A (2, N) VISUAL CRYPTOGRAPHIC TECHNIQUE FOR BANKING APPLICATIONS

Jayanta Kumar Pal[1], J. K. Mandal[2] and Kousik Dasgupta[3]

[1]Department of Computer Science and Engineering, Kalyani Government Engineering College, Kalyani-741235, West Bengal, India
jkp_it08@yahoo.com
[2] Department of Computer Science and Engineering, University of Kalyani, Kalyani-741235, West Bengal, India
jkm.cse@gmail.com
[3] Department of Computer Science and Engineering, Kalyani Government Engineering College, Kalyani-741235, West Bengal, India
kousik.dasgupta@gmail.com

ABSTRACT

In this paper a novel (2, n) visual cryptographic scheme has been proposed which may be useful in banking operations in the "either or survivor" mode where n is the number of generated shares, from which n-1 is the number of account holders in an account and one share should be kept to the bank authority. In this technique one account holder should stack his/her share with the share of the bank authority and the secret image for user authentication will be revealed. In this technique two consecutive pixels are taken as the one time input for the share generation process. This technique generates shares with less space overhead compared to existing techniques and may provide better security. It is also easy to implement like other techniques of visual cryptography.

KEYWORDS

(2, n) Visual cryptography, Share

1. INTRODUCTION

Visual cryptography is a new type of cryptographic technique in which no cryptographic computation is needed at the decryption end. In this technique text or picture should be fed as a digital image in the system as the input and the system generates 'n' ($2 \leq n$) numbers of different images (called shares), look like images of random noise. Among 'n' number of shares user has to stack 'k' number of shares, where $2 \leq k \leq n$, to reveal the secret image.

The remaining portion of this paper has been organized as follows. Section 2 gives some basic definitions of visual cryptography. Section 3 presents a brief overview of the related works. Section 4 describes the proposed technique. An example of the share generation process of the proposed technique is presented in the Section 5. Analysis of the performance of the proposed technique is presented in the Section 6. Section 7 draws the conclusions of the work.

2. SOME BASIC DEFINITIONS

2.1. (n, n) visual cryptography

In this type of visual cryptographic scheme, the system generates n ($n \geq 2$) number of shares and all shares are needed to be stacked together to get back the secret information.

DOI : 10.5121/ijnsa.2010.2410

2.2. (k, n) visual cryptography

In this type of visual cryptographic scheme, the system generates n ($n \geq 2$) number of shares and at least any k ($2 \leq k \leq n$) shares are needed to regenerate the secret information.

3. RELATED WORKS

The Visual Cryptography was first introduced by Moni Naor and Adi Shamir [1] in 1994. According to their algorithm, (2, n) visual cryptography can be solved by the following m×n matrices.

C_0 = {all the matrices obtained by permuting the columns of $\begin{bmatrix} 1\,0\,0\ldots\,0 \\ 1\,0\,0\ldots\,0 \\ \ldots \\ 1\,0\,0\ldots\,0 \end{bmatrix}$ }

C_1 = {all the matrices obtained by permuting the columns of $\begin{bmatrix} 1\,0\,0\ldots\,0 \\ 0\,1\,0\ldots\,0 \\ \ldots \\ 0\,0\,0\ldots\,1 \end{bmatrix}$ }

Here matrix C_0 refers the matrix for constructing pixels for the white pixels and C_1 for the black one.

In year 2000 a neural network based approach for visual cryptography has been proposed by Tai-Wen Yue and Suchen Chiang [2]. In this technique combination of two b/w pixels are generated with two different options for each pixel with equal probability.

