Implementation of Colored Visual Cryptography for Generating Digital and Physical Shares

Ahmad Zaky | 13512076[1]
Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jl. Ganeca 10 Bandung 40132, Indonesia
[1]ahmadzaky003@gmail.com

***Abstract*—Visual Cryptography is a secret message sharing method for visual messages, such as digital images. The result will be several images, which will reveal the secret message when stacked or combined with a proper way. However, for colored images, the stacking procedure will produce different result if different color models were used. This paper will analyze the colored visual cryptography when it is applied to different color models. The additive and subtractive color models will be used as comparation, as both color models are used to represent colors in digital and physical media.**

Keywords—additive and subtractive color models, halftone image, visual cryptography

I. Introduction

The concept of Visual Cryptography (VC) was first introduced by Moni Naor and Adi Shamir in 1995 [1]. It is a new (at that time) techniques of message sharing, using a digital image as the secret information. In the general *k*-out-of-*n* visual cryptography (usually expressed as (*k, n*)-VC) the image is divided into *n* other images, which will be called as *shares* and will be distributed to *n* participants. In order to recover the secret message, at least *k* participants should combine their shares. Any combination of less than *k* will not reveal anything about the original message. Combining can be interpreted as stacking the image shares if those shares are printed onto transparencies, XOR-ing the pixel information, etc.

The original VC was intended for black-and-white secret and share images. In the next few years after the paper was published, a lot of researches was conducted in this field. Many better methods was introduced, such as extending black-and-white to grayscale even colored images. The term extended VC was also introduced, where the shares are not random noise, but meaningful images themselves.

Colored VC is tricky, because combining colors is different when the media is different. If the shares are digital images and are meant to be combined digitally (stacking them into one by using some image processing software/tools), then RGB color model should be used. In the other hand, physical shares which are printed onto transparancies should use CMY or CMYK color model. Further explanation about color models is provided in the second chapter.

This paper will not provide new technique of VC. Instead, we will examine an implementation of one of the methods on both media, digitally and physically. One of the first VC method for color images was introduced by Young-Chang Hou in 2002, using (2, 2) and (3, 3) schemes [2]. The method was one of the simplest methods yet still produce nice result, although it generates random shares. CMY color model was used there. We will analyze the result when using RGB color model instead.

II. Fundamentals of Visual Cryptography

A. Visual Cryptography

The more general term of sharing a message is *secret sharing* or simply *message sharing*. This term was first introduced by Adi Shamir in 1979 [3]. Generally, a (*k, n*) message sharing encrypts a secret message into *n* shares to be distributed to *n* participants. Each share wil not reveal anything about the original message. The number *k* means that it is necessary to have at least *k* of the *n* shares to recover the secret message. Any combination consisting of at least *k* shares will do, but on the contrary, any combination consisting less than *k* shares will not reveal anything.

Visual Cryptography is secret sharing for which the secret is an image. The recovery can be done by stacking share images, XOR-ing pixel information, or anything else, which should be known by all of the participants. Recovering means that the resulted image can be recognised visually by human eyes. A more formal definition about this can be found in [4].

B. Standard VC Method

The standard VC method refers to the original method proposed by Shamir and Naor. The method was for black-and-white images. The procedure for (2, 2)-VC is given as follows. Each pixel in the secret image will be encrypted as 2×2 pixels in both shares, thus the width and the height of the shares will be twice as large as the secret image. The encoding table is given in figure 1. One may choose any of the six possible encoding for each pixel randomly, and independently to other pixels. This will produce random noise-like shares.

The idea for general (*k, n*)-VC is similar. Instead of 2×2 pixels, each pixel in the secret image will be interpreted as larger matrix. This will not be covered in this paper, because the method that will be implemented is only using (2 2) scheme. In order to work with color images, choosing proper color models and halftoning images are necessary.

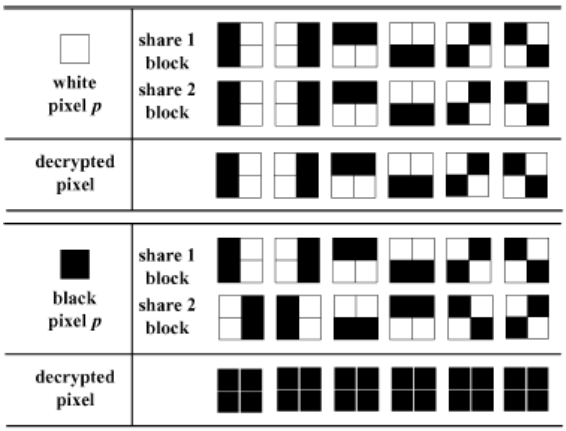

Figure 1. The encoding table for standard (2, 2)-VC. A pixel is encoded into four subpixels.

