A NEW XOR-BASED VISUAL CRYPTOGRAPHY SCHEME FOR AUTHENTIC REMOTE VOTING SYSTEM

Mahmoud E. Hodeish[1], Vikas T. Humbe[2]

[1]School of Computational Sciences, S.R.T.M. University, Nanded, India.
mah_hodesih@yahoo.com
[2]School of Technology, S.R.T.M. University, Sub-Centre, Latur, India.
vikashumbe@gmail.com

ABSTRACT

The current technological era demands high security and verifiability, especially in the Remote Voting System (RVS) through the Internet in order to resist the cheating case in election process. In this paper, a new Visual Cryptography (VC) scheme is proposed to authenticate the voters in a RVS. Unlike the traditional VC, the current scheme is designed on the basis of creating a new matrices in the light of the bitwise XOR operation. This authentication scheme is suitable for RVS due to using a structural similarity measures such as Mean square Error (MSE) and Peak Signal to Noise Ratio (PSNR) for verification process. The experimental results reveal that the proposed scheme has a low computational cost and provides a balance between the security, storage, and performance.

KEYWORDS

Visual Cryptography (VC), Remote Voting System, MSE, PSNR, Internet Voting

I. INTRODUCTION

In democratic countries, citizens have rights to elect their representatives among themselves to form a governing body, such as a parliament. One of the democratic styles is electronic voting which allows voters to transmit their secure and secret voted ballot to election officials through the internet. The RVS can be referred to as Internet voting which allows people to cast their votes remotely through the Internet. It provides a good solution for voters who live in a far off election centre.

In some democratic system countries, like the USA, Switzerland, etc. commonly follow the RVS in the election. There were cast 69% voters balloted through the mail general election in Washington State in general election [1].

Though the Internet voting presents risks to the voter's privacy and the election's integrity, evidence seems to point out that Internet voting has become to stay [2]. According to the Krimmer's et al. (2007) study [3], numerous Internet elections (~140) had already occurred worldwide and many of them (~40%) were actual real binding elections. These numbers have been increasing as more countries perform trials or adopt the Internet voting channel. Notable examples are the cases in Switzerland and Estonia which are moving to/already have national binding Internet elections. A more recent example is Norway which had a trial on the Internet voting system in the 2011 local government elections (Ministry of local Government and Regional Development, 2012 [4]).

The authentication of user's identity remains the important issue in RVSs. Therefore; it is necessary to develop such secured authentication strategies in order to prevent any unauthenticated voter from casting duplicated votes.

To some extent, the biometric can be applicable for authentication, based on unique individual characteristics. The biometric authentication process consists of several stages: measurement, signal processing, pattern matching and decision making. As a matter of fact, the biometric systems have disadvantages, 1) Environment and usage can affect measurements. 2) Systems are not 100% accurate. 3) Require integration and/or additional hardware. 4) Cannot be reset once compromised. These disadvantages lead to an urgent need to develop such system without using biometric function authentication of the voter. Thus, VC is a helpful and suitable technique for RVS which can improve the security against eavesdropping or substitution attacks and reduce the operational costs. In addition, it is easy to be implemented and it consumes less battery power for increasing life time of the power continuation.

II. VISUAL CRYPTOGRAPHY OVERVIEW

The VC is a new cryptographic technique used to encrypt the secret message in visual form (like image) by breaking it into *n* shares then be transmitted securely via internet or any other communication channels. The original image can only be recovered when a sufficient number of shares superimposing together [5]. The basic model of VC was invented and innovated by Naor and Shamir [6] for protecting the security of visual information transmitted to different participants over public network. It is expressed as two-out-of-two scheme by using 2 subpixels. The basic matrices of the two-out-of-two scheme is a collection of n × n matrices as follows:

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

$$C_1 = \{\text{all the matrices obtained by permuting the columns of } \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}\}.$$

Under this scheme, a secret binary image is encoded by using a codebook (shown as figure 1) into two shares. Every pixel (*p*) in the secret image is split into two subpixels (*black/white and white/black*) located next to each other in each of the two generated shares. If a *p* is white, four pixels will be selected randomly from the pixels opposite to the white pixel in the codebook. In contrast, if a *p* is black, four pixels will be selected randomly from the pixels opposite to the black pixel in the codebook. The original image is recovered by OR-ed the two shares together.

