International Journal of Computer and Communication Technology

Volume 1 | Issue 4 Article 1

October 2010

A Simple Scheme for Visual Cryptography

Mihir Das
Dept. of Computer Sc. & Engg., University of Kalyani, Kalyani, India, das.mihir20@gmail.com

Jayanta I 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

A Simple Scheme for Visual Cryptography

Mihir Das[1], Jayanta Kumar Paul [2], Priya Ranjan Sinha Mahapatra [3],
Dept. of Computer Sc. & Engg.,
University of Kalyani,
Kalyani, India,
E-mail:das.mihir20@gmail.com [1] , E-mail:jayantakumar18@yahoo.co.in[2] , E-mail: priya_cskly@yahoo.co.in[3]

Abstract—**Here an algorithm is proposed to implement (2, 2) secret sharing problem which reduces the size (resolution) of the generated shares. Instead of considering one pixel at a time to generate the share, two consecutive pixels of the original image are considered row wise. Finally a pixel share having six pixels is generated for the considered two consecutive pixels. Thus we get six pixels instead of eight pixels in the shares corresponding to two pixels in the original image. As a result two pixels (8-6 = 2) in the share are reduced corresponding to two pixels of original image.**

Keywords-Secret share;pixel share;complement pixel share;

I. Introduction

Now a day the transmission of data through computer networks is increasing rapidly. So the security of the transmitted data becomes mandatory. Cryptography is the desired technique to provide security of the transmitted data. There are two processes in cryptography. Encryption is the first process in which the plain text or readable text is converted into cipher text or unreadable text. The second process is called decryption process in which the cipher text or unreadable text is converted to plain text or readable text. To encrypt data, we apply an encryption algorithm at the sender end and to reveal the data at the receiving end, we apply a decryption algorithm. So in cryptography we have to use an encryption as well as a decryption algorithm. But we need to consider the situation where there is no option to use the decryption algorithm during the decryption process. In Visual cryptography mainly visual information is encrypted using encryption algorithm but here there is no need of decryption algorithm to revel the visual information. Here the decryption process is done simply by human visual system. During the encryption process we simply add some noise in the original image to hide the original information and during the decryption process we reduce the noise to unhide the original information.

In the proposed scheme, we implement the (2, 2) sharing problem i.e. two shares are generated from the original image. Aspect ratio of the produced image shares is broken. But the size of the shares is reduced compare to the other implementation of the (2, 2) secret sharing problem. Thus size of the generated shares is taken as parameter of the encryption.

Suppose we have an original image of resolution 150×100 i.e. aspect ratio =height: width=3:2, then the resolution of each of the produced image share is 300×150 i.e. aspect ratio=2:1 thus we get shares of resolution 300×150 instead of 300×300 which is the size of the other implementation of the (2,2) secret sharing problem.

Here the proposed scheme is described in section- 4. Results of the proposed scheme are given in section- 5. Comparison of the proposed scheme with other algorithms is done in section- 6.

II. Some Basic Definitions

Let us first understand some definition of visual cryptography.

Secret Share:-

In visual cryptography the visual information (image) that is to be encrypted, is broken into number of images which are collection of black and white pixels. Each of the images is called secret share. It is impossible to get any of information about the original image from this secret share individually.

Here each pixel of original image corresponds to some fixed number of pixels in each share. That fixed number of pixels is called pixel share.

(k, n) secret sharing problem:-

In this problem, n secret shares from the original image are generated but if k of the shares are stacked properly, the original information of the image can be revealed. We cannot get any information about the original image from k-1 shares. Here both k and n are positive integer.

(n, n) secret sharing problem:-

In this problem, n secret shares are generated from the original image and all of n shares are required to decrypt the hidden information. We cannot get any information about the original image from any n-1 shares. Here also n must be positive integer.

(2, 2) Secret Sharing problem:-

Here we generate 2 secret shares from the original image and it is impossible to reveal any information about the encrypted image from any one of the shares. After stacking properly, the two shares produce the information of the encrypted image.

III. Related Works

Shami and Naor have given the algorithm to implement the (2, 2) secret sharing scheme [1].In their scheme four pixels are generated from a single pixel of the original image. Among the four pixels two pixels are white and two pixels are black. Since we have to make 2 pixels black out of 4 pixels so there are 4C2=6 pixel shares. During the encryption process each pixel of the original image is scanned separately. If the scanned pixel is black then we choose one of the six pixel shares as shown in fig- 1.Then we put the selected pixel share in one of the share to be generated and simultaneously put the complement pixel share of the selected pixel share in the other share. Again if the scanned pixel is white then one pixel share from the six pixel shares of the fig-1 is selected and put the selected pixel share in both the shares.