C. Color Models

A color model defines the composition of a color. Each defined color is composed by certain amount of *primitive colors*. The primitive colors are the colors which cannot be derived from other colors. Different color model has different primitive colors and color mixing rules.

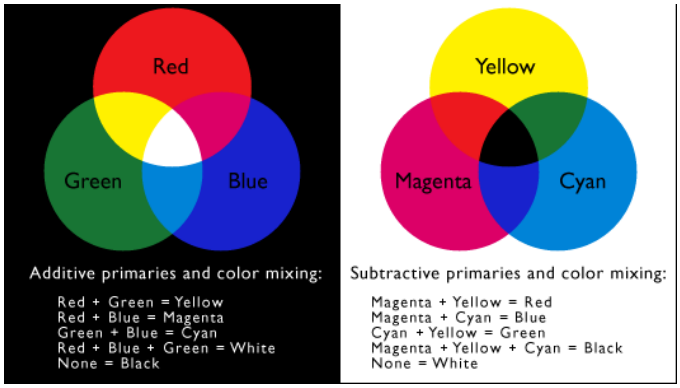

Figure 2. Two different color models, additive and subtractive.

There are two widely used color models: *additive* and *subtractive* color models. In the additive color model, the primary colors are red, green, and blue. Hence, it is also called RGB color model. This color model is the one composing visible light. Every visible colors can be obtained by mixing certain intensity of red, green, and blue lights. More color added, more brightness will result. When all primitive colors are mixed, white color will result. That is the reason behind the name. Every electronic screen use this color model for defining colors.

The subtractive color model has cyan, magenta, and yellow as its primitive colors. It is the reverse of the additive color mode. More color added, it eventually become darker. All colors combined will result black. Color printer is the example for it. In most application, a key element is added to the model, thus producing CMYK model. The key element is actually black; it was widely used in printer because black ink is cheaper than colored ones.

In the implementation, the additive color model will be used when the share images are combined digitally. By giving the images the right amount of transparency, the secret image will be recovered by stacking at least *k* shares. On the other hand, the subtractive color model will be used when dealing with physical shares, where each of them are printed on the transparent papers.

D. Halftone Image

Halftone image is a quality reduction of an image, but still producing visually equivalent image. For a grayscale 8-bits-per-pixel image, the halftone image is 1-bit black-and-white image. Although it can only represent black and white colors, it actually can simulate different level of gray. For example, in the part with dark gray, the density of black is high around there.

Halftoning image is important because some image processing techniques is easier when processed as binary image. In some cases, it is even impossible to process non-binary image. A dot matrix printer is a good example for this. The printer can only put a black ink to certain pixel or not, and cannot print a certain level of grayness. Before printing an image or document, the printer first halftone it into binary image.

The same halftone technology can also be applied to color images. In a 24-bit RGB image, there are three color channels, each consisted of 8 bits. Halftoning RGB image is as simple as halftoning each channel separately, and then combine them into 3-bit RGB image. The same holds for CMY or CMYK images.

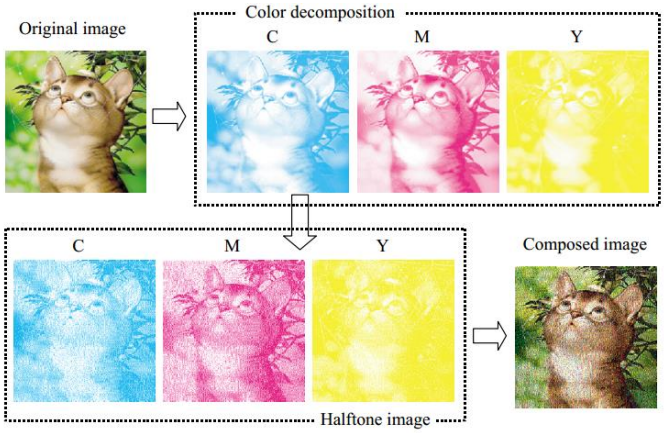

Figure 3. The process of generating halftone image with a 24-bit CMY color image. First, the image is decomposed according to its color channels. Then, each image in each color channel is treated as grayscale image and is then halftoned. Then, the combination of three halftone images from all channels produce the desired image.

