VISUAL CRYPTOGRAPHY FOR SECRET IMAGES: COLOR SCHEME AND PIXEL/BIT SIEVES SCHEME

[1]PARUL SHAH, [2]S.A.MORE

[1,2]Electronics and Telecommunication Engineering,
Department of E & TC India,
RCPIT College of Engineering, Shirpur
E-mail: [1]parul2213@gmail.com, [2]sagar.more27@gmail.com

Abstract— In this paper we used the new color scheme and bit/pixel sieve method for secret image transmission. In new color scheme the secret image was encrypted with natural images without altering the parent image. This will avoid the problem of pixel expansion. The encryption process extracts the feature of the natural image and secret image to form new encrypted image. Bit/ pixel sieve method is a primitive method in cryptography. In this method an encryption was using user defined key and secret image. This method is more suitable for the image whose pixel ratio of black to white pixel is 1. Both the method new color scheme and bit sieve method has specific advantages like data transmission without pixel expansion, ease of data recovered, data quality maintained, no distortion, it reduces the transmission loss & risk. These methods are suitable for the grey, black and white and color images. Both methods are stable and adequate control during transmission. But still there is opportunity to improve for multiple image and pixel / bit sieve method for the image used for more security of data transmission.

Keywords— Visual Cryptography, Key Management, Key Expansion, Secret Sharing, Pixel Expansion & Transmission Risk.

I. INTRODUCTION

Since the use of the Internet and mobile services traffic is increasing and hence the exchange of important data is growing, the security of the exchange of data has become important. There is lot of opportunity for hackers to hack the data of weak link hence securing data is of most important. Cryptography includes some techniques for securing the transmitting or storing data. Cryptography can be categorized into three different scheme s: symmetric cryptography, secret sharing and asymmetric cryptography.

In 1994 Moni Naor and Adi Shamir [1] combined the two mechanisms: secret sharing and traditional cryptography. They introduced a new concept named Visual Cryptography (VC) for the encryption and decryption of printed materials such as text or images. The new scheme used here does not require the complex mathematical operations but only the human visual system for the deciphering of a given printed material. The images consist of randomly located black and white pixels. When stacking these images together, the secret image is revealed. The decryption is executed by the human vision system and only the ownership of all images can reveal the secret. The shares generated by the above method are meaningless and look like random dots. The meaningless shares revels the existence of secrete image and due to that attackers can easily look in to the share. When the shares produced are meaningful images, then the attackers cannot find the secret image. There have been many more image encryption algorithms based on chaotic maps. Also other encryption algorithms based on concepts such as block cipher and selective encryption has been used. Further, encryption process uses chaotic sequence generated by symmetric keys to ensure the security of the used algorithm. The Application of visual cryptography is widely used and discussed, such as: protection of copyright, fingerprint authentication, the bank certification system, control missile launchers, and so on [6-7].

The main concern of all the encryption technique is to secure the important data from being tampered or hacked. The idea of splitting the message into n different pieces such that the original message is visible only when k (or more) of them are used together, but totally invisible if fewer of the k -pieces are used for getting the message. In this method each message is considered as an image of black and white pixels. This image is divided into n slides called transparency. The main objective of this concept is to protect the data develop high security for transmission of images in an open network.

A new cryptographic scheme for securing color image based on visual cryptography scheme used for the encryption and decryption of a color image was a key input. The secret color image which needs to be communicated was spitted, then these images were then converted into binary image, and finally the obtained binary images were encrypted using binary key image. In the decryption process, the shares were decrypted, and then obtained binary images were inversed and combined to get secret color image. Modern day cryptography entails complex and advance mathematical algorithms that are applied to encryption of text and images as well as other file formats.

II. METHODOLOGY

2.1. Method I : New Color Scheme

A new color scheme [2] used natural images randomly and a noise-like share image for transmission to pass a color secret image. Simulation helps to increase in ease of management, pixel expansion and reducing passing risk to effectively protect the transfer image. Process of transfer is explained below in details.

Permutation-based methods have been successfully applied to image encryption, which can obtain encrypted image composed of appearance like Clutter pixels [4-5].

