A Novel Two Stage Binary Image Security System Using (2,2) Visual Cryptography Scheme.

Mr. ROHITH S
Lecturer,
Department of E&C,
NCET, Bangalore,
Karnataka, India-562110

Mr. VINAY G
Student.
Department of E&C,
NCET, Bangalore,
Karnataka, India-562110

Abstract: Visual Cryptography Scheme (VCS) is an encryption method used to encode secret written materials. The idea is to convert the written material into a binary image and encode this image into n shadow image, it is also called as shares of images. The decoding only requires selecting some subset of these n shadow images, making transparencies of them and stacking them on top of each other. Main advantage of this scheme is mathematical computation complexity is reduced compared to conventional cryptographic techniques.

This paper presents design of two stage binary image security scheme using (2,2)Visual Cryptography Technique such that we are not able to get back the original image at the first decoding stage. As the cryptographic algorithm becomes more relevant, it will become inefficient. So, the basic model of Visual Cryptography is not an efficient tool to hide the information anymore. This method aims to improve efficiency of VCS. The performance of proposed algorithm is compared with three different binary images. Result shows that there is no residual information present in the shares.

Key word: Visual Cryptography Scheme, LFSR, Binary Image Security.

I Introduction

With the invention of the Internet, more and more digital data can be accessed via the network. Internet users can transmit and store images with less secured channels. To secure the information one possible technique is cryptography where information is encrypted using key and same key is used to decrypt the information. Here computation complexity of decryption algorithm increases the information security[9]. Visual Cryptography is a technique which provides information security and uses simple decryption algorithm unlike the computationally complex algorithms used in traditional cryptography schemes. This technique allows Visual information such as pictures, text, etc. to be encrypted in such a way that their decryption can be performed by the human visual system. This technique encrypts a secret image into shares such that stacking a sufficient number of shares reveals the secret image [1-4]. In this paper an overview of the emerging Visual Cryptography scheme and design of the proposed scheme is discussed.

An example of (2, 2) Visual Cryptography Scheme is given in figure1a to 1d. Original binary image is shown in Figure1a. Figure 1b & 1c are share1 and share2 generated from original image by (2, 2) Visual Cryptography Scheme discussed in section IV. Figure 1d reconstructed image by application of stacking process (BIT OR operation) on share1and share2. The reconstructed image is visually identical to the original image.

The rest of the paper is organized as follows. The section II gives brief description about earlier work. Applications of Visual Cryptography Schemes are discussed in section III. Design preliminaries are discussed in section IV. Proposed scheme is given section V. In Section VI Results of proposed schemes are discussed. Conclusion is given in section VII.

Figure1a Original Binary Image

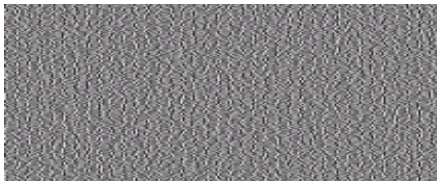


Figure1b Share 1

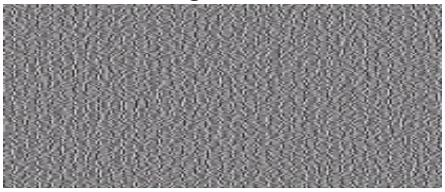


Figure 1c Share 2

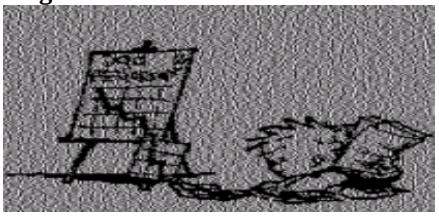


Figure 1d Reconstructed Image by Stacking Process

II Previous Work.

Many authors published different Visual Cryptography Schemes [1-8] for different applications. Each scheme has its own advantages and disadvantages. Few such schemes were given in Table1.

Table 1 Previous work in Visual cryptography

Authors	Features of the Work
Naor and Shamir [2]	Basic (2,2) Visual Cryptography Scheme was discussed
Ateniese *et al*[8]	Elegant VCS for general access structures based on the cumulative array method was discussed.
Tzeng and Hu[1]	In this VC scheme secret image can be either darker or lighter than the background
Naor and Pinkas[7]	Methods of authentication and identification between two participants were discussed
Yang et al [6]	Cheating method against some VC schemes were discussed. In their cheating method, the cheater needs to know the exact distribution of black and white sub pixels of the shares of honest participants. Based on this characteristic they proposed a cheat preventing method to prevent the cheater from obtaining the distribution.

III Application of VCS

There are many applications incorporated with the Visual Cryptography Scheme. Two main applications are discussed in this section.

