PERGAMON

Pattern Recognition 36 (2003) 1619–1629

PATTERN RECOGNITION
THE JOURNAL OF THE PATTERN RECOGNITION SOCIETY

www.elsevier.com/locate/patcog

Visual cryptography for color images

Young-Chang Hou*

Department of Information Management, National Central University, Jung Li, Taiwan 320, ROC

Received 6 June 2002; accepted 26 August 2002

Abstract

Visual cryptography, an emerging cryptography technology, uses the characteristics of human vision to decrypt encrypted images. It needs neither cryptography knowledge nor complex computation. For security concerns, it also ensures that hackers cannot perceive any clues about a secret image from individual cover images. Since Naor and Shamir proposed the basic model of visual cryptography, researchers have published many related studies. Most of these studies, however, concentrate on binary images; few of them proposed methods for processing gray-level and color images. This paper proposes three methods for visual cryptography of gray-level and color images based on past studies in black-and-white visual cryptography, the halftone technology, and the color decomposition method. Our methods not only retain the advantages of black-and-white visual cryptography, which exploits the human visual system to decrypt secret images without computation, but also have the backward compatibility with the previous results in black-and-white visual cryptography, such as the t out of n threshold scheme, and can be applied to gray-level and color images easily.

Keywords: Visual cryptography; Halftone technology; Color decomposition; Information sharing

1. Introduction

It is now common to transfer multimedia data via the Internet. With the coming 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.

Naor and Shamir [1] proposed a new cryptography area, visual cryptography, in 1994. The most notable feature of this approach is that it can recover a secret image without any computation. It exploits the human visual system to read the secret message from some overlapping shares, thus overcoming the disadvantage of complex computation required in the traditional cryptography. The threshold scheme [1–3] makes the application of visual cryptography more flexible. With the t out of n threshold scheme ($t \leqslant n$), the manager can first produces n copies of transparency drawn from the secret image, one for each of his members. If any t of them stacks their transparencies together, the content of the secret image will show up. If the number of transparencies is less than t, the content of the secret image will remain hidden.

There have been many published studies [1–10] of visual cryptography. Most of them, however, have concentrated on discussing black-and-white images, and just few of them have proposed methods for processing gray-level and color images. Rijmen and Preneel [8] have proposed a visual cryptography approach for color images. In their approach, each pixel of the color secret image is expanded into a 2×2 block to form two sharing images. Each 2×2 block on the sharing image is filled with red, green, blue and white (transparent), respectively, and hence no clue about the secret image can be identified from any one of these two shares alone. Rijman and Preneel claimed that there would be 24 possible combinations according to the permutation of the four

* Tel.: +886-3-426-7255.

E-mail address: ychou@mgt.ncu.edu.tw (Y.-C. Hou).

0031-3203/03/$30.00 © 2003 Pattern Recognition Society. Published by Elsevier Science Ltd. All rights reserved.
PII: S0031-3203(02)00258-3

colors. Because human eyes cannot detect the color of a very tiny subpixel, the four-pixel colors will be treated as an average color. When stacking the corresponding blocks of the two shares, there would be 24^2 variations of the resultant color for forming a color image. The approach of Rijmen and Preneel indeed can produce visual cryptography for color images. But from the viewpoint of either the additive model or the subtractive model of chromatology, it is not appropriate to fill the blocks with red, green, blue, and white (transparent) colors [11]. Besides, if we use the average of the four-pixel colors in the stacking blocks to represent the corresponding pixel color in the original image, the problem of circular permutations occurs. Since two circular permutations of a stacking block are not considered different, two average colors with different permutations will be the same in the stacking block if they have the same combination. Hence the number of possible color variation is fewer than the authors claimed 24^2.

Recently, Chang et al. [12] proposed a color image sharing technique. The algorithm first creates a palette of a secret image and assigns a unique code to each color on the palette. It then selects two colored cover images, O^1 and O^2, with size the same as the secret image. Every pixel in the two cover images will be expanded into a block with $M(=k \times k)$ subpixels, of which $\lfloor M/2 \rfloor + 1$ subpixels are randomly selected and filled with the color of the expanded pixel and the rest are filled with white (transparent) color. The selection condition is that N positions of the two expanded blocks are overlapped, where N is the index of the palette of the secret image and is used to indicate the pixel color shared by the two expanded blocks. When recovering the secret image, the algorithm computes the number of the overlapping subpixels of every $k \times k$ block in the two camouflage images and then retrieves the Nth color from the palette to reconstruct the color of the corresponding pixel of the secret image. But this method can only deal with a color image with limited different colors. For example, if k equals 3, $\lfloor M/2 \rfloor + 1$ is at most 5, which is obviously too small and unreasonably restrictive for today's applications.

Hou et al. [13,14] proposed a method to improve the above drawback. They used the binary encoding to represent the subpixels selected for each block and applied the AND/OR operation randomly to compute the binary code for the stacking subpixels of every block in the cover images. The code ranges from 0 to 255, but it can be even larger depending on the expanding factor. Consequently, a secret image can be a 256 color or true-color one.

Although Chang and Hou et al. [12–14] achieved a certain degree of sharing color image information, the drawback is that secret images must be decrypted with heavy computation, which would violate the principle of visual cryptography that uses human eyes to decrypt secret images.

Hou et al. [15] used the concepts of color decomposition and contrast adjustment to produce two shares needed by visual cryptography. Overlapping these two shares will reveal the secret information automatically. Although this method requires no mass computation to reconstruct secret images, it is nonetheless difficult to obtain totally random noise shares. Some image boundaries might be found on each share, thus compromising the secrecy required.

