Substitution Based (2,8) Chaos Secret ImageSharing Scheme For Enhancing Security In Visual Cryptography- A Review

Somprabha Verma[1] , Dolly Gautam[2]

M. Tech Scholer
[1]Department of Electronics and Telecommunication
Rungta College of Engineering & Technology Bhilai, C.G.
vermasomprabha569@gmail.com

Assistant Professor
Department of Electronics and Telecommunication
Rungta College of Engineering & Technology Bhilai, C.G.
dolly_gautam2009@yahoo.com

Abstract ***Visual Cryptography (VC) is a revolutionary encryption methodology to share the image secret information in a secure way. Secret Image sharing refers to a cryptographic technique in which secret image is divided into a number of share images with or without modification and the secret image can be retrieved by combining all or predefined collection of share images. In this project introduces a (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. In this project substitution process is using with permutation process which gives excellent performance for security of secret image. Index Terms Visual Cryptography, Secret Image Sharing Scheme, chaotic Map, 3D Permutation.***

Keywords: Visual Cryptography, Secret Image Sharing Scheme, chaotic Map, 3D Permutation**.**

1. Introduction

With rapid growth of networking technology, digital data can be transferred easily over the Internet. But security and protection of sensitive digital information during transmission is a great concern in commercial, medical and military applications. Two methods cryptography and data hiding have been used to increase the security of the digital data such as images. Nevertheless, one of the common vulnerabilities of both these methods is single point of failure (SPOF) as they use single storage mechanism and therefore data can be easily misplaced or damaged. The concept of secret sharing was developed many years back, when Adi Shamir has shown this idea in his paper in1979. Secret image sharing schemes (SISS) are useful options. The basic idea behind secret sharing is to transform a secret into n number of shadows or shares that can be carried and stored disjointedly. The secret can only be restored from any k shadows ($k \leq n$) and any (k-1) or fewer shadows cannot reveal anything close to that secret. Naor & Shamir shows a new concept using images in the paper "Visual Cryptography". They extend their new scheme to secret sharing problem. That paper is the seed of the visual cryptography and visual secret sharing and every work was published in this area with the reference of this paper. After this basic concept many researcher find out different schemes for the visual cryptography. Cryptography is the science or study of techniques of secret writing and message hiding. Cryptography is as broad as formal linguistics which means from those without formal training. It is also as specific as modern encryption algorithms used to secure transactions made across digital networks. Cryptography constitutes any method in which someone attempts to hide a message. The basic service provided by cryptography is the ability to converters: send information between participants in a way that prevents others from reading it [2]. In a core banking Chaotic cryptography describes the use of chaos theory to perform different cryptographic tasks in a cryptographic system. Chaos theory deals with systems that evolve in time to a particular kind of dynamical behavior [9]. Visual Secret sharing scheme, there is a secret picture to be shared among n participants. The picture is divided into n transparencies (shadows) such that if any m transparencies are placed together, the picture becomes visible. However, if fewer than m transparencies are placed together, or analyzed by any other means; nothing can be seen. Visual Secret Sharing scheme uses mathematical secret sharing but implements in hardware, printed on transparencies. It once created, it requires no technology, and however resolution and contrast is lost [3]. In this project, it introduced a new chaos-based secret image sharing scheme combining the chaos-based image encryption with the secret image sharing. In this project permutation and substitution operations of cryptography will be used which is highly secure the secret images transition.

2. Literature Review

Visual cryptography is a cryptographic technique which allows visual information (pictures, text, etc.) to be encrypted in the way that decryption becomes a mechanical

operation. Visual Cryptography utilizes two transparent images. One image contains random or noisy pixels and the other image contains the secret data. It is almost impossible to retrieve the secret information from encrypted images. Both transparent images and layers are required to reveal the information. The easiest way to implement a Visual Cryptography is to print the two layers onto one transparent sheet [7].

