embedded depending upon 7^{th} and 8^{th} bit. It is robust against SPA (sample pair analysis) attack.
But to increase security, cryptography is used in combination with steganography. Moreover, compression techniques are also used to increase the payload capacity of stego-object. A system application was designed in [**8**] using lossless compression technique LZW to reduce size of hidden text before encryption. Further, tiny encryption algorithm (TEA) is applied and then LSB method is used to conceal message inside cover image. This is implemented on the android platform. This method provides double security and different types of noise like Gaussian noise addition, salt and pepper noise were added to check results which proved that the stego-image is resistant to noise addition. A new approach was proposed in [**9**] where steganography was achieved in two ways. In first method, an image is secured directly by encrypting it using S-DES algorithm and secret key then embedding this encrypted text in some other image. In second method, image was encrypted directly using S-DES algorithm and image key. The methods have been implemented using MATLAB and experimental results proved them secure.
Further improvement in LSB based color image steganography was proposed in [**10**]. Image is split into red, green and blue channels. Then, a matrix of the least significant bits of each Red, Green and Blue channel

respectively is generated. Then, LSBs of green channel are X-ORed with original color image. Cryptographic algorithm RSA is used for authentication to prevent forgery of hidden message.

A Novel Huffman Encoding Method in [**11**] compress message file to be hidden using Huffman encoding. Then, embedding is done using LSB of pixels of cover medium. Size of compressed message nd the Huffman table are also added as header inside cover image along with secret message.

Some researchers proposed the concept of hash-based approach. In [**12**], a novel hash-based approach was proposed where perfect hash function algorithm for color images was used that provides better speed. Earlier, hash based approaches using MD5 and SHA have some limitations caused by checksum method and cryptographic algorithms based on symmetric key are slower and do not work well for large amount of data. It can be used with different formats of images like jpeg, bmp, tiff, gif.

In [**13**], a method of concealing of data in Black and White images was proposed that used blocks to hide information instead of changing one or a pair **of** bits of pixels. A block of suitable size 2*2, 3*3 is selected and maximum two pixels are changed in 3*3 block and only one pixel in 2*2 block to keep up visual quality of the image. An odd-even feature of blocks was used. Bit 1 is inserted in odd numbered blocks and bit 0 is inserted in even numbered blocks. Central pixel is used to check whether bit is present in that block or not.

A new steganographic algorithm for RGB images was proposed in [**14**], where two different methods namely, Matrix Pattern (MP) and Least Significant Bit (LSB) were combined. Spatial domain of images is used by these two methods. In MP method, covered image is split into B×B blocks that are non-overlapping. Message is converted into $t_1 \times t_2$ matrix patterns. Then, data is hidden inside 4^{th} through 7^{th} bits of blue channel in that covered image. In the proposed algorithm, message is hidden inside first three bit layers and 4^{th} to 7^{th} bit layer of RGB cover image combining LSB and MP methods. The results showed that this new methodology has better capability than LSB and MP methods used separately. The stego-image has also a good PSNR value.

Some researchers proposed the concept of Visual Cryptography (VC) with image steganography. It is proposed by Naor and Shamir, and is a cryptographic scheme in which visual information is encrypted in such a way that it is not possible to get the secret information from a single image. For k out of n (k, n) visual secret sharing a secret image, shares of images are created which are sent independently over communication channel. They are meaningless images until k shares are combined as only then secret message can be retrieved [**15**]. A safe transmission method utilizing visual cryptography was proposed in [**16**] where secret message is encrypted using TEA and resultant message is embedded inside image. The resultant stego image is separated into n number of shares utilizing VC.

Another scheme is proposed in [**17**] using VC. Here, message is encoded simply using LSB Steganography replacing 8^{th} bit of each channel of RGB image with message bits. Then, (2, 2) shares of stego-image are created where one matrix has black pixels and other matrix has white pixels. Thus, for decoding OR of two shares is calculated at receiver end. Single share can not reveal hidden information.

The concept of Genetic Algorithm (GA) was used with VC in [**18**] . LSB based steganography is used to embed data where GA modifies the locations of pixels in stego-image so that detection of the presence of the embedded message becomes difficult. Finally, the resultant image is encrypted using VC. Two shares of stego-image are created based on threshold. It ensures enhanced security and improved reliability. It is resistant to RS attacks and stego-image has increased PSNR and MSE values due to changed pixel locations.

An improved technique in [**19**] is the one that uses most significant bit (MSB) to conceal secret message bit. The difference between bit no 5 and 6 is calculated based on which bit no 5 is replaced by bits of text message. If the difference is zero, bit 0 of the secret message is hidden and if difference is 1 then bit 1 is hidden. LSB's have become a lot of vulnerable to attacks by hackers. So, MSB is used in this technique so that stego-image cannot be easily detected by steganalysis techniques. Moreover, the results showed that the technique has better PSNR and payload capacity as well.

V. PERFORMANCE EVALUATION PARAMETERS

The main performance evaluation parameters for steganographic algorithms are following as shown in Table I:

TABLE I. PERFORMANCE EVALUATION PARAMETERS

S. No.	Parameter	Value
1.	Hiding Capacity	It should be high.
2.	Distortion Measure	It should be less.
3.	Security	It should be high.
4.	Algorithm Complexity	It should be less.

