Visual Cryptographic Technique for Enhancing the Security of Image Transaction

Akshatha M M, Lokesh B, Nuthan A C

Student, Dept. of ECE, SIT, Mangalore, India

Associate Professor Dept. of EEE, SIT, Mangalore, India Jain University, Bangalore, India

Research Scholar, SIT, Mangalore, India Jain University, Bangalore, India

ABSTRACT: As the growth in the technology increases maintaining the security of visual information during its transaction has to be increased. Rapid growth in the techniques for doing so is also increasing. Internet has become most commonly used media for communication and hence text, voice, video, Images and many more are transmitted through Internet. These might include Military Secrets, Commercial Secrets and Information of individuals and therefore it has to be transmitted by safer means with enhanced security. In the process of Visual Cryptography a secret image is encrypted into shares which refuse to divulge information about the original secret image. In this paper, Chaotic Pseudo – Random Number generation, Zigzag Scan Pattern Method, Method to reduce the degradation of the resultant image is proposed by an extension from gray to colour image. Pixel Index Method is discussed to improve the security for images. An integration of this technique of Visual Cryptography with (n, k, p) gray image is also proposed.

KEYWORDS: Security, Visual Cryptography, Visual Secret Share.

I. INTRODUCTION

Cryptography refers to the study of mathematical techniques and related aspects of information security like data confidentiality, data integrity and of data authentication. In the process of Visual Cryptography a secret image is encrypted into shares which refuse to divulge information about the original secret image. Decryption is through a separate decryption algorithm. A basic model for Visual Cryptography for natural images was proposed by Naor and Shamir, where the resultant image is twice the size of secret image.

As the advent of electronic applications increases, providing the security for information in an open network environment is required. Encryption is a method of transforming original data, called plain text or clear text into a form that appears to be random and unreadable which is called Cipher text. Plain text is either in the form that can be understood by a person (document) or by a computer (executable code).

Once it is transformed into Cipher text, neither human nor machine can properly process it until it is decrypted. This enables the transmission of confidential information over insecure channels without unauthorized disclosure. When data is stored on a computer it is protected by logical and physical access controls. When this same sensitive information is sent over a network,the information is in much more vulnerable state. Naor and Shamir introduced the new concept of Visual Cryptography in 1994[1], requiring no computation except human Visual System to decrypt. They proposed a basic (2,2) Visual Cryptography scheme where a secret image is divided into 2 shares, revealing the secret image through Share Stacking.
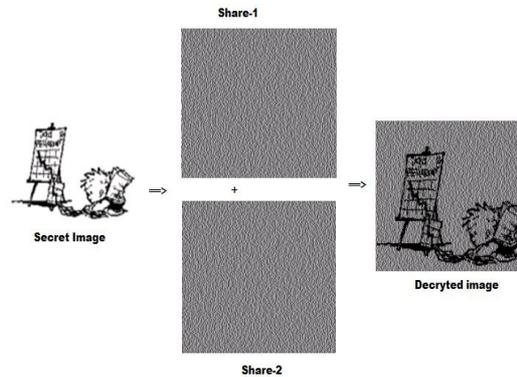
Fig. 1 Example of Visual Cryptography

In figure 1 a secret image that has to be sent is divided into shares. When these two shares are stacked together and put into a Human Visual System the resultant image is revealed.In the visual secret sharing model [1], a secret picture must be shared among n participants. The picture is divided into n shares so that if m transparencies (shares) are placed together the picture is visible. When there are fewer m transparencies it is invisible. This ensures that the secret picture is viewed as a set of black and white pixels with each pixel being handled separately.

II. RELATED WORK

2.1 Basic (2,2) Scheme

The (2, 2) VC scheme divides the secret image into two shares so that reconstruction of an image from a share is impossible. Each share is printed in transparency. A share is a random noise. Encryption is performed for each pixel. Fig.2 shows the 2 different shares for black and white pixels. The figure shows how a pixel in a image in divided into two sub pixels depending on whether the pixel is black or white. By doing so the width of the share increases. This is termed as Pixel Expansion.

Fig. 2 A (2,2) Visual Cryptography Scheme

Figure 2 shows the problem of Pixel expansion where a Pixel in the image is divided into 2 sub pixels which increase the width of the entire image and thus there will be increase in bandwidth required and so increase in the power consumption.

