International Journal of Advanced Information Science and Technology (IJAIST) ISSN: 2319:268
Vol.3, No.4, April 2014 DOI:10.15693/ijaist/2014.v3i4.57-60

A New Least Significant Bit Insertion Steganographic Method for High Imperceptibility

Mohanasundaram S S
Assistant Professor/Department of ECE,
P. A. College of Engineering and Technology,
Pollachi, Tamil Nadu, India.

Mani Bharathi V
PG Scholar/Department of PG Electrical Science
P. A. College of Engineering and Technology,
Pollachi, Tamil Nadu, India.

***Abstract*—Steganography is the art of hiding and transmitting data through apparently innocuous carriers in an effort to conceal the existence of the data, the word Steganography literally means covered or hiding writing as derived from Greek. Steganography has its place in security. It is not intended to replace cryptography but supplement it. Hiding a message with Steganography methods reduces the chance of a message being detected. Different carrier file formats like text, audio, image, video can be used, but digital images are the most popular to hide secret information because the slight modification in the cover image is hard to distinguish by human visual system (HVS).**

***Index terms* —Steganography, Stego-image, Cover-image, message, LSB, MSB.**

I. INTRODUCTION

Information security is essential for confidential data transfer. Security measures have become very necessary issue in the age of digital transmission of information via Internet. Two schemes are used to protect secret messages from being captured during transmission. One is encryption where the secret information is encoded in another form by using a secret key before sending, which can only be decoded with secret keys. The most popular encryption techniques are DES, RSA etc. Other way is steganography which is a technique of hiding secret information into a cover media or carrier.

In this paper steganography is discussed in detail. Steganography" is a Greek origin word which means "hidden writing". Steganography word is classified into two parts: Steganos which means "secret or covered" (where you want to hide the secret messages) and the graphic which means "writing" (text). However, in the hiding information the meaning of Steganography is hiding text or secret messages into another media file such as image, text, sound, and video.

The design of a steganographic system can be categorized into spatial domain methods and transform domain methods. In spatial domain methods, the processing is applied on the image pixel values directly. The advantage of these methods is simplicity. The disadvantage is low ability to bear signal processing operations. Least Significant Bit Insertion methods, Pallet based methods come under this category. In transform domain methods, the first step is to transform the cover image into different domain. Then the transformed coefficients are processed to hide the secret information. These changed coefficients are transformed back into spatial domain to get stego image. The advantage of transform domain methods is the high ability to face signal processing operations. However, methods of this type are computationally complex. Steganography methods using DCT (Discrete Cosine Transforms), DWT (Discrete Wavelet Transforms), IWT, DFT (Discrete Fourier Transforms) come under this category.

Steganography, one of the ways used for secure transmission of confidential information, contains two main branches: digital watermarking and steganography. The former is mainly used for copyright protection of electronic products while, the latter is a way of covert communication. Avoiding communication through well-known channels greatly reduces the risk of information being leaked in transit.

II. IMAGE STEGANOGRAPHY

Image steganography is about exploiting the limited powers of the human visual system (HVS). Within reason, any plain text, cipher text, other images, or anything that can be embedded in a bit stream can be hidden in an image. The message in encrypted form or in the original form is embedded as the secret message to be sent into a graphic file. This results in the production of what is called a stego-image. In image steganography, unlike watermarks which embed added information in every part of the image, only the complex parts of the image holds added information. There are many reasons to hide data but they all boil down to the desire to prevent unauthorized persons from becoming aware of the existence of a message. The motivation behind developing image Steganography methods according to its use in various organizations to communicate between its members, as well as, it can be used for communication between members of the military or intelligence operatives or agents of companies to hide secret messages.

In the business world Steganography can be used to hide a secret chemical formula or plans for a new invention. Steganography can also be used in the non-commercial sector to keep private digital information protected for number of

purposes such as secret data hiding, copyright protection. Data authentication, ensuring authenticated data availability for academic usage, monitoring of data piracy, labeling electronic data/contents, ownership identification, providing confidentiality and integrity enhancement control of electronic data piracy etc.The main terminologies used in the Steganography systems are: the cover message, secret message, and secret key and embedding algorithm.

