

"Randomized Visual Cryptography scheme for color images"

Miss. Pallavi M. Sapate¹, Miss. Vanita D. Jadhav²

¹SVERI's College of Engg, Pandharpur Dist. Solapur, State: Maharashtra

²SVERI's College of Engg, Pandharpur Dist. Solapur, State: Maharashtra

Abstract: In this paper, we propose a new color visual cryptography scheme which is based on modified visual cryptography. Visual Cryptography is based on cryptography where n images are encoded in a way that only the human visual system can decrypt the hidden message without any cryptographic computations when all shares are stacked together. In this scheme sender can share $n-1$ natural images and one secret image of variable size with the server and it make the encryption with extraction of feature of natural images without altering the contents of natural images. When the receiver identification is done that time server make the decryption process and send the secret image with transmitted by highly secure secret channel. Moreover, this approach avoids the pixel expansion problem and makes it possible to recover secret images without any distortion.

Keywords: Color image, Natural Image, Transmission risk, Visual Cryptograph

I. Introduction

Visual cryptography technique allows the visual information to be encrypted in such a way that their decryption can be performed by human visual system. Security has become an inseparable issue as Information Technology is ruling the world now. Cryptography in the study of mathematical techniques related aspects of information security such as confidentiality, data security, entity authentication, but it is not only the means of providing information security, rather one of the techniques. Visual cryptography can be applied for copy right for images, access control to user images, visual authentication and identification any kind images of images like (normal or digital). Visual cryptography is a new technique which provides information security which user simple algorithm. In 1994, Noar and Shamir proposed a new field of cryptography called visual cryptography scheme (VCS) [1]. Who introduce simple but very secure way that allows sharing secret image without any cryptographic computation witch termed as Visual Cryptography Scheme (VCS). The simplest Visual Cryptography Scheme is given by the idea of A secret image consists of a collection of black and white pixels where each pixel is treated independently [2].

In Secret sharing scheme, the secret information is sharing among the group of participants. Each participant gets the part of secret image witch called a share. In a (k, n) visual cryptography scheme, a dealer encodes a secret into n shares and gives each participant a share, where each share is a transparency. The secret is visible if any k (or more) of participants stack their transparencies together, but none can see the shared secret if fewer than k transparencies are stacked together. The application of visual cryptography is widely discussed, such as: protection of copyright, the bank certification system, control missile launchers, fingerprint authentication and so on. In the last decade various Secret Sharing Scheme were proposed, but most of them require lot of computation to decode the shared secret information. While this method gives security for text and binary images, the growth of digital media requires the expansion of this technique to provide security for gray and color images. Several methods have been developed for securing gray and color images, including halftoning, dithering, color subpixel groupings [3].

A new color visual cryptography scheme, which shares a color secret image over $n-1$ arbitrary natural images and one noise-like share image. Simulation results show that the proposal improves the ease of management and reduces passing risk to effectively protect the passer and secret image [4]. This scheme is denoted as the $((n-1, 1), n)$ -VCS. Any $(n-1)$ natural images and a noise-like share image are selected as a medium to share a color secret image. These natural images can be grayscale or color advertising pictures. The encryption process just extracts the characteristics of the natural image, without changing any details of the natural image. Encryption process is divided into the natural image feature extraction and encryption. The reminder of this paper is organized as follows. Section 2 deals with the related works.

II. Related Works

A rapid growth in E-Commerce market is seen in recent time throughout the world. With ever increasing popularity of online shopping, Debit or Credit card fraud and personal information security are major concerns for customers, merchants and banks specifically in the case of CNP (Card Not Present). This paper presents a new approach for providing limited information only that is necessary for fund transfer during online

shopping thereby safeguarding customer data and increasing customer confidence and preventing identity theft. The method uses combined application of steganography and visual cryptography for this purpose. So a brief survey in visual cryptography is given in this section.

Visual cryptography is the concept of dividing a secret image into "n" shares and revealing secret image by stacking a qualified subset of "n" shares. The scheme is perfectly secure and very easy to implement. Visual cryptography takes the input as one secret image and creates the shares by the process of encryption, later decryption is done by human visual system(HVS).VC scheme eliminates complex computation problem in decryption process, and the secret images can be restored by stacking operation. This property makes visual cryptography especially useful for the low computation load requirement. The field of VC has been developed over the last several years.

