An Enhanced Visual Cryptography

Piyali Ghosh
Jain Deemed to be University, Kanakpura, Bangalore

Abstract- *An Enhanced Visual cryptography is a cryptographic technique to achieve visual secret sharing. Shares are distributed to every participant and overlapping a number of shares can recover the original secret. We are reviewing four shares in this project. This system can be used to hide the original image information from an intruder or an unwanted user. The images can be in any standard format. Information is to be protected and a binary image used as key to encrypt and decrypt are taken as input. Here, a secret image which needs to be communicated is decomposed into four monochromatic images. The encrypted image is sent to the destination through the network and then the image is decrypted. Here, we are using Symmetric-key cryptography.*

Keywords- Visual Cryptography, Secret shares, Symmetric key cryptography, Matrix algorithm.

I. INTRODUCTION

In 1994, a new cryptographic paradigm, called visual cryptography or visual secret sharing (VSS), was introduced by Naor and Shamir.

Basic Visual Cryptography (VC) is used for secured transfer of images, handwritten documents, financial documents, text images, topological maps used in military operations, satellite communication etc. in a secured manner. This is a method of encrypting a Secret image into shares such that stacking a sufficient number of shares reveals the secret image. Shares are nothing but the binary images of the secret image.

The decryption can be performed by simply stack the shares over each other and view the secret image that appears on the stacked shares by human visual system. The simplest way to implement Visual Cryptography is to print the two layers onto a transparent sheet.

Halftoning is a technique of generating binary images from gray scale images. This technique is used in various applications such as laser printing, facsimile (FAX) etc.

An Enhanced Visual Cryptography (VC) is used for secured transfer of images, handwritten documents, financial documents, text images, topological maps used in military operations, satellite communication etc. in a secured manner. In this paper we have implemented for two shares and reviewed for four shares.

Share generation of the binary image from the secret image is followed by the watermarking technique, which provides the additional security over the basic visual cryptography scheme.

We will generate the shares using basic visual cryptography model and then we will generate the compliment images of the cover image over which, the shares of the secret image will be embedded. The decryption will be done by the human visual system.

In section 2 we will discuss the basic visual cryptography system, threshold scheme and its basic approach . Proposed work is discussed in section3. We will discuss the proposed algorithm for generation of binary images from secret image in section 4.The simulation result is discussing in section 5 and finally conclude the whole text in section 6 and also mention the future enhancement of this work.

II. VISUAL CRYPTOGRAPHY SYSTEM

Visual Cryptography is an encryption technique that hide the information (images, text) when it is transmitted over the communication channel, which can be decrypted easily by human visual system without using any decryption algorithm.
Visual cryptography scheme (VCS) is basically a secret-sharing scheme which means the generation of share images of secret images that are transmitted over the channel. The decryption of the secret image does not require the prior knowledge about cryptography nor requires any complex computation. The secret image can be obtained only by stacking required number of shares on to each other.

It can encrypt a black-and-white secret image into n shares, which are transmitted over the channel. Depending on the type of threshold scheme the required numbers of shares out of n number are stacked together to get back the secret image.

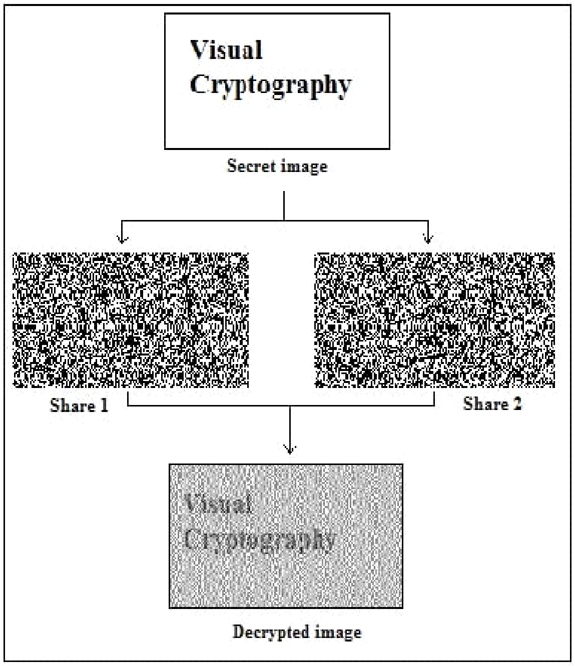


Fig. 1: Simple Visual Cryptography Scheme

2.1 THRESHOLD SCHEME

(2, 2) – Threshold VCS:

This is the simplest threshold scheme in which a secret image is encrypted into two different shares. Then it reveals the secret image that shares and stacked on to each other.