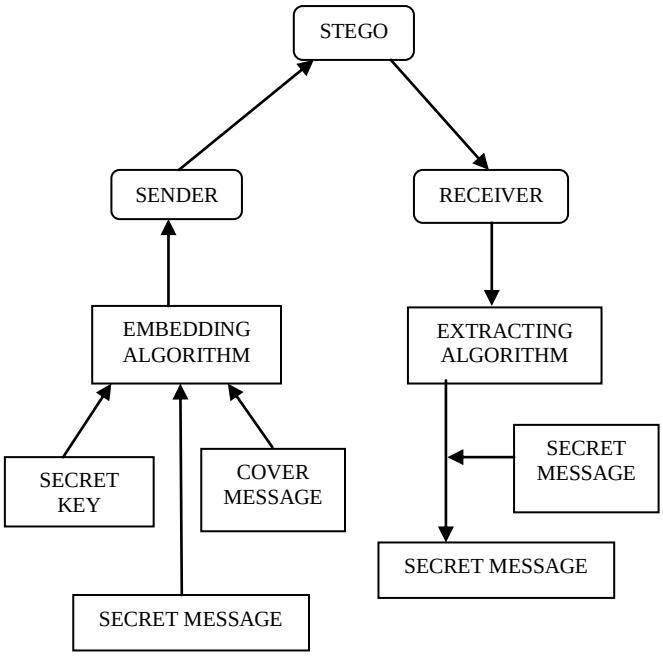

Figure 1. Steganography System Scenario

In the Steganography system scenario, before the hiding process, the sender must select the appropriate message carrier (i.e. image, video, audio, text) and select the effective secret messages as well as the robust password (which supposed to be known by the receiver). The effective and appropriate Steganography algorithm must be selected that able to encode the message in more secure technique. Then the sender may send the Stego file by email or chatting, or by other modern techniques. The Stego file is the carried message with the secret information. After receiving the message by the receiver, he can decode it using the extracting algorithm and the same password used by the Sender.

There are some factors to be considered when designing a steganography system:

Invisibility: Invisibility is the ability to be unnoticed by the human.

Security: Even if an attacker realizes the existence of the information in the stego object it should be impossible for the attacker to detect the information. The closer the stego image to the cover image, the higher the security. It is measured in terms of PSNR.

$$\text{PSNR} = 10 \log_{10} \frac{L^2}{\sqrt{MSE}} dB$$

where L = maximum value, MSE = Mean Square Error.

$$MSE = \frac{1}{N} \sum_{I=1}^{N} |X_i - X_i'|\text{^}2$$

where X = original value, X' = stego value and N = number of samples. High PSNR value indicates high security because it indicates minimum difference between the original and stego values. So no one can suspect the hidden information.

If the message is also encrypted then it provides another layer of protection. Some Steganographic methods combine traditional Cryptography with Steganography; the sender encrypts the secret message prior to the overall communication process, as it is more difficult for an attacker to detect embedded cipher text in a cover. In the fields of information hiding, there is a visual requirements model, which is called magic triangle, given in Fig. 1 (Johnson, Duric, &Jajodia, 2001). The first requirement, called ***capacity*** or also embedding payload, is determined by the number of secret bits embedded in each cover pixel. A higher capacity allows much more the secret data to be inserted into the cover image. The second requirement, named ***imperceptibility***, is usually calculated by peak signal-to-noise ratio (PSNR). When the difference between the cover image and the stego image is small, the PSNR value is high. Thus, the stego image quality is considered to be good with the imperceptibility is high. The last requirement called ***robustness*** which prevents the secret data from being attacked or stolen.

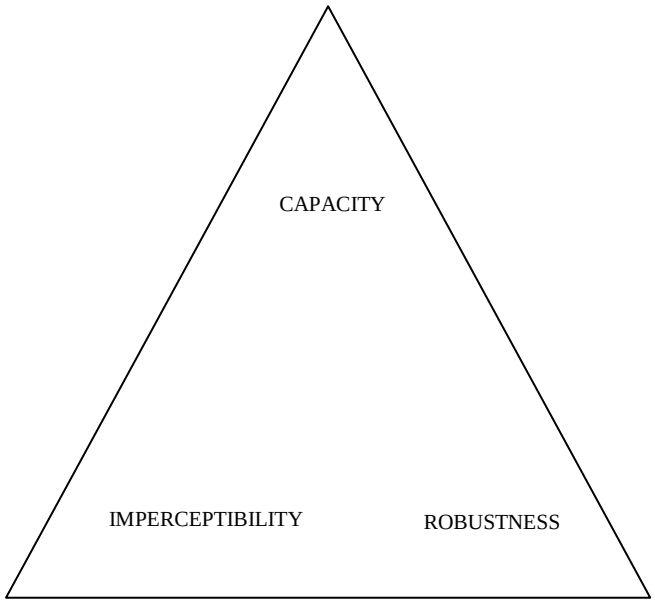

Figure 2. Magic Triangle- Three Requirements Model

Many carrier messages can be used in the recent technologies, such as Image, text video and many others. The image file is the most popular used for this purpose because it easy to send during the communication between the sender and receiver. The images are divided into three types: binary (Black- White), Gray scale and Red-Green-Blue (RGB)

images. The binary image has one bit value per pixel represent by 0 for black and 1 for white pixels. While the gray scale image has 8 bits value per pixel represent from 00000000 for black and 11111111 for white pixels. The RGB image has 24 bits values per pixel represent by (00000000, 00000000 and 00000000) for black and (11111111, 1111111 and 11111111) for white pixels. The RGB image is the most suitable because it contains a lot of information that help in hiding the secret information with a bit change in the image resolution which does not affect the image quality and make the message more secure. In this research paper the RGB images are used as a carrier message to hide the secret messages by the Least Significant Bit hiding method (LSB) as well as the proposed method.

