ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

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

Aartika Chandrakar
M. Tech (Information Security),
Department of Computer Science and Engineering,
DIMAT, Raipur, Chhattisgarh - 492101, India.

Manoj Kumar Singh
Assistant Professor,
Department of Computer Science and Engineering,
DIMAT, Raipur, Chhattisgarh - 492101, India.

Abstract

Information security has become one of the main factors in the field of information technology and communication. The need for information security has increased because of the dependency of individuals and organization on computer has increased. Users highly pay attention on the security of their private information. Cryptography is the science and study of secret writing for achieving security by encoding message to make them non- readable, it is used for secure communication over an insecure communication channel. Visual cryptography is one of the branches 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. Visual Cryptography is used by various critical security issues like identifying the difference between human and machine, scanning, printing, captcha, protecting the biometric data such as Fingerprint images, iris codes and face image.

In the current scenario electronic communication is increased and its usage in E-business has also increased. To keep the information secure we use chaos based visual cryptography, which is the combination of chaos based image encryption and secret image sharing using visual cryptography. So that the useful information or secret information should be protected in a high security level. Using chaotic map we generate chaotic sequence or chaotic stream which are dynamic in nature and by using those sequence we apply visual cryptography for secret image sharing. The whole process is known as chaos based secret image sharing scheme.

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

1. INTRODUCTION

1.1 Overview

This chapter contains all the description and introduction of the preliminaries used in the project. It gives a brief introduction about the different terms used which is related to the main goal of the project, It also includes a brief description about the cryptography, its history and types, different traits used in cryptographic system and also description of the system, how it works through flow chart. This section also contains the outline of the thesis.

1.2 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. Whereas 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 [10].

1.3 Need for information security

In the current environment, organizations 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 organization.

Cite this article as: Aartika Chandrakar & Manoj Kumar Singh, "A Novel Secret Image Sharing Scheme by use of Chaos based Visual Cryptography", International Journal & Magazine of Engineering, Technology, Management and Research, Volume 5 Issue 5, 2018, Page 79-89.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Following are the basic needs for security [10].

- 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 organisation's network can destroy information.

1.4 Cryptography

Cryptography is the science and study of secret writing for achieving security by encoding message to make them non- readable. The basic service provided by the cryptography is to send or receive message between participants in such a way so that unauthorised or unwanted users can not access it. In short it is used for secure communication over an insecure communication channel [11].

Plain text refers to the original text, message or secret image which is to send from one end to another through the communication channel.

Encryption refers to the process of hiding or encoding the original message or information of plain text using encryption key.

Cipher text is the output of the encryption process; it is encoded form of pain text. It is not readable by the unauthorised users.

Decryption is the process by which the original message or plain text is regenerated from the cipher text through decryption key.

Key is a secret string of the characters used for encryption and decryption of the message.

Cryptography is the study of techniques for secure communication in the presence of insecure people or third parties from reading private messages. The aim of cryptography is achieved through encryption and decryption. Encryption is the process of converting ordinary information called plain text into unintelligible text called cipher text. Decryption is the reverse, in other words, moving from the unintelligible cipher text back to plaintext. A cipher is a pair of algorithms that create the encryption and the reversing decryption. The detailed operation of a cipher is controlled both by the algorithm and in each instance by a key. The key is a secret short string of characters, which is needed to encrypt the plain text and to decrypt the cipher text. Key is ideally known only by the communicants [17].

Cryptosystem is the ordered list of elements of possible plain texts, cipher texts, keys, and the encryption and decryption algorithms which correspond to each key. Keys are very important. Ciphers without variable keys can be trivially broken with only the knowledge of the cipher used and are therefore useless. Cipher does not need any additional procedure like authentication or integrity checks, it is directly used for encryption or decryption [11].

There are two types of cryptography, symmetric key cryptography and asymmetric key cryptography.