In this paper, we will combine the previous results in visual cryptography, the halftone technology, and the color decomposition principle to develop algorithms of visual cryptography for gray-level and color images. Our method retains the advantage of traditional visual cryptography, namely, decrypting secret images by human eyes without any cryptography computation. For information security, it also ensures that hackers cannot perceive any clue about the secret image from any individual sharing image.

This paper is organized as follows. Section 2 first briefly reviews the basic theorems of visual cryptography and halftone technology. A visual cryptography suitable for gray-scale images based on halftone technology is then proposed. Based on this gray-scale technique, Section 3 presents three different visual cryptography schemes suitable for color images. It also reports and discusses some experimental results. Finally, conclusions appear in Section 4.

2. Visual cryptography for gray-level images

2.1. Basic theorem of visual cryptography

Because the output media of visual cryptography are transparencies, we treat the white pixels of black-and-white images as transparent. 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

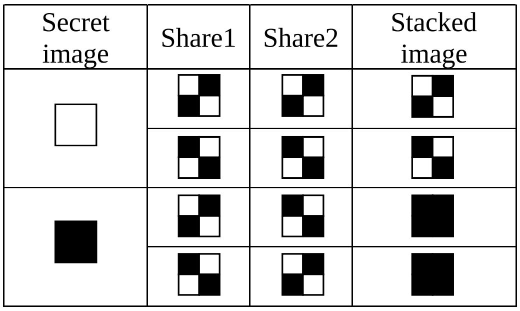


Fig. 1. Sharing and stacking scheme of black and white pixels.

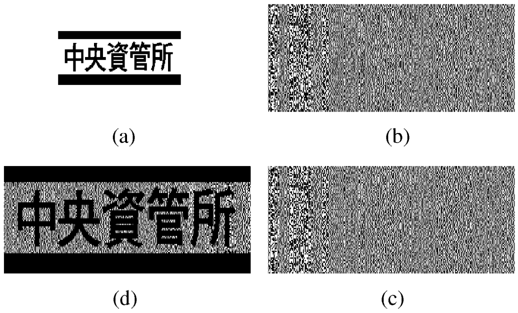


Fig. 2. Visual cryptography for "中央資管所": (a) Secret image; (b) Share image 1; (c) Share image 2; (d) Recovering image.

content of the block in the two transparencies; when a pixel is black, it chooses one of the other two combinations. Then, the characteristics of two stacked pixels are: black and black is black, white and black is black, and white and white is white. Therefore, when stacking two transparencies, the blocks corresponding to black pixels in the secret image are full black, and those corresponding to white pixels are half-black-and-half-white, which can be seen as 50% gray 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) with the words of "中央資管所" is decomposed into two visual cryptography transparencies (b) and (c). When stacking the two transparencies, we can obtain the reconstructed image (d). Even though the contrast of the resulting image is degraded by 50%, human eyes can still identify the content of the secret image easily.

2.2. The halftone technology

According to their physical characteristics, different media use different ways to represent the color level of images. 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" [11] and transforms an image with gray level into a binary image before processing. 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.

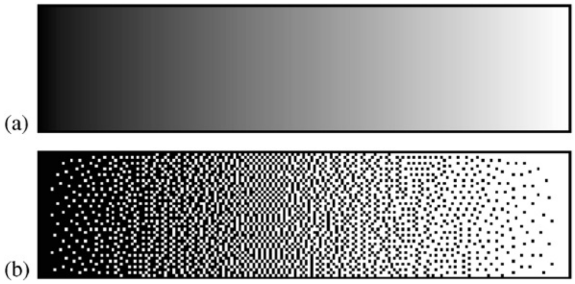


Fig. 3. (a) Continuous tone, and (b) Halftone.

2.3. Gray-level visual cryptography

Since most printers have to transform gray-level images into halftone ones before printing, and the transformed halftone images are black-and-white only, such an image format is very suitable for the traditional method to generate the shares of visual cryptography. So in this paper, we use transformed halftone images to generate the visual cryptography for gray-level images. The algorithm is as follows:

1. Transform the gray-level image into a black-and-white halftone image.
2. For each black or white pixel in the halftone image, decompose it into a 2×2 block of the two transparencies according to the rules in Fig. 1. If the pixel is white, randomly select one combination from the former two rows in Fig. 1 as the content of blocks in Shares 1 and 2. If the pixel is black, randomly select one combination from the latter two rows as the content of the blocks in the two transparencies.
3. Repeat Step 2 until every pixel in the halftone image is decomposed, hence resulting in two transparencies of visual cryptography to share the secret image.

2.4. Experiment and discussion

According to the above algorithm, we first transformed the gray-level image in Fig. 4a into a halftone image (Fig. 4b) and then generated two transparencies of visual cryptography (Fig. 5a and 5b). Obviously, we indeed cannot detect any information about the secret image from the two sharing transparencies individually, but when stacking them together, the result clearly shows a picture of a little boy as shown in Fig. 5c.

