Random-grid-based Visual Cryptography Schemes

Young-Chang Hou, Shih-Chieh Wei, and Chia-Yin Lin

***Abstract*—This study discusses a random-grid-based non-expanded visual cryptography scheme for generating both meaningful and noise-like shares. First, the distribution of black pixels on the share-images and the stack-image is analyzed. A probability allocation method is then proposed which is capable of producing the best contrast in both of the share-images and the stack-image. With our method, not only can different cover images be used to hide the secret image, but the contrast can be set as needed. The most important result is the improvement of the visual quality of both the share-images and the stack-image to their theoretical maximum. Our meaningful visual secret sharing method is shown in experiments to be superior to past methods.**

***Index Terms*—Meaningful shares, random grid, secret sharing, visual cryptography.**

I. Introduction

To ensure the confidentiality, integrity and availability of data transmission over the Internet, traditional cryptography uses a secret key and complicated computing to convert plain text into meaningless text. The biggest drawback is that a computer is needed for the encryption and decryption processes, resulting in extensive execution time and wastage of computational resources.

Naor and Shamir (1995) proposed a visual secret sharing method, namely visual cryptography (VC), which can encode a secret image into n noise-like shares. The secret image can be decrypted by the human eye when any k or more shares are stacked together. The greatest advantage of this decryption process is that neither complex computations nor any knowledge about VC are needed. It is a simple and safe secret sharing method for the decoding of secret images when computer-resources are lacking. However, since VC uses a pixel expansion method to decompose the secret image, the share-images are larger than the original secret image. The drawbacks of this are wastage of storage space, image distortion and the share-images are difficult to carry. Since the concept of visual cryptography was first proposed, there have been several studies making efforts to deal with the pixel expansion problem [2-11]. Most of these have fallen into the category of probability visual cryptography schemes.

Ito *et al*. [2] and Yang [5] used the concept of probability to interpret the meaning of the Boolean matrices proposed by the conventional VC and proposed a pixel non-expansion method suitable for binary images. However, the random nature of probability means that the shares have poor display quality. Tu and Hou [4] adopted Ito's method [2] but utilized multiple successive pixels in the secret image as the unit of encryption. They generated smooth-looking shares of invariant size for gray-level secret images.

In 1987, Kafri and Keren [6] proposed a random grid visual secret sharing (RGVSS) method, which has gained more attention over the years. In their method, each pixel of the image is treated as a grid, with a random variable used to encrypt the secret image. The biggest benefit of the RGVSS method for encryption is that it generates unexpanded share-images. In 2007 Shyu [7] extended Kafri and Keren's RGVSS model, proposing three different models utilizing a (2, 2)-threshold scheme. Shyu [8] and Chen and Tsao [9] also presented (2, n)- and (n, n)-threshold RGVSS schemes, so this method is no longer limited to the (2, 2)-threshold scheme.

Both traditional VC and RGVSS produced meaningless share-images, which can create some management problems for those participating in many secret sharing projects because they have to keep track of many different share-images. Moreover, transmission of a meaningless image can arouse the suspicion of an outsider, who may realize that this image may carry some type of secret message. This attracts attention and could strengthen their desire to uncover the secret image, thus reducing the security of the share-image. Ateniese *et al*. [13] first applied the strategy of steganography to generate meaningful share-images in VC. Following Ateniese, Hou and Wu [14] proposed a method which uses the halftone and color composition/decomposition techniques to generate meaningful grey or color share-images. Zhou *et al*. [15] and Wang *et al*. [16] also improved upon Ateniese's method by developing VC algorithms for dealing with halftone images designed to make the recovered stack-image less unclear. Chang *et al*. [17] found a way to hide a color secret image in two color cover images.

Manuscript received xx; revised xx; accepted xx. This paper was partially financially supported by the National Science Council of the Republic of China under contract NSC99-2221-E-032-051.

Young-Chang Hou is with the Department of Information Management, Tamkang University, Tamsui Dist., New Taipei City 25137, Taiwan (R.O.C.) (e-mail: ychou@mail.im.tku.edu.tw).

Shih-Chieh Wei is with the Department of Information Management, Tamkang University, Tamsui Dist., New Taipei City 25137, Taiwan (R.O.C.) (Corresponding author, e-mail: seke@mail.im.tku.edu.tw).

Chia-Yin Lin is with the Department of Information Management, Tamkang University, Tamsui Dist., New Taipei City 25137, Taiwan (R.O.C.) (e-mail: bestyuka@gmail.com).

Nakajima and Yamaguchi [18] presented a scheme for encrypting a natural image. All of above methods used pixel expansion method to generate meaningful color share-images. For example, with the methods of Chang *et al*. [17] and Nakajima and Yamaguchi [18], pixel expansion made the share images nine times larger than the original image. Fang [19] proposed a progressive VC scheme which could also produce meaningful share-images, but pixel expansion meant that they were still four times larger than the original image. Thien and Lin [20] proposed a pixel non-expansion method that could produce a meaningful share-image but a computer was needed to decrypt the secret image, losing the advantage of visual cryptography which is decryption directly by the human eye.

While all of the above VC methods can produce meaningful share-images, no one method completely solves the problem of pixel expansion. A good solution would be to use a random grid method to encrypt the secret image. Chen and Tsao [10] first proposed a user-friendly random grid visual secret sharing (Friendly RGVSS) method which achieved the goal of producing meaningful share-images and pixel non-expansion, but their method still had many restrictions. In that method, pixels are taken from the secret image and the cover image to generate the needed share-images. The result is that the contrast in the stack-image and share-images is not as good as that obtained with methods that use all the pixels to display the secret image or the cover image (e.g., Ateniese *et al*.'s EVCS). In extreme situations, when an insufficient number of black pixels are taken from the secret image, it may be impossible to display the content of the secret-image in the stack-image. In addition, with this method, only one picture can be used as the cover image, and the colors of the two share-images must be complementary to each other.

Lou *et al*. [11] proposed a visual secret sharing scheme capable of hiding a secret image and an extra confidential image within two meaningful cover images. The two share-images could be stacked to obtain the secret image without any complex computation. The shifting of one of the share-images by a certain unit could allow the receiver to obtain an extra confidential image with which to check the validity of the revealed secret image. However, with this system the visual quality is poor, because of the extra image hidden in the share-images, and the cover image cannot be concealed when the share-images are stacked. All these disadvantages reduce the visual quality of the share-images and the stack-image. Lee and Chiu [12] proposed an extended visual cryptography algorithm for general access structures to create unexpanded meaningful shares to hide a secret image. It operates in two phases. In the first phase, based on a given access structure and conventional VC schemes, meaningless shares are constructed by using an optimization strategy. In the second phase, cover images are directly added to each share by a stamping algorithm to generate meaningful shares. However, the ratio of incremental pixel density of the cover image to be stamped on the shares will heavily influence the contrast in the share-images and the stack-image. Increasing the contrast of the share-image will always decrease the contrast of the stack-image, and vice versa.

In this study we propose a probability-based visual secret sharing method. Our method is an improvement upon the method of Chen and Tsao [10], allowing the contrast of the share-image and the stack-image to reach the theoretical maximum, which in turn increases the clarity of the images. The remainder of this paper is organized as follows. In the next section, a concise introduction of work related to VC and RGVSS is given. In Section 3, the probability-based visual secret sharing models with meaningful and noise-like shares is described. The experimental results are described in Section 4. Finally, a discussion of visual quality analysis, security analysis and conclusions is given in Section 5.

II. Related Work

A. Visual Cryptography

The process of visual cryptography proposed by Naor and Shamir [1] involves the encoding of a secret image into n transparencies, where each pixel is expanded m times. One transparency is distributed to each participant. The secret image cannot be seen from one transparency, but when k or more transparencies are stacked together the image will begin to emerge as the contrast between the black and white pixels becomes sufficient that the human eye will be able to recognize the secret image. Neither computational devices nor cryptographic knowledge are required for the decryption process. This approach is called (k, n)-threshold visual secret sharing.