1.4.1 Symmetric key cryptography

Symmetric key cryptography **is** one of the types of cryptography in which a single key called secret key is used for encryption and decryption both. Secret key is shared by transmitter and the receiver. Encryption of the plain text is done through secret key and then we get the cipher text of the same length as plain text, for decryption also we need the same key as encryption and reverse the process to get the original message which is plain text. Symmetric key cryptography is also referred as secret key cryptography or conventional cryptography [10].

1.4.2 Asymmetric key cryptography

Asymmetric key cryptography is the type of cryptography in which each individual has two keys that is private and public key. Unlike secret key

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

cryptography the key is not shared by the transmitter and receiver. it uses two different keys for encryption and decryption. Public key is used for encryption and private key is used for decryption. Public key is known to everyone and private key is kept secret, it need not to be revealed to anyone. Sometimes it is also known as public key cryptography [1].

1.5 Visual cryptography

Visual cryptography is one of the branches 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 [2]. Here we use human visual system for decryption process. It involved breaking up the image into n shares so that only someone with specific combination of those shares could decrypt the image successfully by overlaying each of the shares over each other. Practically, this can be done by printing each share on a separate transparency and then placing all of the transparencies on top of each other [2].

In the community of information security, visual cryptography is famous because of its special, interesting and different function. The generation model of the secret image sharing is called (k,n) secret image sharing system. In this system the original image is breaking into n shares and the combination of k or greater than k shares will result the successful regeneration of the original image, combination of less than k image shares will result noise like image with no information about the original image.

1.6 Chaotic system

The basic principle of encryption with chaos is based on the ability of some dynamic system to produce sequence of numbers that are random in nature [4]. This sequence is used to encrypt the message, for decryption, the sequence of random number is highly dependent upon the initial condition used for generating this sequence.

1.7 Chaos based visual cryptography

In the current scenario high rate of data is being used through internet, information security has become one of the main factors in the field of information technology and communication [10]. Users highly pay attention on the security of their private information. To keep this information secure we use chaos based visual cryptography, which is the combination of chaos based image encryption and secret image sharing using visual cryptography. So that the useful information or secret information should be protected in a high security level. Using chaotic map we generate chaotic sequence or chaotic stream which are dynamic in nature and by using those sequence we apply visual cryptography for secret image sharing. The whole process is known as chaos based secret image sharing scheme [10].

1.8 Application of Chaos based Visual Cryptography

Visual Cryptography has a very special feature in which the decryption can be performed by the human visual capability [5]. Visual Cryptography is used by various critical security issues like identifying the difference between human and machine, scanning, printing, captcha. In the current scenario electronic communication is increased and its usage in E-business has also increased [3]. It needs high security level while transaction between the two parties and required data protection, that complies increasing utility of network security.

Cryptography is the reliable system when the parties exchanging sensitive business information. E-voting is also an application of the secret image sharing that requires two goals, one is the data should be secure and the other is data should be available [8]. Another application of Visual cryptography is preserving the privacy of digital biometric data [8]. It is used for protecting the biometric data such as Fingerprint images, iris codes and face image.

2. LITERATURE SURVEY

2.1 Overview

This chapter contains all the work done in past related with enhancing or providing security to cryptography. This chapter deals with literature which has already been

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

done while Researching for the Methods to provide Security using visual Cryptography and Chaotic Algorithm.

2.2 Review of related work

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.

3. PROBLEM IDENTIFICATION

3.1 Overview

In this chapter, problem is identified and we discuss about the problem as well as the un-satisfaction in previous work.

3.2 Problem Study

As we discuss earlier about the different method used in the literature review. The research work results the problems we find to solve. The literature review shows detailed methods applied to the cryptographic system using different traits for establishment of a system which successfully transfer the secret information by one end to the other. Here we focus on the system through which a secret image can be transfer using Chaos based Visual Cryptography. We focus on some problems like pixel expansion, low contrast and security issues. In this section we will discuss problems and the solution which is implemented on project to overcome it.

