



## Design and Performance Evaluation of Advance Visual Crypto System

**Cheenu Kukreja (M TECH)**  
Dept of CSE, NNSS  
SGI, KUK, Harayana, India

**Arpana Dureja**  
Asth Prof, Dept of CSE, NNSS,  
SGI, KUK, Harayana, India

**Jawad Ahmad Dar (M TECH)**  
Dept of CSE, NNSS  
SGI, KUK, Harayana, India

**Abstract**— *With the coming era of electronic commerce, there is an urgent need to solve the problem of ensuring information safety in today's increasingly open network environment. The encrypting technologies of traditional cryptography are usually used to protect information security. With such technologies, the data become disordered after being encrypted and can then be recovered by a correct key. Without the correct key, the encrypted source content can hardly be detected even though unauthorized persons steal the data. Visual cryptography, an emerging cryptography technology, uses the characteristics of human vision to decrypt encrypted images. It needs neither cryptography knowledge nor complex computation. For security concerns, it also ensures that hackers cannot perceive any clues about a secret image from individual cover images. So, there is a need to design a method by which a binary image could be encrypted and decrypted easily in a secure manner. This work will focus on designing for the efficient visual crypto system. The key concept of proposed system is based upon visual cryptography. Proposed cryptography method will encrypts secret information into two pieces (on the bases of white and black color) called as shares. These two shares are operations together by logical operation to reveal the original secret. Proposed visual cryptography will encrypts the secret in various levels. The encryption will be expansion less. The original secret size will be retained in the shares at all levels.*

**Keywords**— *Shares, watermarking, cover image, carrier image, stego image.*

### I. INTRODUCTION

In this *paper* we consider the security of shares in visual cryptography and generating more meaningful shares with respect to cryptographic approach. Basically visual cryptographic is used for encryption of visual information like written material, textual images, handwritten notes, print and scanned material etc in perfectly secure way so that decryption can be performed by human visual system [3]. Among different kinds of the carrier media, digital images are the most popularly used data on the Internet. A host image used to hide the secret data is called the cover image or the carrier image. When the secret data has got embedded into the cover image, the resultant image is called the stego image. This era of technology and increasing the wide use of Internet, face a big problem that is security. People need a safe and secured way to transmit information. The one of the best way for secure data communication is Visual cryptography [5]. The encrypting technologies of traditional cryptography are usually used to protect information security. With such technologies, the data become disordered after being encrypted and can then be recovered by a correct key. Without the correct key, the encrypted source content can hardly be detected even though unauthorized persons steal the data. The most notable feature of this approach is that it can recover a secret image without any computation. It exploits the human visual system to read the secret message from some overlapping shares, thus overcoming the disadvantage of complex computation required in the traditional cryptography [2].

### II. VISUAL CRYPTOGRAPHIC

Visual Cryptography (VC) [1] is a method of encrypting a Secret image into shares such that stacking a sufficient number of shares reveals the secret image. Shares are binary images usually presented in transparencies. Each participant holds a transparency (share). Unlike conventional cryptographic methods, VC needs no complicated computation for recovering the secret. The act of decryption is to simply stack shares and view the Secret image that appears on the stacked shares. Access Structure of Visual Cryptography To encode the image, original image is split into  $n$  modified versions referred as shares. It involved breaking up the image into  $n$  shares so that only someone with all  $n$  shares could decrypt the image by overlaying each of the shares over each other. Practically, this can be done by printing each share on a separate transparency and then placing all of the transparencies on top of each other. Decoding can be done by simply stacking subset  $s$  of those  $n$  shares. In their technique  $n-1$  shares reveals no information about the original image. Figure 1 depicts the working of Visual Cryptography. This can be achieved by using any one of the following access structures [1].

I. (2, 2) VCS —this is a very simplest VCS scheme in which secret image is encrypted into 2 shares. To reveal the secret image 2 shares are overlaid or combined.

- II. (2, n) VCS —this scheme encrypts the secret image into n shares such that when any two (or more) shares are overlaid the secret image is revealed.
- III. (n, n) VCS —this scheme encrypts the secret image into n shares such that it can be revealed only when all n shares are overlaid.
- IV. (k, n) VCS —this scheme encrypts the secret image into n shares such that when at least k shares are combined secret image can be revealed.

