Progressive Visual Cryptography with Friendly and Size Invariant Shares

Young-Chang Hou[1], Zen-Yu Quan[2], and Chih-Fong Tsai[2]
[1]Department of Information Management, Tamkang University, Taiwan
[2]Department of Information Management, National Central University, Taiwan

Abstract: *Visual cryptography is an important data encoding method, where a secret image is encoded into n pieces of noise-like shares. As long as there are over k shares stacked out of n shares, the secret image can be directly decoded by the human naked eye; this cannot be done if less than k shares are available. This is called the* (*k, n*)*-threshold Visual Secret Sharing Scheme* (*VSS*)*. Progressive Visual Cryptography* (*PVC*) *differs from the traditional VSS, in that the hidden image is gradually decoded by superimposing two or more shares. As more and more shares are stacked, the outline of the hidden image becomes clearer. In this study, we develop an image sharing method based on the theory of PVC, which utilizes meaningful non-expanded shares. Using four elementary matrices* (C_0-C_3) *as the building blocks, our dispatching matrices* (M_0 - M_3) *are designed to be expandable so that the contrast in both the shares and the restored image can be adjusted based on user needs. In addition, the recovered pixels in the black region of the secret image are guaranteed to be black, which improves the display quality of the restored image. The image content can thus be displayed more clearly than that by previous methods.*

Keywords: *Visual cryptography, progressive visual cryptography, secret sharing, unexpanded share, meaningful (Friendly) share.*

Received April 8, 2015; accepted October 7, 2015

1. Introduction

Secret communication has always been a sought-after goal throughout history. During times of war, preserving the secrecy of important information can be a key factor to the winning of battles. Thus, great effort has been devoted to the development of the fields of cryptography and steganography as the means to transmit data safely. In cryptography, the secret information is transformed into a series of meaningless messages. However, the meaningless appearance of the messages may actually attract the attackers' attention and strengthen their intention to break the code. Steganography is used to reduce the chance of data being intercepted and decoded by the attackers. Here, the senders conceal the secret information in an innocent looking image, which provides another layer of security.

In traditional cryptography and steganography, the decoding key is only given to a single individual. If he/she has bad intentions, that information is no longer safe. Several secret sharing schemes have been developed to solve this problem [1, 16]. For example, a secret image is encoded into *n* pieces of shares (or shadow image) that are then distributed to *n* participants. The secret image can be restored only when *k* or more shares are available. No information regarding the secret image will be revealed with *k*-1 or fewer shares. This scheme is called the (*k, n*)-threshold secret sharing. Shamir [12] first adapted this concept to develop a method for concealing the pixel values of asecret image in the constant term of a polynomial equation of degree *k*-1. This equation is then used to generate shares for each participant. The coefficients for the polynomial equation can be resolved when more than *k* participants present their shares, and this constant is then used to reconstruct the secret image. This scheme is perfectly secure, but only one pixel value can be concealed in a *k*-1 polynomial equation at a time. Therefore, the size of the share is as big as the secret image. Thien and Lin [13] extended Shamir's [12] strategy to a size-reduction sharing method. This method takes *r* successive pixels of the secret image simultaneously and uses these pixel values as the coefficients of the polynomial of degree *r*-1 to generate a share for each participant. The size of the share is reduced to 1/*r* times. Thien and Lin [13] also used a steganographic method to conceal the shares in different cover images which improved their safety. Chen and Lin [2] rearranged the bit pattern of each pixel in the secret image, to transmit secret information in a progressive way. Wang and Shyu [16] adapted Thien and Lin's model [13] to propose three progressive versions of secret image sharing. However, the encoding and decoding processes used in these studies all require complex mathematic computation. In contrast, Naor and Shamir [11] proposed a new cryptographic method, called Visual Cryptography (VC). In their approach, the secret image can be decoded simply by viewing the stacked shares. In this method, 1/0 bit strings of a share become the black/white pixels of the image. The

method has the advantages that no cryptographic knowledge or computing facilities are needed for decoding.

Naor and Shamir's [11] VC method has many advantages, but there remain some interesting issues that must be discussed. The first issue is related to pixel expansion. Each secret pixel will be extended *m* times. This means that the size of the reconstructed image will be *m* times larger than the original one, which increases the need for storage space and transmission time. Ito *et al*. [9] used the concept of probability to propose a pixel unexpanded method suitable for binary images. However, the random nature of probability means that the shares have poor display quality. Tu and Hou [14] adopted Ito's *et al.* method [9] 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.

