International Journal of Engineering Research-Online
A Peer Reviewed International Journal
Articles available online http://www.ijoer.in

Vol.3., Issue.2, 2015

RESEARCH ARTICLE

ISSN: 2321-7758

VISUAL SECRET SHARING SCHEME BASED ON RANDOM GRID METHOD FOR MULTIPLE SECRET SHARES

SHRIDEVI AVVANNI[1], RAVISHANKAR K[2]

[1]Depatment of CSE, VTU, SIT Valachil MANGALORE, KARNATAKA, INDIA

[2]Depatment of CSE Associate.Prof, SIT Valachil MANGALORE, KARNATAKA, INDIA

Article Received: 11/04/2015 | Article Revised on:15/04/2015 | Article Accepted on:18/04/2015

SHRIDEVI AVVANNI

ABSTRACT

The Hill cipher is used to divide an image into sub-images and then the concept of random grid is applied to sub-images for construction of encrypted image. This scheme suffers from security issues. Although, the random grid is used as a second layer of security, it does not play any effective role during decryption. Secondly, even a crude guess of the coefficient matrix used in Hill cipher equations can reveal the secret. In the proposed method, a system of linear equations with secret keys (coefficients) is used to divide a secret image into sub images of smaller size. Then the concept of random grid with XOR operation is applied to the sub images for construction of the shared images. It is impossible to reveal the secret image without the knowledge of four coefficients values, encoded shares and random grid values.

KEYWORDS: Visual secret scheme, Random grid, Linear equation, Hill cipher

I.INTRODUCTION

Information security and privacy is one of the primary necessities in the world of information and communication technology. Cryptographic methods and tools play a big role in making the information secure. In view of the unprecedented increase in the information flow over the network, secure communication has become a critical issue. Nowadays images containing private and confidential information are widely communicated through open channels and therefore it has become increasingly important to device secure methods to protect such information from intentional or unintentional intrusion. As a solution to secure image sharing problem, Naor and Shamir proposed a Visual Secret Sharing (VSS) scheme in 1994 [1], that laid the foundation of visual cryptography. VSS scheme is a cryptographic technique suitable for applications to image data. In this scheme, a secret image is decomposed into n ($n > 1$) meaningless shares. Stacking k ($k \leq n$) or more shares reveals the secret. The most important feature of this technique is that the decryption does not require any complex computation and depends only on the human visual system. This scheme is also known as (k, n) VSS scheme, as any set of less than k shares does not reveal any information about the secret.

Although the VSS scheme introduced by Naor and Shamir was an innovative and secure solution to image sharing, it suffered from two main

drawbacks. First, every pixel of an image was represented by more than one pixel in a given share. This is known as pixel expansion. Second, the recovered image suffers from low contrast. Further, each image is split into share images of higher size, resulting in high memory requirement. To address these issues, many researchers have given solutions that deal with one or more aspects of the VSS issues [13]. However, it has not been possible to provide a single efficient solution addressing efficiently all the concerns of the VSS scheme. Some single secrets schemes have been developed with the help of many cryptographic ciphers like Hill ciphers and random grid [7, 10].

In 1994 Naor and Shamir introduced a VSSS(Visual secret sharing scheme)inthis method sharing the secret images in to the group of participants and later start constructing a (k,n) threshold VSS. The original image is constructed from the k-shares through the human vision. The vsss algorithm has constructed the 'n' number of shares with 'n' number of secret keys that is called as (n,n) combination method. The (k,n) vsss technique has been improved by Naor and Shamir and pixel expansion is generated by hyper graph color methods.

The scheme claims to provide secure communication with easy decryption. However, the present authors have observed the following issues with the scheme (1) Even an approximate guess of encryption key can reveal the secret information (2) Even if the attacker does not have Hill cipher keys, secret image is partly revealed if random grid is simply XOR'ed with the encrypted sub images. This motivated us to define another VSS scheme using linear equations and random grid. The present scheme takes care of issues mentioned above and hence provides a more secure solution. In the proposed method, a system of linear equations with secret keys (coefficients) is used to divide a secret image into sub images of smaller size. Then the concept of random grid with XOR operation is applied to the sub images for construction of the shared images. It is impossible to reveal the secret image without the knowledge of four coefficients values, encoded shares and random grid.

II. SYSTEM ARCHITECTURE

System architecture is the conceptual design that defines the structure and behavior of a system. An architecture description is a formal description of a system, organized in a way that supports reasoning about the structural properties of the system. It defines the system components or building blocks and provides a plan from which products can be procured, and systems developed, that will work together to implement the overall system.

