International Journal of Computer and Communication Technology

Volume 1 | Issue 3 Article 11

July 2010

Design and Implementation of a (2, 2) and a (2, 3) Visual Cryptographic Scheme

Ujjwal Chakraborty
Dept. of Computer Sc. & Engg., University of Kalyani, Kalyani, India, chakrababi@gmail.com

Jayanta l Kumar Pau
Dept. of Computer Sc. & Engg., Kalyani Govt. Engg. College, Kalyani, India,, jayantakumar18@yahoo.co.in

Priya Ranjan Sinha Mahapatra
Dept. of Computer Sc. & Engg., University of Kalyani, Kalyani, India,, priya_cskly@yahoo.co.in

Design and Implementation of a (2, 2) and a (2, 3) Visual Cryptographic Scheme

Ujjwal Chakraborty,
Dept. of Computer Sc. & Engg.,
University of Kalyani,
Kalyani, India,
E-mail:chakrababi@gmail.com

Jayanta Kumar Paul
Dept. of Computer Sc. & Engg.,
Kalyani Govt. Engg. College,
Kalyani, India,
Email:jayantakumar18@yahoo.co.in

Priya Ranjan Sinha Mahapatra,
Dept. of Computer Sc. & Engg.,
University of Kalyani,
Kalyani, India,
E-mail:priya_cskly@yahoo.co.in

***Abstract*— In this paper two methods for (2, 2) and (2, 3) visual cryptographic scheme(VCS) is proposed.**

The first scheme considers 4 pixels of input image at a time and generates 4 output pixels in each share. As 4 output pixels are generated from 4 input pixels dimension and aspect ratio of the decrypted image remain same during the process.

The second scheme considers 2 pixels (1 block) of input image at a time and generates 3 output pixels in each share. Here probability of $^1/_3$ for black pixel is maintained in each share. The scheme improves the contrast of output image. The dimension of revealed image is increased by 1.5 times in horizontal direction and remains same in vertical direction.

I. INTRODUCTION

Visual cryptography was introduced by M. Naor and A. Shamir in 1994[1]. Key feature of visual cryptography is that it does not need any computation at the decryption end. This cryptography can be applied[3] in key management, authorization, message concealment, authentication, identification etc**.**

In visual cryptographic scheme[1,8] an image is encrypted into n number of shares and at least k number of shares can reveal the actual image when properly stacked; but any (k - 1) shares can not reveal the original image[1,2]. This is referred as 'k out of n visual secret sharing problem'[1,6]. It is denoted as (k, n) visual cryptographic scheme(VCS). 'OR' of shares is the underlying operation. Some VCS use 'EX-OR'[2] also.

The main problems with every visual cryptographic schemes for binary image[7] are decreasing visual fidelity of output image and increasing size of generated shares.

The proposed visual cryptographic schemes have tried to overcome these shortcomings. The size of the shares is decreased. Visual fidelity and contrast[4] of the revealed image is improved.

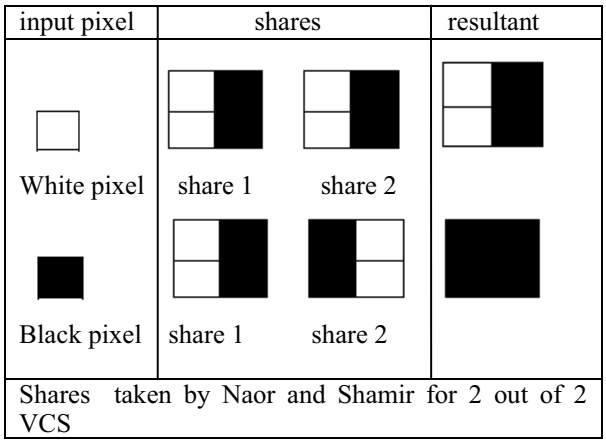
Proposed algorithms are on (2, 2) and (2, 3) visual cryptographic scheme. The 'OR' ed image[2,4] of the shares reveal the secret image successfully. We have also successfully implemented these two schemes in 'C' language.

Here the proposed schemes are described in section-3. Results of implementation are shown in section-4. Comparison of proposed visual cryptographic scheme and other schemes is shown in section 5. Possible future works are described in section 6.

II. RELATED WORKS

Actual idea was developed by M. Naor and A. Shamir[1] of Weizmann institute of Science. They suggested general k out of n visual cryptographic scheme[1].When shares are combined it gives OR of superimposed pixels. Gray level is proportional to hamming weight H(v)[1,2].