The advantage of visual cryptography scheme is that it eliminates computation problem during decryption process, and the secret image can be restored by stacking operation. This property makes the visual cryptography especially useful for the low computation method. The visual cryptography scheme was introduced by Naor & Shamir 1994. It is a secret sharing scheme with good security for binary image. Another distinguished advantage of this is that it decodes directly during human vision. There are different levels of visual cryptography techniques. In this paper we will discussed the work done on the

a. Binary images
b. Gray Images
c. Color Images.

A. Randomized Visual Secret Sharing Scheme application was suggested where the customer has to present the share during all of his transactions. The (2, 2) randomize visual cryptography in practice where the shares are generated based on pixel reversal, random reduction in original pixel and subtractions of the original pixel with previous shares pixel. The original secret image is divided in such a way that after OR operation of qualified shares and reveals the secret image. In the (3, 3) visual secret sharing scheme shares are generated based on pixel reversal, random reduction in original pixel and subtractions of the original pixel with previous shares pixel and storing the final value of the share pixel after reversal into the shares in round robin fashion. The result of the three shares and after OR operation using stacking of all these qualified shares the original secret reveal. Schemes have shown less pixel expansion which is desirable and good for the final retrieval of the secret image. Some contrast is change and impairments are still visible in the results of these schemes. However by dividing the pixels into two or more sub pixel retrieve the secret picture with more impairments and bad resolutions. However size of pixel increases provides more easiness for alignment of the shares. This is the still researchable area to reduce this effect [3].

B. Based On Substitution Cipher

Visual Cryptography is basically a cryptographic method in which decryption is performed by human visual system. In this paper, present a novel visual cryptography scheme based on a substitution cipher and random grid. The scheme uses two-fold encryption. In the first fold of encryption, Caesar cipher is used to encrypt the image row wise and then column wise using a key of the size equal to the greatest common devisor of the number of rows and columns in the secret image. Then a random matrix is generated and the transformed secret image is XOR end with this random matrix to enhance the security. The scheme is shown to be secure and decryption is also lossless. In this scheme author has used substitution technique. To increase the security further, some invertible combination of substitution and permutation can be applied [6].

C. Improved Grayscale Visual Information Security

The proposed scheme extends the 2 out of 2 basic visual secret sharing method into Improved Gray Scale Visual Secret Sharing (IGVSS) scheme using dynamic threshold method. The proposed algorithm helps to generate high quality meaningful share images. Future studies should therefore investigate on 3D visual cryptography with higher visual quality of the reconstructed secret images [5].

D. Error Diffusion in Forward And Backward Direction

This paper work is an implementation of improved halftone visual secret sharing scheme by applying a new error diffusion filters that distribute error in both forward and backward direction to improve the visual quality of the recovered secret image in experimental Results shows that the recovered image obtained using proposed error diffusion filter are much better than existing error filters and proposed error filter gives maximum values for PSNR, NCC, UQI than others. It is complex computational process for reconstruct the secret image [2].

E. Encryption Using Chaos Theory

Compared with the single chaotic map scheme, the proposed algorithm will exhibit higher security. Due to the structure similar to the style of block cipher, the proposed algorithm can complete the encryption of two pixel blocks at one time, which is helpful for increasing data throughput. The security analysis shows that the method can resist many forms of cryptanalysis. An image encryption scheme based on chaotic standard map is proposed. Bit level permutation not only changes the locations of the image pixels, but also modifies their values. Such a design can enhance the randomness, even under finite precision implementation. Due to features of bit level permutation, proposed a bit level confusion and dependent diffusion to enhance the security of cryptosystem [1].

