Visual Cryptography of Animated GIF Image Based on XOR Operation

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

***Abstract*—This paper describes application of a secret colour image sharing scheme based on XOR operation to the animated GIF images. The scheme is performed without expanding every pixel in the secret image so that size of shared images are equal to size of the secret images. Originally the scheme supports RGB images. In this paper we apply the scheme to the animated GIF image. A GIF image consists of a color palette and a matrix which entries (pixel values) refer to the palette row. XOR operation is not performed to RGB palette of GIF image, but to the matrix. The scheme is applied to each frame of the animated GIF image. As a result, each participant has his (or her) own share, each share is an animated GIF image where the frames look like the random images. The experiment shows that the scheme could be applied to the animated GIF image well. The original animated GIF image could be reconstructed exactly.**

Keywords—animated GIF image, secret color image sharing, XOR operation, frame

I. INTRODUCTION

An visual information (text, image, etc) could be encrypted with a conventional cipher (DES, AES, RC6, etc). However, the computation for encryption and decryption is more complex and the cost is expensive. Visual cryptography is a kind of cryptography with less computation, especially for decryption. To encrypt a secret image, the image is encoded into some transparencies (also called as *shares*). Decyption of the image does not require a computer, but by using human visual system. The image is reconstructed by stacking the transparencies and user see information in the image visually. This concept is called the secret image sharing scheme and firstly was published 1994 by Naor and Shamir [1]. The scheme is denoted as k out of n sharing scheme or (k, n) threshold scheme. In this scheme, n participants get their own share. To decode the secret information, k or more participants can see the information by stacking their shares. However, $k - 1$ or less participants gain no information. The simple scheme is (2, 2) threshold scheme where a secret image is split into two shares, and to reconstruct the secret image, the two shares are stacked together.

Originally Naor and Shamir defined their visual cryptography concept only to black and white images. Next, some researchers developed visual cryptography for grayscale and colour images [2,4]. For examples, Rijmen & Preneel [2] and Verheul & Tilborg [3] proposed the secret sharing scheme for color images. Not only proposed the secret sharing schemes, some researchers also proposed the visual cryptography schemes combined to steganography. The schemes share and hide the color image into multiple meaningfull images [4, 7].

Unfortunately, all of secret image sharing schemes expand one pixel into multiple sub-pixels, for example one pixel to four subpixels. Of course the resolution size of the shared image increases four times larger. In addition, the reconstructed image loss of contrast. It contains noises that make it look like a noisy image. In 2005, Wang et al. proposed a secret color image sharing scheme without pixel expansion and better contrast [5]. The secret image can be reconstructed by using XOR operation. The scheme is called (n, n) threshold scheme with and can recover the image same exactly with the original image.

The Wang's scheme supports the bitmap images in *RGB* colour space (R = red, G = green, B = blue). 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. A popular format of bitmap image is BMP format, however BMP images is rarely used in *World Wide Web* because of their large size. Alternatively, there is other kind of RGB image but as indexed image, namely GIF image. GIF (*Graphics Interchange Format*) image is a kind of the indexed image. GIF was introduced by Compuserve in 1987 and come into widespread usage on the World Wide Web because of its wide support and portablility. A GIF image uses a palette of up to 256 colors from the 24-bit RGB color space with values in the range [0,1]. The pixel values represent index to a palette row. GIF format supports animaton of images, we call it the animated GIF images. The animated GIF images consist of a number of frames. Each frame was displayed in succession like a video. The animated GIF images is usually used for displaying cartoon, funny images, or other interesting images.

Suppose you have an animated GIF image and want to share the image to n participants by using a secret image sharing scheme. You want the resolution size of the shares are equal to original image and the original image is reconstructed perfectly (from n shares of the participants) without loss of contrast. In addition, the GIF image can be animated such as the original image. The solution is by using Wang's scheme, namely (n, n) threshold scheme.

