THE VISUAL SECRET SHARING SCHEME BASED ON THE RGB COLOR SYSTEM

Eric Christiandi Sulaiman[1) and Mariskha Tri Adithia[2)
[1, 2)Department of Informatics, Parahyangan Catholic University
Jl. Ciumbuleuit No. 94, Bandung
e-mail: erichristiandi@gmail.com[1), mariskha@unpar.ac.id[2)

ABSTRAK

Skema visual secret sharing (vss) adalah suatu metode untuk menjaga kerahasiaan suatu gambar rahasia dengan membagikannya kepada beberapa partisipan. Vss (k,n) membagi gambar rahasia menjadi n buah bagian di mana masing-masing bagian ini disebut shadow; untuk mendapatkan gambar rahasianya kembali, k buah shadows ditumpukkan. Beberapa metode vss sudah dibangun untuk gambar berwarna. Namun, metode-metode yang sudah ada hanya cocok digunakan untuk gambar dengan banyak warna yang terbatas. Jika gambar memuat banyak warna, hasil penumpukan shadows akan menjadi tidak jelas. Selain itu, semakin banyak warna, semakin besar pula ukuran dari shadows tersebut. Kami membangun metode baru yang mengimplementasikan vss dengan berdasarkan sistem warna rgb. Dengan menggunakan metode kami, permasalahan terkait ketidakjelasan gambar hasil tumpukan shadows dapat diatasi.

Kata Kunci: *gambar berwarna, shadow, sistem warna RGB, visual secret sharing*

ABSTRACT

The visual secret sharing (VSS) scheme is a method to maintain the confidentiality of a secret image by sharing it to some number participants. A (k, n) VSS divides the secret images into n parts, that are called shadows ; to recover the secret back, k shadows should be stacked. Some methods have been developed to implement VSS for color images. However, the methods are only suitable for images with limited number of colors. When more colors are used, the resulted stacked shadow image becomes unclear. Besides that, the size of the shadows becomes bigger as more colors are used. We develop a new method implementing the VSS using the RGB color system. Using our method, the problem related to the unclear stacked shadow image can be overcome.

Keywords: *color image, RGB color system, shadow, visual secret sharing*

I. INTRODUCTION

A secret sharing scheme is a way to secure information by dividing it into several pieces. In a (k,n) secret sharing scheme, n pieces of data is created in such way that the information can only be retrieved when k pieces of them are combined [5].

The Visual Secret Sharing (VSS) scheme is a method to encode a secret image containing texts, shapes, or even photos [1][2][3][4][7]. It was first introduced by Naor and Shamir in 1994 [4]. A VSS scheme creates random images called *shadows* from the secret image which then be printed to transparent papers. Each shadow reveals no information about the secret image until some shadows are combined by stacking them.

A threshold (k,n) VSS scheme creates n shadows from the secret image. To recover the secret image back, k of them should be combined [4].

The decoding process for VSS does not need any computational method. To get the original image from the shadows, simply stack k of the shadows. This simple method makes the VSS good for securing information especially in situation without computer and electricity.

The VSS scheme can also be used for gray-scale and color secret images [8][9]. However, the VSS still have problems especially when dealing with color images. As more colors are used in the VSS, the stacked image becomes more unclear and the size of the shadows becomes bigger. With these problems in mind, we develop a new VSS scheme that uses the RGB color system which makes the stacked image clearer and shadows have more reasonable size.

The rest of this paper is organized as follows. In Section 2, we explain some related work in VSS schemes. Section 3, we describe our proposed scheme which is called the RGBVSS scheme. We also provide an example to give a more clearer description. In Section 4, we show the performance of our proposed scheme by using some experiments. In this section, we also compare our scheme and the scheme proposed in [9]. Section 5 concludes the paper.

II. VSS Scheme

The VSS scheme was first introduced by Naor and Shamir in 1994 [4]. The input secret images in the scheme are black and white images. Each pixel in the secret image is expanded so that each pixel in the shadow consists of several subpixels.

The (*k*,*n*) VSS scheme requires two base boolean matrices of size (*n* × *m*), namely S_{white} and S_{black}, with *m* is the pixel expansion value. Each row of these two matrices represents a pixel in the shadow. Each element represents a subpixel; the value 1 and 0 represent white and black subpixel, respectively. The generation of these two base matrices is specified in [4].

