Comparison of Secret Color Image Sharing Based on XOR Operation in RGB and YCbCr Color Model

Rinaldi Munir
School of Electrical Engineering and Informatics
Institut Teknologi Bandung (ITB)
Bandung, Indonesia
rinaldi.munir@itb.ac.id

***Abstract*—Visual cryptography schemes for color images usually is performed by expanding every pixel in the secret image into some subpixels in the shared images. Wang's schemes are secret image schemes based on XOR operation without expansion of the pixels so that size of shared images are equal to size of the secret images. The schemes are applied to RGB images. In this paper, a method to perform the schemes with minimal computation is proposed. The secret images in RGB color is transformed to *YCbCr* color model, and computation is performed only on *Y* component. The comparison of computation between *RGB* and *YCbCr* has been done. The results show that by applying the Wang's schemes in *YCbCr* can minimize the computation without loss of quality.**

Keywords*—visual cryptography, color images, Wang's schemes, RGB, YCbCr

I. Introduction

Visual cryptography is a kind of cryptography for visual information (image). It encodes (encrypts) a secret image into some transparancies (also called as *shares*). It decodes (decrypt) information directly by human visual system without using a computer at all. The secret information in the image is decoded by stacking the transparancies and then we see the information visually. Visual cryptography is claimed to be perfectly secure because a share contains no information about the secret image. This concept of visual cryptography firstly was published 1994 by Naor and Shamir [1]. In the simple case, a secret image is split into two shares, and to reconstruct the secret image, the two shares are stacked together (Fig. 1). The scheme is then extended to *k* out of *n* sharing scheme or we call it as (*k*, *n*) threshold scheme. In the threshold scheme, a secret image is split into *n* shares, every participant get an individual share. To decode the secret information, *k* or more participants stack their shares. However, no information obtained when *k* – 1 participants stack their shares.

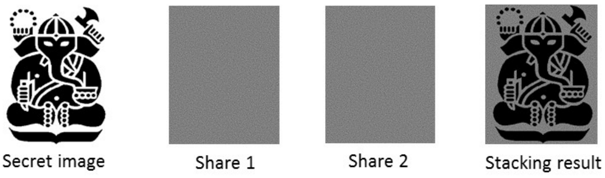


Fig. 1 Example of Naor and Shamir's visual cryptography scheme

Originally, Naor and Shamir applied their scheme on black and white image only. In their scheme, a pixel is split into two subpixels. A pixel is encrypted as two subpixels in each of the two shares. In 1996 and 1997, Rijmen & Preneel [2] and Verheul & Tilborg [3] developed the schemes that applied to color secret images. Next, some researchers developed more advanced visual cryptography schemes based on steganography by sharing and hiding the color image into multiple meaningfull images [4, 5].

All of secret image sharing schemes, in encoding phase, expand one pixel into multiple sub-pixels. For example, one pixel is expanded into four subpixels. As the consequence, size of the shared image increases four times larger than the original image. In addition, the reconstructed image loss of contrast. It contains noises that make it look like a noisy image. In 2005, Wang et all proposed a secret color image sharing with easy encryption, decryption, lower computation complexity, without pixel expansion and better contrast [6]. The secret image can be reconstructed by using XOR operation. In computer XOR is a elementer and simple operation that make it apply to cryptographic system. There are two threshold scheme that was be proposed (later we call them "the Wang's schemes"). The first scheme is (*n*, *n*) threshold scheme with no pixel expansion and the relative contrast difference is 1, which the secret image is reconstructed based on XOR operation. The second scheme is (2, *n*) with no pixel expansion and the relative contrast difference is ½., the secret image can be reconstructed by using XOR and AND operation. The (*n*, *n*) threshold scheme can recover the image same exactly with the original image, whereas in the (2, *n*) scheme the recovered image contains noises.

