International Journal of Research
Available at https://edupediapublications.org/journals
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 05 Issue 15
May 2018

A Survey on Secret Image Sharing Scheme by use of Chaos based Visual Cryptography

Aartika Chandrakar & Manoj Kumar Singh
[1]*M. Tech (Information security), DIMAT, Raipur, Chhattisgarh, India.*

[2]*Assistant Professor, Department of Computer Science and Engineering, DIMAT, Raipur, Chhattisgarh, India.*

Abstract - *Visual cryptography is one of the branch of cryptography in which the plain text is divided into shares and at the receiving end we visually identify the original plain text by stacking those shares. This Research introduces a survey report on Secret image sharing using chaos based visual cryptography by use of (2,8) chaos based visual cryptographic system. That means the secret image is broken up into 8 image shares and combination of two or more shares will regenerate the original image or secret image. There are some security hurdles to enhance the security of sharing system so that the secret image remains secret. The shares are noise like images, no information is shown on those images. This process results less pixel expansion, good output picture quality and having high security system.*

Keywords: Visual cryptography, chaotic system, secret image sharing.

I. INTRODUCTION

As the Internet and digital media are getting more and more popular, requirement of secure transmission of data also increased. Information Security is not simply computer security. Where as computer security relates to securing computing systems against unwanted access and use, information security also includes issues such as information management, information privacy and data integrity. In the current environment, organisations are becoming more and more dependent on their information systems. The public is increasingly concerned about the proper use of information, particularly personal data. Valuing and protecting information are crucial tasks for the modern organisation. The need for information security has increased because of the dependency of individuals and organization on computer has increased. Without security organization cannot successfully operate in global market unless and until they take adequate measures to secure the information. The database which is used or processed by organization and the data in the database is confidential. Information security affects every structural and behavioural aspect of an organisation, a gap in a security fence can permit information to be stolen; a virally infected computer connected to an organization's network can destroy information.

II. LITERATURE REVIEW

Initially the concept of Visual Cryptography was introduced by Naor and Shamir[2] in 1995, they introduced a new type of cryptographic scheme which does not need any cryptographic computation for revealing the secret image. They convert the secret image into n secret shares and by stacking any k secret shares or transparencies can regain the secret image. But any k-1 transparencies or secret shares can not reveal the original image. Hence this sytem is called (k,n) Visual Cryptography. The secret image consists of a collection of black and white pixels according to the secret message, each pixel is converted into n modified version of pixel or subpixels for n secret shares, each share is a collection of m black and white subpixels which are close proximity to each other so that the human eyes will identify the stacked transparencies by averaging the black and white subpixels. But the output image is larger in the size because each pixel of the secret image is divided into n subpixels so the resulting image is also n times greater than the original image and it looks poor in quality. J.Ramya and B.Parvathavarthini [5] presented a research paper in which various visual cryptography schemes are studied and their performance is evaluated on the basis of four parameters such as no. of secret images, pixel expansion, image format and type of share generated. From this survey, the researchers can able to know about several techniques existing in the visual cryptography and can know their performance. Hou and Zen-Yu Young-Chang Quan [13] proposes a method, in this method, the possibility for either black or white pixels of the secret image to appear as black pixels on the shares is the same, which approximates to 1/n. When superimposing k (sheets of share), the