As described in Naor and Shamir [1], a solution to the (k, n) VSS Scheme can be represented as two collections of $n\times m$ Boolean matrices, C_0 and C_1. To share a white (black) pixel, the dealer randomly chooses one row of the Boolean matrix C_0 (C_1) and dispatches it to the corresponding shadow. The chosen row defines the gray level of the m sub-pixels in each one of the n shadows. A VSS Scheme is considered valid if the following three conditions are met [1]:

1. For any S in C_0, the Boolean "OR"-ed V of any k of the n rows satisfies $H(V) \le d - \alpha\cdot m$;
2. For any S in C_1, the Boolean "OR"-ed V of any k of the n rows satisfies $H(V) \ge d$;
3. For any subset $\{i_1, i_1, \dots, i_q\}$ of $\{1, 2, \dots, n\}$ with $q < k$, the two collections of $q\times m$ matrices obtained by restricting each $n\times m$ matrix in B_0 and B_1, to rows i_1, i_1, …, i_q are indistinguishable in the sense that they contain the same matrices with the same frequencies.

The first two conditions are called *contrast* and the third condition is called *security*. Due to the security condition, we cannot obtain any information about the shared secret image if we do not have more than k shadows.

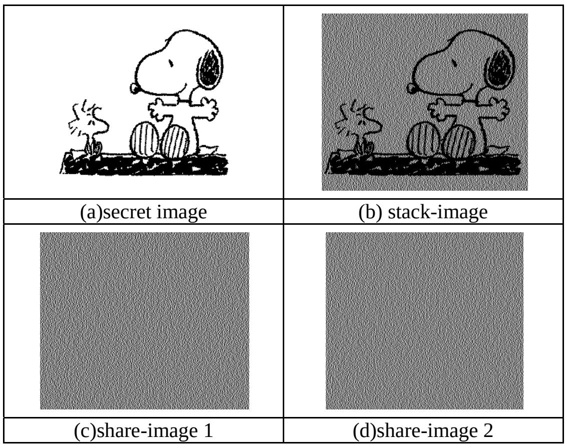
Taking the (2, 2)-threshold as an example, the distribution matrices can be designed as follows:

$$M_0 = \begin{bmatrix} 1 & 0 \\ 1 & 0 \end{bmatrix}$$
$$M_1 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \qquad (1)$$

where M_0 is used to encode the white secret pixels and M_1 is used to encode the black ones. The elements in the matrix, 0 and 1, indicate the white and black pixels, respectively. During the encryption process, the dealer chooses matrix corresponding to the color of the secret pixel. The two pixels in the first row are distributed to the first share-image and the two pixels in the second row to the second share-image. In order to ensure that each of the encoded shares appears random, the column vectors of the distribution matrix are randomly rearranged each time they are dispatched. The sharing module is shown in Table I. Since each encoded block is represented as one black and one white sub-pixel, regardless of whether the secret pixel is black or white, the share-image will not reveal any indication of the secret image. When two share-images are stacked together, the blocks corresponding to black pixels in the secret image are fully black, and those corresponding to white pixels are 50% black, producing enough contrast to reveal the secret content. Fig. 1 shows the experimental results obtained with the dispatch patterns given in Table I.

TABLE I
(2, 2)-THRESHOLD VISUAL CRYPTOGRAPHY SHARING MODULE

Secret	Share1	Share2	Stack
■	■□	□■	■■
	□■	■□	■■
□	■□	■□	■□
	□■	□■	□■



(a)secret image

(b) stack-image

(c)share-image 1

(d)share-image 2

Fig 1. Experimental results of visual cryptography.

B. Random Grids

In addition to the problem of pixel expansion encountered in traditional Visual Cryptography, designing the matrix for encryption is also a difficult task [21]. In the random-grid based visual secret sharing (RGVSS) method first proposed by Kafri and Keren [6], each pixel of the share-image is treated as a grid, and the color of the grid is randomly assigned. In the basic encryption process of RGVSS, the color of grid R_1 in the first share-image is randomly assigned. After R_1 is determined, the color of grid R_2 in the second share-image is either a complementary color or the same color depending on the color of the corresponding secret pixel. In this way, every pixel in each share-image has the same probability of becoming black or white, making it impossible to see the secret content from any single share-image. When two share-images are stacked together however, there will be 50% black pixels within the area which should look white meaning the light transmittance is 1/2 and the area which should be black is fully black (the light transmittance is 0). This creates 50% contrast between the black and white areas, which is sufficient to see the secret image in the stack-image. The RGVSS method not only avoids the pixel expansion problems, but there is no need for dispatching matrices. It is a simple and low cost technology.

Shyu [7] extended Kafri and Keren's scheme to propose three algorithms offering different light transmittance. The models are shown in Table II. In his first model, if the pixel in the secret image is white, R_1 and R_2 are the same color; if the pixel in the secret image is black, R_1 and R_2 are complementary in color (in fact, this is the same as Kafri and Keren's method). This generates 100% black in black areas and 50% black in white areas when the two share-images are stacked together. In the second model, if the pixel in the secret image is white, R_1 and R_2 are the same color; if the pixel in the secret image is black, the color of R_2 is randomly assigned. This generates 75% black in the black areas and 50% black in the white areas when the two share-images are stacked together. In the third model, if the pixel in the secret image is white, the color of R_2 is randomly assigned; if the pixel in the secret image is black, R_2 is complementary in color to R_1. This generates 100% black in the black areas and 75% black in the white area when the two share-images are stacked together.

In all three models, no matter what the color of the secret pixel is, the probability of it being black in the share-image is 1/2. This ensures the security of the secret image. The contrasts produced by the three models are 50%, 25% and 25% which are sufficient for an observer to identify the confidential information in the stack-image with the naked eye.

TABLE II
SHYU'S SHARE MODELS

Method	Secret image	Incidence	R_1	R_2	Stacking result	Light transmission
Model 1	□	1/2	□	□	□	1/2
		1/2	■	■	■	
	■	1/2	□	■	■	0
		1/2	■	□	■	
Model 2	□	1/2	□	□	□	1/2
		1/2	■	■	■	
	■	1/4	□	□	□	1/4
		1/4	□	■	■	
		1/4	■	□	■	
		1/4	■	■	■	
Model 3	□	1/4	□	□	□	1/4
		1/4	□	■	■	
		1/4	■	□	■	
		1/4	■	■	■	
	■	1/2	□	■	■	0
		1/2	■	□	■	

C. Extended Visual Cryptography

Ateniese *et al*. [13] proposed the Extended Scheme for Visual Cryptography (EVCS) which allowed for meaningful content in the cover-image to appear on the share-image.

During the encryption process, a row from a codebook (Table III) is selected according to the colors of the secret-image and two cover images, followed by random permutation of the sub-pixels in each block synchronously. The resultant codes are then assigned to share-image 1 and share-image 2. Incidentally, this will expand each pixel of the secret image into a 2×2-pixel block.

TABLE III
ATENIESE'S CODEBOOK

Secret	Cover1	Cover2	Code for Share1	Code for Share2	Stacking result
□	□	□	■□ □■	■□ ■□	■□ ■■ 75% black
	□	■	■□ □■	■□ ■■	
	■	□	■□ ■■	■□ ■□	
	■	■	■□ ■■	■□ ■■	
■	□	□	■□ □■	□■ ■□	■ 100% black
	□	■	■□ □■	□■ ■■	
	■	■	■□ ■■	□■ ■□	
	■	■	■□ ■■	□■ ■■	

In Ateniese *et al.*'s codebook, regardless of whether the secret image pixel is white or black, in each share-image, a block with two black and two white pixels is represented as a white pixel in the cover-image, and a block with three black and one white pixel is represented as a black pixel. Thus the share-image will not reveal any information about secret image, and the 25% contrast is enough to ensure that we can see the profile of the cover-image. When two share-images are stacked, a block corresponding to a white area in the secret image will have three black and one white pixels within it, and a block corresponding to a black area in the secret image will be fully black. This also creates 25% contrast between the white and black areas, enough to see the content of the secret image with the naked eye.