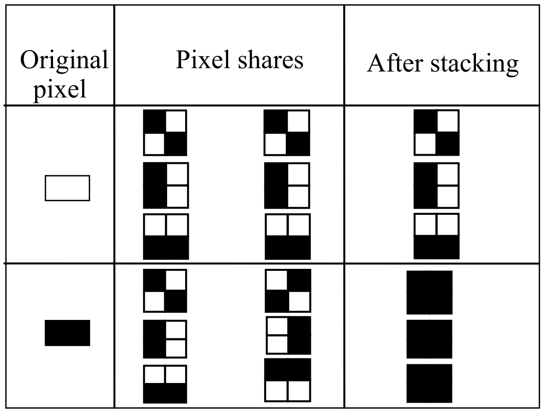


Figure 1. Original pixels and their pixel shares.

Debasish Jena and Sanjay Kumar Jena introduced DHCOD algorithm to hide image data [2]. In their proposed scheme, there are two phases of encryption. In the first phase original image is split into two shares. Then in the second phase watermarked shares are generated using DHCOD algorithm. In this phase a cover image is used.

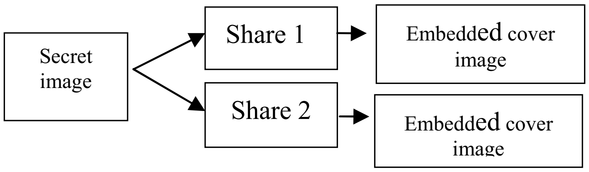


Figure 2. Structure of scheme proposed by Jena and Jena [2].

Tai-Wen and Suchen Chiang have used Neural Network to implement visual cryptography [3]. All the above mentioned algorithms work only for binary images. Algorithms on visual cryptography are also proposed for gray scale image[5,10] and color images[6,8,9].

IV. The Scheme

In this scheme we consider two consecutive pixel rows wise instead of considering a single pixel in the original image. During share generation, since we are considering two consecutive pixels row wise, the following four cases arise.

Case 1:- Both the pixels are black.
Case 2:- Both the pixels are white
Case 3:-First pixel is black and second pixel is white.
Case 4:- First pixel white and second pixel black.
Now let us consider the following pixel shares

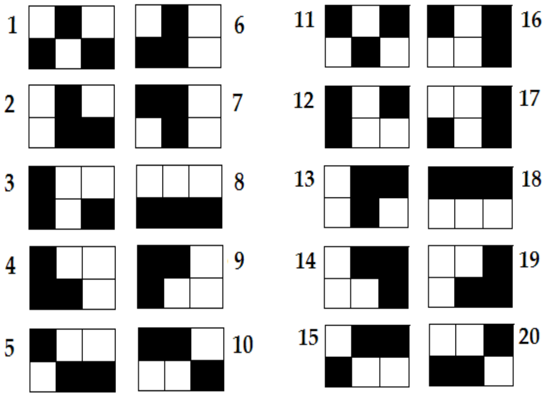


Figure 3. Pixel shares of two black or white pixels.

Above we have 20 pixels shares which will be used to generate the two shares .Now above mentioned four cases are discussed.

Case 1:-

In this case both the pixels are black. We choose randomly one of the 20 pixel shares and place it in the first image share and simultaneously we put the complement of the chosen pixel share in the other image share so that when these two image shares are stacked properly, the area generated by the pixel shares becomes black. In the above shown pixel shares 1 and are complement to each other as if we stack them properly they produce a complete 2×3 black pixel area. Similarly 2 and 12, 3 and 13, 4 and 14, 5 and 15, 6 and 16, 7 and 17, 8 and 18, 9 and 19, 10 and 20 are complement to each other.

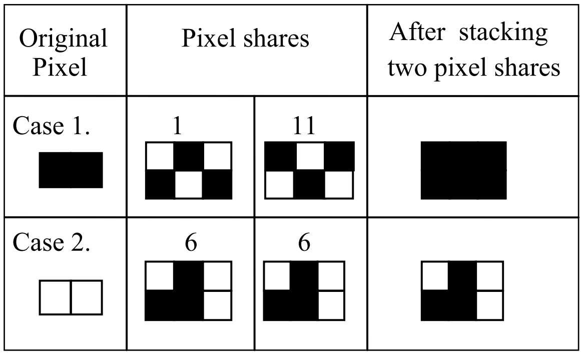


Figure 4. Selected pixel shares from 20 pixel shares shown in fig-2.