possibility for the white pixels being stacked into black pixels remains 1/n, while the possibility rises to k/n for the black pixels, after that the contrast rises to (n − 1)/n. Shiji Johny and Anil Antony [14] presented a scheme ,in which secret image is decomposed into three color channels (R,G,B) and then the color channels are transformed into the grayscale version. Digital Halftoning is applied on these images for converting the grayscale and three channel images into halftone versions. This technique helps to recovering the exact color of the secret image while decryption. Rituraj Roy, Sayantani Bandyopadhyay, Shyamalendu Kandar and Bibhas Chandra Dhara [15] proposed a (3, 4) image secret sharing scheme and adopted the concept of visual cryptography over the 2 × 2 block. The blocks are scrambled using pseudo random sequence to enhance the security level. Shruthi K Joseph and Ramesh R [16] introduces a method that uses a common share to transmit n binary secrets. The binary secret image is divided into two share images (random grids) as in (2, 2) visual cryptography scheme. By using n+1 share images to transmit n secrets and the extra share is common to all n secrets. Since RG is used it creates shares without pixel expansion. This scheme can be viewed as a modified scheme of (2, 2) random grid. It makes efficient network bandwidth utilization. K. Shankar and Dr. P. Eswaran [17] proposes a method that specified new condition for random matrices and then XOR operations are performed to generate the 'n' transparencies. It is possible to decode the secret image visually by superimposing a k subset of transparencies. The proposed (k, n) VC scheme offers a consistent protection for communicating images over the public channels. Vandana Purushothaman and Sreela Sreedhar [18] done a research, in which effective technique of share generation based on XOR-based visual cryptography for General Access Structures is introduced. Perfect restoration of the secret, no pixel expansion and no code book requirement are the advantages that the algorithm is expected to have. The generated shares are then covered in an image using steganography which provides additional security. Daoshun Wang, Lei Zhang, Nina Ma and Xiaobo Li [19] introduces a probabilistic (2, n) scheme for binary images and a deterministic (n, n) scheme for grayscale images. Both use simple Boolean operations and both have no pixel expansion. The (2, n) scheme provides a better contrast and significantly smaller recognized areas. The (n, n) scheme gives an exact reconstruction. Barnoli Gupta Barik and Samir Kumar Bandyopodhyay [20] proposed a new technique of Image Steganography has been proposed which is using Lorenz Chaotic Encryption to encrypt the secret message, 3 level Discrete Wavelet Transform to hide encrypted data and visual cryptography to share stego image in secret communication. Long Bao, Yicong Zhou* and C. L. Philip Chen [1] introduces a new (2, 8)-secret image sharing scheme integrating the chaos-based image encryption with secret image sharing. It divides the secret image into 8 encrypted shares. Combining any two or more shares is able to completely reconstruct the secret image without any distortion. Each image share is only one pixel larger than the secret image in row and column directions. The proposed scheme is able to directly process the secret images with various formats such as the binary, grayscale, and color images. Experimental and comparison results demonstrate the excellent performance of the proposed scheme.

III. PROBLEM IDENTIFICATION

The research work results the problems we find to solve the problems like pixel expansion, low contrast and security issues.

Pixel Expansion: We have some factors for improvement, one of them is pixel expansion[18]. Pixel expansion refers to the number of sub-pixels in the generated shares that represents a pixel of the original input image. According to the review of the literature survey, pixel expansion is the major drawback of the visual cryptography because each pixel is converted into sub-pixels according to the visual cryptographic scheme and the original single image is divided into many shares, so the size of the shares is also increased, It represents the loss of resolution in the reconstructed image and requires a large storage to store the shares[9].

