Volume: 03, Issue: 05, Pages:1379-1384 (2012)

A Review of Color Visual Cryptographic Schemes

Prof. Richa K. Makhijani
Department of Computer Science & Engg., S.S.G.B.C.O.E.T., Bhusawal, MS, India.
Email: richa_makhijani@yahoo.co.in
Prof. Lavina D. Panjwani
Department of Computer Science & Engg., S.S.G.B.C.O.E.T., Bhusawal, MS, India.
Email: lavina.no1@gmail.com

----------ABSTRACT----------
Visual Cryptography is a special encryption technique to hide information in images in such a way that it can be decrypted by the human vision if the correct key image is used. It is a cryptographic technique which allows visual information (pictures, text, etc.) to be encrypted in such a way that the decryption can be performed by the human visual system, without the aid of computers. The technique was proposed by Naor and Shamir in 1994. This paper reviews two methods for visual cryptography of color images based on past studies in black-and-white visual cryptography, the halftone technology, and the color decomposition method.

Keywords - **Visual cryptography, Color visual cryptography, Halftone technology, Color decomposition, Meaningful shares, Images.**

Date of Submission: December 10, 2011 Revised: February 05, 2012 Date of Acceptance: February 15, 2012

1. INTRODUCTION

With the advent of transmitting multimedia data over the internet, it has become important that the security of data be given much importance. As a result of the astonishingly rapid advancement of various kinds of Internet technologies, more information is transmitted to all parts of the world from everywhere through the Net. Some of the objects transmitted online may be important secret images, and in such cases the senders have to take information security issues into consideration before they can trustingly enjoy the speed and convenience that nothing in this world but the Internet can offer. With the ongoing era of electronic commerce, there is an urgent need to solve the problem of ensuring information safety in today's increasingly open network environment. The encrypting technologies of traditional cryptography are usually used to protect information security. With such technologies, the data become disordered after being encrypted and can then be recovered by a correct key. Without the correct key, the encrypted source content can hardly be detected even though unauthorized persons steal the data.

Visual cryptography, an emerging cryptography technology, was proposed in 1994 by Naor and Shamir [1], which used the characteristics of human vision to decrypt encrypted images. It needed neither cryptography knowledge nor complex computation. For security concerns, it also ensured that hackers could not perceive any clues about a secret image from individual cover images. They proposed a cryptography scheme called the "(k, n)-threshold visual secret sharing scheme," and the idea they raised has ever since been referred to as "visual cryptography (VC)" [1]. The major feature of their scheme was that the secret image can be decrypted simply by the human visual system without having to resort to any complex computation. Naor and Shamir's scheme could hide the secret image in n distinct images called shares. The secret image could then be revealed by simply stacking together as many as k of the shares. Each of the shares looked like a collection of random pixels and of course appeared meaningless by itself. Naturally, any single share, before being stacked up with the others, reveals nothing about the secret image. This way, the security level of the secret image when transmitted via the Internet was effectively lifted up. Since Noar and Shamir published their VC scheme, many related methods have been developed and proposed. However, in addition to the meaningless shares they produce, those schemes take only binary images as secret images, which mean the contents of the secret images in most cases can be nothing but text or simple black-and-white designs. It is only natural now that researchers are more interested in developing new cryptography schemes that can also process secret color images that are more complex. .

A visual cryptography scheme (VCS for short) for a set P of n participants is a method to encode a secret image into n shadow images in the form of transparencies, called shares, where each participant in P receives one share. Certain subsets of participants, called qualified sets, can "visually" recover the secret image, but other subsets of participants, called forbidden sets, have no information on the secret image. A "visual" recovery for a set X _ P consists of superimposing the shares (transparencies) given to the participants in X. The participants in a qualified set X will be able to see the secret image without any

knowledge of cryptography and without performing any cryptographic computation. Forbidden sets of participants will have no information on the secret image. This was the cryptographic paradigm introduced by Naor and Shamir. They analyzed the case of (k, n)-threshold VCS, in which a black and white (b&w for short) secret image is visible if and only if any k transparencies are stacked together. It should be noted that the color white is actually the transparent color.