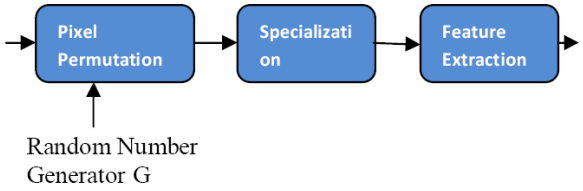

Figure 1 : The Feature Extraction Module

In this process image will be encrypted by extracting the feature of secret images and natural images. During this process input will be original transfer image and other three natural images (n-1). Pixels sizes of natural image and secret images are analyzed. All images are converted to standard bit for analyzing the data. Features extraction process is shown below. Original image and all other natural images are split as per RBG to extract the feature.

If the size of natural and secret image both is W×H, the size of partition block is 8×8pixels.(a,b) denotes the pixel coordinate 1≤ a ≤ W& 1≤ b ≤ H. (a_β, b_β) denotes the pixel coordinate of block β in the top left corner.

$H_\propto^{a,b}$ Is RGB pixel value assumption of (a, b) in $I\alpha$

$$H_\propto^{a,b} = P_{\propto,R}^{a,b} + P_{\propto,G}^{a,b} + P_{\propto,B}^{xa,b}$$

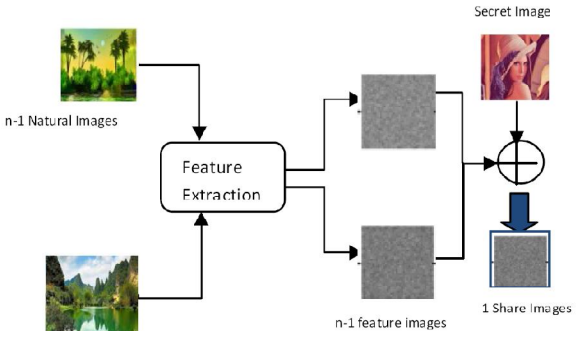

Figure 2: Encryption Process

Random number is use to select the co-ordinates and then values are exchanged. Average value is calculated and then converted into 8x8 bit value. Then XOR operation is used for these values in the process to increase the data security.

M_α^β denotes the average of all the pixel value in block $\beta(H_\propto^{a_\beta,b_\beta}, \ldots, H_\alpha^{a_{\beta+7},b_{\beta+7}})$. & $I\alpha$ denotes the natural share image α , 1≤α<n.

F_α is $I\alpha$ feature matrix. Element $f_\propto^{a,b} \in F_\alpha$is feature matrix of (a,b) $f_\propto^{a,b} = 1$ denotes $I\alpha$ feature matrix in coordinate (a,b) , $f_\propto^{a,b} = 0$ denotes white pixel.

The feature extraction method is represented as $f_\propto^{a,b}$

$$a_\beta \le a \le a_\beta + 7, b_\beta \le b \le b_\beta + 7$$

$$f_\propto^{a,b} = \{^{1, H_\propto^{a,b} < M_\propto^\beta}_{0, otherwise}$$

$P_{\alpha,\emptyset}^{a,b}$denotes the pixel value of I_α color ϕ in the coordinate of (a,b), $\phi \in \{R, G, B\}$.

Natural share image $I\alpha$ is on the plate of color ϕ & $(a$, b) coordinate's pixel value $P_{\alpha,\emptyset}^{a,b}$can be specialized by:

$$p_{\alpha,\emptyset}^{a,b} \leftarrow p_{prev} \oplus p_{\propto,\varphi}^{a,b}$$

The ((n-1, 1), n) can encrypt a sheet of true color image with (n-1) sheets of natural images and a noise-like share. RBG represent the true color image and if the each image represented by 8bit gray then each pixel need to be 24bit. So true color image need to be binary feature matrix and it should be expanded to 24 bit/pixel. Before encryptions natural image feature are extracted and XOR operation with (n-1) feature matrices giving final bit plane. Here to encrypt and decrypt 24bit image is require so it is important to check the bit value of the image and if require convert to 24bit value.