The basic model of visual cryptography proposed by Naor and Shamir [1] accepts binary image "I" as secret image, which is divided into "n" number of shares. Each pixel of image "I" is represented by "m" sub pixels in each of the "n" shared images. The resulting structure of each shared image is described by Boolean matrix "S" Where $S = [S_{ij}]$ an $[n \times m]$ matrix $S_{ij}=1$ if the j th sub pixel in the i th share is black $S_{ij}=0$ if the j th sub pixel in the i th share is white When the shares are stacked together secret image can be seen but the size is increased by "m" times. The grey level of each pixel in the reconstructed image is proportional to the hamming weight $H(V)$ of the OR – ed Vector "V", where vector "V" is the stacked sub pixels for each original pixel. A solution of the "n" out of "n" visual secret sharing consists of two collections of $n \times m$ Boolean Matrices C_0 and C_1 . To share a white pixel, randomly choose one of the matrices from C_0 , and to share a black pixel, randomly choose one of the matrices from C_1 .

The following conditions are considered for the construction of the matrices:

1. For any "S" in C_0 , the OR-ed "V" of "n" rows satisfies $H(V) = n - I \cdot m$.
2. For any "S" in C_1 , the OR-ed "V" of any "n" rows satisfies $H(V) = n$.

By stacking fewer than "n" shares, even an infinitely powerful cryptanalyst cannot gain any advantage in deciding whether the shared pixel was white or black. Let us describe the construction of matrix for (n, n) visual cryptography for $n=3$. $C_0 = \{ \text{all the matrices obtained by permuting the columns complement of } [BI] \}$ $C_1 = \{ \text{all the matrices obtained by permuting the columns of } [BI] \}$ Where, B is the matrix of order $n \times (n-2)$ which contains only ones I is the identity matrix of order $n \times n$. The basic model was then extended to (k, n) threshold cryptography where any "k" or more shares will reveal the secret image. The construction of "k" out of "n" visual secret sharing is similar to the basic model with one difference. That is in basic model the threshold value is n where as here it is k which is the subset of n [5].















III. Types of visual cryptography

3.1 Black and White Visual Cryptography Schemes

a) Sharing Single Secret

Naor and Shamir's [1] 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 Table 1 is chosen to generate Share1 and Share2. Similarly If pixel is black one of the below two rows of Table 1 is chosen to generate Share1 and Share2. Here each share pixel p is encoded into two white and two black pixels each share alone gives no clue about the pixel p whether it is white or black. Secret image is shown only when both shares are superimposed.

Table1. Naor and Shamir's scheme for encoding a binary pixel into two shares

Pixel	Probability	Share ₁	Share ₂	Share ₁ ⊗ Share ₂
	50%			
	50%			
	50%			
	50%			

b) Sharing Multiple Secrets

Wu and Chen [2] were first researchers to 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 $A \otimes B$, and the second secret can be obtained

by first rotating A Θ anti-clockwise. They designed the rotation angle Θ to be 90° . However, it is easy to obtain that Θ can be 180° or 270° .

3.2 Color Visual Cryptography Schemes

a) Sharing Single Secret:

To hide a color secret image into multiple colored images it is desired that the generated share image as a noise. This formed by considering the some color images and with secrete image by doing encryption process between them. Xiao-Yi Liu [4] proposed a new visual cryptography scheme called as $((n-1, 1), n)$ -VCS. In this scheme encryption is done without altering the content.

b) Sharing Multiple Secrets

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 macro 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.

IV. Program Structure

To trim down the risk of passing share image, the basic assumption is the impassive cover image has non-suspicious and the lowest transmission risk, so it is more secure than the noise-like and meaningful image.

Based on the above assumptions, we propose a new color visual cryptography, denoted by $((n-1, 1), n)$ -VCS. Any $(n-1)$ natural images and a noise-like share image are selected as a medium to share a color secret image. These natural images can be grayscale or color advertising pictures, such as life photos, landscape photos, even photos online public. The encryption process just extracts the characteristics of the natural image, without changing any details of the natural image. No-modification of the natural image sharing figure can be spread by innocent third party, electronic bulletin boards, or network communication to the public.