There are many techniques to halftone an image. The quality of the generated images vary, depending on the algorithm used. Some of the techniques are screening/masking, error diffusion, noise-shaping, and direct binary search [5]. In this paper, we will use error diffusion technique. The method is simple and fast, without sacrificing the quality of the image.

E. Error Diffusion to Halftone an Image

In error diffusion, the error at each pixel (difference between the chosen bit and the actual level of grayness) is filtered and fed into a set of future inputs. First, it computes the sum of input value as follows.

$$d(m,n) = f(m,n) - \sum h(k,l) \times e(m-k, n-l) \quad (1)$$

where $d(m,n)$ is the sum of input value and the diffused error, $f(m,n)$ is the pixel value at position (m,n). $e(m,n)$ is the difference between $d(m,n)$ and $f(m,n)$. The value of $h(k,l)$ highly determine the output. A widely used filter is the error weight which originally proposed by Floyd and Steinberg

$$h(k,l) = \frac{1}{16} \times \begin{bmatrix} & x & 7 \\ 3 & 5 & 1 \end{bmatrix} \quad (2)$$

where x is the current processed pixel.

The output value, $g(m,n)$ is defined as follows, where $t(m,n)$ is the threshold value, which can be position-dependant.

$$g(m,n) = \begin{cases} 1, & \text{if } d(m,n) \geq t(m,n) \\ 0, & \text{otherwise.} \end{cases} \quad (3)$$

III. The Implemented Method

The implemented method will be the method number 3 in [2]. We will describe the algorithm briefly.

First, the image is decomposed into several images according to the color model used. Then, each image is encrypted using the standard (2, 2)-VC method for grayscale image, where each pixel becomes 2×2 pixels in the output. In the process, the image is halftoned into binary image. Then, each pixel is encoded according to figure Figure 1. The encoding table for standard (2, 2)-VC. A pixel is encoded into four subpixels. The result is the combination of the three images from all color channels.

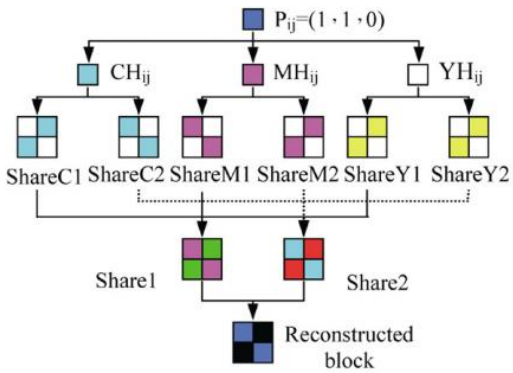

Figure 4. The process of pixel encryption and decryption.

Digital images are usually represented in 24-bit RGB values for each pixel. When converting to CMY values, the method below is widely used.

$$\begin{aligned} C &= 1 - \frac{R}{255} \\ M &= 1 - \frac{G}{255} \\ Y &= 1 - \frac{B}{255} \end{aligned} \quad (4)$$

where R, G, and B are the pixel values from 0 to 255, and C, M, Y are the desired CMY values ranging from 0 to 1. However, this method may produce incorrect result. A more proper way is to use ICC profiles, which comply to the standards promulgated by the International Color Consortium (ICC). Several parties have provided such ICC profiles. The implementation here will use ICC profiles provided by Adobe™.

IV. Experimental Result

A. The Implementation Details

We implement the algorithm using Java. Java has its own digital image processing library. The image is first read as a binary file. Then we store the pixel values information in arrays of integers. Now we can manipulate the image by manipulating those arrays. After applying algorithm explained in chapter III, then the shares result (still in array form) are converted back to images in desired format. We also simulate the process of combining those shares by applying OR binary operation on each color channel.

B. The Comparison between Digital and Physical Shares

The exactly same digital image will be encrypted using both additive and subtractive color models, or RGB and CMY color models respectively. The detailed process, together with the images which are generated in each process are provided in figure Figure 6. The process of generating shares using RGB and CMY color model.. Both color models generate random noise-like shares, and almost undistinguishable. When combined, the following images are created. Although the quaility is not that good, it still produces images which are identifiable with human eyes.

