A Novel Multiple Visual Secret Data Hiding Scheme

Sesha Pallavi Indrakanti [#] Avadhani P.S [*]

[#] *Department of Computer Applications, GVP Degree College (Autonomous),*
Visakhapatnam, Andhra Pradesh, INDIA

** Department of Computer Science and Systems Engineering, Andhra University College of Engineering (Autonomous),*
Visakhapatnam, Andhra Pradesh, INDIA

***Abstract* - Current advances in the technology are demanding novel secret sharing techniques. Splitting of textual information into shares is an age old process, wherein image encryption has gathered its own demand in the current technology. Visual cryptography is a technique which encrypts images into shares and has been proved to be different from traditional cryptographic techniques, as it involves less mathematical computations for decryption. Current research concentrates mostly on dividing a single secret into two or more shares. Stacking the shares on each other reveals the secret. This paper proposes a new approach of generating 4 shares out of 3 secrets. The concept of visual cryptography is used in generating the shares and in viewing the secret also. This sharing scheme can handle more images for encryption i.e. embed more information and is more secure than traditional visual cryptography.**

***Keywords*- Visual cryptography, encryption, decryption, shares.**

I. INTRODUCTION

With the expansion of internet, the eavesdropper may try to use the trapdoor entry to capture sensitive data. Security and Confidentiality of the data during transmission has become a challenging issue. Traditional cryptographic techniques are complex and expensive too. To reduce the computational complexity and increase confidentiality, Naor and Shamir [1] proposed a scheme called visual cryptography in 1994. Visual cryptography is a scheme which encrypts a secret image into two shares, which on stacking reveal the secret. Decryption is done without any complexity, and the secret can be identified with normal eyes. The first visual cryptography scheme is used for black-and-white images. This black and white image is processed to give 2 disordered images. These disordered images are called “shares” which may be regarded as the cipher text; some treat them as the key also. Eavesdroppers cannot decrypt the secret message from one share.

Visual cryptography has been extended from a basic (2, 2) scheme to (k, n) – threshold visual secret sharing scheme that divides secret image into n transparencies or shares and distribute among n users. The decryption requires at least k transparencies or more to stack. In 1998, Chen and Wu [2] proposed a new visual cryptography scheme which overcomes the drawbacks of the traditional visual cryptography that only two share images can be used to embed one confidential message. Lots of work [3],[4],[5],[7],[8],[9] is being carried out to encrypt more secret images and obtain least possible shares from them. For example, according to traditional cryptography, if 2 images are encrypted, 4 shares are expected. Same way the expected number shares from 3 secret images are 6.

II. PREVIOUS SCHEMES

In visual cryptography concept proposed by Noar and Shamir [1] that involves stacking of 2 shares to recover secret image involves the concept of expanding each pixel into 4 sub pixels. The expanded pixel can take any of the form, from the given six combinations in Fig. 1.

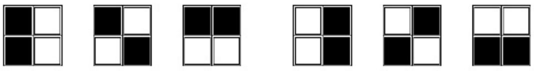

Fig.1 The six combinations

Each share consists of combination of white and black values .The Shares of the image are generated based on these 6 combinations and the color value in the pixel i.e white or black. The white pixel is represented as a combination two white and two black values; black pixel is represented as four black values. Chen and Wu [2] in 1998 proposed a new visual cryptography scheme that rotating the share image and stacking them to reveal two messages from two shares. The shares are generated based on the encoding process proposed by them. Latter in 2006 Fang and Wang [6] proposed an improved (3, 3)-visual secret sharing scheme, which can be used to embed three secret messages into three shares and improve security. This process involves a random generation of the first main share and the other two shares based on the first share.

III. THE PROPOSED SCHEME

In traditional visual secret sharing scheme, one secret can be made into two, three or four shares. This paper is an enhancement of the (3, 3) secret sharing scheme proposed by Fang and Wang [6]. The philosophy proposed by Fang and Wang is used but more processing is done to increase security and shares are further bifurcated. The proposed scheme includes 3 processing’s. Fig. 2 explains the encoding scheme. The first step is to create share A and share Temp which is same as the previous scheme. The second step is to further process share A into share A1 and share A2.Then finally the third processing involves the share Temp being encoded into share B and share C. This further splitting of shares involves more number of shares and users.