Encryption Process

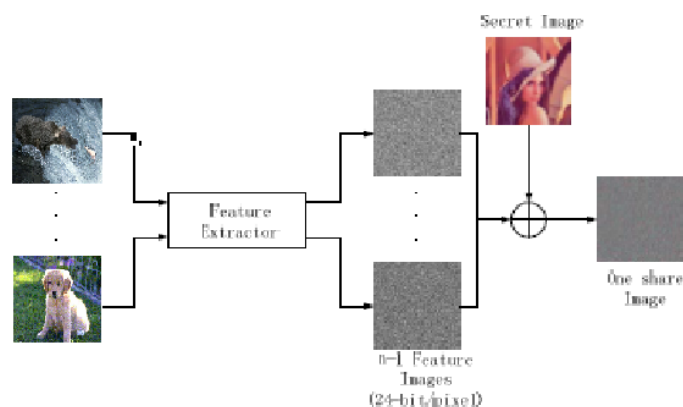


Fig.1 Encryption Process

First we have to apply the feature extraction process. In which we convert natural images into meaningless format. In the paper, the proposed scheme uses the original image as a true color image, each pixel is represented by red, green, blue (RGB) with 24-bit depth. In the stage of feature extraction use the pixel switching module for RGB three colors select randomly a pair of pixel position and exchange natural image pixel elements. The random sequence with exchange pixels is determined by the random number generator G and the switching times, the random number seed is the part of secret. When the times of exchanging is enough, the natural image veins after processing can be completely eliminated, just like meaningless noise-like image.

Consider any size($W \times H$) of natural images as well as secrete image.

N_α denotes the natural share image α , $1 \leq \alpha < n$.

- N_α denotes the natural share image α , $1 \leq \alpha < n$.
- (x, y) denotes the pixel coordinate, $1 \leq x \leq W$, $1 \leq y \leq H$.
- $P_{\alpha, \phi}^{(x,y)}$ denotes the pixel value of N_α 's color ϕ in the coordinate of (x, y) , $\phi \in \{R, G, B\}$.
- $H_\alpha^{x,y}$ is RGB pixel value assumption of (x, y) in N_α ,

$$H_{\alpha}^{x,y} = p_{\alpha,R}^{x,y} + p_{\alpha,G}^{x,y} + p_{\alpha,B}^{x,y} \quad (1)$$

- M_{α}^{β} denotes the average of all the pixel value in block $\beta(H_{\alpha}^{(x_{\beta},y_{\beta})}, \dots, H_{\alpha}^{(x_{\beta}+7,y_{\beta}+7)})$. (2)

f_{α} is N_{α} 's feature matrix. Member of $f_{\alpha}^{x,y} \in f_{\alpha}$ is feature matrix of (x, y). $f_{\alpha}^{x,y} = 1$ denotes N_{α} 's feature matrix in coordinate (x, y), $f_{\alpha}^{x,y} = 0$ indicate pixel is white

The extracted method of Feature value $f_{\alpha}^{x,y}$, $x_{\beta} \leq x \leq x_{\beta} + 7, y_{\beta} \leq y \leq y_{\beta} + 7$ is

$$f_{\alpha}^{x,y} = \begin{cases} 1, & H_{\alpha}^{x,y} < M_{\alpha}^{\beta} \\ 0, & \text{otherwise} \end{cases} \quad (3)$$

When the encryption/decryption sides appointed well the exchanging times and the random number seed of natural image, the program can use any natural images in the public domain for encryption.

Encryption consists of feature extracted images and secret image, which are obtained by following step.

First we have to do feature extraction process for all natural images by repeating all step.

- 1) Select two random pixel coordinate from natural image
- 2) Swap these two pixel with each other .this process repeat t_p times.
- 3) Perform the pixel specialization process as per bellow

$P_{\text{prv}} = 0$

$$P_{\alpha,\phi}^{(x,y)} = P_{\text{prv}} + P_{\alpha,\phi}^{(x,y)}$$

This repeat for every pixel coordinate until $W \times H$.

- 4) Image N_{α} is divide into t blocks with 8×8 pixels.
- 5) Calculate $H_{\alpha}^{x,y}$ within block for every pixel by using eq(1).
- 6) Calculate M_{α}^{β} using eq(2).
- 7) Calculate $f_{\alpha}^{x,y}$ using eq(3).
- 8) Finally encrypt this calculate result with the secret image by doing XOR operation. In this process we chose any size natural image and secret image, it will apply the mod operation during encryption for over come on the exiting drawback regarding size of image.