(2, n) – Threshold VCS

In this scheme the secret image is encrypted into n number of shares and it is transmitted over the channel. At the receiver end when two or more shares are stacked over each other, then secret image will be revealed back.

(n,n) – Threshold VCS

In this scheme the secret image is encrypted into n number of shares and when only n number of shares are stacked together then only secret image can be revealed back.

(k, n) – Threshold VCS

In this scheme the secret image is encrypted into n shares and when at least k numbers of shares (or more) are stacked together then only secret image can be revealed back.

2.2 APPROACHES FOR PIXEL GENERATION

Basic visual cryptography scheme for generation of shares is based on the breaking of pixel into subpixels or expansions of pixels. In Fig. 1 pixel is expanded into 2 sub pixels.

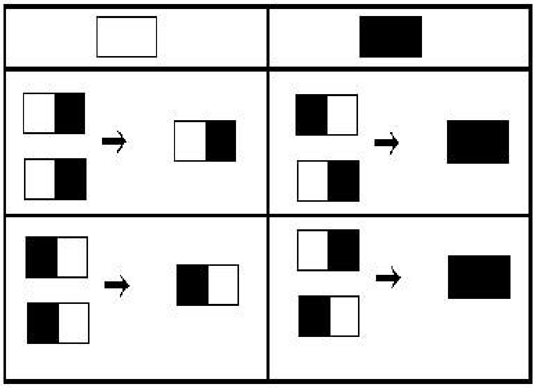


Fig. 2(a): View of white and black pixel in resultant shares.

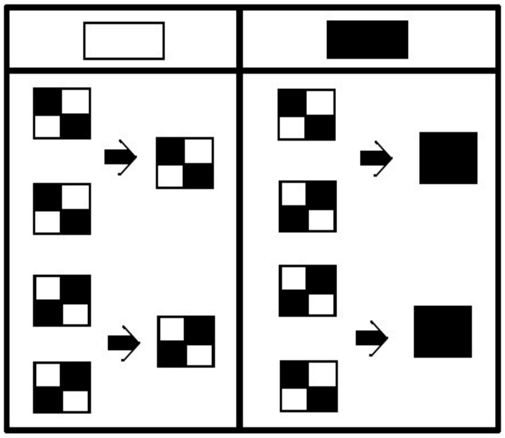


Fig. 2(b): Alternative view of resultant shares.

In Fig. 2, pixel is broken into 4 sub pixels. There are six different encryption rules ($^4C_2$=6 cases) for both white as well as black pixel. By using symmetric key cryptography, encryption is done by splitting the white (or black) pixel into two shares. Decryption can be done by simply overlapping of two shares, which will give the secret image as a result.

For encryption any one rule is chosen and accordingly white or black pixels are spitted into 2 shares. For decryption just overlapping (stacking) of two shares are required which provide the secret image as a result.

Ran-Zan Wang [7] proposed Region Incrementing Visual cryptography for sharing visual secrets in multiple secrecy level in a single image.

III. PROPOSED WORK

The proposed work is basically a framework design with two modules :

1. Data Hiding using multiple bits replacement scheme and
2. Visual Cryptography using Multi-layer Multi-shares method. An input image is accepted as a cover image for the secret image to be hidden.

The original picture(information) is revealed by placing the shares with the key over the page with the cipher, even though each one of them is indistinguishable from random noise. The model for visual secret sharing is as follows. There is a secret picture(information) to be shared among n participants. The picture is divided into n shares such that if the required number of shares are placed together, the picture becomes visible. If fewer than the total number of shares are placed together, picture is not seen. The word cryptography is derived from two Greek words which mean “secret writing”. Cryptography is the process of rearranging the original text by scrambling and substituting the original text, arranging it in an unreadable format for others.

