I J C T A, 9(24), 2016, pp. 119-124 ISSN: 0974-5572

An Efficient Steganography Algorithm Based on Visual Cryptography and Least Significant Bit Embedding

A. Velmurugan* and E. Logashanmugam**

ABSTRACT

Steganography is the process of concealing data within another data. The data may be in any form such as file, image, audio or video. The data to be concealed into another data is called secret data. The original data is called as cover data that hides the secret data. In this paper, an efficient steganography technique is presented which combine the visual cryptography with Least Significant Bit (LSB) embedding approach. The secret data is divided into two data called as shares by random grid techniques. The LSB process inserts one of the shares into the cover image. The remaining share is used by the receiver to recover the secret data. MATLAB is used to implement the proposed system, and the results show the effectiveness of the proposed system.

Keywords: Steganography, visual cryptography, least significant bit, data hiding.

1. INTRODUCTION

Security is critical in many application areas such as communication and information technology. Different types of methods used to hide the secret data within the original data. The secret information is hidden in random pixels in [1]. The selection of random pixels is based on location, shape, and colour of the pixels in the cover image. After selecting the random pixels, LSB approach is used to hide the secret information. An approach to hide more information with acceptable embedded rate is discussed in [2]. The information hiding problem is solved by applying modern algebra.

Pixel Value Differencing (PVD) method is discussed in [3] for secret data embedding in each of the component of a pixel in a colour image. The pixel values in the embedded image may exceed the range 0~255. This issue can be eliminated by using a different number of bits in various pixel components. Four-pixel differencing and modified LSB substitution based steganographic method is described in [4]. The edge features are considered as they can tolerate more changes without making any distortion than smooth regions.

An audio steganography approach is discussed in [5]. Audio signals have an inherent redundancy and unpredictable nature which make them ideal for secret data embedding. At first, an audio signal is converted into bits, and then the secret data is embedded by using LSB. In [6], a letter-based visual cryptography scheme is described to create meaningful shares for sharing many secrets utilized for both binary and gray scale images. Text files with natural language letters are generated instead of shares in visual cryptography. A detailed literature on steganography and visual cryptography are given in [7].

Genetic algorithm and visual cryptography based algorithm is designed in [8] to transmit over networks. At first, LSB approach is used for hiding secret into cover. The security of the secret data is increased by modifying the location of pixels based on genetic algorithm. This data is split by visual cryptography into two shares. In order to retrieve the secret data, the receiver has to apply the reverse process using the secret

* Research Scholar, *Email: an.velmurugan@rediffmail.com*

** Professor Department of Electronics and Communication Engineering Sathyabama University Chennai, India.

key. A simple LSB substitution algorithm using an optimal pixel adjustment process is discussed in [9]. The size of the secret data is rearranged as same as the cover data. Then, a subset of pixels is selected, and k LSB of the cover image is replaced.

A modified LSB image steganography technique is described in [10]. Braille method is used for representing secret data by six bits only. Among the six bits, three bits are hidden in the red layer; two bits are on the green layer and one bit in the blue. An approach for securing image by steganographic and cryptographic techniques is implemented in [11]. The key used for the encryption is obtained from the pixels. For colour pixels, there are 24 bits are available. The encryption of red, green and blue pixels are used the first, middle, and last 10 bits respectively. Then, LSB approach is used to hide the encrypted image into a cover image.

An addition security is offered in the form of symmetric key based encryption is described in [12]. At first, the secret data is encrypted by the symmetric key and then secret sharing algorithm is applied to the encrypted image to generate meaningful shares. An approach for multiple secret sharing schemes is discussed in [13]. From the two secret data, only two shares are created by XOR operations and then, they are encrypted. While decoding, the secret data can not be validated if decryption is not possible.

In this paper, an efficient approach is presented for hiding data using visual cryptography and LSB embedding process. The paper is arranged in the following order. In section 2, the methods and materials used by the proposed approach are discussed. The results obtained by the proposed system are discussed in section 3, and finally, the conclusion is given in section 4.

2. METHODS AND MATERIALS

A very simple steganography approach is the LSB. In LSB, the secret data is embedded directly into the cover image in a pixel by pixel manner. In the embedding process, the LSB of each pixel is replaced by the permuted bits of the secret data. Hence, the complexity of the LSB manipulation is very less. However, the security of such method is very low as the recovery approach is very simple. The proposed system uses visual cryptography to strengthen the LSB based approach. In LSB, the secret data is hidden directly. In the proposed approach visual cryptography is used to protect the secret data. To create shares from the secret data random grid technique is applied. At first, a binary share is created by randomly which consists of 1's and 0's. The size of the created share is same as original data. Then, a second share is created using secret data and randomly created share. Table 1 shows the process of share creation.

