Remote Voting System with Digital Gray-Level Image Visual Cryptography

[1]Pramod Bachiphale, [2]Nitish Zulpe

[1]Research Scholar, College of Computer Science and Information Technology, Latur India
[2]Principal, College of Computer Science and Information Technology, Latur India
Email: [1]pbachiphale@gmail.com, [2]nitishzulpe@gmail.com

Abstract: Technologies demand more security and less computation. A visual cryptography scheme is established by Naor and Shamir. The proposed scheme is designed to create random matrices and shares are created with the bitwise-xor operation. This Scheme requires very less computation and memory, with the lower appeal of more bandwidth. Unlike the traditional VSS proposed scheme overcome pixel Recent image. This scheme's verifiability is analyzed using statistical methods like Peak Signal Noise Ratio (PSNR), and Mean Square Error. This method found a more correct outcome as related to another present scheme**.**

Index terms*: PSNR, MSE, Visual Cryptography Scheme (VCS), Remote Voting System, XOR, Meaningful share, Visual quality*

I. Introduction

In traditional cryptography techniques, computational security is provided and has more overhead of encoding and decoding algorithms. in the Visual Secret Sharing Scheme, less computation and perfect security are maintained. Visual Cryptography is a recent technique to encode and reveal concealed image information. This technique is encoding an image by dividing it into multiple shares, these n various shares are transferred through the Internet or any communication medium. Original image or information is revealed when all n multiple shares are stacked together [1].

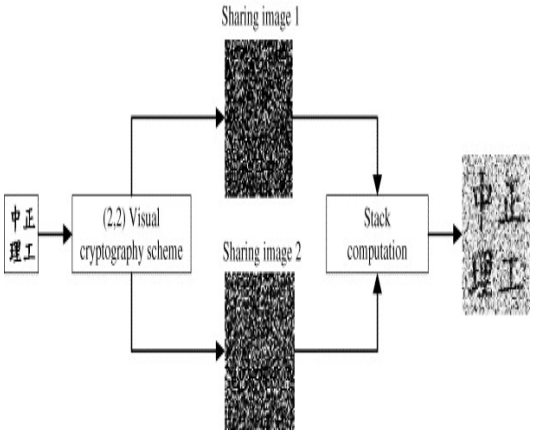

Fig 1. (2,2) VSS SCHEME

Visual cryptography consists of different schemes above fig shows the basic two by two Visual Cryptography Schemes. The original image is divided into 2 different shares. These two different share images are superimposed together to get the original image. There is different Visual cryptographic scheme one is a simple (2,2) scheme where out of two, two secrets are required to reveal original information not less than 2 will generate information. Only a sufficient amount of share is required in visual cryptography to reveal the original image, the user who has a sufficient amount of share can reveal the secret. This scheme is a low computational cost, decoding is performed just by visualizing two superimposed images but it has some disadvantages like pixel expansion and loss of pixel information. There is a different technique to reduce pixel expansion and loss of pixel expansion, sharing multiple secret gray or color images by overcoming pixel expansion and without loss of pixel information, original and reconstructed images are the same by using Boolean operators [2].

Unlike traditional visual cryptography provides less computation but the generated image is bigger in size than the original image, avoiding this complex size problem by using the Boolean xor operation. This scheme uses a deterministic and non-deterministic method for gray and color images, the Boolean operation to avoid pixel expansion and reconstruct the same image as the original image, avoiding complex bigger image size problems [3]. halftoning changing the size of dots and space between creates an optical illusion of the image or image looking like a continuous tone the image [4].Visual cryptography with Boolean xor is used for less computation, used for different an application such as remote voting systems medical, and is efficiently suitable for storage and, performance [5].
In this work, the planned method performs halftoning gray-level image and generate different share by using different random matrices. Random matrices are used for producing shares and these shares generate the original image. The output image is the equal quality as the input image for this planned method is used and applied tothe online voting system to check whether a vote is cast or not. A Boolean operation can be used to generate shares and then reveal original information by stacking a share together. The proposed method avoids pixel expansion and provides a better contrast output image.[6]

