THE IMPROVEMENT OF FLIP (2,2) VISUAL CRYPTOGRAPHY IMAGES USING TWO KEY IMAGES

Ratnadewi[1]; Putri Kartika Sari[2]

[1,2]Department of Electrical Engineering, Faculty of Engineering, Maranatha Christian University,
65th Prof. Drg. Suria Sumantri Street, Bandung, 40164
[1]ratnadewi@engineer.com; [2]pvtrikartika@gmail.com

ABSTRACT

The Flip (2, 2) Visual Cryptography (FVC) is one of the techniques used to encrypt the two secret images into two dual purpose transparencies. The two transparencies can be sent to the objective person. The first secret images can be obtained by stacking the two transparencies and the second secret images can be obtained by stacking the one transparency with the flipping other transparency. Unfortunately, the result decryption processes still have noise and the quality of decrypted secret image is not as same as original secret image. This article proposed the new algorithm to improve the quality of decryption secret image. In this process, the two secret images from decryption process were compared with the two original secret images. The different values of each pixel, which was counted from subtraction of decryption image and original secret images, will be inserted to the two key images. The experimental results of this improvement have a good similarity. The noise in decryption process can be eliminated so the two secret images reconstruction similar to the original secret images.

Keywords: *Flip improvement, Flip Visual Cryptography (FVC), key images*

INTRODUCTION

According to Naor and Shamir (1995), (2,2) Visual Cryptography (VC) is a technique for encrypting the image by dividing the image into two, three or more portions (commonly called a transparency). The portions will be sent to the recipient by the sender and the recipient will obtain information about the secret image, the receiver must have transparency in the appropriate amount and then stack them to get the information. The decryption process can be done by piling up transparency. If the amount of transparency that is stacked less than the amount specified, the recipient will get no information at all about the image being sent .There are two portions of the raw image whose pixel is altered by a block two or four subpixels which do not overlap as shown in Figure 1.

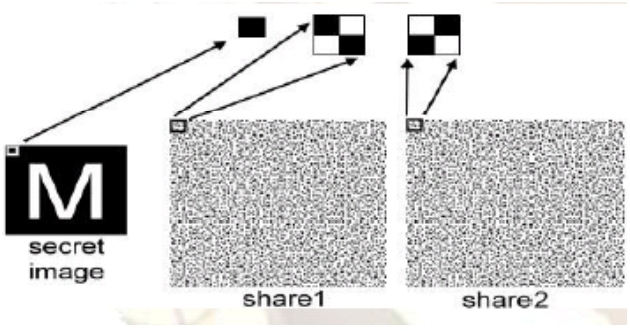

Figure 1 (2,2) Visual Cryptography Scheme

Naor and Shamir (1995) stated that one pixel white in the secret image is expanded, becoming two sub pixels. Because of it, expanded subpixels the size of image would be expanded two times, two subpixels contained in two identical blocks is the result of trimmed from a white pixel and two subpixels contained in two complementary blocks is resulted from the trimming of black pixel. It means that the white pixel in secret image would be expanded into identical two sub pixels in both image portions. For the black pixel in secret image would be expanded into complementary two sub pixels in the first share image and the second share image. The probability of the scheme is the same that fifty percent. This construction of (2,2) can be seen in Figure 2.

Each of the two pixel portions is obtained from converting each pixel to subpixels pair. The results are one black and one white subpixels superpositioned from a white pixel. On the other hand, subpixels which are black are resulted if the superpositioned pixel is black. A loss of intensity during the conversion occurs, however the reverted pixel is visibly available. The attackers can recognize no useful information about the individual portion since the shares in the layers occur as random noise. It is impossible to decode the message or information, thanks to availability limitation of the portion even with the existence of computer. The drawback of the above method is its unpredictability with no visual information. Although Extended Visual Cryptography have been suggested, it still suffers from the same drawbacks of unpredictability.