From the two base matrices, two sets are formed: C_{white} and C_{black}. C_{white} and C_{black} contain all column-permutation matrices of the mattrix S_{white} and S_{black}, respectively. To share a white pixel, choose a random element from C_{white}, and to share the black one, choose a random element from C_{black}.

The contrast, notated by α, is the ratio between the difference of the number of black and white subpixel and the pixel expansion value.

Since each pixel in the Naor and Shamir VSS scheme is expanded, the size of the shadow becomes greater than it is in the secret image. When the expansion pixel value is not a square number, the aspect ratio of the shadow changes and the image length and width become unbalanced.

Ching-Nung Yang proposed a new method to overcome the problems [6] in which each pixel is not expanded. This method is also called the probabilistic VSS scheme. The S_{white} and S_{black} matrices are also used in this method. Instead of forming the sets C_{white} and C_{black}, sets of Cp_{white} and Cp_{black} containing all columns of S_{white} and S_{black}, respecively, are formed. The same way, as in the Naor and Shamir VSS scheme, the sets Cp_{white} and Cp_{black} are used to share the white and black pixel.

The probabilistic method in [6], is then used to share grayscale images [8]. In this grayscale VSS (GVSS) scheme, the term grayscale level of images is introduced. Images with a high grayscale level are smoother than those with a lower one. Note that, black and white images are grayscale images with a grayscale level of 2.

In [9], the scheme to share color images is developed. In this scheme, the input secret images are color images that use the palette system. Different from the Naor and Shamir VSS scheme, the color VSS (CVSS) scheme may use many colors other than white and black.

To form the shadow, the (*k*,*n*) CVSS scheme with *c* colors, the color matrix C_i, with $i = 0,1,\ldots,c-1$, is formed based on the modified base matrices S_{white} and S_{black}. The value 0's in the matrices are changed to values of used colors, while the value 1's are changed to a symbol "•". Equation 1 shows the matrix for color *i* containing the concatenation of the matrix S_{white} for color *i* and matrices S_{black} for other colors.

$$C_i = \left(S_{white}^{0\to i,1\to\bullet}\right) \circ \left(S_{black}^{0\to j_0,1\to\bullet}\right) \circ \cdots \circ \left(S_{black}^{0\to j_c,1\to\bullet}\right) \tag{1}$$

In the (1), the matrices are concatenated using the symbol ∘. To change the values in the modified matrices S_{white} and S_{black}, the following notation $S^{(0\to a,1\to\bullet)}$, which means the 0 and 1 elements are substituted with a value *a* and • (which is a black color), respectively. $j_0,\ldots,j_c \in (0,1,\ldots,c-1)-i$ are other colors excluding color *i*. The size of the resulted matrix C_i is (*n*×*m*'), with *m*'=*c*·*m*. The contrast is calculated as $\alpha^{color} = \dfrac{\alpha}{c}$, with α is the contrast obtained from the base matrices in the Naor and Shamir VSS scheme.

To share a pixel, the set CC_i is generated. CC_i, with *i* = 0,…,*gl*–1, contains *c* matrices; the matrices are resulted by permuting *s* columns of the matrix C_i, *s* is the pixel expansion value, with $1 \le s \le m'$. The value of *s* determines the size of the shadows. To share a pixel of color *i*, chooses a random element in CC_i.

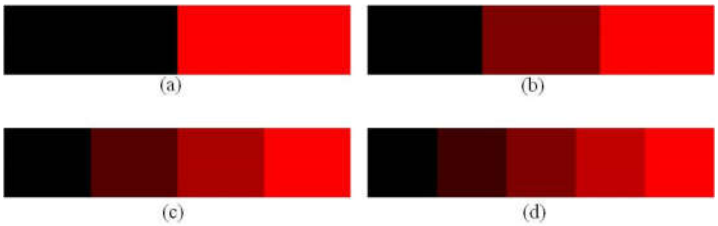

Figure 1 Red color with (a) two, (b) three, (c) four, and (d) five color intensity levels

III. RGBVSS Scheme

In the CVSS scheme, as the number of colors used in the scheme increases, the size of the matrix C_i becomes really big and the contrast becomes really small. For example, for the CVSS scheme with 256 colors and the size of S_{white} and S_{black} are 2×2, the size of the matrix C_i becomes 2×512. This causes a low quality image since the color occurrence frequency is very low.