A. Initial Processing

The first processing involves the generation of share A and share temp from the 3 secret images. The share A is randomly generated. Each pixel in the secret image is expanded to 4 random blocks as shown in Fig. 2.

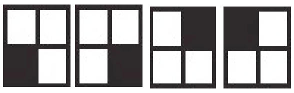

Fig.2 The four combinations

The process of generating share A and Share temp is illustrated in the algorithm below.

Step1: Consider 3 secret images S1, S2, S3 of the same size. Let the size of the secret images be n x n.

Step2: Let i,j represent the pixel coordinates of the 3 secret images. Compare pixel by pixel values of 3 secret images. S1(i,j) represents value of (i,j) pixel it can be either 0(white pixel) or 1(black pixel).

Step3: Select a random value in the range from 0 to 3. Based on these values Share A is generated.

```
Step4: (a) If random=0, with location (i, j) then
               Share A(2*i,2*j)=1
               Share A(2*i+1,2*j)=0
               Share A(2*i,2*j+1)=0
               Share A(2*i+1,2*j+1)=0
       (b) If random=1, with location(i, j) then
               Share A(2*i,2*j)=0
               Share A(2*i+1,2*j)=1
               Share A(2*i,2*j+1)=0
               Share A(2*i+1,2*j+1)=0
       (c) If random=2 , with location(i, j) then
               Share A(2*i,2*j)=0
               Share A(2*i+1,2*j)=0
               Share A(2*i+1,2*j+1)=1
               Share A(2*i,2*j+1)=0
       (d) If random=3 , with location(i,j) then
               Share A(2*i,2*j)=0
               Share A(2*i+1,2*j)=0
               Share A(2*i+1,2*j+1)=0
               Share A(2*i,2*j+1)=1
```

Step5: Share temp is generated based on the (i,j)th pixel location in each secret image and the random values.

Step6: Finally Share Temp and Share A will be of 2n x 2n of size. The pixel positions are defined as follows:

i,j	i+1 ,j
i,j+1	i+1,j+1

The share temp generation is based on the i,j pixel location in each secret image , the random value in the range of 0 to 3 and the generated share A. The sample generation is represented in the form of a matrix where o represents a white and 1 represents a black. The representation of share A and temp is given below:

(S1(i ,j),S2(i ,j),S3(i ,j)) → [A(2i,2j) ,A(2i+1,2j) , A(2i+1,2j+1), A(2i,2j+1), T(2i,2j), T(2i+1,2j), T(2i+1,2j+1), T(2i,2j+1)]

The combination of Share A and Share temp will depend on the random value from 0 to 3.

$$(0, 0, 0) \rightarrow \begin{vmatrix} R=0 \rightarrow 1\,0\,0\,0 & 0\,0\,1\,0 \\ R=1 \rightarrow 0\,1\,0\,0 & 0\,0\,0\,1 \\ R=2 \rightarrow 0\,0\,1\,0 & 1\,0\,0\,0 \\ R=3 \rightarrow 0\,0\,0\,1 & 0\,1\,0\,0 \end{vmatrix}$$

$$(0, 0, 1) \rightarrow \begin{vmatrix} 1\,0\,0\,0 & 1\,1\,0\,0 \\ 0\,1\,0\,0 & 0\,1\,1\,0 \\ 0\,0\,1\,0 & 0\,0\,1\,1 \\ 0\,0\,0\,1 & 1\,0\,0\,1 \end{vmatrix}$$

$$(0, 1, 0) \rightarrow \begin{vmatrix} 1\,0\,0\,0 & 1\,0\,0\,1 \\ 0\,1\,0\,0 & 0\,1\,1\,0 \\ 0\,0\,1\,0 & 0\,0\,1\,1 \\ 0\,0\,0\,1 & 1\,0\,0\,1 \end{vmatrix}$$