(a) (b)

Figure 5. The result of stacking shares generated with (a) RGB and (b) CMY color model

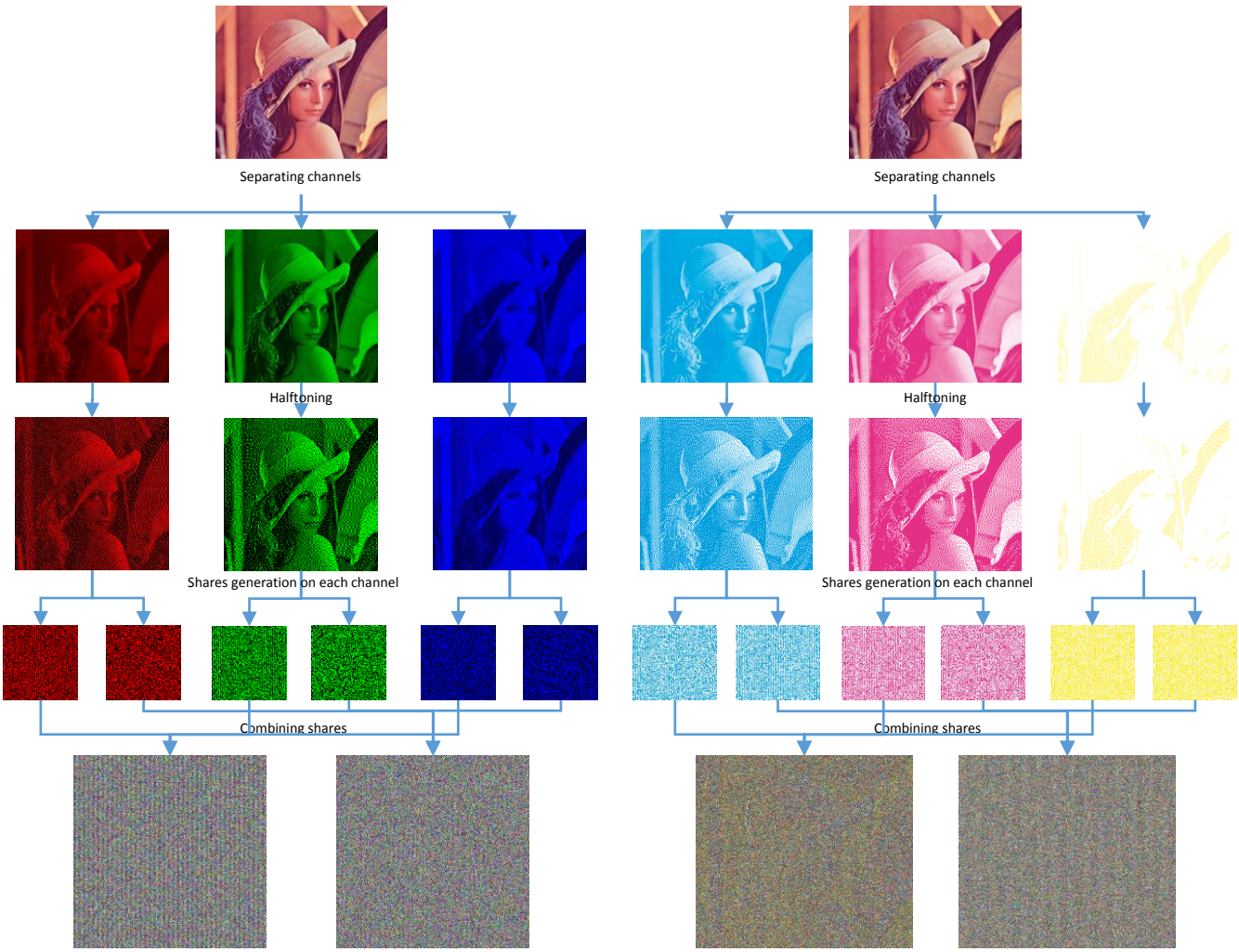

Figure 6. The process of generating shares using RGB and CMY color model.

V. Analysis

We will analyze the implementation of that method by several factors, which are security and the quality of the image itself. Finally, we will show that there are better methods out there, even for extended colored VC.

A. Security

From the definition of the VC itself, the method can be considered secure if any combination of less than *k* shares will not reveal anything about the secret image. All the four shares in figure 6 (two for each color model) are random noise-like pattern, which do not mean anything to us visually. Hence, the requirement is satisfied.

However, in the other hand, the noise-like images will lead to suspiction. This can be avoided by using extended VC, in which all the shares are meaningful images.

B. Image Quality

The images in figure 5 are the decrypted images from both color model. Those images are obtained by stacking the generated shares. Both of them look alike, in terms of its similarity with the original picture. Both have fair-enough quality; not so good, but can still be recognised by human eyes. Additionally, the RGB result is brighter than the CMY result. This is explained very well using the color model used. The RGB result uses additive color model as explained in chapter II, hence adding more color results in increasing brightness. Conversely, CMY result uses subtractive color model, and adding more color will darken the image.