Secondly, Naor and Shamir's scheme [11] works only for black-and-white images. Hou [5] applied color decomposition and halftone techniques to simulate continuous tone images. Color decomposition was used to separate the image into cyan, magenta, and yellow pixels to form three monochromatic images. In the halftone technique, the density of the dots is manipulated to simulate the gray level. Therefore, the gray level image can be transformed into a binary image by adjusting the density of black pixels. Hou extended the application of VC techniques to both gray-level and color images. Tu and Hsu [15] adopted Hou's method and developed a protection scheme for digital images.

The third issue to be dealt with is that traditional VC produces noise-like shares, whose appearance may easily attract an interceptor's attention. Furthermore, noise-like shares will cause some management problems for those who participate in many secret sharing projects. To solve these types of problem, Ateniese *et al*. [1] proposed an extended visual cryptography scheme in which the secret image is hidden in two meaningful camouflage images. However, their method is only good for black and white images. Hou and Wu [8] later introduced a visual cryptography model which extends Ateniese's *et al.* sharing model [1] for gray scale and color images.

Lastly, traditional VC is an all-or-nothing concept. It means that nothing can be seen in the stacked image with fewer than *k* shares (i.e., below a specified threshold). But after *k* shares are gathered (above the threshold), the contours of the secret image will become visible. In other words, the result of the stacking of shares will either be the recovery of the secret image or nothing at all. The progressive mode [3, 4, 6, 7, 10] refers to the fact that as the number of shares increases, the content of the confidential information becomes more and more complete.

In this study, we propose a user friendly and unexpanded progressive visual cryptographic method designed to improve on the drawbacks of [3, 4, 6]. Our dispatching matrices prevent the leakage of any information from the shadow image or the restored image to ensure the requirements of better security. In addition, the black pixels in the secret image appear fully black in the restored image, to meet the requirements of better visual quality. The rest of this paper is organized as follows. Section 2 briefly reviews the works related to progressive visual cryptography. The proposed scheme is introduced in section 3. The design concepts behind the dispatching matrices are explained. The experimental results and a discussion appear in section 4. Finally, some conclusions are outlined in the last section.

2. Progressive Visual Cryptography

The recovery of confidential information in VC is based on the threshold scheme. Confidential information can be decrypted by the human eye when more than *k* shares are stacked together. If less than *k* shares are available, no sensitive information can be seen. The progressive mode refers to the fact that as the number of shares increases, the content of the confidential information becomes more and more complete.

Jin *et al.* [10] proposed a multi-resolution approach to sharing a secret image that can be applied to visual cryptography. They expanded pixels to 3×3 blocks in which one of them is used to store the halftoned value of the secret image and the remaining eight are used to represent the grey value of each pixel. The first digit (the halftoned value of the secret image) was handled according to the rules of logical XOR operation. The remaining eight binary digits were handled by conventional visual cryptography. Therefore, they could either perfectly reconstruct the halftoned secret image by utilizing computer equipments or obtain an obscure secret image by directly stacking shares. In fact, Jin's work cannot disclose the secret image progressively. At the most, we can say that they proposed a multi-resolution scheme via different approaches to share secret images. Their method expanded every secret pixel to a 3×3 block. Hence, their shares will be further expanded to 6×6 times larger because of the pixel expanded scheme, which causes a severe waste of storage and transmission time.

Fang and Lin [3] applied visual cryptography for progressive visualization of an image. The secret information is progressively decrypted through superimposing shadow images. However, these shadow images have a noise-like appearance. Since every noise-style share looks similar, it is difficult for a person who joined many secret sharing projects to pick the right shadow image for the decryption process. To address these management difficulties, Fang [4] extended this method to develop a

meaningful progressive sharing method for confidential images.

Fang [4] first spread every pixel into a 2×2 block. When the secret pixel is black, it is expanded into a completely black block. If the pixel is white, then it is arbitrarily set to be a 2-black and 2-white block. This expanded image is called the basement image. The blocks' content of the shares (S_i) can be determined based on the camouflage image (T) and a basement image (O') (as shown in Table 1).

Table 1. Fang's sharing method [4].

O(*x*,*y*)	O'	T(*x*,*y*)	S_i
■	■	■	
		□	
□	■□	■	
		□	
	■□	■	
		□	
	■□	■	
		□	
	■□	■	
		□	
	■□	■	
		□	
	■□	■	
		□	

Although with Fang's [4] sharing method, the shares show meaningful camouflage rather than meaningless noise-style images, there are still some drawbacks. First, the dispatching model is based on pixel expansion. Thus, the size of the shares will be 4 times that of the secret image. Second, when the pixels of the camouflage image are white and the secret pixels are black, there is a 1/5 (or 4/5) probability that they will be distributed as a block with the 0-black (or 1-black) pixels. On the other hand, if the secret pixels are white, it has a 1/3 (or 2/3) probability of being distributed as a block with 0-black (or 1-black) pixels. Consequently, the expected values of having black pixels in a 2×2 block (grey area in Table 1) are 4/5 or 2/3, depending on whether the secret pixel is black or white. This creates a contrast of 2/15 in the white regions on each share, which leads to leakage of the outlines of the secret image and creates a severe security problem. Third, since the blocks in the shares are selected randomly, when these shares are superimposed, it cannot be guaranteed that the black pixels in the secret image will be restored as entirely black. In the same way, white pixels in the secret image may not be able to be restored to 50% black. This is why it poses a quality problem when restoring the secret image.

