International Journal of Computer Applications (0975 8887)
Volume 92 - No. 4, April 2014

A Secret shearing Algorithm based on LSB Substitution

Bhaskar Mondal
Department of Mathematics
National Institute of technology Jamshedpur
Jharkhand, India-831014

Tarni Mandal (PhD)
Department of Mathematics
National Institute of technology Jamshedpur
Jharkhand, India-831014

ABSTRACT

This paper proposed a highly secure secret sharing scheme for multimedia image communication. The proposed scheme may used for generation of n number shares of a secret image. Both the construction and revealing of shares are based on LSB subtraction. In previously proposed schemes were surfers from several problems. Like in case of images having completely single color other than the color black, the shares were having strip patterns rather than being random or pixel expansion. The proposed scheme is applicable for any size of image, has no pixel expansion and can reconstruct the secret image precisely. The proposed scheme includes no matrix multiplication for construction of shares with computational complexity equal to LSB method. The scheme can be directly applied for any of the binary, grayscale or color image. Experimental results show that the scheme is simple and effective.

General Terms:

Security, Chaos, secret sharing

Keywords:

security; secret sharing; steganography; LSB

1. INTRODUCTION

With the rapid development of computer technique and communication network, more and more people and organizations rely on the internet to transmit important information. However in recent years hackers have intruded many computer network systems to steal or corrupt the important information, which has caused a great loss to organizations and personal profits. Hence information security has become a very important issue in modern society. Many techniques have been developed to protect the security of information including visual cryptography [10], secret sharing, steganography [9], and other encryption techniques.
Secret sharing (SS), was first proposed by Blakley [1] and Shamir [14] independently, which encode a secret image into n shares. The secret image can only be reconstructed from any k or more shares. Knowledge of $k-1$ or fewer shares provides absolutely no information about the secret. SS can not only guarantee the security of information, but also greatly reduce the possibility of secret inaccessible due to misfortune or betrayal, thus it has attracted many scholars attention. A secret sharing scheme can be evaluated by its security, contrast (reconstruction precision), computational complexity, and pixel expansion (storage requirement).

The previous scheme proposed by Dong and Ku [3] makes the use of matrix multiplication property for construction of shares and addition of shares to reconstruct the secret image.Zhang et. al. [16] proposed an image encryption and sharing algorithm based on chaos and indeterminate equation. The authors have improved the share construction technique by reducing the computational complexity by applying matrix addition instead of matrix multiplication. However image reconstruction still uses the matrix addition property. Latter B. Mondal et. al. [12] proposed a novel scheme of secret image sharing based on matrix addition. The scheme has no pixel expansion and retains the contrast of the original secret image. Considering an image of size hh pixels, the computational complexity of matrix multiplication is $O(h3)$, whereas that of matrix addition is $O(h2)$. The complexity of share generation improves in the scheme as compared to Dong and Ku [3]. Hence the proposed scheme adds to the merits of already known secret sharing schemes and optimizes it.
[8] proposed a chaotic steganography scheme.
In the proposed scheme the secret image is scrambled [6] using a chaotic logistic map and decomposed into bit-maps. The bit maps are embedded onto the Cover images using LSB substitution.

2. SECRET SHARING

Secret Sharing refers to a method for distributing a secret amongst a group of participants. Each of whom is allocated a share of the secret. The secret can be reconstructed only when a sufficient number of shares are combined together: Individual shares are of no use on their own. The definition [14] of secret sharing scheme is as follows:

A (k, n) secret sharing scheme divides a secret S into n shares S_i (where $i \leq n$) such that the following terms and conditions are satisfied:

The secret A is recoverable from any k shares, i.e., for any set of k indices, $H(S|S_i : i = 1, 2, 3k)$

Knowledge of $k-1$ or fewer shares provides absolutely no information about S.