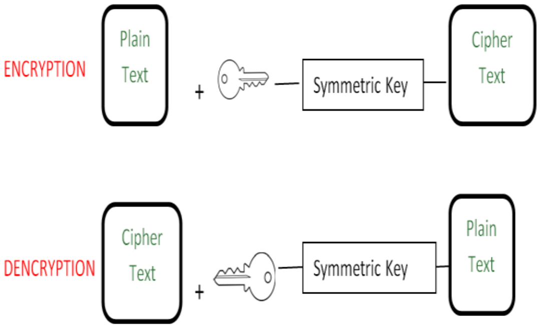
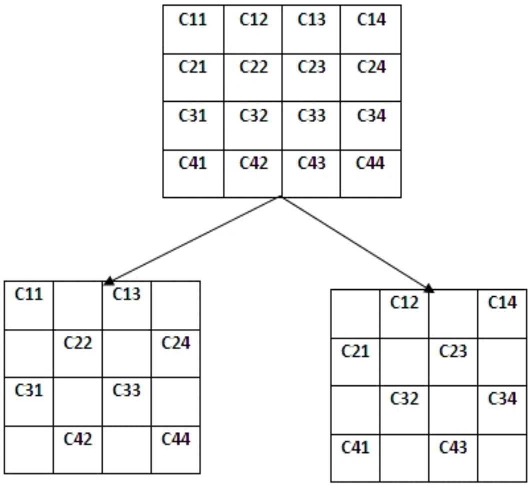


Fig 3: System design

IV. PROPOSED ALGORITHM

4.1 GENERATION OF COMPLIMENT IMAGES OF COVER IMAGE:

Here in this section the proposed concept of generation of compliment images of a cover image is given, which are used for embedding the shares of secret image. The advantages of this concept are discussed in the later section.



C11	C12	C13	C14
C21	C22	C23	C24
C31	C32	C33	C34
C41	C42	C43	C44

C11		C13	
	C22		C24
C31		C33	
	C42		C44

	C12		C14
C21		C23	
	C32		C34
C41		C43	

Fig. 4: View of the cover being spitted into two compliment images

Here, as shown in the Fig. 3, the cover image is splitted into two images. The two images hence obtained are compliment to each other in a sense that none of their pixel content matches, but when combined together they result in the original secret image.

4.2 MATRIX ALGORITHM

We have secret as an n-bit binary string, and we want to split this key into say two shares in such a way that no single share reveals information about the secret.We define the two shares in the following way:

· Share 1 is n-bit randomly generated string.
· Share 2 is Share 1 XOR secret.

Now shares can be simply recomputed by Share 1 XOR Share 2. Let’s consider the following case as an example. n= 5

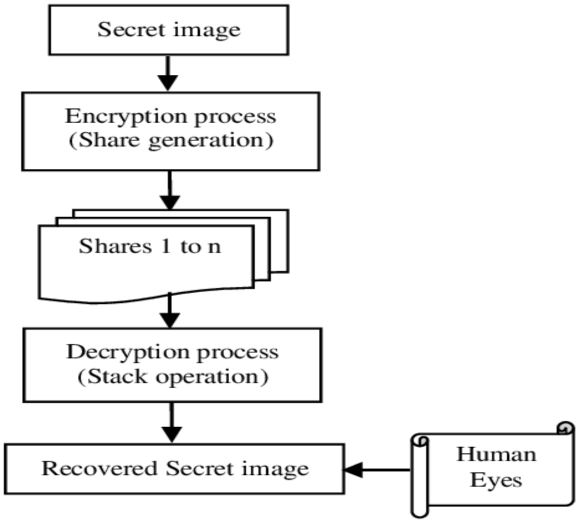


Fig 1: Basic flowchart of Visual Cryptography

Secret= 10100
Share 1= 01101
Share 2= 11001

White pixel is identical matrix and looks like this:

$$\begin{bmatrix} 0 & 1 \\ 0 & 1 \end{bmatrix} \text{ or } \begin{bmatrix} 1 & 0 \\ 1 & 0 \end{bmatrix}$$

Black pixel is complementary and looks like this:

$$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \text{ or } \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

2 out of N Visual Sharing Scheme :

For a (2, n) VCS, the solution is obtained as follows for S0 and S1:

S0 – It is the matrix which has all rows of column 1 set as 1 and all other cells as 0. S1 – It is the identity matrix. From these S0 and S1 , the collection C0 is obtained by all permutations of S0 and C1 is the collection of all permutations of S1 .