Hou proposed a VC scheme for color images [2]. These schemes are termed as color visual cryptographic schemes (CVS). Based on the halftone technique and color decomposition, it decomposed the secret image into three colors *C*, *M* and *Y*. By manipulating the three color values, the color pixels in the secret image could be represented. Many other techniques have been developed by researchers for CVS.

The introduction of the paper should explain the nature of the problem, previous work, purpose, and the contribution of the paper. The contents of each section may be provided to understand easily about the paper.

2. LITERATURE SURVEY

2.1 Gray –Level Visual cryptography

2.1.1 Basic visual cryptographic model

The white pixels of black-and-white images are treated as transparent. This is because the output of visual cryptography is transparencies. Typically, the black-and-white visual cryptography decomposes every pixel in a secret image into a 2×2 block in the two transparencies according to the rules in Fig. 1. When a pixel is white, the method chooses one of the two combinations for white pixels in Fig. 1 to form the content of the block in the two transparencies; when a pixel is black, it chooses one of the other two combinations.

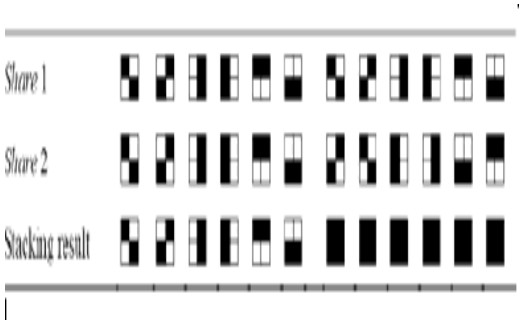


Figure 1: Sharing and stacking scheme of black and white pixels.

As for information security, there are six possible patterns from which every block in a transparency can randomly choose, so the secret image cannot be identified from a single transparency. Take Fig. 2 for example. The secret image (a) is decomposed into two visual cryptography transparencies (b) and (c). When stacking the two transparencies, the reconstructed image (d) is obtained. Even though the contrast of the resulting image is degraded by 50%, human eyes can still identify the content of the secret image.

2.2 The Halftone Technology

Different media use different ways to represent the color level of images, based on their physical characteristics.

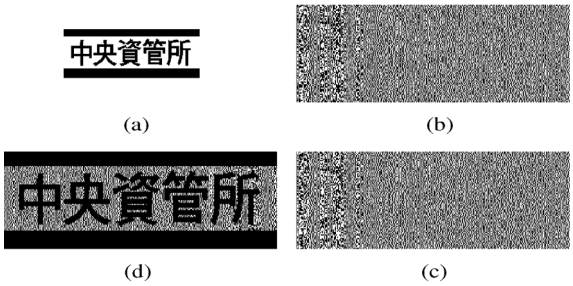


Figure 2: Visual cryptography (a) Secret image; (b) Share image 1; (c) Share image 2; (d) Recovering image.

The computer screen uses the electric current to control the lightness of the pixels. The diversity of the lightness generates different color levels. The general printer, such as dot matrix printers, laser printers, and jet printers, can only control a single pixel to be printed (black pixel) or not to be printed (white pixel), instead of displaying the gray level or the color tone of an image directly. As such, the way to represent the gray level of images is to use the density of printed dots; for example, the printed dots in the bright part of an image are sparse, and those in the dark part are dense (Fig. 3). The method that uses the density of the net dots to simulate the gray level is called “Halftone” and transforms an image with gray level into a binary image before processing.

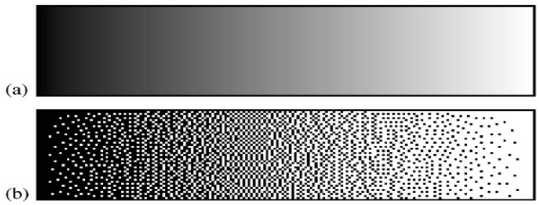


Figure 3: (a) Continuous tone; (b) Halftone

Figure 4 (a): Continuous tone; and (b): Halftone.