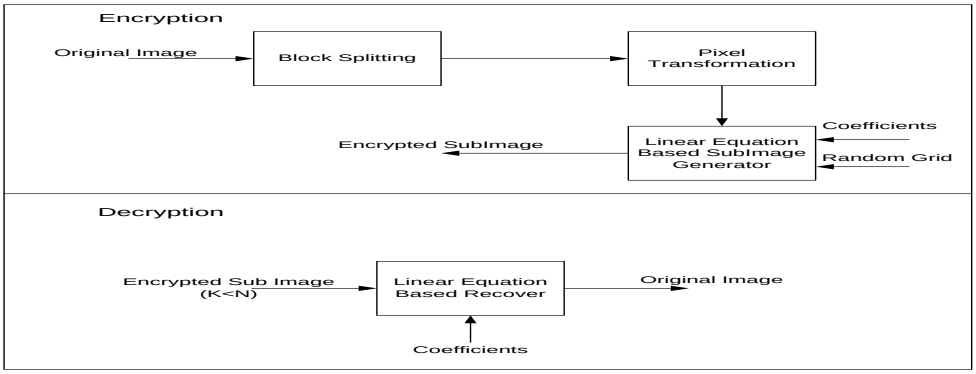


Figure 1.System Architecture

III. RELATED WORK

A Hill cipher method is symmetric key algorithm it has few disadvantages the decrypted images are with low contrast, high storage requirement, pixel expansion problem. An advanced Hill cipher method has been proposed a combination of affine Hill cipher and Hill cipher method. This advanced hill cipher method used for to enhance for security [3]. The Hill Cipher used for matrix manipulations. It has some drawbacks; first every key matrix is invertible. Secondly the Hill cipher it compromised to the known attacks. In Vss scheme based on Hill cipher and random grid method, first the image is subdivided into two intermediary encrypted sub-

images E_1 and E_2 by using Hill cipher method. Then the random grid R is generated it has a matrix ranges from 0 to 255. XOR operation is performed for two final encrypted images.

IV. PROPOSED METHOD

The proposed scheme is similar to vss scheme. In this scheme which allows encryption and decryption process by using linear equation method using co-efficient values.

$AX_1+BX_2=Y_1$ (1)

$CX_1+DX_2=Y_2$ (2)

The coefficient matrix is invertible (AD-BC#0) and we assume that A=1 and D=(BC-1) mod 256 this produces coefficient matrix for integer solutions. The image size is M*N and random grid R size is M*N/2. Let the integer value between 0 to 255. A pair of pixel values is randomly selected by using R. The encryption is performed as follows-

I_1= (AX+BY) mod 256 (3)

I_2= (CX+DY) mod256 (4)

Where $X=P_1+A$ (5)

$Y=P_2+D$ (6)

STEPS FOR ENCRYPTION METHOD

1] An image of I of size M*N is divided into sub blocks it having consecutive pixels.

2] The first block of a sub image its pixels are p_1 and p_2 are transformed to I_1 and I_2.

3] Construct the two sub images I_1 and I_2 with the size of M*N/2.

4] The random grid R and two sub images I_1 and I_2 to construct the encrypted images

E_1 and E_2.

$E_1(i,j)=R(i,j)+I_1(i,j)$ (7)

$E_2(i,j)=R(I,j)+I_2(i.j)$ (8)

STEPS FOR DECRYPTION METHOD

1] Use the encrypted images E_1 and E_2 and random grid R.

2] Construct the sub- images I_1 and I_2 by using random grid R and encrypted images.

3] Generate I_1 and I_2 and with coefficient values of A, B, C, D get the values of X' and Y'

$I_1'=AX'+BY'$ (9)

$I_2'=CX'+DY'$ (10)

4] Generate the pixels and retrieved secret the images.

$P_1'=(X'-A) \bmod 256$ (11)

$P_2'=(Y'-D) \bmod 256$ (12)

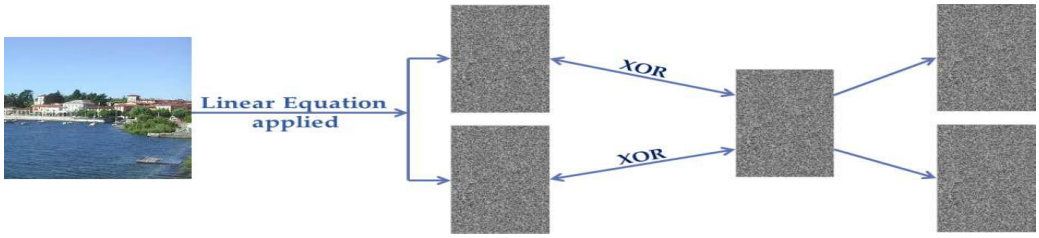
5]The original image generated by using the below equations.