The first condition is called precision and the second condition is called security. When $k = n$, it is the definition of (n, n) secret

sharing scheme. [7]

3. CHAOTIC LOGISTIC MAP

A chaotic system is a dynamic, deterministic system, which changes its state specifically with time. A chaotic logistic map [5, 13] is used here for scrambling the secret image pixels.

$$x_{k+1} = f(x) = \mu x_k(1 - x_k)$$
$$\mu \in (0, 4), x_k \in (0, 1) \quad (1)$$

The Logistic map defined by equation 1 is used to generate a chaotic sequence. The first 2000 values of the sequence are ignored as a part of the transient phase. The initial conditions are chosen such that a belongs to the range $(3.65, 3.95)$ and x_0 belongs to the range $(0, 1)$. The values are chosen with a precision of 10 digits. All the values are transformed into integers by multiplying it by an arbitrary value and then taking its floor.

4. LSB SUBSTITUTION TECHNIQUE

A most widely used steganography method is the least significant bit (LSB) substitution technique [2]. From figure 1, it is observed that first 3 LSB bit planes are appeared as randomly where rest of the bit planes carries most of visual information. So modifying out of first 3 LSB bits of the cover image will degrade excessively the quality of the stego-image.

The secret message extraction process from the stego-image is a

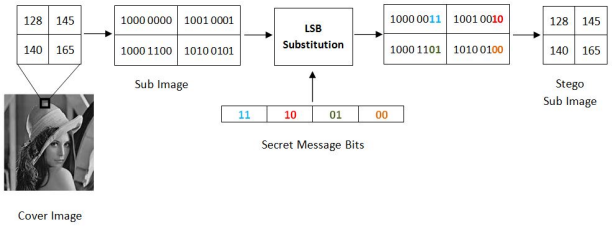


Fig. 1. A typical diagram of LSB Substitution techniques

straight forward process where the secret message bits are extracted from the concealed LSB bits of each pixel in the stego-image sequentially. Both the embedding and the extracting processes of the LSB substitution scheme do not require complex computations. Thus, this scheme is very simple and has less computational overhead [11].

In digital image most of the significant information is carried out by the most significant bits (MSB) so changing the parts of MSB of the cover image will seriously degrade the quality of the stego-image. Thus, the LSB substitution scheme decides to embed sensitive data into the parts of LSB of the cover image. Figure 2 depicts the processes of the LSB substitution scheme where 8 bits secret message are embedded into the sub-image of size 2×2 by replacing first 2 LSB bits of each pixel. After embedding all secret message bits into the cover image, the cover image containing the secret message is termed as the stego-image.

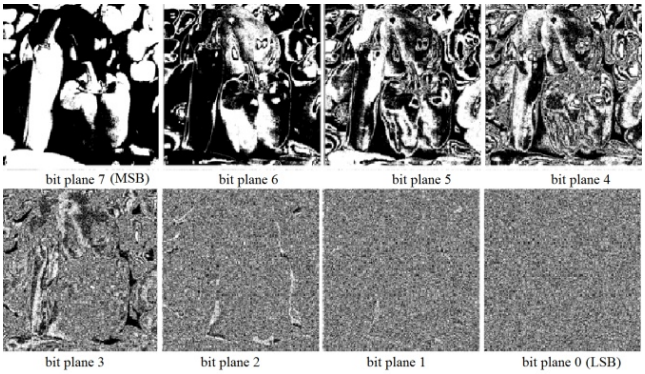


Fig. 2. Bit plane Decomposition of Pepper Image.

5. THE SCHEME

In this proposed scheme firstly the secret gray scale image has been scrambled using the chaos map first then decomposed into 8 bitmaps.

Again from these bit maps it is possible to generate n numbers of binary matrix by distributing the elements randomly in n matrixes. Secondly this bit maps are embedded into n number of cover images using LSB techniques.

Thou we can hide maximum three bitmaps in a Cover image. And we have chosen these bit maps randomly out of n bitmaps generated from the secret image.

To select these randomly, a key (initial value) has been used to generate random numbers from the chaos map. So each cover image can carry maximum three bitmaps.