After creating the 2nd share, it must be supplied with the receiver to extract the secret data. The LSB process uses the randomly created share and the cover image to create the embedded image. Table 2 shows

Table 1
Share creation using secret data and randomly created share

Secret data	*Randomly created share*	*Another share*
0	0	0
0	1	1
1	0	1
1	1	0

Table 2
LSB Process to hide the data

Share 1	*Cover Image*	*Hided data*
0	0	0
0	1	0
1	0	1
1	1	1

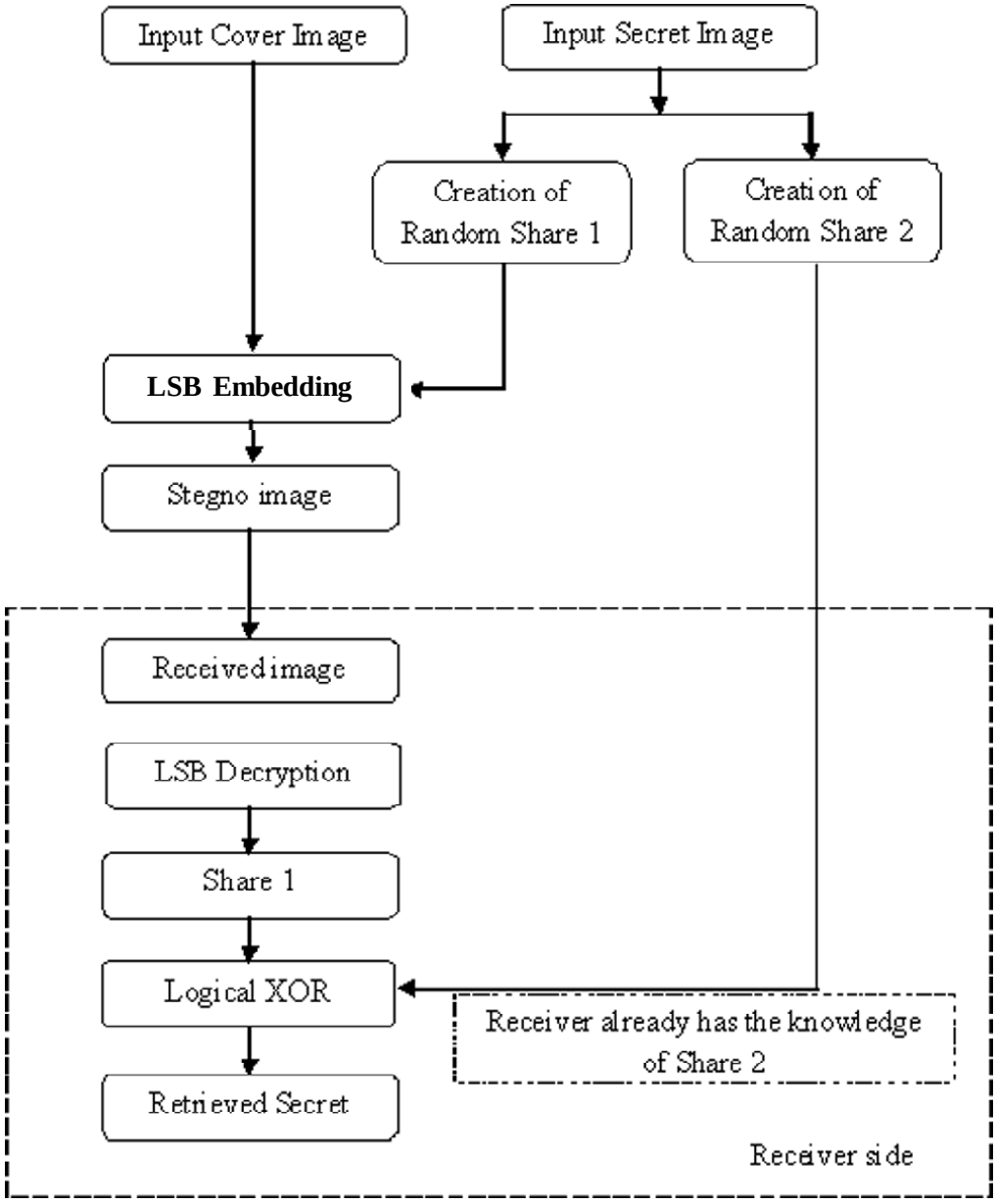

Figure 1: Block Diagram of Proposed Architecture

the LSB method to hide the secret data. Figure 1 shows the proposed steganography system using LSB and visual cryptography.