$$I_1'(i,j)=R(i,j)\oplus E_1(i,j)$$

$$I_2'(i,j)=R(i,j)\oplus E_2(i,j)$$

V. EXPERIMMENTAL RESULTS

In this section, the proposed method is implemented on the gray scale image Lena of the size 256× 256 as the secret image (Fig.2 (a)). The random grid R with size 256×128 generated using a random number generating function is also shown in Fig.2 (c). Values for the coefficients *A, B, C* and *D* are chosen as 12, 125, 209 and 1. These values for the coefficients *B* and *C* are only to encrypt the first two pixels of the original image. For further pixel blocks, these values will be randomized with help of the Eq. (11) and (12). *A* will depend on *B* and *C* . *D* will remain 1 for the entire experiment. Images obtained after steps E3-E4 are shown in Fig. 2(b) and the final encrypted images after step E5 are shown in Fig 1(d). In order to decrypt the secret image, encrypted sub images, coefficients values and random grid are collected (as shown in Fig. 3(a) and (b)) and after step D2 sub-images are obtained shown in Fig. 3(c). The pixels of the original image are obtained after step D3-D4 and as the pixels are obtained the secret image is retrieved as shown in Fig. 3(d).



(a) *b)* *(c)* *(d)*

Figure 2. (a) The secret image with size 256× 256, (b) the sub-images I1 and I2 with size 256× 128, (c) the random grid R with size 256× 128, and (d) theencrypted images E1 and E2 with size 256× 128.

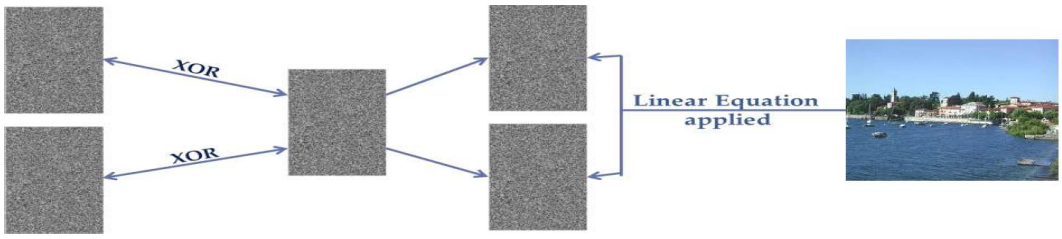


Figure 3. (a) the encrypted images E1 and E2 with size 256×128, (b) the random grid with size 256×128, (c) the retrieved sub-images I1' and I2', (d) the retrieved original image with size 256×256.

So, in the case of Chen's scheme, random grid fails to provide second layer of security (Fig. 4, 5). However, in the proposed scheme until the second layer of decryption is applied, nothing can be guessed about the secret image as is evident from Fig. 3(c). Since the coefficients *B*, *C* are based on random grid *R* and are different for each block of the image, it becomes highly impossible for an intruder to guess the numbers. To recover the secret image, one must have encrypted images, random grid and key values (coefficients *A, B, C* and *D*) hence the proposed scheme also increases the security of the original image. Advantage of the scheme is that no one can retrieve the secret without having random grid, coefficients value and encrypted images. In this scheme we are also able to improve upon the issue of lossy recovery and pixel expansion. Random grid and encrypted images have smaller size than the original secret image so storage space requirement is the same as that in [5].

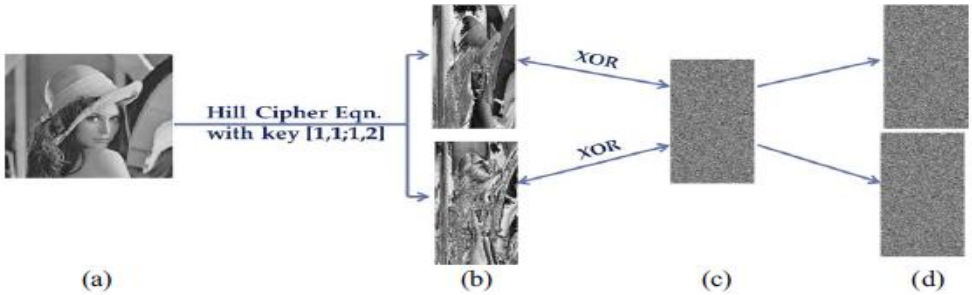


Figure 4. (a) The secret image with size 256× 256, (b) the two sub-images with size 256× 128, (c) the random grid with size 256× 128, and (d) the encrypted images with size 256× 128