$$(1, 0, 0) \rightarrow \begin{vmatrix} 1\,0\,0\,0 & 0\,1\,0\,1 \\ 0\,1\,0\,0 & 1\,0\,1\,0 \\ 0\,0\,1\,0 & 0\,1\,0\,1 \\ 0\,0\,0\,1 & 1\,0\,1\,0 \end{vmatrix}$$

$$(1,1,1) \rightarrow \begin{vmatrix} 1\,0\,0\,0 & 1\,1\,0\,1 \\ 0\,1\,0\,0 & 1\,1\,1\,0 \\ 0\,0\,1\,0 & 0\,1\,1\,1 \\ 0\,0\,0\,1 & 1\,0\,1\,1 \end{vmatrix}$$

$$(0,1,1) \rightarrow \begin{vmatrix} 1\,0\,0\,0 & 1\,0\,1\,0 \\ 0\,1\,0\,0 & 0\,1\,0\,1 \\ 0\,0\,1\,0 & 1\,0\,1\,0 \\ 0\,0\,0\,1 & 0\,1\,0\,1 \end{vmatrix}$$

$$(1,0,1) \rightarrow \begin{vmatrix} 1\,0\,0\,0 & 0\,1\,1\,0 \\ 0\,1\,0\,0 & 0\,0\,1\,1 \\ 0\,0\,1\,0 & 1\,0\,0\,1 \\ 0\,0\,0\,1 & 1\,1\,0\,0 \end{vmatrix}$$

$$(1,1,0) \rightarrow \begin{vmatrix} 1\,0\,0\,0 & 0\,0\,1\,1 \\ 0\,1\,0\,0 & 1\,0\,0\,1 \\ 0\,0\,1\,0 & 1\,1\,0\,0 \\ 0\,0\,0\,1 & 0\,1\,1\,0 \end{vmatrix}$$

The matrix for generating share A and Share Temp are shown in above. For example, if the (i,j)th pixel of the three shares is white i.e (0,0,0) and if the random value is 0 then the share A is of the order(1 0 0 0) and share temp is of the order (0 0 1 0). So (0 0 0) has 4 combinations of share A and share Temp. This happens for eight different patterns and 4 combinations of each pattern resulting in 32 different combinations. The eight different patterns are (0 0 0), (0 0 1), (0 1 0), (1 0 0), (1 1 1), (0 1 1), (1 0 1), (1 1 0).

The advantage of using 4 different combinations (random numbers) in each pattern avoids the permutation of repeating the combination or pattern.

B. Generating Shares A1 & A2

The results of the initial processing are share A and share Temp. The share A is subjected to further processing and share A1 and share A2 are generated. The following are the steps for obtaining share A1 and share A2:

```
Step1: Let share A of size n x n.
Step2: If A(i ,j)=0 then
            A1(i ,j)=0 ,A2(n-i-1,j)=0      (or)
            A1(i ,j)=1 ,A2(n-i-1,j)=1
Step3: If A(i ,j)=1 then
            A1(i ,j)=0 ,A2(n-i-1,j)=1      (or)
            A1(i ,j)=1 ,A2(n-i-1,j)=0
```

According to the algorithm, suppose let share A be of n x n size, if the (i,j)th pixel of share A is white(0) then the (i,j)th pixel of A1 can be either white or black, so will be the (n-i-1,j)th pixel of A2. On the other hand if the (i,j)th pixel of share A is black(1), then the (i,j)th pixel of share A1 will be white and the (n-i-1,j)th pixel of share A2 will be black. This is how it works vice-versa for A(i,j)=1 and same if A(i,j) =0. This encoding process increases the security.

C. Generating Shares B & C

The result obtained from the initial processing is share A and share Temp. The share Temp is subjected to further processing to obtain share B and share C. The generation process of share A1, share A2, share B and share D is almost the same except the slight variation in the pixel location. If the value in share Temp is white(0), then (i,j)th pixel of share B and share C, will be either black or white. On the other hand if the (i,j)th pixel of share Temp is black(1), then the (i,j)th pixel of share B will be white and the (i,j)th pixel of share C will be black or vice-versa. This encoding process has been carefully planned to increase the security.