D. User-friendly Random Grid Visual Secret Sharing

Chen and Tsao [10] proposed a RGVSS scheme which could produce meaningful share-images. Chen and Tsao's method takes some pixels from the secret image and some pixels from the cover image to generate the needed share-images. Pixels from the secret image are encrypted by assigning the colors of share-images R_1 and R_2 according to Shyu's model (Table II). This has the desired effect, i.e., the appearance of each share-image is meaningless, but the content of the secret image will become clear when two share images are stacked together. On the other hand, for pixels coming from the cover-image, the colors in share-images R_1 and R_2 will be generated according to $F_M(.)$ using (2).

$$F_M(.):\begin{cases} prob(G^1(i,j)=0)=\rho,\ prob(G^2(i,j)=0)=\frac{T_S^W}{\rho} \\ \quad if\ \ M(i,j)=0 \\ prob(G^1(i,j)=0)=\frac{T_S^W}{\rho},\ prob(G^2(i,j)=0)=\rho \\ \quad if\ \ M(i,j)=1 \end{cases} \tag{2}$$

where M is the color of the cover-image; G^1 and G^2 represent the colors of share-image 1 and share-image 2, respectively; ρ is a predefined probability value; and ${T_S}^W$ is the average light transmission obtained in the stack-image using Shyu's model. The effects are that the black area should be darker and the white area should be lighter in share-image 1, which helps to highlight the content of the cover-image. In contrast, the black area will be lighter and the white area will be darker in share-image 2, in order to highlight the content of the cover-image in this share-image 2. However, the color will be complementary to the color of the cover-image, hence, also complementary to the color of share-image 1. After stacking, the content of the cover-image will disappear, because of the complementary color of the two share-images. This will create the effect that only the encrypted secret image will remain in the stack-image.

Chen and Tsao's method has many drawbacks. First, some pixels in the share-image are used for encrypting the secret image and others are used for showing the content of the cover-image, meaning that the contrast in both the stack-image and share-image is not as good as that obtained with those methods that use all pixels to display the secret image or the cover image (e.g., Ateniese *et al.*'s EVCS). Second, only one picture can be used for the cover image, and the colors of two share-images are complementary to each other. Although in their "Further Extension" subsection, they briefly proposed a scheme to meet the requirements when two cover images are needed. However, the scheme is totally different, not a natural extension, of the methods that are discussed in this paper. The key concept discussed in this paper can only be used for one cover image. Third, in extreme situations, when an insufficient number of black pixels are taken from the secret image, the secret-image may not be visible in the stack-image at all.

The disadvantages of Chen and Tsao's method [10] can be overcome by analyzing the probability distribution of black pixels in the share-image and the stack-image for the meaningless and the meaningful visual secret sharing method, and proposing a new RGVSS-based encryption method.

III. THE PROPOSED SCHEME

In this study, the black-appearing-probability is utilized to analyze changes in chromaticity in the share-image and the stack-image. An area with pixels assigned a higher probability of appearing black has a higher density of black pixels, making this area look darker. On the other hand, when the probability is low, the density of black pixels in this area is also low, and the area looks lighter. With these two different probabilities, we can produce light and dark contrast in the image, that is, show a black and white pattern.

A. User-friendly Visual Secret Sharing

With the user-friendly visual secret sharing method the share-images should show a cover image. There needs to have two different probabilities that a pixel will appear black in the share-image to produce the contrast between the dark and light areas in the cover image. These two different black-pixel-probabilities are called X and Y, where X represents the black-appearing-probability when the pixel in the cover-image is white and Y represents the black-appearing-probability when the pixel in the cover-image is black. It is clear that $X < Y$.

When two share-images are stacked, different probabilities of pixels appearing black in the stack-image are created given the different color combinations created by stacking the two share-images. The variations are described as follows:

1. If the pixel color in the two cover-images is black, each pixel has Y opportunity to be black. When the black pixels in the two share-images are stacked, the possibilities may vary from totally overlapping to not overlapping at all, meaning that the black-pixel-appearing-probability in those areas of the stack-image will be in the range between Y and $2Y$.
2. If the pixel color in the two cover-images is white, each pixel has X opportunity to be black. When the black pixels on the two share-images are stacked, the possible results may vary from totally overlapping to not overlapping at all, meaning that the black-pixel-appearing-probability in those areas of the stack-image will be between X and $2X$.
3. If the pixel color in one of the two cover-images is black and the other is white, when two share-images are stacked, the black-appearing-probability in those areas of the stack-image will be between Y and $X+Y$.

The black-pixel-appearing-probabilities for the white and black pixels in the stack-image are represented by Z and W, respectively. According to the above derivations, we know that the value of Z and W under different combinations of colors in the cover-image will be between X and $2Y$. However, black (white) may be achieved in the stack-image by stacking two black pixels, one black pixel and one pixel, or two white pixels from two share-images. It is hoped that the chromaticity within either the dark areas or the light areas will be uniform, to avoid the impression of inconsistent shading in the stack-image. Consequently, the ideal probabilities of Z and W should be within the range from Y to $2X$, which is the range that any color combination of the cover images can be achieved by stacking. If Z and W are set to values outside the range between Y and $2X$, black (white) pixels cannot be obtained in the stack-image by stacking two white (black) pixels in the share-images. It is clear that $Z < W$.

The relationship of black-pixel-appearing-probabilities in share-images X and Y, and the probabilities in stack-images Z and W can be expressed as in Fig. 2.

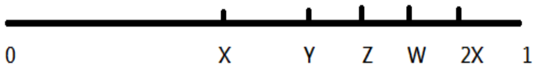


Fig 2. Relationship between X, Y, Z and W in the user-friendly visual secret sharing scheme.

In Fig. 2, X, Y, Z and W represent black-pixel-appearing-probabilities with values between 0 and 1. Furthermore, $Y > X$, and $W > Z$, where Z and W can have any value between Y and $2X$. The maximum contrast in the stack-image will happen in the situation when $Z = Y$ and $W = 2X$. The maximum probability value is 1, from which we can deduce that the relationship between X, Y, Z and W is $0 < X < Y \leq Z < W \leq 2X \leq 1$. When $Y = Z$, the contrast in the share-image and stack-image will influence each other. The greater the contrast $Y - X$ in the share-image is, the smaller the contrast $2X - Y$ in the stack-image will be. In contrast, the smaller the contrast $Y - X$ in the share-image is, the greater the contrast $2X - Y$ in the stack-image will be. If we want to maximize the contrasts in the share-image and the stack-image simultaneously, the contrasts on both image should be equal to each other, $Y - X = 2X - Y$, where Y must be equal to $1.5X$.

Generally, it is hoped that the contrast in both the share-image and the stack-image can be kept as great as possible, so the following probability values will be assigned: $Y = 1.5X$, $Z = Y$ and $W = 2X$. When X is smaller than 0.5, the contrast in the share-image and stack-image increases with X, but when X is greater than 0.5, since $W = \min(2X, 1)$, the contrast in the stack-image becomes $W - Z = 1 - 1.5X$, and the contrast in the stack-image will decrease with increasing X. Therefore, the best visual effect is obtained when $X = 0.5$, so that both share-image and stack-image have the same maximum contrast at the same time.

B. User-friendly Visual Secret Sharing Scheme

The meaningful visual secret sharing codebook shown in Table IV is designed through the above analysis. The color of the secret image can be produced by the stacking of different colors from the two cover-images. There are eight possible combinations.

As in RGVSS, we first assign the pixel color in the first share-image (S1), and then assign the color in the second share-image as in Table IV. Regardless of the color of the secret image, whenever the corresponding pixel in cover-image1 is black, each pixel in S1 should have Y percentage of appearing black; on the other hand, when the pixel in the cover-image1 is white, it has X percentage of appearing black in S1. To find the probability of appearing black in the second share-image (S2) one needs to consider the corresponding pixel color in the secret image and S1. Let us look at the second combination (■, ■, □) in Table IV as an example to explain how to set the black appearing probability of each share-image.