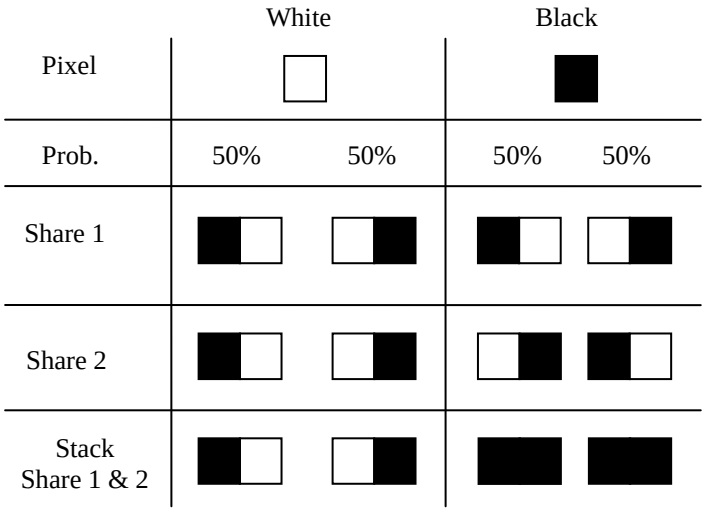

Figure 2 Construction of (2,2) Visual Cryptography Scheme

Chettri (2014) stated that the 2 out of 2 visual cryptography schemes based on pixel expansion m=2 in detail. The scheme explained is based on k out of k visual cryptography scheme. One single share cannot disclose the secret. To extract the secret message both the shares are needed to superimpose one on another. He provide (2,2) Visual Cryptography (VC) in detail for black and white image based on pixel expansion scheme.

Dhole and Janwe (2013) stated that Visual Cryptography is a new Cryptography technique which is used to secure image. In this article, applying algorithms in Visual Cryptography in images is discussed. Start with black and white image or binary images. In 2004, Binary Visual Cryptography scheme is applied to images with gray level, that gray level image will then be converted into images having tone half of the original. Binary image is obtained through transformation of gray level image using the halftone technique. Lastly, Visual Cryptography is used in color images. In color image, each pixel of 32 bit digital color image is divided into four parts, namely Alpha, Red, Green and Blue. Alpha part represents degree of transparency.

According to Verma and Khemchandani (2012), there are several plannings in converting the pixels of the secret image. In this planning, each pixel in the secret image is extracted into four sub pixels. Each of the two pixel portions is obtained from converting each pixel to subpixels pair. The results are one black and one white subpixels superpositioned from a white pixel. On the other hand, subpixels which are black are resulted if the superpositioned pixel is black. It means that the white pixel in secret image would be expanded into identical four sub pixels in the both share images. (Share image sometimes known as transparencies image). For the black pixel in secret image would be expanded into complementary four sub pixels in the first share image and the second share image. Figure 3 illustrates the variation this plan of converting one pixel into four sub pixels in a (2, 2) Visual Cryptography scheme. This plan encrypts the pixels in the raw image evenly. These portions vary from Vertical, Horizontal, to Diagonal portion as shown in the Figure 3.

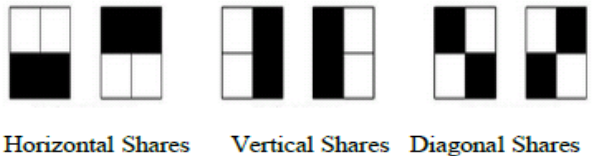

Figure 3 Pixel encoding in (2, 2) Visual Cryptography scheme

Example five bits an image is (0 0 1 0 1) where '0' represents white or transparent and '1' represents black or opaque , then the first share and the second share can be looked in Table 1. There still another example of alternative variation because the election randomly to choice horizontal, vertical or diagonal shares.