They designed 2 out of 2 scheme with 4 sub pixels. Here are some generated shares for their 2 out of 2 scheme-



Shares taken by Naor and Shamir for 2 out of 2 VCS

Figure 1: Shares used by Naor and Shamir in (2, 2) VCS

This scheme makes size of decrypted image four times of original. Visual fidelity is lost by 50%.

Tai-wen Yue and Suchen Chian introduced a scheme based on neural network approach[3]. They used the following type of shares[4]-

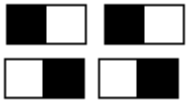
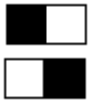
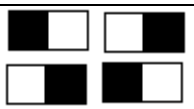
Input pixel	shares	resultant
		
		

Figure 2: Shares used by Tai-wen and Suchen Chian

The dimension of share becomes twice of original image in the horizontal direction and remains same in the vertical direction. As the probability of black pixel is ½ it gives same result as Naor and Shamir 2 out of 2 scheme with respect to contrast.

D. Jena and S. K. Jena proposed data hiding in halftone images using conjugate ordered dithering (DHCOD)[2]. They considered security of shares[2] in visual cryptography. Firstly, shares are generated using basic scheme. Then these shares are watermarked[2] with some cover image using DHCOD[2]. The decryption is made by human visual system.

Abhisek Parakh and Subhas Kak proposed a (2, 3) VCS based on recursive hiding scheme[5] where 3 output pixels are generated for one input pixel. So, size of shares becomes 3 times in horizontal direction.

All the above mentioned schemes increase the size of shares and loss visual fidelity.

III. THE SCHEMES

The first scheme is on (2, 2) secret sharing problem. In this scheme we have used the same matrices used by M.Naor and A. Shamir[1] in their (2, 2) secret sharing problem. The difference is in approach. We have considered 4 pixels of input image at a time and generated 4 output pixels for each shares using the matrices used by them. 5 cases may arise.

The picture below will help to understand the cases.

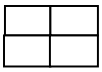
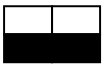
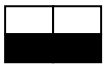
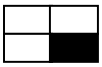
Original 4 pixels	Same 4 pixels in two shares	
	Share 1	Share 2
Case 1: Four original pixels are white 		
Case 2: Four original pixels are black 		
Case 3: Any two pixels are black & two pixels are white 		
Case 4: Any three pixels are white and rest is Black 		
Case 5: Any three pixels are black and rest is white 		

Figure 3: 5 cases and shares for all the cases.

Case1: Any same two pixels are made black in each share.

Csae2: Any two pixels are made black in one share and other two pixels in second share.

Case3: Any two pixels including one original black pixel are made black in first share. For second share the rest black pixel of original and the other white pixel of original which was blacken in first share are made black.

Case4: Any two pixels including the original black pixel are made black in first share. For second share the first share is repeated.

Case5: Any two of original black pixels are made black in one share. In second share the third black pixel of original and any other black pixel from original is made black.

The second scheme is more elegant than the first one. It is (2, 3) scheme. Here 3 pixels are generated for 2 pixels from the original image. There are four cases –

First: 2 pixels are white.

Second: 2 pixels are black.

Third: Left pixel is black and right is white.

Four: Left pixel is white and right pixel is black

Here are the four cases.

Case 1: 

Case 2: 

Case 3: 

Case 4: 

Probability of $^1/_3$ is maintained for black pixels in generated shares. So, one can not get any information about the original image from one generated share. The matrices below depict the fact. Here 1 denotes black & 0 denotes white.

Original matrices for two pixels(one Block)	Matrices for block of 3 pixels generated from original 2 pixels.	
$\begin{bmatrix}1 & 1\end{bmatrix}$	$\begin{pmatrix}1 & 0 & 0\\ 0 & 1 & 0\\ 0 & 0 & 1\end{pmatrix}$	You can take all the combination of matrices by permuting the columns. Choose each row for one share.
$\begin{bmatrix}0 & 0\end{bmatrix}$	$\begin{pmatrix}1 & 0 & 0\\ 1 & 0 & 0\\ 1 & 0 & 0\end{pmatrix}$	You can take all the combination of matrices by permuting the columns. Choose each row for one share.
$\begin{bmatrix}1 & 0\end{bmatrix}$	$\begin{pmatrix}1 & 0 & 0\\ 0 & 1 & 0\end{pmatrix}$	Right column should be intact. Other two can change place. Take any row for each share. The last will repeat any of the previous.
$\begin{bmatrix}0 & 1\end{bmatrix}$	$\begin{pmatrix}0 & 0 & 1\\ 0 & 1 & 0\end{pmatrix}$	Left column should be intact. Other two can change place. Take any row for each share. The last will repeat any of the previous.