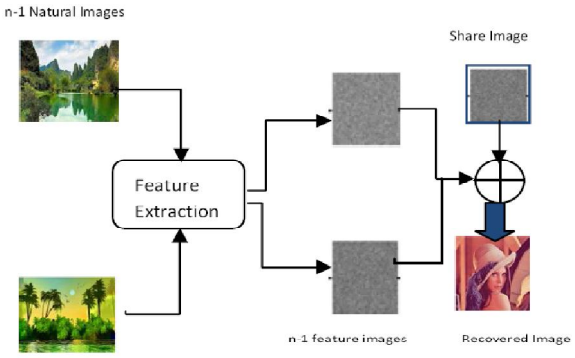

Figure 3: Decryption process

The image used in ((n-1, 1), n)-VCS encryption & decryption algorithm must be a 24-bit/pixel true color image. In this method of new scheme process of encryption of every pixel of bit feature value from secret image is extracted and encrypted with natural image to generate corresponding feature value in matrix. So during decryption reverse logic is followed to get the secret image. Therefore, during decryption image extraction is a process of feature extraction image but also sharing image has not the pixel expansion problem. Accordingly, the process of decryption will also not lead to any pixel expansion.

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

2.2. Method II: Pixel Sieve and Bit Sieve

Pixel Sieve [8] and Bit Sieve [9] is the very basic and simple method used for cryptographic. The cryptographic primitive in discussion here is the pixel-sieve method. After that the bit-sieve method is used in which the black and white pixels from the pixel- sieve, are replaced with 1's and 0's of a binary file. The pixel-sieve is a 2 by 2 secret sharing visual cryptographic method. The sieving process is used to copy the pixels of the original image in one of the shares according to the value of a pixel of the key image. Depending on the value of the pixel of the key, type pixels of the original image are used to create new image.

Table 1: The Basic Bit Sieve

Parameter	Case I	Case II	Case III	Case IV
Image	1	0	1	0
Key	0	1	1	0
S1	x	0	1	x
S0	1	x	x	0

Table 2

Clear Text	1	0	0	1	0	1	0	1	0	1	0	0	1
Key	0	0	0	0	1	1	0	1	0	1	1	0	1
Share 1	x	x	x	x	0	1	x	1	x	1	0	x	1
Share 0	1	0	0	1	x	x	0	x	0	x	x	0	x

Here the share of the image and key is used to encrypt the image. There are few scenario where value is x means won't get any value. Key is given by the user and random number is use and which introduce in the share as noise. In the original pixel sieve method each pixel of the key sieve encrypts only the corresponding pixel in the original image.

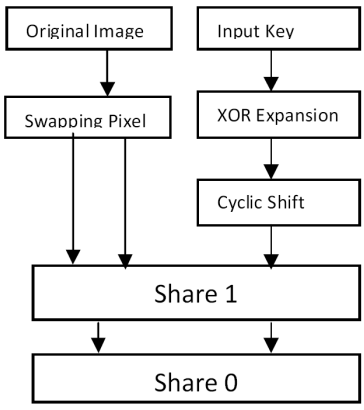

Figure 4: Pixel and Bit sieving

For instance black pixel is 1 while a white pixel is 0. With this the bit-sieve method is produced in Fig. 8. Below scenario are applicable for the output. Hence, if we use a key with some incorrect pixels to decrypt the image, only corresponding pixels will be decrypted incorrectly, while other pixels will be decrypted successfully. Here we have two variables which can be modified to get accurate data. 1) Pixel swapping before encryption 2) Modify the inputted key.

The pixel-sieve method has a problem and it occurs when pixel are concentrated of same type. For example any secret image has more of black pixel then there is opportunity of not able to encrypt the image properly occurs when the number of a color in the key image, is much in favor of one share. Regardless of the quantity of the noise added to the share, because a lot of original data is already in a certain share, the image can be visually interpreted from that share only without the need of decryption. With the reference of few research work there are empirical tests which suggest that a maximum ratio between black and white pixels of the key should not be higher than 3. An ideal ratio between black and white pixels would be 1. Thus the shares could get an equal number of pixels from the original image.

$$R_k = \frac{m}{n} \cong 1 \leftrightarrow m \cong n$$

With R_k is the ratio between black (n) and white (m) pixels of the key.

Here we prefer more swap options to generate more 0's & 1's. Blank or x will be reducing due to factor of 4 to swap the position.