Case 2:-

In this case both the pixels are white. So we choose randomly one of the pixel shares among the 20 pixel shares. Then the selected pixel share is put in both the share. Now when we stack the image share, the area generated by this two pixel shares becomes gray (not black) or semi white.

Case 3:-

In this case first pixel is black and the second pixel is white. Here we construct the 2×3 matrix as follows…

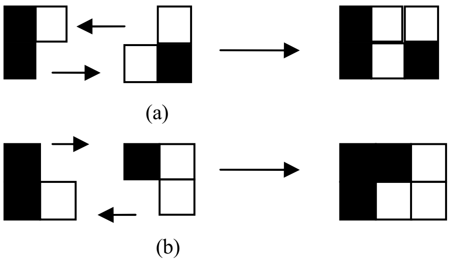


Figure 5. (a) Process 1 of breaking 2×3 matrix.
(b) Process 2 of breaking 2×3 matrix.

Now we have the following pixel shares for each pixel.

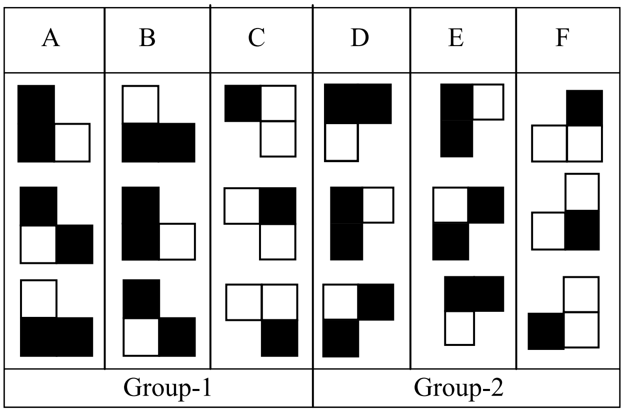


Figure 6. Various pixel shares related to case- 3.

In this case we choose one of the groups between Group-1 and Group-2. Suppose we have chosen Group-2. Now we choose one of the pixel share among F .Now we choose one pixel share from D and corresponding pixel share from E. If we choose first pixel share of D then we have to choose first pixel share of E. Now we put the selected pixel share from F in both the share .The selected pixel share from D is put in the first share and corresponding selected pixel share from E is put in the second share.

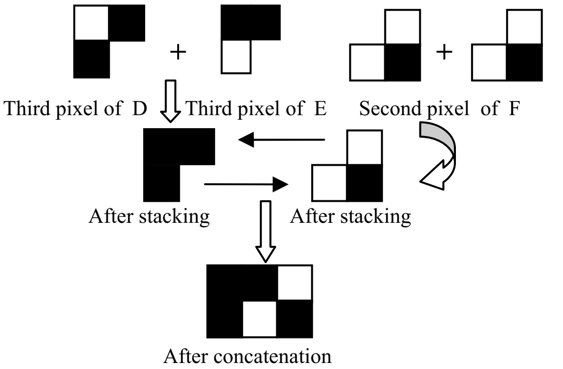


Figure 7. Structure of pixel share related to case-3.

Case 4:-

In this case first pixel is white and the second pixel is black. Here also we construct the 2×3 matrix as follows...

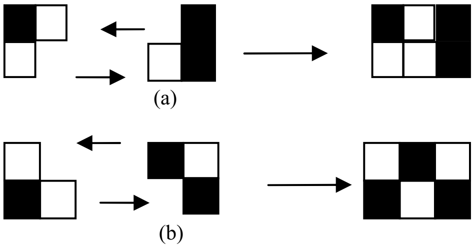


Figure 8. (a) Process 1 of breaking 2×3 matrix.
(b) Process 2 of breaking 2×3 matrix.

Now we have the following pixel shares for each pixel.

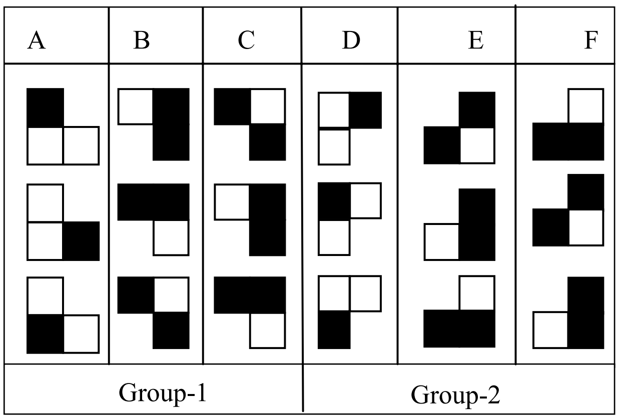


Figure 9. Various pixel shares related to case- 4.