II. REVIEW

The key advantage of VC is to generate share images and decoding is performed only through the human eye and an algorithm or computer is not required. The constructed image looks like the original image with overcoming pixel expansion [7]. A best image-hiding mechanism is developed by halftoning an original increasing creates different shares of good quality in which the dimensions of the input image and output image, share images are similar [8].
The proposed scheme uses a random matrix and probability method to crate sufficient s images. The results are very good shared contrast images and reconstructed images for the human visual system and also process developed makes the encryption process much more flexible in terms of pixel adjustment [9].
Alex and Anbarsi[10] have proposed a scheme that provides high-quality image output by applying halftoning and error diffusion techniques on images. A reconstructed halftone image is generated with high quality avoiding the problem. Zhou et al. [11]as a spotlight on the general method to halftone images by applying different cluster and void algorithms for halftoning images and image share generated by this proposed method is best as compared to the contrast-sharer visual cryptography methods.
Feng Liu et al. [12] demonstrated a technique that advances the graphic quality of different share images along with generating meaningful share and only qualifying.Xiaotian Wu a, Wei Sun [15]have the spotlight on Boolean OR and XOR-based visual cryptography in which reconstructed images without any computational devices and in some cases on lightweight devices by using XOR operation. The XOR-based scheme generates good-quality images and shares as compared to the traditional VC scheme.
Shyong Jian Shyu[16] proposed a simple practical method for encoding images by using multiple grids. Multiple transparencies are encoded into the image and superimposing all transparencies can reconstruct the original image. proposed scheme avoids pixel expansion and security is maintained while transmission of data using a random grid.
S.J. Shyu[17] Proposed a method to reveal a secret using a random grid and the secret can be shared with a random grid, after stacking all random grid secret is revealed. This method needs low computation to reveal the secret. This method creates two random grids and information is revealed by stacking two girds, a few numbers of random grids are unable to disclose the input image. This scheme uses (2,2) Visual cryptography techniques for random grids. S. Chen et al. [18] developed a system for efficient visual cryptography with a random grid. This scheme proposes two methods called (2, n) and (2, ∞). This first method is used when shares are predefined or fixed and the second method is used when shares are not fixed or we can extend it to any number of shares. The proposed first method gives a theoretically closer result as expected and the second method achieves the result as expected in terms of contrast.

III. Proposed Scheme

Overview of Remote Authentication System In every democratic country voting is an important process by which all voters in the country choose their representative in government. Some democratic countries like the USA use Remote Voting Systems for elections. The voter needs to register with the Remote Voting System and after registration counting server or dealer generates one image embedding user or voter information. On the user-generated image apply the proposed visual cryptographic scheme to generate three random shares and one main share. After creating shares one share is sent to the user through the mail. The first share is directed towards the voting server, and the other remaining shares and the key share are deposited at the dealer or counting server. At the time of voting, the voter uploads their share to the voting service voting server and sends one user share and one of its shares to the counting server or dealer. The dealer counting server combines voter share and voting server share its's two shares and calculates MSE and PSNR.MSE=0 and PSNR = ∞ then a vote will be cast.

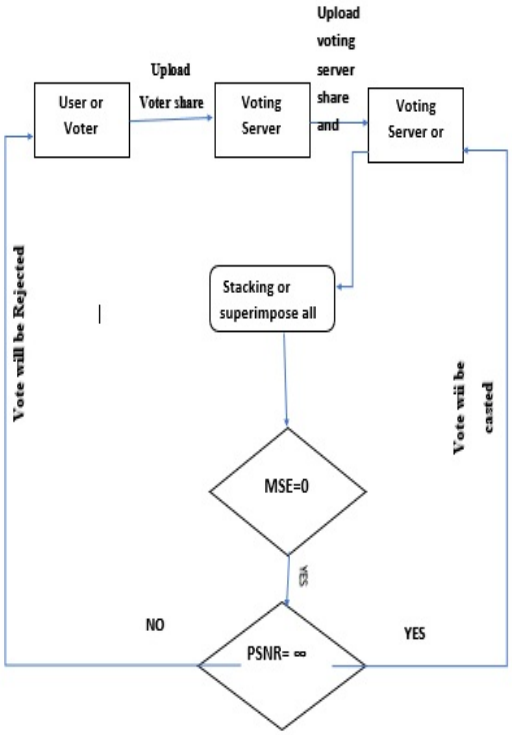

Figure 2: Remote Voting Process.

Process: a. Share construction

1. Read the color image
2. Convert the color input image to gray level image
3. Apply the Jarvis Halftone algorithm to convert it into a halftone image.

4 Define four share images of the same size as the original image and initialize each share with a value zero.

5. Define four matrices of the same dimension theas input image and initialized by zero and fill with Random values to form a grid.
6. Compute four shares by using bit XOR operation on different random matrices.