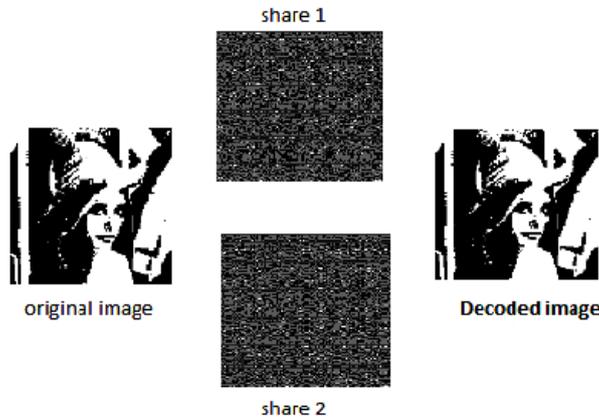


Figure 1. Basic VCS Scheme [1]

### III. VCS ALGORITHM

VCS Scheme normally involves two algorithms:

- Algorithm for creating shares
- Algorithm for combining shares

VCS algorithm’s efficiency is very critical factor and reliability and level of security are some more metric which we need to consider while designing a VCS algorithm. The VCS system should be reliable enough such a way that intruders are not able to read the original image. One important functional requirement of any VCS system is size of shares which should be same as that of original image to prevent doubt for unauthorized user.

Algorithm for creating shares:

This algorithm divides secret image into n number of shares. The shares created by this algorithm will be in unreadable format such that it is impossible to reveal secret image. Single share cannot reveal the secret image. If these individual shares are transmitted separately through communication network, security is achieved.

Algorithm for combining shares:

This algorithm reveals the secret image by taking the number of shares as input. Some algorithm may take all shares as input and some other algorithm may take subset of shares as input. Decryption is done by merging shares which has taken as input [1].

Visual Cryptography Schemes:

I. Black and White Visual Cryptography Scheme:

Sharing Single Secret: In this scheme Author proposed encoding scheme to share a binary image into two shares Share1 and Share2. If pixel is white one of the above two rows of Table1 is chosen to generate Share1 and Share2. Similarly If pixel is black one of the below two rows of Table1 is chosen to generate Share1 and Share2. Here each share pixel code denote two white and two black pixels each of share alone gives noise clue about the pixel whether it is white or black.

Table 1. Naor and Shamir’s scheme for encoding a binary pixel into two shares [4].

Pixel	Probability	Share <sub>1</sub>	Share <sub>2</sub>	Share <sub>1</sub> ⊗ Share <sub>2</sub>
□	50%	█ □	█ □	█ □
	50%	□ █	□ █	□ █
■	50%	█ █	□ █	█ █
	50%	█ █	█ □	█ █

**Sharing Multiple Secrets:** In this scheme author present the visual cryptography schemes to share two secret images in two shares. They hidden two secret binary images into two random Shares, namely A and B, such that the first secret can be seen by stacking the two shares, denoted by A ⊗ B, and the second secret can be obtained by first rotating A ⊖ anti-clock wise.

#### IV. COLOR VISUAL CRYPTOGRAPHY SCHEMES

Sharing Single Secret: Until the year 1997 visual cryptography schemes were applied to only black and white images. First colored visual cryptography scheme was developed by Verheul and Van Tilborg. Colored secret images can be shared with the concept of arcs to construct a colored visual cryptography scheme. In c-colorful visual cryptography scheme one pixel is transformed into m sub pixels, and each sub pixel is divided into c color regions. In each sub pixel, there is exactly one color region colored, and all the other color regions are black. The color of one pixel depends on the interrelations between the stacked sub pixels. For a colored visual cryptography scheme with c colors, the pixel expansion m is  $c \times 3$ .

Sharing Multiple Secret: Tzung-Her Chen et. al. anticipated a multi-secrets visual cryptography which is extended from traditional visual secret sharing. The codebook of traditional visual secret sharing implemented to generate share images macro block by block in such a way that multiple secret images are turned into only two share images and decode all the secrets one by one by stacking two of share images in a way of shifting. This scheme can be used for multiple binary, gray and color secret images with pixel expansion.

#### V. APPLICATION OF VISUAL CRYPTOGRAPHY-WATERMARKING

With data and multimedia taking on digital format, there is a need to protect digital property. There are two ways of accomplishing this: encryption and watermarking. Encryption protects information during transmission, but after its arrival at its destination, it is decrypted and is no longer protected. Watermarking is meant to compliment encryption in an effort to protect data after it has been decrypted. Watermarking is the technique of embedding a secret image into a cover image without affecting its perceptual quality so that secret image can be revealed by some process. One significant advantage of watermarking is the inseparability of the watermark (secret image) from the cover image. Some of the vital characteristics of the watermark are: hard to perceive, resists ordinary distortions, carries numerous bits of information, capable of coexisting with other watermarks, and demands little computation to insert and extract Watermarks [5].