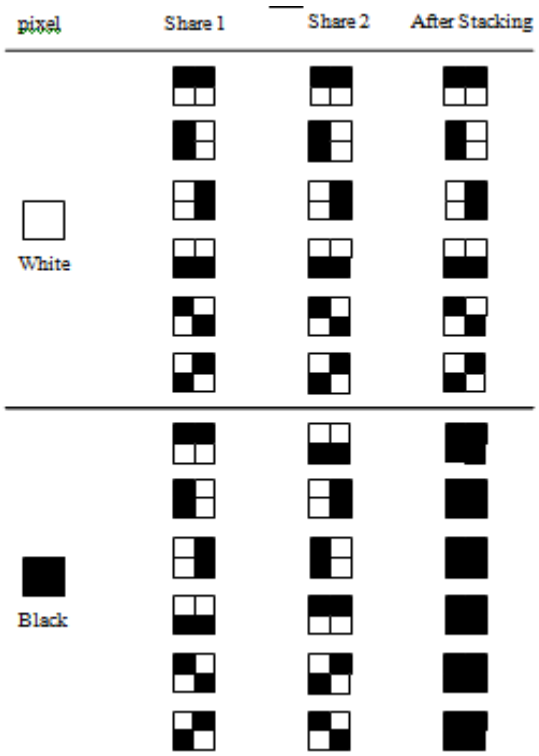

Fig 3.1: Pixel expansion in (2,2) visual cryptography scheme with four subpixel.

Low Contrast: Another factor which needs to be improved is low contrast. Contrast is the relative difference between black and white pixels in the reconstructed image[1]. It demonstrates the quality of the reconstructed image. In general, smaller the value of pixel expansion will reduce the loss in resolution and higher the value of contrast will increase the quality of the reconstructed image. As mentioned, if the pixel expansion is decreased, the quality of the reconstructed image will be increased[19].

Security: The last one is security issues, while transferring information through internet we need to make sure that the system follows the three security essentials that is confidentiality, integrity and authentication.

IV. SOLUTION METHODOLOGY

In this system we used different algorithm to overcome the the issues of the system. Here we use Chaos based Visual Cryptography, that results no pixel expansion as well as better quality of revealed image and also improved security using different methods. In this system we input an image which is known as secret image and process it through different algorithms and the output is encrypted shares and at receiver end process the shares and then perform the decryption process to get the original image. Here we are using (2,8) visual cryptographic scheme. The following is the description of the design and implementation of the system.

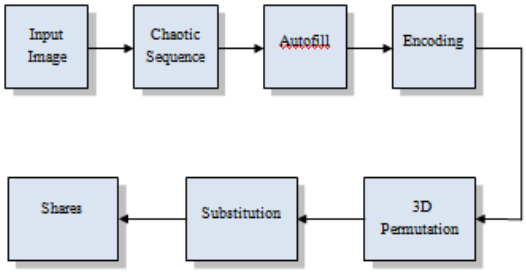

Fig 3.2: Encryption process at the Sender side

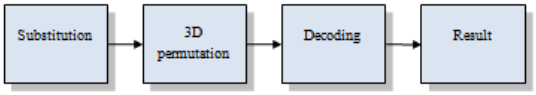

Fig 3.3: Decryption process at the receiver end.

As we see the figure above, the process starts from input image which has to be transmit secretly and ends with the resulting output image which comes from decoding the shares. It has two parts one is Generation phase and another is Reconstruction phase.

The generation phase: Generation phase is for creating or generating shares. Since it is (2,8) chaos based secret image sharing system hence it generates 8 different shares of similar size. The shares are noise like images, no body can determine anything from them. And to make the system more secure various security levels are added into the generation phase. Generation phase consist of five steps including chaotic sequence generation, autofilling, encoding, 3D permutation and substitution. Using chaotic map we generate chaotic sequence or chaotic stream which are dynamic in nature and by using those sequence we apply autofilling process then we encode them into 8 image shares. After generating the shares we apply 3D permutation process to each image share to change the positions of the pixel values to make it unrecognizable

and at last to make it more secure we apply another security hurdle which is a substitution method called Blowfish algorithm into the image shares which is a variable length key block cipher.

The Reconstruction phase: Reconstruction phase is for regenerating the secret image from the shares without any distortion. Reconstruction phase is the inverse process of the generation phase. This phase is used at the receiver end of the communication system. It consist of decrypting the encrypted format and convert it into the original one. In a (k,n) visual cryptography system any combination of k shares will regenerate the original secret image, less than k shares will generate noise like image. Since it is (2,8) chaos based secret image sharing system hence the combination of any two shares can regenerates the secret image[1]. Reconstruction phase consist of three steps including Substitution, Inverse 3D permutation and Decoding process. In substitution process we decrypt the shares which is encrypted by the same algorithm. Inverse 3D permutation is for rearranging the original locations of the pixels which are permuted by the 3D permutation process in the Generation phase and the last one is decoding process which is used for regenerate the original secret image by decode the shares and then we extract the chaotic sequence from the background of the image by performing inverse process of autofilling.