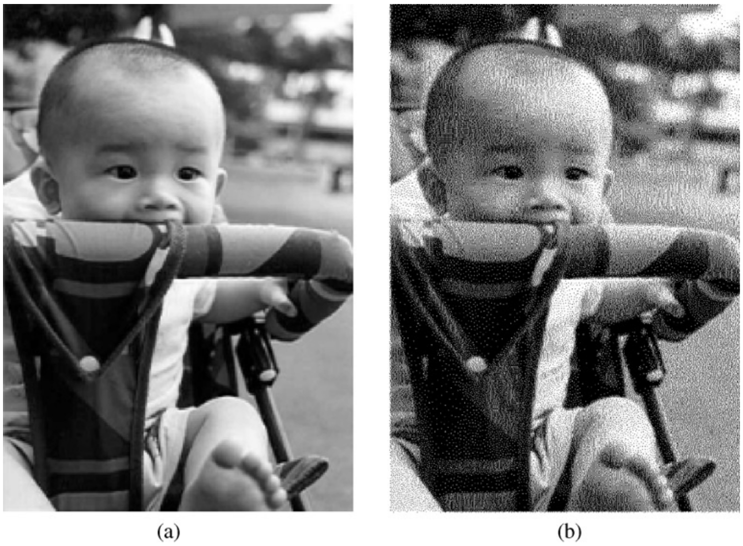


Fig. 4. (a) Continuous tone, and (b) Halftone.

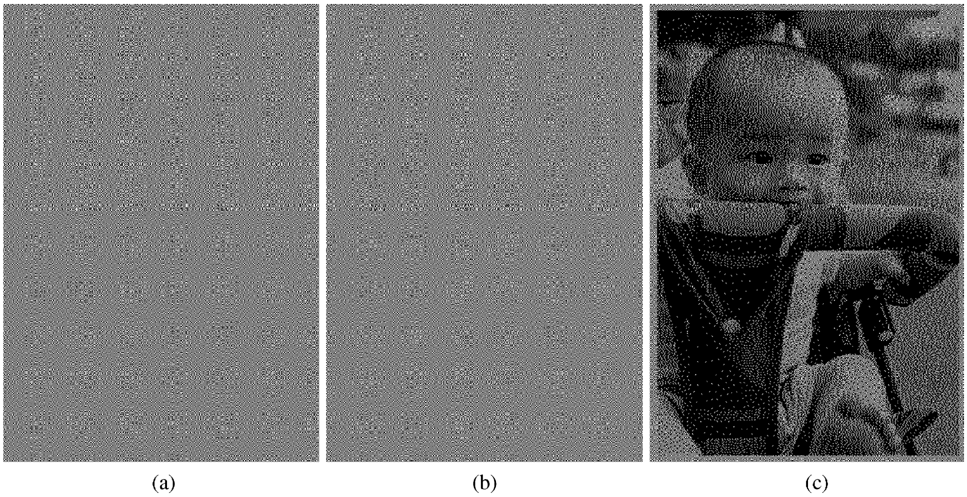
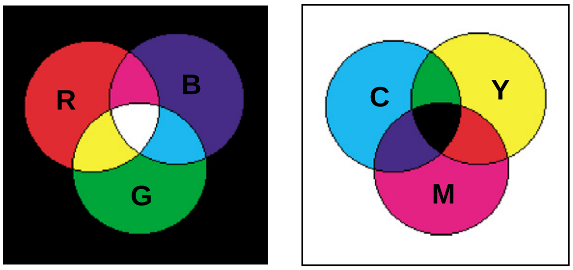


Fig. 5. Generation and stacking of gray-level visual cryptography: (a) Transparency 1, (b) Transparency 2, and (c) Transparency 1+ Transparency 2.

3. Visual cryptography for color images

3.1. Basic principles of color

The additive and subtractive models (Fig. 6) are commonly used to describe the constitutions of colors [11]. 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 more 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 model. 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)



(a) (b)

Fig. 6. (a) Additive model, and (b) Subtractive model.

pigments, we 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.

The above discussion illustrates that Rijmen and Preneel's [8] approach, which uses red, green, blue, and white (transparent) colors to fill the blocks, is not appropriate. In the additive model, any color mixed with white color is still white color. 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, we use sharing images as the decryption tool; that is, the final outputs are transparencies. Because the subtractive model is more suitable for printing colors on transparencies, we will use the CMY model to represent colors in what follows. 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. Print of color images

Because most color printers use C, M, Y inks to display color, a color image must be processed by the color-decomposed procedure before printing. Color decomposition mainly is to separate C, M, and Y colors from colors within every pixel of the image. These three components form three monochromatic images. (Because colored ink is expensive and the mechanical tolerances may cause the three inks to be printed slightly out of register, the black edges will suffer colored tinges. So, some printers add the black ink when printing black color, resulting in four separate color images.) These monochromatic images are like gray-level images in which every pixel has its own color level and has to be transformed into a halftone image before printing. The three monochromatic halftone images will be (cyan, white), (magenta, white) and (yellow, white) binary images, respectively. After stacking these images, all kinds of the colors in the original image can be displayed. Fig. 7 illustrates the procedure of printing color images.

We can see from the figure that every pixel P_{ij} of the composed color image P is obtained by combining the corresponding pixels C_{ij}, M_{ij}, Y_{ij} in the three C, M, and Y separating halftone images, where C, M, and Y images are all binary. For any pixel, C_{ij}, M_{ij} or Y_{ij}, there are only two possible values: blank or not blank, where 0 denotes blank, and 1 denotes the corresponding color. Hence P_{ij} has the following possible combinations: (0, 0, 0), (1, 0, 0), (0, 1, 0), (0, 0, 1), (1, 1, 0), (1, 0, 1), (0, 1, 1), and (1, 1, 1), where P_{ij} (0, 0, 0) denotes a white pixel, and (1, 1, 1) denotes a black pixel. Because C, M, and Y are primitive colors in the subtractive model, they retain the usual characteristics that C (M or Y) plus C (M or Y) is C (M or Y), C (M or Y) plus white is C (M or Y), and white plus white is white, when stacking them on transparent media. In the following sections, we will introduce our three methods for color visual cryptography.