Hiding capacity is defined as the maximum range of bits that can be embedded inside the cover. Hiding capacity is expressed as bits per pixel (bpp) or bits per bytes (bpb). If the hiding capacity is higher, the technique will be better.

Distortion measure is the most commonly used parameter for performance evaluation. It is mainly measured using two metrics called MSE (Mean Square Error) and PSNR (Peak Signal to Noise Ratio). Their mathematical formulae are as follows:

$$\text{MSE} = \frac{1}{m \times n} \sum_{i=1}^{m} \sum_{j=1}^{n} (p_{ij} - q_{ij})^2$$

Where p_{ij} - the pixel values of original image at i^{th} row and j^{th} column.

q_{ij} - the pixel values of stego-image at i^{th} row and j^{th} column.

m - Number of rows in image.

n - Number of columns in image.

$$\text{PSNR} = 10 \times \log_{10} \frac{255 \times 255}{MSE}$$

The value of MSE should be less. The value of MSE is zero if the stego-image and original image are same. PSNR is

calculated using MSE. Higher the PSNR value, superior the image quality. The value of PSNR which is more than 40 decibels (dB) is very good [**2**]. The value between 30 dB and 40 dB is acceptable. But if value of PSNR is less than 30 dB, the distortion becomes higher. This makes value less than 30 dB unsatisfactory.

The security of steganographic technique is analyzed by its resistance towards various steganalytic schemes like RS analysis, pixel difference histogram analysis.

VI. CONCLUSION

Steganography aims to hide the existence of communication by embedding messages within another covered object. The overview of various steganographic techniques is presented in this paper based on the examination of techniques proposed in the literature of last few years. Steganography is being used in areas where the use of cryptography and strong encryptions are not enough. LSB is the most commonly used method. Different approaches have been used in combination with LSB to make this technique more robust. A lot of work has been done on RGB images also. Many steganographic techniques have been developed and used in practical applications for secure communication among different organizations.

Like any other science, there are also disadvantages along with numerous advantages. Terrorists and criminals use this effective technique for ill purposes thus making it dangerous at times. A special attention is thus needed towards this challenging area to make it more valuable.

REFERENCES

1. S. Aravind Kumar, J.Ramesh, K. Gunavathi S. Ahwin, "Novel and Secure Encoding and Hiding Techniques using Image Steganography:A Survey," in International Conference on Emerging Trends in Electrical Engineering and Energy Management, Coimbatore,India, 2012, pp. 171-177.
2. Kumar Sahu, G. Swain, K. Raja Sekhar, A. Pradhan, "Performance Evaluation Parameters of Image Steganography techniques," 2016.

A. Kumar Bhaumik, S. Bhowmik, "A New Approach in Color Image Steganography with high level of perceptibility and security," IEEE, pp. 283-286, 2016.

3. T. Tuithung, Kh. Manglem Singh, Y. Chanu, "A short survey on Image Steganography and Steganalysis Techniques," 2012.
4. S. Bansal, R.K. Bansal, S. Kaur, "Steganography and classification of Image Stegangraphy Techniques," IEEE, pp. 870-875, 2014.
5. Md. Saifur Rahman, Md. Ismail Hossain S.M. Masud Karim, "A new approach for LSB based Image Steganography using secret key," in Proceedin), Dhaka, Bangladesh, 2011.
6. M. Sharma K.Gupta, "Signature Hiding Standard(Hiding Binary Image into RGB Based Image)," 2014.
7. G. Budiman, L. Novamizanti S. Putra, "Implementation of Steganography using LSB with encrypted and compressed text using TEA-LZW on Android," 2014.
8. Madhusudan Vipul Sharma, "Two new approaches for Image Steganography using Cruyptography," in International Conference on image information processing, 2015, pp. 202-207.
9. W. Gong , WenLong Fu, LianJing Jin Xinyi Zhou, "An improved method for LSB based color image steganography combined with cryptography," 2016.
10. T RigDas, "A novel steganography method for image based on huffman encoding," in 3rd National Conference on Emerging Trends & Applications in Computer Science (NCETACS 2012).
11. Bajwa, M. Zaman Ali, R. Riasat, "A Hash based appphyroach for color Image Steganography," 2011 IEEE.
12. S. Shinde G. Chhajed, "Efficient Embedding in B&W Picture Images," 2010.
13. Nilchi, Amirfarhad Nilizadeh, "A novel Steganography method on Matrix Pattern and LSB algorithms in RGB Images," 20165.
14. P. Venkateswaran, Souvik Roy, "Online Payment System using Steganography and Visual Cryptography," IEEE, 2014.
15. P. Patel , D. Dubey, R. Jabi, "An efficient secure data tranmision based on visual cryptography ," 2016.
16. L. Anbarasi, M. Vincent D.R.L. Prasanna, "A novel approach for secret data transfer using image steganography and visual cryptography".
17. S. Natarajan G. Prema, "Steganography using genetic algorithm along with Visual Cryptography for wireless network application," no. IEEE, 2013.
18. F. Khalid,M. Shah, Z. Khan ,T. Mahmood,A. Khan A. Islam, "An Improved Image Steganography Technique Based On MSB using Bit Differencing, " IEEE, pp. 265-269, 2016.