Table 1 Example Horizontal, Vertical and Diagonal share

Image secret	Share 1	Share 2
(0 0 1 0 1)	Horizontal shares	Horizontal shares
	(0 0 0 0 1 1 0 0 1 1)	(0 0 0 0 0 0 0 0 0 0)
	(1 1 1 1 0 0 1 1 0 0)	(1 1 1 1 1 1 1 1 1 1)
(0 0 1 0 1)	Horizontal shares	Horizontal shares
	(0 0 1 1 1 1 0 0 1 1)	(0 0 1 1 0 0 0 0 0 0)
	(1 1 0 0 0 0 1 1 0 0)	(1 1 0 0 1 1 1 1 1 1)
(0 0 1 0 1)	Vertical Shares	Vertical Shares
	(0 1 0 1 1 0 1 0 1 0)	(0 1 0 1 0 1 1 0 0 1)
	(0 1 0 1 1 0 1 0 1 0)	(0 1 0 1 0 1 1 0 0 1)
(0 0 1 0 1)	Vertical Shares	Vertical Shares
	(0 1 1 0 1 0 0 1 0 1)	(0 1 1 0 0 1 0 1 1 0)
	(0 1 1 0 1 0 0 1 0 1)	(0 1 1 0 0 1 0 1 1 0)
(0 0 1 0 1)	Diagonal Shares	Diagonal Shares
	(1 0 1 0 0 1 0 1 1 0)	(1 0 1 0 1 0 0 1 0 1)
	(0 1 0 1 1 0 1 0 0 1)	(0 1 0 1 0 1 1 0 1 0)
(0 0 1 0 1)	Diagonal Shares	Diagonal Shares
	(1 0 0 1 0 1 1 0 1 0)	(1 0 0 1 1 0 1 0 0 1)
	(0 1 1 0 1 0 0 1 0 1)	(0 1 1 0 0 1 0 1 1 0)

Encrypting an image by random grids was introduced by Shyu (2007). A binary secret image is encoded into two noise-like transparencies with the same size of the original secret image, and stacking of the two transparencies reveals the content of the secret. Comparing random grids with basis matrices, one of the major advantages is that the size of generated transparencies is unexpanded.

Lin *et al.* (2010) stated that the proposed Flip Visual Cryptography scheme encodes two secret images into two dual purpose transparencies. Stacking the two transparencies can reveal one secret image. Flipping one of the two transparencies and then stacking with the other transparency can reveal the second secret image. Lin *et al.* (2010) explained a method Flip Visual Cryptography does not create expansion pixels either on image transparency or on image decryption results. Four pixel values of secret image can be read in certain positions. The four pixel values are used as reference to obtain the base matrix. After determining the base matrix, four pixel values at random are chosen. These values are laid into matrix transparency with the same position on reading the pixel values of secret image. This is why flip visual cryptography has no expansion pixels. Unfortunately, the result decryption process still has noise. This article proposed improvement of image decryption. In this new algorithm process, the two secret images from decryption process are compared with the two original secret images. The different values of each pixel, which is counted from subtraction of decrypted image and original secret images, will be inserted to the two key images. The experimental results of this improvement have a good secret image. The noise in decryption process can be eliminated so the two secret images are similar with the original secret images.

The two secret images, that image secret 1 and image secret 2 is presented in Figure 4 and Figure 5. The result of encryption is transparency 1 (Figure 6) and transparency 2 (Figure 7). The flip transparency 1 can be described in Figure 8. When transparency 1 and transparency 2 are stacked, the decrypted secret image 1 (Figure 9) will be obtained. When transparency 1 and transparency 2 are flipped, obtain decrypted secret image 2 (Figure 10) will be obtained.

Figure 4 Secret Image 1

Figure 5 Secret Image 2

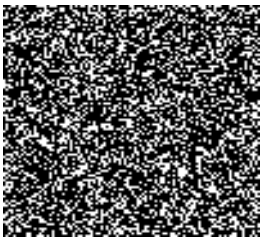

Figure 6 Transparency 1

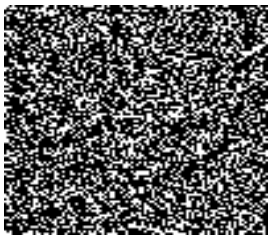

Figure 7 Transparency 2

Figure 8 Flip Transparency 1

Figure 9 Decrypt Secret Image 1

Figure 10 Decrypt Secret Image 2

In this Flip Visual Cryptography process, secret image results of decryption still have noise, therefore in this article, a key value on key image for secret image 1 and secret image 2 is added.

