A Unique visual cryptographic mechanism for hiding secret message in an Image

Pankaj Rakheja, Sneha Bhatia, Aditi Lakra

Abstract— Security of the information following in a network vulnerable to numerous attacks is a matter of great concern in todays world. Cryptography is a branch of science which deals with making the information non readable to avoid unauthorized access only the one who know about encoding process and key can decrypt it. Visual cryptography is a technique where visual information in form of text, image etc is encrypted in such a way that decryption does not need computer as it is just a mechanical operation. Here in this paper we have tried to modify the existing visual cryptographic schemes to make it more effective. More the degree of uncertainity in a cipher mechanism better it is , our designed mechanism hides the secret message in Image by LSB insertion method in a random fashion which makes it highly effective and results show that cover image and watermarked image are almost identical.

Index Terms— cipher, decryption, encryption, LSB, MSB, share, watermark

1 INTRODUCTION

Protecting data in a safe and secure way is an immensely difficult and important research problem, cryptography easily solves this problem**.** Now a days the transmission of data through computer network is increasing rapidly. So the security of transmitted data is very important issue. To provide the security to transmitted data we can use Cryptography. It consists of two main algorithms
1) Encryption algorithm and
2) Decryption Algorithm.
Encryption algorithm is used to convert the information into unreadable cipher data. Decryption algorithm is used exactly reverse of the encryption algorithm. Above processes require the computation knowledge to recover the secret information.

Cryptography is the techniques for secure communication in the presence of third party. Cryptography is used for securing data during transmission.
Cryptography [1] [2] uses two main styles or forms of encrypting data; symmetrical and asymmetrical. Symmetric encryptions, or algorithms, use the same key for encryption as they do for decryption. Other names for this type of encryption are secret-key, shared-key, and private-key. The encryption key can be loosely related to the decryption key; it does not necessarily need to be an exact copy.

Visual cryptography [3-6] [8] is a cryptographic technique which allows visual information (pictures, text, etc.) to be encrypted in such a way that decryption becomes a mechanical operation that does not require a computer. One of the best-known techniques has been prposed by Moni Naor and Adi Shamir in 1994.
Visual cryptography provides a very powerful technique by which one secret can be distributed into two or more shares. When the shares on transparencies are superimposed exactly together, the original secret can be discovered without computer participation.

2 OVERVIEW

In the following scheme we have used various method for a reliable encryption of the data. All the methods used in our scheme has been discussed briefly.

Share generation deals with generating 'n' shares of the black and white image to be encrypted. Here we have used the simplest access structure which is the 2 out of 2 scheme where the secret image is encrypted into 2 shares and both needed for a successful decryption. These shares are random dots without revealing the secret information.
The back pixel is denoted by 1 and white pixel as 0.

Element division is the technique in which every image is divided into two arrays one with the elements at odd positions and the other with elements at even position.

Manchester encoding is one of the digital encoding technique that is are introduced for security of data and fast transmission.. It is quite different from other digital encoding techniques because each data bit length is fixed by default. The bit state is determined according to the transition direction. Different systems represent bit status in different ways, but most systems represent 1 bit against low to high transition and 0 bit for high to low transition. Signaling synchronization is the major advantage of Manchester encoding. Synchronization of signals provides higher reliability with the same data rate compared to other methods. But programmers should note that Manchester encoding has some disadvantages too. For example, the Manchester encoded signal consumes more bandwidth than the original signal.

Manchester encoding has the following characteristics:

- Each bit is transmitted in fixed time.
- A '1' is noted when high to low transition occurs; 0 is expressed when a low to high transition is made.
- The transition that is used to note 1 or 0 accurately occurs at the mid-point of a period.

Digital Watermarking- have been proposed recently as the means for ownership protection of multimedia data. Represents a watermarking-based visual cryptography scheme with meaning-

ful shares is to embed a hidden watermark message into a host object such that the hidden message is inseparable. Earlier watermarking was applied to text only. Now days watermarking is applied to all types of media. The scheme does not change the original pixel expansion, and not only applies for black and white binary images, but also for any gray and color images. Meanwhile, the embedded image in a meaningful share is robust. Before and after being extracted the image's quality did not change significantly. The scheme is easy to implement and highly feasible. There are many research articles exploring the watermark method Digital watermarking is applied to video also to stop piracy which results in loss of revenue. There should be no perceptible difference between the watermarked and original signal, and the watermark should be difficult to remove or alter without damaging the host object.