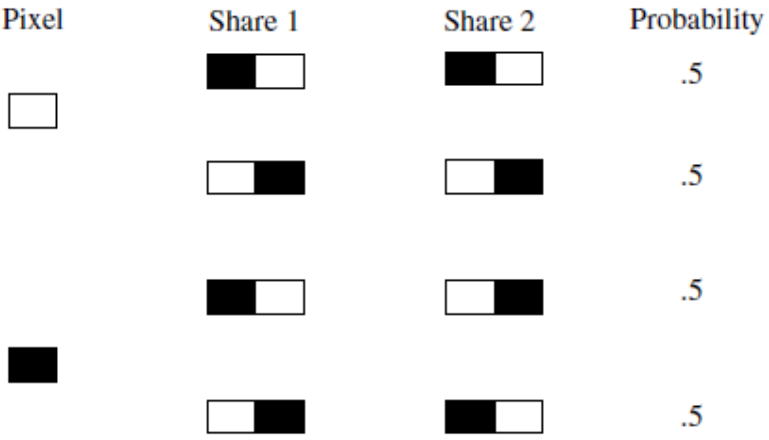

Figure 2. Share generation by Tai-Wen Yue and Suchen Chiang [2]

Jena and Jena [3] devised a technique for (2, 2) visual cryptography in 2008 where a single pixel generates either two pixels or four pixels in each share.

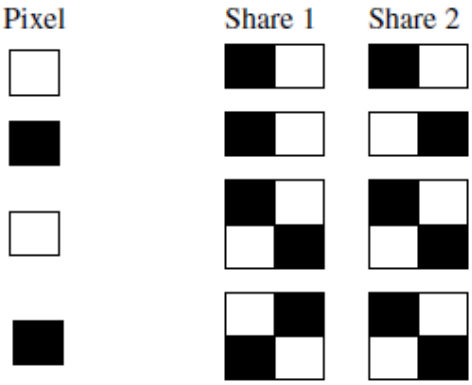

Figure 3. Share generation technique by the proposed algorithm by Jena and Jena [3]

In 2008 an algorithm for visual cryptography has been developed by Chetana Hegde, Manu S, P Deepa Shenoy, Venugopal K R, and L. M. Patnaik for Banking Applications [4]. The aim of the algorithm was to design an efficient technique for checking authenticity of the customer in core-banking and internet banking applications. The black pixel, denoted by 1, is an information pixel and the white pixel, denoted by 0 represents background. The initial Boolean matrices for white pixel, S_0 and for black pixel, S_1 for two shares in (2, 2) scheme is given below.

$$S_0 = \begin{bmatrix} 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 \end{bmatrix}$$

$$S_1 = \begin{bmatrix} 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \end{bmatrix}$$

In 2008 Avishek Adhikari and Bimal Roy have proposed On some Constructions of Monochrome Visual Cryptographic Schemes [5], which is a (2, n) visual cryptographic scheme.

In 2010 Jayanta Kumar Pal, J. K. Mandal and Kousik Dasgupta developed a (2, 2) Visual cryptography where two consecutive pixels had taken at a time as the one time input. The pixel generation technique by this process is given in the Figure 4.

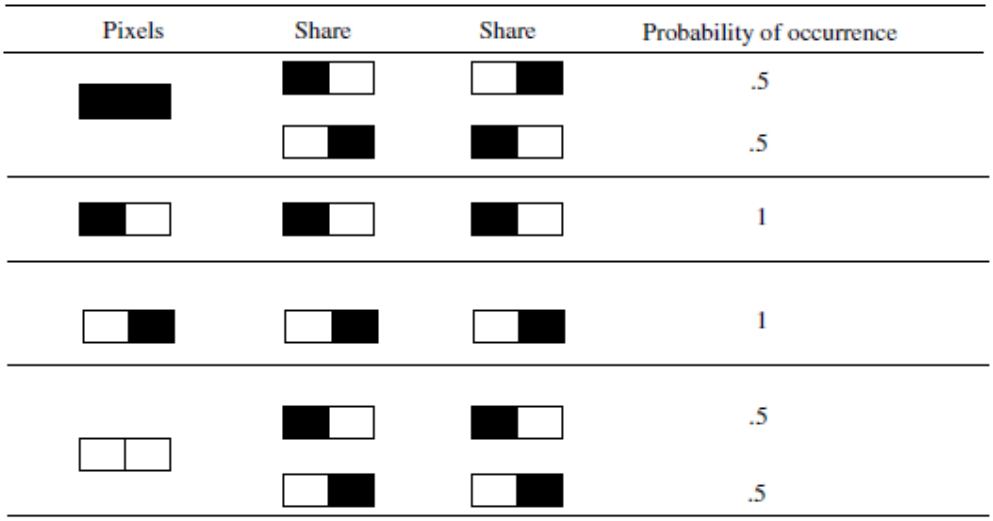

Figure 4. Share generation by Jayanta Kumar Pal, J. K. Mandal, and Kousik Dasgupta [6]

