

# Visual Cryptography Scheme for Colored Image using XOR with Random Key Generation

T. Ambritha<sup>1</sup>, J. Poorani Sri<sup>2</sup>, J. Jessintha Jebarani<sup>3</sup>, M. Pradhiba Selvarani<sup>4</sup>

UG Student, Department of Computer Science and Engineering<sup>1, 2, 3</sup>

Assistant Professor, Department of Computer Science and Engineering<sup>4</sup>

Kamaraj College of Engineering and Technology, Virudhunagar, TamilNadu<sup>1, 2, 3, 4</sup>

**Abstract**—Visual Cryptography (VC), a cryptographic technique which allows visual information to be encrypted in such a way that the decryption can be performed by the Human Visual System (HVS), without the help of computers. Visual Cryptography Scheme (VCS) eliminates complex computation problem in decryption process, by stacking operation we can restore the secret image. This property makes VC especially useful for the low computation load requirement. During encryption, the image is encrypted and then it is divided into two shares. Two shares are superimposed to reveal the secret image in the decryption process. The objective of our project is to get the better quality of decrypted image with the same size as the original image. The OR based VCS degrades the contrast by its monotone property. In XOR based scheme, the share images are superimposed with the help of XOR operation which results in perfect reconstruction. Hence, the XOR operation is proposed in decoding process to enhance the contrast, quality, and to reduce noise.

**Index Terms**— Visual Cryptography, Secret image Sharing, Human Visual System.

## INTRODUCTION

With the growth of the Internet, more and more data can be accessed via network. In today's communication, sharing images securely is the major issue. To secure the information Cryptography is a possible technique. The Visual Cryptography technique is used for security. Visual Cryptography is a cryptographic technique that allows visual information to be encrypted in such a way that decryption is done with a mechanical operation that does not require a computer. Visual information such as images, pictures, text, etc is allowed in this technique to be encrypted in such a way that their decryption can be performed with the help of the Human Visual System. The information security will be increased with the complexity of decryption algorithm. This technique encrypts a secret image into shares such that superimposing the shares reveals the secret image.

The decrypted image is obtained by superimposing the shares [10] together. The secret image without additional computations or any knowledge of cryptographic keys can be revealed by overlapping shares that contain random information. However, the decrypted image is darker and contains numerous of visual impairments, due to the nature of the algorithm. Most of Visual Cryptography solutions increase the spatial resolution of the secret image. The requirement for inputs of the binary or dithered nature only limits the applicability of visual cryptography.

## PROBLEM STATEMENT

The common drawbacks of the VCS are we are unable to recover the original input image with good clarity. When no pixels are expanded, a poor quality image is recovered. While using OR gate, shadow is developed which cannot be undone. In XOR based scheme, the share images are superimposed using XOR operation which results in perfect reconstruction.

## SCOPE OF THE PROJECT

The major drawback in OR based VCS is the contrast is degraded by its monotone property. When each pixel expands, image with contrast is recovered. When group of pixels expand, it yields better results. The main objective of our project is to get the better quality of decrypted image with the same size as the original image. In XOR based scheme, the share images are superimposed with the help of XOR operation which results in perfect reconstruction. Hence, the XOR operation is proposed in decoding process to enhance the contrast, quality, and to reduce noise.

## LITERATURE SURVEY

[1] Visual cryptography, introduced by Noar and Shamir [1] is a type of secret sharing techniques for images. The idea of VCS is to split an image into number of shares which separately reveals no information about the original secret image. The image is made up of black and white pixels, and can be recovered by superimposing all the shares without doing any computations. By

applying the Noar and Shamir 2-out-of-2 visual cryptography algorithm, two shares are created, which separately produces no information about the original secret image. It can only be recovered when both of the shares are obtained and superimposed. This technique can be extended to n-out-of-n visual cryptography scheme. This technique [1] makes use of the human visual system to perform the OR logical operation on the superimposed pixel of the shares. The two blocks of 2x2 pixels will be viewed as the two black pixels and the two white pixels in each pixel block are averaged out. If we print those two pixel block separately onto a transparencies and superimpose. According to leaking, information about the original secret image is not meant from any given share of the secret image, an unbounded adversary which has unlimited computational power should not be able to gain any information about the secret image other than the size of it. This scheme is considered insecure if the shape pattern or color of just a portion of the secret image can be recovered from any given share.