We proposed a new VSS scheme by using the RGB (Red, Green, Blue) color system, which is widely used in the computer graphic area. By setting up the intensity of those three colors, many other colors can be produced. When a pixel has a high intensity of all those three colors, the pixel becomes close to white. On the other hand, when it has a low intensity of all those three colors, the pixel becomes close to black.

In the RGB Visual Secret Sharing (RGBVSS) scheme proposed, the secret image is an image with the RGB color system. Different from the CVSS scheme which uses palette colors, the RGVSS scheme uses the base colors RGB where each color has *cl* levels of color intensity. Figure 1 shows the color intensity level and the resulted colors. The number of colors that can be produced using this method is $(cl)^3$.

The shadows of the (k,n) threshold scheme RGBVSS with the color intensity level of $cl \geq 2$ is formed by first generating the color matrix $R_iG_jB_k$ with $i, j, k = 0,\ldots,cl-1$. The matrix $R_iG_jB_k$ is a concatenation of the base matrices S_{white} and S_{black} in the binary VSS by Naor and Shamir, that have been modified as given in Equation 2.

$$\begin{aligned} R_iG_jB_k = {} & \left(S_{white}^{0\to r,1\to\bullet}\right)^i \circ \left(S_{black}^{0\to r,1\to\bullet}\right)^{(cl-1-i)} \circ \\ & \left(S_{white}^{0\to g,1\to\bullet}\right)^i \circ \left(S_{black}^{0\to g,1\to\bullet}\right)^{(cl-1-i)} \circ \\ & \left(S_{white}^{0\to b,1\to\bullet}\right)^i \circ \left(S_{black}^{0\to b,1\to\bullet}\right)^{(cl-1-i)} \end{aligned} \tag{2}$$

The matrix $R_iG_jB_k$ is similar to the matrix C_i in the CVSS scheme, only the colors are notated by *r*, *g*, and *b*, representing red, green, and blue, respectively.

The notation ∘ means the matrix concatenation operation. Then, the notation *superscript* S^i is the concatenation of the matrix *S* and itself for *i* times, and *superscript* $S^{(0\to a,1\to\bullet)}$ shows that all 0 and 1 elements in the matrix *S* are substituted with a color *a* and black, respectively. The resulted matrix is of size $(n\times m^{rgb})$ with the value of $m^{rgb}=3\cdot(cl-1)\cdot m$. The contrast between each color intensity level, α^{rgb}, is $\frac{\alpha}{3\cdot(cl-1)}$.

Note that α^{rgb} is the contrast between the matrices $R_iG_jB_k$ and with $a+b+c = i+j+k+1$ and $a, b, c, i, j, k = 0,\ldots, cl-1$. Which means, the difference of the color intensity level between the matrices is 1.

The next step is to form a set of matrices of size $(n\times s)$, $CR_iG_jB_k$, with *s* is the number of pixel expansion. The matrix $CR_iG_jB_k$ contains all permutation of *s* columns of the matrix $R_iG_jB_k$, as given in Equation 3. The value of *s* determines the size of the shadows. To distribute red, green, and blue pixels with the intensity level of *r*, *g*, and *b*, respectively, a matrix in $CR_rG_gB_b$ specified in Equation 3 is randomly picked.

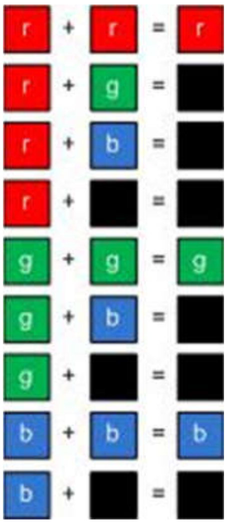

Figure 2 The stacking results

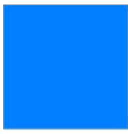

Figure 3 The secret image

$$CR_iG_jB_k = \{\text{The permutation of } s \text{ columns of the matrix } R_iG_jB_k\} \quad (3)$$

Equation (2) is developed based on equations in GVSS and CVSS methods. This is because the main idea of the RGBVSS scheme is to make the base color RGB has a color intensity level. Thus, the method in the GVSS scheme is used to implement the color intensity level, while the method in the CVSS scheme is used to form the base color matrix.

By using this method, the size of the shadows is smaller, yet containing more colors compared to those in the CVSS scheme. For example, for a scheme with 8 color intensity levels and S_{white} and S_{black} of size 2×2, the size of the matrix $R_iG_jB_k$ is 2×42. With this relatively small size of matrix, the number of colors resulted is 512.