Take the gray-level image in Fig. 4a for example. Every pixel of the transformed halftone image (Fig. 4b) has only

two possible color levels (black or white). Because human eyes cannot identify too tiny printed dots and, when viewing a dot, tend to cover its nearby dots, we can simulate different gray levels through the density of printed dots, even though the transformed image actually has only two colors—black and white.

3. THEORY

3.1. Visual Cryptography for Color Images

3.1.1 Basic principle of color.

The additive and subtractive models (Fig. 5(a) and (b)) are commonly used to describe the constitutions of colors. In the additive system, the primaries are red, green and blue (RGB), with desired colors being obtained by mixing different RGB components. By controlling the intensity of red (green or blue) component, we can modulate the amount of red (green or blue) in the compound light. The mixed colored-lights, the more is the brightness of the light. When mixing all red, green and blue components with equal intensity, white color will result. The computer monitor is a good example of the additive mode. In the subtractive model, color is represented by applying the combinations of colored-lights reflected from the surface of an object (because most objects do not radiate by themselves). Take an apple under the natural light for example. The surface of the apple absorbs green and blue part of the natural light and reflects the red light to human eyes, so it becomes a red apple. By mixing cyan (C) with magenta (M) and yellow (Y).pigments, it can produce a wide range of colors. The more the pigment we add, the lower is the intensity of the light, and thus the darker is the light. This is why it is called the subtractive model. C, M and Y are the three primitive colors of pigment, which cannot be composed from other colors. The color printer is a typical application of the subtractive model. In the additive model, any color mixed with white color is still white color.

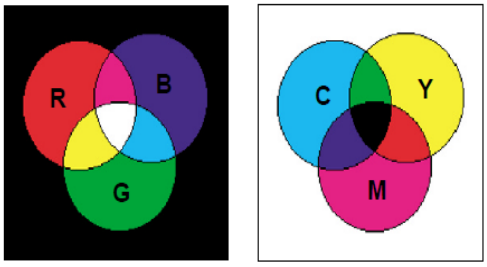


Figure 5 (a): Additive model ; (b): Subtractive model.

It thus seems more reasonable to use red, green, blue, and black colors to fill the blocks. On the other hand, in the subtractive model, the combination of any two of R, G, and B colors results in black color. R, G or B combined with white color will not change and can only result in the same color. Consequently, it is more appropriate to fill the blocks with cyan, magenta, yellow and white colors. In computer systems, Application Interfaces (APIs) provided by most image processing software as well as the Windows operating system are based on the RGB model. This is mainly because they use monitors as the primary output media. Monitors themselves generate color images by sending out RGB light into human's retina. In true color systems, R, G, B are each represented by 8 bits, and therefore each single color of R, G, B can represent 0–255 variations of scale, resulting in 16.77 million possible colors. When using (R, G, B) to describe a color pixel, (0; 0; 0) represents full black and (255; 255; 255) represents full white. In visual cryptography, the decryption tool is the use of sharing images; that is, the final outputs are transparencies. Because the subtractive model is more suitable for printing colors on transparencies, the CMY model is used to represent colors. Because (R, G, B) and (C, M, Y) are complementary colors, in the true color model, (R, G, B) and (C, M, Y) possess the following relationships: $C = 255-R$, $M = 255-G$, $Y = 255-B$, Thus, in the (C, M, Y) representation, (0; 0; 0) represents full white and (255; 255; 255) represents full black.

3.2 Methodologies and Implementation

3.2.1 Method 1

One of the methods proposed by Hou [2], used the procedure illustrated in Fig. 6 to transform a color secret image into three C, M, and Y halftone images. Then, every pixel of the halftone images was expanded into a 2×2 block to which a color is assigned according to the model presented in Fig. 1. Every block of the sharing images therefore included two transparent (white) pixels and two color pixels so that the entropy reached its maximum to conceal the content of the secret image. Furthermore, a half black-and-white mask was designed to shade unexpected colors on the stacked sharing images so that only the expected colors showed up. Take Fig. 7 for example [2]. If pixel Pij of the composed image was (0; 0; 0), the distribution of the color pixels in the three sharing images was assigned as the first row in Fig. 7. After stacked by the mask image, all the color pixels on the three sharing images were shaded by black pixels and only the white pixels could reveal, thus showing a white-like colour. If pixel Pij was (1; 1; 0), only the C and M components were revealed, with the Y component being covered by the black mask. The distribution of the color pixels in the three sharing images was as the fifth row in Fig. 7, thus showing a blue-liked (cyan plus magenta) color. If pixel Pij was (1; 1; 1), the C, M, and Y parts could all be revealed, thus showing a black color. The distribution of the color pixels in the three sharing images was as the eighth row in Fig. 7. The eight combinations of the three primary colors of the composed image under this method are illustrated in Fig. 7.

