

Sharing a Secret Image Based in CMY model using RSA Method in Visual Cryptography

Asmaa HILMI, Soufiane MEZROUI, Ahmed EL OUALKADI
Abdelmalek Essaadi University
National school of applied sciences of Tangier (ENSAT)
Laboratory of Information and Communication Technologies (LabTIC)
ENSA Tanger, Route Ziaten, BP 1818, Tanger principale, Morocco

Abstract. Many technics in visual cryptography are proposed for sharing a secret message. Among the methods cited in the literature the one of creation the secure shares based in RGB color, using AES (Advanced Encryption Standard), and ECC (Elliptical Curve Cryptography) algorithms. Our proposed technique consists to share the secret image in multiple shares. First the original image is decomposed to the CMY colors, after we created the multiple shares. This multiple shares are used to transfer the secret image by using the encryption and decryption RSA algorithm. The principle consists the created the number of shares based on the number of basics matrices, after we apply the RSA algorithm in the encryption process for each share and decryption process.

Keywords: visual cryptography, XOR, share, RSA, encryption, decryption

1 Introduction

In the face of cyber theft, internet thread and hacker, there is a big demand to organisation for realising a transmission secure and realable of these informations and properties. Based on Naor and Shamir method [1], visual cryptographic scheme (VCS) is a special type of secret sharing scheme, where the secret is a black and white image. A VCS is able to code a secret image into k shadow image, the general principle that with k or more than k we reconstruct the secret image, but we cannot have any information with less than k . All share is printed on a distinct transparency [2], encryption and decryption method are done for each share. When all shares are superimposed, the original image should be visible. color visual cryptography is presented [3], which can encrypt the color secret messages into RGB color or with the complementary color CMY (Cyan, Magenta, Yellow). Two mathematical operations used: the booleen OR and the booleen XOR [4]. However the schemes based on operation OR (OVCS) suffer from the huge size of sharing (reflected by the pixel expansion) and poor quality (reflected by contrast) of the recovered secret image. It is for this reason that the schemes based on operation XOR (XVCS) has been studier to achieve advanced properties such as good contrast and resolution.

This paper is organized as follows. A review of some related works is given in Section II. Section III the proposed methodology and gives an overview about RSA cryptosystem. Section IV presents the implementation of the proposed method scheme, the original image,

the shares and the encrypted and decrypted shares. Finally, the conclusion is given in Section V.

2 Related Works

In [5], Shankar K and Eswaran created a modern cryptographic technique of sharing a secret with encapsulated shares. They created a separate matrix R_i , G_i , B_i from the RGB color. The basic matrices of RGB color are obtained by dividing each and every value in R_i , G_i and B_i by 2. Once the shares are created, it is encrypted separately by using Advanced Encryption Standard (AES) algorithm.

In [6,7], the proposed method of Shankar K and Eswaran is used to create the shares from their pixel value of RGB, the extracted pixel values are used to create the multiple shares (share1, share2, ..., share n) and then the image shares are divided into blocks. The blocks of each share are encrypted by using ECC (Elliptical curve cryptography) method and the encrypted image is decrypted by using the decryption of ECC method.

3 Proposed methodology

As we reworked in related work, the methods proposed in the state of art consist in creating the shares of each color R, G and B, after encrypting and decrypting them. In our proposed methodology, we have tried to create the shares from the three colors, ie; each share will contain $C_i + M_i + Y_i$.

The proposed methodology is used to send the original image from the sender to the receiver. The figure 1 shows the block diagram of the proposed method.

From the original image we based on the model CMY to present the colors, because (R, G, B) and (C, M, Y) are complementary colors. In fact the two models colors (R, G, B) and (C, M, Y) have the following relationships: $C = 255-R$; $M = 255-G$; $Y = 255-B$; white (0, 0, 0) and complete black (255,255,255).