The main contribution of the paper is the application of Wang's scheme to the animated GIF images. The paper is

978-1-5386-0607-0/17 $31.00 © 2017 IEEE
DOI 10.1109/ACOMP.2017.14

organized into five sections. The first section is this introduction. The second section will review the related works about the Wang's schemes and GIF image. 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. Wang's Secret Color Image Sharing Schemes

On 2005, Wang et. al proposed a secret color image sharing schemes based on XOR operation [5]. The schemes support the color image in *RGB* model. XOR operation is defined as follows:

$$1 \oplus 1 = 0$$
$$1 \oplus 0 = 1$$
$$0 \oplus 1 = 1$$
$$0 \oplus 0 = 0$$

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,* $a_{ij} \in \{0, 1, ..., c-1\}$, $i = 1, 2, ..., M$, $j = 1, 2, ..., N$. 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. This paper describes the (n, n) threshold scheme only, because it is used in the method.

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:

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

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. Fig. 1 shows experiment results of the (3, 3) scheme to image of Lenna (128 × 128) [5]. There are three shares with the same size as the original image. By XOR-ing all shares we will recover the original image exactly.

Refer to authors of the scheme, the algorithm complexity to construct n shares is $O(k_1 n)$ where k_1 is equal to $M \times N$, and the algorithm complexity to reconstruct the image is also $O(k_1 n)$ [5].

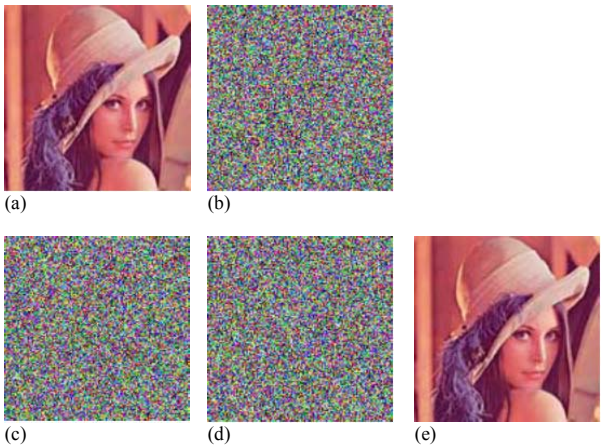


Fig.1. Experiment results [5]. (a) Original secret image with 256 colors; (b)-(d) The shares with the same size as (a); (d) The reconstructed image from the three shares.

B. Animated GIF Images

A GIF image consists of a color palette and a matrix which entries (pixel values) refer to the palette row. Color of the pixel is combination of each channel red (*R*), green (*G*), and blue (*B*) in the palette row. Fig. 2 shows model of a GIF image, the pixel value 5 represents the fifth row of the palette ($R = 0.2902$, $G = 0.0627$, $B = 0.0627$). The color depth of the GIF images is up to 256 colors, therefore the GIF images are suitable for human-made graphics such as cartoon, animation.

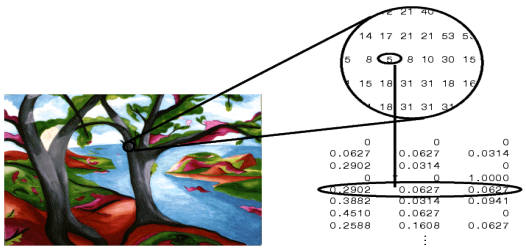


Fig. 2. GIF image structure (Source: Matlab)

The animated GIF images consist of a number of frames, each frame may has independent palette itself. Fig. 3 shows the six frames of 48 frames of an animated GIF image (*walk.GIF*). Every animated GIF image has a property that is called "delay time" in hundredth of seconds. It specifies delay every frame. For example, an animated GIF image contains 40 frames, with

a 0.03 second delay specified between each frame. It means the animated GIF has runtime of 1.2 seconds per loop [6].

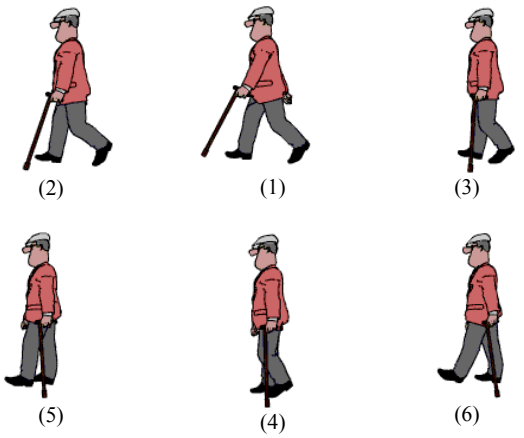


Fig. 3. The first six frames of an animated GIF image [6]