Moreover, it could also analyze the color distribution of the stacked image in terms of color quantity. For example, the first row in Fig. 7 shows that black color occupies half of the 2×2 block in the composed image. Since black can be seen as the composition of C, M, and Y, which means that C, M, and Y occupy half of the whole block

respectively, the densities of C, M, and Y components within a 2×2 block are all 12 . If the distribution of color pixels in the composed image is was the fifth row in Fig. 7, only C and M were revealed with Y being covered by the black mask. Since black can be seen as the composition of C, M, and Y, C and M could appear in all four blocks of a 2×2 block in the composed image, but yellow only appeared in two. So the Color intensity of C, M and Y could be denoted as (1, 1, 1/2).If the distribution of color pixels in the composed image was as the eighth row in Fig. 7, four blocks are all black and the color intensity (C, M, Y) can be denoted as (1; 1; 1). Thus, with this method, they could use (1/2,1/2,1/2) (1,1/2,1/2) (1/2,1,1/2) (1/2,1/2,1) (1,1,1/2) (1/2,1,1) (1,1/2,1) (1,1,1) to denote the combinations of the primary colors in a composed image. As a result, white pixels in a stacked image were no longer pure white (0; 0; 0), but were half black-and-white (1/2, 1/2,1/2) instead.

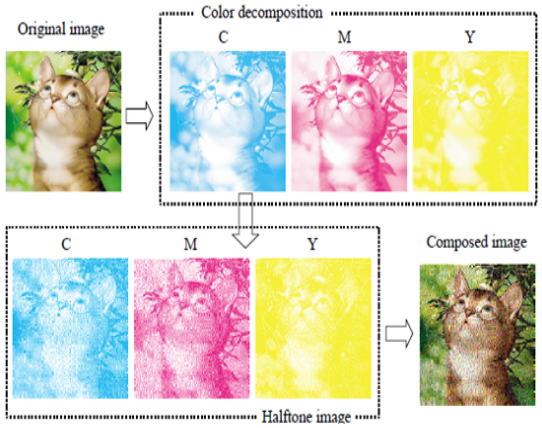


Figure 6: Color Image Printing

Mask	Revealed color (C,M,Y)	Share1(C)	Share2(M)	Share3(Y)	Stacked image	Revealed color quantity (C,M,Y)
	(0, 0, 0)					(1/2, 1/2, 1/2)
	(1, 0, 0)					(1, 1/2, 1/2)
	(0, 1, 0)					(1/2, 1, 1/2)
	(0, 0, 1)					(1/2, 1/2, 1)
	(1, 1, 0)					(1, 1, 1/2)
	(0, 1, 1)					(1/2, 1, 1)
	(1, 0, 1)					(1, 1/2, 1)
	(1, 1, 1)					(1, 1, 1)

Figure 7: Scheme of Color Cryptography.

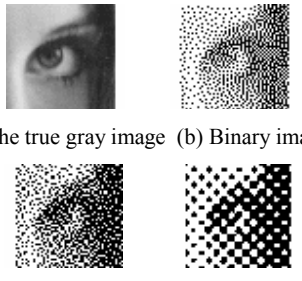
Accordingly, the colors in a stacked image were no longer distributed between (0; 0; 0) and (1; 1; 1), but were distributed between (1/2,1/2,1/2)) and (1; 1; 1). This result was similar to the contrast loss occurred in black-and-white visual cryptography. In this method, there were thus 6 (=C (4; 2)) possible combinations of the distribution of black pixels in the mask, each one corresponding to a different distribution of Shares 1, 2, and 3. For implementation, it could randomly select the mask and the corresponding distribution of shares to raise the difficulty of cracking.