The pixel values are taken into consideration to create the basic matrices (C_i, M_i, Y_i). The basic matrices C_1, C_2, C_3 , M_1, M_2, M_3 and Y_1, Y_2, Y_3 are obtained by using modulo 3 in C_i, M_i and Y_i . After we created the shares, in this case we have 2^3 shares for each C_i, M_i, Y_i colors. The multiple shares are encrypted by using the RSA method, and the encryption shares are decrypted by using RSA method. The public and private keys in encryption and decryption are using randomly. The final image will be compared to the original image.

2.1 Shares creation

The original image is extracted in three pixel color CMY and given by,

$$PIXEL = \sum C + M + Y \quad (1)$$

A pixel value is considered for each color. With these pixel value, we crate the basics matrices., these values are separated in three basic matrices according to the following relations:

$$C1 = M1 = Y1 = 1 \text{ mod } 3 \quad (2)$$

$$C2 = M2 = Y2 = 2 \text{ mod } 3 \quad (3)$$

$$C3 = M3 = Y3 = 1 \text{ mod } 3 \quad (4)$$

We have three basics matrices (i=3), then the number of shares is equal $2^3 = 8$.

The basic matrices constructed from the pixel value of the C,M, Y and the shares are created according to the following :

$$Cs1 = C1 \oplus Km \oplus 128 \quad (5)$$

$$Cs2 = Cs1 \oplus C2 \quad (6)$$

$$Cs3 = C \oplus 128 \quad (7)$$

$$Cs4 = Cs3 \oplus Km \quad (8)$$

$$Cs5 = Cs1 \oplus C \quad (9)$$

$$Cs6 = C \oplus C2 \oplus Km \oplus 128 \quad (10)$$

$$Cs7 = C \oplus C3 \oplus Km \oplus 128 \quad (11)$$

$$Cs8 = Cs6 \oplus Km \quad (12)$$

Csi, i=1...8, denote the shares, Ci, i=1..3, denote the basic matrices, C is the Cyan color and Km is the generated random key, its size is that of the original image.

We repeat the same process to two other pixels to get the eight shares of Magenta color; Ms1,Ms2....Ms8, and the eight shares of yellow color; Ys1, Ys2....Ys3.

2.2 RSA cryptosystem

RSA Cryptosystem is one of the first public-key cryptosystems and is widely used to secure data transmission. In such a cryptosystem, the encryption key is public and it is different from the decryption key which is kept secret (private). [8].

The RSA public-key cryptosystem was developed by R.L. Rivest, A. Shamir, and L. Adleman in 1978 [9]. The RSA cryptosystem is simply the modular exponentiation.

The modulus n is the product of two large prime's p and q, public and private keys are obtained by:

$$ed = 1 \text{ mod } \varphi(n) \quad (13)$$

The encryption operation is performed using the public key n and e as follows:

$$C = M^e \text{ (mod } n) \quad (14)$$

Where M is the plaintext such that $0 < M < n$ and C is the ciphertext which can be decrypted using the private key n and d as follows:

$$M = C^d \pmod{n} \quad (15)$$

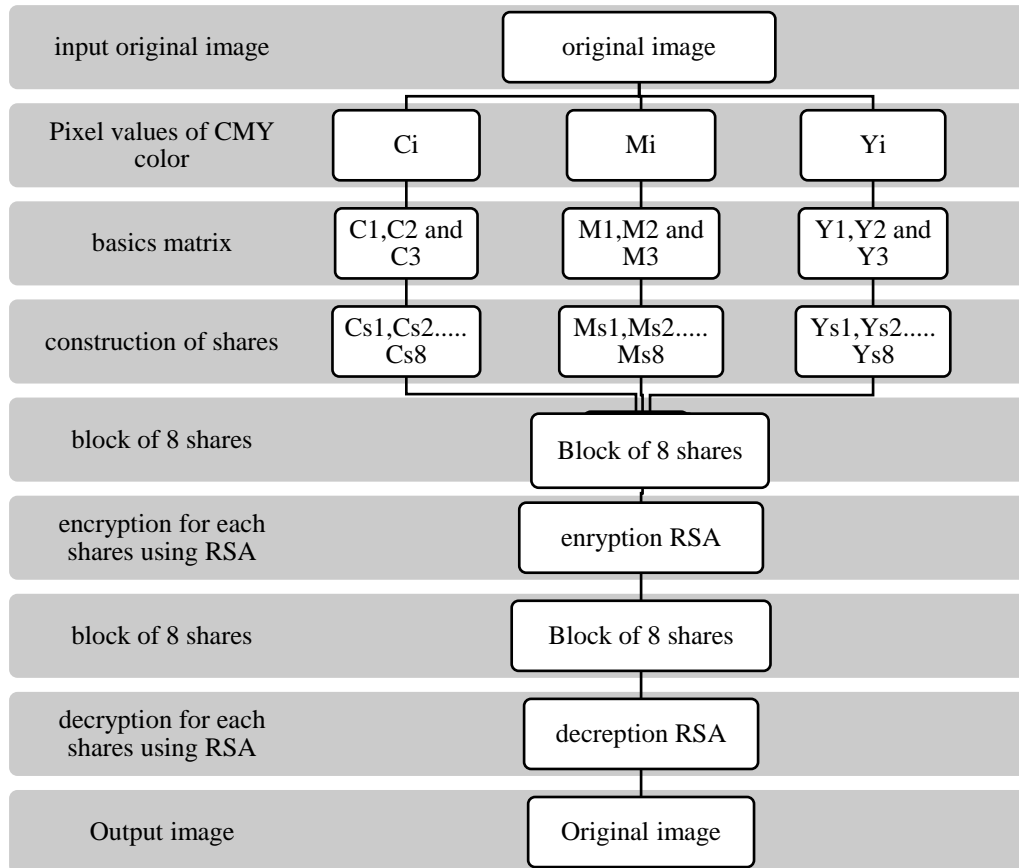


Fig. 1. Block diagram of the proposed method.

3 Results and discussions

In this paragraph we have presented the methods to realize our proposition, as well as a recapulative table which presents the shares, encrypted and decrypted shares.

3.1 Pseudo code of proposed methodology

In Step1, we input the original image, after we extract the pixel values from the input image to create the basic matrices. One key matrix is generate randomly with size of the original image. The multiple shares are created from CMY pixel values where $s=2^i$. The shares for each color are created using the XOR function according to the algorithm above.

$$\begin{aligned} \text{SHARE1} &= C_{s1} + M_{s1} + Y_{s1}. \\ \text{SHARE2} &= C_{s2} + M_{s2} + Y_{s2}. \\ \text{SHARE3} &= C_{s3} + M_{s3} + Y_{s3}. \\ \text{SHARE4} &= C_{s4} + M_{s4} + Y_{s4}. \\ \text{SHARE5} &= C_{s5} + M_{s5} + Y_{s5}. \\ \text{SHARE6} &= C_{s6} + M_{s6} + Y_{s6}. \\ \text{SHARE7} &= C_{s7} + M_{s7} + Y_{s7}. \\ \text{SHARE8} &= C_{s8} + M_{s8} + Y_{s8}. \end{aligned}$$

We apply the encryption method based on RSA method for each shares using the public key, in the decryption method private key is used to decrypt the 8 encrypt shares. All decrypt shares are stacked together to get the original image.

3.2 Experimental results

The proposed method is implemented by using MATLAB Simulator. The experimental result obtained from the implementation of the proposed method scheme, the original image, the shares and the encrypted and decrypted shares are represented in table2.

Table 1. Decomposition of image in RGB model and CMY model.


