A New Procedure of Visual Cryptography for Maintaining the Security of Visual Information Transaction using Java Based Approach

Krishna Kumari & ShashiYadav *Deptt. of Computer Science and Engg., India*[*Krishnadhankhar1992@gmail.com*](mailto:Krishnadhankhar1992@gmail.com)

Deptt. ofComputer Science and Engg., India
Yadavshashi8feb@gmail.com

ABSTRACT:

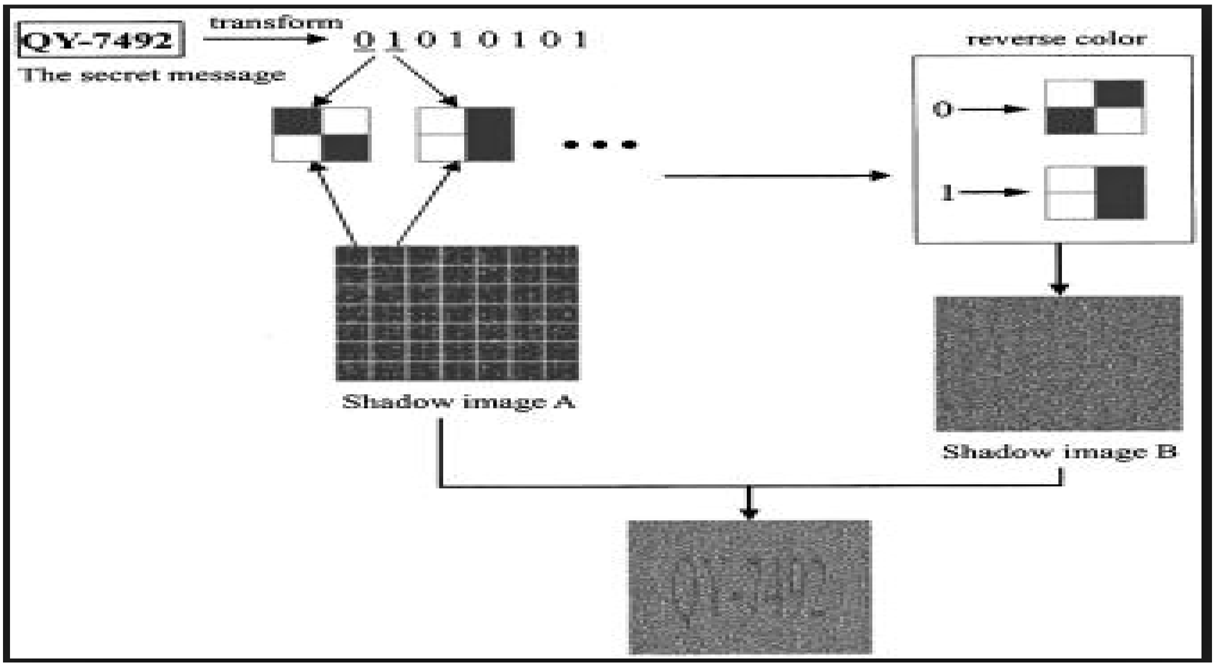
Rapid growth in the techniques for doing so is also increasing. Internet has become most commonly used media for communication and hence text, voice, video, Images and many more are transmitted through Internet. As the growth in the technology increases maintaining the security of visual information during its transaction has to be increased. 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. These might include Military Secrets, Commercial Secrets and Information of individuals and therefore it has to be transmitted by safer means with enhanced security. Pixel Index Method is discussed to improve the security for images. The Secret whose text format subjected to encryption using substitution cipher and the resultant encrypted text were embedded into the image. When the shares on transparencies are superimposed exactly together the original secret can be discovered without computer participation. Our idea aims at Visual cryptography which provides a very powerful technique by which one secret can be distributed into two or more pieces known as shares.