Process: b. Share superimposition

1. Read four share images
2. Create 3 grids same dimension as the input image and initialized with zeros.
3. Compute original image G by using bitwise XOR operation on four shares.
4. Show the reconstructed image for the remote voting system application

III. EXPERIMENTAL OUTCOMES AND PERFORMANCE ANALYSIS

A test is performed on a gray image and a gray image halftoning is performed. n random matrices are generated, all random matrices are of the equal dimension as the input image and have values between 0 to 255. Random matrices are used to create n-1 random shares and one main share is created by using the bitwise xor operation. Original images and shared images are of the same dimension to avoid pixel expansion.

Figure 2. demonstrates the effectiveness of our scheme in the case of quality output or reconstructed image by applying the scheme to the original image(e), creating different shares (a), (b),(c), and one key share(d), Reconstructed image (f). This demonstrates our reconstructed image with high visual quality with no pixel expansion.

Visual cryptography schemes with Boolean X-OR can be used to construct high-quality images along with minimizing pixel expansion. This scheme also creates meaningful shares and better adjustment of generated shares [13]. Random Grid is a scheme used to create meaningful share but with less visual quality output image rather this is lessened through the visual cryptography (n, n) method [14].

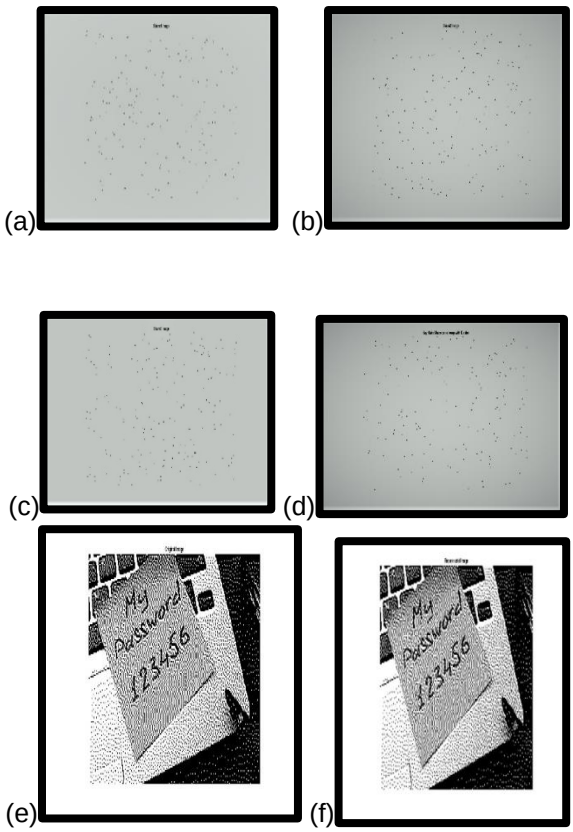

Fig (3). The proposed method (a), (b), (c) shared images, (d) key share, (e) original Image, (f) reconstructed image

IV. Performance Analysis

The proposed process provides diverse advantages It provides images without losing information, original and reconstructed images being the same in pixel size, requiring less computation, lessen the demand for more. bandwidth while transferring images to the network or internet. This process is testable by MSE or PSNR

The equation represented below is a mathematical expression for calculating MSE and PSNR.

MSE= 1/M*N∑i =1M ∑j=1 N (hij-h`ij)2 --(1)

PSNR = 10 * log R2/MSE --(2)

In the above equation, R is the extreme probable value of the pixel image or maximum changes in the data type of the input image. The maximum possible value for our image pixel or 8-bit pixel-represented image value is 255. MSE is evaluated in the above equation by the M*N dimension of the image and the calculating difference between the original and reconstructed image in terms of noise. PSNR should be higher and MSE should be low for high-quality images, PSNR depends on MSE value. MSE determines noise and PSNR determines a quality measure for the input and output image. MSE noise value

.

is zero then PSNR is infinity, this denotes that the input and output image is the same for the human visual system, with no loss of information.

Table 1 displays acceptance values of MSE and PSNR for different types of voters, if values are zero and infinity respectively of different shares stacked together then the voter vote is accepted otherwise rejected.

Table. 1 PSNR and MSE measures for validating vote acceptance

MEASURES	VALUES
MSE	0
PSNR	∞

V. Conclusion

In this work, a novel proposed method is used with bit-wise XOR. The proposed scheme requires less computation, and memory and lessens the request for more bandwidth. The proposed scheme provides better information hiding security. The proposed method also provides a better-reconstructed image with no information loss. this scheme can be used in medical, banking, and remote voting applications and reduce pixel expansion.