In the (■, ■, □)combination, the following probability conditions should be met: there is W percentage of black pixels appearing in the stack-image, and Y and X percentage in share-image 1 and share-image 2, respectively.

TABLE IV
USER-FRIENDLY VISUAL SECRET SHARING CODEBOOK

Secret image	Cover1	Cover2	Share1	Share2	Stack image (stacking result)	Secret image	Cover1	Cover2	Share1	Share2	Stack image (stacking result)
■ Black	■ Black	■ Black	■ (*Y probability of being black*)	■ (*$\frac{2Y-W}{Y}$probability of being black*)	■ *Y percent of pixels are stacked into black*	□ White	■ Black	■ Black	■ (*Y probability of being black*)	■ (*$\frac{2Y-Z}{Y}$ probability of being black*)	■ *Y percent of pixels are stacked into black*
			□ (1 −*Y probability of being white*)	■ (*$\frac{W-Y}{1-Y}$probability of being black*)	■ *W – Y percent of pixels are stacked into black*				□ (1 −*Y probability of being white*)	■ (*$\frac{Z-Y}{1-Y}$ probability of being black*)	■ *Z −Y percent of pixels are stacked into black*
			There are *Y* percent of black pixels on share1	There are *Y* percent of black pixels on share2	There are *W* percent of black pixels on the stack-image				There are *Y* percent of black pixels on share1	There are *Y* percent of black pixels on share2	There are *Z* percent of black pixels on the stack-image
	■ Black	□ White	(a1) ■ (*Y probability of being black*)	(a2) ■ (*$\frac{X+Y-W}{Y}$ probability of being black*)	(a3) ■ *Y percent of pixels are stacked into black*		■ Black	□ White	■ (*Y probability of being black*)	■ (*$\frac{X+Y-Z}{Y}$ probability of being black*)	■ *Y percent of pixels are stacked into black*
			(a4) □ (1 −*Y probability of being white*)	(a5) ■ (*$\frac{W-Y}{1-Y}$ probability of being black*)	(a6) ■ *W – Y percent of pixels are stacked into black*				□ (1 −*Y probability of being white*)	■ (*$\frac{Z-Y}{1-Y}$ probabilityof being black*)	■ *Z −Y percent of pixels are stacked into black*
			(a7) There are *Y* percent of black pixels on share1	(a8) There are *X* percent of black pixels on share2	(a9) There are *W* percent of black pixels on the stack-image				There are *Y* percent of black pixels on share1	There are *X* percent of black pixels on share2	There are *Z* percent of black pixels on the stack-image
	□ White	■ Black	■ (*X probability of being black*)	■ (*$\frac{X+Y-W}{X}$probability of being black*)	■ *X percent of pixels are stacked into black*		□ White	■ Black	■ (*X probability of being black*)	■ (*$\frac{X+Y-Z}{X}$ probability of being black*)	■ *X percent of pixels are stacked into black*
			□ (1 −*X probability of being white*)	■ (*$\frac{W-X}{1-X}$ probability of being black*)	■ *W −X percent of pixels are stacked into black*				□ (1 −*X probability of being white*)	■ (*$\frac{Z-X}{1-X}$ probability of being black*)	■ *Z −X percent of pixels are stacked into black*
			There are *X* percent of black pixels on share1	There are *Y* percent of black pixels on share2	There are *W* percent of black pixels on the stack-image				There are *X* percent of black pixels on share1	There are *Y* percent of black pixels on share2	There are *Z* percent of black pixels on the stack-image
	□ White	□ White	■ (*X probability of being black*)	■ (*$\frac{2X-W}{X}$ probability of being black*)	■ *X percent of pixels are stacked into black*		□ White	□ White	■ (*X probability of being black*)	■ (*$\frac{2X-Z}{X}$ probability of being black*)	■ *X percent of pixels are stacked into black*
			□ (1 −*X probability of being white*)	■ (*$\frac{W-X}{1-X}$ probability of being black*)	■ *W−X percent of pixels are stacked into black*				□ (1 −*X probability of being white*)	■ (*$\frac{Z-X}{1-X}$ probability of being black*)	■ *Z −X percent of pixels are stacked into black*
			There are *X* percent of black pixels on share1	There are *X* percent of black pixels on share2	There are *W* percent of black pixels on the stack-image				There are *X* percent of black pixels on share1	There are *X* percent of black pixels on share2	There are *Z* percent of black pixels on the stack-image

As in RGVSS, black pixels are randomly assigned to S1. In S1, pixels have *Y* percentage of being assigned as black (a1 in Table IV), and 1 – *Y* percentage of being assigned to be white (a4 in Table IV). Thus, S1 should look darker, because it has *Y* percentage chance of being black (a7 in Table IV). Since S1 is black, the result on the stack-image must be black, regardless of whether the corresponding S2 pixel is black or white. This generates *Y* percent of black pixels in the stack-image (a3 = a1 in Table IV). Because the color of the secret pixel is black, we need the *W* ratio of black pixels to be represented on the stack-image (a9 in Table IV). This means that when S1 is white, it should generate a (*W* – *Y*) ratio of black pixels on the stack-image (a6 = a9 – a3 in Table IV). Therefore, when S1 is white, the corresponding pixels have a $(W - Y) / (1 - Y)$ percent likelihood of being black on S2 (a5 = a6 / a4 in Table IV). This means that it can generate $(W - Y)$ percent of black pixels on the stack-image produced by stacking two share-images (a6 = a4 × a5 in Table IV). Thus, there are W percent of black pixels (a9 = a3 + a6 in Table IV) in the stack-image, making this area look darker.

Since cover-image2 is white with this combination (■, ■, □), one needs to generate X percent of black pixels in S2 (a8 in Table IV). According to the derivation discussed above, the probability assigned for pixels to be black in S2 is $(W - Y) / (1 - Y)$ when the pixels are white in S1 (a5 in Table IV). So there is a $(X + Y - W) / Y$ probability for pixels in S2 to be black when S1 is black (a2= (a8 – a4 × a5) / a1) in Table IV). In this way, X percent of these S2 pixels appear black (a8 = a1 × a2 + a4 × a5 in Table IV), making this area look lighter and representing the white area in the share-image 2.

Through the above discussion, it can be seen that share-image 1 has Y percent black pixels (a7), share-image 2 has X percent black pixels (a8), and the stack-image has W percent black pixels (a9), meaning the images display the combination (■, ■, □) in the corresponding area. The rest of the combinations in Table IV are similar to the example above, so there is no need to discuss them one by one. The interested reader may trace them by himself.

The proposed probability-based user-friendly visual secret sharing algorithm is illustrated below.

```
The user-friendly visual secret sharing algorithm:
INPUT: An L×H secret image P, two L×H cover-images C1 and C2, and
    probability parameters X, Y, Z and W, where 0 < X < Y ≤ Z < W ≤
    2X ≤ 1.
OUTPUT: Two L×H share-images S1 andS2.
Step 1.Read the pixel color of P(i, j), C1(i, j) and C2(i, j) sequentially, to
    judge what the combination is.
Step 2. Based on the combination, assign S1 and S2 an appropriate
    black-appearing-probability according to the design described in
    Table IV.
Step 3. Repeat steps 1 and 2 until all the pixels of P are encrypted.
```

Our algorithm is secure, because, whether the color on the secret image is white or black, the pixels on the share-image will have X percent chance of appearing black in the area corresponding to white in the cover-image; likewise, the pixels on the share-image will have Y percent chance of appearing black in the area corresponding to black in the cover-image. Thus, no clues about the secret image are exposed in the share-image, and the pattern of the cover-image that emerges on that share-image has a contrast of $(Y - X)$. The area in the stack-image corresponding to white in the secret image has Z percent black pixels in the stacked image, while the area corresponding to black in the secret image can be stacked to have W percent black pixels. Therefore the contrast in the stack-image is $(W - Z)$, enough to reveal the secret pattern. The color in the stack-image is only related to the color of the secret image, not the cover-image, so the pattern of the secret image shows no outline of the cover-image.

