LINEAR EQUATION BASEDVISUAL SECRET SHARING SCHEME FOR SECURE IMAGE SECRET SHARING

Shridevi Avvanni
Student
Srinivas Institute of technology,VTU Belgaum
Valachil,Mangalore,Karnataka,India

Ravishankar K
AssociateProfessor
Srinivas Institute of technology, VTU Belgaum
Valachil, Mangalore,Karnataka,India

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 randomgridvalues.

Keywords: Visual secret scheme, Randomgrid, Linearequation, Hill cipher;

I. INTRODUCTION

Visual cryptography is a cryptographic technique which allows the Visual information Ex: Pictures, images etc , to be encrypted in such way that decryption becomes mechanical operation that does not require a computer.Now a day’s images are transmitted by channels, and images containing private and confidential information therefore it has become increasingly important to device secure method to protect the information. Cryphographic methods and tools a big role in making information secure. VSS scheme is a cryptographic technique. In this scheme a secret image is decomposed into n (n>1) meaningless shares. The most important of this feature is decryption process does not hold complex difficulties; it depends on human visual system. Thisscheme is known as vss scheme as any set of less than k shares does not it does not reveal the any information about the secret.

The VSS schemeintroduced by Naor and Shamir was an innovative and protected image sharing scheme[2]. In secure sharing scheme it has some limitations. First each shares of secret image is larger because to improve the efficiency and maintaining security. Secondly a secret scheme uses a random bit to distribute among random bits[2]. It suffered from few drawbacks. First, each pixel of an image was represented by more than one pixel in a share of image. Secondly, each image is divided into shares of higher size, require high memory, decryption process suffers from low contrast.

In 2010 Feng proposed a VSS schemeit is based on Boolean operations. First ‘n’ number of random matrices are generated to calculate n matrices. Then “AND” operation is applied between matrices and XOR operation is performed on shadow images. Basic idea of the scheme is to divide a secret image into n shares. Two operations are performed as Encryption and Decryption to reveal the information. In existing Hill cipher method it suffers from lossy recovery and pixel expansion problems, high storage requirements to overcome these drawbacks chen proposed gray scale image. The encryption is used to divide a secret images into sub images and then apply XOR operation between sub-images and random grid is to encrypt the images and then reverse process produces for decryption operation. In proposed method linear equations with coefficients is used to divide the images into sub images in smaller size and then perform the random grid with XOR operation to construct the shared images.

II. 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.

III. PROPOSED SCHEME

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

$$I_1= (AX+BY) \bmod 256 \qquad (3)$$

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_1andI_{2by} using random grid R and encrypted images.

3] GenerateI_1 and I_2 and with coefficient values of A, B, C, D get the values of X ’and $Y^{'}$

$I_1^{'}$=AX’+BY’

$I_2^{'}$=CX’+$DY^{'}$

4] Generate the pixels and retrieved secret theimages.

P_1’= ($X^{'}$-A) mod 256

P_2’= (Y’-D) mod256

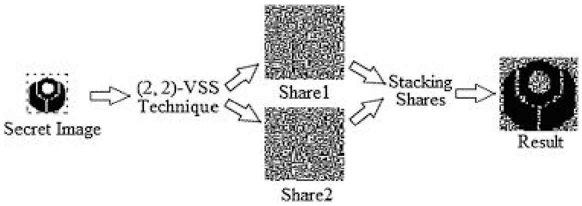

Fig1.visual secret sharing scheme

Fig1 shows that visual secret sharing scheme by using the coefficient values with random gridmethod[4].

IV.EXPERIMENTAL RESULTS

The proposed method is implemented on color image of the size 256*256 as the secret image. The random grid R with size 256*128 generated using a random number generating function is shown in Figure2. Values for the coefficients A, B, C and D are chosen as 1,20,30,40. 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 wih help of Eq (7) and (8). A will depend on B and C. D will remain 1 for the entire result. Finally encrypted images are generated. In order to decrypt the secret image, encrypted sub images coefficient values and random grid are collected and after original images is obtained by step D3-D4 and as all pixels are obtained the secret image is retrieved.

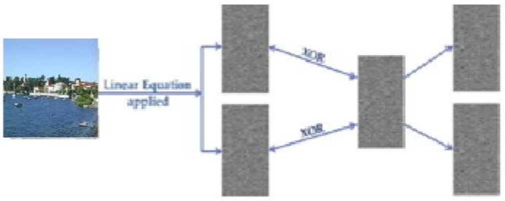

Figure 2.Encryption process of original image with size of 256*256

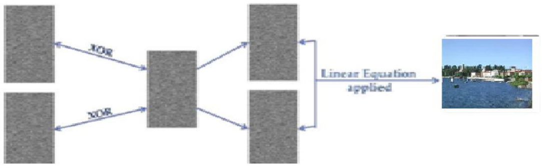

Figure 3. Decryption Process of original image with size of 256*256

IV.CONCLUSION

In this paper we suggest an efficient and secureVSS scheme based on linear equations. The scheme is secure than the Hill cipher scheme. To recover the secret image, availability of correct coefficient values, random grid and both encrypted images are necessary. Proposed method uses 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. 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] Hill L.s “cryptography in an algebraic Alphabets” the American mathematical Monthly 306-312,1929

[2] chen T-H Tsao and KH, “Visual secret Sharing by random grids j pattern Recognition vol 42 pp 2203-2217,2009

[3] M.Naor and Shamir “visual cryptography Advances in cryptology eurocrypt,vol 950,pp 1-12,1994

[4] Jen bang Fenga Hsien-chu wub Chwei-Shyong tsaic ya Fen chanb and Yen-ping

[5] imple Kapoor1, Swati Keshari2, Saurabh kumar 2014 lord krish college 2012