III. METHOD

Suppose an animated GIF image will be share to n participants. The (n, n) threshold scheme will produce n shares, each share is an animated GIF image that look like random image. To recover the original animated GIF image, all participants must be XOR-ing their own shares. As we know, an animated GIF images contains many frames. Assume that there are m frames (A_1, A_2, …, A_m) that denote index matrix of each frame, therefore in order to apply the (n, n) threshold scheme we need to generate $m \times (n-1)$ random matrix B_{k_i} ($k = 1, 2, \ldots, m$, $i = 1, 2, \ldots, n$) as follows:

$\{ B_{1_1}, B_{1_2}, ..., B_{1_{n-1}} \}$: set of random matrix for frame 1

$\{ B_{2_1}, B_{2_2}, ..., B_{2_{n-1}} \}$: set of random matrix for frame 2

⋮

$\{ B_{k_1}, B_{k_2}, ..., B_{k_{n-1}} \}$: set of random matrix for frame k

⋮

$\{ B_{m_1}, B_{m_2}, ..., B_{m_{n-1}} \}$: set of random matrix for frame m

Every set of B_{k_i} will be used to produce n shares A_{k_i} of each frame A_i. In other word, each frame has n shares. Every share with number i ($i = 1, 2, \ldots, n$) of frame k ($k = 1, 2, \ldots, m$) is combined to produce an animated GIF image i. For example, for $n = 3$ and $m = 6$, sequence of XOR operation to produce three shares of each frames A_{k_i} are as follows:

$$\begin{aligned} A_{1_1} &= B_{1_1} & A_{2_1} &= B_{2_1} & A_{3_1} &= B_{3_1} \\ A_{1_2} &= B_{1_1} \oplus B_{1_2} \; ; & A_{2_2} &= B_{2_1} \oplus B_{2_2} \; ; & A_{3_2} &= B_{3_1} \oplus B_{3_2} \\ A_{1_3} &= B_{1_2} \oplus A_1 & A_{2_3} &= B_{2_2} \oplus A_2 & A_{3_3} &= B_{3_2} \oplus A_3 \end{aligned}$$

$$\begin{aligned} A_{4_1} &= B_{4_1} & A_{5_1} &= B_{5_1} & A_{6_1} &= B_{6_1} \\ A_{4_2} &= B_{4_1} \oplus B_{4_2} \; ; & A_{5_2} &= B_{5_1} \oplus B_{5_2} \; ; & A_{6_2} &= B_{6_1} \oplus B_{6_2} \\ A_{4_3} &= B_{4_2} \oplus A_4 & A_{5_3} &= B_{5_2} \oplus A_5 & A_{6_3} &= B_{6_2} \oplus A_6 \end{aligned}$$

Combine all corresponding share to produce three animated GIF images, every animated GIF image for each participants:

The 1st animated GIF image: $\{A_{1_1}, A_{2_1}, A_{3_1}, A_{4_1}, A_{5_1}, A_{6_1}\}$

The 2nd animated GIF image: $\{A_{1_2}, A_{2_2}, A_{3_2}, A_{4_2}, A_{5_2}, A_{6_3}\}$

The 3rd animated GIF image: $\{A_{1_3}, A_{2_3}, A_{3_3}, A_{4_3}, A_{5_3}, A_{6_3}\}$

To reconstruct the animated GIF image, XOR-ing all the shares of each frame i to recovere frame i as follows:

$A_{1_1} \oplus A_{1_2} \oplus A_{1_3} = A_1$ → frame 1

$A_{2_1} \oplus A_{2_2} \oplus A_{2_3} = A_2$ → frame 2

$A_{3_1} \oplus A_{3_2} \oplus A_{3_3} = A_3$ → frame 3

$A_{4_1} \oplus A_{4_2} \oplus A_{4_3} = A_4$ → frame 4

$A_{5_1} \oplus A_{5_2} \oplus A_{5_3} = A_5$ → frame 5

$A_{6_1} \oplus A_{6_2} \oplus A_{6_3} = A_6$ → frame 6

Combine all frames to produce the original GIF images as follows:

$\{A_1, A_2, A_3, A_4, A_5, A_6\}$ → recovered animated GIF image

Fig. 4 shows process to produce the shares of each frame with using (3, 3) threshold scheme. To reconstructed the original frame, three shares (1, 2, 3) will be XOR-ed together to yield the corresponding frame.