978-1-5386-0475-5/17/$31.00 ©2017 IEEE

The Wang's schemes apply to binary images, grayscale images, and color images. For color images, the schemes support the bitmap images in *RGB* color space. Red, green, and blue are primary color components of the color space. Every single component is represented by 8 bits, therefore each component represents integer values 0-255. XOR operation can be applied to each color component. Because of there are three color components, therefore XOR operation must be performed three times, each for *R*, *G*, and *B* component. It is not efficient and time consuming. To evercome this problem, the secret color image in the *RGB* model is transformed to other color model which contains the luminance component. One of the color model is *YCbCr*, *Y* is the luminance component, *Cb* and *Cr* are the chrominances components. XOR operation is sufficient performed to the luminance component only. After applying the Wang's schemes, the shares or the reconstructed image must be transformed back to the *RGB* model. This paper will explain a method to apply the Wang's schemes in *YCbCr* model and compare its performances with *RGB* model.

The paper is organized into five sections. The first section is this introduction. The second section will review the related works about visual cryptography, the Wang's schemes, and the color space models (*RGB* and *YCbCr*). The method will be explained in the third section. The fourth section will discuss the experiment results. We resume the conclusion in the last section.

II. Related Works

A. Naor and Shamir's Visual Cryptography Scheme

Naor and Shamir proposed a visual cryptography scheme for binary images. In this scheme, an binary image is assumed as a collection of white and black pixels. Each pixel is subdivided into a collection of *m* black and white subpixels in each of *n* shares. A white subpixel is represented as a 0 and a black subpixel is represented as a 1. Fig. 2 illustrates a scheme with $m = 2$. When two shares are stacked, human visual will perceive the reconstructed pixel as "black" or "white". Black pixel will be sight as perfect black, whereas white pixel will sight contains noises, however human visual can still perceive information in the reconstructed image.

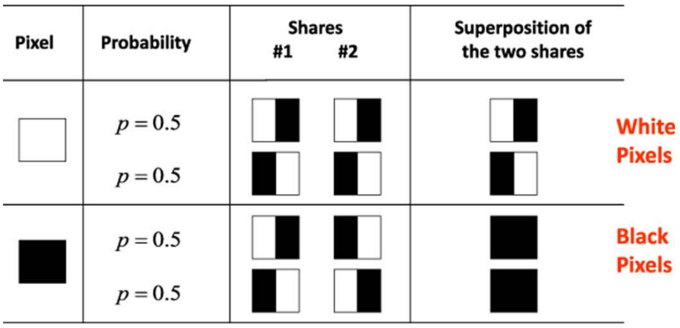


Fig. 2 Illustration of a 2-out-of-2 scheme with 2 subpixel construction [7]

Parameter *m* is pixel expansion. It refers as the number of sub-pixels in the share to represent a pixel in the original image. The greater *m* causes loss of the resolution in the reconstructed image. Therefore, it is desirable *m* is as minimum as possible [6].

The reconstructed image will be loss of contrast. The contrast is defined as the difference gray level of black and white pixels. The relative difference contrast α is defined as the difference in contrast between the original image and the reconstructed image [6]. The α represents loss of contrast. To minimize of loss of contrast, it is desirable the relative contrast difference α as large as possible.

B. Wang's Secret Color Image Sharing Schemes

On 2005, Wang et. al proposed a secret color image sharing schemes based on XOR operation [6]. The schemes support the color image in *RGB* model. XOR operation is defined as follows: $1 \oplus 1 = 1$, $1 \oplus 0 = 1$, $0 \oplus 1 = 1$, and $0 \oplus 0 = 1$. Assume that the original image which has resolution of $M \times N$ is represented as matrix $A = [a_{ij}]$, a_{ij} represents gray level of the pixel, $a_{ij} \in \{0, 1, ..., c-1\}$, $i = 1, 2, \ldots, M, j = 1, 2, \ldots, N$. There are two proposed scheme. The first scheme is (*n*, *n*) threshold scheme with no pixel expansion and the relative contrast difference is 1. The second scheme is (2, *n*) with no pixel expansion and the relative contrast difference is ½., the secret image can be reconstructed by using XOR and AND operation. The (*n*, *n*) threshold scheme can recover the image same exactly with the original image, whereas in the (2, *n*) scheme the recovered image contains noises. Both schemes will be described below.

a. The (*n*, *n*) threshold scheme

Assume that the shared images are $A_1, A_2, \ldots, A_n$. Algorithm of the (*n*, *n*) threshold scheme can be resumed as follows:

(i) Generate $n - 1$ random matrix $B_1, B_2, \ldots, B_{n-1}$ of the same size as matrix *A*. Matrix $B_k = [b_{ij}]$, $b_{ij} \in \{0, 1, ..., c-1\}$.