3.3 Problem Identification

We discuss earlier about the different methods used in literature review for different techniques of visual cryptography system. We conclude that some areas can be improved by using different methods and can be apply in future to make a system for better performance.

3.3.1 Pixel Expansion

We have some factors for improvement; one of them is pixel expansion. 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].

3.3.2 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.

3.3.2 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.

3.4 Design & Implementation

In this system we used different algorithm to overcome 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.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

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 processes 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.

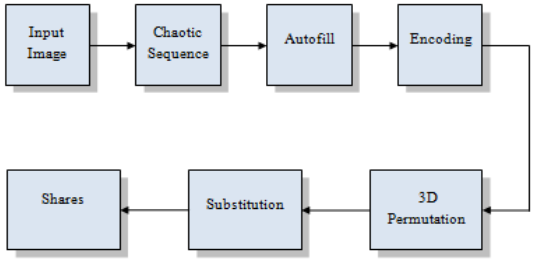

Fig 3.1: Encryption process at the Sender side

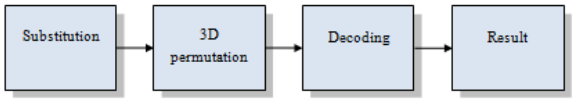

Fig 3.2: Decryption process at the receiver end.

As we see the figure above, the process starts from input image which has to be transmitting secretly and ends with the resulting output image which comes from decoding the shares. We can also justify this image by showing the process through the dataflow diagram. It has two parts one is Generation phase and another is Reconstruction phase.

3.4.1 Description of Generation of shares:

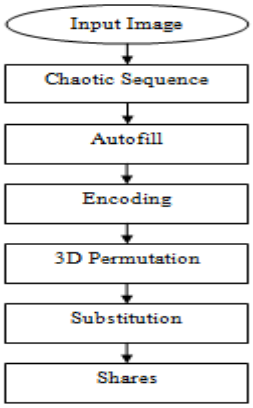

Fig 3.3: Data Flow Diagram of Generation phase.

The dataflow diagram shows how the following steps works during the Generation of shares:

1. Input the image of any type binary, grey or colored.
2. Generate the Chaotic sequence.
3. Arrange that chaotic sequence in the outline of the image.
4. Convert each pixel into binary and encode them into eight shares.
5. Apply 3D Permutation on those shares.
6. Apply a Substitution method.

3.4.2 Description of Reconstruction of image:

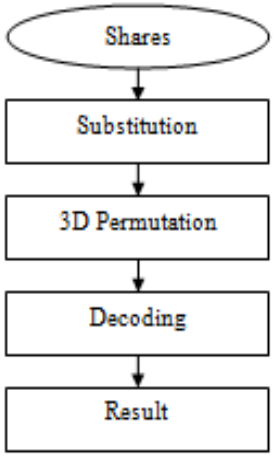

Fig 3.4: Dataflow diagram for Reconstruction phase.

As same as we have another dataflow diagram for the reconstruction of the image which have the steps below:

1. Input the Shares to the system.
2. Perform Substitution process.
3. Apply Inverse 3D permutation process to get the original bit values.
4. Then finally apply Decoding process to combine the shares to get the reconstructed image.

4. METHODOLOGY

4.1 Overview

In this chapter we discuss about the methodology used to make a cryptographic system for secret image sharing. It uses combination of visual cryptography and chaotic sequence.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

4.2 Proposed methodology

Here, we are introducing Secret image sharing using chaos based visual cryptography, in which we are using (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 generate the original image or secret image [1]. To enhance the security of sharing system we added some security hurdles so that the secret image remains secret. Nobody can use those image shares, because the shares are noise like images, no information is shown on those images.

The whole process consists of two phases, the generation phase and reconstruction phase. Generation phase is for creating image shares which are noise like images and send those images through the communication channel and at the receiver end we use reconstruction phase, its reconstruction phase is reverse of the generation phase, to apply the reverse process we will get the original image.