Now again we choose one of the groups between Group-1 and Group-2. Suppose we have chosen Group-1. Now we choose one of the pixel shares among A .Now we choose one pixel share from B and corresponding pixel share from C is selected .If we choose first pixel share of B then we have to choose first pixel share of C. Now we put the selected pixel share from A in both the share and selected pixel share from B is put in the first share and corresponding selected pixel share from C is put in the second share.

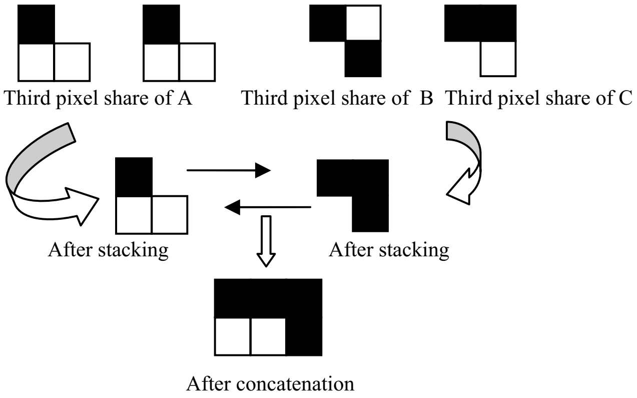
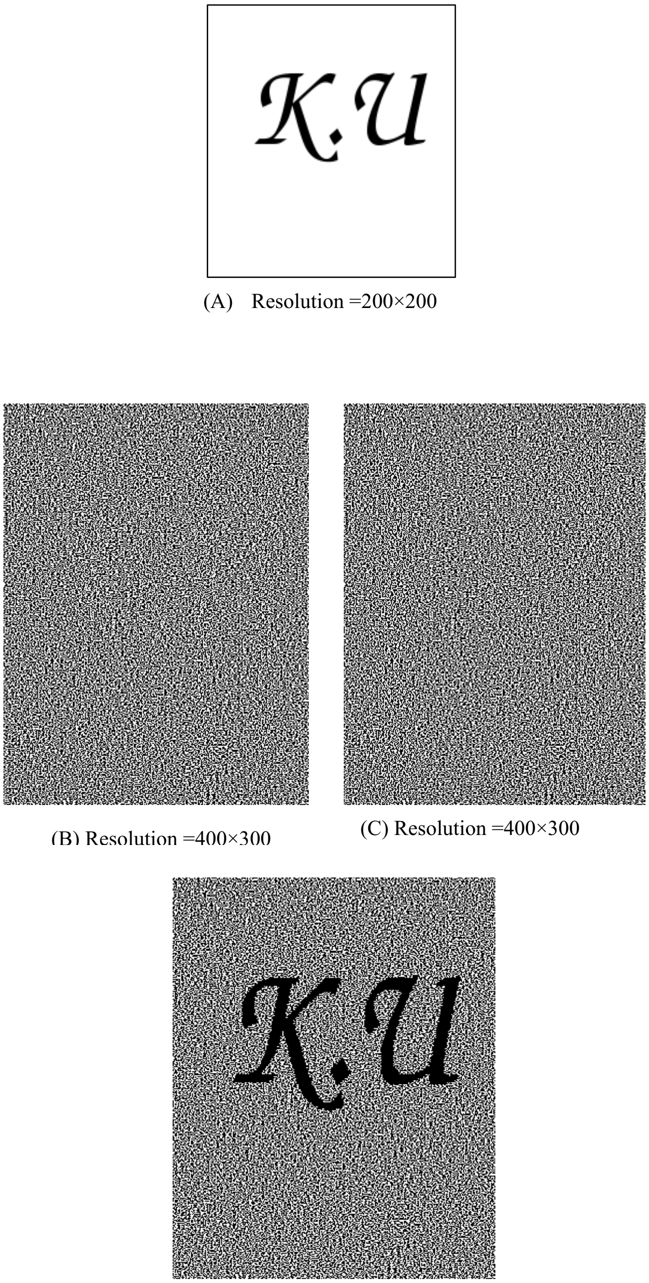


Figure 10. Structure of pixel share related to case-4.

