IJISET - International Journal of Innovative Science, Engineering & Technology, Vol. 2 Issue 4, April 2015.
www.ijiset.com
ISSN 2348 – 7968

Information hiding with LSB based Image Steganography

Shikha Mohan[#1] and Satnam Singh[*2]

[1#] M.Tech Scholar, ECE Department, SSCET,Badhani,Punjab, India
[*2]AP, ECE Department, SSCET, Badhani, Punjab, India

***Abstract* — Steganography is the technique used to hide information inside some multimedia carriers like video, audio or images. Steganography means covered or hidden writing. Information or data is the wealth of any organization therefore security issues are top priority to an organization dealing with confidential data. Steganography is the science that involves communicating secret data by hiding the data into some object/carrier. This paper intends to give an overview of image steganography along with the description of various techniques used in steganography. We modify the LSB based image steganography and evaluate the performance of the modified algorithm.**

Keywords – **LSB, PSNR, steganography, steganalysis.**

I. INTRODUCTION

Steganography means covered or hidden and is derived from Greek words 'steganos' meaning covered or secret and 'graphy' meaning writing or drawing. Image Steganography is the technique for hiding information by embedding messages within image. It is widely used in military, diplomatic, personal and intellectual property applications. Steganography is the term applied to any number of processes that will hide a message within an object particularly an image, where the hidden message will not be apparent to an observer. Typically, the message is embedded within another object (image) known as a cover object, by tweaking its properties. The resulting output, known as a stego object or stegogramme is engineered such that it is a near identical perceptual model of the cover object, but it will also contain the hidden message [1, 2].Steganography differs from cryptography because the latter does not attempt to hide the fact that a message exists. Instead, cryptography merely obscures the integrity of the information so that it does not make sense to anyone but the creator and the recipient. The adversary will be able to see that a message exists, and the inverse process of cryptanalysis involves trying to turn the meaningless information into its original form.

Steganography in the modern day sense of the word usually refers to information or a file that has been concealed inside a digital Picture, Video or Audio file. What Steganography essentially does is exploit human perception; human senses are not trained to look for files that have information hidden inside of them. Steganography is employed in various useful applications, e.g., for human rights organizations, as encryption is prohibited in some countries copyright control of materials, enhancing robustness of image search engines and smart identity cards, where details of every person are embedded in their photographs [3]. Other applications are video-audio synchronization, companies' safe circulation of secret data, TV broadcasting, TCP/IP packets, for instance a unique ID can be embedded into an image to analyze the network traffic of particular users, and also checksum embedding [4]. Almost all digital file formats can be used for steganography, but the formats that are more suitable are those with a high degree of redundancy. Redundancy can be defined as the bits of an object that provide accuracy far greater than necessary for the object's use and display. The redundant bits of an object are those bits that can be altered without the alteration being detected easily. Image and audio files especially comply with this requirement, while research has also uncovered other file formats that can be used for information hiding. Since, images are quite popular cover or carrier objects used for steganography. In the domain of digital images many different image file formats exist, most of them for specific applications. For these different image file formats, different steganographic algorithms exist. To hide information in audio files similar techniques are used as for image files. One different technique unique to audio steganography is masking, which exploits the properties of the human ear to hide information unnoticeably. A faint, but audible, sound becomes inaudible in presence of another louder audible sound. This property creates a channel in which to hide information. Although nearly equal to images in steganography potential, the larger size of meaningful audio files makes them less popular to use than images.

II. SPATIAL DOMAIN IMAGE STEGANOGRAPHY

Image steganography techniques can be classified into two broad categories: Spatial-domain based steganography and Transform-domain based steganography.

In spatial domain scheme, the secret messages are embedded directly. Here, the most common and simplest steganography method is the least significant bits (LSB) insertion method. In the LSB technique, the least significant bits of the pixels are replaced by the message bits which are permuted before embedding. Most steganography software hide information by replacing only the least-significant bits (LSB) of an image with bits from the file that is to be hidden.

