Ingénierie des Systèmes d'Information
Vol. 24, No. 6, December, 2019, pp. 627-632
Journal homepage: http://iieta.org/journals/isi

A Novel Approach to Key Management Using Visual Cryptography

Mundukur Nirupama Bhat[1*], Suvarna Buradagunta[1], Kuruba Usha Rani[2]

[1] VFSTR Deemed to be University, Vadalamudi 522213, Andhra Pradesh, India
[2] Sri Padmavati Mahila Viswavidyalayam, Tirupati 517502, Andhra Pradesh, India

Corresponding Author Email: drmnb_cse@vignan.ac.in

https://doi.org/10.18280/isi.240610

Received: 12 May 2019
Accepted: 6 August 2019

Keywords:
trusted third party, XOR based visual cryptography, regeneration, redistribution, key management

ABSTRACT

Visual Cryptography encrypts the secret or key into 'n' shares or portions and distributes them to a group of 'n' participants. The secret is recovered only when shares of all the participants in the group are stacked upon one another depending on the method used. This technique eliminates complex computations during decryption. It uses simple OR or XOR Boolean operations. Once the secret is revealed, it is no more a secret. So, a new secret acts as a key, that is to be again shared confidentially. The same process is performed and new shares are generated and distributed. The generation and distribution of shares must be done every time when a new secret or a combinational key is shared. In this paper, a trusted third party generates the shares and distributes it to the group of participants. It also generates an extra share for itself. To reveal the secret, the third party's share is also used along with other participants shares. Every time when the secret is to be changed, the third party regenerates its share only, instead of generating shares for all participants. This method reduces the overhead of regeneration and redistribution of shares to all participants with every change of the secret or key. This method of key management also retains the perfect contrast and security. The OR based method leads to noise during recovery. XOR based operations during recovery recovers lossless image. So, XOR operation is more preferable during recovery of the secret.

1. INTRODUCTION

Humans have a tendency to preserve and protect important things and messages or information from possible misuse or loss. Things can be stored in safe places with lock and key system. But this can be stolen in two ways. If the key is found, it can be taken away by opening the lock. When the key is not found, the system can be physically broken down. To make the key more secure, some combinational key system is devised. This combinational key can be shared among different people or it can be divided into pieces (shares), which can be placed at different locations. To open the lock, this distributed information must be brought together and the key is identified. Sometimes, the information may need to be transmitted securely from one place to another place. The transmission of this information by preserving its privacy is very much essential. Cryptography is the science of encoding and decoding the confidential data, where the secret is stored or transmitted by encoding it into a non-understandable form. This information can be exchanged in a secured way in the insecure environment through the digital communication media. The exchanged or stored information can be decoded whenever needed.

The basic principle of Visual Cryptography Scheme is a secret sharing mechanism where a secret (image) is divided into one or more shares, by generating the shares and distributing them among the participants and reconstructing the secret back by stacking up the shares. The operation underlying this scheme is Boolean OR operation [1]. The evaluation of the scheme can be done with respect to computation complexity, reconstruction precision and security. As the number of shares increases, the contrast of the stacked output decreases, size of the secret image increases. But it provides perfect secrecy. But the deterioration of contrast, resolution, increase in the size of the recovered image, make the system unsuitable for practical purposes. It degrades the visual quality of the recovered secret. If XOR operation is performed during the decoding, the contrast is enhanced and original secret(image) is recovered, without any deterioration in contrast. But the decryption process needs the assistance of computer or special hardware.

In this paper section two emphasizes on literature survey, Section three deals with a simple XOR based scheme. Section Four deals with proposed algorithm for key management and its description, followed by experimental results in section Five. Analysis of the results is in Section Six. Conclusion and Future scope of this article is in the Section seven.

2. RELATED WORKS

Key Management is an important area of Cryptography where the cryptographic keys are generated and distributed to various parties in a secured manner. Noar et al. [2] has constructed a robust key management schemes for a cryptographic system by dividing the key into pieces and stored or distributed among the participants. This Secret Sharing Scheme functions securely and reliably even when some pieces are destroyed. Shamir's scheme is based on polynomial interpolation over finite fields.