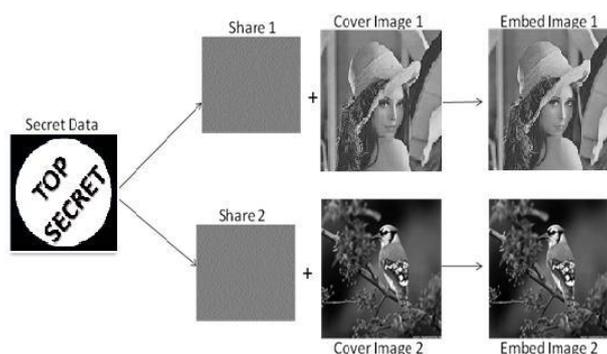


Figure 2. Secret Data Embedding Process using Visual Cryptography [5]

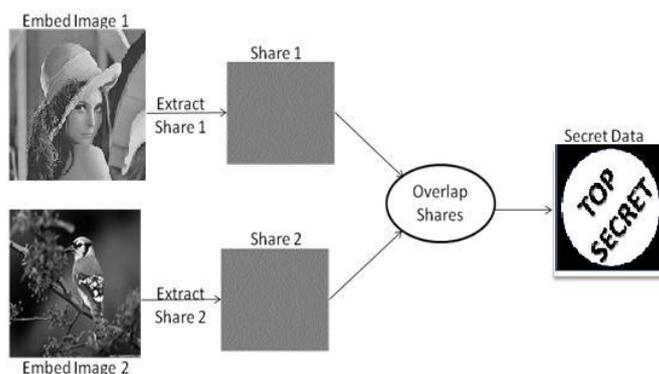


Figure 3. Data Extracting Process using Visual Cryptography [5]

#### VI. PROPOSED METHODOLOGY

All the simulation work has been implemented in MATLAB environment 2013 using general MATLAB toolbox and Image processing toolbox. We have taken an input grayscale image “watermark128.bmp” as test image for cryptography and applied the following steps:

- [1] Reading of Input Binary Secret Image.
- [2] Display of input Binary Secret image.
- [3] Calculation of size of input Binary Secret image.
- [4] Creation of share 1 according to the size of input Binary Secret image having all elements equal to zero.
- [5] Creation of share 2 according to the size of input Binary Secret image having all elements equal to zero.

**(a). White Pixel share combinations**

- [6] Finding of white pixel indices in input Binary Secret image.
- [7] Calculation of number of rows of white pixel.
- [8] Random permutation the share generation
- [9] Updating of share 1 and share 2 randomly for white pixel.

**(b). Black Pixel share combinations**

- [10] Finding of black pixel indices in input Binary Secret image.
- [11] Calculation of number of rows of black pixel.
- [12] Random permutation the share generation
- [13] Updating of share 1 and share 2 randomly for black pixel.
- [14] Display of share 1 image.
- [15] Display of share 2 image.
- [16] Overlapping of share 1 and share 2 using Logical OR operation.
- [17] Display of overlapped image

**VII. RESULT**

All the simulation work has been implemented in MATLAB environment 2013 using general MATLAB toolbox and Image processing toolbox. We have taken an input grayscale image “watermark128.bmp” as test image for cryptography as shown in figure 4. The size of input image is 32KB and dimension of pixels is 512 x 512. This is the final binary representation of input image. According to the size of this image Share1 and share 2 images has been prepared just contacting zeros as all the elements. These zero elements will be updated or modified by random permutation according to white and black pixel positions of binary input image for both the shares. These updated shares i.e. share 1 and share 2 are shown in figure 5 and figure 6 respectively. Finally after over lapping of both the shares using logical OR operation we traced the secret binary input image as shown in figure 7. Also, we have evaluated and analyzed the performance of a proposed methodology using PSNR as output parameter. PSNR of both shares has been calculated which is 51.1750 db (for both). The PSNR of our method is compared by that of [6]. The size of test image used by [6] is 2.95KB and dimension is 512 x 512. The PSNR of its share is 9.93db and 5.53db.