Moreover, the image quality can be calculated using peak signal to noise ratio. The RGB result has PSNR value equals to -37.173, while the CMY result has PSNR equals to -35.586. Those values are negative, indicating that there is huge difference between the decrypted image and the original image. Thus, this method is not suggested when the image quality is very important.

C. Better Implementation and Methods

There are so many other methods which are proved better than this. The author chose this method because this is the first ever VC for colored images. This algorithm is also the fastest

and the simplest method compared to the other. The consequence is that the image quality must suffer.

Among other methods, the best method existed according to the author's opinion is the one proposed by Kang, InKoo et. al. from Korea. The method is explained very well in [5]. The method also uses error diffusion to halftone images, but it is improved extremely by using visual information pixel (VIP) synchronization, also using error diffusion inside there.

The method works not only for meaningful shares, but also works for general (*k*, *n*)-VC schemes. The image quality is also very high, both for the shares and the decrypted image. The PSNR values for the shares ranging from 10 to 11, but the PSNR values for decrypted image are not provided in the paper.

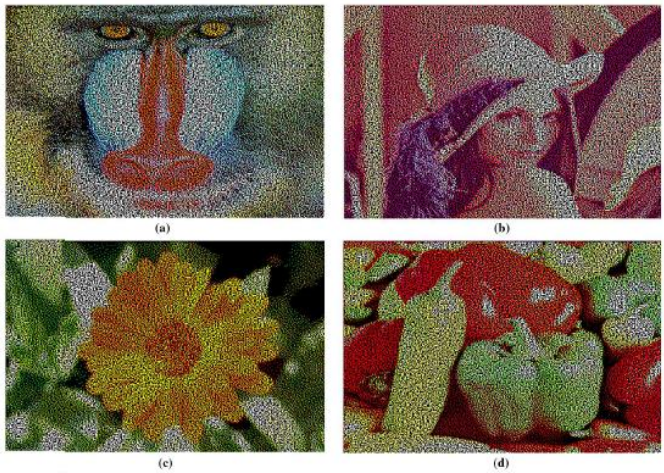

Figure 7. The generated shares using (3, 4)-VC scheme.

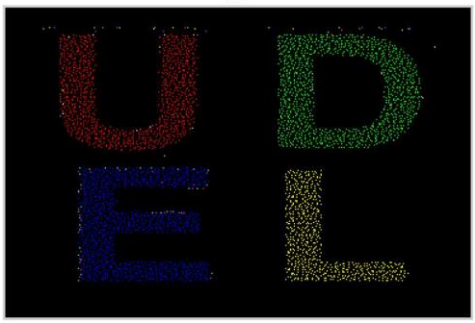

Figure 8. The decrypted image by stacking shares (a)-(d) in Figure 7.

VI. Conclusion

Visual Cryptography is very useful in message sharing using digital image secrets. There are many methods out there, and we have successfully implemented and analyzed Young-Chang Hou's method for color images. This method can be applied to different color models, according to which media is used. The digital media should use additive/RGB color model, while the physical media should use subtractive/CMY color model. Both produce similar result, and additive result is brighter than subtractive one as expected. Although the result is fine visually, it is actually a relatively bad in terms of PSNR values.

Acknowledgment

The author thanks to Mr. Rinaldi Munir for teaching Cryptography course and consequently introducing visual cryptography and other great concepts to the author for the first time. The author also thanks to his friends and fellow students of Informatics/Computer Science ITB for their help and assistance all this time.

References

[1] M. Naor and A. Shamir, "Visual Cryptography". EUROCRYPT, *Lecture Notes Computer Science*, vol. 950, pp. 1-12, 1995.

[2] Hou, Young-Chang. "Visual Cryptography for Color Images". Pattern Recognition, Vol. 36, pp.1619-1629, 2003.

[3] Shamir, Adi. "How to share a secret". Communications of the ACM 22 (11): 612–613, 1979.

[4] Kang, InKoo, Arce, Gonzalo R., and Lee, Heung-Kyu. "Color Extended Visual Cryptography Using Error Diffusion". IEEE Transactions on Image Processing, Vol. 20, No. 1, January 2011.

[5] Evans, Brian L.. "Error Diffusion Halftoning Methods for High-Quality Printed and Displayed Images". Department of Electrical and Computer Engineering, The University of Texas at Austin. November 2002.

Statement

Hereby I stated that this paper is my own writing, not a copy nor a translation of the work of the others, and not a plagiarism.

Bandung, May 11th 2015

Ahmad Zaky - 13512076