It is clearly observed from table 1 that the secret data is recovered by simply stake the two shares. If the receiver has the knowledge of the 2nd share, then the recovery of secret data is possible. The algorithm for embedding and retrieving secret information is as follows:

Algorithm 1: Hiding Secret data into cover image

Step 1: Read the Input cover image

Step 2: Read the secret binary image.

Step 4: Generate Share 1 randomly.

Step 5: Generate Share 2 by using Share 1 and secret binary image (Table 1).

Step 6: Replace the LSB of cover image with the LSB of Share1 in a pixel by pixel manner. (Table 2)

Algorithm 2: Retrieve the secret data

Step 1: Read the received image.

Step 2: Retrieve the Share 1 from the LSB of the received image.

Step 3: Stake (logical XOR operation) the retrieved Share 1 and Share 2

3. RESULTS AND DISCUSSIONS

The performance of the proposed steganography algorithm is discussed in this section. The proposed system is successfully implemented in MATLAB. In order to analyze the performance of the system in terms of Peak Signal to Noise Ratio (PSNR) and Self-Similarity Matrix (SSIM), the same secret data is hidden into different types of cover images. The definition of PSNR and SSIM are given below:

The PSNR is a quality measure used to observe the quality of the data after its modification. In this case, the cover image is considered as input data and the embedded image is the noisy version of the input data. The mean squared error is the cumulative squared error between the compressed and the original image. It is defined as:

$$RMSE = \sqrt{\frac{1}{MN}\sum_{x=0}^{M-1}\sum_{y=0}^{N-1}\left[\hat{f}(x,y) - f(x,y)\right]^2} = \sigma_e \tag{1}$$

The PSNR is defined as

$$PSNR = 10.\log_{10}\frac{(peak-to-peak\ value\quad of\ the\ referenced\ image)^2}{\sigma_e^2} \tag{2}$$

For gray scale images, the peak to peak value is 255. The PSNR is calculated from the error using the above formula. SSIM is considered to assess the similarity between the embedded data and the cover data. Generally, SSIM is a full reference metric, which measures the image quality based on the original image as reference image [14].

$$SSIM = \frac{(2\mu_x\mu_y + c_1)(2\sigma_{xy} + c_2)}{(\mu_x^2 + \mu_y^2 + c_1)(\sigma_x^2 + \sigma_y^2 + c_2)} \tag{3}$$

where μ_x and μ_y is the average of *x* and *y*. σ_x^2 and σ_y^2 is the variance of *x* and *y*. σ_{xy} is the covariance of the same. $c_1 = (k_1L)^2$ and $c_2 = (k_2L)^2$ are used to stabilize the division with the weak denominator, where L is the

Figure 2: Cover images used in the proposed steganography algorithm

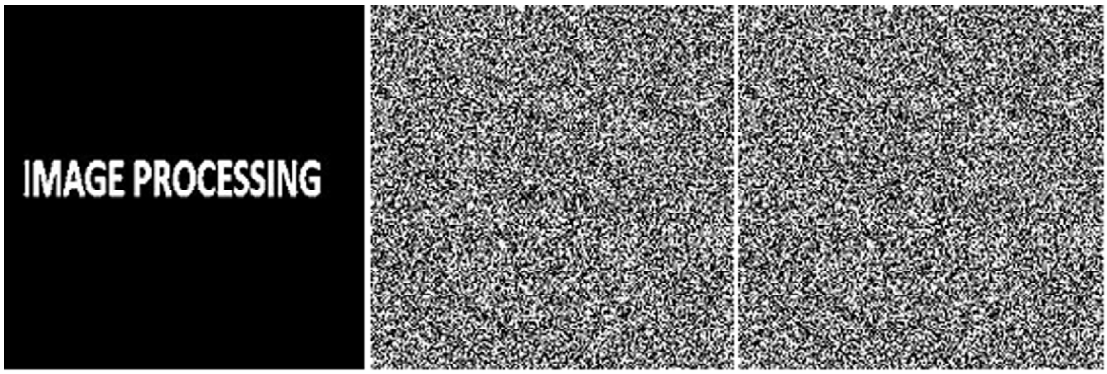

Figure 3: Secret image and its shares

dynamic range of the pixel values. k_1 and k_2 are 0.01 and 0.03. Figure 2 shows the cover images used in the proposed steganography algorithm for performance evaluation. Figure 3 shows the secret image and its shares created by the random grid

The proposed system uses the share 1 created by the random grid technique and the share 2 is given to the receiver to validate the secret image. The performance measures computed by using the cover image and the embedded image are shown in table 3.