Figure 4: Matrices for (2, 3) VCS

For first two arrays you can take all the combination of arrays by permuting the columns. Choose each row for one share.

For third array right column should be intact other two can change place .Take any row for any one share .The last will repeat any of the previous.

For fourth array left column should be intact other two can change place .Take any row for any share. The last will repeat any of the previous.

Below is the picture for explanation:

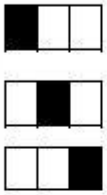
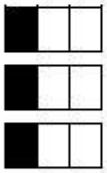
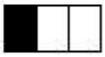
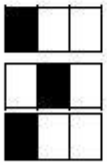
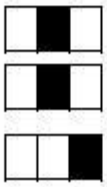
Original 2-pixel-block	Generated 3-Pixel blocks in three shares (One combination is shown, you can make others from the array above)	Share1+Share2+ Share3
		
		
		
		

Figure 5: Shares for all the cases of (2, 3) VCS

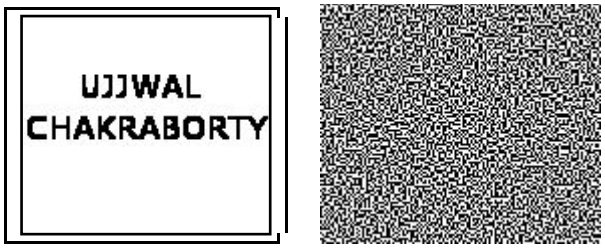
This scheme maintains in every share a probability of $^1/_3$ for black pixel and $^2/_3$ for white pixel. So only when we make OR of any 2 shares we can get an overview of original image.

As the probability of black pixel is decreasing to $^1/_3$ from $^1/_2$ the visual fidelity is improved. Also size is reduced. Naor and Shamir algorithm makes the share four times of original image, but this algorithm makes it only 1½ times of original. The only draw back is the aspect ratio of original image can not be maintained in this algorithm.

IV. RESULTS

The two above mentioned algorithm is implemented in 'C' language. The results are as per expectation.

Below is the results-



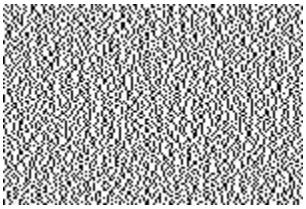
(a).Original Image (140×120) (b).Share 1 (140×120)

(c).Share 2 (140×120) (d).Decrypted Image(140×120)

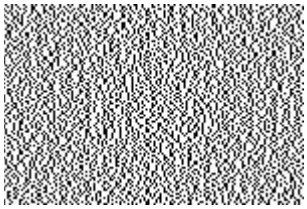
Figure 6(a-d): Result for (2, 2) VCS

Below is the result for(2, 3) VCS.

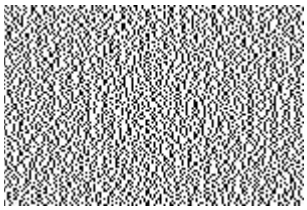
(a).Original Image (100×100)



(b).Share 1 (150×100)



(c).Share 2 (150×100)



(d).Share 3 (150×100)

(e).Share 1+ share 2(150×100)

(f).Share 2 + share 3(150×100)

(g).Share 1+share 3(150×100)

(h).Share 1+Share 2+Share 3(150×100)

Figure 7(a-h): Result for (2, 3) VCS

V. COMPARISON

The existing algorithms on visual cryptography increase size of the decrypted image and decrease the quality of visual fidelity. Proposed algorithms in this paper make improvements.

The first algorithm improves with respect to size and second one with respect to visual fidelity as well as size. The below chart depicts the fact:

	Original Image	Each share of Basic (2, 2) VCS	Each share of Naor and Shammir (2, 2) VCS	Each share of Proposed (2, 2) VCS	Each share of Proposed (2, 3) VCS
Number of pixel	100	200	400	100	150

Figure 8: Comparison of Algorithms showing data analysis.

