Rotation Visual Cryptography Using Basic (2, 2) Scheme

[1]B. Dinesh Reddy, [2]V. Valli Kumari, [3]KVSVN Raju, [4]Y.H. Prassanna Raju
[1]Vignan Institute of Information Technology, Andhra Pradesh
[2,3]Andhra University, Andhra Pradesh
[4]MVGR College of Engineering, Andhra Pradesh
[1]dinesh4net@gmail.com, [2]vallikumari@gmail.com, [3]kvsvn.raju @gmail.com, [4]prasan.aru @gmail.com

***Abstract*—Visual cryptography scheme is the concept of encrypting a secret image into n(more than one) shares. Rotation Visual Cryptography scheme (RVCS) allows four secret images to be encrypted into two shares. Using Human Visual System, again the four secret images can be easily recovered by placing the two shares on top of each other with different angles. In this paper proposes a Rotation Visual Cryptography using basic (2,2) scheme which encrypts three secret images into three shares and each secret image can be easily revealed by overlaying one share with the 1800 anticlockwise rotation of another share. In this way the combination of any of the two shares reveals one secret image with the help of 1800 anticlockwise rotation. The reconstructed original three secret images have the same contrast as achieved in the basic visual cryptography scheme (2, 2).**

Keywords- Visual Cryptography, Rotational cryptography, secret sharing algorithm

I. INTRODUCTION

Visual cryptography (VC) is the concept of dividing a secret image into 'n' shares and revealing secret image by stacking a qualified subset of 'n' shares. The scheme is perfectly secure and very easy to implement. Visual cryptography takes the input as one secret image and creates the shares (more than one encrypted images) by the process of encryption, later decryption is done by human visual system. Decryption is by done by printing each share on a separate transparency sheet and then placing them on each other. Visual cryptography scheme has many applications like secret sharing scheme, Copyright protection, Halftoning process and Watermarking. Visual cryptography scheme can also be used for authentication and identification process (visual authentication and identification) this scheme was first introduced by Naor and Shamir [1] in 1994. Ateniese, Blundo, Stinson [2] extended this concept as Visual Cryptography for General Access Structures in which only the qualified subsets of participants can recover the secret image, but other, forbidden, sets of participants can't gain information related to secret image. The basic visual cryptography is applied for black & white images only. However, with the invention of visual cryptography for color images [3], it has become feasible for color images. Then the halftone visual cryptography [4] came to into the picture to provide the better quality images when compared to any available cryptography methods.

Right from the basic model of visual cryptography, researchers have come up with many related studies. But most of these studies concentrated on sharing the single secret. Bin Yu, Xiaohui Xu, Liguo Fang [5] solved this problem by introducing a multi secret scheme in which the combination of different shares results in different secret images. Lina Ge, Shaohua Tang [6] gave the solution to share multi secrets based on circle properties. Later Weir, WeiQi Yan [7] introduced a new scheme to share multiple secrets with the help of generating master key.

Zhengxin Fu, Bin Yu [8] introduced a new concept of rotation to share multiple secrets with a method RVCS in which four secret images are encrypted into two shares and the decryption is done by combining two shares with different angles. In this paper proposes a Rotation Visual Cryptography using basic (2,2) scheme, which encrypts three secret images into three shares and each secret image is obtained by combining one share with the 180^0 anticlockwise rotation of another share. The scheme uses the basis matrices concept in basic (2, 2) scheme.

II. VISUAL CRYPTOGRAPHY

Visual Cryptography (VC) is a new technique of cryptographic scheme, which can decrypt encrypted images (shares) without any mathematical computations but with the help of human visual system. There are various schemes of visual cryptography. Each scheme uses different matrices to generate the shares [1]. The revealed secret image will lose contrast compared to original image

A. Various Schemes of VC

- (2,2)–Scheme: This scheme encrypts the secret image into two shares and obtains the secret image when two shares are superimposed.
- (2,n)–Scheme: This scheme encrypts the secret image into n shares and obtains the secret image when two or more of the shares are overlaid. Where 'n' represents the number of participants.
- (n,n)–Scheme: This scheme encrypts the secret image into n shares and obtains the secret image when all n of the shares are overlaid, but any n -1 of them will not produce any hint about the secret

image. The user has to give the value of n, the number of participants.