3.3. Method 1

Our first method uses the procedure illustrated in Fig. 7 to transform a color secret image into three C, M, and Y halftone images. Then, every pixel of the halftone images is 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 includes two transparent (white) pixels and two color pixels so that the entropy reaches its maximum to conceal the content of the secret image. Furthermore, we design a half black-and-white mask to shade unexpected colors on the stacked sharing images so that only the expected colors show up.

Take Fig. 8 for example. If pixel P_{ij} of the composed image is (0, 0, 0), the distribution of the color pixels in the three sharing images is assigned as the first row in Fig. 8. After stacked by the mask image, all the color pixels on the

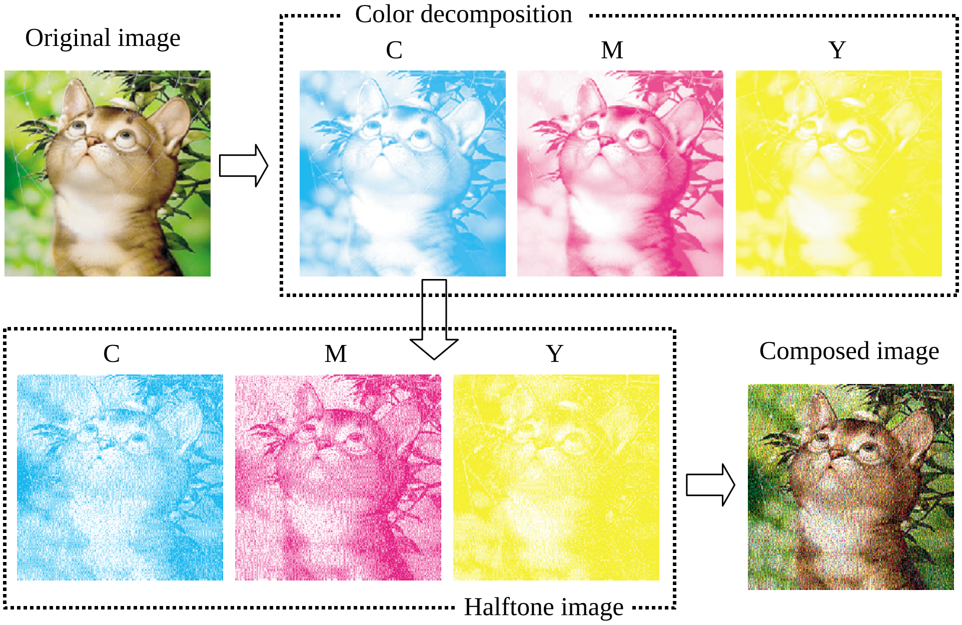


Fig. 7. Color image printing.

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)

Fig. 8. Scheme 1 of color cryptography.

three sharing images are shaded by black pixels and only the white pixels can reveal, thus showing a white-like color. If pixel P_{ij} is (1, 1, 0), only the C and M components are revealed, with the Y component being covered by the black mask. The distribution of the color pixels in the three sharing images is as the fifth row in Fig. 8, thus showing a blue-liked (cyan plus magenta) color. If pixel P_{ij} is (1, 1, 1), the C, M, and Y parts can all be revealed, thus showing a black color. The distribution of the color pixels in the three sharing images is as the eighth row in Fig. 8. The eight combinations of the three primary colors of the composed image under this method are illustrated in Fig. 8.

Moreover, we can also analyze the color distribution of the stacked image in terms of color quantity. For example, the first row in Fig. 8 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 $\frac{1}{2}$. If the distribution of color pixels in the composed image is as the fifth row in Fig. 8, only C and M are 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 can appear in all four blocks of a 2×2 block in the composed image, but yellow only appears in two. So the color intensity of C, M and Y can be denoted as $(1, 1, \frac{1}{2})$. If the distribution of color pixels in the composed image is as the eighth row in Fig. 8, four blocks are all black and the color intensity (C, M, Y) can be denoted as (1, 1, 1). Thus, with this method, we can use $(\frac{1}{2}, \frac{1}{2}, \frac{1}{2})$, $(1, \frac{1}{2}, \frac{1}{2})$, $(\frac{1}{2}, 1, \frac{1}{2})$,

$(\frac{1}{2}, \frac{1}{2}, 1)$, $(1, 1, \frac{1}{2})$, $(\frac{1}{2}, 1, 1)$, $(1, \frac{1}{2}, 1)$, and $(1, 1, 1)$ to denote the combinations of the primary colors in a composed image. As a result, white pixels in a stacked image are no longer pure white $(0, 0, 0)$, but are half black-and-white $(\frac{1}{2}, \frac{1}{2}, \frac{1}{2})$ instead. Accordingly, the colors in a stacked image are no longer distributed between $(0, 0, 0)$ and $(1, 1, 1)$, but are distributed between $(\frac{1}{2}, \frac{1}{2}, \frac{1}{2})$ and $(1, 1, 1)$. This result is similar to the contrast loss occurred in black-and-white visual cryptography.

In this method, there are 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, we can randomly select the mask and the corresponding distribution of shares to raise the difficulty of cracking. The following describes our first algorithm.