Various other algorithms [7, 8, 9, 10] are available for different visual cryptographic schemes, where efforts have been made to enhance the security. From the literature it can also be traced that efforts has also been made to increase the ease of use of the visual cryptography. For example Wei-Qi [11] developed a scheme for proper alignment of the shares.

In this paper a new visual cryptographic technique has been proposed, which may be useful in secure banking applications, where computer is not available. In case of previously proposed algorithm by Chetana Hegde et. al. [4], only one user can join in the banking process against an account, but the proposed algorithm is applicable for the accounts of joint account holders as well.

4. THE TECHNIQUE

Proposed technique considered two consecutive pixels as the one time input in the source image and as a result there shall be four cases in input. These are as follows:

(i) Black and Black, (ii) Black and White, (iii) White and Black, (iv) White and White

To develop a (2, n) visual cryptographic scheme two things are considered as major point of references[12]. These are:

(i) Hamming weight of every block in each share should be the same.

(ii) Hamming weight of a black block will be greater than the other blocks in the stacked shares.

Let N is the number of participants (i.e no. of account holders). m=integer part of (n/2), where n= number of total shares. The bank authority has to select the value of n, such that the relation ${}^{n}C_{m} \geq \min\{(N+1)\}$ (where C represents the combination operation) holds.

Hamming weight of each block of each share (H) = Integer part of $({}^{n}C_{m})/2$;

Now Let us consider the four possible cases of input pixels:

(i) Black and Black: In this case arrangement of black pixels in the output block will be different from other blocks. This ensures that after stacking the shares, Hamming weight of the stacked black blocks will become greater than the other blocks.

(ii) Black and White: Here the all the black pixels will be kept together from the first position of the output block.

(iii) White and Black: Where the all the black pixels will be kept together from the last position of the output block

(iv) White and White: All black pixels will be kept together in the output block

Now if the number of pixels in the input image is odd then the last pixel will be kept as it is in the shares.

5. ILLUSTRATIVE EXAMPLES

Let us take an illustrative example of the proposed algorithm for better understanding. Suppose two users want to open the account jointly thus the number of shares to be generated is three, (i.e. two for two users and one for bank authority)

So, here (N+1) =3. Now consider n=2. Therefore m= integer part of (2/2) =1.

Now, ${}^{2}C_{1}=2<(N+1)$. So, value of n should be greater than 2. If n=3 then, m= integer part of (3/2) =1 and ${}^{3}C_{1}=3=(N+1)$. So, this value of n is acceptable and the scheme will be a (2, 3) visual cryptographic scheme.

So, the Hamming weight of each block of each share will be the integer part of (3/2), i.e. 1.

Again, let three users want to open the account jointly. Therefore the number of shares should be generated is four, (i.e. three for three users and one for bank authority).

So, here (N+1) =4. Now consider n =3. Therefore m= integer part of (3/2) =1.

Now, ${}^{3}C_{1}=3<(N+1)$. So, value of n should be greater than 3.

If n=4 then, m= integer part of (4/2) =2 and ${}^{4}C_{2}=6>(N+1)$. So, this value of n is acceptable and the scheme will be a (2, 6) visual cryptographic scheme.

So, the Hamming weight of each block of each share will be the integer part of (6/2), i.e. 3.

From the above data we can generate the shares for the banking purpose.