(ii) The shares are produced as a sequence of XOR operation:

$$\begin{aligned} &A_1 = B_1 \\ &A_2 = B_1 \oplus B_2 \\ &\ldots \\ &A_{n-1} = B_{n-2} \oplus B_{n-1} \\ &A_n = B_{n-1} \oplus A \end{aligned} \tag{1}$$

To reconstruct the image, XOR-ing all the shares as follows:

$$A_1 \oplus A_2 \oplus A_3 \oplus \ldots \oplus A_{n-1} \oplus A_n$$
$$= B_1 \oplus (B_1 \oplus B_2) \oplus (B_2 \oplus B_3) \oplus \ldots \oplus (B_{n-2} \oplus B_{n-1}) \oplus B_{n-1} \oplus A$$
$$= (B_1 \oplus B_1) \oplus (B_2 \oplus B_2) \oplus (B_3 \oplus \ldots \oplus B_{n-2}) \oplus (B_{n-1} \oplus B_{n-1}) \oplus A$$
$$= (0 \oplus 0 \oplus \ldots \oplus 0) \oplus A = 0 \oplus A = A$$

The reconstruction process above implies the (*n*, *n*) scheme can recover the image same exactly with the original image

b. The (2, *n*) threshold scheme

This scheme uses AND operation (symbolized by ∧) and XOR operation. Algorithm of the (2, *n*) threshold scheme can be resumed as follows:

978-1-5386-0475-5/17/$31.00 ©2017 IEEE

(i) Generate $n + 1$ random matrix $B_1, B_2, \ldots, B_{n+1}$ of the same size as matrix A. Matrix $B_k = [b_{ij}]$, $b_{ij} \in \{0, 1, ..., c - 1\}$.

(ii) The shares are produced as a sequence of XOR operation:

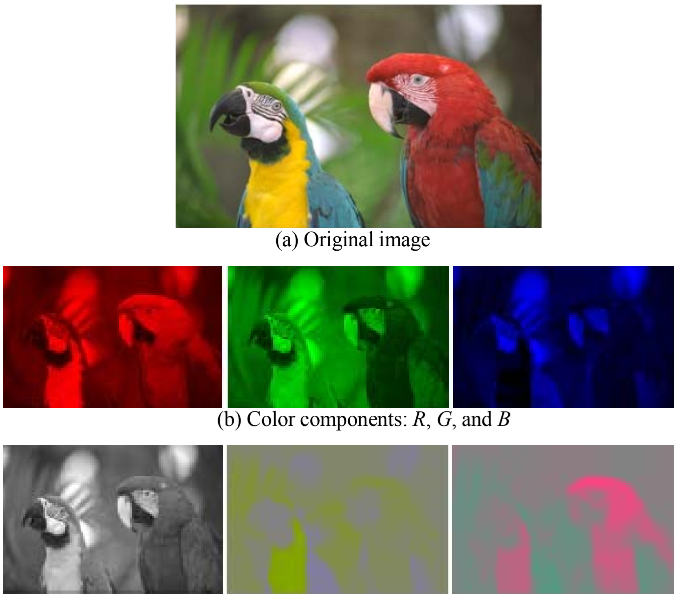
$$\begin{aligned} C_i &= B_i \wedge A \quad (i = 1, 2, \ldots, n) \\ A_i &= B_{n+1} \oplus C_i \quad (i = 1, 2, \ldots, n) \end{aligned} \tag{2}$$

To reconstruct the image, XOR-ing any two shares, however the reconstructed image will contain noises, but the information in the image still could be perceived.

C. RGB to YCbCr Conversion

Real images usually are represented in *RGB* color space. However, in digital image processing, the image in *RGB* color space need to be converted to other color space, since the human visual system has different sensitivity to color and brightness [9]. One of the color space is *YCbCr*. *YCbCr* color space is widely used because we could take advantage of the lower resolution capability of the human visual system for color with respect to luminosity [8].