- [2] Ligu Fang recommended a (2, n) scheme based on the process of balancing the performance between pixel expansion and contrast. Xiaoping and Tan suggested Threshold visual secret sharing schemes with mixed XOR and OR operation and was based on binary linear error correcting code [2]. The other issues are the problem of expansion in the size of decrypted image and the quality of the decrypted image. In this approach, the input image is first divided into channel images and color error diffusion technique is applied for dithering (halftoning) to improve the quality of image. This technique produces better results as compared to other dithering techniques. As dithering is used, image is reproduced with high quality [2]. Disadvantages are Only single set of secret messages can be hidden, so for sharing large amount of secret messages several shares should be generated and the key must be sent securely.
- [3] Han-Yu Lin, and Yi-Shiung Yeh proposed a dynamic multi-secret sharing scheme based on the one way hash function [3]. If someone wants to share 100 images with others he has to obtain 100 shares, which is difficult to manage. This scheme solves this problem by keeping only one share image and decrypts all other secret images with its share (Universal share). The major characteristics of its design are multi-use of the secret shares and that different group secrets can be reconstructed according to the number of threshold values that provides more flexibility. While applying successive one-way hash functions and the XOR operations, this scheme [3] is secure against serious attacks even though the pseudo secret shares are compromised. Advantage in this scheme is multiple images can be shared easily. In this scheme [3] mathematical calculations are not performed here key safeguarding is missing.
- [4] Verheul and Van Tilborg proposed first color visual cryptography scheme [4]. In this scheme one pixel is substituted by m sub pixels, and each sub pixel is divided into c color regions. In each sub pixel, mostly one color region is colored. A new approach was proposed by Liu, Wu and Lin for colored visual cryptography scheme. They proposed three different approaches for color image representation: In the first case, colors in the secret image can be printed on the shares directly; in the second case individual RGB/CMY channels are used. Then normal visual cryptography scheme is applied to each of the color channels. In the third case, the secret image is encrypted at bit-level by binary representation of color of a pixel. Advantage in this scheme [4] is reduced pixel expansion. In this approach good quality of image is obtained.
- [5] A New Secure Image Transmission using Mosaic Images [5] have proposed a new scheme for secure image transmission in which the secret image is converted into a meaningful mosaic image with the same size and looks like a preselected target image. Secret key controls transformation process and that secret image is only recovered by that key without any loss from mosaic image. The proposed method is extended by Lai and Tsai, in which a new type of computer art image, called secret-fragment visible mosaic image, was introduced. The mosaic image is the output of rearrangement of the fragments of a secret image in disguise of another image called the target image preselected from a database [5]. There is no loss during reconstruction of images [5]. Fragmentation - tedious process.

## PROPOSED SYSTEM

In our proposed method, XOR based scheme is used. Here three phases are used to perform Visual Cryptography as shown in Fig.1 (i.e.,) Preprocessing, Generation of shares and Reconstruction. In XOR based scheme, the share images are superimposed with the help of XOR operation which results in perfect reconstruction.

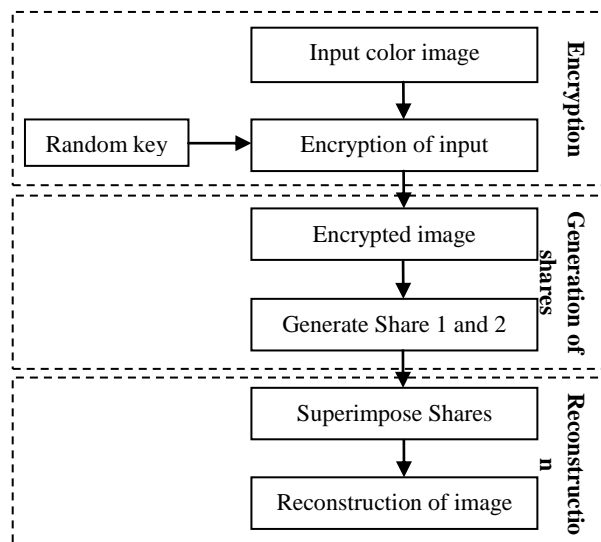


Fig.1 Block diagram of Visual Cryptography for Colored image

A. *Preprocessing*1) *Input image:*

The color image is taken as an input image. It must be of same height and width. If the height and width varies, the image must be resized. The extension of the image it may be of any type like \*.Jpeg,\*.bmp,\*.png etc.