- For each pixel a different permutation is used hence confusion is introduced.
- This confusion adds to the security of the algorithm.

Secret image

Secret image is the image which has to be secured in a communication between two parties.

Encryption Process

The secret image is encrypted during the communication by dividing the secret image into n shares. In this project we are implementing for two shares and reviewing about generating 4 shares of

Fig 5: Block Diagram

the secret image along with encryption of each share within a host image.

Shares 1 to N

N shares i.e, small bits of secret image are generated.

Decryption Process

All the generated N shares has to be combined together i.e., stacked to get back the secret image.

Recovered Secret image

The image is recovered by decryption and can be seen by human eyes.

Following three phases of proposed algorithm:

PHASE 1:

In the First phase of the algorithm the basic visual cryptography scheme is carried out. We will generate the shares S1 and S2 from the binary image. Each share is generated as a result of this phase is meaningless if we consider the share independently.

PHASE 2:

In the Second phase the embedded images with the help of compliment images of the secret (cover) image is generated. Let the cover image be C and its complimented images are C1 and C2.

Then four embedded images X11, X12, X21, X22 are generated which are to be transmitted to the destination through transmission channel. These shares can be generated by simply embedding the shares S1 and S2 over the compliments of cover image i.e. C1 and C2.

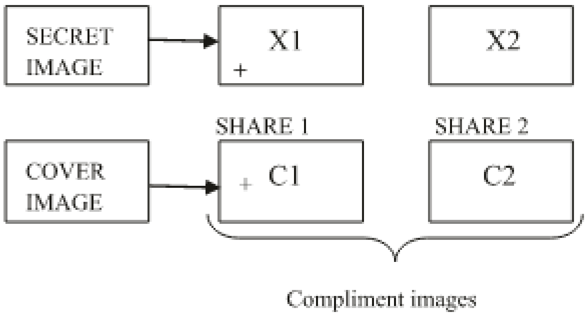


Fig. 6(a): Proposed scheme structure

X11= EMBEDDED(S1,C1)
X12= EMBEDDED(S1,C2)
X21= EMBEDDED(S2,C1)
X22= EMBEDDED(S2,C2)

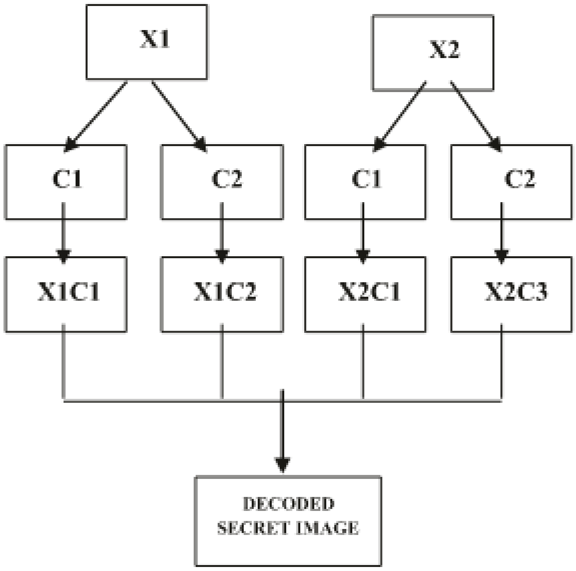


Fig. 6(b): Proposed scheme structure

PHASE 3:

The last phase of our proposed algorithm is marked by the decryption process. Visual decryption process is simply done by human visual system without using any hard complex computations. The images obtained from the second phase in which shares are embedded over the compliment images are simply stacked over each other that reveals back to the original secret image.

4.3 BENEFITS

In the given following points we are highlights the advantages of our proposed algorithm.