IV. DECRYPTION PROCESS

The Fig. 3. explains the decryption process in the proposed scheme. The recipients have to bring their valid share to view the secret. The decryption process is explained below.

```
Step1:  Share A1 and share A2 are processed and stacked
        to obtain share A.
Step 2: let share A1, A2 be of size n*m.
        Share A (i,j)= shareA1(i, j) ⊗
                           Share A2(n-i-1,j)
Step3:  Share Temp(i, j)=Share B(i, j) ⊗
                           Share C(i, j)
```

Share A is in turn stacked on share Temp to reveal secret1. Share A is rotated clock wise and anti clockwise and stacked on share Temp to reveal secret 2 and secret 3.

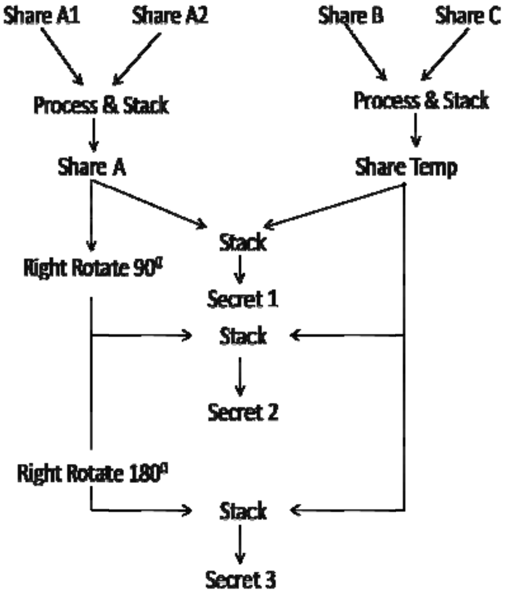

Fig. 3 The Decryption Process

The Decryption finally involves the process of processing the secret images obtained from stacking. This processing is required as the encrypted result is four times the size of the original secrets and they also have noise in them. Below are the steps in the final processing.

```
Step1:  Let recovered secret be RSecret and be o f
        Size 2n*2n. Processed result be PRSecret
        and be of size n*n size
Step2:  For i=0 to n-1 repeat steps 3 & 4
Step3:  Calculate the number of black pixels in
        recovered secret of positions(count) (2i,2j)
        (2i+1,2j) (2i,2j+1) (2i+1,2j+1)
Step4:  if count>2 then set processed pixel value as black
        i.e
              PRSecret(i,j) = black or 1
        Else
              PRSecret (i, j) = white or 0
```

V. EXPERIMENTAL RESULTS

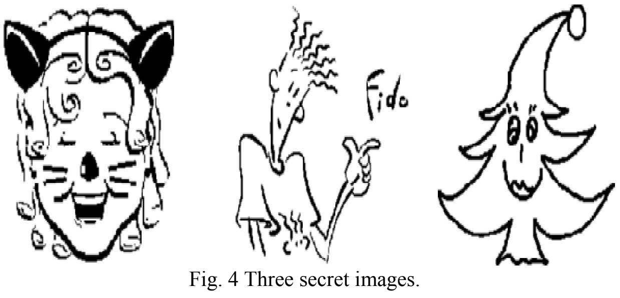

Fig. 4 Three secret images.

The 3 secret images shown in Fig. 4 are encrypted into 4 shares which are shown in Fig. 5.

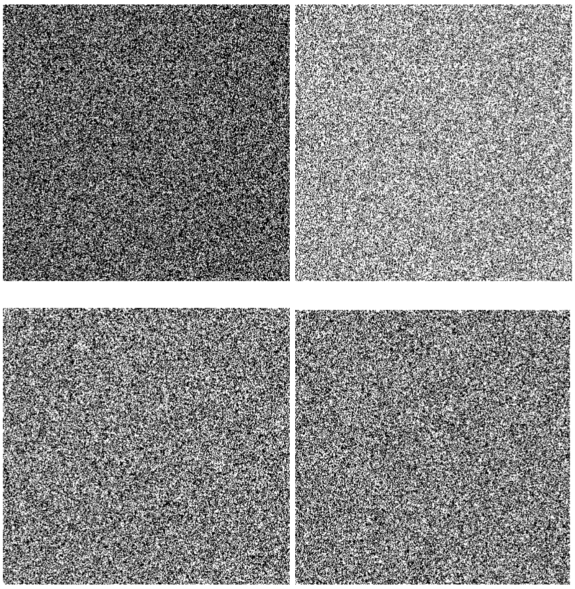

Fig. 5 Four shares after three coding process.