2) *Encryption:*

Encryption is the process of encoding messages or information. Encryption does not prevent interception, but denies the message content to the interceptor. In an encryption scheme, the intended communication message or information, referred to as plaintext, can be encrypted using an encryption algorithm, generating cipher text that can be read only if decrypted. For technical reasons, an encryption scheme usually uses generation of random encryption key. Decrypting the message without possessing the key is possible, but, for a well-designed encryption scheme, large computational methods and skills are required. An authorized recipient can easily decrypt the message with the key given by the sender to receiver, but not to unauthorized interceptors. After image is encrypted, the shares [8] are generated.

B. *Generation of shares*

The encrypted image is divided into shares. Each share consists of pixels [6]. Pixel is the smallest unit of an image. Each pixel is divided into subpixels (white & black). A white subpixel represented by 0. A Black subpixel represented by 1 as shown in Fig 2.

















Original pixel	Share 1	Share 2	Share 1 and 2
			
			
			
			

Fig.2 Share Generation

C. *Reconstruction*

The process of transforming encrypted information so that the original information is obtained is called decryption. It is the process of taking encoded or encrypted text or other data and converting it back into text that the computer or the human can read and understand. This could be used to describe a method of decrypting the data manually or with decrypting the data using the proper codes or keys. If a decryption pass code or key is not available, the special software may be needed to decrypt the data using algorithms to crack the decryption and make the data readable. A sender transmits the input image which is divided into shares. When all of these shares are aligned and superimposed, the secret image information could be exposed to the receiver. Once all shares are received at the receiver end, the shares are superimposed (XORed) to get the original image.

## COMPARITIVE STUDY

The comparison of various VCS having the parameters like number of secret images, security level and quality of reconstructed image.

TABLE I COMPARISON OF DIFFERENT ALGORITHM

Technique Used	No. of secret images	Security	Result
RIVC	2	Increase	Poor
VCS (with Random Key)	1	Increase	Good
(2,2)VCS	1	Increase	Fair

Digital Watermarking	2	Increase	Fair
----------------------	---	----------	------

## I. EXPERIMENTAL RESULTS

The colored input image is obtained from the user as shown in the Fig. 3.



Fig.3 Input Image

The input color image is encrypted with the random key generation as shown in the Fig. 4.

- A random number is generated by a sequence of values based on the current state using the following computation.
- Here, less computation is enough.