4.3 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; nobody 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 block diagram is as shown in the fig 4.1:

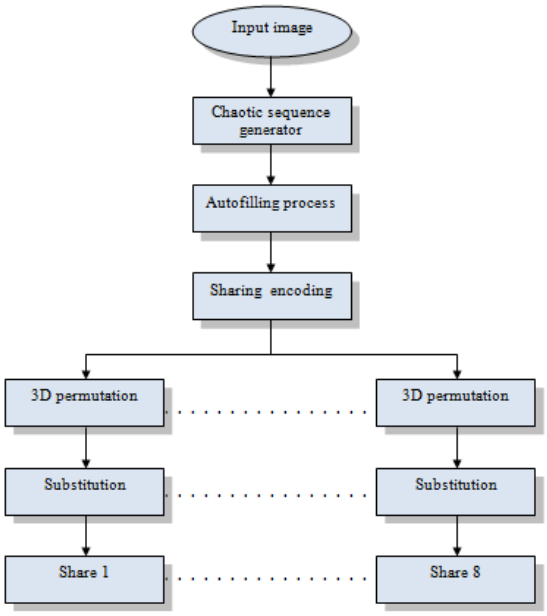

Fig 4.1: The generation phase

4.4 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 consists of decrypting the encrypted format and converts 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 are 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. The block diagram is as shown in the fig 4.6.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

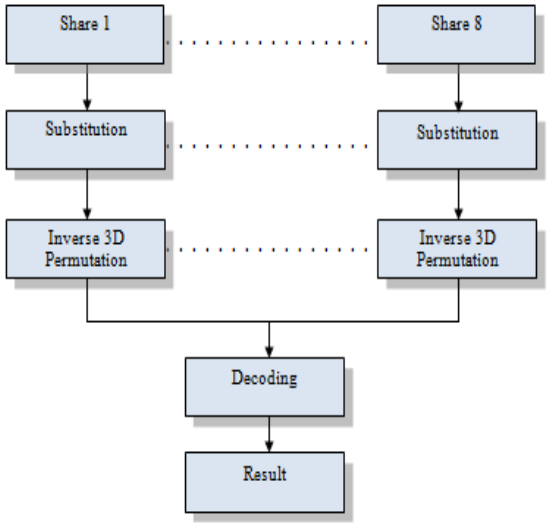

Fig 4.6: The Reconstruction phase

5. EXPERIMENTAL SETUP AND RESULTS

5.1 Overview

This chapter concludes results of the method applied. It also contains a short detail about the methods used for the system.

5.2 Result

This project introduces 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.

The whole process consists of two phases, the generation phase and reconstruction phase. Generation phase is for creating image shares then send those images through the communication channel and the reconstruction phase is used at the at the receiver end, its reconstruction phase is reverse of the generation phase, after applying the reverse process original image will regenerate.

Generation phase consist of five steps including chaotic sequence generation, autofilling, encoding, 3D permutation and substitution. Chaotic map is for generating chaotic sequence or chaotic stream which are dynamic in nature then autofilling process is done by using those sequence after that encode the autofilled image into 8 image shares. After generating shares, 3D permutation process is applied to each image share for changing the position of the pixel values to make it unrecognizable and at last to make it more secure another security hurdle is added which is a substitution method called Blowfish algorithm into the image shares which is a variable length key block cipher.

Reconstruction phase is for regenerating the secret image from the shares without any distortion. This phase is used at the receiver end of the communication system. It consists of decrypting the encrypted format and converts it into the original one. Reconstruction phase consist of three steps including Substitution, Inverse 3D permutation and decoding process. Substitution process is used for decrypting 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 regenerating the original secret image by decode the shares and then extract the chaotic sequence from the background of the image by performing inverse process of autofilling.