The share generation in the case of two joint account holder is given in the Figure. 5

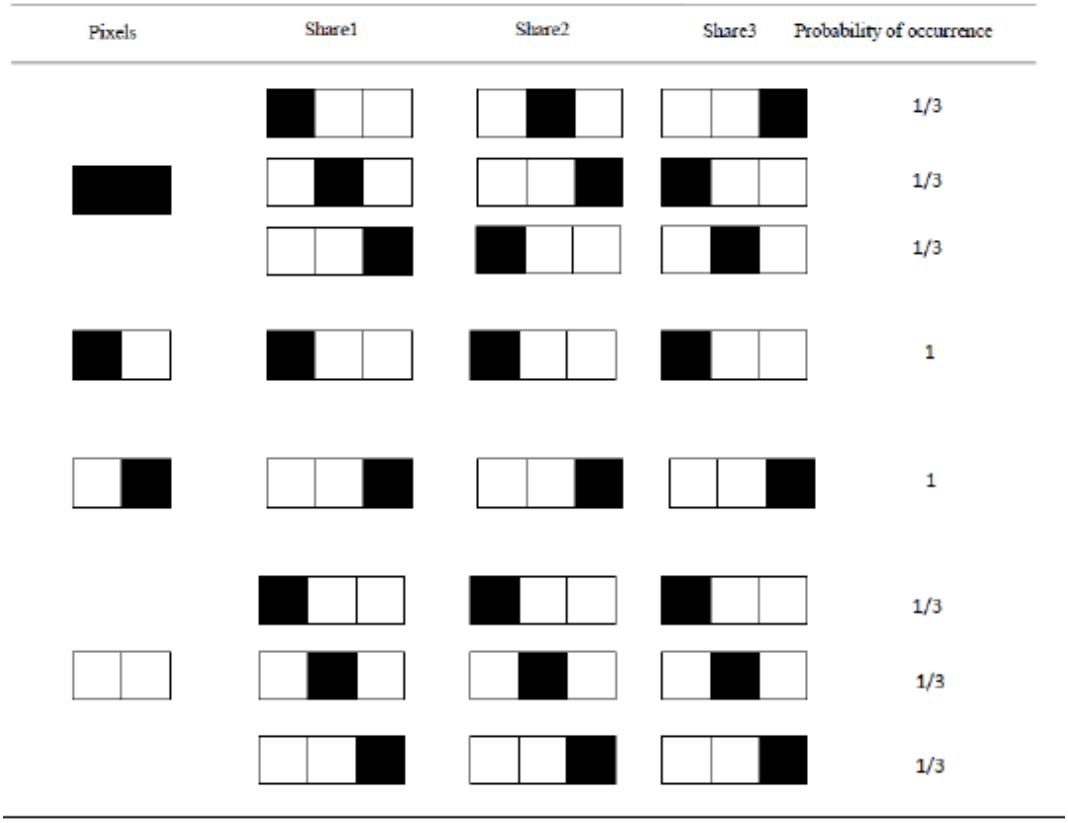

Figure 5. Share generation method by the proposed technique

We can represent the Figure 5. by matrix. Let C1, C2, C3, C4 are four matrices and they represents the share generation of the set of pixels black and black, black and white, white and black, white and white respectively, where 1 represents the black pixel and 0 represents the white pixel.

$$C_0 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \qquad C_1 = \begin{bmatrix} 1 & 0 & 0 \end{bmatrix}$$

$$C_2 = \begin{bmatrix} 0 & 0 & 1 \end{bmatrix} \qquad C_3 = \begin{bmatrix} 1 & 0 & 0 \\ 1 & 0 & 0 \\ 1 & 0 & 0 \end{bmatrix}$$

Fig. 3, Fig. 4 and Fig. 5 represents three shares generated from Fig. 2 . Fig. 6, Fig. 7 and Fig. 8 represent the stacked shares respectively.

Let us take an illustrative example of the proposed algorithm for better understanding. Consider the image in Figure 6 is as input image.