Blakley [3] has applied projective geometric ideas to safeguard the cryptographic keys. Simmons's [4] scheme was

in terms of geometric techniques. Ito et al.'s [5] construction of Secret Sharing Scheme for any General Access Structures is an example for an application under access control. Brickell [6] has designed Secret Sharing Schemes with Vector Space Construction. Most of the schemes are practical with the involvement of limited number of participants. These secret sharing schemes are extended to images and was termed as Visual Cryptography Schemes (VCS).

The reconstruction of the secret in Visual secret sharing (VSS) schemes [7-12] uses the human visual system. It uses OR based reconstruction. It requires very little or no computation. Pixel expansion is the main drawback of these schemes where each original pixel is replaced with x subpixels in the generated share. As the value of x increases, it becomes impractical for use.

Wu et al. [13] devised (2,2) XOR based Random grid based visual cryptography. He improved the scheme into a generalized (2,n) RG-based VC and a(n,n) XOR-based VCS using meaningful images are deived and used for different application scenarios.. The visual quality of the recovered image has increased.

Tuyls et al. [14] investigated the threshold VSS associated to XOR operation (modulo two addition). They studied the (n,n), (2,n) and (k,n) schemes and derived bounds on the contrast and resolution of XOR based schemes.

Liu et al. [15] in their studies showed the smallest optimal pixel expansion and the largest possible contrast for the (2, n) XOR based VCS. It also shows that the construction of the basis matrix of optimal contrast for (2, n) XOR based VCS is equivalent to the construction of binary codes when they reach the maximum capability.

Han et al. [16] offered a verifiable visual cryptography scheme based on XOR algorithm. It can check the correctness and authenticity of every share image, the recovery of verifiable image and secret image is simple without any pixel expansion. The relation between OR based VCS and XOR based VCS was investigated by Yang et al. [17] and theoretically proved that the basis matrices of (*k*, *n*)-OR based VCS can be used in (*k*, *n*)-XOR based VCS.

Threshold visual secret sharing schemes, by mixing XOR and OR operation with reversing and based on binary linear error-correcting code was suggested by Tan [18]. The Visual Cryptography Schemes can also be extended to dynamic groups where the size of the group changes dynamically as users join/leave the group.

Lin et al. [19] has proposed a (t,n) VCS with unlimited users based on probabilistic model. This allows users change dynamically without regenerating and redistributing the shares.

3. SIMPLE XOR BASED VISUAL CRYPTOGRAPHY SCHEME

In size invariant XOR based (2, 2) VCS, the shares generated are of the same size as that of the secret image. The pixel expansion is not used.

3.1 Description of the algorithm

The algorithm is elaborated in **two** phases.
Phase -I Creation of shares for the initial secret.
Phase -II Regeneration of the secret.

In Phase-I, the construction steps of the creation of two shares are as follows:

Input: A secret binary image A.
Output: Two distinct shares A1 and A2
Construction:

1. The initial secret image is taken.
2. Two basis matrice C0 and C1 are taken as follows:

$C0 = \left\{\begin{bmatrix}0\\0\end{bmatrix}, \begin{bmatrix}1\\1\end{bmatrix}\right\}$ and $C1 = \left\{\begin{bmatrix}0\\1\end{bmatrix}, \begin{bmatrix}1\\0\end{bmatrix}\right\}$

3. For each pixel value in the secret image,
   a) if the value is 1, any one of the columns of C0 is selected and the values in the column is distributed to each of the shares.
   b) if the value is 0, any one of the columns of C1 is selected and the values in the column is distributed to each of the shares.
4. Step 3 is performed for all the values in the secret image.
5. Thus two shares X and Y are generated.

In Phase-II, the reconstruction of original image is done as follows:

Input: Two shares X and y are taken as input.
Output: Recovered secret image
Construction:

1. Two shares X and Y are taken.
2. For each pixel in X and Y, the values are XORed and the result is stored as recovered image.
3. Step 2 is repeated for all the corresponding pixels of the two shares.

The truth table for XOR operation is given in Table 1.