The observations are subjected to further studies on how swap changes the key's entropy. Later the groups of authors further improve the method by adding a cross merge function to a group of 4 shares obtained with the basic sieving method [10].Another team has embedded the sieving technique in a more advanced encryption algorithm [11].

2.2.1 Key Expansion

a) XOR expansion

This operation called modulus 2 addition (or subtraction, which is identical).[12] are used for this. User entered key is generally weak so here proposal is to make key strong and below XOR expansion method can be used. Let there be a binary key X={x_i (0,1)} we intend to build the key Y ={y_i} as follows. First XOR the first two bits of the key X.

$$y_1 = x_1 \text{ XOR } x_2$$

The result is XOR-ed with the second bit of the key. The new result is XOR-ed with the third bit and so on.

$$y_i = y_{i-1} \text{ XOR } x_i \quad i=2,n$$

This is recurring process and we can generate new keys from original keys and XOR-ing them with the current bit of the generated key before repetition of block occurs. We can write the following formula:

$$y_{n+i} = x_i \text{ XOR } y_{n+i-1} \text{ or } y_k = x_{k \bmod n} \text{ XOR } y_{k-1}$$

Where n is the length of the original key and k=(1.2n).There is advantage of this method as with a

small change in original key it led to large changes in expanded key.

b) The cyclical shift

To further increase the length of the generated key we will continue with the same XOR-ing operation but after cyclically shifting the bits of the original key.

$(x_1, x_2, \ldots x_{n-1}, x_n) \rightarrow (x_2, x_3, \ldots, x_n, x_1)$

$x_n = x_1$ and $x_i = x_{i+1}$, $i=(1..n-1)$

For example for an 8 bit (1 byte) long key the expanded keys length is 124 bit.

III. RESULTS AND DISCUSSION

3.1. New Scheme Color Cryptography

From below results for Method I for color scheme with input of secret image and three natural images. After encryption encrypted image is form and later image is decrypted using same natural images.

Figure 5: Input to the Method I

Above secret image is used as input and other natural images N1, N2 & N3 are used to encryption. Encrypted image is used for transmission. And during transmission if there are any attacks then it is difficult to get the secret image as attacker not able to identify all the three images.

One data received by the receiver then image can be decrypted using the natural images as shown below. The original image and encrypted image is same as identified using PSNR and MSE ratio. There is data transferred safely with no pixel expansion. This scheme can be used for both color and gray images. We also try to show the gray color image transfer using another method II.

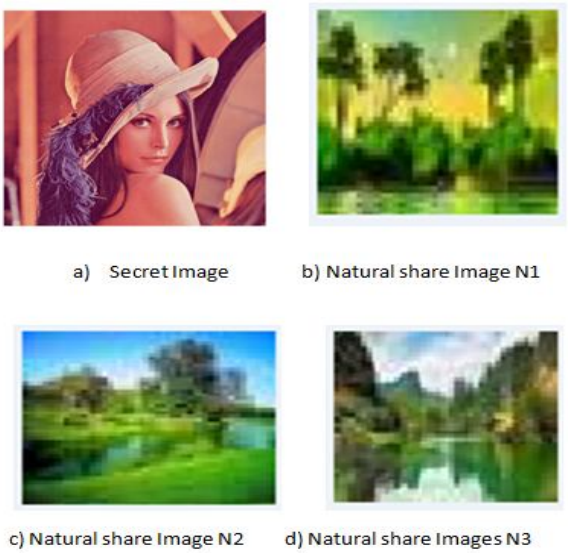

Figure 6: Output of Method I

3.2. Results of Method II : Pixel / Bit sieve.

Secret image is input as shown below and Share image I and share image 2 are the image used for transmission. Encryption with secret image with the key inputted by user. Then share1 and share 2 images was used for transmission. Then using same key the image was decrypted. Original image and decrypted image are same with PSNR = ∞

Figure 7: Result of Method II

If the ratio of the black to white pixel is greater than one then it is preferred to use Method I for transmission. This scheme can be used for both color and gray images.