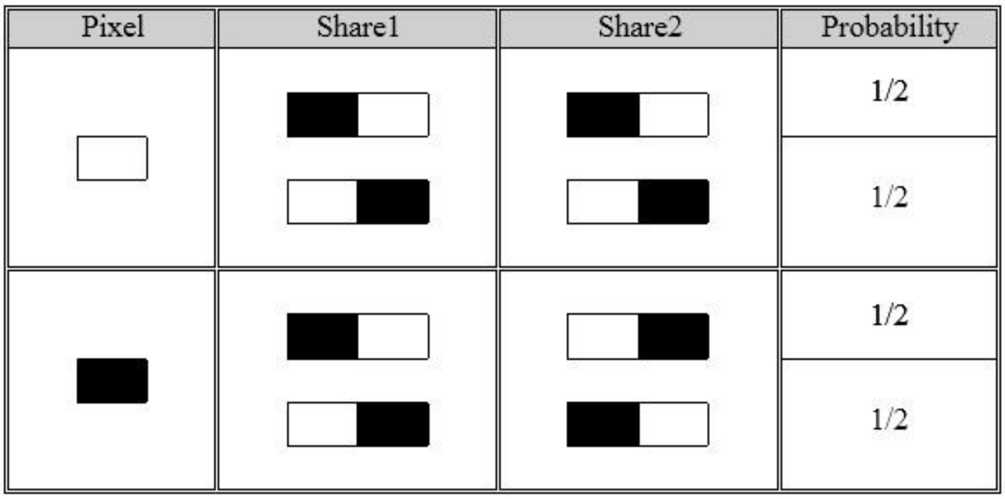

Pixel
Share1
Share2
Probability
1/2
1/2
1/2
1/2

Figure 1. The codebook of (2,2) secret sharing scheme (two pixel expansion)

In fact, this scheme faces many problems which can be represented in pixel expansion and poor contrast. The pixel expansion leads to generate shares with double size of the original image and loss some information, whereas the poor contrast indicates that the variation between the secret image and the reconstructed image is too high. A comprehensive review of VC can be provided in [7]. Recently, many schemes have been proposed in order to solve the above problems in different access structures such as (2,2), (n,n) or (k,n). For example (Ito et al., 1999 [8]; Yang, 2004 [9]; Tuyls et al., 2005 [10]; Yang and

Chen, 2005, 2006 [11-12]; Liu et al., 2009 [13]; Pal et al., 2010 [14]; Hodeish and Humbe, 2015 [15]; Hodeish et al., 2016 [16]).

Moreover, the VC with RVS offering a facility to cast vote for critical and confidential decisions. It is approachable as it allows casting of vote from any place remotely so that election can be held confidentially. Many RVSs with VC have been proposed by researchers like Pawar et al., 2015 [1]; Kate and Katti, 2016 [17]; Nisha and Madheswari, 2016 [18]; Naidu et al., 2016 [19].

This paper provides a proper and suitable VC scheme for authentication process in RVSs to save the storage space of voter and server, providing a secure and fast transmission and making the verification process done through structural similarity measures with no much computational costs.

The rest part of this paper is structured as follows: Part 3 describes the Scenario of Authentication in RVS using the proposed VC scheme. The proposed scheme is described in details in part 4. Experimental results and performance analysis are provided in part 5. Finally, the conclusion is drawn in part 6.

III. SCENARIO OF AUTHENTICATION IN RVS USING VC

The following scenario is assumed that in order to perform the proposed VC scheme for authentication purpose:
1. Once user makes a registration in the voting system, server generates a random ticket based on the personal information of the user/voter and embeds it into a binary blank image.
2. After embedding process, the proposed VC scheme is applied on the generated image in order to generate two shares.
3. Once the shares are generated, one share to be sent to the voter through his registered email ID and another share is saved in the server data base.
4. Once voter chooses his candidate in the voting system, he will be asked to upload his private share to the server.
5. Subsequently, server superimposes the two identical shares and calculates the MSE value between the superimposed image and its identical original image.
6. If MSE=0, then voter is authenticated and his vote will be casted and counted to his selected candidate, otherwise; his vote will be denied as shown in figure 2.