- (k,n)–Scheme: This scheme encrypts the secret image into n shares and decrypts the secret image when any group of k shares is overlaid, but any k -1 of them will not give any hint about the secret image. The user has to give the value of k, the threshold, and n, the number of participants.

B. Basic (2, 2) Scheme

Basic visual cryptography relies upon breaking of pixels into some sub pixels, in other words we can say expansion of pixels. Fig 1 shows the approach for basic (2, 2) –scheme.

Pixel	White		Black	
Probability	Way1 50%	Way2 50%	Way1 50%	Way2 50%
Share1				
Share2				
Share1+Share2				

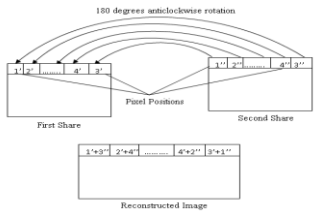
Fig. 1: Visual Cryptography (2, 2) Scheme [4]

In this scheme one white or black pixel is expanded into two sub pixels by randomly selecting one of the two ways with the 50% probability as shown in figure1. For black pixel, we get the result in the form of complete black when shares 1 and 2 are combined together, but for white pixel we get the result in the form of gray (it's partially white and black but seems to be like gray color) because 50% of the contrast is lost for white pixel in the encryption process.

III. PROPOSED SCHEME

This paper proposes a new scheme in Rotation Visual Cryptography called Rotation Visual Cryptography using basic (2, 2) scheme in which three secret images are encrypted into three shares using the basic (2, 2) visual cryptography scheme with the help of basis matrices concept.

A. Visual Cryptographic Decryption



Reconstructed Image = First Share (+) anticlockwise (Second Share $^{\pi}$)

Fig. 2: Visual Cryptographic Decryption

Each secret image could be obtained by superimposing one share with the 180^0 anticlockwise rotation of another share. Figure 2 shows the procedure for obtaining the secret images. Let us consider two shares with the pixel positions as shown in figure2. Each share consists of a number of rows depending upon the secret image. For the first row of two shares do the following process. The first pixel (1') in the first share is overlapped with the last pixel of second share (3") and the second pixel (2') in the first share is overlapped with the last but one pixel (4") of second share and so on. The same is repeated for the remaining rows of two shares. This process is called superimposition of one share with the 180 degrees anticlockwise rotation of another share. The resultant reconstructed image has the form as shown in above figure2. In the mathematical sense we can represent the decryption process as shown below:

- Share1(+)anticlockwise(Share2π) = SecretImage1
- Share2 (+) anticlockwise (Share3π) = SecretImage2
- Share3 (+) anticlockwise (Share1π) = SecretImage3

Consider a scenario where accessing a computer require high authentication (military). Let the scenario contain three people (A, B, C). To access the system we require two people (AB, AC, BC).Here this method will be the best for authentication. We use thee secret images each contain secret password. We use Rotation Visual Cryptography using basic (2, 2) scheme to generate three shares which are distributed to each person (A, B, C). Any two members together with their shares can get the secret password and access the system. This method can easily authenticate the two persons.

B. Visual Cryptographic Encryption (Shares Generation)

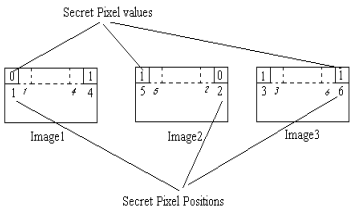


Fig. 3(a). Three Secret Images with Pixel Positions and Their Corresponding Values

In this proposed scheme we generate three shares from three secret images using basic (2, 2) scheme. The constraint is three secret images should be of same size with even column dimension.