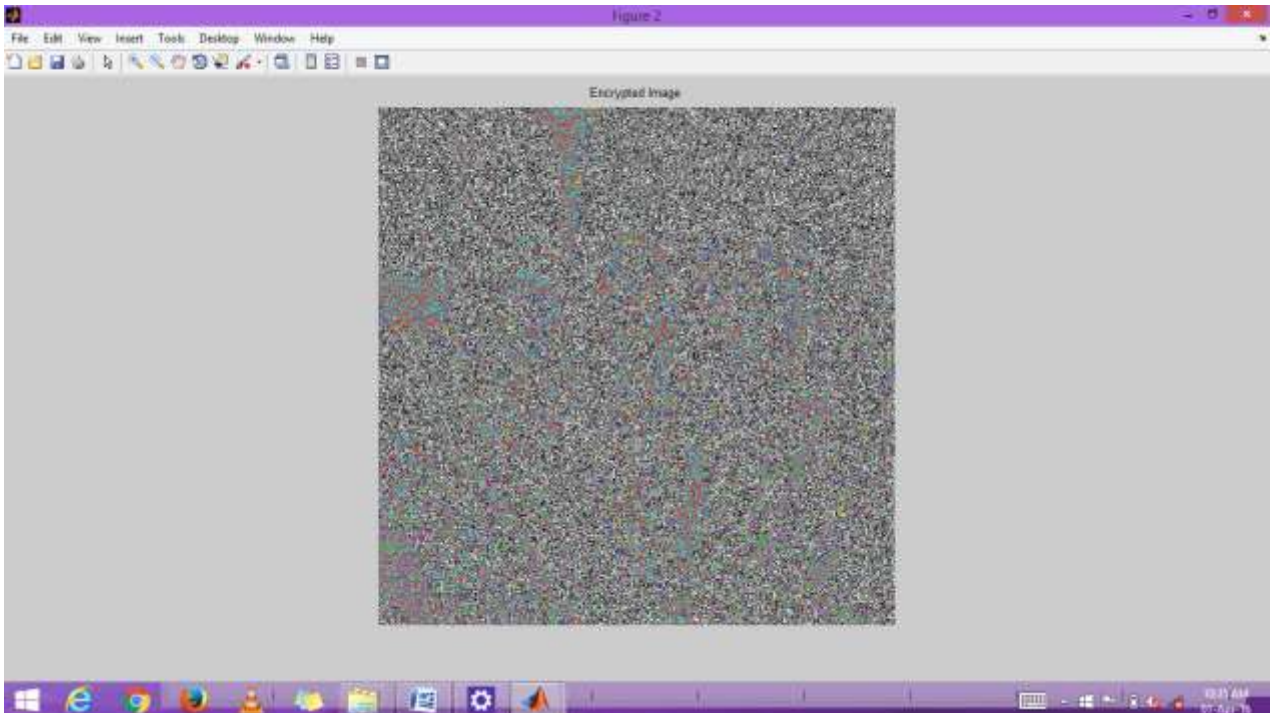


Fig.4 Encrypted Image

The keys are generated randomly during encryption which is evident as in the Fig. 5 which can be obtained with the formula  $\text{randomnumber} = \text{rand}(20,3)$