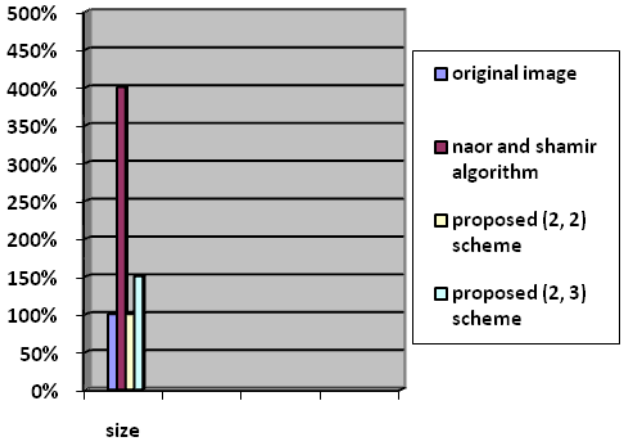


Figure 9: Comparison between algorithms with respect to size of revealed image.

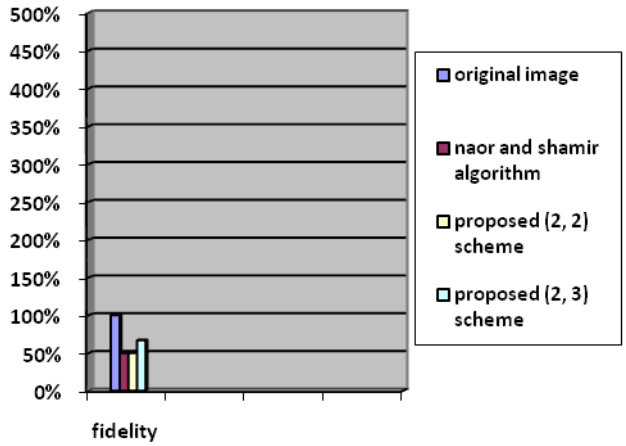


Figure 10: Comparison between algorithms with respect to visual fidelity of revealed image

VI. FUTURE WORK AND CONCLUSION:

The proposed (2, 2) scheme can be extended to (3, 4) scheme when probability of ¼ is maintained for black pixel in each block of every share.

The (2, 3) scheme can also be extended to (3, 6) scheme. For this we have to consider 4 pixels (i.e., 1 block) of original image at a time. Every share generates 6-pixel-block for that 4-pixel-block of original image. A probability of $^1/_6$ is maintained for black pixel in each block of every share.

As conclusion it can be said that the proposed (2, 2) VCS is undoubtedly fine for text image. Where the size is a concern this algorithm is fantastic to apply. The second scheme is sounder than the first one and it is applicable to any kind of binary image. From shown results it is clear that visual fidelity is much more improved in proposed (2, 3) scheme.

ACKNOWLEDGMENT

Authors thank Department of Computer Science, University of Kalyani for providing the resources to work in such a new and interesting field of cryptography.

REFERENCES

[1] M. Naor and A. Shamir, "Visual cryptography," . Advances in Cryptology EUROCRYPT '94. Lecture Notes in Computer Science,1995,(950):pp. 1-12.

[2] Debasish Jena and Sanjay Kumar Jena, "A Novel Visual Cryptographic Scheme," IEEE,2008, pp. 207–211.

[3] Tai- Wen Yue and Suchen Chiang, "A Neural Network Approach for Visual Cryptography". Proceedings of the IEE-INNS-ENNS International Joint Conference on Neural Networks(IJCNN'00) .pp. 1-2.

[4] Feng Liu,ChuanKun Wu and Xijun Lin, "A new definition of the contrast of visual cryptographic scheme," Information Processing Letters,2008.

[5] Abhisek Parakh and Subhas Kak, " A Recursive Threshold Visual Cryptography Scheme", Dept. of Computer Science, Oklahoma State University.

[6] Mizuho NAKAJIMA and Yasushi YAMAGUCHI, "EXTENDED VISUAL CRYPTOGRAPHY FOR NATURAL IMAGES," Dept. of Graphics and Computer Sciences,The University of Tokyo.

[7] Nagraj V. Dharwadkar , B. B. Ambedkar, Sushil Raj Joshi,"Visual cryptography for color Image using Color Error Diffusion," ICGST – GVIP Journal, ISSN :1687-398X, Volume10 ,Issue1,February 2010.