V. Results

The implementation of the algorithm is done by using c language taking a binary image of resolution 200×200 and we get the result as desired, i.e. we get two shares of resolution 400×300 each. And the two shares are nothing but constituting an image of black and white dotted pattern. When the generated shares are stacked properly then the original information which was encrypted is revealed.



(A) Resolution =200×200

(B) Resolution =400×300

(C) Resolution =400×300

(D) Resolution=400×300

Figure 11. (A)Original image
(B)Share 1
(C)Share 2
(D)Stacking of share 1and share 2.

VI. Comparison

The algorithm which was proposed by Shamir and Naor to implement (2, 2) secret sharing problem raises the size (resolution) of the generated shares. But in the above algorithm size (resolution) of the generated shares is reduced. In case of Shamir and Naor implementation of (2,2) secret sharing problem the size(resolution) of the share is increased twice of the original image in both horizontal and vertical direction but in case of above described algorithm the size of the image share is increased twice in vertical direction but increased 1.5 multiple in horizontal direction. Also visual fidelity is enhanced in the described algorithm.

In the table given below shows the improvement of size of the share in our proposed scheme.

Table 1. Comparison between Shami and Naor scheme and our scheme.

Schemes	Total no of Pixel(s)		
	Original	Share	Increase(%)
Shami Naor	1	4	400
Tai-Wen and Suchen Chiang	1	2	200
Jena and Jena	1	2 or 4	200 or 400
Proposed scheme	1		300

The chart given below compares the proposed scheme to the other eschemes with respect to the increase(%) of the original image.

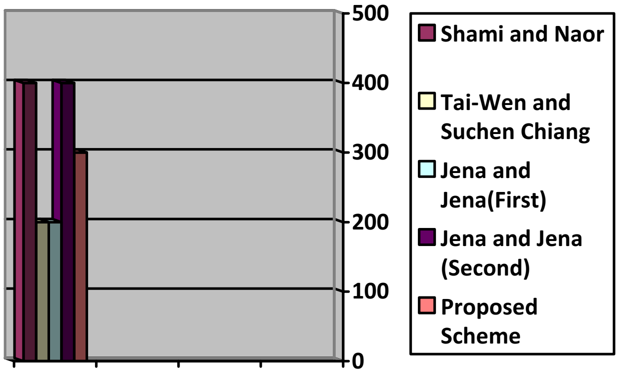


Figure 12. Bar chart showing comparison of proposed scheme with others scheme.

VII. Conclusion and Future works

The proposed scheme mainly reduces the number of pixels in the generated shares. But the aspect ratio of the shares is broken. In future works we would like to maintain the aspect ratio of the generated shares.

Acknowledgment

The authors are grateful to the Department of Computer Science, University of Kalyani for providing the resources to wok in such an interesting field.

References

[1] M.Naor and A. Shamir “Visual cryptography”. Advances in Cryptology EUROCRYPT ’94. Lecture Notes in Computer Science, (950):1–12, 1995.

[2] Debasish Jena, Sanjay Kumar Jena “A Novel Visual Cryptography Scheme”,2008.

[3] Tai-Wen Yueand and Suchen Chiang “A Neural Network Approach for Visual Cryptography”, IJCNN'00,2000.

[4] Data Communications and Networking-Behrouz A.Forouzan fourth edition.

[5] Mizuho Nakajima and Yasushi Yamaguchi “Extended Visual Cryptography for Natural Images”.

[6] Nagaraj V . Dharwadkar, B . B . Amberker , Sushil Raj Joshi “Visual Cryptography for Color Image using Color Error Difusion” ICGST GVIP Journal ISSN:1687-398X,Volume 10,Issue 1,February 2010.

[7] Feng Liu, ChuanKun Wu,XiJun Lin, “A new definition of the contrast of visual cryptography scheme”, Information Processing Letters(2010),doi:10.1016/j.ipl.2010.01.003.

[8] Hao Luo, Faxin Yu, Jeng-Shyang Pan and Zhe-Ming Lu “Robust and Progressive Color Image Visual Secret Sharing Cooperated with Data Hiding”, 8th International Conference on Intelligent Systems Design and Applications, Vol. 3, pp. 431-436.

[9] Young-Chang Hou “Visual cryptography for color images”, Pattern Recognition,Volume:36,Issue: 7, July, 2003, pp. 1619-1629.

[10] Carlo Blundo, Alfredo De Santis, and Moni Naor, “Visual cryptography for grey level images” Volume 75,Issue 630 November 2000, Pages 255-259.