The same as other VSS methods, to reconstruct the secret, the shadows should be stacked. In the CVSS scheme, the stacking of different colors produces an undefined color. Different from the CVSS scheme, in the RGBVSS scheme, stacking two different colors yields a black color. However, in this method, there may not be stacking of two different colors, other than with a black color. See Figure 2.

The following is an example of a (2,2) RGBVSS scheme with a color intensity level of cl = 3. The secret image used is an image of 1×1 pixel, with colors red, r = 0, green, g = 1, and blue b = 2, as given in Figure 2. The first step is generating the matrices S_{white} and S_{black}, as given in Equation 4.

$$S_{white} = \begin{bmatrix} 1 & 0 \\ 1 & 0 \end{bmatrix} \qquad S_{black} = \begin{bmatrix} 1 & 1 \\ 0 & 0 \end{bmatrix} \quad (4)$$

Secondly, based on the obtained S_{white} and S_{black}, the matrix $R_iG_jB_k$ with i, j, k= 0, 1, 2 is formed. The matrices $R_iG_jB_k$ of size (n×m^{rgb}) and a pixel expansion of m^{rgb}=12 is given in Equation 5. Based on the contrast $\alpha=\frac{1}{2}$ from the Naor and Shamir's base matrices, the contrast between each color intensity level is computed as $\alpha^{rgb} = \frac{\alpha}{3\cdot 2} = \frac{1}{12}$.

$$\begin{aligned} R_0G_1B_2 = & \left(\begin{bmatrix} \bullet & r \\ \bullet & r \end{bmatrix}\right)^0 \circ \left(\begin{bmatrix} \bullet & r \\ r & \bullet \end{bmatrix}\right)^2 \circ \\ & \left(\begin{bmatrix} \bullet & g \\ \bullet & g \end{bmatrix}\right)^1 \circ \left(\begin{bmatrix} \bullet & g \\ g & \bullet \end{bmatrix}\right)^1 \circ \\ & \left(\begin{bmatrix} \bullet & b \\ \bullet & b \end{bmatrix}\right)^2 \circ \left(\begin{bmatrix} \bullet & b \\ b & \bullet \end{bmatrix}\right)^1 \\ = & \begin{bmatrix} \bullet & r & \bullet & r & \bullet & g & \bullet & g & \bullet & b & \bullet & b \\ r & \bullet & r & \bullet & \bullet & g & g & \bullet & \bullet & b & \bullet & b \end{bmatrix} \end{aligned} \tag{5}$$

Next, the value of *s*, with $1 \le s \le m^{rgb}$ is chosen. With $s = 4$, the set of matrices $CR_iG_jB_k$ is given in Equation 6.

$$CR_0G_1B_2 = \left\{ \begin{bmatrix} \bullet & r & \bullet & r \\ r & \bullet & r & \bullet \end{bmatrix}, \begin{bmatrix} \bullet & r & g & b \\ r & \bullet & g & b \end{bmatrix}, \ldots \right\} \tag{6}$$

To form the shadow, one matrix at random from $CR_0G_1B_2$ is chosen. Suppose that the matrix *M* in Equation 7 is chosen.

$$M = \begin{bmatrix} r & g & b & b \\ \bullet & g & b & b \end{bmatrix} \tag{7}$$

Based on the matrix *M*, the resulted shadows are given in Figure 3. The result of stacking two shadows is shown in Figure 4.

IV. Experimental Results

We apply our proposed approach to distribute the image of Lenna, using a (2,2) scheme. In this case, the color intensity levels for the scheme are 2, 3, and 4, with no pixel expansion. The different color intensity levels are used so that we can observe how the approach works with different number of colors. In all cases, the original contrast $\alpha=\frac{1}{2}$. The image to be shared, and the stacking results are shown in Figure 5.