In *YCbCr* color space, *Y* is luminance, *Cb* is Chrominance-blue and *Cr* is Chrominance-red components. *Y* component represent the brightness of the pixel, whereas the two chrominance components represent the color perception of the pixel. Fig. 3 shows an image and its three components each in *RGB* and *YCbCr* color space [10].



(a) Original image

(b) Color components: *R*, *G*, and *B*

(c) Color components: Y, Cb, Cr

Fig. 3 Example if an image in RGB and YCbCr color space [10]

To convert an image from *RGB* to *YCbCr* color space in range of 8 bits, use the following equation [11]:

$$\begin{bmatrix} Y \\ Cb \\ Cr \end{bmatrix} = \begin{bmatrix} 0 \\ 128 \\ 128 \end{bmatrix} + \begin{bmatrix} 0.299 & 0.587 & 0.114 \\ -0.169 & -0.331 & 0.500 \\ 0.500 & -0.419 & -0.081 \end{bmatrix} \begin{bmatrix} R \\ G \\ B \end{bmatrix} \tag{3}$$

Conversely, to recover *RGB* color from *YCbCr* color, use the following equation [11]:

$$\begin{bmatrix} R \\ G \\ B \end{bmatrix} = \begin{bmatrix} 1.000 & 0.000 & 1.400 \\ 1.000 & -0.343 & -0.711 \\ 1.00 & 1.765 & 0.000 \end{bmatrix} \begin{bmatrix} Y \\ (Cb - 128) \\ (Cr - 128) \end{bmatrix} \tag{4}$$

In two equation above, range of *R*, *G*, and *B* is [0..255], and range of *YCbCr* is also [0..255].

III. Method

Wang's schemes could be applied to any binary images, grayscale images, or color images. The schemes support the color image in *RGB* model. When we apply it to *RGB* model, have to perform computation each for *R*, *G*, and *B* component. Therefore, to minimize cost of computation, we transform image in *RGB* model to *YCbCr* model.

This section describes methods to apply Wang's schemes in *RGB* model and *YCbCr* model.

A. Applying Wang's Schemes in RGB Model

Suppose the secret image *A* has a size three dimensions, i.e $M \times N \times 3$. Matrix *A* has sub-matrices *R*, *G*, and *B* of the size $M \times N$. For (n, n) scheme, we have to generate $n - 1$ random matrices B_i which has a size $M \times N \times 3$, whereas for $(2, n)$ scheme we have to generate $n + 1$ random matrices B_i. Each of the matrices has sub-matrices *R*, *G*, and *B*. Perform all of operation in equation (1) or (2) three times, each for *R*, *G*, and *B*. The results are the shared images in *RGB* model. To reconstruct the secret image, perform XOR operation to the shares three times, each for matrix *R*, *G*, and *B*.

B. Applying Wang's Schemes in YCbCr Model

Before applying the Wangs's schems, we have to transform the secret image *A* in *RGB* to *YCbCr* model by using equation (3). The result is matrix *A*' which has three submatrix *Y*, *Cb*, and *Cr*. We operate Wang's schemes on *Y* component only. Random matrices B_i have a size $M \times N$. The results are the shared images in *YCbCr* color space. Finally, we transform back the images from *YCbCr* to *RGB* color space by using equation (4). However, *Cb* and *Cr* components do not change so that the shared images still show shadow of the secret image. In order to the shared images look like the random images, we need to perform XOR operation between matrix *Cb* and a random matrix *R* before conversion to *RGB*, so do for matrix *Cr*. Fig. 4 shows applying Wang's schemes in *YCbCr* model to generate the shared images, whereas to reconstruct the secret image is showed in Fig. 5.