Table 1. Truth table for XOR based operation

⊕	0	1
0	0	1
1	1	0

C0 and C1 are the basis matrix used for the (2,2) XOR based VCS.

If the secret has a white pixel, randomly one of the columns of C_0 is selected and pixel in each row is distributed among the 2 shares. If the secret has a black pixel, randomly one of the columns of C_1 is selected and pixel in each row is distributed among the 2 shares. This process is completed till all the pixels of the secret is accessed and distributed among the shares. The recovery of the secret needs an XOR operation to be performed on the shares and the pixels are toggled to get back the original image.

The scheme is applied on image with 100 X 200 pixels, as shown in Figure 1a. The two shares generated are shown in Figure 1b and Figure 1c. The recovered image is seen in Figure 1d. The security of the system is maintained and there is no pixel expansion. It is also found that the mean squared error between the original image and recovered image is 0, which means that the original image is same as that of the recovered image. This scheme also maintains the secrecy while generating the shares. Both security and quality of the reconstructed image are maintained.

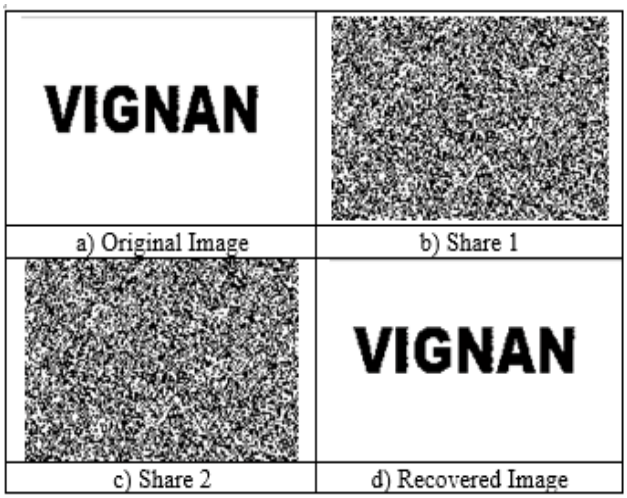

Figure 1. Experimental results of simple XOR based visual cryptography method

4. PROPOSED SYSTEM AND ITS DESCRIPTION

Wang et al. [20] has designed a (n,n) secret sharing scheme based on the XOR operation for gray scale images. This scheme is used on the binary image for sharing the key as secret. The proposed scheme is a visual cryptographic model where shares are generated using a generation model. It uses a simple XOR based visual cryptography scheme to generate shares. It is designed to create a fixed number of shares during the initial generation of shares in the group. The trusted third party generates the shares of the secret or key for all the members of the group and distributes among them by keeping a share with itself.

Suppose there are 'n' users in the group. 'n+1' image shares are generated from the given secret image and distributed to n persons. One of the shares is stored with the dealer. A dealer is a trusted person, who creates the shares and distributes the shares among the participants. The original secret is reconstructed by appling the exclusive-OR (XOR) operation on all the shares i.e. n+1 shares, by stacking them together.

4.1 Description of the algorithm

The proposed algorithm is elaborated in **two** phases.

Phase -I Creation of shares for the initial group.

Phase -II Changing the secret, when it is revealed, without recreating and distributing the shares of the group.

In Phase -I, the construction steps of the generative model in creation of shares for the initial group is as follows:

Input: An integer n with >=2, and the secret binary image A.
Output: n distinct matrices A1, ..., An, An+1 called shares or shadow images.
Construction: n random matrices B1, ..., Bn−1, Bn are generated
The sharesA1, A2, ……. are calculated as below

$A_1 = B_1$
$A_2 = B_1 \oplus B_2$
$A_3 = B_2 \oplus B_3$
. . . . . .
$A_{n-1} = B_{n-2} \oplus B_{n-1}$,
$A_n = B_{n-1} \oplus B_n$
$A_{n+1} = B_n \oplus A$

The original secret or key is found by stacking all the shares together using XOR operation. Suppose A' is the secret found after XOR operation.

A' = A1 ⊕A2 ⊕· · ⊕An⊕An+1.