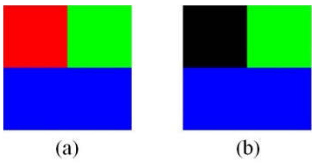

Figure 4 The resulted shadows (a) Shadow 1, (b) Shadow 2

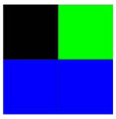

Figure 5 The stacking of two shadows

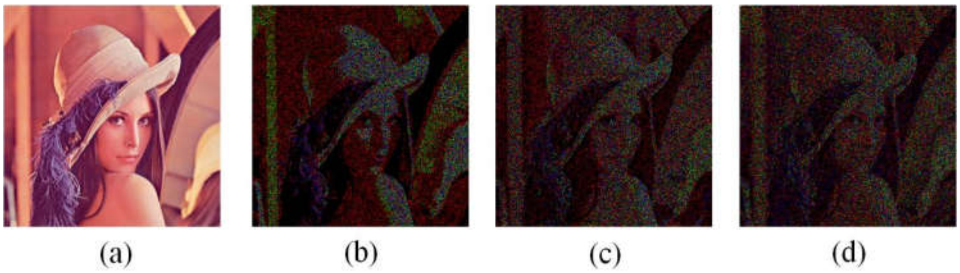

Figure 6 (a) The image of Lenna and the stacking of shadows with (b) two, (c) three, and (d) four color intensity levels

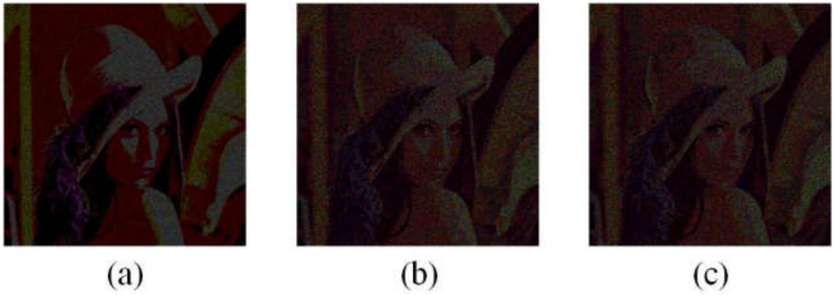

Figure 7 The stacking of shadows obtained from the (2,2) RGBVSS scheme with a pixel expansion of 4, using (a) 2 levels of color intensity , (b) 3 levels of color intensity, and (c) 4 levels of color intensity

Visually, the image with lowest color intensity level (Figure 6b) has a higher contrast compared to the higher ones (see Figure 6c and d). Therefore, the Figure 6b is visible than the others. Mathematically, the contrast of the stacking results with 2, 3, and 4 color intensity levels are $\frac{1}{6}$, $\frac{1}{12}$, and $\frac{1}{18}$, respectively.

As the color intensity level increases, the number of colors used also increases. Thus, the image with highest color intensity level involves the highest number of colors. With a color of intensity of 2, 3, and 4, the numbers of colors used are 8, 27, and 64 colors. Since more colors are used, the image quality becomes smoother. This is shown in Figure 5d.

In the previous cases, the pixels are not expanded. In our next experiment, the pixel expansion value used is 4. The stacking results are given in Figure 7. As given by Figure 7, we can see that all the stacking results are a lot smoother, compared to the results in the previous case (see Figure 6). This is because in this case, each pixel does not contain only one color, but may contain at most 4 different colors. Therefore, the color changing from one pixel to another becomes smoother.

We also compare the results of the RGBVSS and the CVSS schemes. The (2,2) scheme of both schemes are used to distribute two images; the second image contains more bright colors than the first one. In both cases, the contrast $\alpha = \frac{1}{2}$. The pixel expansion value, *s*, used is 1. In the RGBVSS scheme, we use the minimum value of the color intensity level, which is 2. It means that 8 colors can be resulted. To make both schemes comparable, 8 colors are also used in the CVSS scheme, namely black, red, green, blue, cyan, magenta, yellow, and white. Note that, the size of the color matrix $R_iG_jB_k$ in this case is 2×6, which is a lot smaller than the size of C_i, which equals to 2×16.

The first comparison result is shown in Figure 8. In this comparison, we distribute the image of Lenna again as the first image to be distributed. Figure 8a and b show the stacking results when we use the RGBVSS and the CVSS scheme, respectively.

Figure 8 shows that the stacking result of the RGBVSS scheme is more visible than those of the CVSS scheme. This is because, the result of the RGBVSS scheme has a higher contrast value, which is $\alpha^{rgb} = \frac{\alpha}{3 \cdot 1} = \frac{1}{6}$, compared to those of the CVSS scheme, which equals to $\frac{\alpha}{8} = \frac{1}{16}$.

For the second comparison, we use an image containing more bright colors. The comparison results are shown in igure 9.