Decryption process

Decryption is done just inverse of encryption using proposed algorithm for obtaining the secrete image.

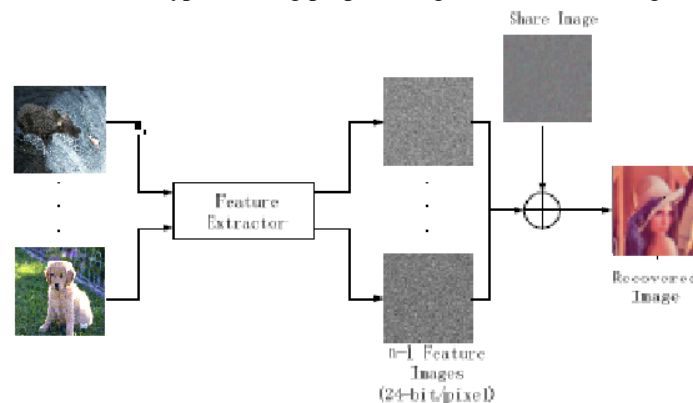


Fig.2 Decryption Process

In this process noise like share image and all used feature extracted natural images during encryption are used to achieve the secret image.

V. Experimental Result

In this section we take three natural images and secret image for our experiment purpose, we can take any size of and any number of natural images.

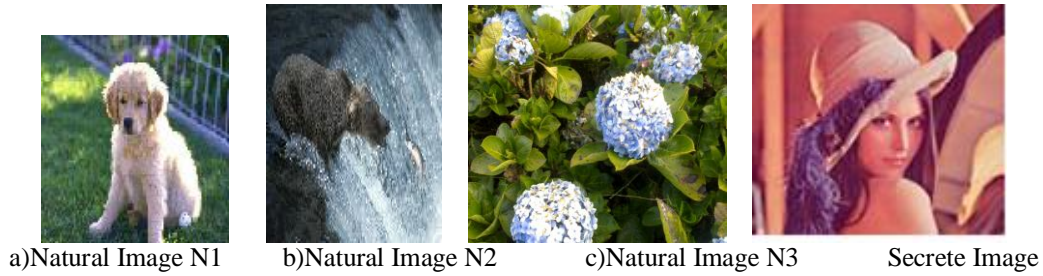


Fig.3 Natural Images and Secrete Image

By considering figure 3 images we are doing the decryption process, in which we get the feature extracted images figure 4(a)-(c) for above natural images. In this paper we can consider the any size natural as well secret image for visual cryptography process. Figure 5(d) is the share image witch obtained by applying encryption algorithm and figure 4(e)-(j) are the any random combination of share image with any number of feature extracted natural image/image. If any combination other than figure 4(k) for all combination it will not generated secrete image. These all natural image can be act as share, in proposed schemes are for gray scale image, color image and by stacking the shares; the resultant image achieved in same size with original secret image as like figure 4(k).