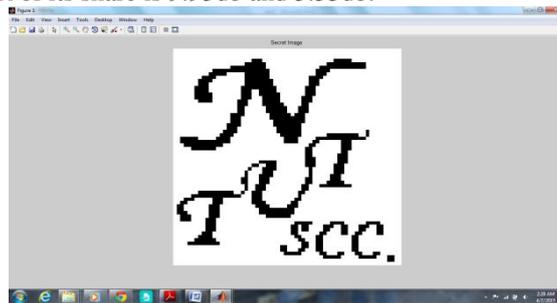


Figure 4. Snapshot of Secret Binary Input Image

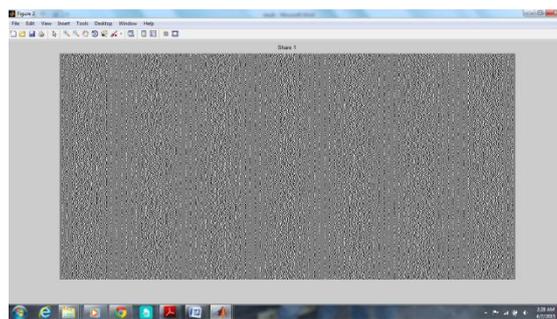


Figure 5. Snapshot of Share 1

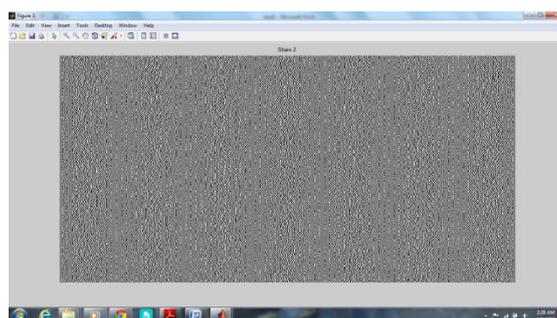


Figure 6. Snapshot of Share 2

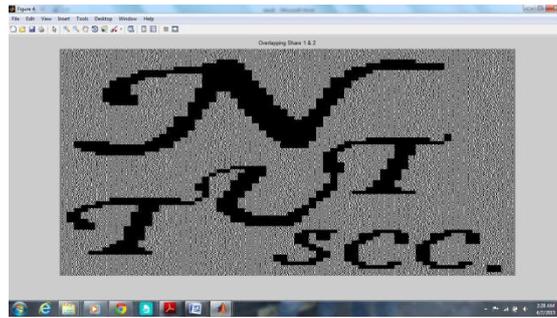


Figure 7. Snapshot of overlapped image of share 1 and share 2

### VIII. CONCLUSION AND FUTURE SCOPE

Visual Cryptography provides one of the secure ways to transfer images on the Internet. The advantage of visual cryptography is that it exploits human eyes to decrypt secret images with no computation required. A new visual cryptographic technique has been introduced in this research work. This work contains some details about Visual Cryptography Scheme. This work rectifies the problem of security of encoded images i.e. share 1 and share 2 as intruder can access all communication channels but cant reconstruct the secret image random permutation is used for creation of shares . Also, the traditional VCS suffer from pixel expansion problem. Proposed method also overcomes this problem. The concept of random permutation along with traditional VCS is combined in this work to give a secured image sharing system. As we have compared the performance of proposed method with that of existing method in terms of PSNR. It can be easily concluded that proposed method is performing much better than existing one, by comparing the PSNR of both shares. The proposed method not only improves the PSNR but also increases the visual quality as compared to other methods. The performance analysis of proposed method reveals that the proposed encryption method is ideal. If lossless Image compression methodology is applied before encryption we can strengthen cryptographic security. Because compressed image has less redundancy than the original image, cryptanalysis will be difficult. The proposed system can be extended such that it can be applied to all types of image formats like Jpeg, png etc.

### REFERENCES

- [1] Ranjan Kumar H S, Prasanna Kumar H R, Sudeepa K B and Ganesh Aithal, “Enhanced Security System using Symmetric Encryption and Visual Cryptography”, International Journal of Advances in Engineering & Technology ©IJAET, Vol. 6, Issue 3, pp. 1211-1219, July 2013, ISSN: 22311963.
- [2] Yogesh Bani, Dr. B.Majhi, Ram S. Mangrulkar, “A Novel approach for Visual Cryptographic using a Watermarking Technique”, Proceedings of the 2<sup>nd</sup> National Conference; INDIA-Com-2008.
- [3] Young-Chang Hou, “Visual cryptography for color images”, The Journal of the Pattern Recognition Society, Pattern Recognition 36 (2003) 1619 – 1629.
- [4] Thottempudi Kiran, K. Rajani Devi, “ A Review on Visual Cryptographic Scheme”, Journal of Global Research in Computer Science, Volume 3, No. 6, June 2012, ISSN-2229-371X.
- [5] Mr. Abhay Sharma, Mrs. Rekha Chaturvedi, Mr. Naveen Hemrajani, Mr. Dinesh Goyal, “New Improved and Robust Watermarking Technique based on 3<sup>rd</sup> LSB substitution method”, International Journal of Scientific and Research Publications, Volume 2, Issue 3, March 2012 , ISSN 2250-3153.
- [6] Shital B. Pawar, Prof.N.M.Shahane, “Visual Secret Sharing Using Cryptography”, International Journal of Engineering Research, Volume No.3, Issue No.1, pp : 31-33 , 01 Jan. 2014, ISSN:2319-6890.