2.2 Pseudo Randomized Visual Cryptography Scheme

Figure 3 shows how the shares are generated by pixel reversal and using pseudo random technique. Each pixel is being handled separately. The input is a secret image and the output is the shares. Here there is no pixel expansion. The decoded image and the original secret image are of the same sizes. But the secret image which is decoded had a darker resolution than the original image. Pre-processing technique was used to overcome this problem.
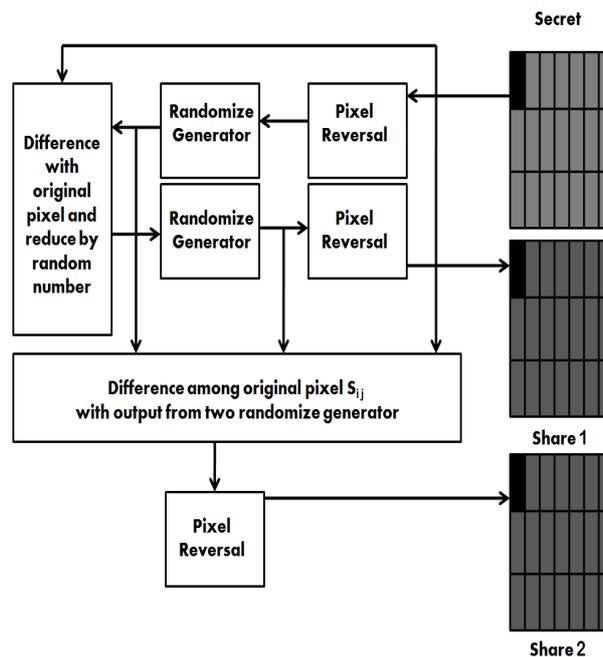

Fig. 3 Pseudo Random Scheme

Figure 3 shows the elimination of problem of pixel expansion and the generation of share 1 and share 2 for a gray image.

III. PROPOSED WORK

In this paper, the problem of pixel expansion is eliminated and also a method is proposed for color image usage and thus the degradation of the resultant image is reduced. A secret image is taken and is split into RGB components. Each component is handled separately. Each pixel is decomposed using Bit Plane Decomposition technique. ATMF and De – noising is done to eliminate the presence of noise. This result is then encrypted using Chaotic Random Number Generator and the bit planes are re – ordered and Re – combined. Pixel Index Reversal is done to reverse the index of the pixel to improve the Security. At this stage Zigzag Scan Pattern is applied to increase the scrambling, thus increasing the Security. The output after the Scan is then applied to Pseudo Random Scheme as shown in Figure 3.
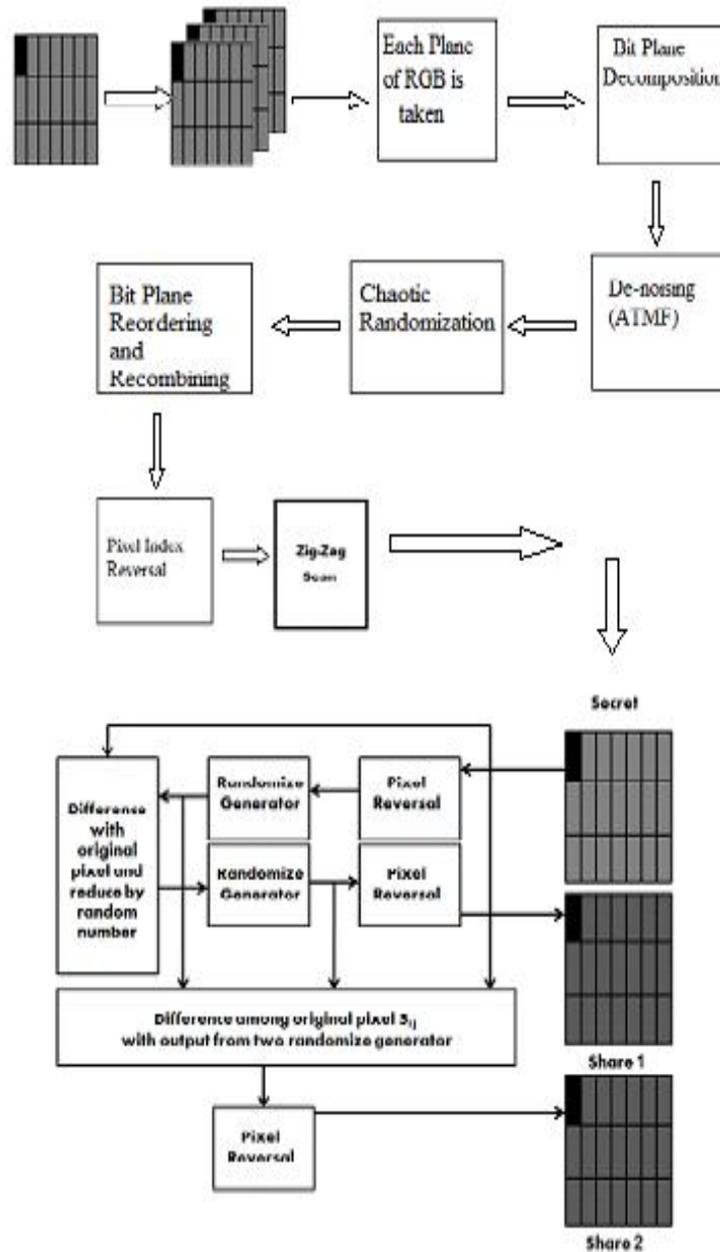
Figure 4: Integration of VC with (n, k, p) Gray Image

Figure 4 shows the integration of concept of Visual Cryptography with pixel index reversal, Zigzag Scan of the image for a colour image with its integration with (n, k, p) gray codes.

3.1Simulations and Results

The algorithm is implemented in MATLAB. Figure 5 shows the experiment results for the gray image.