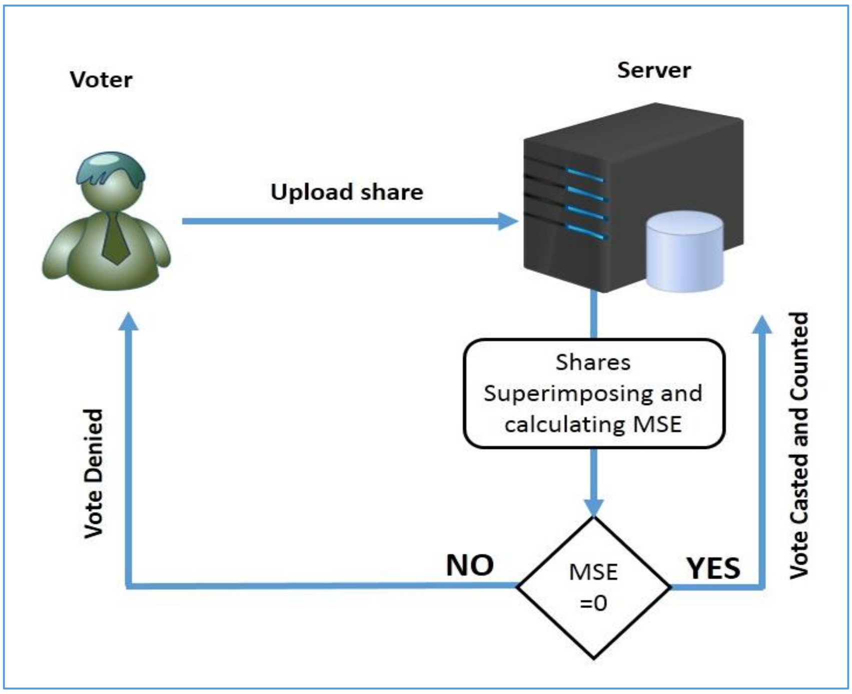


Figure 2. Authentication process through VC in RVS

IV. THE PROPOSED METHOD

The proposed scheme includes basic matrices creation, codebook design, shares generation phase, and recovery phase as follows:

4.1. Matrices Creation

The basic matrices of the current scheme are designed according to the truth table of the bitwise XOR operation. The current scheme is *two-out-of-two* VC scheme which consists of two collections of 2 × 2 Boolean matrices C_0 and C_1 which can be represented as follows:

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

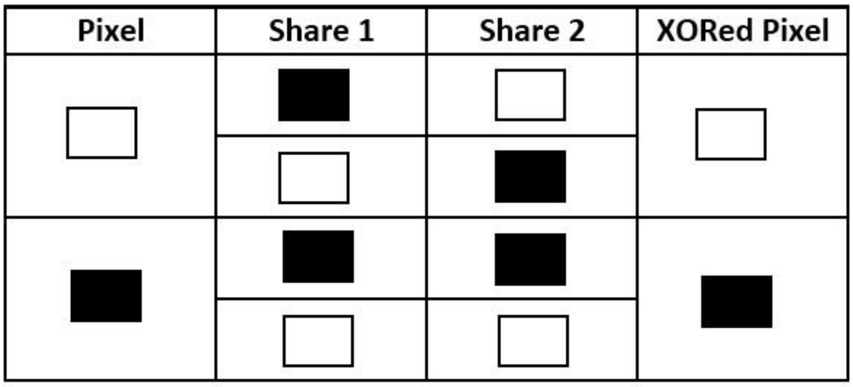
The proposed scheme is designed to be non-expansible scheme. Therefore, to encode a white pixel, one row of the C_0 randomly chosen, and to encode a black pixel, the associate randomly chooses one row of the C_1. Then, one element of each row will be assigned to one share and another element to another share. Moreover, the pixel expansion *m* equals to one and the Hamming weight *H* equals to two.