Keywords: Security; Visual Information; Visual Cryptography

1. INTRODUCTION

In the process of Visual Cryptography a secret image is encrypted into shares which refuse to divulge information about the original secret image. Cryptography refers to the study of mathematical techniques and related aspects of information security like data confidentiality, data integrity and of data authentication. Decryption is through a separate decryption algorithm 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. . 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. 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 inmuch 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. .Our idea aims at Visual cryptography which provides a very powerful technique by which one secret can be distributed into two or more pieces known as shares. The Secret whose text format subjected to encryption using substitution cipher and the resultant encrypted text were embedded into the image. When the shares on transparencies are superimposed exactly together the original secret can be discovered without computer participation.



EXAMPLES OF VISUAL CRYPTOGRAPHY

In figure 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, 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.

2. 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 ashare 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 an 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.

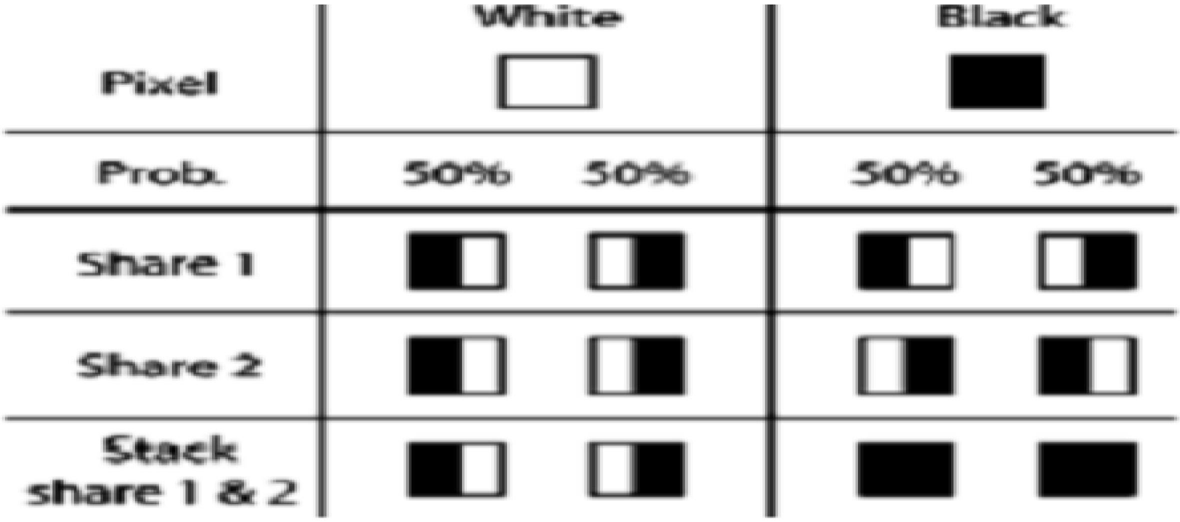


Fig. 2 A (2, 2) Visual Cryptography Scheme

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.