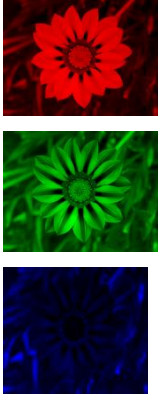








Image RGB	Decomposition color RGB	Convert to CMY	Image CMY
			

Table 2. Proposed method the secret image, the shares, encrypted, decrypted and final image.

Input image	Eight shares	Encrypted shares	Decrypted shares	Output image	Convert to RGB
					

3.3 Discussions and Comparisons

The simulation gives three final images; the first we apply the XOR with the image given after decryption and the model RGB, the second is the image realized after decryption, the third we apply the XOR with the image given after decryption and the model CMY.

The table 2 summarizes the results of our work, also it compares our results with the case of Shankar and Erswan.

The SHANKAR and ERSWAN method is working on the ordinary decomposition color RGB. In our methodology we work with the CMY model, which presents more details of the colors. The choice of RSA cryptosystem is based on the type of encryption that is encrypted by block of characters, which prevents a cryptanalyst from using the frequency analysis to try to break the keys. Moreover, with this method; the encryption is asymmetric which solves the problem of key communication. However AES is a symmetric encryption and ECC needs more computation during encryption and signature verification.

The figure 2 presents a comparison the different steps of construction the two methods. SHANKAR and ERSWAN method create 4 shares for each color, which gives 12 shares to encrypt and decrypt, that increases the processing time of encryption and decryption, on the other hand in our methodology, we have encrypted and decrypted only 8 shares. The algorithm proposes in our method to mix the three colors in each share increases the level of security and make the deciphering for a hacker a difficult thing.

Table 3. Table presents a comparison to results of our methodology and Shankar and Erswan methodology.

	Color decomposition	Basics matrix	Number of shares	Encryption and Decryption method
Our Methodology	CMY	3	8	RSA
SHANKAR,ERSWAN Methodology[5,6,7]	RGB	2	4	AES, ECC