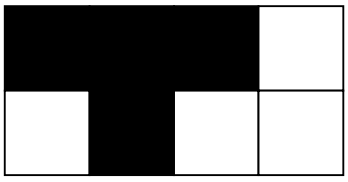

Figure 6. Input image

If we read the image in Figure 6 in row major order first we are getting two black pixels, followed by one black and one white, among next two, one white and one black and lastly two white pixels. The generated shares by the proposed algorithm are given in the Figure 7, 8 and 9 respectively.

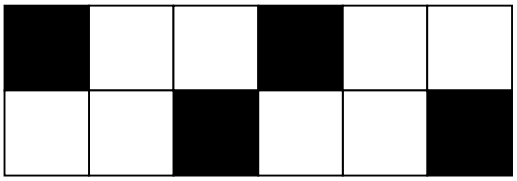

Figure 7. Share1

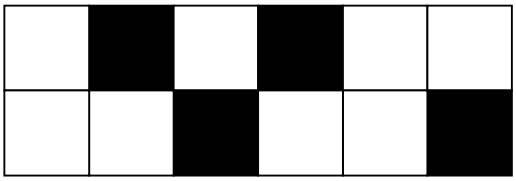

Figure 8. Share2

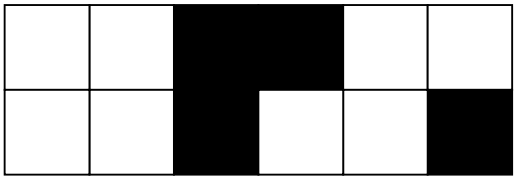

Figure 9. Share3

Now, we are to consider a real life image and we are applying the proposed technique into the Figure 10 given below. We are generating three shares given in the three transparencies after the figure. It can easily be observed that after staking any two of the shares with proper alignment the hidden image reveals with some noise in the background.

Figure 10. Input image

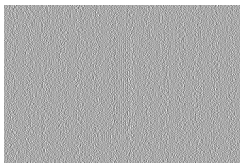

Figure 11. Share1

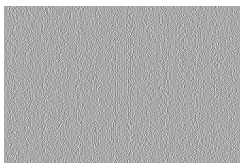

Figure 12. Share 2

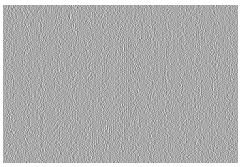

Figure 13. Share3

Figure 14. Share1+Share2

Figure 15. Share 2+Share3

Figure 16. Share3+Share1

6. PERFORMANCE ANALYSIS

From the literature study it is seen that the paper [4] developed by Chetana Hegde, Manu S, P Deepa Shenoy, Venugopal K R, L M Patnaik , was an work for secure banking applications using visual cryptography. Let us compare the characteristic features of the proposed algorithm with the algorithm developer by Chetana Hegde et. al.

Table 1. Performance analysis

Features	**Algorithm proposed by Chetana Hegde et. al.[4]**	**Proposed Algorithm**
Type of the algorithm	(2,2) visual cryptography	(2,n)visual cryptography
Applicability	Maximum number of account holder is one	No limit in the number of account holder
Pixel expansion	4 times	variable
Number of pixel per input	one	two
Type of the algorithm	(2,2) visual cryptography	(2, n) visual cryptography

Table 1 presents the comparison of some salient features between the proposed algorithm and the algorithm proposed by Chetana Hegde et. al. [4] where it is clear that in case of proposed technique the space overhead has been reduced as two input pixels are clubbed together in input and taken as single pixel for share generation and the propose algorithm is more useful than previous one.

7. CONCLUSIONS

In this paper a novel (2, n) visual cryptographic technique has been proposed which is easy to implement and it is capable to provide security like other existing algorithms. One most important feature in the proposed algorithm is it can be used for any number joint account holders. Though it takes two consecutive pixels as the one time input, it may offer space efficiency compared to the algorithms which take single pixel as the one time input.

REFERENCES

[1] M. Naor, and A. Shamir, (1994) "Visual Cryptography", *Advances in Cryptography-Eurocrypt '94*, vis Lecture Notes in Computer Science 950, pp. 1-12.