3.2.1.1. Discussion

Hou's method used four halftone images, cyan, magenta, yellow and black, to share the secret image. In the theory of black-and-white visual cryptography, every pixel of a sharing image is displayed as half back-and-white to maximize the entropy of the sharing image. As such, although the black parts of the stacked image are still pure black, the white parts are no longer pure white but are half black-and-white instead. Also, the contrast of the stacked image is somewhat downgraded, but the content of the image can still be easily identified; in fact, 50% loss in contrast under his method is comparable to that under the traditional visual cryptography for binary images. In this method he used a black mask to cover the colors that he wanted to conceal in the stacked image. The regular black pixels were treated as image background and would not interfere with the meaningful part of the secret image. The human visual system could easily differentiate them and identify the content of the secret image. Without stacking the black mask on the top of the three sharing images, the unexpected colors would reveal on the stacked image and mix up with the meaningful part of the secret image. Consequently, the secrecy of the secret image could remain intact. This scheme therefore could enable a two-level security control in practice. For example, as long as a manager of a company keeps the black mask of a secret image and gives the rest three shares to his subordinates, the content of the image will remain confidential, even though all his subordinates plot to steal the secret information. Thus, under these circumstances, the black mask share can be regarded as the signature of the manager.

3.2.2 Method 2

A yet another method of color visual cryptography was proposed by Qiao, Yin and Liang, which was based on the CMY color model and the halftone technique [3]. In their method, firstly, a chromatic image was decomposed into three monochromatic images in tones of cyan, magenta and yellow. Secondly, these three images were transformed into binary images by halftone technique. Finally, the traditional binary secret sharing scheme was used to get the sharing images.



(a) The true gray image (b) Binary image1

(c) Binary image2 (d) Binary image3

Figure 8: Basic Principle of Halftone Technique

Halftone technique is a method to display a gray image with black-and-white spots, as discussed above. Fig. 8 shows the basic principle of the halftone technique. The more black spots the image includes, the more the image will be alike the true gray image. Construct to the other two binary images shown in Fig. 8(c) and (d), Figure 8(b) is closest to the true gray image.In their method, they used the Floyd-Steinberg Algorithm to get the halftone images. For an 8-bit grayscale image, the gray value of the image is from 0(black) to 255(white).the halftone images.

Letting b=0, w=255, t= int [(b+w)/2] =128.

Assuming *g* is the gray value of the image, which location is *P (x, y)*, *e* is the difference between the computed value and the correct value. Then the Floyd-Steinberg Algorithm can be described as following:

If g > t then

print white;

e=g-w;

else

print black;

e=g-b;

(3/8 × e) is added to P (x+1, y);

(3/8 × e) is added to P (x, y+1);

(1/4 × e) is added to P (x+1, y+1);

End if

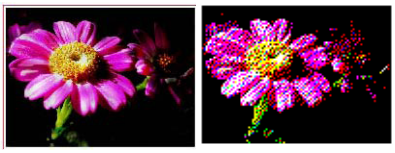
For example, a point with the gray value of 130 in an image should be gray point. Since the intensity of general image changes continuously, so the values of adjacent pixels are likely close to 130, and the surrounding region is also gray. According to the Algorithm, the number 130 is bigger than 128, then a white point is printed on the new image. But 130 are away from the real white 255. While -46(-125 multiplied by 3/8) added to adjacent pixel, the value of adjacent pixel is close to 0; the adjacent pixel comes to black. Next time, *e* also become positive, the adjacent pixel comes to white, so a white one after a black one, gray is demonstrated. If not transmitting the error, the pixel in the new image is white. Take another example; if the gray value of a point is 250, it should be white in gray image, and *e* equals to -5, it has little impact on the adjacent pixel. This certificates the correctness of the algorithm.