Table: Comparison of Method I & Method II

Sr. No	Parameter	New color Scheme	Pixel/ Bit
	Input		
1	Images	Secret + Natural Images (n-1)	Secret Images
2	Key	No	Yes
	Processing		
1	Encryption & Decryption	Encryption & Decryption with Natural images	Encryption & Decryption with Key
2	Methodology	Feature extraction using natural images	Pixel / bit sieving with key expansion
3	Random no.	Random no. generation	key used as random no.
	Output		
1	Pixel expansion	PSNR = ∞ MSE = 0	PSNR = ∞ MSE = 0
2	Key management	no	no
3	Additional data structure	Natural Images	Key
4	Image co-relation	1	1
5	Processing time	More	Less
6	Risk control	More	Less R = m/n = 1 (pixel ratio)

CONCLUSIONS

Here visual cryptography is used to transfer the image. As the encryption was with the combination of the natural image or Key then there is no pixel expansion and secret image is extracted in original form. Sharing quality is intact with the original image. Decryption method was reverse of the original image which led to restoring image quality to match with the original image quality and with ease of extraction. Also there was no distortion of the image due to new color scheme and pixel and bit sieving.

Here two methods are discussed with both color and gray image transfer. Both the method is capable to handle the color and gray images. Pixel /bit sieving method are more ideal for the black to white pixel is 1. While color scheme method is suitable for all type of images. Processing time for color scheme is more compare to pixel/ bit sieving method. Depending on application we can choose to adopt appropriate method. Meanwhile the used method is of great security.

ACKNOWLEDGMENTS

It is a privilege for us to have been associated with Prof. S. A. MORE our guide, during this research work. We have been greatly benefited by his valuable suggestions and ideas. It is with great pleasure that we express our deep sense of gratitude for his valuable guidance, constant encouragement and patience throughout this work. We express our gratitude to Prof. Dr. P. J. Deore, Head, and Department of Electronics & Telecommunication for his constant encouragement, co-operation, and support.

REFERENCES

[1] M. Naor and A. Shamir, "Visual cryptography," in *Proc.Eurocrypt'94*LNCS 950, pp. 1–12, 1995.
[2] Xiao-Yi Liu, Ming-Song Chen, and Ya-Li Zhang, "A New Color Visual Cryptography Scheme withPerfect Contrast" 8th International Conference on Communications and Networking in China (CHINACOM), IEEE, 978-1-4799-1406-7,2013.
[3] Incze Arpad "Cryptographic key issues and solutions for the bit sieve/pixel-sieve method" , IEEE, 978-1-4799-3732-5,2014.
[4] LONG Zhuo-min, YU Bin. Chosen Plaintext Attack for Hyper-chaotic System Image Encryption Algorithm . Computer Engineering, 38(17):148-151,2012.
[5] SHU Yong-lu, ZHANG Yu-shu, LI Jing. Image encryption algorithm based on the synchronization of permutation and diffusion . Journal of Lanzhou University (Natural Sciences), 48(2): 113-116,2012.
[6] G D Park, E J Yoon, and K Y Yoo.A New Copyright Protection Scheme with Visual Cryptography. Second International Conference on Future Generation Communication and Networking Symposia,60 - 63,2008.
[7] M Ulutas, G Ulutas, and V V Nabiyev. Medical image security and EPR hiding using Shamir's secret sharing scheme. Journal of Systems and Software9,84(3):341-353,2011.
[8] Incze A., "Pixel Sieve method for secret sharing & visual cryptography", Proceedings of the 9th RoEduNet IEEE International conference, Sibiu,24-25 June, 2010.
[9] Incze A., Moldovan Gr., Muntean M. "From pixel sieve to bit sieve. Bit level based secret sharing cryptographic method", in proceedings 11th International symposium CINTI, Budapest, 978-1-4244- 9278-7, Nov 2010.
[10] Choudhary v., Kumar P., Kumar K., D.S. Singh "An improved Pixel Sieve method for Visual Cryptography", International Journal of Computer Applications, Volume 12 No., ISSN 0975-8887, 9 January 2011.
[11] Venkatesh M.R. , Roopanjali. Daddi, "SDS Technique for Secret Image Encryption", International Journal of Engineering Research & Technology (IJERT) Vol. 2 Issue 4, ISSN: 2278-0181, April – 2013.
[12] Churchhouse, R. " Codes and Ciphers: Julius Caesar, the Enigma and the Internet", Cambridge: Cambridge University Press,ISBN 978-0-521-00890-7,2002.

★★★