METHODS

Lin *et al.* (2010) stated that two *n x m* binary secret images, denoted by S_1 and S_2, are encoded to get two *n x m* transparencies T_1 and T_2, respectively. Without the loss of generality, the goal of the proposed Flip Visual Cryptography scheme is that the secret image S_1 can be decoded by stacking $T_1$and T_2 together; whereas the secret image S_2 can be decoded by flipping T_1 over and then stacking with T_2. Figure 11 illustrates the operation to flip a transparency over, the operation to have a secret image reconstruction, and the operation to process the key image.

Let $S_1 = \{s_1(i,j)|0 \le i \le n-1, 0 \le j \le m-1\}$ and $S_2 = \{s_2(i,j)|0 \le i \le n-1, 0 \le j \le m-1\}$ be the two given black-and-white secret images. Each pixel $s_1(i,j)$ and each pixel $s_2(i,j)$ are binary in value W (white) pixel or B (black) pixel). Let $T_1 = \{t_1(i,j)|0 \le i \le n-1, 0 \le j \le m-1\}$ and $T_2 = \{t_2(i,j)|0 \le i \le n-1, 0 \le j \le m-1\}$ be the two transparencies to be generated. In the design of transparencies T_1 and T_2, represent every ‘‘opaque” pixel of a transparency by 1, and represent every ‘‘transparent” pixel of a transparency by 0. (To distinguish between secret image and transparency image, the words ‘‘opaque and transparent”, rather than ‘‘Black and White”, are used when the image being talked about is a transparency, rather than an input secret image.). The table of creation matrix can be seen in Lin *et al.* (2010). In Definition 1, the stacking operation is symbolized by the symbol ‘‘+” which is in fact the OR operator. This coincides with the real world experience: in real world, if two transparencies are stacked, the places which can be seen through are the places where both transparencies can be seen as transparent (both are 0s). Definition 1. Stacking operation $+$. The stacking operation for transparencies is symbolized by ‘‘+”, where 0 + 0 = 0, 0 +1 = 1,1+0 = 1, and 1 + 1 = 1.

Figure 11 illustrates the effect of stacking two transparencies T_1 and T_2 and describes what will happen when people flip T_1 over and then stack it withT_2. The two pixel values $[s_1(i,j), s_1(i,m-1-j)]$ are called a symmetric pair, and so are$[s_2(i,j), s_2(i,m-1-j)]$. To design a flip visual cryptography (FVC) scheme, possible values of the quadruple $[s_1(i,j),\ s_1(i,m-1-j),\ s_2(i,j),\ s_2(i,m-1-j)\ ]$ for $0 \le i \le n-1$, and $0 \le j \le m/2-1$ should be considered simultaneouly. For each quadruple $[s_1(i,j),\ s_1(i,m-1-j),\ s_2(i,j),\ s_2(i,m-1-j)\ ]$ of secret pixels, the quadruple $[t_1(i,j),\ t_1(i,m-1-j),\ t_2(i,j),\ t_2(i,m-1-j)\ ]$ of transparency pixels must meet the following four requirements simultaneously: The quadruple $[t_1(i,j),\ t_1(i,m-1-j),\ t_2(i,j),\ t_2(i,m-1-j)\ ]$ of transparency pixels is obtained from 16 basis matrix stated in Lin *et al.* (2010).