III. EXISTING STEGANOGRAPHY WITH LOW IMPERCEPTIBILITY

Least Significant Bit (LSB) Hiding Technique is the most popular Steganography technique. It hides the secret message in the RGB image based on it its binary coding.LSB hiding technique hide the secret message directly in the least significant bits in the image pixels. Most Significant Bit (MSB) contains 80% of information about the image. Hence the MSB bits of secret image that has to be hidden from the intruders is replaced in the LSB of cover image. This is due to the fact that LSB carries only 20% of information only. Now this image data contains secret image's MSB and Cover image's MSB which is known as *Stego Image*. This stego-image is like a normal digital image. It does not attract the hackers' attention. At the receiver end, various methods are used to recover the MSB of secret image from the stego-image. The following two methodologies are involved in extracting the secret image.

METHODOLOGY 1: On recovery process, only the MSB is recovered. Now ambiguity arises in recovering the LSB of the secret message. In this method, the LSB of the secret image at the receiver side is made as either 0's or 1's.

METHODOLOGY 2: The procedure for this method is same as the Method 1. The only difference is, after extraction the LSB from the Stego image, interchanging of LSB as MSB and MSB as LSB is made, but faced a loss of 45% of information.

In methodology 2, PSNR value achieved is greater than the previous method. But imperceptibility is poor. Figure 4 shows the cover image, original image, stego image and the recovered image.

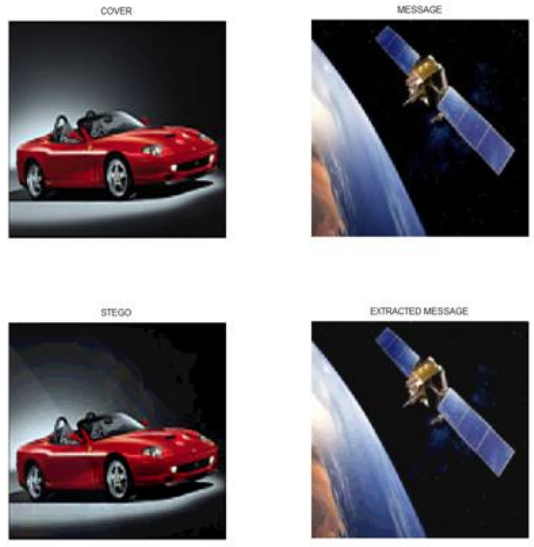

Figure 3. Result of Methodology 1

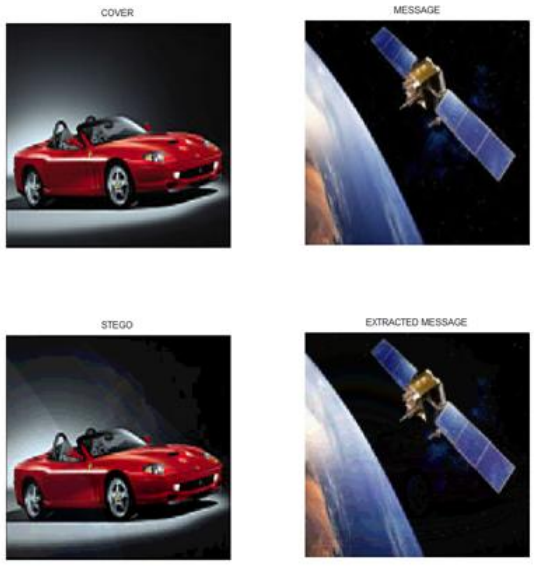

Figure 4. Result of Methodology 2

IV. PROPOSED METHOD WITH HIGH IMPERCEPTIBILITY

Resizing the cover image in such a way that number of pixel rows in cover image should be double the size of message image.

1. To preserve the information in message image we have to follow two steps
   a. Extract MSB from Message image and let it be **X**.
   b. Extract LSB from Message image and let it be **Y**.
2. To form a stego image replace X for Cover image first half's LSB and replace Y for Cover image second half's LSB. By doing this we can preserver both MSB and LSB of the message image.

Finally it is found that this Proposed Methodology is much more suitable for chaotic encryption based stego process. A good PSNR after the Extraction and Decryption process is also obtained.