It is necessary to maintain the sequence of shares to retrieve the

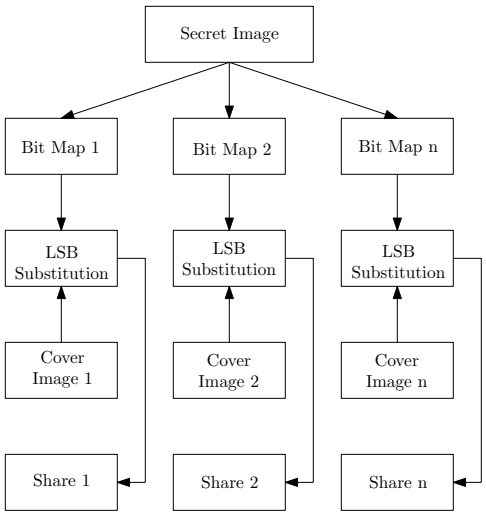


Fig. 3. A Diagram of the proposed Secret sharing Scheme.

secret image. Numbers of share may be more than 8 by breaking the bit maps again. The proposed scheme is shown in pictorial form in figure 3

For reconstruct the secret it will need to collect all the cover images. Then retrieve the bit maps from the cover images. The secret message bits are concealed into a digital cover image by

replacing a number of the least significant bits (LSB) of the cover image.

6. EXPERIMENTAL RESULTS

P In this the secret image used is a gray scale image of size $x \times y$ to construct three shares or three cover images. Fig. 7a. the secret image to be shared, 7b. Histogram of secret Image before embedding, 7c, Histogram of secret image after retrieving. Fig. 4a, 5a, 6a are three cover images, 5b, 6b are their corresponding Histogram. 4c, 5c, 6c are corresponding histogram after embedding the secret.

7. SECURITY ANALYSIS

The Further, to demonstrate the features of proposed new category of secret sharing scheme, in this paper the (n, n) sharing scheme has been compared with the other two categories in terms of four criteria: security, share generation operation & its computational complexity, pixel expansion and contrast.

The proposed scheme requires all the shares or cover images in proper sequence or the key to reconstruct the secret image properly; knowledge of few shares will not reveal any information. An image usually consists of many pixels, the possibility of finding the secret image would be $(k)m \times n$, where $m \times n$ is the no of pixels in the shares of the image and k is the number of gray levels of the image.

7.1 Histogram analysis

The histogram of the original image and that of the encrypted image are plotted in Figure 4, 5, 6, 7. It shows that the histogram of the encrypted image is uniform which makes statistical attacks difficult.

7.2 Information Entropy

The information entropy is defined as the degree of uncertainties in the system. The greater the entropy, the more is the randomness in the image, or the image is more uniform. Thus statistical attacks become difficult. Entropy is defined as equation **??**

$$H(m) = \sum_{i=0}^{2^N-1} p(m_i) \times log_2 \left[\frac{1}{p(m_i)} \right] \quad (2)$$

For an ideal random image, the entropy is calculated to be 8. So closer to 8, better is the randomness in the image. The entropy of the image was calculated to be 7.9998.

7.3 Share generation operation and its computational complexity

Considering an image of size $m \times n$ pixels, [4, 15] uses the Boolean operation (XOR) to generate the shares and the complexity of this operation is $O(m \times n)$. The [4, 15] uses matrix multiplication to generate shares, computational complexity of which is $O(m^3)$ and it works only for square images which is not a versatile scheme for all images. Whereas, that of the proposed scheme uses LSB subtraction which is a simple operation as compared to XOR operation used in [4, 15] and its computational complexity is $O(mn)$ which is better as compared to [3]. Hence the complexity of share generation improves drastically in the scheme.

7.4 Key Space

We are using Logistic map equation which involves two numbers as their initial condition. Also we use this equation twice, once for permutation and other for substitution. Because the precision of the parameters are $10 - 10$, the key space is 1040 which is roughly equal to 2133. This large key space eliminates all brute force and exhaustive attacks.

7.5 Key sensitivity

The system is very sensitive to the initial conditions which form the cipher key for the encryption/decryption process. Certain tests were done to examine the sensitivity of the key. If we increase the value of x_0 by $-1e10$ in the decryption process

7.6 Pixel expansion and Contrast

The proposed scheme generates the shares may be of different size but can reconstruct the secret image precisely whereas others lack the precision. [3] Reconstructs the secret image precisely. The proposed scheme can also reconstruct the secret image precisely.