0	0	1	1	1	1
1	2	3	4	5	6

6 Secret Pixels Unit

Fig. 3(b). 6 Secret Pixel Units Collected from the Three Secret Images

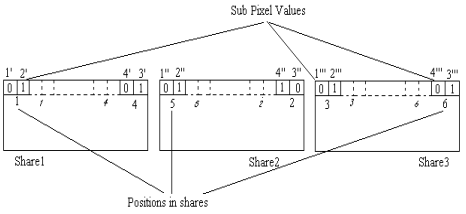


Fig. 3(c). Three Shares Containing the Sub Pixel Values Corresponding to 6 Secret Pixels

Figure 3(a) & figure 3(c) states that reconstruction of secret pixels depends on the positions in the shares. Secret pixel1 depends on the 1st and 2nd positions in share1 and share2 respectively. Similarly secret pixel2 depends on the 2nd and 3rd positions and secret pixel3 depends on the 3rd and 4th positions and secret pixel4 depends on the 4th and 5th positions and secret pixel5 depends on the 5th and 6th positions and secret pixel6 depends on the 6th and 1st positions.

1. Generation of Sub Pixel Values in Shares

Algorithm Encryption
Begin:
Input: Three noise added secret images I1, I2, I3.
Output: Three Shares
n:= row size of noise added secret image;
m:=column size of noise added secret image;
for i:= 0 to n do
for j:= 0 to m/2 do
x:= random();
x:=x%2;
if x:=0 then
S1(i,2j):=0; S1(i,2j+1):=1;
else
S1(i,2j):=1; S1(i,2j+1):=0;
End // If
S2(i,2m-2j):=(I1(i,j):=0)? S1(i,2j+1): S1(i,2j);
S2(i,2m-2j+1):=1-S2(i,2m-2j);
S3(i,2j):=(I2(i,m-j):=0)?S2(i,2m-2j+1): S2(i,2m- 2j);
S3(i,2j+1):=1-S3(i,2j);
S1(i,2m-2j):=(I3(i,j):=0)? S3(i,2j+1): S3(i,2j);
S1(i,2m-2j+1):=1-S1(i,2m-2j);
S2(i,2j):=(I1(i,m-j):=0)**?**S1(i,2m-2j+1): S1(i,2m-2j);
S2(i,2j+1):=1-S2(i,2j);
S3(i,2m-2j):=(I2(i,m-j):=0)**?**
S2(i,2m-2j+1): S2(i,2m-2j);
S3(i,2m-2j+1):=1-S3(i,2m-2j);
End j loop
End i loop
End Algorithm

C. Adding Noise to Three Secret Images

Three secret images are given as input to the *add noise* phase. Noise is added to three secret images based on the selection of 6 secret pixel units**.**

D. Selection of 6 secret pixel units

Two secret pixels are collected from each secret image to make 6 secret pixel units. Let us start from considering the first rows of three secret images. First and last secret pixels are considered from each secret image to make first 6 secret pixel units. Second and last but one secret pixels are considered from each secret image to make another 6 secret pixel unit and so on. It is shown in figure 3(a) & 3(b). The same is applied for the remaining rows of three secret images. The number of 6 secret pixel units generation depends on the size of secret image which has been taken as input.

E. Reason to add noise

If the selected 6 secret pixels contains odd number of black pixels (1's) then the proposed algorithm doesn't work. To avoid this problem some noise is to be added to three secret images in the form of converting one white pixel to black pixel to make the odd number of black pixels to even number of black pixels in the selected 6 pixels. Black pixels contain the actual (secret) information, so converting a white pixel to black pixel doesn't affect the secret information.

F. Addition noise to the image

For the proposed method, select each 6 secret pixel unit from three secret images and check whether it contains odd number of black pixels. If so, convert one white pixel to black pixel.

But the problem is which white pixel to be converted as black pixel with in the 6 secret pixel unit. One solution is: select the white pixel which has the maximum number of neighboring white pixels.

G. Structure of proposed scheme

We take the three input images as black & white images of same size with even column dimension. Proposed scheme structure

Phase 1: We use the section 3.3
Phase 2: We use the section 3.2
Phase 3: We use the section 3.1
is shown in below figure4.