V. RESULTS

For the binary secret images, first transform the binary image into a grayscale image by combining eight neighboring binary pixels together to generate a pixel in the grayscale image. The proposed Scheme is then applied to this gray-scale image to generate eight image shares. Finally, converting each pixel in the grayscale image shares into eight neighboring binary pixels yields the corresponding binary image shares. And for the color image, the proposed scheme is applied to each color component individually and then combines the corresponding shares to generate color shares. As shown in Fig. 4(a), input chooses a grayscale image as the original secret image. The proposed scheme is able to transform it into eight different noise-like image shares which are also grayscale images. In the reconstruction process, only one share is unable to reconstruct the original secret image. However, any two or more image shares will reconstruct the original secret image without any distortion, as shown in Fig. 4(b). Another example of colored image shown in fig 5(a) and 5(b). The output from both type of input gives the output image without any distortion. Thus, the proposed secret image sharing by use of chaos based visual cryptography is a lossless secret image sharing scheme.

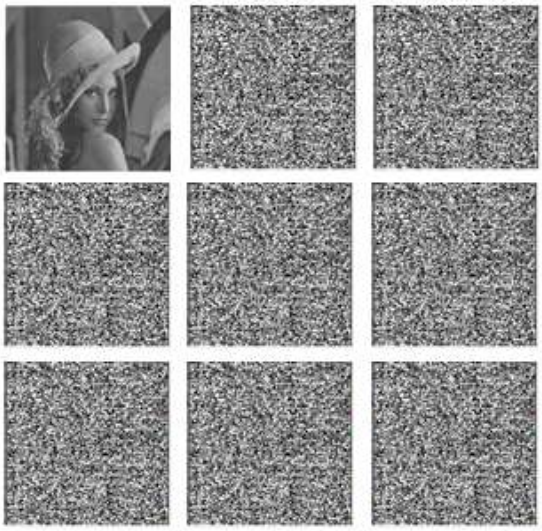

Fig 4(a): Input secret grayscale image and its 8 noise like shares

Fig 4(b): The Reconstructed image

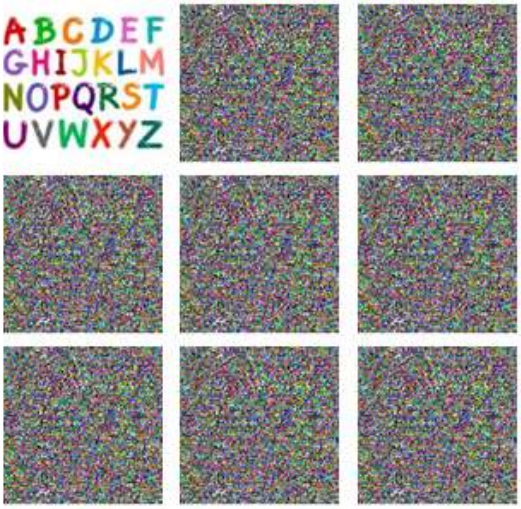

Fig 5(a): Input secret colored image and its 8 noise like shares

Fig 5(b): The Reconstructed image

Mean Squared Error: This can be demonstrated by the quantitative results of the MSE defined by the following Equation[1] . Let I_1 and I_2 are two images with a size of M × N.

$$MSE = \frac{1}{MN}\sum_{i=0}^{M}\sum_{j=0}^{N}(I_1(i,j) - I_2(i,j))^2$$

MSE is used to measure the differences between the reconstructed images and the original secret image. A larger MSE value means a bigger difference between two images. results are shown in the f table 1. The MSE result of the reconstructed image by any two or more shares is equal to zero, indicating that the reconstructed image is as same as the original secret image. Therefore, the proposed scheme is able to reconstruct the original secret image without any distortion.