Because of the Wang's scheme is repeated to m frames, therefore the algorithm complexity to construct all shares of the animated GIF image is $O(k_1nm)$ where k_1 is equal to $M \times N$, and the algorithm complexity to reconstruct the animated image is also $O(k_1nm)$.

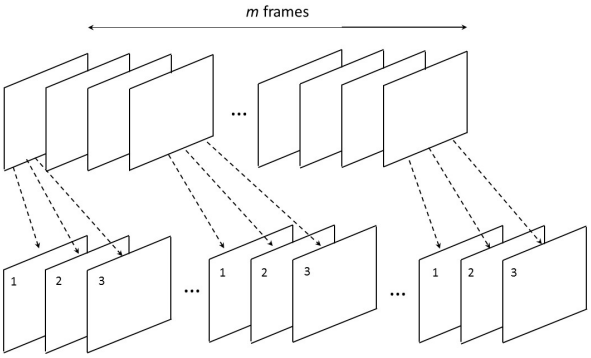
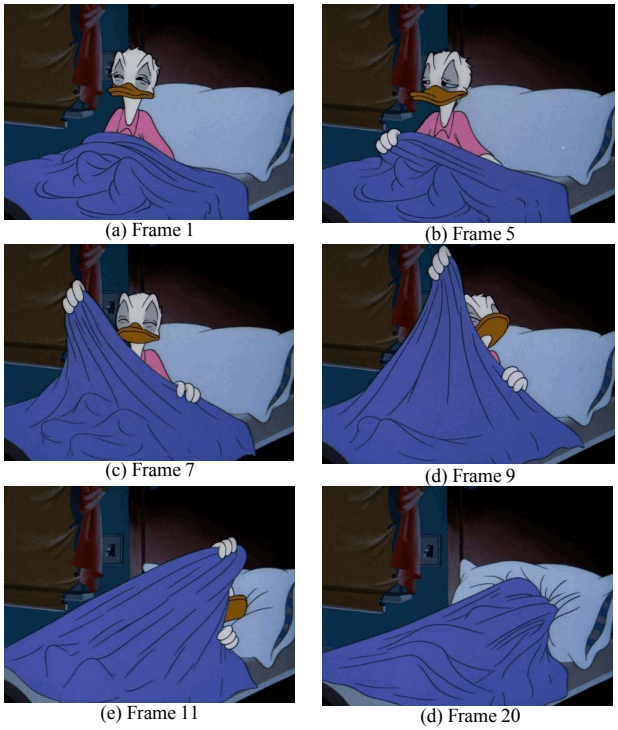


Fig. 4. Process to produce the shares of each frame

IV. Experiment Results and Discussion

The method above has been implemented into a program and experiments has been done. The test animated GIF image is `donald.gif` which has 20 frames. Some frames are displayed in Fig. 5.



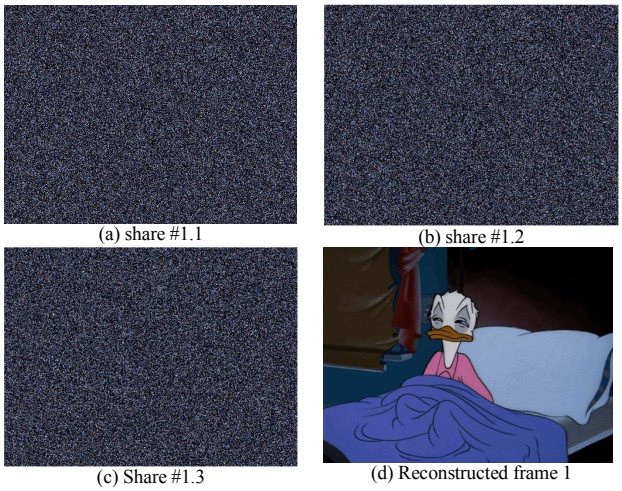
(a) Frame 1 (b) Frame 5

(c) Frame 7 (d) Frame 9

(e) Frame 11 (d) Frame 20

Fig. 5 Some frames of animated GIF image (`donald.gif`)

Suppose there are 3 participants. The `donald.gif` image will be shared to the participants by using (3,3) threshold scheme. The results are three animated GIF images, one for each participant.