C. Meaningless Share-Image Visual Secret Sharing

The focal point of the meaningless share-image visual secret sharing method is that there should be obvious contrast between black and white areas in the stack-image indicative of the pattern of the secret image, but such contrast should not be visible in the share-image, which should present a noise-like image. This is accomplished by having the same probability of each pixel in the share-image being black, regardless of whether the corresponding color of the cover image is black or white. In this case, there is only one kind of black-pixel-probability X in the share-image, and Fig. 2 is modified to become Fig. 3.

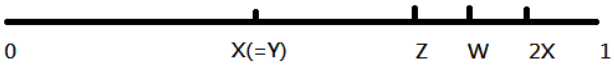


Fig. 3. Probability distribution line graph for meaningless visual secret sharing.

In Fig. 3, Z and W can have any probability value between X and $2X$. When the value of Z approaches closer to X and the value of W is closer to $2X$, the difference between Z and W grows, and the black and white contrast in the stack-image will become larger. When $Z = X$ and $W = 2X$, the stack-image has maximum contrast. That is to say, the maximum contrast reached in the stack-image is $(W - Z) = (2X - X) = X$, where X is the probability of each pixel on the share-image being black.

The maximum value of the probability is 1, therefore, the maximum value of W can be written as W=min($2X$, 1). When $X \leq 0.5$, the larger the value of X, the more obvious the black and white contrast, which is equal to $2X - X$, in the stack-image will be. When $X = 0.5$, the best contrast obtainable in the stack-image would be 50% (= 1 – 0.5). However, when $X > 0.5$, the contrast in the stack-image will become $(1 - X)$, so that a larger X causes a greater decrease in the contrast in the stack-image.

In the condition $X = Y$, the user-friendly visual secret sharing codebook (Table IV) can be reduced to the meaningless visual secret sharing codebook (Table V). Both share-image 1 and share-image 2 will have X percentage of black pixels, regardless of whether the corresponding area on the secret image is black or white. This can produce share-images with a noise-like appearance showing no clues about the secret image. When these two share-images are stacked, the pixels in areas corresponding to the black areas in the secret image will have W percent chance of being black, and the pixels in areas corresponding to white in the secret image will have Z percent chance of being black. This creates contrast between the black and white areas in the stack-image, so the secret pattern can be clearly seen.

TABLE V
MEANINGLESS VISUAL SECRET SHARING CODEBOOK

Secret image	Share1	Share2	Stack-image (stacked result)
■	■ (*X probability of being black*)	■ ($\frac{2X-W}{X}$*probability of being black*)	■ *X percent of pixels are stacked into black*
	□ (1– *X probability of being black*)	■ ($\frac{W-X}{1-X}$*probability of being black*)	■ *W – X percent of pixels are stacked into black*
	There are *X* percent of black pixels on share1	There are *X* percent of black pixels on share2	There are *W* ratio of black pixels on the stack-image
□	■ (*X probability of being black*)	■ ($\frac{2X-Z}{X}$ *probability of being black*)	■ *X percent of pixels are stacked into black*
	□ (1– *X probability of being black*)	■ ($\frac{Z-X}{1-X}$ *probability of being black*)	■ *Z –X percent of pixels are stacked into black*
	There are *X* percent of black pixels on share1	There are *X* percent of black pixels on share2	There are *Z* ratio black pixels on the stack-image

The algorithm for the proposed meaningless visual secret sharing scheme is illustrated below.

```
The meaningless visual secret sharing scheme
INPUT: An $L×H$ secret image P, and parameters $X$, $Z$ and $W$, where $0 < X \le Z < W \le 2X \le 1$.
OUTPUT: Two $L×H$ share-images S1and S2.
1   Assign S1($i, j$) to be black pixel with $X$ probability.
2   Assign the black appearing probability for S2($i, j$) under the
    consideration of the colors of P($i, j$) andS1($i, j$).
2.1 IF P($i, j$) = black
        IF S1($i, j$) = black, assign S2($i, j$) to be black pixel with $\frac{2X-W}{X}$ probability;
        IF S1($i, j$) = white, assignS2($i, j$) to be black pixel with $\frac{W-X}{1-X}$ probability.
2.2 IF P($i, j$) = white
        IF S1($i, j$) = black, assign S2($i, j$) to be black pixel with $\frac{2X-Z}{X}$ probability;
        IF S1($i, j$) = white, assign S2($i, j$) to be black pixel with $\frac{Z-X}{1-X}$ probability.
3   Repeat steps 1 and 2 until all pixels of P are encrypted.
```

The experiments demonstrating the proposed random-grid-based user-friendly and meaningless visual secret sharing schemes based on above analysis are discussed below.

IV. EXPERIMENTAL RESULTS

The experiments were performed on a personal computer equipped with an Intel Core(tm) i5-2410 2.30GHz CPU, with 4GB memory using the Windows 7 platform. The development language was JAVA. Experimental images in Figs. 4 (a-f) show six 256×256 black-and-white images, and Figs. 4 (g-i) three 2048×2048 color images.

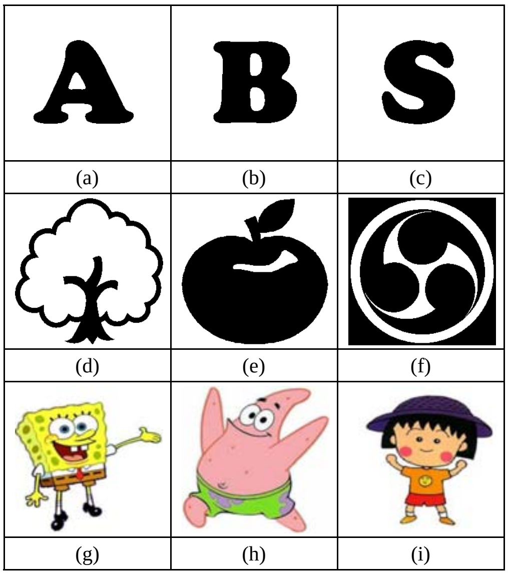
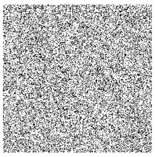
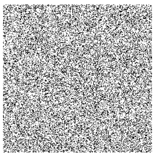
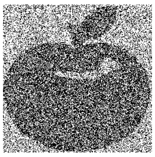


Fig. 4. Experimental images.

A. Experiment 1: The Meaningless Share-Image

In this experiment, we try to find the different visual effects obtained by assigning different black-pixel-appearing-probabilities *X*. In order to make the contrast in the stack-image more obvious, we set parameter *Z* equal to *X* and parameter *W* equal to 2*X*. From Fig. 5 it can be seen that the greater *X* we give, the deeper the color on the share-images, but no matter what the value of *X*, we can find no clues about the secret image on the share-images. When *X* < 0.5, the stack-image will display *X* contrast from which we can identify the secret image pattern; therefore the greater *X* we assign, the greater the contrast the stack-image is, and the more obvious the content in the stack-image becomes (Figs. 5 (a-b)). When *X* = 0.5, the dark areas in the stack-image will be 100% black and the light areas will be 50% black, giving 50% contrast between the black and white area, which is the best visual effect (Fig. 5 (b)). This result is consistent with that obtained by Ito *et al.'s* method [2] and Shyu's model 1 [7] (Table II). When *X* > 0.5, the dark areas in the stack-image will be at most 100% black, but the light areas will be more than 50% black, so the contrast becomes (1 – *X*), In other words, the contrast gets lower with increasing *X* (Fig. 5 (c)).