Digital Watermarking stages:
1) Embedding a watermark
2) Attempt to remove/distort watermark
3) Detection of the watermark

Introduction of digital watermarking technology, we propose a new visual cryptography scheme while share image as a digital watermarking imbeds into a meaningful picture.
After scheme structure and experimental simulation, the scheme has the following advantages-

(1) **Transparency**: the embedded watermark pattern does not visually spoil the original image fidelity and should be perceptually invisible. Meaningful share image can avoid the aware of active attackers.
(2) **Pixel expansion unchanged**: compared to the previous schemes proposed in the literatures, the scheme does not change the original pixel expansion.
(3**) Robustness**: the watermark pattern is hard to detect and remove in an illegal way.
(4) **Portability**: the scheme not only applies for black and white binary images, but also for any gray and color images.
(5) **Feasibility**: what we chose is a class of watermarking, so the scheme is easy to implement and highly feasible.

3 PROPOSED MECHANISM

1. ENCRYPTION PROCESS

Step1. Binary image is given to share generation algorithm which gives two shares [3].

Step2. Every share is then divided into two arrays with one array containing elements at odd positions and other at even positions thus giving a total of four shares.

Step3. Every share is then encoded using Manchester coding.

Step4. Every encoded share is then again divided into two shares based on their positioning (even or odd) in the share.

Step5. The eight shares are embedded into the cover image by first choosing the image plane where it can be embedded using LSB bit encryption method. The plane choosing is performed by taking a random sequence the sequence is also embedded in the cover image.

Step6. The result of the LSB bit encryption method is just the cover image.

2. DECRYPTION PROCESS

Step1. The stegnographed image is given as input to the LSB bit decryption method, which gives us the 8 shares.

Step2. The eight shares are grouped into two respective shares which can generate four shares .

Step3. The four shares are then decoded using Manchester decoding.

Step4. The decoded shares are then grouped to form two shares.

Step5. The resulting shares are given as input to share combining algorithm.

Step6. The resulting image is the image which has been encrypted.

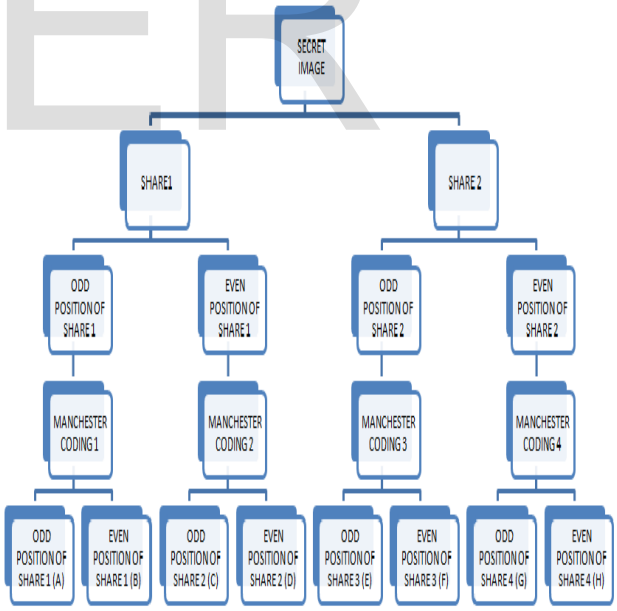


Figure 1: Flowchart of the Scheme

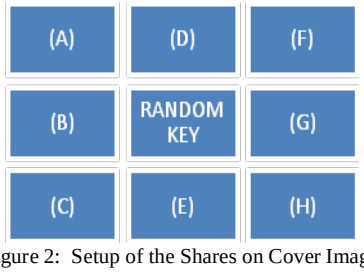


Figure 2: Setup of the Shares on Cover Image

4 IMPLEMENTATION

ENCRYPTION:

The first stage involves the generation of two shares [3] using share generation algorithm of the binary image. The black pixel is denoted by 1 and white pixel is denoted by 0. Any one option is selected from six options. Every pixel gets one 2 x 2 combination according to the option selected with two rows one row goes in share1 and the other in share 2.