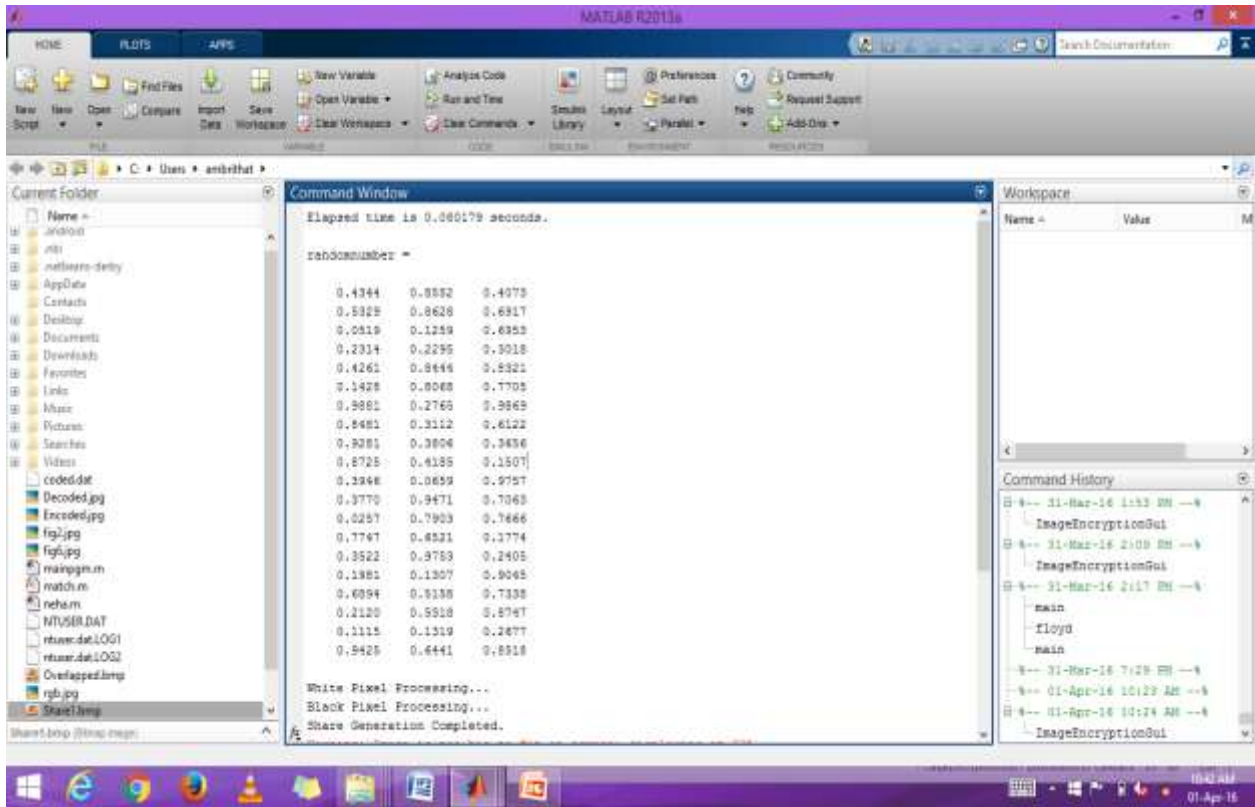


Fig. 5 Random key generation

The encrypted image is divided into two shares as in Fig. 6 with the help of following computations.

- share1 = zeros(s(1), (2 \* s(2)));
- share2 = zeros(s(1), (2 \* s(2)));
- pixShare=generateShare(sa,sb);

Share 1 is obtained as in Fig. 6.1 and Share 2 is obtained as in Fig. 6.2.

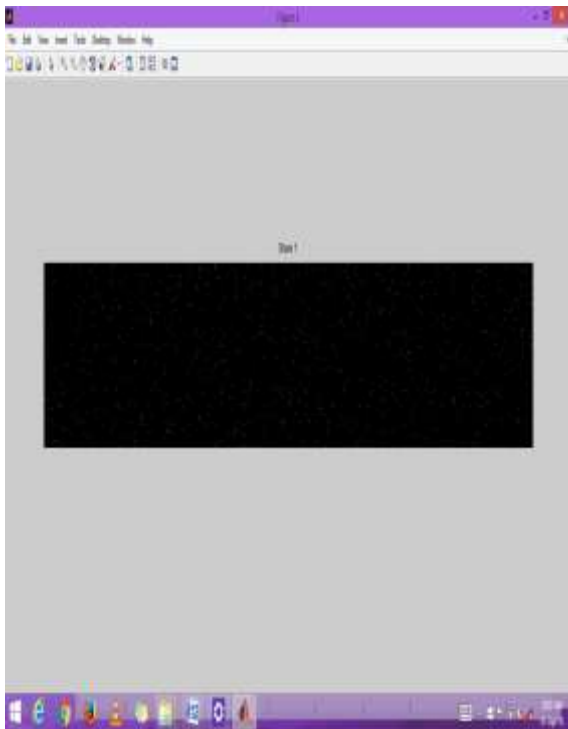


Fig.6.1 Share 1



Fig.6.2 Share 2

Fig.6 Share Generation

Two shares are superimposed as in Fig. 7 to get the secret image using the following computation;  
 $\text{share12}=\text{bitxor}(\text{share1}, \text{share2});$



Fig. 7 Reconstructed Image

In our technique, we have used XOR Scheme hence the quality of reconstructed image is good as shown in Table II.

Table II Experimental Result

Algorithm	Complexity	Pixel Expansion	Security	Quality
Naor Shamir (basic 2×2)	Medium	Double	Increase	Poor
<b>Proposed Technique</b>	<b>Less</b>	<b>Double</b>	<b>Increase</b>	<b>Good</b>

## CONCLUSION

The step construction on VCS has been studied. The literature survey has been made on how to use the VCS for cheating prevention. The previous cheat-preventing schemes were examined and found that they are either not robust enough or still improvable. The metrics required for designing the system: pixel expansion and contrast has been analyzed. The transformation to be proposed in this project is expected to incur minimum overhead on contrast and quality of the image using XOR.