Assume the quadruple $[s_1(i,j),\ s_1(i,m-1-j),\ s_2(i,j),\ s_2(i,m-1-j)\ ]$ have the values (0,1,0,0) and one of 16 basis matrix stated in Lin *et al.* (2010) for (0,1,0,0) can be looked in Table 2. This basis matrix have 6 column.One of column matrix randomization is chosen. After getting one column of basis matrix, then this value will be the quadruple $[t_1(i,j),\ t_1(i,m-1-j),\ t_2(i,j),\ t_2(i,m-1-j)\ ]$ of transparency pixels.Suppose with random process, column 3 can be owned, then the value of transparency is (1,0,1,1). From this value $t_1(i,j) = 1,\ t_1(i,m-1-j) = 0,\ t_2(i,j) = 1,\ t_2(i,m-1-j) = 1$.

Table 2 One of the Basis Matrix Stated in Lin *et al.* (2010)

$[s_1(i,j), s_1(i,m-1-j), s_2(i,j), s_2(i,m-1-j)]$		Col 1	Col 2	Col 3	Col 4	Col 5	Col6
(0,1,0,0)	$t_1(i,j)$	0	0	1	1	1	1
	$t_1(i,m-1-j)$	0	1	0	1	1	1
	$t_2(i,j)$	0	1	1	1	1	0
	$t_2(i,m-1-j)$	1	0	1	1	1	0

(1) $s_1'(i,j)$ is decoded by stacking $t_1(i,j)$ and $t_2(i,j)$;
equal to $s_1'(i,j) = t_1(i,j) + t_2(i,j)$
(2) $s_1'(i,m-1-j)$ is decoded by stacking $t_1(i,m-1-j)$ and $t_2(i,m-1-j)$;
equal to $s_1'(i,m-1-j) = t_1(i,m-1-j) + t_2(i,m-1-j)$
(3) $s_2'(i,j)$ is decoded by stacking $t_1(i,m-1-j)$ and $t_2(i,j)$;
equal to $s_2'(i,j) = t_1(i,m-1-j) + t_2(i,j)$
(4) $s_2'(i,m-1-j)$ is decoded by stacking $t_1(i,j)$ and$t_2(i,m-1-j)$;
equal to $s_2'(i,m-1-j) = t_1(i,j) + t_2(i,m-1-j)$

From $[t_1(i,j), t_1(i,m-1-j), t_2(i,j), t_2(i,m-1-j)] = (1,0,1,1)$, the stacking result $[s_1'(i,j), s_1'(i,m-1-j), s_2'(i,j), s_2'(i,m-1-j)]$ can be counted.

Example:
$s_1'(i,j) = t_1(i,j) + t_2(i,j) = 1 + 1 = 1.$
$s_1'(i,m-1-j) = t_1(i,m-1-j) + t_2(i,m-1-j) = 0 + 1 = 1.$
$s_2'(i,j) = t_1(i,m-1-j) + t_2(i,j) = 0 + 1 = 1.$
$s_2'(i,m-1-j) = t_1(i,j) + t_2(i,m-1-j) = 1 + 1 = 1.$

Here, $[s_1'(i,j), s_1'(i,m-1-j), s_2'(i,j), s_2'(i,m-1-j)] = (1,1,1,1)$ are the stacking results to show the quadruple$[s_1(i,j), s_1(i,m-1-j), s_2(i,j), s_2(i,m-1-j)] = (1,0,1,1)$. Dealing visual decoding, the stacking results $[s_1(i,j), s_1(i,m-1-j), s_2(i,j), s_2(i,m-1-j)]$ do not need to be completely identical to the original secret values $[s_1(i,j), s_1(i,m-1-j), s_2(i,j), s_2(i,m-1-j)]$ ..

Therefore, a key has been added to key image to improve the stacking result.It is done by inserting a key into a key image. The two n x m color image is used to bring keys. Each pixel $s_1(i,j)$minus each pixel $s_1'(i,j)$is key value $k_1'(i,j)$, and each pixel $s_2(i,j)$minus each pixel $s_2'(i,j)$ is key value $k_2'(i,j)$. Key value is 1 or 0 , 1 means pixel values secret image stacking result $s_1(i,j)$ needs modification, and 0 means pixel values secret image stacking result $s_1'(i,j)$ no need modification. Modification pixel is done by changing the pixel value reversely when pixel value is 0 then change itto 1 or when pixel value is 1 then change it to 0. This process is done to secret image stacking result $s_2'(i,j)$ too.