3.2.2.1. Results and Discussion

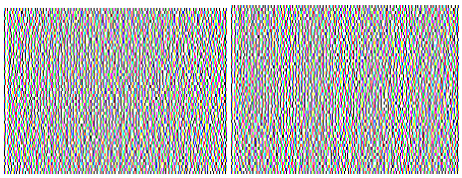
In the experiment carried out in [3], authors made a (2, 3) visual threshold scheme for natural images, which could be extended to general access structures. The basic matrixes used were as following:

$$M0=\begin{matrix}0\ 1\ 1\\0\ 1\ 1\\0\ 1\ 1\end{matrix}\qquad M1=\begin{matrix}1\ 0\ 1\\1\ 0\ 1\\1\ 0\ 1\end{matrix}\qquad M2=\begin{matrix}1\ 1\ 0\\1\ 1\ 0\\1\ 1\ 0\end{matrix}$$

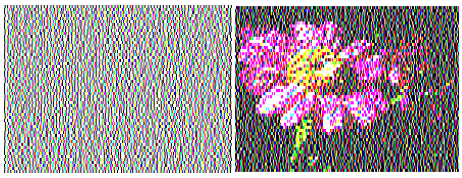
They showed the results taking Fig. 9 as an example. Figure 9(a) was an original chromatic image. Firstly it was decomposed into three monochromatic images in tones of cyan, magenta and yellow. Secondly, these three images were transformed into binary images by halftone technique. If those three monochromatic images were composed into a chromatic image, Figure 9(b) was obtained. Thirdly, every monochromatic image was considered as a secret image and traditional binary image-sharing scheme was used to divide it into three secret shares with same color, and then, any three different colors were chosen, of which to compose them into three colored shares S1, S2 and S3, as shown in Figure9(c), (d) and (e). As shown in Figure 9(f), (g), (h) and (i), the original secret information was visible by stacking any 2 or 3 transparencies, but none secret information will be revealed by only one transparency. This new secret color image sharing scheme provided an efficient way to recover the shared secret information.



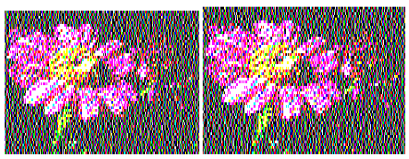
(a) Original (b) Halftone



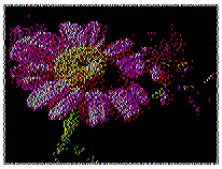
(c) S1 (d) S2



(e) S3 (f) S1+S2



(g) S3+S2 (h) S1+S3



(i) S1+S2+S3

Figure 9: Simulation results for (2, 3) scheme

4. CONCLUSION

Currently, many new schemes are proposed in the field of Color Visual Cryptography. We have seen that all the schemes discussed above, use Naor and Shamir's basic model of visual cryptography as the basis. But at the same time, the shares produced by all the methods above are either meaningless or are dependent upon some factors like the number of colors in the secret image. The disadvantage of Hou's method is that the stacked image is somewhat downgraded, and there is 50% loss in contrast under his method. In method 2, it was shown that the size of the shares and the implementation complexity in these schemes did not depend on the number of colors appearing in the secret image. Furthermore, according to different basic matrixes, the present method could be easily extended to (k, n) threshold and arbitrary use of the visual structure for natural images processing. This was the advantage of method 2. In method 1 and 2, it was seen that very few color VC schemes produce meaningful shares, but we consider this a pretty meaningful field of research to explore.

REFERENCES

[1]. M. Naor, A. Shamir, in: A. De Santis (Ed.), Visual Cryptography, Advances in Cryptology: Eurpocrypt'94, Lecture Notes in Computer Science, Vol. 950, Springer, Berlin, 1995, pp. 1–12.

[2]. Y. C. Hou, "Visual cryptography for color images," *Pattern Recognition*, Vol. 36, pp.1619-1629, 2003.

[3]. Wei Qiao, Hongdong Yin, Huaqing Liang, "*A Kind of Visual Cryptography Scheme For Color Images Based on Halftone Technique*", 2009 International Conference on Measuring Technology and Mechatronics Automation.

[4]. Hsien-Chu Wu1, Hao-Cheng Wang2, and Rui-Wen Yu3, "*Color Visual Cryptography Scheme Using Meaningful Shares*", Eighth International Conference on Intelligent Systems Design and Applications, 2008.

[5]. 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, pp. 179-196, 1997.