## FUTURE ENHANCEMENT

The future work is to implement Biometrics using Visual Cryptographic Scheme. Where image obtained from Biometric is separated into shares and single share is sent to the receiver which may also be considered as private key. The receiver inputs an image and it is converted into shares and one share is superimposed on the incoming share to get the original image.

## REFERENCES

- [1] Pooja, Dr. Lalitha Y. S, “*Non Expanded Visual Cryptography for Color Images using Pseudo-Randomized Authentication*”, International Journal of Engineering Research and Development, Volume 10, Issue 6, June 2014.
- [2] Gayathri.D, Dr.T.Gunasekran, “*Design of XOR based visual cryptography scheme*”, International Journal of Advanced Research in Electronics and Communication Engineering (IJARECE), Volume 4, Issue 2, February 2015.
- [3] Isha Padiya, Vinod Manure, Ashok Vidhate , “*Visual Secret Sharing Scheme Using Encrypting Multiple Images*”, International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering, Vol. 4, Issue 1, January 2015.
- [4] Mary Shanthi Rani, Germin Mary, “*MSKS for Data Hiding and Retrieval using Visual Cryptography Images*”, International Journal of Computer Applications, Volume 108 – No. 4, December 2014.
- [5] Mr. Praveen Chouksey, Mr.Reetesh.Rai, “*Secret Sharing based Visual Cryptography Scheme for color preservation using RGB Color Space*”, IRACST - International Journal of Computer Science and Information Technology & Security (IJCSITS), ISSN: 2249-9555 Vol. 5, No5, October 2015.
- [6] Karthik K, Sudeepa K B, “*Visual Cryptography Scheme for colour images based on meaningful shares*”, International Journal of Combined Research & Development (IJCRD), Volume: 4, Issue: 6, June 2015.
- [7] D.R.Denslin Brabin, Divya Venkatesan, Divyalakshmi Singaravelan, LekhaSri Rajendran, “*Region Based Visual Cryptography Scheme for Color Images*”, International Journal of Advanced Research in Computer and Communication Engineering Vol. 2, Issue 3, March 2013.
- [8] Dr.N.Radha, A.Nandhinipreetha, “*A Survey on Visual Cryptography Shares*”, International Journal of Engineering Sciences & Research Technology, March 2015.
- [9] Ching-Nung Yang, Dao-Shun Wang, “*Property Analysis of XOR-Based Visual Cryptography*”, IEEE transactions on circuits and systems for video technology, vol. 24, no. 2, february 2014.
- [10] Shankar K, Eswaran P, “*Sharing a Secret Image with Encapsulated Shares in Visual Cryptography*”, 4th International Conference on Eco-friendly Computing and Communication Systems, ICECCS 2015

#### BIBLIOGRAPHY



Ambritha. T pursuing her UG - B.E (Computer Science and Engineering) degree in Kamaraj College of Engineering and Technology, Virudhunagar, India. She is a Life Member of Indian Society of Technical Education (ISTE). Her area of interest encompasses Visual Cryptography and Network Security.



Poorani Sri. J pursuing her UG - B.E (Computer Science and Engineering) degree in Kamaraj College of Engineering and Technology, Virudhunagar, India. She is a Life Member of Indian Society of Technical Education (ISTE). Her area of interest encompasses Visual Cryptography and Digital Image Processing.



Jessintha Jebarani. J pursuing her UG - B.E (Computer Science and Engineering) degree in Kamaraj College of Engineering and Technology, Virudhunagar, India. She is a Life Member of Indian Society of Technical Education (ISTE). Her area of interest encompasses Visual Cryptography and Digital Image Processing.



Pradhiba Selvarani. M received her UG - B.Tech (Information Technology) degree in 2009 from Idhaya Engineering College for Women, Chinnasalem. She then completed her P.G - M.E degree in Computer and Communication Engineering at National Engineering College, Kovilpatti in 2011. She is currently working as an Assistant Professor in Kamaraj College of Engineering and Technology, Virudhunagar, India. She is a Life Member of Indian Society of Technical Education (ISTE). Her area of interest encompasses Pedagogy, Visual Cryptography, Software Engineering and Digital Image Processing.