Another process in the system is a key insertion process. A key insertion process is done by adding key value $k(i,j)$ on every last significant bit (LSB) in the key image $K(i,j)$.

$$k_1'(i,j) = |s_1(i,j) - s_1'(i,j)| = |1-1| = 0$$
$$k_1'(i,m-1-j) = |s_1(i,m-1-j) - s_1'(i,m-1-j)| = |0-1| = 1$$

$$k_2'(i,j) = |s_2(i,j) - s_2'(i,j)| = |1-1| = 0$$
$$k_2'(i,m-1-j) = |s_2(i,m-1-j) - s_2'(i,m-1-j)| = |1-1| = 0$$

From this counting, key value$[k_1'(i,j),\ k_1'(i,m-1-j),\ k_2'(i,j),\ k_2'(i,m-1-j)] = (0,\ 1,\ 0,\ 0)$ is obtained. Assume that key image is denoted by K_1 and K_2. K_1 and K_2 is two $n \times m$ colour images. Each pixel $k_1\ (i,j)$ and each pixel $k_2\ (i,j)$ are 24 bit in value before insertion key. The key value is added to last significant bit at 24 bit key value with this equation:

$$k_1\ (i,j) = k_1\ (i,j) + k_1'(i,j)$$
$$k_2\ (i,j) = k_2\ (i,j) + k_2'(i,j)$$

Where $k_1'(i,j)$ and $k_2'(i,j)$are key value(i, j) , k_1 (i, j) and k_1 (i, j) are pixel value key image respectively.

To reveal the keys back, it takes a new image that has not inserted a key and a new image that has been inserted the key. The difference in the pixel values of the second image is the key inserted .In decoded process the key value is extracted from key image. The secret image description is repaired by guidance of key value. Bit operation changes is done when the key value is 1 and bit operation changes is not done when the key value is 0.

What it means is that $[k_1'(i,j),\ k_1'(i,m-1-j),\ k_2'(i,j),\ k_2'(i,m-1-j)] = (0,\ 1,\ 0,\ 0)$? Look at this key value: (1) $k_1'(i,j) = 0$. Changing not occur and $s_1(i,j) = s_1'(i,j)$. This mean if $s_1'(i,j) = 1$ then $s_1(i,j) = 1$. (2) $k_1'(i,m-1-j) = 1$. Changing occur and $s_1(i,m-1-j) \neq s_1'(i,m-1-j)$. This mean if $s_1'(i,m-1-j) = 1$ then $s_1(i,m-1-j) = 0$. (3) $k_2'(i,j) = 0$. Changing not occur and $s_2(i,j) = s_2'(i,j)$. This mean if $s_2'(i,j) = 1$then $s_2(i,j) = 1$. (4) $k_2'(i,m-1-j) = 0$. Changing not occur and $s_2(i,m-1-j) = s_2'(i,m-1-j)$. This mean if $s_2'(i,m-1-j) = 1$then $s_2(i,m-1-j) = 1$.

The insertion of key value can be described in Figure 12. An image is formed by some pixels. Each pixel consists of 24 bit binary value, which is 0 or 1. A key value is added with a twenty fourth binary value. Assume the original binary value is 1 and the key value is 1. Addition of two values will be produce 10, then the twenty fourth binary value is 0. If the original binary value is 1 and the key value is 0. Addition of two values will be produce1. Assume the original binary value is 0 and the key value is 1. Addition of two values will be produce 1. If the original binary value is 0 and the key value is 0. Addition of two values will be produce Addition of two values will be produce 0.

The tracking insertion key process starts from upper left corner image and goes to upper right corner image. First track line located at the uppermost of the image. The second line located one line next to the uppermost line and so on until the process reached the lowest line.