8. CONCLUSION

In this paper, the authors have proposed a (n, n) secret image sharing scheme based on LSB subtraction of bit plains of the secret image for the construction and reconstruction operation. Compared with the other sharing schemes, the proposed (n, n) scheme for grayscale image can construct random shares and reconstruct the secret image precisely with low computational complexity. Common software tools, such as Matlab can be used to implement the method and reconstruct the secret images. To achieve higher security the author has select the bitmaps randomly at the time of generating the share images. This unique approach can be easily extended to binary and color image. The obvious advantages of this schemes in terms of low computation complexity, no pixel expansion and high reconstruction contrast/accuracy are encouraging. Secret sharing schemes have a vast scope of improvement. In future, the present work could be further extended to a more general (k, n) scheme and other schemes like multi-image sharing and audio and video.

9. ACKNOWLEDGEMENTS

The authors would like to thank the reviewers for their valuable comments. This work is supported by Department of Mathematics, N.I.T. Jamshedpur, India.

10. REFERENCES

[1] George Robert Blakley. Safeguarding cryptographic keys. In *Managing Requirements Knowledge, International Workshop on*, pages 313–313. IEEE Computer Society, 1899.

[2] Chi-Kwong Chan and L.M. Cheng. Hiding data in images by simple {LSB} substitution. *Pattern Recognition*, 37(3):469 – 474, 2004.

[3] Lin Dong and Min Ku. Novel (n, n) secret image sharing scheme based on addition. In *Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP), 2010 Sixth International Conference on*, pages 583–586. IEEE, 2010.

[4] N. Ma X.B. Li D.S.Wang, L. Zhang. Two secret sharing schemes based on boolean operations. *Pattern Recognition*, 40, 2007.

[5] Chong Fu, Zhen-chuan Zhang, Ying Chen, and Xing-wei Wang. An improved chaos-based image encryption scheme. *Computational ScienceICCS 2007*, pages 575–582, 2007.

[6] Jiankun Hu and Fengling Han. A pixel-based scrambling scheme for digital medical images protection. *Journal of Network and Computer Applications*, 32(4):788 – 794, 2009.

[7] Mitsugu Iwamoto and Hirosuke Yamamoto. The optimal n out of n visual secret sharing scheme for gray-scale images. *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, 85(10):2238–2247, 2002.

[8] Der-Chyuan Lou and Chia-Hung Sung. A steganographic scheme for secure communications based on the chaos and euler theorem. *Multimedia, IEEE Transactions on*, 6(3):501–509, June 2004.

[9] Bhaskar Mondal and Tarni Mandal. A multilevel security scheme using chaos based encryption and steganography for secure audio communication. *International Journal of Research in Engineering and technology*, (10):399–403.

[10] Bhaskar Mondal, Tarni Mandal, Sunil Kumar Singh, and Krishana Mohan Acharjee. A novel (k, n) secret key sharing scheme based on linear equations. *International Journal of Engineering Research Technology (IJERT)*, 2(10):1679–1682, 2013.

[11] Bhaskar Mondal and Sunil Kumar Singh. A highly secure steganography scheme for secure communication. *International Conference of Computation and Communication Advancement (IC3A)-2013*, 2013.

[12] Bhaskar Mondal, Deep Sinha, Navin Kumar Gupta, Nishant Kumar, and Pankaj Goyal. An optimal (n, n) secret image sharing scheme. *UACEE International Journal of Computer Science and Its Applications*, 2(3):61–66, 2012.

[13] N.K. Pareek, Vinod Patidar, and K.K. Sud. Image encryption using chaotic logistic map. *Image and Vision Computing*, 24(9):926 – 934, 2006.

[14] Adi Shamir. How to share a secret. *Commun. ACM*, 22(11):612–613, November 1979.

[15] F. Yi, D.S. Wang, P. Luo, and Y.q. Dai. Two new color (n, n)-secret sharing schemes. *Journal on Communications (Chinese)*, 28(5), 2007.

[16] Zhang Yuan-Biao and Wang De. An image encryption and sharing algorithm based on chaos and indeterminate equation. In *Computational Intelligence and Software Engineering, 2009. CiSE 2009. International Conference on*, pages 1–4, Dec 2009.