F. Chaos based Visual Cryptography

The generation model of secret image sharing is called the (k, n) secret image sharing which generates n differentimage shares. Only when the number of utilized shares islarger than or equal to k, the successful reconstruction ofthe original secret image will be achieved. Otherwise,combining less than k image shares yields a noise-like image with no information about the original secret image.This paper introduces a new (2, 8)-secret image sharingscheme integrating the chaos-based image encryption withsecret image sharing. It divides the secret

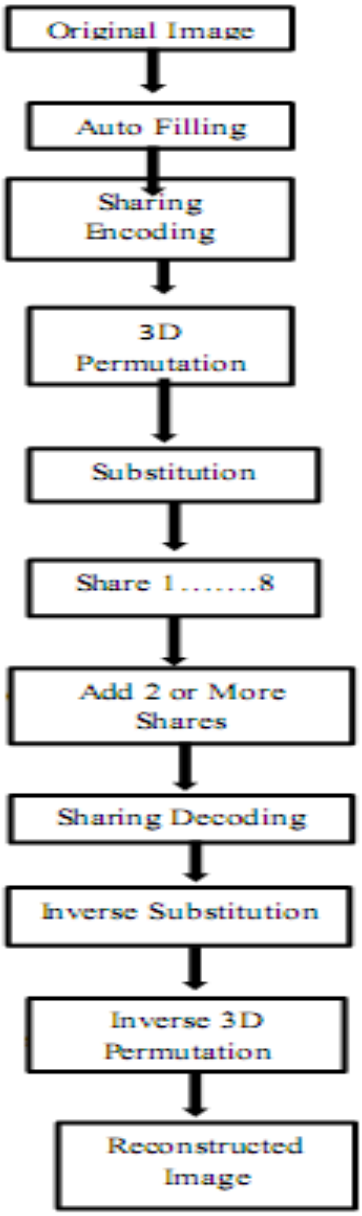
image into 8encrypted shares. Combining any two or more shares is able to completely reconstruct the secret image without anydistortion. Each image share is only one pixel larger than the secret image in row and column directions. This scheme is able to directly process the secret images with various formats such as the binary, grayscale, and color images [4].

3. Proposed System

Secret image sharing is an effective scheme which provides confidentiality and integrity of the sensitive image. But in previous method only permutation encryption operation is used for securing the secret image in visual cryptography secret image sharing scheme. A single encryption process does not give perfect high level of security for secure images like government details, military, biomedical etc. In this project, a new chaos-based secret image sharing scheme combining the chaos-based image encryption with the secret image sharing is proposed. The proposed method is able to protect the original secret image with a high level of security. It can transform the secret images into eight image shares in which any two or more shares are able to completely reconstruct the original secret image without any distortion Figure 1: The proposed (2, 8) substitution
image sharing scheme. (a) The generation phareconstruction phase.

3.1 Generation Phase

The generation phase of the proposed at transforming the original secret image into s like shares. It consists of 4 steps: auto-fil encoding, 3D Permutation and substitution. secret image is with a size of W×L. Auto Filling The auto filling process first uses a chq a random generator to produce a chaotic sequence has the same data range of the secret image a of 2W+2L+4. This random sequence is one-t unpredictable. It is then put in the surround original secret image to produce a new image A) with a size of (W+2) × (L+2).



3.2 Sharing Encoding

The image A is decomposed into 8 bit planes, namely A1, A2, A8, where Ai (1≤ i≤ 8) is the it bit-plane.

3.3 3D Permutation

Eight bit-planes of each image form a 3D binary matrix. The 3D permutation is to change all data positions
within this binary matrix. As a result, the positions and pixel values are changed. Each image share becomes unrecognized visually.

3.4 Substitution Process

The encryption process also needs to be dynamic in order to face new technique and more advance methods seed by cryptanalysis. Substitution box (s-box) is keystone of modern symmetric cryptosystem .They bring on

linearity to cryptosystem and strengthen their cryptographic security. In this paper RC4 algorithm which well known stream cipher is used to generate S-box for advance encryption standard (AES). The generated S-boxes re more dynamic and key dependent which will increase he complexity and also make the differential and linear cryptanalysis (DC&LC) more difficult. Various andomness tests are applied to the customized AES (AES-RC4) algorithm and the results shown that the new design ass all tests which proven its security.

3.5 Secret Reconstruction Phase

Because the proposed VCSISS is a (2, 8) scheme, any two shares can reconstruct the original image without any distortion. The CSISS reconstruction phase is an inverse process of its share generation phase. It consists of wok steps: the sharing decoding and inverse 3D permutation. As defined in Equation, the sharing decoding uses two Shares E1 and E2 with the size of (W+2) × (L+2) to reconstruct the image R.