When A and A' are compared, it is found that A=A'

The proposed method is analysed with respect to parameters like Contrasts, Pixel Expansion, Group Size, Security.

Suppose 'n' is the number of participants among whom the shares were to be distributed. Here n+ 1 share is created initially using the above algorithm and distributed among the n participants. Creation of the initial shares in the group are shown in the Figure 2. n +1thshare is secretly stored with the dealer. During the revealing of the secret all n+1 shares, including the dealer's share must be XORed together. The secret can be changed every time the key is revealed without changing the share of the participants.

Phase -II The algorithm for changing the secret, when it is revealed, without recreating and distributing the shares of the group is as follows:

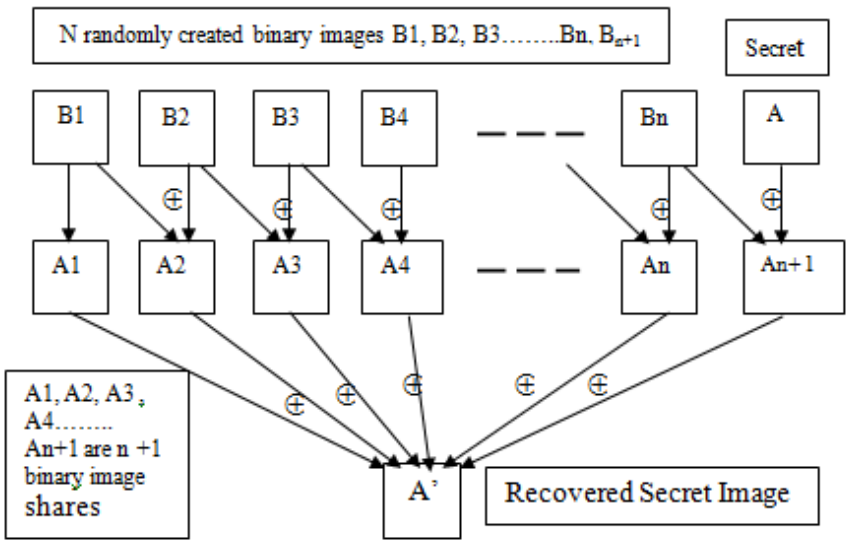

Figure 2. Creation of the initial shares for the group

Input: A_{n+1}theDealers share, the secret image A, *and new secret image* A_{new}
Output: $A_{newshare}$ share (Dealer's newshare)
Construction: To change the secret, following step is performed:
Dealer's share $A_{newshare} = A_{n+1} \oplus A_{new} \oplus A$

The dealer uses his share to change the secret. The old secret and the new secret are XORed with the dealer's share. This becomes the new share of the dealer. This is shown in Figure 3.

To get back the secret now, all the participants shares are XORed along with the dealers newshare.

$A_{new}' = A_1 \oplus A_2 \oplus \cdot \oplus A_n \oplus A_{newshare}$

When A_{new} and A_{new}' are compared, it is found that $A_{new} = A_{new}'$

During the revealing of the secret all n+1 shares, including the dealer's share must be XORed together. The secret can be changed every time the key is revealed without changing the share of the participants.

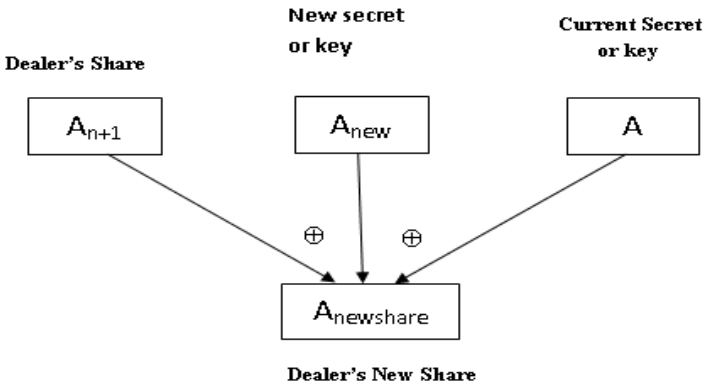

Figure 3. Creating new share by the dealer when the secret is revealed

5. EXPERIMENTAL RESULTS

Two binary images (secrets) with size 100 X 200 pixels each are used in the implementation of this scheme. It is shown in Figure 4.