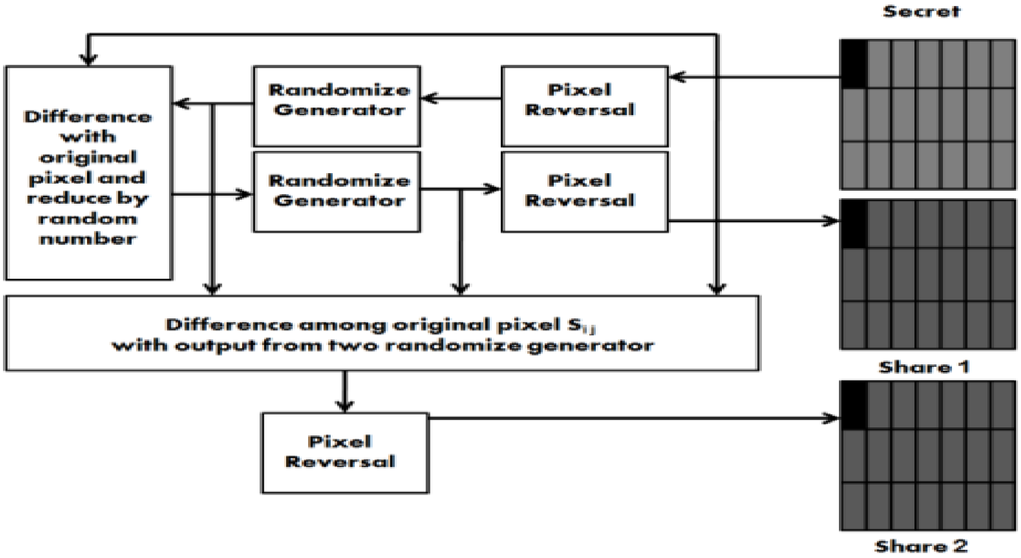

Secret
Difference with original pixel and reduce by random number
Randomize Generator
Pixel Reversal
Randomize Generator
Pixel Reversal
Difference among original pixel S_{ij} with output from two randomize generator
Share 1
Pixel Reversal
Share 2

Fig. 3 Pseudo Random Scheme

3. PROPOSED WORK

In this paper, the problem of pixel expansion is eliminated and also a method is proposed for colourimage 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.

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. Conventional visual secret sharing schemes generate noise-like random pixels on shares to hide secret images. It suffers a management problem, because of which dealers cannot visually identify each share. This problem is solved by the extended visual cryptography scheme (EVCS), which adds a meaningful cover image in each share. However, the previous approaches involving the EVCS for general access structures suffer from a pixel expansion problem. In addition, the visual cryptography (VC)-based approach needs a sophisticated codebook design for various schemes. In this paper, we propose a general approach to solve the above-mentioned problems; the approach can be used for binary secret images in no computer-aided decryption environments. The pro- posed approach consists of two phases. In the first phase, based on a given access structure, we construct meaningless shares using an optimization technique and the construction for conventional VC schemes. In the second phase, cover images are added in each share directly by a stamping algorithm. The experimental results indicate that a solution to the pixel expansion problem of the EVCS for GASs is achieved. Moreover, the display quality of the recovered image is very close to that obtained using conventional VC schemes.