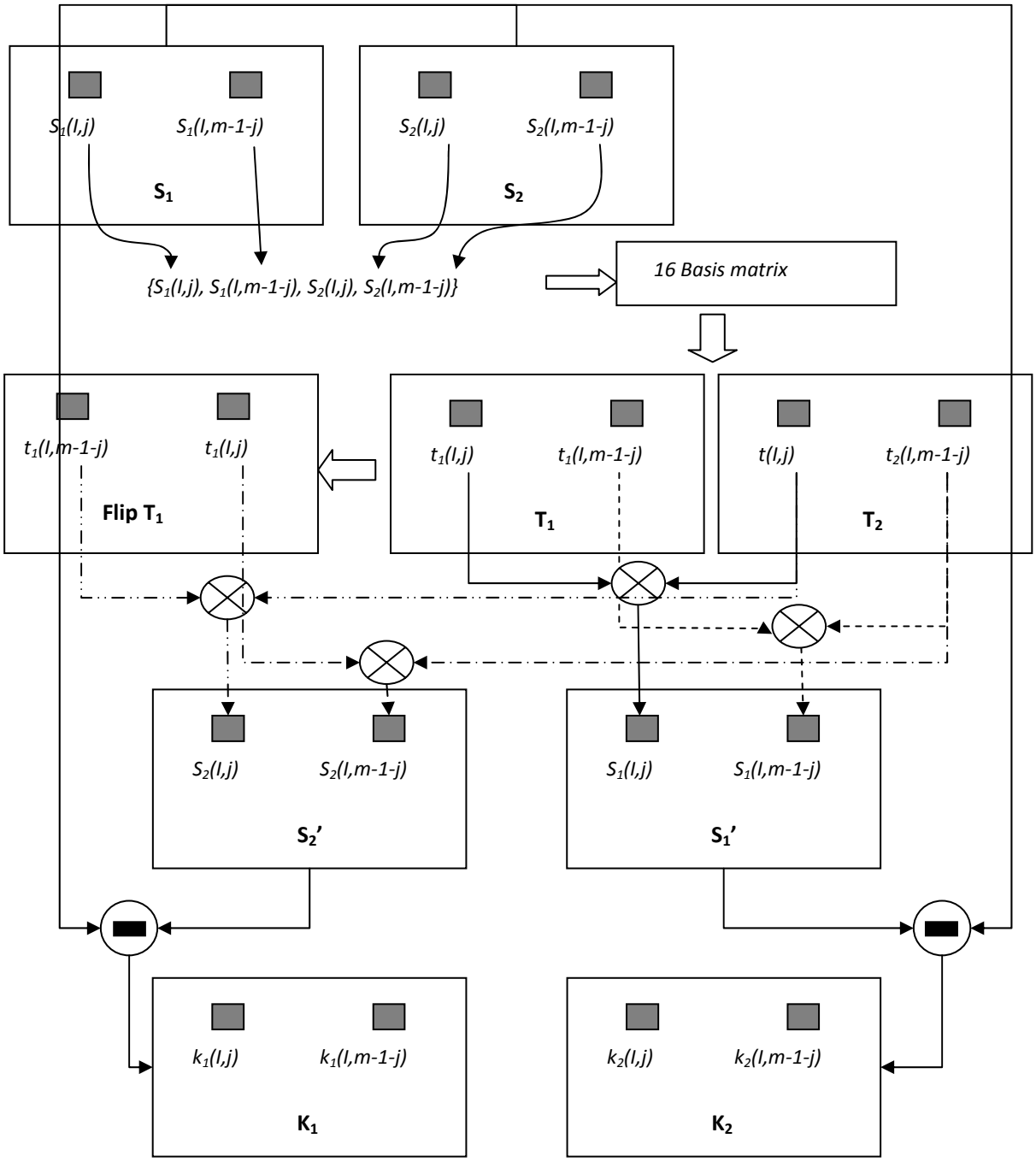

Figure 11 Improvement Flip Visual Cryptography

Original pixel image

1	2	3	4	5	6	7	8	.....	20	21	22	23	24

Insertion key value to pixel image

1	2	3	4	5	6	7	8	.....	20	21	22	23	key

Figure 12 The Insertion of Key Value

RESULTS AND DISCUSSIONS

Every testing process uses two black and white secret images and two color key images. All images have the same size n x m pixels. The n represent the width of image and m is the height of image. The two transparency images have the same size that is n x m pixels.