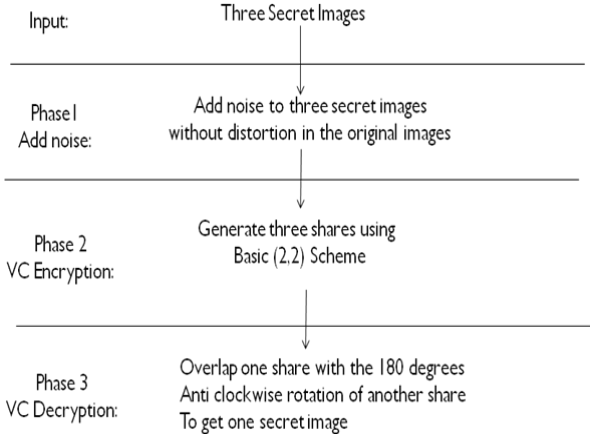


Fig. 4: Structure of Proposed Scheme

IV. EXPERIMENTAL RESULTS

Experimental results of proposed scheme are shown in the below figures. For experimental results MATLAB 7.0 tool is used. The three secret images are of size 240x100.

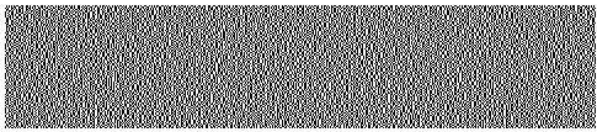
A. Input Images

Secret Image1 Secret Image2 Secret Image3

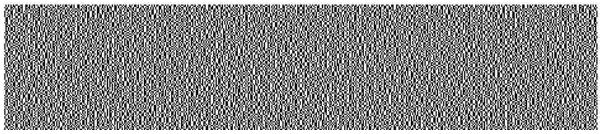
B. After Phase1

Secret Image1 Secret Image2 Secret Image3

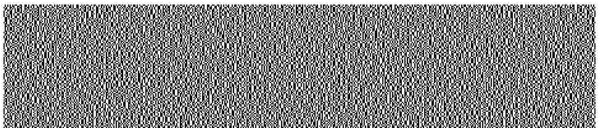
C. After Phase2



Share1

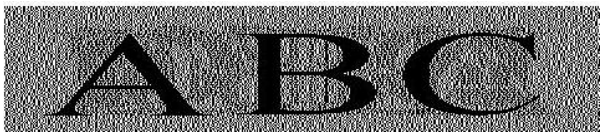


Share2

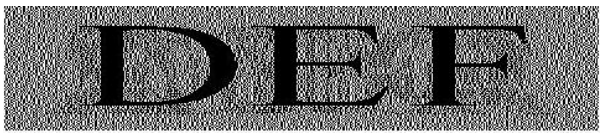


Share3

H. After Phase3



Share1 (+) anticlockwise (Share2$^{\pi}$) = Secret Image1



Share2 (+) anticlockwise (Share3$^{\pi}$) = Secret Image2

Share3 (+) anticlockwise (Share1$^{\pi}$) = Secret Image3

V. CONCLUSION

The proposed scheme Rotation Visual Cryptography using basic (2, 2) scheme is designed for encrypting three secret images into three shares using the basic (2, 2) visual cryptography scheme. The reconstruction of secret images could be done by stacking one share with the 180^0 anticlockwise rotation of another share. In this scheme we have used the concept of basis matrices for generating the sub pixel values. Reconstructed image contrast is same as in the (2, 2) scheme.

REFERENCES

[1] M. Naor and A. Shamir "Visual cryptography", Advances in cryptology EUROCRYPT '94. Lecture notes in Computer Science, (950):1–12, 1995.

[2] G. Ateniese, C. Blundo, A. de Santis, and D. Stinson. Visual Cryptography for general access structures. Information and Computation, 129(2):86–106, 1996.

[3] Y-C Hou, "Visual cryptography for color images", Pattern Recognition Society, 2003.

[4] Z. Zhou, G.R. Arce and G. Di Crescenzo "Halftone visual cryptography" 0-7803-7750-8/03, 2003 IEEE.

[5] B. Yu, X. Xu, L. Fang. Multi-secret Sharing Threshold Visual Cryptography Scheme. International Conference on Computational Intelligence and Security, 2007.

[6] L. Ge, S. Tang, Sharing Multi-secret Based on Circle Properties, 2008 International Conference on Computational Intelligence and Security.

[7] J. Weir, W-Q Yan, Sharing Multiple Secrets Using Visual Cryptography, 978-1-244-3828-0/09/, 2009 IEEE.

[8] Z. Fu, B. Yu, Research on Rotation Visual Cryptography Scheme, 2009, International Symposium on Information Engineering and ElectronicCommerce.