Definition 1 (Basic Matrix of (2,2) XOR-based VC scheme*) let n, m and h be positive integers satisfying* $0 < h \leq m$*. A n×m binary matrix M is called a basis matrix for a (2,2) XOR-based VC scheme, if it satisfies the following condition: the weight of the XOR (denoted by ⊕) of any two rows in M satisfies* $w(j_{i1} \oplus j_{i2}) \geq h$*, where* $j_i (i=1, \ldots, n)$ *is a row of M and h ≥ 1.*

In any basic matric of XOR-based VC, there are some kinds of patterns always exist which consists of a 1 and a 0 as $\begin{bmatrix} 0 \\ 1 \end{bmatrix}$ and $\begin{bmatrix} 1 \\ 0 \end{bmatrix}$. The other patterns $\begin{bmatrix} 0 \\ 0 \end{bmatrix}$ and $\begin{bmatrix} 1 \\ 1 \end{bmatrix}$ do not contribute to the value of weight (*w*) [20]. Thus, the structural similarity measures are going to be used to measure the relevant contrast.

4.2. Codebook Design

The codebook of the current scheme is designed on the base of the created basic matrices as shown in figure 3.



Pixel	Share 1	Share 2	XORed Pixel
□	■	□	□
	□	■	
■	■	■	■
	□	□	

Figure 3. The codebook of the proposed scheme (no pixel expansion)

4.3. Shares Generation Phase

In order to generate two shares under the proposed scheme, each pixel of the original binary image is checked to identify its color. In case the pixel color is white, randomly choose one block from the two blocks that are peer to the white pixel in the codebook (shown as a figure 3) and assign one element to share 1 and the second element to the share 2. In the case of black pixel, randomly choose one block from the two blocks that are peer to the black pixel in the codebook (shown as a figure 3) and assign one element to share 1 and the second element to the share 2. The two shared images will be generated when all pixels of the secret image are scanned.

4.4. Recovery Phase

Using the bitwise XOR operation to stack the two shared images, the original secret image is recovered.

V. Experimental Results and Performance Analysis

In order to show the efficiency and effectiveness of the current scheme, the experiment is conducted on the binary face image as shown in fig. 4 (a) with size of 256×256 as a secret image. Firstly, one pixel is taken as input by raster-scan order. Then each pixel of secret image is successively taken into the codebook of this scheme in order to generate two shares with the same size of the original secret image as shown in fig. 4 (b-c). As noticed, fig. 4 (d) shows the recovered image by stacking the two shared images by performing bitwise XOR operation without any distortion. The XORing operation permits the complete restoration of secret image [21]. The XOR-based VC was firstly suggested to increase the quality of the reconstructed image and solve the problem of pixel expansion [22].

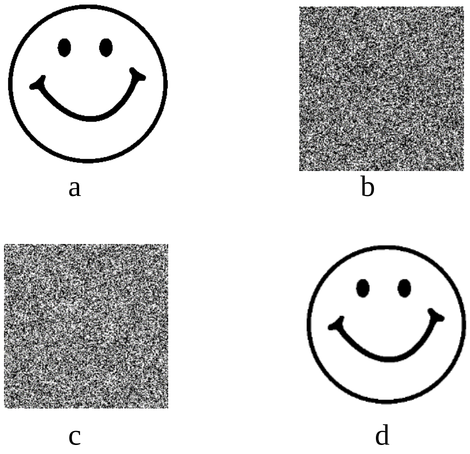


Figure 4. the proposed scheme, (a) the secret image, (b) and (c) the shared images and (d) the reconstructed image.

5.1. Performance Analysis

The proposed scheme results in the following advantages: (1) The reconstructed images have the same size of the original secret image proving that the pixel expansion equals one. (2) Accordingly, it saves the storage space of the voters and the servers, provides fast transmission via public network, Internet, and other communication channels. (3) The image obtained after stacking the shared images appears accurately without losing any information.

As mentioned in the RVS scenario, the verification process can be done by structural similarity measures such as MSE and PSNR. However, in our scenario, the server will calculate the MSE between the original image that stored in the server and the reconstructed image after stacking the share of voter and its corresponding share stored in the server.