- Simplicity of application of this scheme is one of its major merits.
- Security standard is increased comparing to that provided by conventional visual cryptography scheme.

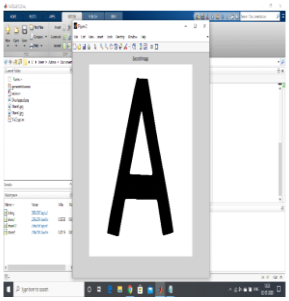
V. SIMULATION RESULT

The Proposed algorithm is implemented and tested on simulator, which is developed in visual studio dot Net platform. Simulation result of proposed work is shown in Fig.7. Figure 6(b) depicts the sequence that we have followed to obtain the desired output.

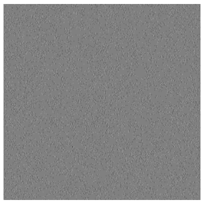
Following are the Snap shots of experimental results:-

- **INPUT:**

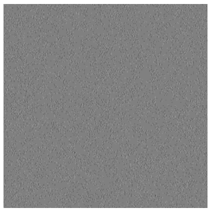
Selection of Secret image



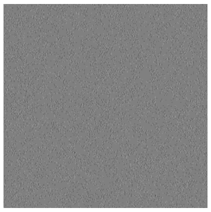
- **OUTPUT:**



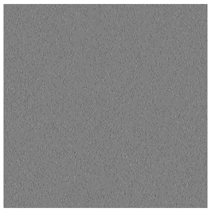
Share 1



Share 2



Share 3



Share 4

Overlapping of shares

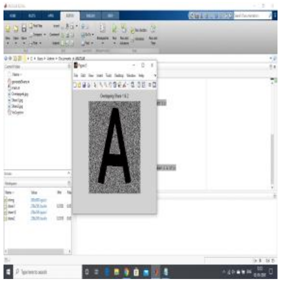


Fig. 7: Simulation result of proposed scheme

Proposed work provides generation of 4 shares instead of 2 shares for more security of the image during a communication. The result includes the secret image, shares and decoded secret image.

VI. CONCLUSION

In this paper we have discussed a new algorithm to enhance the security in visual cryptography system using Matrix algorithm to produce the meaningful shares from the secret image. In this project, we have presented an image cryptographic scheme based on visual cryptography for natural images. This is a review on generating four shares. Hence, the confidentiality is maintained and the authentication can be checked by digital signatures. The work has every scope of development from every angle and hence will be highly effective. This algorithm may used in many fields like military operation in battle field, authentication and validation of remote voting system, satellite transmission of text data, hand written document and image transmission. Our future work is to develop quantitative analysis of this algorithm in the terms of quality, contrast, reliability and clarity of the final decoded secret image that is directly decrypted by human visual system without using any decryption algorithm, so that human save money and time .

REFERENCES

[1] Jena Debasish, Jena Sanjay K., “A novel visual cryptography scheme” 978-0-7695-3516-6/08 © 2008 IEEE.

[2] M. Naor and A. Shamir, “Visual cryptography”. Advances in Cryptology EUROCRYPT, Lecture Notes in Computer Science, (950):1–12, 1995.

[3] G. Ateniese, C. Blundo, A. De Santis, and D. R.Stinson, Visual Cryptography for General Access Structures, Information and Computation, Vol. 129,No. 2, pp. 86-10, .(1996)

[4] Zhongmin Wang and Gonzalo R. Arce, “Halftone visualcryptography through error diffusion”, ISBN 1-42440481-9/06 © 2006 IEEE, pp.109-112.

[5] Digital Image Processing Laboratory: Image Halftoning” April 30, 2006. Purdue University.

[6] Hsu Ching-Sheng and Tu Shu-Fen,, “Digital watermarking scheme with visual cryptography”, Proceedings of the International MultiConference of Engineers and Computer Scientists 2008 Vol. I IMECS 2008, 19-21 March, 2008, Hong Kong

[7] Wang, R.Z.[Ran-Zan], Region Incrementing Visual Cryptography, SPLetters(16), No. 8, August 2009,pp. 659662.