3.3.1. Algorithm of color visual cryptography—method 1

1. Transform the color image into three halftone images: C, M, and Y.
2. For each pixel P_{ij} with color components (C_{ij}, M_{ij} or Y_{ij}) of the composed image P, do the following:
   (a) Select a black mask with a size of 2×2, and assign a black pixel randomly to two of these four positions and leave the rest positions blank (transparent or white). This step will make the black mask a half black-and-white block.
   (b) After selecting a mask, determine the positions of the cyan pixels in the block of the corresponding sharing images. This is done according to the positions of the black pixels in the mask and the value of C_{ij}.

   If $C_{ij} = 1$ (the cyan component will be revealed), fill the positions corresponding to the positions of the white pixels in the mask with a cyan pixel and leave the rest positions blank.

   If $C_{ij} = 0$ (the cyan component will be hidden), fill the colors in the opposite way. That is, fill the positions corresponding to the positions of the black pixels in the mask with a cyan pixel and leave the rest positions blank.

   Finally, add the block to the corresponding position of Share 1.
   (c) In accord with (b), determine the positions of magenta pixels of the block in Share 2 with the value of M_{ij} and those in Share 3 with the value of Y_{ij}.
3. Repeat Step 2 until every pixel of the composed image is decomposed, hence obtaining four transparencies (cyan, magenta, yellow and black) of visual cryptography to share the secret image.
4. After stacking the four sharing images, the secret image can be decrypted by human eyes.

3.3.2. Experiment and discussion

We use four halftone images, cyan, magenta, yellow and black, to share the secret image (Fig. 9). The codes of the four sharing images are fully disordered, and we cannot perceive any clue of the original secret image from any single sharing 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 our method is comparable to that under the traditional visual cryptography for binary images.

In this method we use a black mask to cover the colors that we want to conceal in the stacked image. The regular black pixels are treated as image background and would not interfere with the meaningful part of the secret image. The human visual system can 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 will reveal on the stacked image and mix up with the meaningful part of the secret image. Consequently, the secrecy of the secret image can remain intact. This scheme therefore can 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.

3.4. Method 2

Although there are only 8 different resultant colors in the stacked image based on Method 1, it is still difficult for us to find out that Fig. 9(e) is actually not a continuous-tone image. This is because human eyes cannot identify color pixels that are too tiny, so the nearby color pixels tend to be mixed up by human eyes, thus forming an average color. Because the halftone and color-decomposition techniques can be used to display various colors, another scheme for color visual cryptography can be constructed. The second method expands every pixel of a halftone image into a 2×2 block on two sharing images and fills the block with cyan, magenta, yellow and transparent, respectively. Using these four colors, two stacked images can generate various colors with different permutations. Take Fig. 10 for example. The distributions of colors in Shares 1 and 2 of the first row are the same. Human eyes will mix up and equalize the effect of the four stacked pixels (cyan, magenta, yellow and transparent) and see a white-like color. In terms of color intensity, cyan, magenta, and yellow each occupies a quarter of the block, i.e., $(\frac{1}{4}, \frac{1}{4}, \frac{1}{4})$. Shares 1 and 2 of the second row exchange the positions of cyan and transparent to reveal two cyan pixels, one magenta pixel, and one yellow pixel within the four pixels after stacking. Therefore, the color

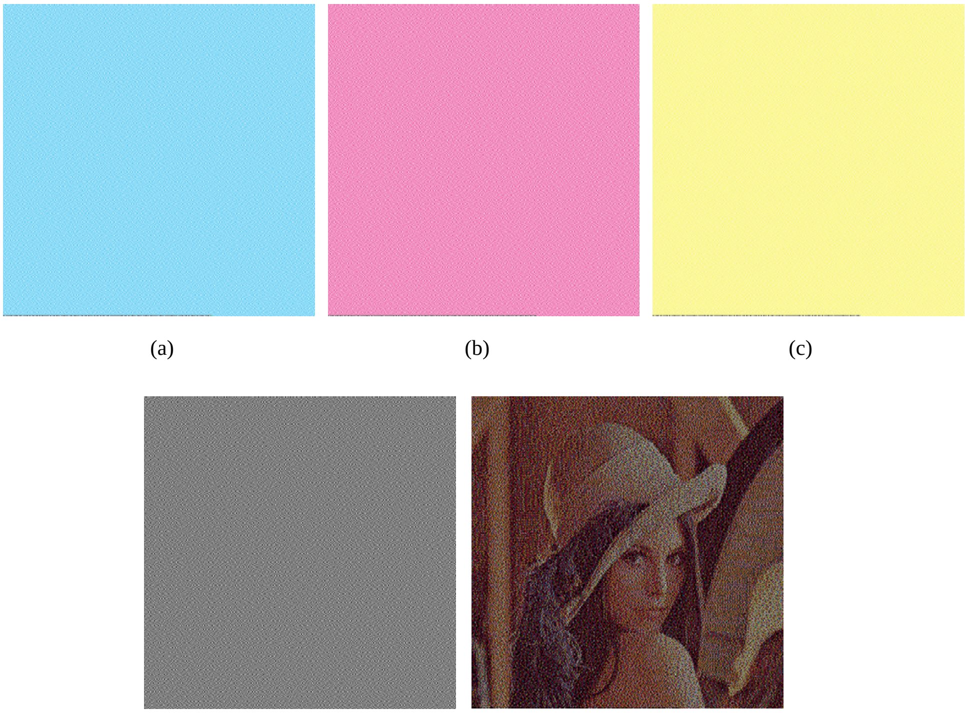


Fig. 9. Four separating shared transparencies and result of stacking: (a) Share 1(C), (b) Share 2(M), (c) Share 3(Y), (d) Mask, and (e) stacked image.