Table 3
PSNR and SSIM values obtained by the proposed system

Image	*PSNR (in dB)*	*SSIM*
Masuda	54.48	0.9956
Airplane	54.17	0.9985
Barbara	54.18	0.9972
Boats	54.20	0.9991
Goldhill	54.29	0.9977
House	54.21	0.9986
Lenna	54.13	0.9964
Peppers	54.23	0.9982
Sailboat	54.21	0.9975
Zelda24	54.24	0.9985

From the table 3, it is observed that the proposed steganography algorithm yields higher PSNR and SSIM. This means that the embedded image is more similar to the cover image. Hence, it is impossible to identify whether any secret is embedded into the cover image or not.

4. CONCLUSION

In this paper, an efficient steganography technique which combines visual cryptography and LSB is presented. The main advantage of the proposed system is that the knowledge of share is required to recover the secret data. Hence, the security of the proposed system is higher than other techniques in the literature. This technique provides an imperceptible image for human vision. The performance of the presented steganographic algorithm is studied, and experimental results also were shown. The proposed system can be extended to colour images also.

REFERENCES

[1] Samidha, Diwedi, and Dipesh Agrawal, “Random image steganography in spatial domain” Emerging trends in VLSI, embedded system, nano electronics and telecommunication system (ICEVENT), 2013 international conference on. IEEE, pp. 1-3, January 2013.

[2] Nguyen, Luong Viet, Trinh Nhat Tien, and Ho VanCanh. “The method of hiding steganography without key exchanging and original image.” Computer Science and Automation Engineering (CSAE), 2012 IEEE International Conference on Vol. 2, pp.408-412, IEEE, May 2012.

[3] J. K. Mandal and Debashis Das (July,2012),”Colour Image Steganography Based on Pixel Value Differencing in Spatial Domain. International Journal of Computer Science and Electronics Engineering (IJCSEE) Volume 1, Issue 2 (2013) ISSN 2320–401X (Print) International Journal of Information Sciences and Techniques (IJIST) Vol.2, No.4.

[4] X. Liao, Q.-Y. Wen, and J. Zhang (2011), “A Steganographic Methodfor Digital Images with Four-Pixel Differencing and Modified LSB substitution,” Journal of Visual Communication and Image Representation, vol. 22, no. 1, pp. 1"8.

[5] Binny, A., & Koilakuntla, M. (2014, September). Hiding Secret Information Using LSB Based Audio Steganography. In Soft Computing and Machine Intelligence (ISCMI), 2014 International Conference on (pp. 56-59). IEEE.

[6] Raphel, R. K., Ilyas, H. M., & Panicker, J. R. (2015). Multiple Secret Sharing Using Natural Language Letter Based Visual Cryptography Scheme. In Algorithms and Architectures for Parallel Processing (pp. 476-486). Springer International Publishing.

[7] George Abboud, Jeffrey Marean, Roman V. Yampolskiy,”Steganography and Visual Cryptography in Computer Forensics,” Fifth International Workshop on Systematic Approaches to Digital Forensic Engineering, IEEE Computer Society, 2010.

[8] Rehana Begum R.D,Sharayu Pradeep , “Best Approach for LSB based Steganography Using Genetic Algorithm and Visual Cryptography Secured Data Hiding and Transmission over Networks,” International Journal of Advanced Research in Computer Science and Software Engineering, vol. 4 Issue 6, June 2014.

[9] C.K Chan and L. Cheng, “Hiding data in images by simple LSB substitution” vol.37,no.3,pp 469-474,2004 Signal Process., vol. 53, no. 10, pt. 2, pp. 3923–3935, Oct. 2005.

[10] Emam, M. M., Aly, A. A., & Omara, F. A. (2015). A Modified Image Steganography Method based on LSB Technique. International Journal of Computer Applications, 125(5).

[11] Prasad, G., & Narayana, S. (2011). A Novel Approach for Concealed Data Sharing and Data Embedding for Secured Communication. International Journal of Computer Science, Engineering and Applications, 1(1).

[12] Bidgar, P., & Shahare, N. Key based Visual Cryptography Scheme using ovel Secret Sharing Technique with Steganography. IOSR Journal of Electronics and Communication Engineering (IOSR-JECE), e-ISSN, 2278-2834.

[13] Khairnar, S., & Kharat, R. (2016). A Secure and Verifiable Multi Secret Sharing Scheme for Encrypting Two Secret Images into Two Shares. International Journal of Computer Applications, 134(11), 27-29.

[14] Longkumer, N., Kumar, M., Jaiswal, A. K and Saxena, R. “Contrast Enhancement Using Various Statistical Operations And Neighborhood Processing”. International Journal on Signal & Image Processing, Vol. 5, No.2, pp. 51-61, 2014.