[2] Tai- Wen Yue and, Suchen Chiang (2000) "A Neural Network Approach for Visual Cryptography", *IEEE-INNS-ENNS International Joint Conference on Neural Networks*, vol.5, pp 494-499.

[3] D. Jena, and S. K .Jena,(2009) "A Novel Visual Cryptography Scheme", *The 2009 International Conference on Advanced Computer Control*, pp- 207-211.

[4] C. Hegde, Manu S, P. D.Shenoy, Venugopal K R and L. M. Patnaik (2008), "Secure Authentication using Image Processing and Visual Cryptography for Banking Applications" *16th International Conference on Advanced Computing and Communication (ADCOM 2008)*, MIT Campus, Anna University, Chennai, India, pp. 433-439.

[5] A. Adhikari and B. Roy (2008) "On some Constructions of Monochrome Visual Cryptographic Schemes" *Proceedings of the 1st International Conference on Information Technology*, Gdansk, Poland.

[6] J. K. Pal, J. K. Mandal and K. Dasgupta (2010) "A Novel Visual Cryptographic Technique through Grey Level Inversion (VCTGLI)" *Proceedings of The Second International conference on Networks & Communications*, Chennai, India, pp. 124-133

[7] M. Heidarinejad, A. A. Yazdi,; K.N. Plataniotis, (2008) "Algebraic Visual Cryptography Scheme for Color Images" *IEEE International Conference on Acoustics, Speech and Signal Processing*, pp. 1761 – 1764.

[8] G.R Zhi Zhou Arce,. G. Di Crescenzo (2006) "Halftone Visual Cryptography". *IEEE Transactions on Image Processing*. , Volume: 15, Issue: 8pp- 2441-2453.

[9] A. Houmansadr, S. Ghaemmaghami, (2006) "A Novel Video Watermarking Method Using Visual Cryptography" *IEEE International Conference on Engineering of Intelligent Systems*, , Islamabad, Pakistan, pp 1-5.

[10] P. Geum-Dal,; Y. Eun-Jun,; Y. Kee-Young , (2008) "A New Copyright Protection Scheme with Visual Cryptography", *Second International Conference on Future Generation Communication and Networking Symposia*. pp. 60-63.

[11] Y. Wei-Qi, J. Duo,; M. S. Kankanhalli, (2004) "Visual Cryptography for Print and Scan Applications". *International Symposium on Circuits and Systems*. pp- 572-575.

[12] S. Gravano,(2001) *Introduction to Error Control Codes*, Oxford University Press, USA.

Authors

Jayanta Kumar Pal has passed B. Tech in Information Technology from JIS College of Engineering, (West Bengal, India) in 2008. He has completed M. Tech in the year of 2010 in the Computer Science and Engineering from Kalyani Government Engineering College (West Bengal, India). He has four publications in different international conferences. He is the life member of Advanced Computing and Communication Society and member of IEEE

J. K. Mandal is Professor in the Department of Computer Science and Engineering in the University of Kalyani (West Bengal, India). Seven scholars have already awarded Ph. D. under his guidance. He has 25 years of teaching and research experience and 140 publications in different international and national journals and conferences . He is the life member of Computer Society of India.

Kousik Dasgupta did his Bachelors in Engineering in Electronics and Power Engineering from Nagpur University, Nagpur, India in 1993. Subsequently, he did his Masters in Computer Science & Engineering in 2007 from West Bengal University of Technology, Kolkata, India. He is currently a Senior Lecturer in the Department of Computer Science and Engineering of Kalyani Government Engineering College, Kalyani, India. He served industries like ABB and L & T during 1993-1996 and as a Technical Assistant in Kalyani Government Engineering College, Kalyani, India before joining the same institute as lecturer in 2001. He is co-author of two books and about 15 research publications. His research interests include soft computing, computer vision and image processing. Dasgupta is a Life Member of ISTE, India, Associate Member of The Institute of Engineers, India and Chartered Engineer [India] of The Institute of Engineers, India. He is a Fellow of OSI, India