Revealed color (C,M,Y)	Share 1	Share 2	Stacked image	Method	Resultant result	Revealed color quantity (C,M,Y)
(0, 0, 0)	🟦🟪 🟨⬜	🟦🟪 🟨⬜	🟦🟪 🟨⬜	Share 1and Share 2 with the same permutation	⬜	(1/4, 1/4, 1/4)
(1, 0, 0)	🟦🟪 🟨⬜	⬜🟪 🟨🟦	🟦🟪 🟨🟦	Swap the position of cyan and transparent	🟦	(1/2, 1/4, 1/4)
(0, 1, 0)	🟦🟪 🟨⬜	🟦⬜ 🟨🟪	🟦🟪 🟨🟪	Swap the position of magenta and transparent	🟪	(1/4, 1/2, 1/4)
(0, 0, 1)	🟦🟪 🟨⬜	🟦🟪 ⬜🟨	🟦🟪 🟨🟨	Swap the position of yellow and transparent	🟨	(1/4, 1/4, 1/2)
(1, 1, 0)	🟦🟪 🟨⬜	🟪🟦 🟨⬜	🔵🔵 🟨⬜	Swap the position of cyan and magenta	🔵	(1/2, 1/2, 1/4)
(0, 1, 1)	🟦🟪 🟨⬜	🟦🟨 🟪⬜	🟦🟥 🟥⬜	Swap the position of yellow and magenta	🟥	(1/4, 1/2, 1/2)
(1, 0, 1)	🟦🟪 🟨⬜	🟨🟪 🟦⬜	🟩🟪 🟩⬜	Swap the position of cyan and yellow	🟩	(1/2, 1/4, 1/2)
(1, 1, 1)	🟦🟪 🟨⬜	⬜🟨 🟪🟦	🟦🟥 🟥🟦	Swap two positions in pair	🟥	(1/2, 1/2, 1/2)

Fig. 10. Scheme 2 for color visual cryptography.

intensity is $(\frac{1}{2}, \frac{1}{4}, \frac{1}{4})$, showing a cyan-liked color. To obtain a composed image, we can follow the instruction in Fig. 10 to select a distribution of colors for the blocks in Shares 1 and 2 and generate two sharing transparencies. After stacking the two sharing transparencies, we can get a stacked image with color intensity ranging from $(\frac{1}{4}, \frac{1}{4}, \frac{1}{4})$ to $(\frac{1}{2}, \frac{1}{2}, \frac{1}{2})$.

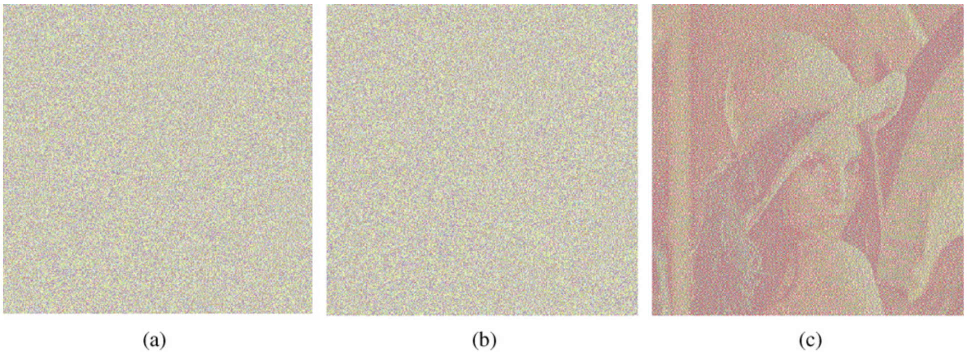


Fig. 11. Two sharing transparencies and stacked effect: (a) Share 1, (b) Share 2, and (c) stacked image.

So, there are $3! = 6$ combinations of color distribution within a 2×2 block on Share 1, which in turn can be used as the basis for generating the corresponding Share 2. As a result, the difficulty of cracking visual cryptograms is increased.

3.4.1. *Algorithm of color visual cryptography—method 2*

1. Transform the color image into three halftone images: C, M, and Y.
2. For each pixel P_{ij} of the composed image, do the following:
   (a) Expand a 2×2 block in Share 1 and fill the block with cyan, magenta, yellow, and transparent randomly.
   (b) Generate a 2×2 block in Share 2 according to the permutation of the four colors of the block in Share 1 and the values of C_{ij}, M_{ij}, Y_{ij}, and determine the color distribution of the corresponding block in Share 2 as illustrated in Fig. 10. Take a pixel with $P_{ij} = (1, 1, 0)$ for example. When deciding the clockwise permutation of the block in Share 1 to be cyan→magenta→white→yellow, swap the positions of cyan and magenta and form the permutation of the corresponding block in Share 2 as magenta→cyan→white→yellow. The stacked result will be a blue-like block, just as the pixel $(1,1,0)$ should be on the secret image.
3. Repeat Step 2 until every pixel of the composed image is decomposed, hence obtaining two visual cryptography transparencies to share the secret image.
4. After stacking the two sharing images, the secret image can be decrypted by human eyes.

3.4.2. *Experiment and discussion*

We exploit the three halftone images of Lenna to generate the two sharing images (Fig. 11). As the figure shows, no clue of the original secret image can be perceived from either one of the sharing images alone, but the content of the image can still be easily identified from the stacked image.