1) **Electronic-Balloting System**: Dilemma et al [3] proposed a secret-Ballot Receipts system that is based on (2,2) binary VCS. It generates an encrypted receipt to every voter which allows them to verify the election outcome even if all election computers and records were compromised. At the polling station, the voter will receive a double-layer receipt that prints his/her voting decision. The voter will be asked to give one of the layers to the poll worker who will destroy it immediately with a paper shredder. The remaining one layer will now become unreadable.
2) **Encrypting Financial Documents**: The VCS principle can also be applied in transmitting confidential financial documents over Internet. Visual Cryptography is an example of this type of system being proposed by Hawkes et al [4]. Visual Cryptography can encode the original drawing document with a specified (k, n) VCS, then send each of the encoded n shares separately through Emails or FAX to the recipient. The decoding only requires bitwise OR operation on all shares in the specified directory, and needs no extra effort of cryptographic computation. Any malicious attacker who intercepts only m of n shares where $m < k$ will not be able to gain any information about the financial document.

IV Design preliminaries.

A) Visual Cryptography

The basic model of Visual Cryptography was introduced by Naor and Shamir [2] in 1994 accepts binary image I(x, y) as secret image, which is divided into 'n' number of shares. Each pixel of image I(x, y) is represented by 'm' black and white sub pixels in each of the 'n' shared images. It is impossible to get any information about the secret images from individual shares. The other advantage of VCS is that, unlike other cryptography techniques, the secret image recovery does not need difficult computations. i.e the secret information can easily be recovered with enough number of shares through stacking process (human vision) instead of special software or hardware devices.

Naor and Shamir proposed a *k* out of *n* scheme and assumed that the image or message is a collection of binary data 0 and 1displayed as black and white pixels. According to their algorithm, the secret image is turned into *n* shares and the secret is revealed if any *k* of them are stacked together. So the image remains hidden if less than *k* shares are stacked.

The main parameters of Visual Cryptography includes image contrast and the number of sub pixels of recovered image. The contrast of a image is a relative difference between the original and retrieved image. As increased in number of sub pixels while creating the shares, size of the share (column) also increases. This increment in turn affects the quality of retrieved image. Some researchers have focused on contrast degradation and introduced methods to improve the contrast of the reconstructed secret image[5].

2-out-of-2 Secret Image Sharing Scheme

The basic idea of 2-out-of-2 Visual Cryptography sharing scheme is illustrated in Table2. Every secret pixel of the original binary image is converted into four sub pixel of two share images and recovered by simple stacking process. This is equivalent to using the logical OR operation between the shares. As illustrated in Table2 four sub pixels are generated from a pixel of the secret image in a way that two sub pixels are white and two sub pixels are black. The black or white pixel selection is based on random selection. In this paper 8 stages LFSR (Linear Feed Back Shift Register) is considered to generate the random bit and design is discussed in subsection B.

Pseudo code of share generation scheme is given below. Based on pixel bit and random sequence bit, share1 and share2 will be generated. The size of obtained share will be twice the as many columns in the original image.

```
For i=1 to Size of the image
        If (pixel == 1)
                If (reandom_bit==1)
                        Share1=[1 0]
                        Share2=[1 0]
                Else
                        Share1=[0 1]
                        Share2=[0 1]
        Else
                If (reandom_bit==1)
                        Share1=[1 0]
                        Share2=[0 1]
                Else
                        Share1=[0 1]
                        Share2=[1 0]
        END
End of the loop
```

Table-2 (2, 2) Visual Cryptography Sharing Scheme

Pixel	White		Black	
Prob.	50%	50%	50%	50%
Share 1				
Share 2				
Stack share 1 & 2				

B. LFSR Design

A Linear Feedback Shift Register(LFSR) is a sequential shift register with combinational logic that makes it to pseudo-randomly cycle through a sequence of binary values. In this paper to generate a random bit an 8 bit LFSR is considered with a polynomial $x^8+x^6+x^5+x^4+1$ and corresponding design is given in the figure 2a. Feedback around an shift register comes from a selection of points (D) in the register chain and constitutes XORing these taps to provide tap(s) back into the register as shown in the figure2a. The 8 bit LFSR case D_0,D_4,D_5,D_6 are XORed and feeding back to MSB bit(D_7) and this bit is used as a sequence bit in future. The 8-bit sequence will repeat every after 255 cycle(1 cycle= one shift) and all generated sequence are purely based on the initial 8-bit data present in the register.

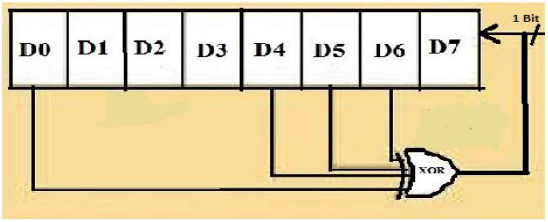


Figure 2a 8 Bit Linear Feed Back Shift Register

V Proposed Scheme

In the Proposed scheme we used (2, 2) Visual Cryptography Scheme. The whole design is divided into two process

1) Encryption(Creating shares)
2) Decryption(Human Visual System)

Encryption process

Encryption process is partitioned into two stages and shown in figure 3b.