	Share1	Share2	Stack-image
(a) $X = 0.3$ $Z = 0.3$ $W= 0.6$			
Contrast	0%	0%	30%

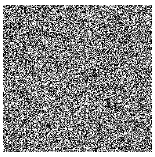
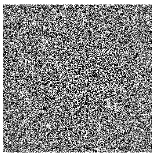
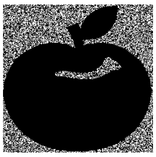
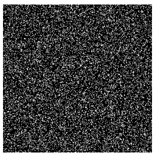
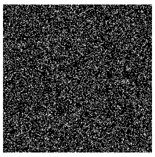
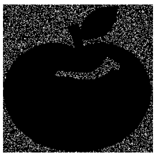
(b) X = 0.5 Z = 0.5 W = 1.0			
Contrast	0%	0%	50%
(c) X = 0.8 Z = 0.8 W = 1.0			
Contrast	0%	0%	20%

Fig. 5. Visual effect comparison for meaningless visual secret sharing.

B. Experiment 2: The User-friendly Share-Image

1) Testing the visual effectiveness with different values of X

Fig. 6 shows the results of experiment 2, in which different visual effects are obtained with different values of X. Comparison is made in the condition that both share-image and stack-image are given equal contrast. When X = 0.5, black areas in the share-image are 75% black and white areas are 50% black, so there is 25% contrast between them. When the black areas in the stack-image are 100% black and the white areas are 75% black, the contrast is also 25% (Fig. 6 (b)). Through the comparison, we can clearly observe that when X = 0.5, 25% contrast is the best result, given the condition that both the share-image and the stack-image have equal clarity. This is identical to the results obtained with Ateniese *et al.*'s method [13], but our method has the advantage of avoiding the 4 time pixel expansion.

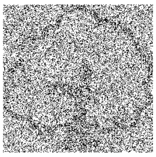
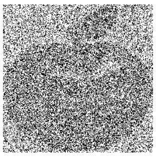
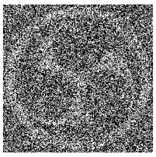
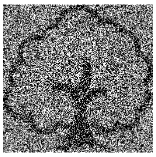
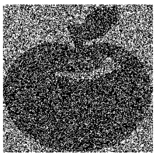
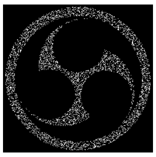
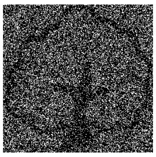
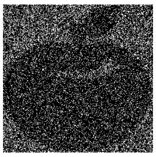
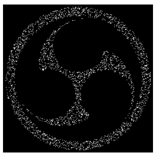
	Share1	Share2	Stack-image
(a) X = 0.3 Y = 0.45 Z = 0.45 W = 0.6			
Contrast	15%	15%	15%
(b) X = 0.5 Y = 0.75 Z = 0.75 W = 1.0			
Contrast	25%	25%	25%
(c) X = 0.7 Y = 0.85 Z = 0.85 W = 1.0			
Contrast	15%	15%	15%

Fig. 6. Comparison of visual effectiveness of user-friend visual secret sharing with different values of X.

2) Different Y, Z and W values are assigned to test the influence on contrast between the share-image and the stack-image.

When Y = Z, the contrast in the share-image and the stack-image will affect each other. When the contrast in the share-image is high, the contrast in the stack-image is low, and vice versa. Look for example at Fig. 7 (b). If we wish the contrast in the stack-image to be higher than 25%, we must sacrifice contrast in the share-image. Conversely, if we let the contrast in the share-image be more than 25%, the contrast of the stack–image must be less than 25%, as shown as Fig. 7 (c). The experimental results are shown in Fig. 7. The best contrast for both images is 25%, given the condition that the share-image and the stack-image have equal contrast (Fig. 7(a)).

Even when the contrast is low, it is still easier to identify the image pattern if the dark areas in the image can be restored to 100% black [22]. Thus, although the contrast in the stack-image (Fig. 7(c)) is small, the dark areas are 100% black. The visual effect is close to stack-images which have large contrast (Figs. 7 (a-b)). In the contrast, although there is greater contrast in the stack-image shown in Fig. 7(d) than the one shown in Fig. 7(c), because the black areas are not 100% black, the visual quality of the stack-image is worse than with stack-images which have poor contrast but where the dark areas that are 100% black (Figs. 7 (a-c)).

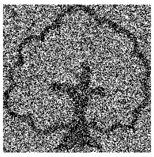
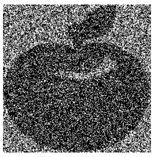
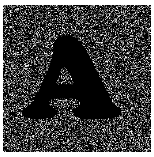
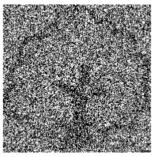
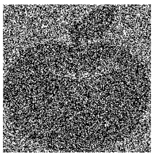
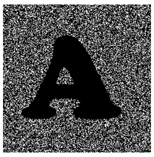
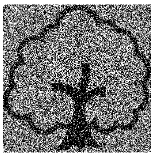
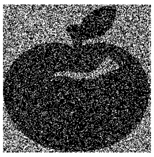
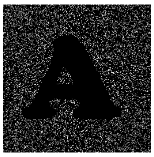
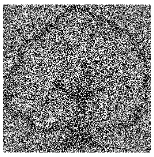
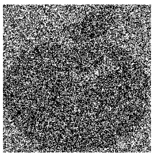
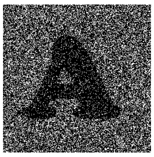
	Share1	Share2	Stack-image
(a) X = 0.5 Y = 0.75 Z = 0.75 W = 1.0			
Contrast	25%	25%	25%
(b) X = 0.5 Y = 0.65 Z = 0.65 W = 1.0			
Contrast	15%	15%	35%
(c) X = 0.5 Y = 0.85 Z = 0.85 W = 1.0			
Contrast	35%	35%	15%
(d) X = 0.5 Y = 0.65 Z = 0.65 W = 0.9			
Contrast	15%	15%	25%

Fig. 7. Fixed X, comparison of the contrast between the share-image and the stack-image with different values of Y, Z and W.

C. Experiment 3: Comparison of our method with Chen and Tsao's[10]

In experiment 3, we use the same contrast (formula (3) as that defined by Shyu [7]) and then compare the visual quality obtained with these two different kinds of encryption algorithms. A higher δ value means that the image contrast is more obvious. Chen and Tsao used a share-image composed of α proportion of secret image pixels and $(1-\alpha)$ proportion of cover-image pixels. Chen and Tsao [10] modified (3) to obtain (4).

$$\delta = \frac{T(B[S(0)])-T(B[S(1)])}{1+T(B[S(1)])} \qquad (3)$$

$$= \frac{T(B[\alpha\times P(0)+(1-\alpha)\times O(0)])-T(B[\alpha\times P(1)+(1-\alpha)\times O(1)])}{1+T(B[\alpha\times P(1)+(1-\alpha)\times O(1)])}, \qquad (4)$$

where $T(B[S(0)])$: the average light transmission in the white areas; $T(B[S(1)])$: the average light transmission in the black area; $T(B[\alpha\times P(0) + (1-\alpha)\times O(0)])$: the average light transmission in white areas that come from the secret image (α proportion) and the cover-image ($(1-\alpha)$ proportion); $T(B[\alpha\times P(1) + (1-\alpha)\times O(1)])$: the average light transmission in black areas that come from the secret image (α proportion) and the cover-image ($(1-\alpha)$ proportion).

The experimental results obtained using Chen and Tsao's algorithm are shown in Figs. 8 (a-c), using model 1 from Table II and $\rho = 1$, as suggested by Chen and Tsao. The pattern in the stack-image is very unclear (δ = 0.07) when encryption is performed with a smaller proportion of secret image pixels (α = 0.2). Conversely, when encryption is performed with a larger proportion of secret image pixels (α = 0.8), the pattern on the share-image is fuzzy (δ = 0.07). Even with the best conditions proposed by Chen and Tsao (α = 0.5), the visual effectiveness of their share-image and stack-image are far worse than the ones obtained with our method (Figs. 8(c-d)). The main reason is that in their scheme, the black areas in the stack-image are not reconstructed as 100% black, reducing the visual effect [22]. Moreover, they can only use a single image as the cover-image, and the two share-images produced have to be complementary in color. Our method has the additional advantage that we can use two different cover-images (please refer to Figs. 8 (e) and 9(c)). The experimental color image is shown in Fig. 9.