The secret S1 in Figure 4a is used for generating the initial shares. Suppose there are three participants present in the group. Four shares A1, A2, A3, A4 are generated using the initial secret S1 according to the procedure discussed in Phase-1.

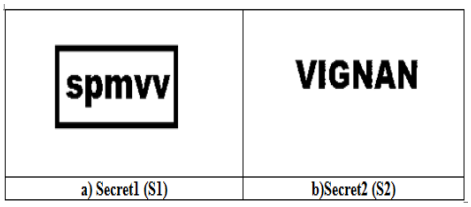

Figure 4. a) Secret1 and b) Secret2 are the old and new secrets used in the procedure

Three shares are distributed among the 3 participants and a 4th share is stored with the dealer. That is shown in the Figure 5a, b, c and d. When all the four shares are XORed together, the original secret is obtained. This is shown in Figure 5e. When the secret or key is used, it has to be changed. Instead of changing all the participants' shares, the dealer's share can be updated to change the secret. Secret S2 is the new secret shown in Figure 4b. As discussed in phase-2, the dealer's share is updated as in Figure 6a. The secret is also changed to S2 and this is shown in Figure 4b. When the participants shares are XORed with the dealer's new share, the new secret is revealed as shown in Figure 6b. Thus, whenever the secret is revealed or used, a new key is set and the dealer changes his share instead of regenerating the shares to every participant. This minimizes the overhead.

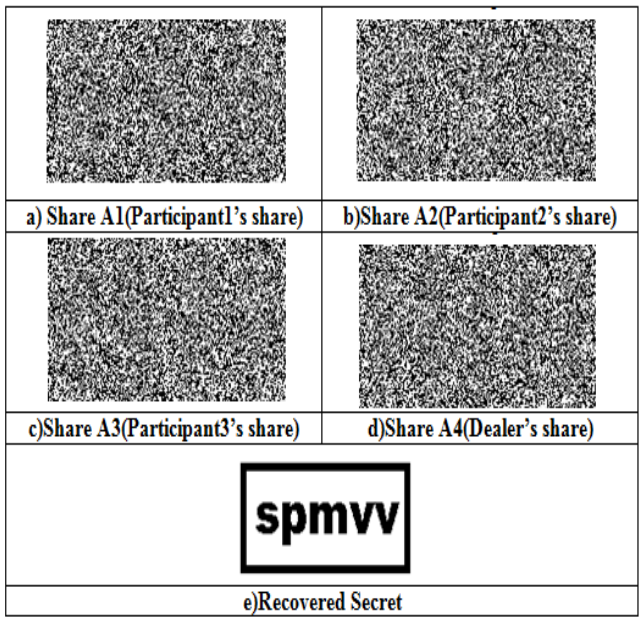

Figure 5. Experimental results of phase-1 of the proposed model

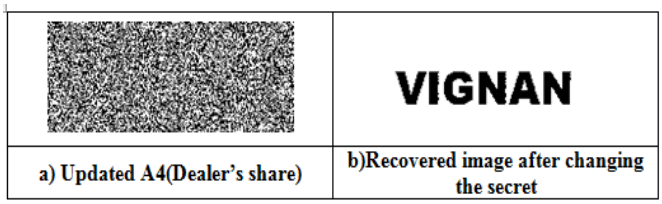

Figure 6. Changed share of the dealer is shown in a). When the participants shares are XORed with the dealers, the new secret or key is revealed (b)

6. ANALYSIS OF THE RESULTS

The proposed model is used to generate shares and change the keys dynamically. It changes the secret or key once it is used. The Dealer, a trusted third party plays an important role in this model.

The Basis Matrix used in the proposed scheme, is a simple matrix of the size of the secret or key. It provides complete security to the generated shares. A single or group of shares less than n shares doesn't reveal or leak any secret, unless all the 'n' shares are stacked together.