The data has been tested by Sari (2015). There are two secret images used in Figure 13 and Figure 14. After Flip Visual Cryptography process two transparency images are obtained (Figure 15 and Figure 16). Figure 17 and Figure 18 is a key image original 1 and a key image original 2 respectively. After the keys for this image are counted, the keys are inserted to key image original 1 and a key image original 2. The key image insertion 1 and a key image insertion 2 can be described in Figure 19 and Figure 20. Figure 21 and Figure 22 is decrypt secret image 1 and decrypt secret image 2 without improvement respectively. Figure 23 and Figure 24 is improvement decrypt secret image 1 and improvement decrypt secret image 2 with improvement respectively.

Figure 13 Secret Image 1

Figure 14 Secret Image 2

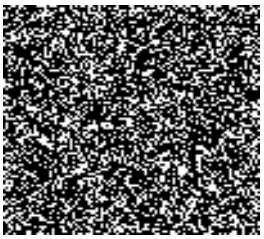

Figure 15 Transparency 1

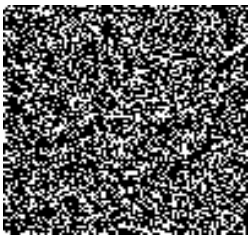

Figure 16 Transparency 2

Figure 17 Key Image original 1

Figure 18 Key Image original 2

Figure 19 Key Image After Insertion 1

Figure 20 Key Image After Insertion 2

Figure 21 Decrypt Secret Image 1

Figure 22 Decrypt Secret Image 2

Figure 23 Improvement Decrypt Secret Image 1

Figure 24 Improvement Decrypt Secret Image 2

Another variation images are used in this experiment. Twenty secret images in ten experiments are used. Each experiment used two secret images. For key image, the authors used two key images. All images that are secret images and key images, have the same size n x m pixels. All experiment results a good similarity with MSE zero that is a decrypted secret image similar to original secret image.

CONCLUSIONS

The improvement of flip visual cryptography is successfully realized by using two key color images to save all key values. Two secret images with no expansion pixel are encrypted. Encryption process resulted two transparency images without pixel expansion. The decryption of two transparency images with two key images result two secret images with better performance.

REFERENCES

Chettri, L. (2014). Visual Cryptography scheme based on pixel expansion for black & white image. *International Journal of Computer Science and Information Techniques (IJCSIT), 5*(3), 4190-4193.

Dhole, A. B., & Janwe N. J. (2013). An implementation of algorithms in Visual Cryptography. *International Journal of Scientific and Research Publications, 3*(3), 1-5.

Lin, S-J., Chen, S-K., & Lin, J-C., (2010). Flip visual cryptography (FVC) with perfect security, conditionally-optimal contrast, and no expansion. *Journal of Visual Communication & Image Representation, 21,* 900-916. doi: 10.1016/j.jvcir.2010.08.006

Naor, M., & Shamir, A. (1995). Visual cryptography. *Proc. Advances in Cryptography (EUROCRYPT'94), 950*, 1–12.

Sari, P. K. (2015). *Visual cryptography for sharing secret images using flip methods (2,2)*. Retrieved from http://repository.maranatha.edu/18590/

Shyu, S. J. (2007). Image encryption by random grids. *Journal of Pattern Recognition*, *40*(3), 1014-1031. doi: 10.1016/j.patcog.2006.02.025

Verma, J., & Khemchandani, D. V. (2012). A Visual Cryptographic Technique to Secure Image Shares. *International journal of Engineering Research and Application (IJERA), 2*(1), 1121-1125.