References

[1] M. Naor and A. Shamir, “Visual cryptography,” Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics), vol. 950, pp. 1–12, 1995, doi: 10.1007/bfb0053419.

[2] T. H. Chen and C. S. Wu, “Efficient multi-secret image sharing based on Boolean operations,” Signal Processing, vol. 91, no. 1, pp. 90–97, 2011, doi: 10.1016/j.sigpro.2010.06.012.

[3] D. S. Wang, L. Zhang, N. Ma, and X. Li, “Two secret sharing schemes based on Boolean operations,” Pattern Recognit., vol. 40, no. 10, pp. 2776–2785, 2007, doi: 10.1016/j.patcog.2006.11.018.

[4] J. Ramya and B. Parvathavarthini, “An extensive review on visual cryptography schemes,” 2014 Int. Conf. Control. Instrumentation, Commun. Comput. Technol. ICCICCT 2014, pp. 223–228, 2014, doi: 10.1109/ICCICCT.2014.6992960.

[5] V. T. H. Mahmoud E. Hodeish, “A New Xor-Based Visual Cryptography Scheme For Authentic Remote Voting System, International Journal of Engineering Sciences & Emerging Technologies,” vol. 9, pp. 95–101, 2017.

[6] D. T. S. and V. T. Humbe, “A Contrast Optimal Visual Cryptography Scheme for Half-tone Images", International Conference on Recent Trends in Image. Processing and Pattern Recognition, Communication in Computer and Information Science (CCIS),” 2020.

[7] K. H. Lee and P. L. Chiu, “An extended visual cryptography algorithm for general access structures,” IEEE Trans. Inf. Forensics Secur., vol. 7, no. 1 PART 2, pp. 219–229, 2012, doi: 10.1109/TIFS.2011.2167611.

[8] M. C. Askari N, Heys HM, “An extended visual cryptography scheme without pixel expansion for halftone images. 2013 26th IEEE Canadian Conference on Electrical and Computer Engineering (CCECE),” 2013, doi: https://doi.org/10.1109/CCECE.2013.6567726.

[9] L. C.-Y. Hou Y-C, Wei S-C, “Random-Grid-Based Visual Cryptography Schemes. Circuits and Systems for Video Technology,” IEEE Trans., vol. 24, no. 5, pp. 733–744, 2014.

[10] N. S. Alex and L. J. Anbarasi, “Enhanced image secret sharing via error diffusion in halftone visual cryptography,” ICECT 2011 - 2011 3rd Int. Conf. Electron. Comput. Technol., vol. 2, pp. 393–397, 2011, doi: 10.1109/ICECTECH.2011.5941725.
[11] Z. Zhou, G. R. Arce, and G. Di Crescenzo, “Halftone visual cryptography,” IEEE Trans. Image Process., vol. 15, no. 8, pp. 2441–2453, 2006, doi: 10.1109/TIP.2006.875249.
[12] F. Liu and C. Wu, “Embedded extended visual cryptography schemes,” IEEE Trans. Inf. Forensics Secur., vol. 6, no. 2, pp. 307–322, 2011, doi: 10.1109/TIFS.2011.2116782.
[13] D. Ou, W. Sun, and X. Wu, “Non-expansible XOR-based visual cryptography scheme with meaningful shares,” Signal Processing, vol. 108, pp. 604–621, 2015, doi: 10.1016/j.sigpro.2014.10.011.
[14] T. Guo, F. Liu, and C. Wu, “K out of k extended visual cryptography scheme by random grids,” Signal Processing, vol. 94, no. 1, pp. 90–101, 2014, doi: 10.1016/j.sigpro.2013.06.003.
[15] X. Wu and W. Sun, “Random grid-based visual secret sharing with abilities of or and XOR decryptions,” J. Vis. Commun. Image Represent., vol. 24, no. 1, pp. 48–62, 2013, doi: 10.1016/j.jvcir.2012.11.001.
[16] S. J. Shyu, “Image encryption by multiple random grids,” Pattern Recognit., vol. 42, no. 7, pp. 1582–1596, 2009, doi: 10.1016/j.patcog.2008.08.023.
[17] S. J. Shyu, “Image encryption by random grids,” Pattern Recognit., vol. 40, no. 3, pp. 1014–1031, 2007, doi: 10.1016/j.patcog.2006.02.025.
[18] S. K. Chen and S. J. Lin, “Optimal (2, n) and (2, infinity) visual secret sharing by generalized random grids,” J. Vis. Commun. Image Represent., vol. 23, no. 4, pp. 677–684, 2012, doi: 10.1016/j.jvcir.2012.03.004.