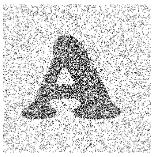
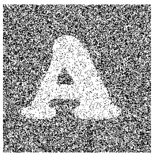
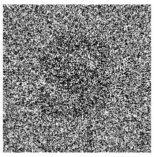
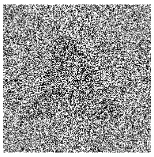
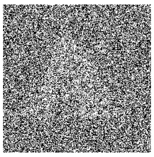
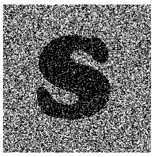
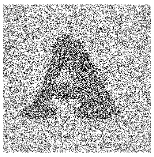
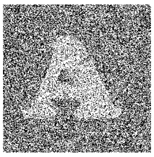
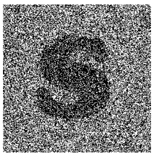
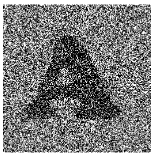
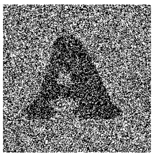
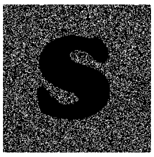
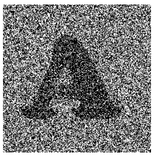
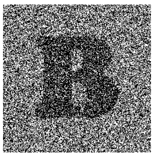
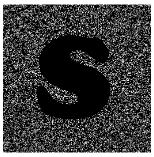
		Share1	Share2	Stack-image
Chen & Tsao [10] (Model 1 ρ = 1)	(a) α = 20%			
		δ = 0.27	δ = 0.27	δ = 0.07
	(b) α = 80%			
		δ = 0.07	δ = 0.07	δ = 0.36
	(c) α = 50%			
		δ = 0.17	δ = 0.17	δ = 0.2
Our study X = 0.5 Y = 0.75 Z = 0.75 W = 1.0	(d) One cover-image			
		δ = 0.2	δ = 0.2	δ = 0.25
	(e) Two cover-images			
		δ = 0.2	δ = 0.2	δ = 0.25

Fig. 8. Comparison of the black and white images from our method and Chen and Tsao's.

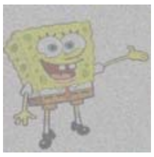
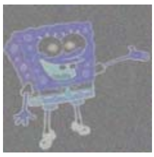
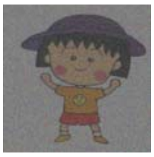
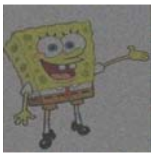
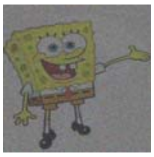
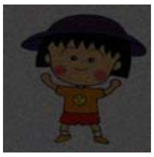
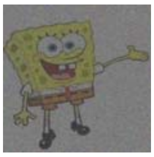
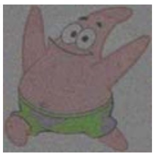
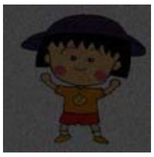
Best effect parameter		Share1	Share2	Stack-image
Chen & Tsao [10] (Model 1 ρ = 1)	(a) α = 50%			
		δ = 0.17	δ = 0.17	δ = 0.2
Our study X = 0.5 Y = 0.75 Z = 0.75 W = 1.0	(b) One cover-image			
		δ = 0.2	δ = 0.2	δ = 0.25
	(c) Two cover-images			
		δ = 0.2	δ = 0.2	δ = 0.25

Fig. 9. Comparison of the color image from our method and Chen and Tsao's.

V. Discussion and Conclusion

A. The advantages of our method

The advantages of our user-friendly secret sharing method are as follows:

1) Improved contrast in the share-image and the stack-image

Since all pixels of the secret image and the cover-image are used for encryption; therefore, the image produced with our algorithm is better than the image produced by a method which only takes part of the pixels from the secret image and part from the cover-image. When X = 0.5, Y = Z = 1.5X, W = 2X, the share-image and stack-image have the same level of clarity, reaching the best theoretical contrast (δ = 0.25).

2) *Reduction of restrictions for the encryption process*

With our algorithm, two cover-images can be used in the encryption process, and the colors of these two share-images need not be complementary to each other. Even if only a single cover image is used, the share-images look more natural. Moreover, with our encryption codebook, it is easier to change the probability of pixels appearing black on both the share-image and stack-image, which makes our method more flexible to use.

B. *Visual quality analysis*

We use the contrast (δ) as the benchmark for assessment of visual quality. When both the share-image and the stack-image need to have the same level of clarity, the ratio between the four parameters is $X : Y : Z : W = 1 : 1.5 : 1.5 : 2$, and $0 < X \leq 0.5$. According to above parameter settings, the formula for the contrast (δ) in the share-image can be rewritten as (5), and for the stack-image as (6).

$$\text{Share-image } \delta = \frac{T(B[S(0)])-T(B[S(1)])}{1+T(B[S(1)])} = \frac{(1-X)-(1-Y)}{1+(1-Y)} = \frac{(1-X)-(1-1.5X)}{1+(1-1.5X)} = \frac{0.5X}{2-1.5X} \tag{5}$$

$$\text{Stack-image } \delta = \frac{T(B[S(0)])-T(B[S(1)])}{1+T(B[S(1)])} = \frac{(1-Z)-(1-W)}{1+(1-W)} = \frac{(1-1.5X)-(1-2X)}{1+(1-2X)} = \frac{0.5X}{2-2X} \tag{6}$$

According to the definition of contrast, when δ is not equal to zero, we have the chance to identify the pattern in the image. The range of X is $0 < X \leq 0.5$, so no matter what the value of X is in (5) and (6), the contrast will be greater than zero. Hence, meaningful patterns can appear in both the share-image and the stack-image produced using our algorithm. In addition, the value of contrast δ will increase with an increasing X value, making the image quality better. Furthermore, the different light transmissions from the stack-image, Z and W, are allocated according to the color of the secret image, which has nothing to do with the cover-image. As a consequence, the secret image can be seen in the stack-image without any blurring from the cover-image.

Chen and Tsao used three kinds of models (Shyu [7]) for secret image encryption. Their contrast formulas for the share-image and the stack-image are collated in Table VI. According to their suggestion the parameters, α = 50% and ρ = 1, can produce the best effect [10]. We obtain the best experimental results using the following parameters: $X = 0.5$, $Y = Z = 1.5X = 0.75$, $W = 2X = 1.0$, in (5) and (6). An examination of Table VI shows that our δ values are better than those achieved by Chen and Tsao in any of their three models. In short, our method offers better images contrast and visual quality than Chen and Tsao's.

TABLE VI
COMPARISON OF AVERAGE LIGHT TRANSMISSION BETWEEN OUR SCHEME AND CHEN AND TSAO'S

	Chen and Tsao [10]			Our study
	Model 1	Model 2	Model 3	
Parameters	α= 50%, ρ= 1			$X = 0.5$, $Y = 0.75$, $Z = 0.75$, $W = 1.0$
δ of share1 and share2	$\frac{(1-\alpha)(\rho-\frac{1}{2\rho})}{1+\frac{1}{2}\alpha+\frac{(1-\alpha)}{2\rho}} = \frac{1}{6}$	$\frac{(1-\alpha)(\rho-\frac{1}{2\rho})}{1+\frac{1}{2}\alpha+\frac{(1-\alpha)}{2\rho}} = \frac{1}{6}$	$\frac{(1-\alpha)(\rho-\frac{1}{4\rho})}{1+\frac{1}{2}\alpha+\frac{(1-\alpha)}{4\rho}} = \frac{1}{11}$	$\frac{(1-X)-(1-Y)}{1+(1-Y)} = \frac{1}{5}$
δ of stack-image	$\frac{\alpha}{3-\alpha} = \frac{1}{5}$	$\frac{a}{6-\alpha} = \frac{1}{11}$	$\frac{a}{5-\alpha} = \frac{1}{9}$	$\frac{(1-Z)-(1-W)}{1+(1-W)} = \frac{1}{4}$

C. *Security analysis*

As can be seen from Table IV, with our user-friendly visual secret sharing method, regardless of whether the color of the secret pixel is black or white, as long as the color of the cover-image is black, we will have a Y percentage chance of producing black pixels at the corresponding position on the share-image. When the color of the cover-image is white, there is X percentage chance of the pixel being black. Similarly, referring to Table V, with our meaningless visual secret sharing method, the share-image will produce X percent of black pixels on the share-image, regardless of whether the secret pixels in the corresponding position are black or white. Therefore no information about the secret image will be leaked in the share-images produced using our method, which satisfies the security requirements for visual cryptography.