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. The stepwise Output of the system while working is given below:

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

5.2.1 The Generation phase

a) Main Page:

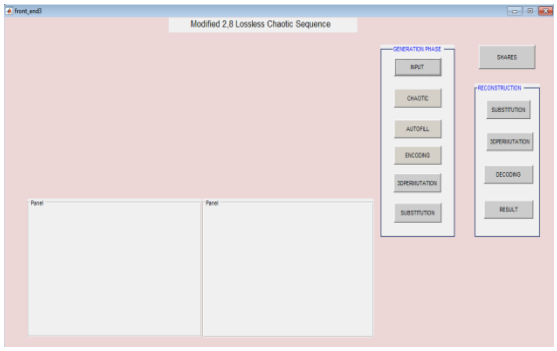

Fig 5.1: Main Page

The above figure shows the main output page of the system.

b) Input of test Image:

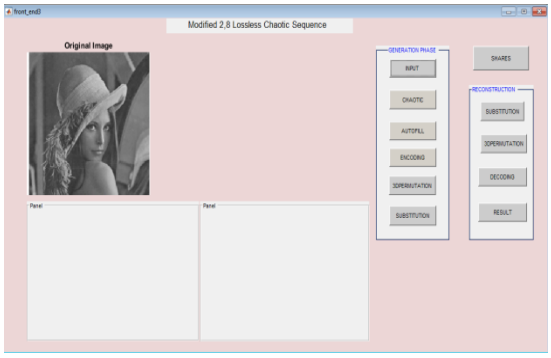

Fig 5.2: Input the test image.

The above figure shows the process of selecting the test image for processing.

c) Autofilling of the image:

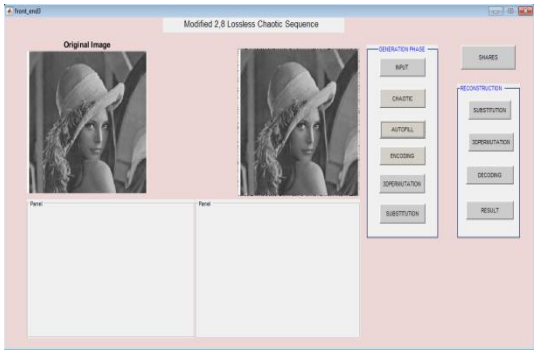

Fig 5.3: Image after applying autofilling process.

Above figure shows how chaotic sequence is added into the background of the test image.

d) Encode the Image into 8 shares:

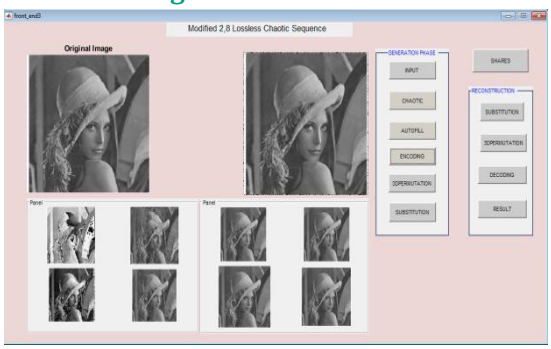

Fig 5.4: Image shares after encoding .

The Figure 5.4 is the next step when the test image is encoded into 8 shares.

e) 3D Permutation:

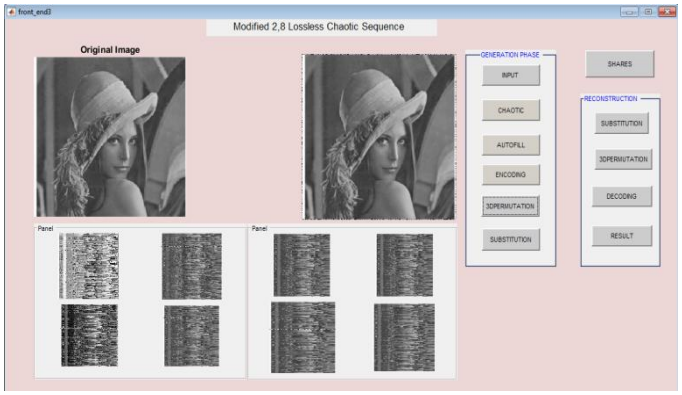

Fig 5.5: Image shares after 3D permutation.