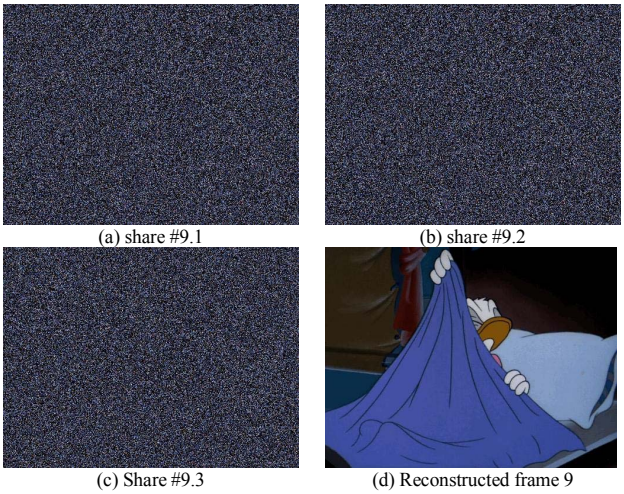
(a) share #1.1 (b) share #1.2

(c) Share #1.3 (d) Reconstructed frame 1

Fig. 6 Three shares of frame 1

Three animated GIF images for every participant are `donald1.gif`, `donald2.gif`, and `donald3.gif`. When the GIF images are displayed on screen, their frames can animate well, but they look like the random images.

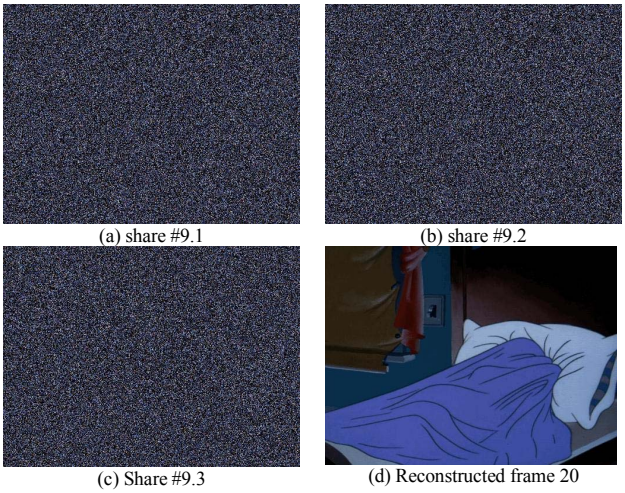
Due to limited space, in this section we show the shares of three frames only. As you see, the shares look like the random images as mentioned above. Fig. 6 shows three shares of frame 1, Fig. 7 show three shares of frame 9, and Fig. 8 shows three shares of frame 20. The shares with number #*x*.1 (*x* = 1, 2, …, 20) are frames in `donald1.gif`, The shares with number #*x*.2 are frames in `donald2.gif`, and The shares with number #*x*.3 are frames in `donald3.gif`. The reconstructed frames are results of XOR-ing of the three shares. The frames can be reconstructed exactly as the original frames.



(a) share #9.1 (b) share #9.2

(c) Share #9.3 (d) Reconstructed frame 9

Fig. 7 Three shares of frame 9



(a) share #9.1 (b) share #9.2

(c) Share #9.3 (d) Reconstructed frame 20

Fig. 8 Three shares of frame 20

V. CONCLUSION

The secret color image sharing of Wang's scheme could be implemented to encrypt the animated GIF image. The scheme is applied to each frame of the image. As a result, each participant has his (or her) own share, each share is an animated GIF image where the frames look like the random images. The experiment shows that the scheme could be applied to the animated GIF image well. The original animated GIF image could be reconstructed exactly. The future work are applying the scheme to other animated image format and digital video.

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

[6] Munir, R., Authentication of Animated GIF Images by Using A Fragile Watermarking Scheme Based on EzStego Algorithm, in proceeding of AUN/SEED-Net Regional Conference for Computer and Information Engineering (RCCIE), Yangon 2016

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