Peak Signal-to-Noise Ratio: PSNR is the ratio between the maximum power of the signal and the power of noise of the signal. Here signal is the original data and noise is the error detected after processing the signal. It is used to measure the quality of the reconstructed image after the encryption[17]. Let *MAX* is the maximum possible pixel value of the image[7]. Then the formula of PSNR can be given by:

$$PSNR = 10.\log_{10}\left(\frac{MAX_I^2}{MSE}\right)$$

There are some example input images and their corresponding MSE and PSNR values as shown below:

Sr. No.	Image Size (Pixel)	MSE	PSNR
1	128×128	0.015122	114.533478
2	128×128	0.011220	115.829495
3	128×128	0.007222	117.742998
4	128×128	0.006711	118.061418
5	128×128	0.005091	119.261235
6	128×128	0.004423	119.872098
7	128×128	0.010023	116.319660
8	128×128	0.006979	117.891667
9	128×128	0.005576	118.865850
10	128×128	0.003553	120.822992

Table 1: Performance of Secret image sharing using Chaos based Visual Cryptography.

Table 2 demonstrates the performance of the proposed scheme with respect to the other relevant scheme in terms of format of input image, no. Of shares, size of shares, reconstructed image quality and security issues. Shankar's algorithm works on color image but having poor reconstructed image quality while stacking n-1 shares. Another problem with this algorithm is there is no encryption or any other algorithm is used to secure the system. In Johny's algorithm the regenerated image quality is good but there is no security system. Roy's algorithm works on only binary and grayscale images and need n-1 shares to reveal the secret image. Joseph's algorithm only works on Binary images and having poor reconstructed image, where as Bao's algorithm having everything is good but the only problem is average security system. Here accuracy is measured by three factors these are less pixel expansion, good contrast or picture quality, less use of data space and high secrecy and privacy. From Previous work the accuracy is increased.

Algorithm	Format of Input image	No. of Shares	Size of Shares	Regenerated image quality	Security
Shankar's algorithm[49]	Color	n	N	Poor	Poor
Johny's algorithm [46]	Color	n	N	Good	Poor
Roy's algorithm [47]	Binary and Grayscal	4	N	Good	Average

	e				
Joseph's algorithm [48]	Binary	2	N	Poor	Average
Bao's algorithm [1]	Binary, greyscale and color	8	N	Excellent	Average
Proposed scheme	Binary, greyscale and color	8	N	Excellent	Excellent

Table 5.2: Comparative analysis of different algorithms

VI. CONCLUSION & FUTURE WORK

In this system we have done the Chaos based Visual cryptography by using chaotic algorithm, visual cryptography and encryption process. Firstly it was see that mostly research has been done in Visual cryptography system having at least one of the issues like pixel expansion, poor quality of regenerated image or security issues. We have tried to improve the system by using the chaotic map as a trait such that it is easy to generated random sequence of numbers. It is having property of uniqueness that means it is not easy to regenerate or guess the sequence. In this system we are using 3D random permutation that changes the position of the pixel values that makes the image unpredictable. To increase the security hurdle we added another security method that is Blowfish algorithm which is a substitution method for making encryption process tighter so that the unauthenticated users can not reveal or regenerate the secret image. Here accuracy is measured by three factors these are less pixel expansion, good contrast or picture quality, less use of data space and high secrecy and privacy. From Previous work the accuracy is increased. Till date less work is being done on chaos based visual cryptography. This will help in many areas for example to identify any machine or human being, security purpose at military and surveillance, maintaining record in organization, E-commerce, E-voting and many more. In future many other media like video can also be protected by using the system. Video can be converted into various frames and every frame is encrypted using this system and protect the highly sensitive data which is in the form of video.