This technique is generally called LSB encoding. One of the most common techniques used in steganography. The following example shows how the letter A can be hidden in the first eight bytes of three pixels in a 24-bit image.

Pixels: (10101111 11101001 10101000)
(10100111 01011000 11101001)
(11011000 10000111 01011001)

Secret message: 01000001

Result: (10101110 11101001 10101000)
(10100110 01011000 11101000)
(11011000 10000111 01011001)

The three bold bits are the only three bits that were actually altered. Since the 8-bit letter A only requires eight bytes to hide it in, the ninth byte of the three pixels can be used to begin hiding the next character of the hidden message. A slight variation of this technique allows for embedding the message in two or more of the least significant bits per byte. This increases the hidden information capacity of the cover-object, but the cover-object is degraded more, and therefore it is more detectable.

Spatial LSB embedding is widely used for its high hiding quality and simplicity to realize. However, the robustness of this method is weak and the message length can be estimated by statistical scheme [5]. In order to solve this problem, some researcher's proposed various methods which are advanced version of LSB techniques.

A reversible histogram transformation function-based LSB steganographic method is proposed by Der-Chyuan Lou and Chen-Hao Huto resists statistical steganalysis [6]. The experimental results show that the proposed method resists not only Regular-Singular (RS) attack but also Chi-Square (χ 2) detection methods. Chia-Chun Wu et al. proposed a novel secret image sharing scheme by applying optimal pixel adjustment process to enhance the image quality under different payload capacity and various authentication bits conditions [7]. The experimental result of proposed scheme shows the improvement of image quality of stego images. He also provides several experiments to demonstrate the efficacy of authentication capability of the proposed scheme and therefore maintains the secret image sharing and authentication ability while enhances the image quality.
Xin Liao et. al. improve the embedding capacity and provide an imperceptible visual quality, by give a novel steganographic method based on four-pixel differencing and modified Least Significant Bit (LSB) substitution [8]. The experimental result of proposed method gives not only an acceptable image quality but also provides a large embedding capacity.

As vast channels for communication such as the Internet are becoming popular, the security of digital media becomes a greater concern. The hiding of a message will reduce the probability of detecting this message. This method hides a gray image in one another. The cover is divided into blocks of equal sizes. Each block size equals the size of the embedding image. Edge Based Steganography is in which only the sharper edge regions are used for hiding the message while keeping the other smoother regions as they are. It is more difficult to observe changes at the sharper edges than those in smoother regions. In this method Enhanced Least Significant Bit algorithm is used which can reduce the rate of pixel modification thereby increasing the security both visually and statistically.

Grey Level Modification Steganography Method steganography method is based on image layers. This method divides the host image into blocks and embeds the corresponding secret message bits into each block using the layers which are made by the binary representation of pixel values. It then performs a search on the rows and columns of the layers for finding the most similar row or column. The location of row/column and its differences from the secret message is then marked by modifying minimum number of bits in the least significant bits of the blocks.

III. Modified LSB Image Steganography

We proposed a new LSB based image steganography algorithm. The performance of the proposed algorithm is evaluated for different images and compare with the conventional LSB method. We modify the LSB based image steganography by applying forward error correction coding with LSB techniques. The modified LSB technique increases the robustness to noise attack. The steps of modified LSB method are given below.

- Read the cover image and secret text message.
- Apply forward error correction coding to secret message to make codeword message.
- Convert text message in 8 bit binary format.
- Calculate LSB of each pixels of cover image.
- Replace LSB of cover image with each bit of secret message one by one.
- Write stego image

IV. Results

The LSB based proposed image steganography algorithm is evaluated with different images of varying size. The randomly selected messages are embedded into the images and performance is evaluated. Basically the proposed LSB

ISSN 2348 – 7968

based method provides more robustness against noise attack than simple LSB techniques.

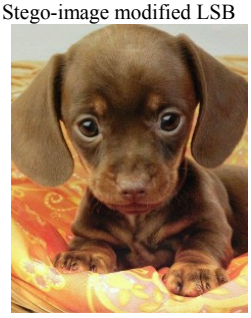
The results of modified LSB based image steganography is shown in figure 1 and figure 2. The results of robustness of the proposed system are depicted in table 1.