Table 2. Details of the pixels in the keys before sharing the secret and after combining the shares and revealing the secret

Secret Images used	White pixels in original secret	Black pixels in original secret	White pixels in recovered secret	Black pixels in recovered secret	% of White pixels recovered	% of Black pixels recovered
S1	16561	3439	16561	3439	100	100
S2	18120	1880	18120	1880	100	100

The pixel details of the original secrets and recovered secrets are given in Table 2. It is found that the percentage of recovery of the white and black pixels are 100% in all of the secrets used. The graphical representation of the above details is shown in Figure 7. It is found that the number of original and recovered pixels are same. This method maintains perfect recovery with no loss in contrast as well as maintains security. regenerating the shares to every participant. This minimizes the overhead. It is also found that the mean square error between the original image and the reconstructed image is Zero. This means there is lossless reconstruction of the secret

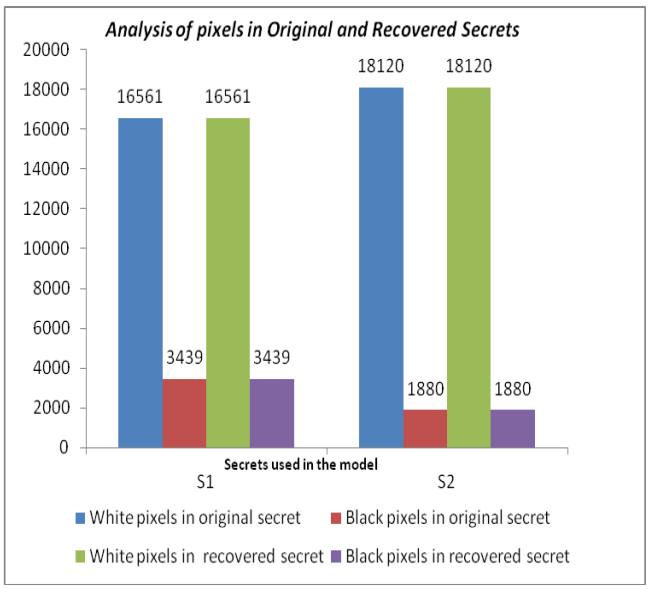

Figure 7. The graph shows that the secrets used as keys in this model is recovered without any change in pixels

7. CONCLUSION AND FUTURE SCOPE

The implemented model uses different secrets in the image form. The secrets were easily recovered by stacking the shares of all participants, including the dealer's or trusted third party's share. There are no complex computations during recovery of the secret. When a new secret is used, without disturbing the participant's share, the secret or key is changed. The size of the original secrets, size of the shares generated and the size of recovered secrets are all same size. There is no pixel expansion and the method sustains size invariance. The proposed model sustains all the required characteristics of performance like invariant size, secured and perfect recovery of the secret. It also provides unconditional security during the generation of shares.

The primary objective of this paper is to reduce the distribution of shared key multiple times when the key is changed. Instead of generating n shares of the key to distribute among n users, only one share of the trusted party is changed.

REFERENCES

[1] Tompa, M., Woll, H. (1979). How to share a secret. Communications of the ACM, 22(11): 612-613. https://doi.org/10.1007/3-540-47721-7_20

[2] Naor, M., Shamir, A. (1994). Visual cryptography II: Improving the contrast via the cover base. International Workshop on Security Protocols, pp. 197-202. https://doi.org/10.1007/3-540-62494-5_18

[3] Blakley, G.R. (1979) Safeguarding cryptographic keys. AFIPS 1979 Nat. Computer Conf., 48: 313-317.