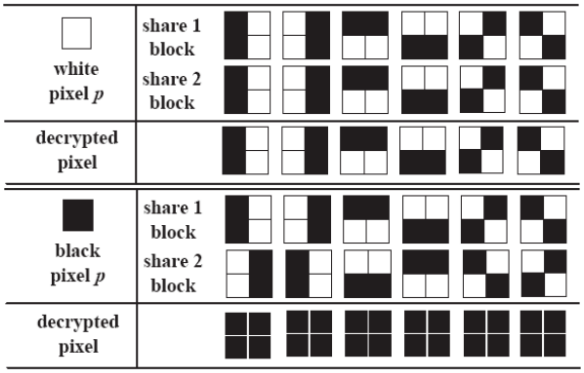


Figure 3: Construction of 2out of 2 Schemes

For decryption the two shares are stacked one over the other, stacking here represents OR operation.

In the next stage the two respective shares are divided into two shares with one share containing the elements at odd position of initial share and the other with elements at even position of the share.

Next all the four shares are encoded using Manchester coding. In Manchester coding every bit gets encoded into two bits if the bit has same value as the preceding one the code is reversed or else it is retained.

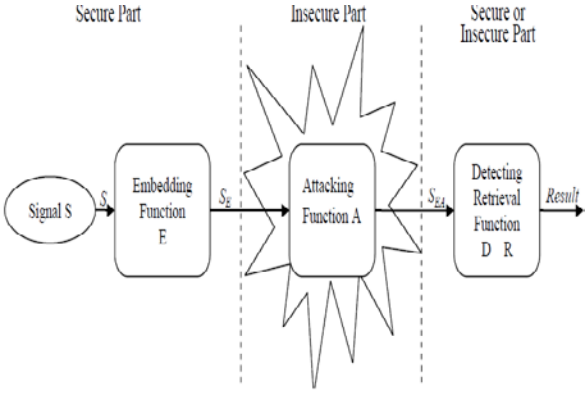


Figure 4: Manchester Coding

After the shares have been encoded they are again divided into two shares one share with elements at odd position and the other with elements at even position. At the end of this step we thus get eight shares which can be watermarked.

These eight share are embedded into the cover image The placement of every share is chosen according to a random sequence. The LSB bit [7] of this pixel value is replaced by the MSB bits of the shares. The centre of the cover image is watermarked with a number that contains the sequence that signifies the position of the shares. This number is changed each time the encryption is performed.

There can be six combinations of the sequence which can be shown by a three bit binary number.

Figure 5: Random possibilities of positioning of 8 Shares

DECRYPTION:

For the decryption the lsb bit of the steganographed image is extracted using LSB extraction algorithm then the number at the center of the image is identified to get the position of the shares.

The combination of share 1 and 2, share 3 and 4, share 5 and 6, share7 and 8 is fed as input to merge these two shares to get 4 shares. These 4 shares have element at odd positions from corresponding odd share and element at even position from corresponding even share.

These four shares are then decoded using Manchester decoding algorithm. after decoding these four shares are again combined into two shares as share1 and 2, share 3 and 4 so that they can be merged to give two shares.

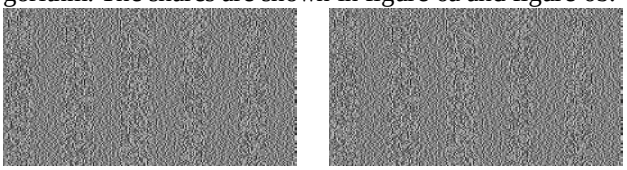
Finally, these two shares thus obtained are stacked one over the other or we can say they undergo an OR operation to give the original binary image.

5 RESULTS

The image ‘athi.bmp’ which needs to be secretly transmitted has dimensions 127x261. It is shown in figure 5. The image is resized to 126x261 so that it has even number of rows.

Figure 6: The Secret Image

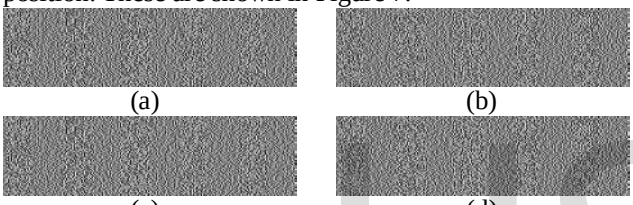
This image is divided into two shares using share generation algorithm. The shares are shown in figure 6a and figure 6b.



(a) (b)

Figure 7: The Generated Shares

Every share is further divided into two shares according to its position. These are shown in Figure 7.