Original image

Stego-image LSB

Noisy stego-image LSB

Stego-image modified LSB



Noisy stego-image Modified LSB

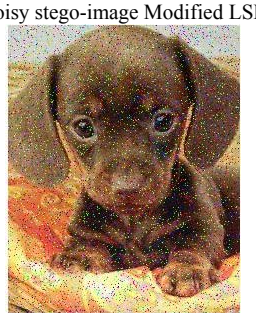


Figure 1: Results of proposed method with dog image.

Original image

Stego-image LSB

Noisy stego-image LSB

Stego-image modified LSB

Noisy stego-image Modified LSB

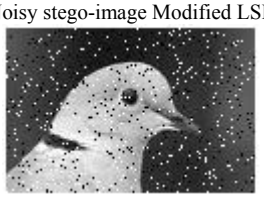


Figure 2: Results of proposed method with dove image.

Noise Intensity	Message Bits	Simple LSB		Proposed LSB with RS Code	
		Bits in Error	Error Rate	Bits in Error	Error Rate
0	128	0	0	0	0
0.05	128	4	0.0312	0	0
0.1	128	8	0.0625	2	0.0156
0.15	128	10	0.0625	3	0.0313
0.2	128	13	0.0782	5	0.0391
0.25	128	17	0.1329	8	0.0625
0.3	128	21	0.164	11	0.086
0.35	128	23	0.18	13	0.102
0.4	128	28	0.2187	15	0.118
0.45	128	34	0.267	18	0.141
0.5	128	38	0.3	20	0.16

IV. Conclusions

In this paper we proposed a modified LSB method which uses forward error correction coding. We implement and test the proposed method. The performance of the modified LSB method is verified and compared with the simple method. The proposed method provides better robustness against noise attack.

References

[1] Abbas Cheddad, Joan Condell, Kevin Curran, Paul McKevitt, "Digital image steganography: Survey and analysis of current methods", Journal of Signal Processing, Elsevier, Vol. 90, 2010, pp: 727–752.

[2] Yambern Jina Chanu, ThemrichonTuithung, Kh. Manglem Singh, "A Short Survey on Image Steganography and Steganalysis Techniques", IEEE 3rd conference on Emerging Trends and Applications in Computer Science (NCETACS), Shillong, 30-31 March 2012, pp: 52 – 55.

[3] Alain Brainos, "A Study of Steganography and The Art of Hiding Information"July,2004, http://www.infosecwriters.com/text_resources/pdf/steganographyDTEC6823.pdf

[4] Paunwala, M.C. Patnaik, S., "Sheltered Identification with Hiding Biometrics", International Conference on Signal and Image Processing (ICSIP), IEEE, Surat, 15-17 Dec., 2010, pp: 191-196.

ISSN 2348 – 7968

[5] R. Shreelekshmi, M. Wilscy, C.E. Veni Madhavan, "Cover Image Preprocessing for More Reliable LSB Replacement Steganography", Proc. of International Conference on Signal Acquisition and Processing, IEEE, Trivandrum, 9-10 Feb., 2010; pp: 153-156.
[6] Der-Chyuan Lou and Chen-Hao Hu, "LSB steganographic method based on reversible histogram transformation function for resisting statistical steganalysis", Journal of Information Sciences, Elsevier, Vol. 188, 2012, pp: 346–358.
[7] Chia-Chun Wu, Shang-Juh Kao and Min-Shiang Hwang, "A high quality image sharing with steganography and adaptive authentication scheme", Journal of Systems and Software, Elsevier, Vol. 84, 2011, pp: 2196– 2207.
[8] Xin Liao, Qiao-yan Wen and Jie Zhang, "A Steganographic method for Digital Images with Four-pixel Differencing and Modified LSB Substitution", Journal of Visual Communication and Image Representation, Elsevier, Vol. 22, 2011, pp: 1–8.