The PSNR and MSE can mathematically be expressed as eq. (1) and eq. (2):

$$MSE=\frac{1}{M\times N}\sum_{i=1}^{M}\sum_{j=1}^{N}\left(h_{ij}-h'_{ij}\right)^{2} \qquad (1)$$

$$PSNR=10\times\log\frac{R^{2}}{MSE} \qquad (2)$$

As a matter of fact, while the MSE value should be low, the PSNR should be higher. A higher PSNR and lower MSE indicate lower variation between the secret image and the reconstructed image with a good visual quality. However, when the PSNR value is equal to ∞ and MSE is equal to 0, it indicates that the scheme provides a maximum visual quality where is no any difference between the recovered image and the original secret image [16].

Table 1 shows the obtained values of MSE and PSNR between the original image and the recovered image for two voters: voter 1 has submitted the original share and voter 2 has submitted a suspected share. These results prove the efficiency and effectiveness of the current scheme due to approaching the standard values of MSE and PSNR. Therefore, it is a suitable scheme for authentication process in RVSs.

Table .1 the MSE and PSNR values of authenticate two voters.

Measures	Voter 1	Voter 2
MSE	0	1.5259e-05
PSNR	∞	48.1648

VI. CONCLUSIONS

In the current paper, a new scheme of VC on the base of the XOR operation is proposed, approaching the standard values of the structural similarity measurements such as MSE and PSNR. The ideal results make the proposed scheme a proper authentication method for RVS. The RVSs with help of the current scheme is useful for conducting election process confidentially with high accuracy to reduce the risks fake voting. Moreover, the proposed scheme has an ability to reduce the operational cost and time as well as satisfying the requirement of security for RVSs with high performance. It can be applicable for wide applications of VC; for example, the protection of military, medical, forensic, and art images.

REFERENCES

[1] Pawar, P., Pansare, T., Shinde, J., Shinde, S., & Suryavanshi, P. (2015) Visual Cryptography in Internet Voting System. In International Journal of Computer Science (IIJCS). Volume 3, Issue 10, pp. 1-4.

[2] Joaquim, R., Ferreira, P., & Ribeiro, C. (2013). EVIV: An end-to-end verifiable Internet voting system. computers & security, 32, 170-191.

[3] Krimmer, R., Triessnig, S., & Volkamer, M. (2007, October). The development of remote e-voting around the world: A review of roads and directions. In International Conference on E-Voting and Identity (pp. 1-15). Springer Berlin Heidelberg.

[4] Ministry of Local Government and Regional Development. e-vote 2011-project web site, http://www.regjeringen.no/en/dep/krd/prosjekter/e-vote-2011-project.html?id¼597658; September 2012.

[5] Himanshu Sharma, Neeraj Kumar and Govind K. Jha. Enhancement of security in Visual Cryptography system using Cover Image share embedded security algorithm (CISEA). In: International Conference on Computer & Communication Technology (ICCCT); 2011. p. 462–467.

[6] M. Naor, and A. Shamir. Visual Cryptography. In: Advances in Cryptography-Eurocrypt '94, vis Lecture Notes in Computer Science 950; 1994. p. 1–12.

[7] Hodeish, M. E., & Humbe, V. T. (2014). State-of-the-Art Visual Cryptography Schemes. International Journal of Electronics Communication and Computer Engineering, 5, 412-420.

[8] Ryo, I. T. O., Kuwakado, H., & Tanaka, H. (1999). Image size invariant visual cryptography. IEICE transactions on fundamentals of electronics, communications and computer sciences, 82(10), 2172-2177.

[9] Yang, C. N. (2004). New visual secret sharing schemes using probabilistic method. Pattern Recognition Letters, 25(4), 481-494.

[10] Tuyls, P., Hollmann, H. D., Lint, J. V., & Tolhuizen, L. M. G. M. (2005). XOR-based visual cryptography schemes. Designs, Codes and Cryptography, 37(1), 169-186.