Above figure shows how shares are transformed after changing the pixel position by applying 3D permutation.

f) Encryption through Substitution process:

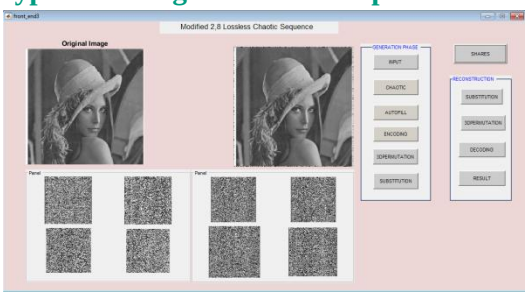

Fig 5.6: Output shares after substitution.

Above figure shows the final output image after encryption using blowfish algorithm.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

5.3.2 The Reconstruction phase

a) Decryption through Substitution process:

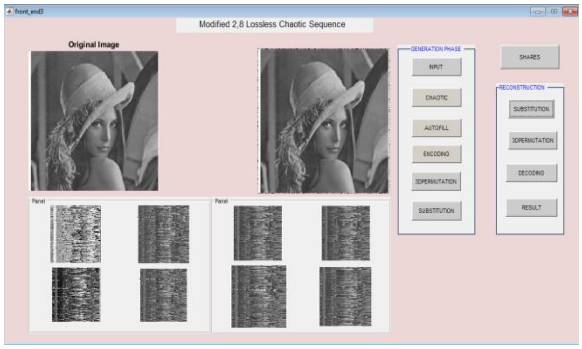

Fig 5.7: Image share after substitution.

Above figure shows the image after decryption in the substitution process.

b) Inverse 3D Permutation:

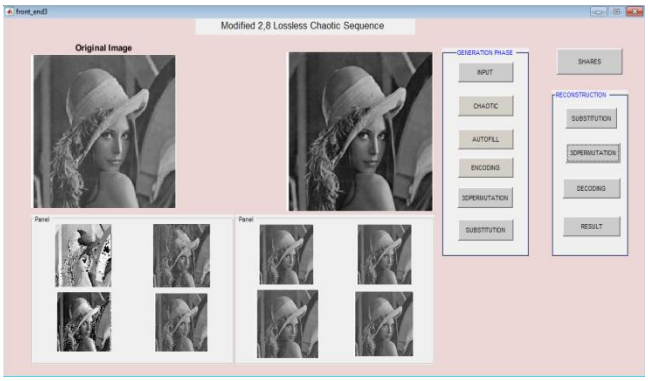

Fig 5.8 Output after inverse 3D permutation.

The original shares are reconstructed after performing inverse 3D permutation process.

c) Decoding shares into a single image:

Fig 5.9: Reconstructed image.

Above figure shows the reconstructed image.