978-1-5386-0475-5/17/$31.00 ©2017 IEEE

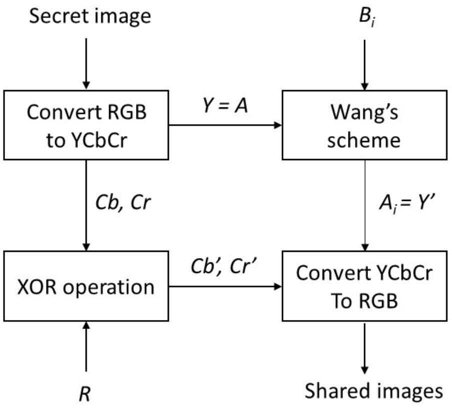


Fig. 4 Generating the shares in *YCbCr* model

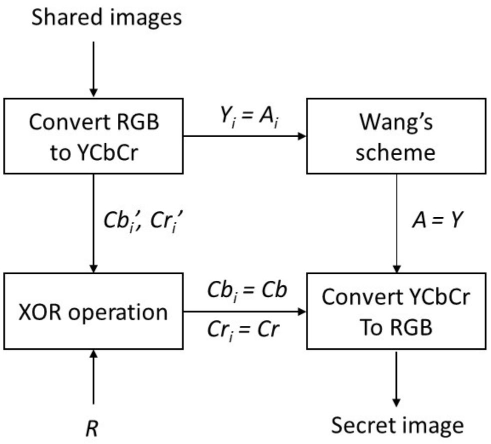


Fig. 5 Reconstruction of the secret image in *YCbCr* model

Now we will calculate time complexity of Wang's schemes when applied in RGB and YCbCr model respectively.

C. Computation complexity of (n, n) scheme in RGB model

There are two computations: generating the random matrices +and XOR operation.

To generate $n - 1$ random matrices B_i of size $M \times N \times 3$, number of computation is

$$T_1(n) = (n - 1) \cdot M \cdot N \cdot 3 = 3MNn - 3MN$$

To yield n shares, number of XOR operation is

$$T_2(n) = (n - 1) \cdot M \cdot N \cdot 3 = 3MNn - 3MN$$

Total of number of computation is

$$T(n) = T_1(n) + T_2(n) = 6MNn - 6MN = O(nMN)$$

To reconstruct the secret image, number of XOR operation is

$$T(n) = (n - 1) \cdot M \cdot N \cdot 3 = 3MNn - 3MN = O(nMN)$$

D. Computation complexity of (2, n) scheme in RGB model

To generate $n + 1$ random matrices B_i of size $N \times N \times 3$, number of computation is

$$T_1(n) = (n + 1) \cdot M \cdot N \cdot 3 = 3MNn + 3MN$$

To yield n shares, number of AND operation and XOR operation is

$$T_2(n) = n \cdot M \cdot N \cdot 3 + n \cdot M \cdot N \cdot 3 = 6MNn$$

Total of number of computation is

$$T(n) = T_1(n) + T_2(n) = 9MNn + 3MN = O(nMN)$$

To reconstruct the secret image, number of XOR operation is

$$T(n) = M \cdot N \cdot 3 = 3MN = O(MN)$$

E. Computation complexity of (n, n) scheme in YCbCr model

To generate $n - 1$ random matrices B_i of size $M \times N$ and one matrix R, number of computation is

$$T_1(n) = (n - 1) \cdot M \cdot N + MN = MNn$$

To yield n shares, number of XOR operation (including XOR operation between Cb/Cr and R) is

$$T_2(n) = (n - 1) \cdot M \cdot N + 2MN = MNn + MN$$

Total of number of computation is

$$T(n) = T_1(n) + T_2(n) = 2MNn + MN = O(nMN)$$

To reconstruct the secret image, number of XOR operation (including XOR operation between Cb/Cr and R) is

$$T(n) = (n - 1) \cdot M \cdot N + 2MN = MNn + MN = O(nMN)$$

F. Computation complexity of (2, n) scheme in YCbCr model

To generate $n + 1$ random matrices B_i of size $N \times N$ and one matrix R, number of computation is

$$T_1(n) = (n + 2) \cdot M \cdot N = MNn + 2MN$$

To yield n shares, number of AND operation and XOR operation (including XOR operation between Cb/Cr and R) is

$$T_2(n) = n \cdot M \cdot N + n \cdot M \cdot N + 2MN = 2MNn + 2MN$$

Total of number of computation is

$$T(n) = T_1(n) + T_2(n) = 3MNn + 4MN = O(nMN)$$

To reconstruct the secret image, number of XOR operation (including XOR operation between Cb/Cr and R) is

$$T(n) = MN + 2MN = 3MN = O(MN)$$

Although application of Wang's schemes in *RGB* and *YCbCr* model has same O-notations, however number of computation of Wang's schemes in *YCbCr* is less than in *RGB* model. This comparison is resumed in Table 1.