Method 2 reduces the inconvenience of Method 1 and requires only two sharing images to encrypt a secret image. However, because the two sharing images have equal privilege, this method cannot provide a two-level control as the Method 1 does. Moreover, as illustrated in Fig. 10, the color intensity of the stacked image is limited between $(\frac{1}{4}, \frac{1}{4}, \frac{1}{4})$ to $(\frac{1}{2}, \frac{1}{2}, \frac{1}{2})$, where the white pixel is $(\frac{1}{4}, \frac{1}{4}, \frac{1}{4})$ and the black pixel is $(\frac{1}{2}, \frac{1}{2}, \frac{1}{2})$. In other words, after stacking the sharing images generated by Method 2, the range of color contrast will be 25% of that of the original image, whereas the range of color contrast of Method 1 will be 50% of that of the original image. So, the color saturation of the stacked image generated by Method 2 will be worse than that generated by Method 1, and a composed image produced by Method 2 will look brighter than that produced by Method 1. But, if the original image is dark in nature, Method 2 might actually generate a better result.

3.5. *Method 3*

In order to alleviate the inconvenience of Method 1, which needs four sharing images, and the loss of image contrast under Method 2, we construct a third method. This method needs only two sharing image and does not sacrifice too much contrast for color visual cryptography. It transforms a color secret image into three halftone images C, M, and Y and exploits the technique of gray-level visual cryptography in Section 2.3 to generate six temporary sharing images C1, C2, M1, M2, Y1, and Y2. Each of these sharing images will have two white pixels and two color pixels in every 2×2 block; i.e. all the color quantities are $\frac{2}{4}$. The method then combines C1, M1, and Y1 to form a colored halftone Share 1 and C2, M2, Y2 to form Share 2. So, for each block in Share 1 and Share 2, the color intensity is $(\frac{1}{2}, \frac{1}{2}, \frac{1}{2})$. After stacking Shares 1 and 2, the range of color intensity is between $(\frac{1}{2}, \frac{1}{2}, \frac{1}{2})$ to $(1, 1, 1)$. Fig. 12 shows how to decompose a blue pixel $(1, 1, 0)$ into two sharing blocks and how to reconstruct the blue-liked block.

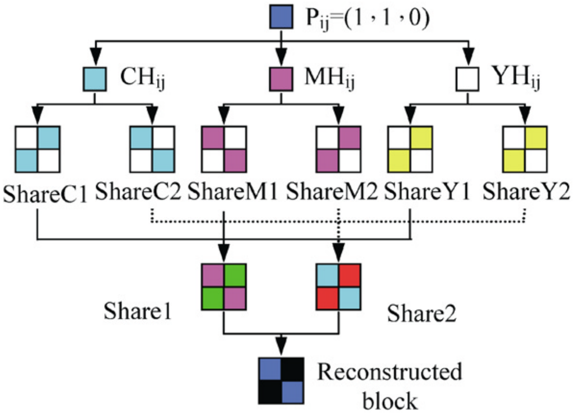


Fig. 12. Color pixel decomposition and reconstruction.

3.5.1. Algorithm of visual cryptography—method 3

1. Transform the color image into three halftone images: C, M, and Y.
2. For each pixel P_{ij} of the composed image, do the following:
   (a) According to the traditional method of black-and-white visual cryptography, expand C_{ij}, M_{ij} and Y_{ij} into six 2×2 blocks, $C1_{ij}, C2_{ij}, M1_{ij}, M2_{ij}$ and $Y1_{ij}$, $Y2_{ij}$.
   (b) Combine the blocks $C1_{ij}, M1_{ij}$ and $Y1_{ij}$ and fill the combined block corresponding to P_{ij} in Share 1.
   (c) Combine the blocks $C2_{ij}, M2_{ij}$ and $Y2_{ij}$ and fill the combined block corresponding to P_{ij} in Share 2.
3. Repeat Step 2 until every pixel of the composed image is decomposed, hence obtaining two visual cryptography transparencies to share the secret image.
4. After stacking the two sharing images, the secret image can be decrypted by human eyes.

3.5.2. Experiment and discussion

We use the Lenna image to generate the two required sharing images (Fig. 13). As the images generated by Methods 1 and 2, no clue of the original secret image can be perceived from any single sharing image and the content of the stacked image can be easily identified. Method 3, however, requires only two sharing images, which is better than Method 1, and loses less image contrast, which is better than Method 2. But like Method 2, the two sharing images generated by Method 3 will have equal privilege, so the method cannot provide a two-level control as Method 1 does.

4. Conclusion

Undoubtedly, Visual Cryptography provides one of the secure ways to transfer images on the Internet. The advantage of visual cryptography is that it exploits human eyes to decrypt secret images with no computation required. Unlike most studies of visual cryptography, which concentrate on black-and-white images, this paper exploits the techniques of halftone technology and color decomposition to construct three methods that can deal with both gray-level and color visual cryptography. Based on the theory of color decomposition, every color on a color image can be decomposed into three primary colors: C, M, and Y. With the halftone technology, we can transform a gray-level image into a binary one suitable for generating visual cryptography. As the traditional schemes for black-and-white visual cryptography, our methods expand every pixel of a color secret image into a 2×2 block in the sharing images and keep two color and two transparent pixels in the block.