4.Security Analysis

Compare different techniques of transferring visual secret image on the basis of their security and encryption techniques.

TABLE I. Security Provided By Different Visual Cryptography Techniques.

Visual Cryptography Techniques	Methods	Security
Only substitution based	Substitution	Medium
Only permutation based	Permutation	Medium
Randomized visual secret sharing scheme	Randomized pixels and shares generation	Medium
Chaos theory	Permutation and substitution	High
Chaos based secret sharing scheme	Chaos map and permutation	High
Substitution based chaos secret sharing scheme (proposed method)	Chaos map, permutation and substitution	Very high

5. Conclusion

To address these VC problems in this paper, introduce a new chaos-based secret image sharing scheme to deal with various types of secret images, including the binary, gray-scale and color images. The proposed method is able to protect the original secret image with a high level of security. It can transform the secret images into eight image shares in which any two or more shares are able to completely reconstruct the original secret image without any distortion. It is a combination of the chaos-based image encryption and secret image sharing. Hence, the original secret images can be protected with a high security level and can be completely reconstructed without any data loss. Moreover, compared with traditional VC methods, the proposed scheme will generates the image shares with a similar size as the original secret image and thus saves a large amount of storage and transmission costs.

References

[1] Minal Govind Avasare ,Vishakha Vivek Kelkar, "Image Encryption using Chaos Theory", IEEE, 2015 International Conference on Communication, Information & Computing Technology (ICCICT), Jan. 16-17, Mumbai, India.

[2] Aman Kamboj, D.K.Gupta, "An improved Halftone Visual Secret Sharing Scheme for gray-level imagesbased on error diffusion in forward and backward direction", IEEE.

[3] Shubhra Dixit, Deepak Kumar Jain , Ankita Saxena, "An Approach for Secret Sharing Using Randomized Visual Secret Sharing", IEEE 2014, Fourth International Conference on Communication Systems and Network Technologies.

[4] Long Bao, Yicong Zhou* and C. L. Philip Chen, "A lossless (2,8)-chaos-based secret image sharing scheme", IEEE 2014, International Conference on Systems, Man, and Cybernetics October 5-8, 2014, San Diego, CA, USA.

[5] A. John Blesswin , Dr. P. Visalakshi " An improved gray scale visual secret sharing scheme for visual information security" , IEEE 2013, Fifth International Conference on Advanced Computing (ICoAC).

[6] Gyan Singh Yadav, Aparajita Ojha, "A Novel Visual Cryptography Scheme Based on Substitution Cipher", IEEE 2013, Second International Conference on Image Information Processing (ICIIP-2013).

[7] Ms. Bhawna Shrivas, Prof.Shweta Yadav, "A Survey on Visual Cryptography Techniques and their Applications", Bhawna Shrivas et al, / (IJCSIT) International Journal of Computer Scienceand Information Technologies, Vol. 6 (2) , 2015, 1076-1079.

[8] Harinandan Tunga, "A New Secret Coloured Image Encryption and Decryp-tion Scheme based on (2, 2) Visual Cryptography Scheme (VCS)", International Journal of Computer Applications (0975 – 8887) Volume 101– No.12, September 2014.

[9] Dao-Shun Wang, Tao Song, Lin Dong, and Ching-Nung Yang, "Optimal Contrast Gray scale Visual Cryptography Schemes With Reversing" , IEEE Transactions On Information Forensics And Security, Vol. 8, 2013.

[10] Aarti, Pushpendra K Rajput, "A Novel Multi Secret Sharing Scheme with MSB Extraction Using EVCS", IEEE 2013.

[11] Surya Sarathi Das, Kaushik Das Sharma, Jitendra Nath Bera, "A Simple Visual Secret Sharing Scheme Employing Particle Swarm Optimization", IEEE 2014 International Conference on Control, Instrumentation, Energy & Communication(CIEC).

www.ijsr.net
IJSR
ISSN (Online): 2319-7064