- **First stage**

  An original binary image of size 100X100 has been considered in our design where each pixel is either 0 or 1.
  A (2, 2) Visual Sharing technique (as discussed in section IV) is applied on original binary image. From this process two binary share images will be generated.

- **Second stage**

  In the second stage four share images are generated from the two share images obtained from first stage using (2,2) VCS, this is called chain share of order 2.
  Further to enhance the security, share encryption is performed on four shares obtained from previous step using 8-bit different LFSR sequence (as discussed in section IV) by XORing the share bit with LFSR bit and it is repeated for whole binary share image. Hence, no two share should generate partial image.

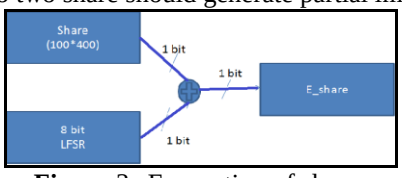


Figure 3a Encryption of shares

Decryption process

Decryption process is reverse process of encryption. It consists of two stages and pictorial representation of decryption process is given in figure3c.

- **First Stage**

  To decrypt the four shares from encrypted shares same LFSR sequence must be used which was used in earlier encryption process and bitwise XOR operation performed between encrypted share and LFSR bit sequence. Otherwise original image will not be recovered in future.

  From four decrypted share of the previous step, two partial shares were obtained by performing bitwise logical ORing between share 1,2 and share 3,4.

- **Second Stage**

  Bitwise logical OR operation performed on two obtained share images from previous stage to get back the retrieved image. The obtained image is identical to original image.

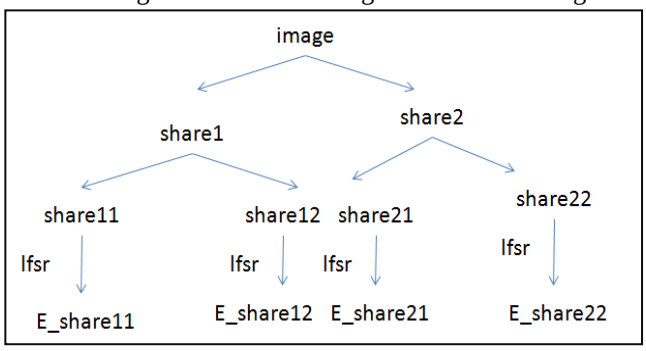


Figure 3b Encryption Process with two stages

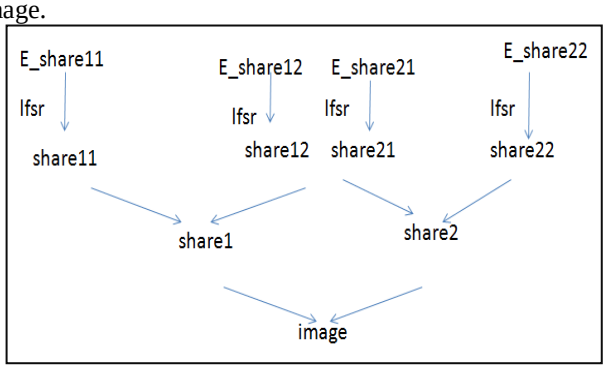


Figure 3c Decryption Process with two stages

VI Results

Matlab 7.1 Software tool is used to analyze the result. To study the performance of proposed scheme three different binary images of size 100X100 were used and shown in figure 5a, 5b, 5c. The stage by stage result of proposed scheme is given in table 3a and 3b.

Figure 5a

Figure 5b

Figure 5c

Table 3a shows the Encryption process of the original binary image. In the table3a Figure4a shows three different original binary images, Figure4b and 4c are shares generated in the 1st stage. The result shows no residual information of original image perceptually observed among the two shares. In the second stage four different shares are generated and is given in figure 4d to 4g. In this four shares stacking process of any two shares gives residue of original information. So to provide additional security share encryption is performed on all the four shares as discussed in section V. Figure 4h to 4k is scrambled shares using 8 stage LFSR sequence.