Our study is the first one that exploits the color-decomposition and halftone technology to generate visual cryptograms for both gray-level and color images. Our methods can also be easily applied to the schemes developed in previous studies, such as the *t* out of *n* threshold scheme [3] and the extended schemes for visual cryptography [5].

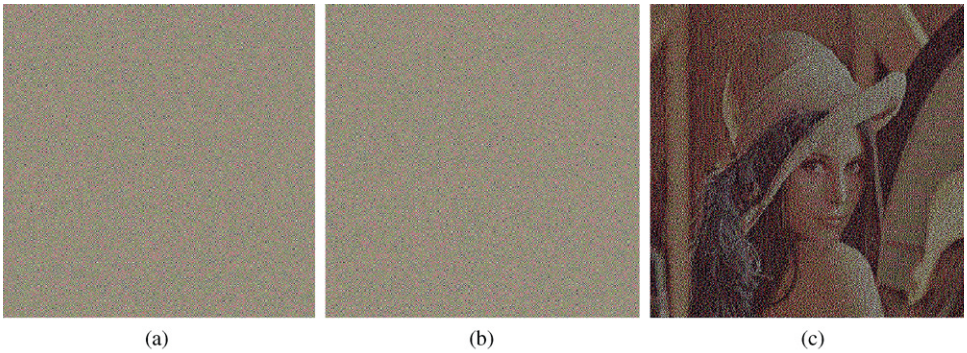


Fig. 13. Two sharing transparencies and stacked effect: (a) Share 1, (b) Share 2, and (c) stacked image.

Although our paper concerns color figures, the principles can be well understood by using black-and-white ones. Since color plates are expensive, the figures in this paper are printed in black-and-white format. Nonetheless, all figures (in Photoshop's format) contained in the paper can be found at http://140.115.82.2/∼ychou/pics/, and any interested reader may refer to the site.

Acknowledgements

This research was partly supported by National Science Council of the Republic of China under contract NSC89-2218-E-008-009. I gratefully acknowledge the valuable comments provided by Eric Wang on earlier drafts of this paper.

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] M. Naor, A. Shamir, in: M. Lomas (Ed.), Visual Cryptography, II: Improving the Contrast via the Cover Base, Presented at Security in Communication Networks, Amalfi, Italy, September 16–17, 1996. Lecture Notes in Computer Science, Vol. 1189, Springer, Berlin, 1997, pp. 197–202. Available also at Theory of Cryptography Library, Report 96-07, http://theory.lcs.mit.edu/∼tcryptol/1996.html.

[3] D.R. Stinson, An introduction to visual cryptography, presented at Public Key Solutions '97, Toronto, Canada, April 28–30, 1997. http://bibd.unl.edu/∼stinson/vcs-pus.ps

[4] G. Ateniese, C. Blundo, A. De Santis, D.R. Stinson, Visual cryptography for general access structures, Inform. Comput. 129 (1996) 86–106.

[5] G. Ateniese, C. Blundo, A. De Santis, D.R. Stinson, Extended schemes for visual cryptography, http://www.disi.unige.it/person/AtenieseG/.

[6] C. Blundo, A. De Santis, D.R. Stinson, On the contrast in visual cryptography schemes. J. Cryptology, Vol. 12, 1999, 261–289. Available also at Theory of Cryptography Library, Report 96-13, http://theory.lcs.mit.edu/∼tcryptol/1996.html.

[7] M. Naor, B. Pinkas, Visual authentication and identification, in: B. Kaliski, Jr. (Ed.), Advances in Cryptology—CRYPTO '97, Lecture Notes in Computer Science, Vol. 1294, Springer, Berlin, 1997, pp. 322–336. http://theory.lcs.mit.edu/∼tcryptol/.

[8] V. Rijmen, B. Preneel, Efficient colour visual encryption for shared colors of Benetton, Eurocrypto'96, Rump Session, Berlin, 1996. Available at http://www.iacr.org/conferences/ec96/rump/preneel.ps.

[9] A.D. Rubin, Independent one-time passwords, Comput. Systems 9 (1996) 15–27.

[10] A. Shamir, Visual cryptanalysis, Proceedings of the Eurocrypt'98, Espoo, 1998.

[11] C.A. Poynton, Frequently asked questions about color, http://www.inforamp.net/∼poynton.

[12] C.C. Chang, C.S. Tsai, T.S. Chen, A technique for sharing a secret color image, Proceedings of the Ninth National Conference on Information Security, Taichung, May 1999, pp. LXIII–LXXII.

[13] Y.C. Hou, F. Lin, C.Y. Chang, Improvement and implementation of the secret color image sharing technique, Proceedings of the Fifth Conference on Information Management, Taipei, November 1999, pp. 592–597.

[14] Y.C. Hou, F. Lin, C.Y. Chang, A new approach on 256 color secret image sharing technique, MIS Review, No. 9, December 1999, pp. 89–105.

[15] Y.C. Hou, C.Y. Chang, F. Lin, Visual cryptography for color images based on color decomposition, Proceedings of the Fifth Conference on Information Management, Taipei, November 1999, pp. 584–591.

About the Author—HOU YOUNG-CHANG was born in Kwangtung, ROC. in 1949. He got his B.S. from the Department of Atmospheric Physics, National Central University in 1972, M.S. from the Division of Computer Application, Asian Institute of Technology, Bangkok, Thailand in 1983, and Ph.D. from Computer Science and Information Engineering, National Chiao-Tung University in 1990. Since 1990, he has been an associate professor of the Department of Information Management, National Central University. His current research interests include soft computing, image processing, information hiding, and cryptography.