AUTHORS PROFILE

Bhaskar Mondal was born in West Bengal, India in 1986. He received B. Tech. degree in Computer Science and Engineering from West Bengal University of Technology in 2008 and M. Tech. degree in Computer Science and Engineering from Kalyani Government Engineering College, West Bengal, India in the year of 2010. He is working at National Institute of Technology, Jamshedpur as Assistant Professor in the department of Computer Science and Engineering since January 2011. His research interest includes Secret Image Sharing, Security and Data Mining.

Dr. Tarni Mandal was born in Bihar, India in 1956. He received Bachelor of Science (Hons.) in Statistics in 1977 followed by Master of Science in Statistics in 1980 from Bhagalpur University. He received Master of Science in Applied Mathematics from Ranchi University in 1995. He was awarded PhD by Ranchi University in 2001. He is working at National Institute of Technology, Jamshedpur as Associate Professor in the department of Mathematics. His research interest includes Secret Image S Operations Research, Security and Fractional Functional Programming Problem.

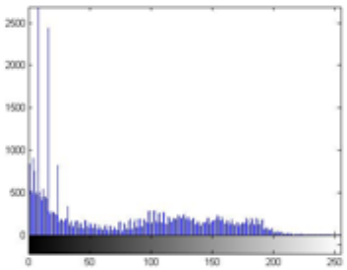
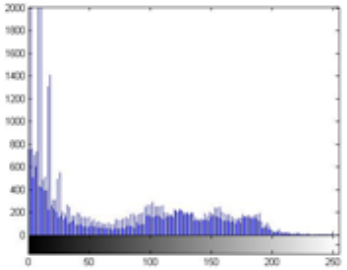
[a.]  [b.]  [c.] 

Fig. 4. a. Coner image 1, b. Histogram of cover image 1, c. Histogram after embedding the share.

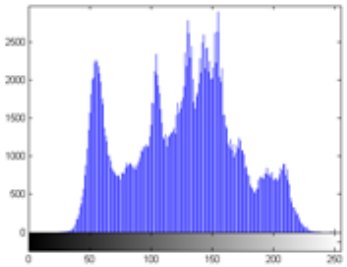
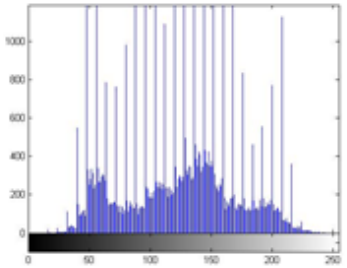
[a.]  [b.]  [c.] 

Fig. 5. a. Coner image 2, b. Histogram of cover image 2, c. Histogram after embedding the share.

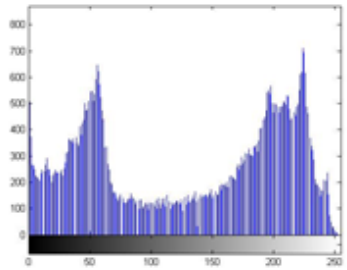
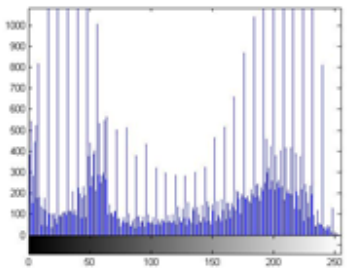
[a.]  [b.]  [c.] 

Fig. 6. a. Coner image 3, b. Histogram of cover image 3, c. Histogram after embedding the share.

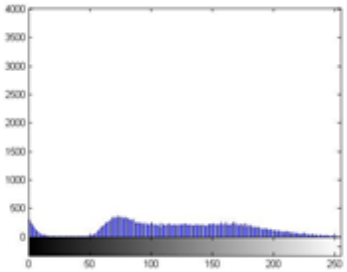
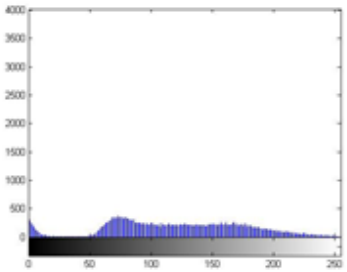
[a.]  [b.]  [c.] 

Fig. 7. a. The secret image, b. Histogram of secret image before encryption, c. Histogram of secret image after reconstruction