[4] Simmon, G.J. (1992). An Introduction to Shared Secret and/or Shared Control Schemes and Their Application This work was performed at Sandia National Laboratories and supported by the U.S. Department of Energy under contract number DEAC0476DPOO789. Wiley-IEEE Press, 441-447. https://doi.org/10.1109/9780470544327.ch9

[5] Ito, M., Saito, A., Nishizeki, T. (1989). Secret sharing schemes realizing general access structure. Electronics and Communications in Japan (Part III: Fundamental Electronic Science), 72(9): 56-64. https://doi.org/10.1002/ecjc.4430720906

[6] Brickell, E.F. (1989). Some ideal secret sharing schemes. In: Quisquater JJ., Vandewalle J. (eds) Advances in Cryptology - EUROCRYPT '89. EUROCRYPT 1989. Lecture Notes in Computer Science, vol 434. Springer, Berlin, Heidelberg. https://doi.org/10.1007/3-540-46885-4_45

[7] Verheul, E.R., Van Tilborg, H.C.A. (1997). Constructions and properties of k out of n visual secret sharing schemes. Des. Codes Cryptography, 11(2): 179-196. https://doi.org/10.1023/A:1008280705142

[8] Blundo, C., De Santis, A., Stinson, D.R. (1999). On the contrast in visual cryptography schemes. J. Cryptology, 12(4): 261-289. https://doi.org/10.1007/s001459900057

[9] Hofmeister, T., Krause, M., Simon, H.U. (2000). Contrast-optimal k out of n secret sharing schemes in visual cryptography. Theoretical Computer Science, 240(2): 471-485. https://doi.org/10.1016/S0304-3975(99)00243-1

[10] Bose, A.M. (2004) A new visual cryptographic scheme using Latin squares. IEICE Transactions on Fundamentals of Electronics Communications and Computer Sciences, pp. 1198-1202.

[11] Lin, C.C., Tsai, W.H. (2003). Visual cryptography for gray-level images by dithering techniques. Pattern Recognition Letters, 24(1-3): 349-358. https://doi.org/10.1016/S0167-8655(02)00259-3

[12] Cimato, S., De Prisco, R., De Santis, A. (2003). Contrast optimal colored visual cryptography schemes. Proceedings 2003 IEEE Information Theory Workshop (Cat. No.03EX674), Paris, France, pp. 139-142. https://doi.org/10.1109/ITW.2003.1216714

[13] Wu, X.T., Sun, W. (2013). Generalized random grid and its applications in visual cryptography. IEEE Transactions on Information Forensics and Security, 8(9): 1541-1553. https://doi.org/10.1109/TIFS.2013.2274955

[14] Tuyls, P., Hollman, H.D.L., Vanlint, J.H., Tolhuizen, L. (2005). XOR-based visual cryptography schemes. Designs, Codes and Cryptography, 37: 169-186. https://doi.org/10.1007/s10623-004-3816-4

[15] Liu, F., Wu, C. (2015). Optimal XOR based (2,n)-visual cryptography schemes. In: Shi YQ., Kim H., Pérez-González F., Yang CN. (eds) Digital-Forensics and Watermarking. IWDW 2014. Lecture Notes in Computer Science, vol 9023. Springer, Cham. https://doi.org/10.1007/978-3-319-19321-2_25

[16] Han, Y., He, W., Dong, H., Liu, J. (2012). A verifiable visual cryptography scheme based on XOR algorithm. Proceedings of IEEE 14th International Conference on Communication Technology, Chengdu, China, pp. 673-677. https://doi.org/10.1109/ICCT.2012.6511290

[17] Yang, C.N, Wang, D.S. (2014). Property analysis of XOR based visual cryptography. IEEE Transactions on Circuits and Systems for Video Technology, 24(2):189-197. https://doi.org/10.1109/TCSVT.2013.2276708

[18] Tan, X.Q. ((2009). Two kinds of ideal contrast visual cryptography schemes. 2009 International Conference on Signal Processing Systems, Singapore, Singapore, pp. 450-453. https://doi.org/10.1109/ICSPS.2009.119

[19] Lin, S.J., Chung, W.H. (2012). A probabilistic model of (t,n) visual cryptography scheme with dynamic group. IEEE Transactions of Information Forensics and Security Information, 7(1): 197-207. https://doi.org/10.1109/TIFS.2011.2167229

[20] Wang, D., Zhang, L., Ma, N., Li, X. (2007). Two secret sharing schemes based on Boolean operations. Pattern Recognition, 40(10): 2776-2785. https://doi.org/10.1016/j.patcog.2006.11.018