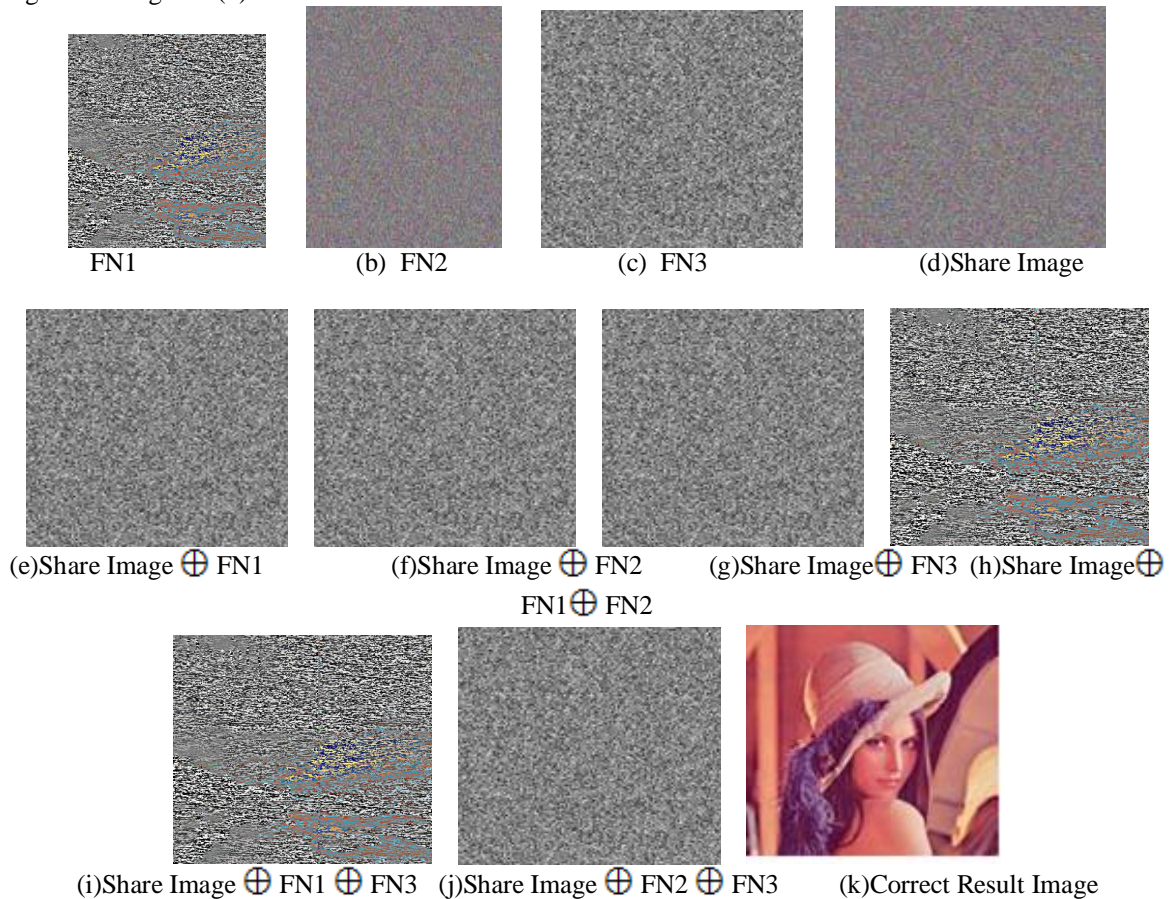


Fig. 4 Experimental Result of three natural images. (a)~(c) is binary feature image of natural images N1, N2 and N3 , (d) Share Image, (e)-(j) share image with all combination of three feature extracted natural images and final (k) is the correct result image.

VI. Conclusion

In this paper, we proposed a visual cryptography scheme in which (n-1) natural images and secret image are used for encryption. This is highly secure for the color image. In this paper methods which we used can overcome existing drawback like whatever natural images and secret image using that require same size. Due to the feature extraction of natural images we are making the changes in those images itself that cause restore secret image as it is without pixel expansion. The shared noise image looks like the dots, so it will

difficult for attacker to identify the secret image. In the future we plan to extend it for mage as well video and text.

References

- [1]. NAOR M, SHAMIR A. Visual cryptography[C]. Proceedings of Eurocrypt'94. New York, 1995. 1-12.
- [2]. JIM CAI 2003. A Short Survey on Visual Cryptography Schemes, www.wisdom.weizmann.ac.il/naor/PUZZLES/visual.html.
- [3]. Pooja and Dr.Lalitha Y. S,"Non Expanded Visual Cryptography for Color Images using Pseudo-Randomized Authentication", International Journal of Engineering Research and Development , Vol. 10, PP.01-08, June 2014.
- [4]. Xiao-Yi Liu, Ming-Song Chen, and Ya-Li Zhang ,“A New Color Visual Cryptography Scheme with Perfect Contrast “,2013 8th International Conference on Communications and Networking in China (CHINACOM)
- [5]. Néelima. Guntupalli, Mr: P.D.Ratna Raju and Mr.Suresh cheekaty, "AN INTRODUCTION TO DIFFERENT TYPES OF VISUAL CRYPTOGRAPHY SCHEMES" , International Journal of Science and Advanced Technology (ISSN 2221-8386), Vol. 1,Sept.2011
- [6]. C.C. Wu, L.H. Chen, "A Study On Visual Cryptography", Master Thesis, Institute of Computer and Information Science, National Chiao Tung University, Taiwan, R.O.C., 1998.