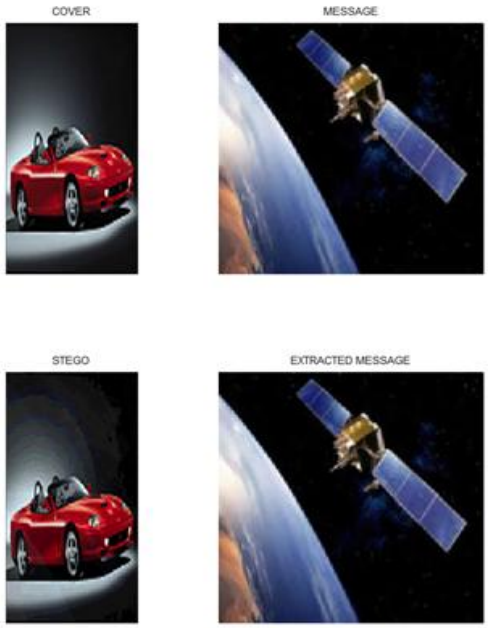

Figure 5. Result of Proposed Methodology

It is evident from the following Figure 5, that the resulting Stego Image from Proposed Methodology is similar to that of Cover Image. The Stego Image attempts to prevent an unintended recipient from suspecting that the data is there.

Table 1: Comparison of Methodologies

Parameter	Method 1*		Method 2*	Proposed Method*
	0000	1111		
PSNR	26.7062	26.7062	32.2911	∞
TIME (sec)	11.5892	11.5892	11.5395	44.7855
*Values slightly varies for different images				

V. CONCLUSION

Thus the proposed Steganographic method provides ***high imperceptibility***. It is found from the simulation result that the peak signal-to-noise ratio is infinite and hence the loss in the proposed technique is null and the image quality is very high. When combined with encryption process, the proposed Steganographic technique provides ***high robustness***. In each cover pixel, four bits of secret message is embedded. Thus the proposed technique has increased ***capacity*** (embedding payload). The three requirements of Magic triangle are achieved. The trade-off of this method is time.

REFERENCE

[1]. Gaurav Prasad and Sujay Narayana, "Two New Approaches For Secured Image Steganography Using Cryptographic Techniques and Type Conversions", An International Journal, December 2010.
[2]. Abhijeet A. Ravankar and Stanislav G. Sedukhin, "Image Scrambling Based on a New Linear Transform", 2011 IEEE.
[3]. Cao Yun and Qiu Run-he, "Integrated Confusion-Diffusion Mechanisms for Chaos Based Image Encryption", 2011 4th International Congress on Image and Signal Processing.
[4]. Chen Wei-bin and Zhang Xin, "Image Encryption Algorithm Based on Henon Chaotic System", 2009 IEEE.
[5]. Fan Jing, Liu Min and Zhu Xian, "Image Scrambling Encryption By Mix Fan Transform Matrixes Technology", 2012 9th International Conference on Fuzzy Systems and Knowledge Discovery (FSKD 2012).
[6]. Keun-Moo Rhee, "Image Encryption Using Self Regressive Function", Fourth International Conference on Networked Computing and Advanced Information Management.
[7]. Liu Wei and Zhang Yun-peng, "Digital Image Encryption Algorithm Based on Chaos and Improved DES", Proceedings of the 2009 IEEE International Conference on Systems, Man, and Cybernetics.
[8]. Qiang Zhang and Shihua Zhou, Xiaopeng Wei, "Image Encryption Algorithm Based on DNA Sequences for the Big Image", 2010 International Conference on Multimedia Information Networking and Security.
[9]. Liu Min, Zhu Xian, Fan Jing, "Image Scrambling Encryption By Mix Fan Transform Matrixes Technology", 2012 9th International Conference on Fuzzy Systems and Knowledge Discovery.
[10]. Shanshan Li and Yinghai Zhao, "Image Scrambling Based on Chaos Theory and Vigen`ere Cipher", 2011 Seventh International Conference on Computational Intelligence and Security.

Authors Profile

Mohanasundaram S S received the B.E. degree in Electronics and Communication Engineering from K. S. R. College of Engineering Anna University, Chennai, India, in 2010. He received M.E. degree in Applied Electronics from Bannari Amman Institute of Technology, Anna University of technology, Coimbatore, India, in 2012. His research interest includes Embedded Systems, Very Large Scale Integration Design, Network Security.

Mani Bharathi V received B.E in Electronics and Communication Engineering from P. A. College of Engineering and Technology, Anna University, Chennai, India, in 2013. Currently pursuing M. E. degree in VLSI Design from P. A. College of Engineering and Technology, Anna University, Chennai, India. Her area of interests includes Network Security and Cryptography, Image Processing, Digital Signal Processing, Digital Communication.