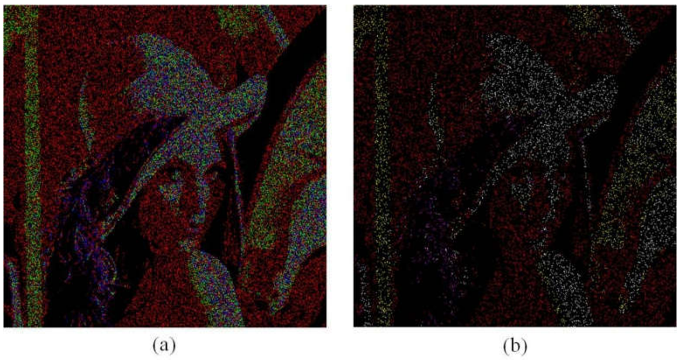

Figure 8 (a) The stacking result of RGBVSS, and (c) CVSS schemes of the image of Lena

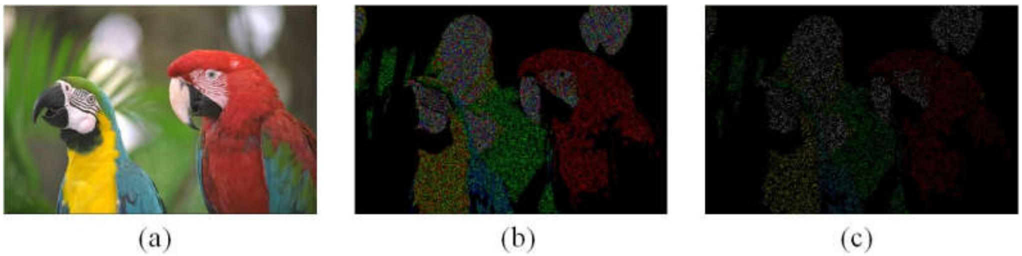

Figure 9 (a) The second image, and the stacking results of (b) RGBVSS and (c) CVSS schemes

The same as the first comparison results, this second one also shows that the stacking result of the RGBVSS scheme is more visible. This is also because of the higher contrast obtained by the RGBVSS scheme.

V. Conclusions

We have developed a new visual secret sharing scheme which is called the RGBVSS. Different from the CVSS scheme which uses the palette color system, our approach employs the RGB color system. Our scheme is able to represent many colors with a small size of the base matrix, compared to those used in the CVSS scheme. As a result, the shadows produced by our scheme have more reasonable sizes. The RGBVSS scheme also produces stacking images with a higher contrast value compared to those produced by the CVSS scheme so that the resulted stacking images are clearer.

References

[1] G. Ateniese, C. Blundo, A. De Santis, and D.R. Stinson, “Visual Cryptography for General Access Structures,” *ECCC, Electronic Colloquium on Computational Complexity (TR96-012)* via WWW using http://www.eccc.uni-trier.de/eccc/, 1996

[2] S. Droste, “New Results on Visual Cryptography,” *Advances in Cryptology-CRYPT’96 Lecture Notes in Computer Science*, vol. 1109, Springer-Verlag, pp. 401-415, 1996

[3] T. Katoh and H. Imai, 1996, “Some Visual Secret Sharing Schemes and Their Share Size,” *Proceedings of International Conferences on Cryptology and Information Security,* pp. 41-47, 1996

[4] M. Naor and A. Shamir, “Visual Cryptography,” *Advances in Cryptology-EUROCRYPT’94 Lecture Notes in Computer Science*, vol. 950, Springer-Verlag, pp. 1-12, 1995

[5] A. Shamir, “How to Share a Secret,” *Communications of the ACM*, vol. 22, pp.612-613, 1979

[6] N. Yang, “New Visual Secret Sharing Schemes Using Probabilistic Method,” *Pattern Recognition Letters*, vol. 25, no. 4, pp. 481-494, 2004

[7] E.R. Verheul and H.C.A. van Tilborg, “Constructions and Properties of k out of n Visual Secret Sharing Schemes,” *Designs, Codes and Cryptography*, vol. 11, No. 2, Kluwer Academic Publishers, pp. 179-196, 1997

[8] D. Wang, F. Yi, and X. Li, X. “Probabilistic Visual Secret Sharing Schemes for Gray-Scale Images and Color Images,” *Information Sciences*, vol. 181, pp. 2189 – 2208, 2011

[9] C.N. Yang and C.S. Laih, “New Colored Visual Secret Sharing Schemes,” *Designs, Codes and Cryptography*, vol. 20, Kluwer Academic Publishers, pp. 325-335, 2000