Fig. 5 Results for gray image as input   Fig. 6 Results for Colour Image as input

Figure 5 shows the result for the basic concept of Visual Cryptography for a Gray Image. Figure 6 shows the results for the basic concept of Visual Cryptography for a Colour Image.
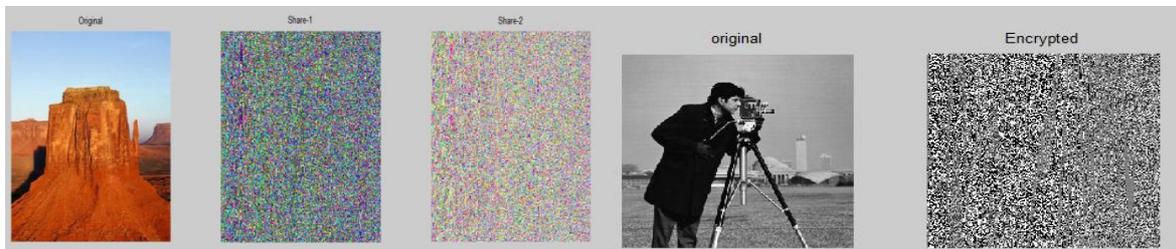

Fig. 7 Results for Colour Image after applying the Security Methods   Fig.8 Completely Encrypted Image

Figure 7 shows the results of the encryption and generation of shares after applying the security measures like Pixel Index reversal, Scan pattern method, Chaotic randomization. Figure 8 shows the integration of Visual Cryptographic concept with (n, k, p) gray code concept.

3.2 Comparison of the Algorithms

Table.1 Comparison of Algorithms

Algorithm	Pixel	Security	Quality
Naor, Shamir	Double	Increase	Poor
(k,n) scheme	Double	Increase	Poor
Existing Method	No Expansion	Increase	Increase
Proposed Work	No Expansion	Increase	Color Image

The above table shows the comparison of the existing and proposed techniques of Visual Cryptography.

IV. CONCLUSION AND FUTURE WORK

The security increases as the scrambling is more. The time consumption is also in terms of Nano seconds and hence this method can be applicable in most of the fields. The problem of pixel expansion is also eliminated. Future work can include the application of this technique for 3D images. Some technique can be made to improve the quality of resultant image and also to reduce the power consumption. Video Encryption using the same method can be worked out.

REFERENCES

1. Adi Shamir, "How to Share a Secret", published in ACM, Laboratory for Computer science, Massachusetts Institute of Technology, 1979.
2. Naor M. and Shamir A, "Visual cryptography" , In Proc. Eurocrypt 94, Perugia, Italy, May 9–12, LNCS 950, Springer Verlag, 1994, 1–12.
3. " What are Visual Secret Sharing Schemes"General concept.
4. Giuseppe Ateniese, Carlo Blundo, Alfredo De
   Santis, and Douglas R. Stinson, "Visual Cryptography for general access structure", ICALP'96, Italy, 1996
5. Frank Stajano, "Visual Cryptography Kit", Computer Laboratory, University of Cambridge, 1998, http://www.cl.cam.ac.uk/~fms27/vck/
6. Zhi Zhou, Gonzalo R. Arce and Giovanni Di Crescenzo, "Half tone Visual Cryptography", IEEE Transaction on image processing, vol.15, no.8, 2006.
7. StelvioCimato, Alfredo De Santis, Anna Lisa , Ferrara, Barbara Masucci, "Ideal contrast visual cryptography schemes with reversing", Information Processing Letters, Elsevier.
8. Jim Cai, "A Short Survey On Visual Cryptography Schemes", 2004.
9. M.Naor and A.Shamir. "Visual cryptography II: Improving the contrast via the cover base". Theory of Cryptography Library, (96-07), 1996.
10. M.Naor and A.Shamir "Visual cryptography, advances in Cryptology". Eurocrypt 94 Proceeding LNCS, 950: 1–12, 1995.
11. Ch. RatnaBabu, M.Shridhar , Dr. B. RaveendraBabu "Information Hiding in a Gray Scale Image using Pseudo – Randomised Visual Cryptography Algorithm for Visual Information Security", IEEE, 2013.
12. Yicong Zhou, Karen Panetta, SosAganian, "(n, k, p) Gray Code for Image System", IEEE Transaction on Cybernetics, vol.43, No.2, April 2013.

BIOGRAPHY

Akshatha M M: Completed her BE under Visvesvaraiah Technological University, Belgaum in Electronics and Communication Engineering. At present she is pursuing her M. Tech degree under the same university in VLSI and Embedded Systems.

Lokesh B: is the Associate Professor and HOD in the department of Electronics and Electricals in SIT, Mangalore. He is also a research scholar under Visveswaraiah Technological University, Belgaum.

Nuthan A C: Completed his BE in Electronics and Communication Engineering and M. Tech in Digital Electronics under Visvesvaraiah Technological University. At present he is working as Assistant Professor in the department of Electronics and Communication in GMIT, Mandya. He is also a research scholar under Jain University, Bangalore.