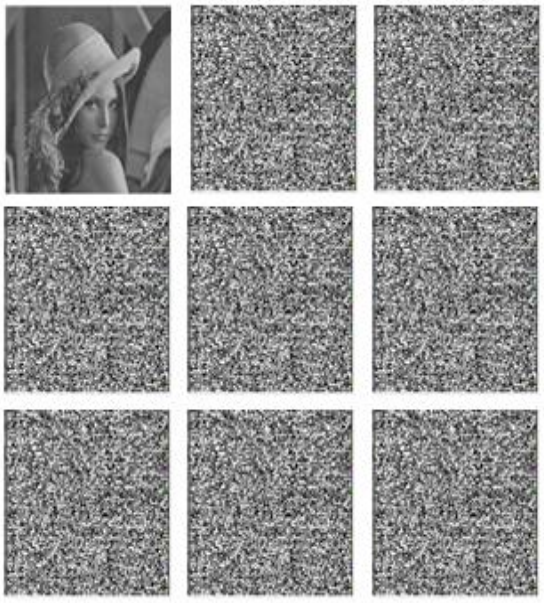

Fig 5.10(a): Input secret grayscale image and its 8 noise like shares

Fig 5.10(b): The Reconstructed image

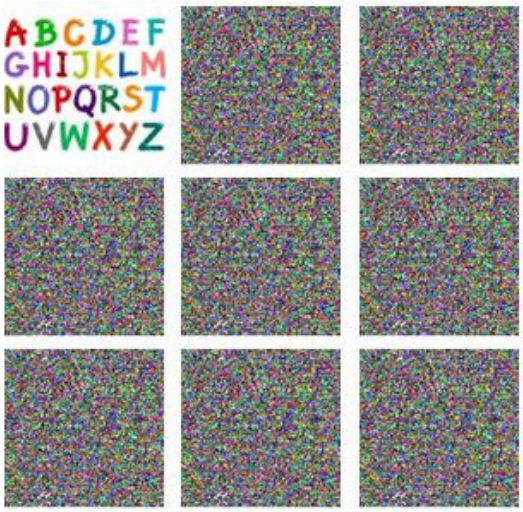

Fig 5.11(a): Input secret colored image and its 8 noise like shares

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Fig 5.11(b): The Reconstructed image

As shown in Fig. 5.10(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. 5.10(b). Another example of colored image shown in fig 5.11(a) and 5.11(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.

6. CONCLUSION AND SCOPE OF 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 organisation, 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] Kunal Kumar Kabi, Chittaranjan Pradhan, Bidyut Jyoti Saha, Ajay Kumar Bisoi, KIIT University, Bhibaneshwar, India, "Comparative study of Image Encryption using 2D Chaotic Map" IEEE 2014.

[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] Sahar Mazloom, Amir-Masud Eftekhari-Moghadam, "Color Image Cryptosystem using Chaotic Maps" IEEE 2011.

[12] F. Liu, C.K. Wu, X.J. Lin, "Color visual cryptography schemes" Vol. 2, No. 4, pp. 151-165, IET Information Security, 2008.

[13] Xing-Yuan Wang, Sheng-Xian Gu, "New chaotic encryption algorithm based on chaotic sequence and plain text" Vol. 8, Iss. 3, pp. 213-216, IET Information Security, 2014.

[14] M. Sangeetha, Vidhyacharan Bhaskar, "PN Codes Vs Chaotic sequences : BER Comparision Prespective" IEEE 2012.

[15] Arun Ross, Senior Member, IEEE and Asem Othman, Student Member, IEEE, "Visual Cryptography for Biometric Privacy" IEEE transactions on Information Forensics and Security, Vol. 6, No. 1, March 2011.

[16] Piyush Marwaha, Paresh Marwaha, "Visual Cryptographic Steganography in Images" Second International Conference on Computing, Communication and Networking Technologies, IEEE, 2010.

[17] Nooka Saikumar, R. Bala Krishnan, S. Meganathan, N.R. Raajan, "An Encryption Approach for Security Enhancement in Images using Key Based Partitioning Technique" International Conference on Circuit, Power and Computing Technologies [ICCPCT], IEEE 2016.

[18] HAN Yanyan, YAO Dong, CHENG Xiaoni, HE Wencai, "VVCS : Verifiable Visual Cryptography Scheme" Seventh International Conference on Computational Intelligence and Security, IEEE 2011.

[19] LU Shou-dong, XU hui, "A New Color Digital Image Scrambling Algorithm Based on Chaotic Sequence" International Conference on Computer and Service System, IEEE 2012.

[20] J. K. Mandal, Mandrita Saha, Pragati Mandal, Madhumita Sengupta, Tandra Pal, Mrinal Kanti Bhowmik, "Adaptive Partial Image Encryption Technique based on Chaotic Map" Fourth International Conference of Emerging Applicationa of Information Technology, IEEE 2014.