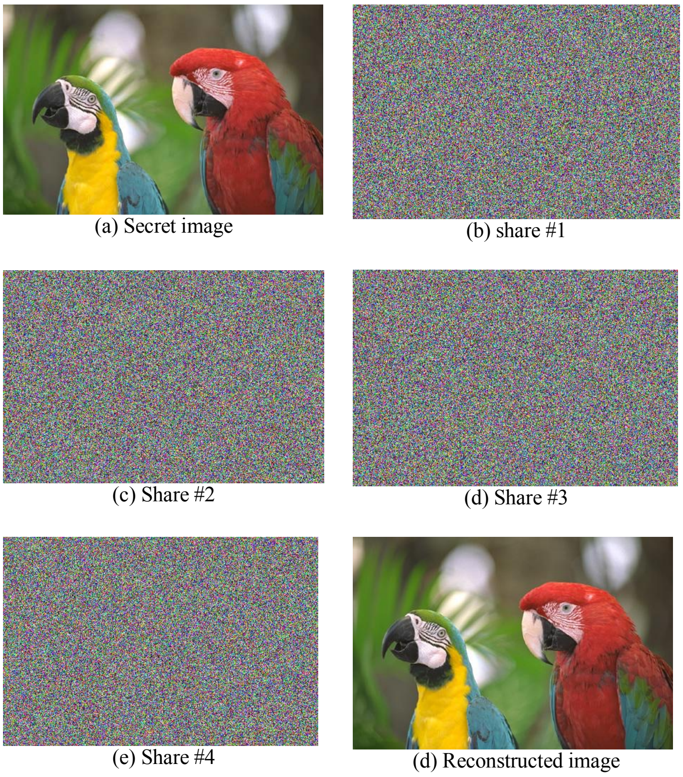
978-1-5386-0475-5/17/$31.00 ©2017 IEEE

TABLE I. COMPARISON OF NUMBER OF COMPUTATION

Scheme	Generating of shares		Image reconstruction	
	RGB	*YCbCr*	*RGB*	*YCbCr*
(n, n)	$6MNn–6MN$	$2MNn+2MN$	$3MNn–3MN$	$MNn+MN$
$(2, n)$	$9MNn+3MN$	$3MNn+4MN$	$3MN$	$3MN$

IV. EXPERIMENT RESULTS AND DISCUSSION

Experiments has been done for both of schemes and color models. We used $n = 4$ for (n, n) and $n = 3$ for $(2, n)$. The test image is *bird.jpg* as shown in Fig. 3(a). It is cropped from [10] and have a resolution 450 × 299. Running time of generating of shares and image reconstruction are noted for each scheme and color model, excluding time for saving the shares and time for displaying the shares or the (reconstructed) image. Reconstructed images of applying the Wang's schemes in *RGB* model and *YCbCr* model are same, we show the secret image, the shares and the reconstructed image in *RGB* and *YCbCr*.