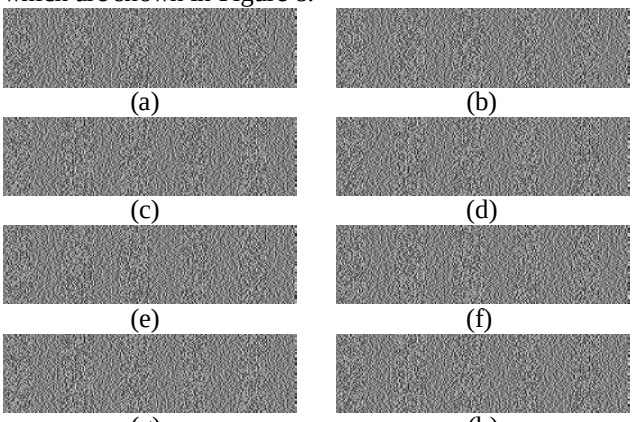


(a) (b)

(c) (d)

Figure 8: The Shares according to the position

These shares are the encoded using Manchester coding. The coded shares are further divided into two according to their position which are shown in Figure 8.



(a) (b)

(c) (d)

(e) (f)

(g) (h)

Figure 9: Eight share needed for watermarking

These 8 shares are then placed on the cover image 'flower.jpg' of size 196x251 shown in Figure 9.

Figure 10: Cover Image

The watermarked image is shown in Figure 10.

Figure 11: Watermarked Image

After the decryption procedure we get the final decrypted image as shown in Figure 11. Here PSNR of cover and water marked Image comes out to be about 30 decibels with 0.9975 correlation between original cover image and water marked image and with insertion of salt pepper noise it does not detoriates much secret message is recovered well too.

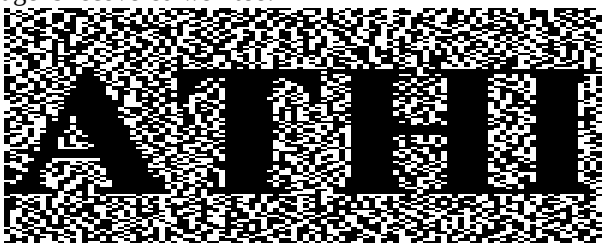


Figure 12: Secret Message Recovered

6 Conclusion & Future scope

Visual cryptography is a technique where visual information in form of text, image etc is encrypted in such a way that decryption does not need computer as it is just a mechanical operation. Here in this paper we have tried to modify the existing visual cryptographic schemes to make it more effective. We have integrated share generation, LSB insertion, Manchester coding and simple mathematical permutations in a single scheme. The simulation results show that cover image and watermarked image are almost

identical and the secret message has been recovered well. So the designed method works well.

In future modular arithmetic can be introduced here to make the process more effective. And better quality images can be given to it as input which will improve its performance.

REFERENCES

[1] B. Schneier, "Applied Cryptography: Protocols, Algorithms, and SourceCode in C", John Wiley & Sons, Inc, 1996.

[2] Piper," Basic principles of cryptography" , IEEE Colloquium on Public Uses of Cryptography, 1996

[3] Ching-Sheng Hsu and Shu-Fen Tu," 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

[4] Shyamalendu Kandar, Bibhas Chandra Dhara," k-n Secret Sharing Visual Cryptography Scheme on Color Image using Random Sequence" *International Journal of Computer Applications (0975 – 8887) Volume 25– No.11, July 2011*

[5] Mrs. Bhandare Shital, Mr. Jhade Manoj, Mrs. Jadhav Angarika," An improved approach for Extended Visual Cryptography Scheme for Colour Images" *International Journal of Computer Applications (0975 – 8887)* Volume 45– No.10, April 2012

[6] Miss. Asha S.N, Dr.Shreedhara , Smt. Anitha G, " Performance Evaluation Of Extended Visual Cryptography Schemes With Embedded Extended Visual Cryptographic Scheme" International Journal of Scientific & Engineering Research Volume 3, Issue 4, April-2012

[7] Gokul.M, Umeshbabu R, Umeshbabu R, Deepak Karthik, " Hybrid Steganography using Visual Cryptography and LSB Encryption Method" International Journal of Computer Applications (0975 – 8887) Volume 59– No.14, December 2012

[8] Vijaya Kumar. Kurapati, Venu Gopal. K, M.Nagaraju," Multiple Watermarking Techniques using Visual Cryptography for Secured Copyright Protection" International Journal of Scientific & Engineering Research Volume 4, Issue 1, January-2013

[9] M. Naor and A. Shamir, "Visual cryptography," in *Proc. OCRYPT' 94*, Berlin, Germany, 1995, vol. 950, pp. 1–12,Springer-Verlag, LNCS.