The receivers have to submit these disordered share images to obtain the right secret images. The share Temp and share A are shown in Fig. 6. These shares do not give any clue about the secret.

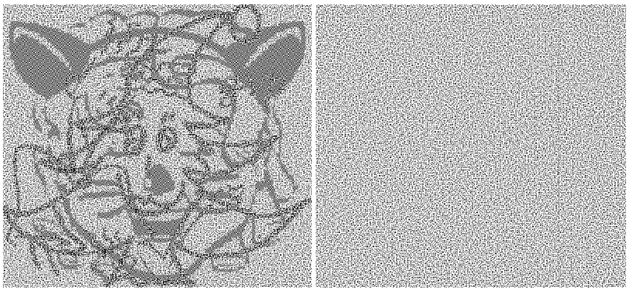

Fig. 6 Share Temp and Share A

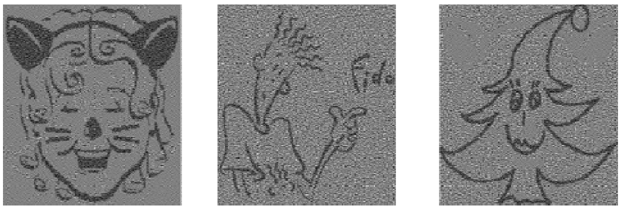

Fig. 7 3 Recovered Secrets.

The three secret intermediate images after decryption are shown in Fig. 7. These Recovered Secrets images are subjected to further processing to obtain the exact same original secret images. These processed results obtained are of the original size and clarity of the secret images.

VI. Conclusions

The original conventional (3, 3)-visual secret sharing scheme, is extended to (4, 4) secret sharing scheme. The clarity of the decrypted image has also been increased here. This work can be further extended to (n, n) secrets sharing and at the same time concentrated in decreasing the bandwidth requirement for (n, n) images transmission.

References

[1] Naor, M. and Shamir, A. 1994, *Visual cryptography*, Eurocrypt'94, Lecture Notes in Computer Science, vol. 950, pp. 1–12.

[2] L.H. Chen, and C.C. Wu, "A Study on Visual Cryptography", Master thesis, Institute of Computer and Information Science, National Chiao Tung University, Taiwan, R.O.C.,1998.

[3] Tzeng, W.G. and Hu, C.M. , "A New Approach for Visual Cryptography", *Designs, Codes and Cryptography*, vol. 27, No. 3, pp. 207–227, 2002

[4] Ming-Shi, Wang and Pei-Fang, Tsai, "The Implement of Visual Cryptography via Two Shares Embed Three Messages", *The 30th Digital Content, Digital Education, and Management Policy*, pp. 69-77, 2005. (in Chinese)

[5] Wu, H.C. and Chang, C.C., "Sharing visual multi-secrets using circle Shares", *Computer Standards & Interfaces*, Vol. 28, pp.123-135 2005.

[6] Pei-Fang Tsai, Ming-Shi Wang, "An (3, 3)-Visual Secret Sharing Scheme for Hiding Three Secret Data," in *Proceedings of JCIS'2006*

[7] Fang, W.P. and Lin, J.C.,"Visual Cryptography with Extra Ability of Hiding Confidential Data", *Journal of Electronic Imaging*, vol. 15, no.2, p. 023020, 2006

[8] I.S.Pallavi, P.S.Avadhani, "Secure Visual Secret Sharing Scheme", in *proceedings of 10th world conference on Integrated Design and Process Technology* held at Antalya, Turkey during 3rd –8th June, 2007

[9] Sesha Pallavi Indrakanti, Venkata Vinay Pragada, Avadhani P.S "Multiple Image Secret Sharing Scheme", in *proceedings of SEDE-2011*, Las Vegas, Nevada, USA during 20th–22nd June, 2011.