(a) Secret image

(b) share #1

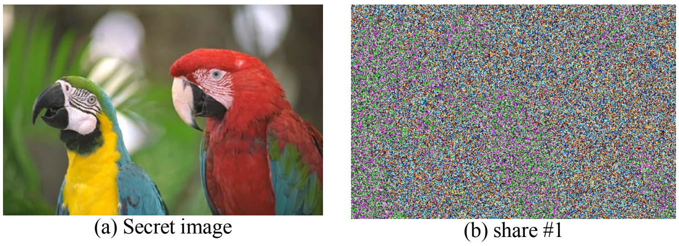
(c) Share #2

(d) Share #3

(e) Share #4

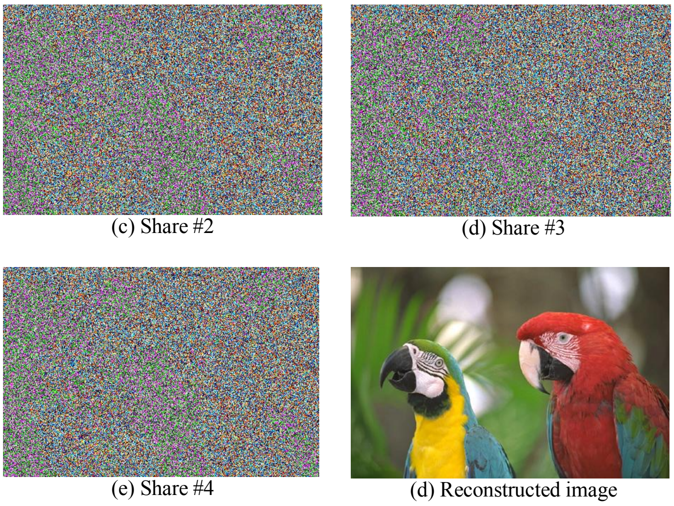
(d) Reconstructed image

Fig. 6 Experiment results of applying (4, 4) threshold scheme in *RGB* color model



(a) Secret image

(b) share #1



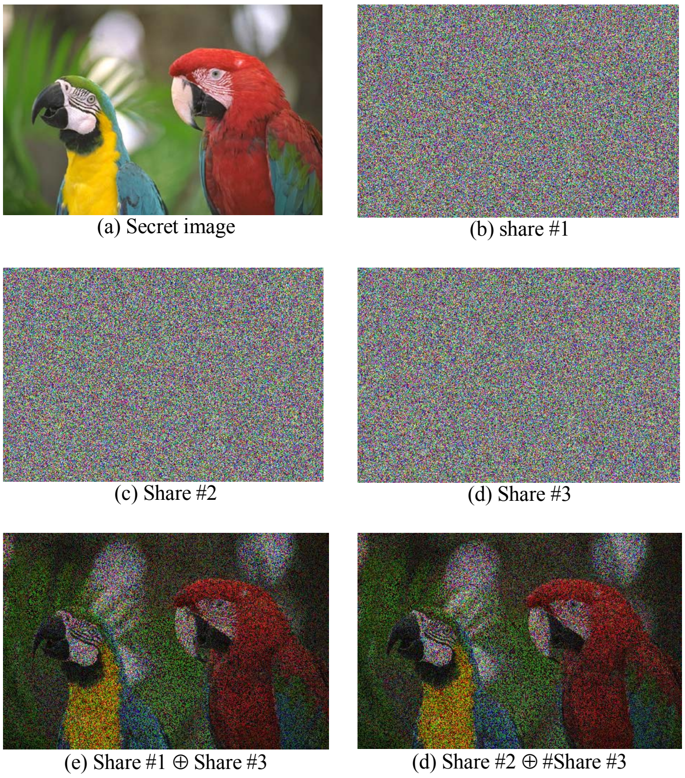
(c) Share #2

(d) Share #3

(e) Share #4

(d) Reconstructed image

Fig. 7 Experiment results of applying (4, 4) threshold scheme in *YCbCr* model



(a) Secret image

(b) share #1

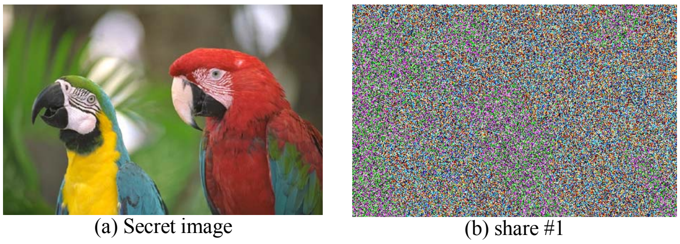
(c) Share #2

(d) Share #3

(e) Share #1 ⊕ Share #3

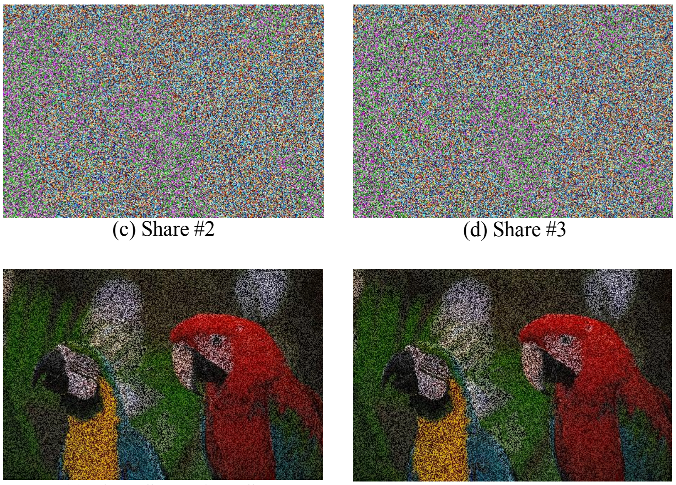
(d) Share #2 ⊕ #Share #3

Fig. 8 Experiment results of applying (2, 3) threshold scheme in *RGB* color model