Table 3a Encryption process

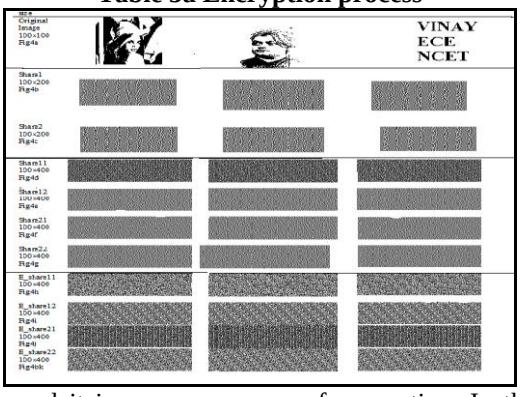
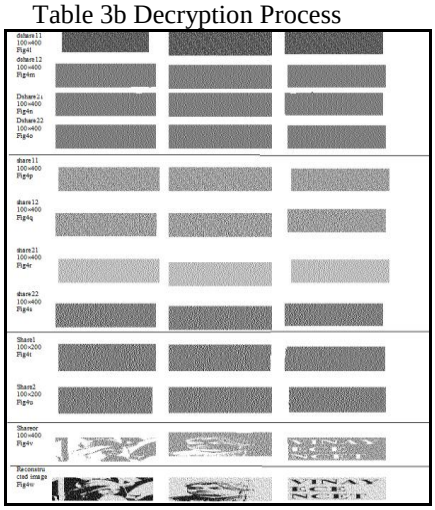


Table 3b gives decryption process and it is reverse process of encryption. In the table3b the figure 4l to 4o is same scrambled share image. The same LFSR initial sequence or key need to be used to get back the four shares. The obtained shares are shown in the figure 4p to 4s. It is observed that no residual information is visually seen. Figure 4t and 4u are the shares obtained from BIT ORing the shares shown in Fig 4p and 4q and Fig 4r and 4s respectively. Reconstructed image given in figure 4v obtained by BIT ORing the previous shares i.e.,Fig4t and 4u. From figure4v image can be easily identified but

contrast is poor. In order to obtain the efficient reconstructed image Bitwise XOR is applied between the shares(Fig4t and 4u) and obtained image shown in figure4w.The figure4w image is identical to original image except the size.

Table 3b Decryption Process



V Conclusion

Using the proposed design original image successfully encoded into 4 share images. In This scheme two stages were used it's very difficult to access the original information by unauthorized receiver. In this paper we used only order 2(two stages) because if we increase the order even though we can generate many number of shares, but quality of the reconstructed image will be poor (more number of columns) and needs more storage space for shares.

Difficulties for image reconstruction by unauthorized receiver

1. **Order and orientation of chain share:** If the order of the chain share is unknown and orientation is mismatched we will not get the original image
2. **LFSR sequence:** We have to use same LFSR sequence for encryption as well as decryption to get back the original image
3. **Number of shares: A**ll the four shares compulsorily necessary to identify the original binary image.

VI Reference

[1] W.-G. Tzeng and C.-M. Hu, "Anewapproach for visual cryptography, *"Designs, Codes, Cryptog*. vol. 27, no. 3, pp. 207–227, 2002.

[2] M. Naor and A. Shamir, "Visual cryptography", *in Eurocrypt'94 Proceeding*, LNCS, vol.950, Spring-Verlag, pp.1-12, 1995.

[3] D Chaum, Secret-ballot receipts: True voter-verifiable elections, IEEE Security and Privacy, 2004,38-47.

[4] W. Hawkes, A. Yasinsac, C. Cline, An Application of Visual Cryptography to Financial Documents, technical report TR001001, Florida State University (2000).

[5] M. Naor and A. Shamir "Visual cryptography: Improving the contrast via the cover base" *IACR Eprint archive*, 1996.

[6] C.-N. Yang and C.-S. Laih, "Some new types of visual secret sharing schemes," in *Proc. Nat. Computer Symp.*, 1999, vol. 3, pp. 260–268.

[7] M. Naor and B. Pinkas, "Visual authentication and identification," in *Proc. Advances in Cryptology*, 1997, vol. 1294, LNCS, pp. 322–336

[8] G. Ateniese, C. Blundo, A. De Santis, and D. R. Stinson, "Visual cryptography for general access structures, Information and computation129 (1996), 86-106

[9] William Stallings," Cryptography and Network Security"4Th Edition, Pearson Education India.

AUTHORS

ROHITH S received B.E. degree in Electronics and Communication engineering in 2006 and M.Tech degree in VLSI Design and Embedded systems in 2008 from Visvesvaraya Technological University, Karnataka. He is currently working as a Lecturer at Nagarjuna College of Engineering and Technology, Bangalore,Karnataka-562110. He has total teaching experience of 4years.His main area of interest includes Digital Watermarking, Steganography, Error Control Coding, Cryptography and VLSI Design.

VINAY G pursuing a Bachelor of Engineering degree at Nagarjuna College of Engineering and Technology, affiliated to Visvesvaraya Technological University, Karnataka. He is involved in hobby projects and also a team member of student satellite (STUDSAT-2) project under the guidance of ISRO. His main area of research includes Embedded Systems, Image Processing, Visual Cryptography.