REFERENCES

[1] Long Bao, Yicong Zhou* and C. L. Philip Chen, "A lossless (2, 8)-chaos-based secret image sharing scheme", *IEEE 2014.*

[2] Moni Noar, Adi Shamir, Dept of Applied Mathematics and Computer Science Weizmann Institute of Science Rehovot 76100. "Visual cryptography" *Eurocrypt 94, Proceeding LNCS, 950:1–12, 1995.*

[3] G.A.Sathishkumar, Dr.K.Bhoopathy bagan and Dr.N.Sriraam, "Image encryption based on Diffusion and multiple Chaotic map", *International Journal of Network Security & Its Applications (IJNSA), Vol.3, No.2, March 2011.*

[4] Tong Zhang, Yicong Zhou, C.L. Philip Chen(IEEE Fellow), "A New Combined Chaotic System for Image Encryption" *IEEE 2012.*

[5] J. Ramya, B. Parvathavarthini, "An Extensive Review on Visual Cryptography Schemes*" 2014 International Conference on Control, Instrumentation, Communication and Computational Technologies (ICCICCT) IEEE 2014.*

[6] Debasish Jena, Sanjay Kumar Jena, Centre for IT Education, Biju Pattanaik University of Technology, Orissa 751010, India "*A Novel Visual Cryptography Scheme" IEEE 2008.*

[7] Rezvaneh Babazade Gorji, Mirsaeid Hosseini Shirvani, Farhad Ramezani Mooziraji, "A new image encryption method using chaotic map" *JMSET, Vol.. 2, Issue 2, February – 2015.*

[8] Jyoti Rao, Dr. Vikram Patil, Research Scholor of JJTU, Rajasthan, India "Visual Cryptography for Image Privacy protection using Diverse Image media" *IEEE 2015.*

[9] Praveen Kumar. P, Sabitha. S, "User Authentication using Visual Cryptography" *International Conference on Control, Communication & Computing India (ICCC), IEEE 2015.*

[10] Mohan Harshana Perera Ranmuthugala, Chandana Gamage "Chaos Theory Based Cryptography in Digital Image Distribution" *International Conference on Advances in ICT for Engineering Regions (ICTer) IEEE 2010.*

[11] Bruce Schneier "Description of a new Varable-Length Key, 64-Bit Block Cipher Blowfish" *(PDF)*

[12] Shafi Goldwasser and Mihir Bellare "Lecture Notes on Cryptography" *(PDF)*

[13] Hou and Zen-Yu Young-Chang Quan "Progressive Visual Cryptography with Unexpected shares" *IEEE 2011*.

[14] Shiji Johny and Anil Antony "Secure Image Transmission using Visual Cryptography Scheme without Changing the color of the Image" *IEEE 2015*.

[15] Rituraj Roy, Sayantani Bandyopadhyay, Shyamalendu Kandar and Bibhas Chandra Dhara "A Novel 3-4 Image Secret Sharing Scheme" *IEEE 2015*.

[16] Shruthi K Joseph and Ramesh R "Random Grid based Visual Cryptography using a common share" *IEEE 2015*.

[17] K. Shankar and Dr. P. Eswaran "A New k out of n Secret Image Sharing Scheme in Visual Cryptography" *IEEE 2016*.

[18] Vandana Purushothaman and Sreela Sreedhar "An improved Secret Sharing using XOR-Based Visual Cryptography" *IEEE 2016*.

[19] Daoshun Wang, Lei Zhang, Nina Ma and Xiaobo Li "Two secret sharing schemes based on Boolean operation" *Elsevier 2006*.

[20] Barnoli Gupta Barik and Samir Kumar Bandyopodhyay "Secret Sharing using 3 level DWT method of Image Steganography based on Lorenz Chaotic Encryption and Visual Cryptography*" IEEE 2015.*