(a) Secret image

(b) share #1



(c) Share #2

(d) Share #3

(e) Share #1 ⊕ Share #3

(d) Share #2 ⊕ #Share #3

Fig. 9 Experiment results of applying (2, 3) threshold scheme in *YCbCr* model

Fig. 6 and Fig. 7 show the shares and the reconstructed image of applying (n, n) threshold scheme in RGB and YCbCr color model respectively (n = 4). All of the shares have the same size with the original image. The reconstructed images in both model are same exactly with the original image.

Next, Fig. 8 and Fig. 7 show the shares and the reconstructed image of applying (2, n) threshold scheme in RGB and YCbCr color model respectively (n = 3). All of the shares have the same size with the original image. However, he reconstructed images in both model are not same exactly with the original image, the images look like noisy images. This is characteristics of the (2, n) threshod scheme.

The experiments also measure running time of applying the schemes in each color model. We measure time for generating of the shares and time for image reconstruction. Experiments are performed three times to every scheme and every color model to get average of running time. Table II resumes results of the average running time measurement. From the table we have proven that running time of applying Wang's schemes in *YCbCr* model always less than in *RGB* model. Table II meet match with Table I.

TABLE II. COMPARISON OF RUNNING TIME

Scheme	Generating of shares (second)		Image reconstruction (second)	
	RGB	*YCbCr*	*RGB*	*YCbCr*
(n, n)	0.0764	0.0435	0.0026	0.0018
(2, n)	0.2275	0.1250	0.0033	0.0034

V. CONCLUSION

The Wang's schemes could be implemented to encrypt the secret images with visual cryptography both in *RGB* and *YCbCr* color model. Applying the schemes in *YCbCr* color model could save computation time. Based on the experiment results, it has been proven the running time of the schemes in YCbCr always less than in RGB model.

REFERENCES

[1] M. Naor and A. Shamir, Visual cryptography. Advances in Cryptology EUROCRYPT '94. *Lecture Notes in Computer Science*, (950):1–12, 1995

[2] V. Rijmen and B. Preneel, "Efficient colour visual encryption or 'Shared colors of benetton'," *Eurocrypt' 96 Rumpsession Talk,* ttp://www.esat.kuleuven.ac.be/~rijmen/vc/.

[3] E. Verheul and H. V. Tilborg., Constructions and properties of k out of n visual secret sharing schemes. *Designs, Codes and Cryptography, 11(2):179–196, 1997.*

[4] C. Chang, C. Tsai, and T. Chen, A new scheme for sharing secret color images in computer network, Proceedings of International Conference on Parallel and Distributed Systems, pages 21–27, July 2000.

[5] C. Yang and C. Laih., New colored visual secret sharing schemes. *Designs, Codes and Cryptography, 20:325–335,2000..*

[6] Wang, D., Zhang, L., Ma, N., Huang, L., *Secret Color Images Sharing Schemes Based on XOR Operation*. 2005.

[7] Ross, A., Visual Cryptography for Biometric Privacy, *IEEE Transaction on Information Forensics and Security*, Vol. 6, No. 1, March 2011.

[8] Compos, N., RGB to YCbCr conversion, Playing with bits and pixels, an article in http://www.sistenix.com/rgb2ycbcr.html, accesed on 9June 2017.

[9] Jack, K. *Video denystified: a handbook for the digital engineer*. Elsevier, 2011

[10] Colour Images, lecture note in http://www.bk.isy.liu.se, accesed on 9 June 2017.

[11] Colour Conversion, an article in http://www.equasys.de, accesed on 9June 2017.

978-1-5386-0475-5/17/$31.00 ©2017 IEEE