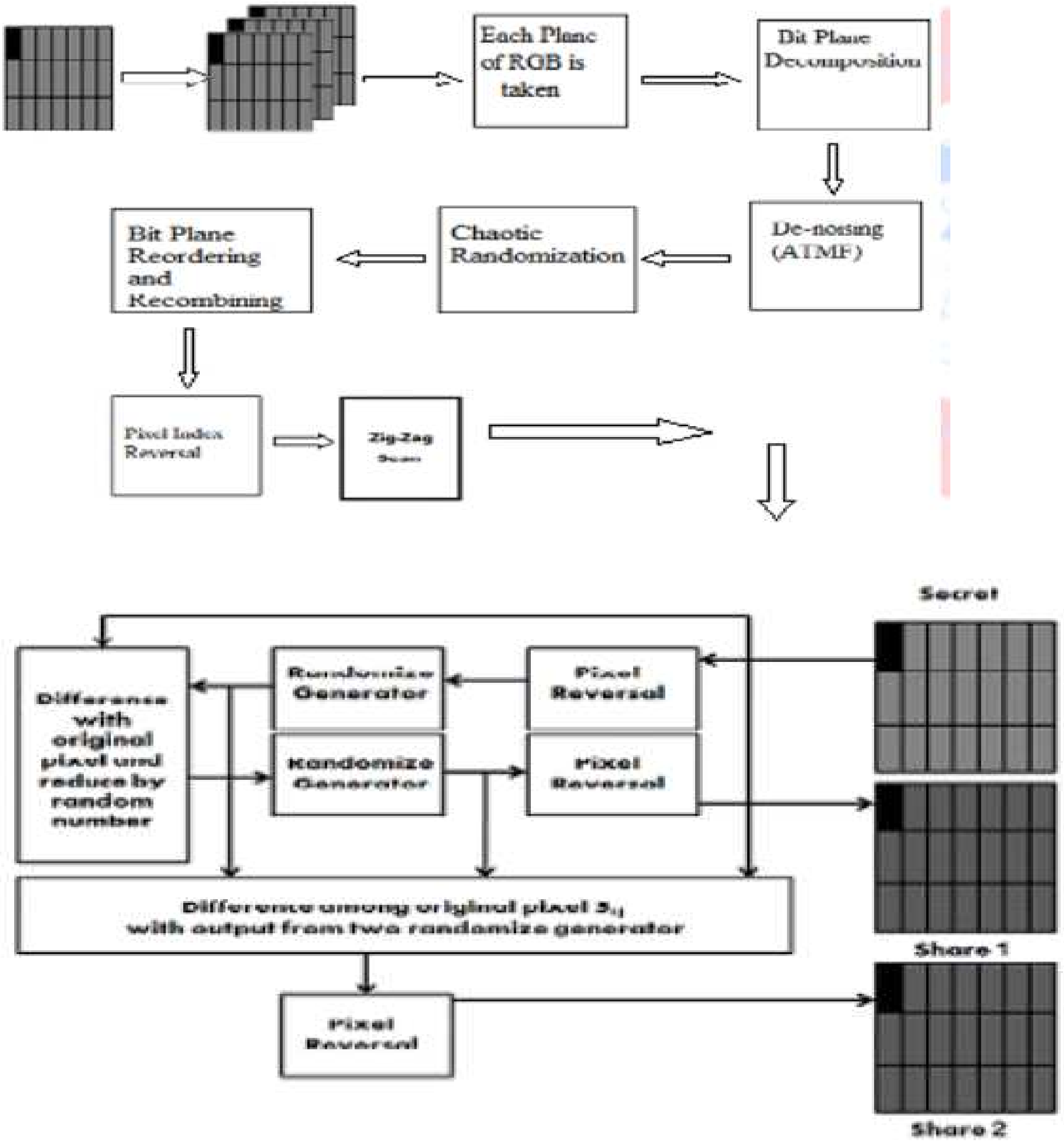

Each Plane of RGB is taken
Bit Plane Decomposition
De-noising (ATMF)
Chaotic Randomization
Bit Plane Reordering and Recombining
Pixel Index Reversal
Zig-Zag Scan
Secret
Difference with original pixel and reduce by random number
Randomize Generator
Pixel Reversal
Randomize Generator
Pixel Reversal
Share 1
Difference among original pixel s_{ij} with output from two randomize generator
Pixel Reversal
Share 2

Figure 4: Integration of VC with (n, k, p) Gray Image

3.1 SIMULATIONS AND RESULTS The algorithm is implemented in MATLAB. Figure 5 shows the experiment results for the gray image:

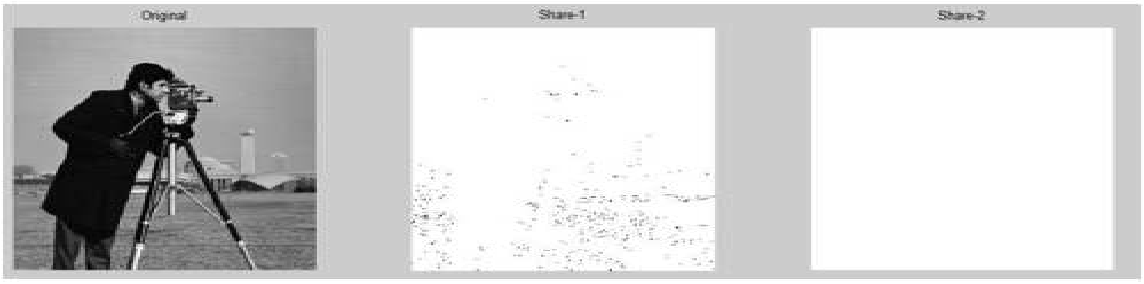


Fig. 5 Results for gray image as input

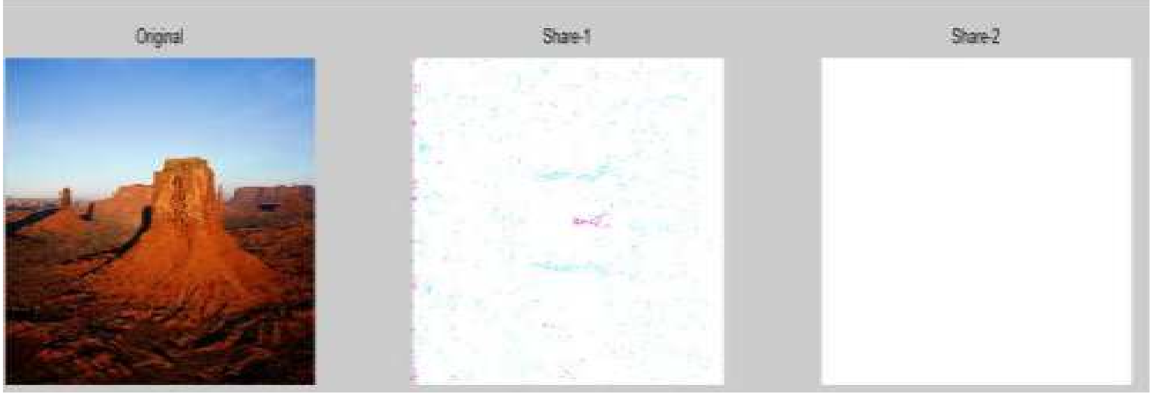


Fig. 6 Results of Color Image As Input

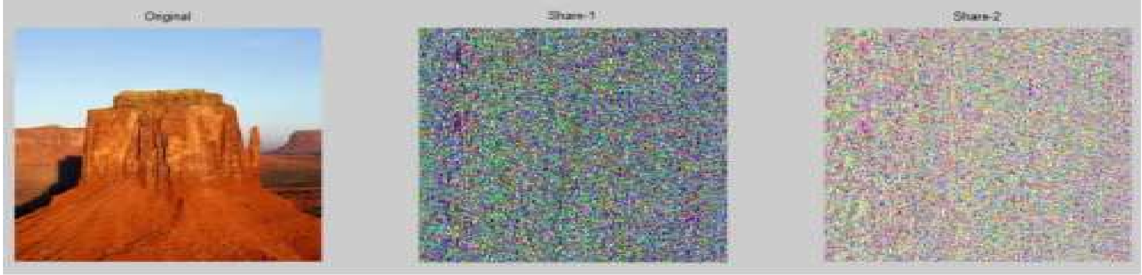


Fig. 7 Results for Color Image after applying the Security Methods

3.2 COMPARISON OF 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

4. 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.

5. REFERENCES

[1] Naor M. and Shamir A, "Visual cryptography".

[2] "What are Visual Secret Sharing Schemes "Generalconcept?

[8] System".

[3] Frank Stefano, "Visual Cryptography Kit", Computer Laboratory, University of Cambridge.

[4] Jim Cain, "A Short Survey On Visual Cryptography Schemes", 2004.

[5] M.Naor and A.Shamir "Visual cryptography, advances in Cryptology".

[6] 6. Ch. Ratna Babu, M.Shridhar , Dr. B. Raveendra Babu "Information Hiding in a Gray Scale Image using Pseudo – Randomised Visual Cryptography Algorithm for Visual Information Security".

[7] Yicong Zhou, Karen Panetta, Sos Aganian, "(n, k, p) Gray Code for Image