Condition 3 mentioned in Section II.A and the probabilistic nature of the random grids guarantee that no information from the secret image is revealed from any collection of less than q shares. If an adversary was able to obtain one $L \times H$ share-image, since each pixel on the second share-image may be black or white, the probability of guessing the pixel color correctly would be 2^{-1}. Therefore, the probability of guessing the right pixel configuration for another share-image would be $2^{-(L \times H)}$, which is very close to 0 when L and H are large. This makes it very difficult for the adversary to uncover the secret image from only one share-image. Although our method cannot achieve information-theoretic security or unconditional security, it still satisfies the requirement of computational security, assuming that any adversaries are computationally limited, as all adversaries are in practice.

D. *Conclusion*

Our user-friendly visual secret sharing scheme, not only maintains the security and pixel non-expanding benefits of the random-grid method, but also allows for the production of meaningful share-images, while satisfying the requirements of being easy to carry and easy to manage. Moreover, all pixels in the cover-image and the secret image are used to perform encryption, which ensures that the contrast on the share-images and the stack-image can reach the theoretical maximum. Our method also removes some unnecessary encryption restrictions (e.g., having to use only one cover-image, having to take enough black pixels from the secret image) which makes the encryption process more flexible. The findings show that our user-friendly visual secret sharing is better than the method proposed by Chen and Tsao [10].

References

[1] M. Naor and A. Shamir, "Visual cryptography," in *Advances in Cryptology-EUROCRYPT '94*, LNCS 950, Springer-Verlag, pp. 1-12, 1995.

[2] R. Ito, H. Kuwakado, and H. Tanaka, "Image size invariant visual cryptography," *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, vol. E82-A, no. 10, pp. 2172-2177, 1999.

[3] T. L. Lin, S. J. Horng, K. H. Lee, P. L. Chiu, T. W. Kao, Y. H. Chen, R. S. Run, J. L. Lai, and R. J. Chen, "A novel visual secret sharing scheme for multiple secrets without pixel expansion," *Expert Systems with Applications*, vol. 37, no. 12, pp. 7858-7869, 2010.

[4] S. F. Tu and Y. C. Hou, "Design of visual cryptographic methods with smooth-looking decoded images of invariant size for gray level images," *Imaging Science Journal*, vol. 55, no. 2, pp. 90–101, 2007.

[5] C. N. Yang, "New visual secret sharing schemes using probabilistic method," *Pattern Recognition Letters*, vol. 25, no. 4, pp. 481-494, 2004.

[6] O. Kafri and E. Keren, "Encryption of pictures and shapes by random grids," *Optics Letters*, vol. 12, no. 6, pp. 377-379, June 1987.

[7] S. J. Shyu, "Image encryption by random grids," *Pattern Recognition*, vol. 40, no. 3, pp. 1014-1031, 2007.

[8] S. J. Shyu, "Image encryption by multiple random grids," *Pattern Recognition*, vol. 42, no. 7, pp. 1582–1596, 2009.

[9] T. H. Chen and K. H. Tsao, "Visual secret sharing by random grids revisited," *Pattern Recognition*, vol. 42, no. 9, pp. 2203-2217, 2009.

[10] T. H. Chen and K. H. Tsao, "User-friendly random-grid-based visual secret sharing," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 21, no. 11, pp. 1693-1703, 2011.

[11] D. C. Lou, H. H. Chen, H. C. Wu, and C. S. Tsai, "A novel authenticatable color visual secret sharing scheme using non-expanded meaningful shares," *Displays*, vol. 32, no. 3, pp. 118-134, 2011.

[12] K. H. Lee and P. L. Chiu, "An extended visual cryptography algorithm for general access structures," *IEEE Transactions on Information Forensics and Security*, vol. 7, no. 1 part 2, pp. 219-229, 2012.

[13] G. Ateniese, C. Blundo, A. De Santis, and D. R. Stinson, "Extended schemes for visual cryptography," *Theoretical Computer Science*, vol. 250, pp. 143-161, 2001.

[14] Y. C. Hou and J. H. Wu, "An extended visual cryptography scheme for concealing color images," *in Proceeding of The 5th Conference on Information Management and Police Administrative Practice*, Taoyuan, Taiwan, pp. 62-69, (in Chinese) 2001.

[15] Z. Zhou, G. R. Arce, and G. D. Crescenzo, "Halftone visual cryptography," *IEEE Transactions on Image Processing*, vol. 15, no. 8, pp. 2441-2453, 2006.

[16] Z. Wang, G. R. Arce, and G. D. Crescenzo, "Halftone visual cryptography via error diffusion," *IEEE Transactions on Information Forensics and Security*, vol. 4, no. 3, pp. 383–396, 2009.

[17] C. C. Chang, W. L. Tai, and C. C. Lin, "Hiding a secret color image in two color images," *Imaging Science Journal*, vol. 53, no. 4, pp. 229–240, 2005.

[18] M. Nakajima and Y. Yamaguchi, "Enhancing registration tolerance of extended visual cryptography for natural images," *Journal of Electronic Imaging*, vol. 13, no. 3, pp. 654–662, 2004.

[19] W. P. Fang, "Friendly progressive visual secret sharing," *Pattern Recognition*, vol. 41, pp. 1410-1414, 2008.

[20] C. C. Thien and J. C. Lin, "An image-sharing method with user-friendly shadow images," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 13, no. 12, pp. 1161–1169, 2003.

[21] T. H. Chen and K. H. Tsao, "Threshold visual secret sharing by random grids," *Journal of Systems and Software*, vol. 84, no. 7, pp. 1197-1208, 2011.

[22] F. Liu, C. K. Wu, and X. J. Lin, "A new definition of the contrast of visual cryptography scheme," *Information Processing Letters*, vol. 110, no. 7, pp. 241-246, 2010.

Young-Chang Hou received his B.S. degree in Atmospheric Physics from National Central University, Taiwan, R.O.C., in 1972, his M.S. degree in Computer Applications from Asian Institute of Technology, Bangkok, Thailand, in 1983, and his Ph.D. degree in Computer Science and Information Engineering from National Chiao-Tung University, Taiwan, R.O.C., in 1990. From 1976 to 1987, he was a senior engineer of Air Navigation and Weather Services, Civil Aeronautical Administration, Taiwan, R.O.C., where his works focused on the automation of weather services. From 1987 to 2004, he was on the faculty at the Department of Information Management, National Central University. Currently he is a Professor in the Department of Information Management, Tamkang University, Taiwan, R.O.C. His research interests include digital watermarking, information hiding, fuzzy logic, genetic algorithms, and visual cryptography.

Shih-Chieh Wei received his B.E. degree in electrical engineering from National Taiwan University, Taiwan, R.O.C., in 1988, his M.S. degree in computer science from National TsingHua University, Taiwan, R.O.C., in 1990, and his Ph.D. degree in systems engineering from Osaka University, Japan, in 1998. He is currently an Assistant Professor with the Department of Information Management, Tamkang University, Taiwan, R.O.C. His areas of interest include information security, information retrieval, and GPU-based high performance computing.

Chia-Yin Lin received her bachelor degree in Information Management from Fu Jen Catholic University, Taiwan, R.O.C. in 2007, her MS degree in Information Management from Tankang University, Taiwan, R.O.C. in 2012. Her research interests include digital image processing, digital watermarking, and visual cryptography.