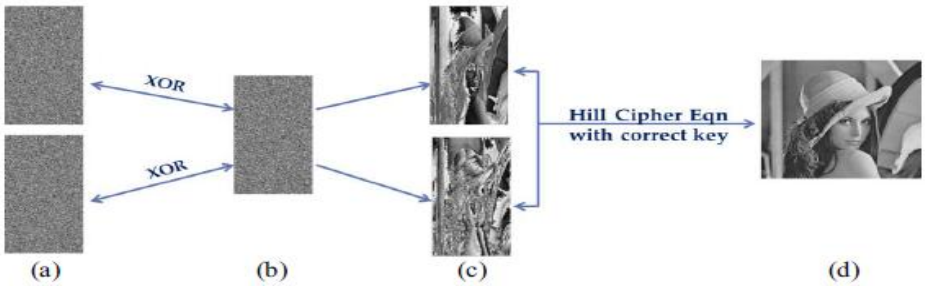


Figure 5. (a) the encrypted images 256×128, (b) the random grid with size 256×128, (c) the retrieved sub-images and (d) the retrieved original image with size 256×256.

VI. CONCLUSION

This paper suggests an efficient and secure VSS scheme based on linear equations. The scheme is more secure than the Hill cipher based scheme proposed in [5]. To recover the secret image, availability of correct coefficient values, random grid and both encrypted images are necessary. Proposed method uses simple linear equation and dependency among their coefficients. Since the coefficients of linear equations employed during encryption are randomized for each pixel block using the random grid, it is not possible to guess the

coefficients. Numerical results demonstrate the effectiveness of the method. The method is proposed for single secret sharing and can also be extended for multi-secret sharing. Further, color image cryptographic method can also be developed using the scheme.

REFERENCES

[1]. M. Naor, and A. Shamir , "Visual cryptography," Advances in Cryptology-Eurocrypt, Lecture Notes in Computer Science, vol. 950,pp. 1–12, 1994.

[2]. Daoshun Wang, Lei Zhang, Ning Ma, and Xiaobo Li, "Two secret sharing schemes based on boolean operations," J. Pattern Recogition Society, vol. 40, pp. 2776–2785, 2007.

[3]. Tzung-Her Chen, and Chang-Sian Wu, "Efficient multi-secret image sharing based on boolean operations," J. Signal Processing, vol. 91, pp. 90–97, 2011.

[4]. Young-Chang Hou, Zen-YU Quan, and Chih-Fong Tsai, A-Yu Tseng "Block-Basedprigressive visual secret sharing," J. Information Sciences, Vol. 233, pp. 290–304, 2013.

[5]. Wei-Kuei Chen, "Image sharing method for gray-level images," J. Systems and Software, vol. 86, pp. 581–585, 2013.

[6]. Hill, L.S., "Cryptography in an algebric alphabet," The American Mathematical Monthly, vol. 36, pp. 306–312, 1929.

[7]. Chen, T.-H., Tsao, and K.-H., "Visual secret sharing by random grids," J. Pattern Recognition, vol. 42, pp. 2203–2217, 2009.

[8]. Jen-Bang Feng, Hsien-Chu Wu, Chwei-Shyong Tsai, and Yen-Ping Chu, "A new multi-secret images sharing shcems using Lagrange's interpolation," J. Systems and Software, vol. 76, pp. 327–339, 2005.

[9]. Tzung-Her Chen, Kai-Hsiang , and Yao-Sheng Lee, "Yet another multiple -image encryption by rotating random grids," J. Signal Processing, vol. 92, pp. 2229–2237, 2012.

[10]. Bibhudendra Acharya, Saro j Kumar Panigrahy, Sarat Kumar Patra , and Ganapati Panda,"Image encryption using advanced hill cipher algorithm," J. Recent Trends in Engineering, vol. 1, pp. 663–667, 2009.

[11]. Feng Liu, Chuankun Wu and Xijun Lin, "Step construction of visual cryptography schemes,"J. IEEE Transactions on Information Forensics and Security , vol 5, pp. 27–38, 2010.

[12]. Kai-Hui Lee and Pei-Ling Chiu, "Image size invariant visual cryptography for general access structures subject to display quality constraints," J. IEEE Transactions on Image Processing,vol. 22, pp. 3830–3841, 2013

[13]. Z. X.Yin, C. C. Lin, and C. C. Chang, "Image sharing with stegnography and authentication, " in Visual Cryptography and Secret Image Sharing, S. Cimato and C. N. Yang , Eds. New york: CRC Press , 2012 , pp.428 – 433.

[14]. Jen-Bang Fenga, Hsien-Chu Wub, Chwei-Shyong Tsaic, Ya-Fen Changb,and Yen-Ping Chu,"Visual secret sharing for multiple secrets," J. Pattern Recognition, vol 41, pp. 3572–3581, 2008.