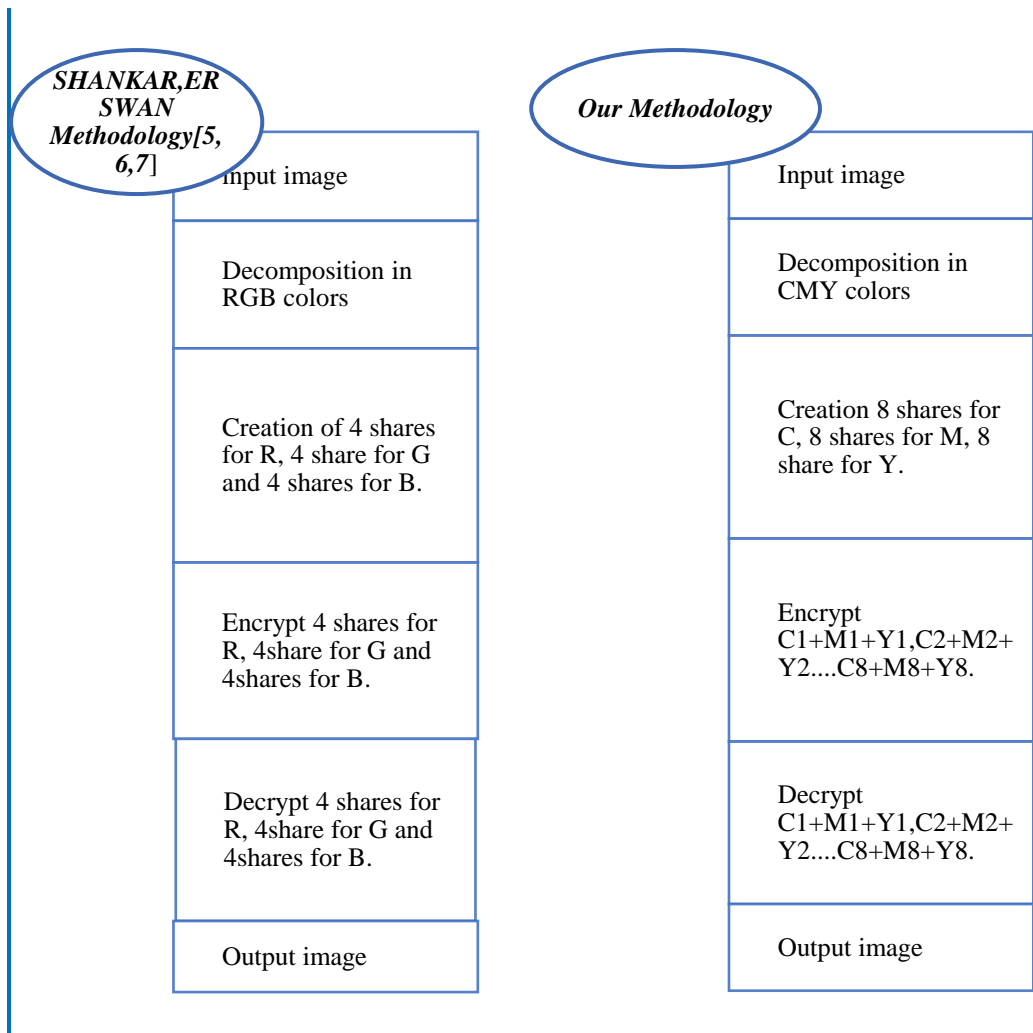


Fig. 2. Comparison between our methodology and SHANKAR,ERSWAN methodology.

4 Conclusion

In this paper, the original image is decomposed in CMY colors, the shares of the secret image are created by using an algorithm of decomposition the basics matrices, after this shares is encrypted and decrypted using the RSA method. This type of work will increase the security of document sharing, it is a method that will be added to the work of shankar and

eswaran. in our methodology, we have to increase the number of basic matrices and the number of shares to augment the degree of security and to make the decryption for an attacker difficult.

References

- [1] M. Naor and A. Shamir, "Visual cryptography," in *Advances in Cryptology — EUROCRYPT'94.*, 1994.
- [2] W.Q. Yan, D. Jin and M. S. Kankanhalli, "Visual cryptography for print and scan applications," in *IEEE International Symposium on Circuits and Systems, Vancouver, 2004.*
- [3] Y.C. Hou, C.Y. Chang, and SF Tu, "Visual cryptography for color images based on halftone technology," in *Proc. of International Conference on Information Systems, Analysis and Synthesis, World Multiconference on Systemics, Cybernetics and Informatics, 2001.*
- [4] A. Adhikari, "Linear algebraic techniques to construct monochrome visual cryptographic schemes for general access structure and its applications to color images," *Des. Codes Cryptogr.*, vol. 73, pp. 865–895, December 2014.
- [5] K. Shankar† and P. Eswaran "Sharing a Secret Image with Encapsulated Shares in Visual Cryptography" *4th International Conference on Eco-friendly Computing and communication Sysrem, ICECCS, 2015.*
- [6] K. Shankar† and P. Eswaran "RGB-Based Secure Share Creation in Visual Cryptography Using Optimal Elliptic Curve Cryptography Technique" *Journal of Circuits, Systems, and Computers Vol. 25, No. 11 (2016) 1650138 (23 pages), 2016.*
- [7] K. Shankar† and P. Eswaran "RGB-Based multiple Share Creation in Visual Cryptography with Aid of Elliptic Curve Cryptography" *Network and Security, China Communication , February 2017.*
- [8] Sami A. Nagar ; Saad Alshamma "High speed implementation of RSA algorithm with modified keys exchange 2012, 6th International Conference on Sciences of Electronics, Technologies of Information and Telecommunications (SETIT), 2012.
- [9] R. L. Rivest, A. Shamir and L. Adleman "A method for obtaining digital signatures and public- key cryptosystems" *Communications of the ACM*, vol. 21, pp. 120-126, 1978.