[11] Yang, C. N., & Chen, T. S. (2005). Aspect ratio invariant visual secret sharing schemes with minimum pixel expansion. Pattern Recognition Letters, 26(2), 193-206.

[12] Ching-Nung, Y. A. N. G., & Tse-Shih, C. H. E. N. (2006). New size-reduced visual secret sharing schemes with half reduction of shadow size. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 89(2), 620-625.

[13] Liu, F., Wu, C. K., & Lin, X. J. (2009). The alignment problem of visual cryptography schemes. Designs, Codes and Cryptography, 50(2), 215-227.

[14] Pal, J. K., Mandal, J. K., & Dasgupta, K. (2010). a (2, n) visual cryptographic technique for banking applications. International Journal of Network Security & Its Applications (IJNSA), 2(4), 118-127.

[15] Hodeish, M. E., & Humbe, V. T. (2015, January). A (2, 2) secret sharing scheme for visual cryptography without Pixel Expansion. In 2015 IEEE International Conference on Electrical, Electronics, Signals, Communication and Optimization (EESCO).

[16] Hodeish, M. E., Bukauskas, L., & Humbe, V. T. (2016). An Optimal (k, n) Visual Secret Sharing Scheme for Information Security. Procedia Computer Science, 93, 760-767.

[17] Kate, N., & Katti, J. V. (2016, August). Security of remote voting system based on Visual Cryptography and SHA. In Computing Communication Control and automation (ICCUBEA), 2016 International Conference on (pp. 1-6). IEEE.

[18] Nisha, S., & Madheswari, A. N.(2016, May) Secured Authentication For Internet Voting In Corporate Companies To Prevent Phishing Attacks. International Journal of Emerging Technology in Computer Science & Electronics (IJETCSE),22(1), 45-49.

[19] Naidu, P. S., Kharat, R., Tekade, R., Mendhe, P., & Magade, V. (2016, August). E-voting system using visual cryptography & secure multi-party computation. In IEEE Computing Communication Control and automation (ICCUBEA), 2016 International Conference on (pp. 1-4).

[20] Liu, F., & Wu, C. (2014, October). Optimal XOR based (2, n)-visual cryptography schemes. In International Workshop on Digital Watermarking (pp. 333-349). Springer International Publishing.

[21] Tuyls, P., Hollmann, H. D., Lint, J. V., & Tolhuizen, L. M. G. M. (2005). XOR-based visual cryptography schemes. Designs, Codes and Cryptography, 37(1), 169-186.

[22] Ou, D., Sun, W., & Wu, X. (2015). Non-expansible XOR-based visual cryptography scheme with meaningful shares. Signal Processing, 108, 604-621.

AUTHORS

Mahmoud E. Hodeish has done his B.Sc. (Computer Science) from the Department of Computer Science, Faculty of Computer Science & Engineering, Hodeidah University, Yemen in June 2006/2007. He worked as a lecturer at the Department of Computer, Faculty of Education-Zabid, Hodeidah University, Yemen 2007-2011. He has received his M.Sc. in Computer Networking from School of Computational Sciences, SRTM University, India in 2013. He was a Guest lecturer at the Department of Computer, Faculty of Education, Technical & Applied Sciences-Bajil, Hodeidah University, Yemen, Second Semester 2014. Currently, he is a Ph.D. scholar at School of Computational Sciences, SRTM University, India. His current research interests include information and network security

Vikas T. Humbe has done his M. Sc. (Computer Science) and Ph. D. (Computer Science) from Department of Computer Science and Information Technology, Dr. Babasaheb Ambedkar Marathwada University, Aurangabad in 2003 and 2008 respectively. He has published over 45 research papers in various National and International Journals and conferences. He is Editorial Member and Reviewer for various International and National Journals and Conferences like Elsevier's Pattern Recognition Letters, IEEE's Signal Processing Letters, Journal on Machine Vision and Applications, IEEE IJCNN 07 and 09, 14 ACVIT-09 etc. Presently he is working as Assistant Professor in School of Technology, SRTM University, Nanded (Sub-campus, Latur) and his area of research interest are Biometrics, Image Processing, Computer Vision and Video Processing.