Hou and Quan [6] developed a method that employed two $n \times n$ matrices C_0, C_1 (to be applied to the white and black portions of the secret image, respectively), to produce n sheets of non-expanded shares. They treat the entire secret image as the object to be recovered. Superimposing one more share on the stacked image will increase the contrast in the reconstructed image by a certain ratio. However, they can only generate noise-like shares, which will tempt the attacker to break it.

On the other hand, Hou *et al*. [7] proposed a block-based progressive visual secret sharing scheme. The secret image is divided into several non-overlapped image blocks. Superimposing one more share on the stacked image will disclose one more secret image block. Therefore, the effects of progressive recovery are achieved by restoring different image blocks step by step. As long as the m^{th} share is absent from the decryption process, the secret information in the image block m will not be exposed. Only when all the shares are superimposed can the secret image be recovered in its entirety.

In this paper, we propose a new progressive visual cryptography method with meaningful and size invariant shares. Our dispatching matrices prevent the leakage of any secret information from the shadow image to ensure better security. In addition, the black pixels in the secret image appear fully black in the restored image for better visual quality.

3. Proposed Methods

3.1. Meaningful Cover Image

If the shares are noise-like images, even though interceptors will not be able to obtain any information about the secret image from any single share, they will suspect that something might be concealed there. This will increase the risk of being attacked. Therefore, having meaningful content on the shares provides a double layer of protection. The first layer of security is that attackers do not suspect that there is confidential information concealed in the shares. So the possibility of offense is reduced. The second layer of security arises from the visual cryptographic mechanism itself. The attacker cannot perceive any secret message from a single shadow image because of the random dispatching scheme. Consequently, the adoption of meaningful-image shares can improve the security of confidential information.

The number of black spots in each block on the noise-like shares is the same. Therefore, there is no obvious contrast between blocks and no contours are shown on individual shares. However, to share an image in a meaningful way, the camouflage image has to be outlined on each share. That is, there must be more black pixels in the regions corresponding to the black parts in the camouflage image. Consequently,

the possibility of black spots appearing in the shadow image will be different for the corresponding black and white areas, resulting in color difference on the shares. In addition, since both black and white spots on the secret image could be superimposed by white spots or black spots in the shares, four dispatching matrices (M^0-M^3) are needed to represent the four possible pixel combinations of the secret and camouflage images, namely (white, white), (white, black), (black, white), and (black, black), respectively.

Before introducing M^0 - M^3, we first design four $n \times n$ elementary dispatching matrices (C_0-C_3), as shown in Table 2. For matrix C_0, the elements in the first row are set to 1 (black); the other elements are all set to 0 (white). For both matrices C_1 and C_2, the elements on the main diagonal are set to 1; the other elements are all set to 0. All elements in matrix C_3 are set to 1. Each row in the matrices represents a possible way of sharing among n participants, and each column represents the content distributed to each participant. For example, if we select the second row of C_1 to dispatch a secret pixel to each participant, only participant 2 will get a black pixel on his/her share. The others will all get a white pixel on their shares. This is because only one "1" appears in the second column and the second row of C_1. Likewise, if we select the first (last) row of C_0 to dispatch a secret pixel, all participants will get a black (white) pixel on his/her share, since every element in the first (last) row of C_0 is set to "1" ("0").

Table 2. Four $n \times n$ elementary matrices.

$C_0 = \begin{bmatrix} 1 & 1 & \cdots & \cdots & 1 \\ 0 & 0 & \cdots & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \cdots & \cdots & 0 \end{bmatrix}_{n \times n}$	$C_1 = \begin{bmatrix} 1 & 0 & \cdots & \cdots & 0 \\ 0 & 1 & 0 & \cdots & 0 \\ \vdots & 0 & \ddots & \vdots & \vdots \\ \vdots & \cdots & \cdots & \ddots & \vdots \\ 0 & \cdots & \cdots & 0 & 1 \end{bmatrix}_{n \times n}$
$C_2 = \begin{bmatrix} 1 & 0 & \cdots & \cdots & 0 \\ 0 & 1 & 0 & \cdots & 0 \\ \vdots & 0 & \ddots & \vdots & \vdots \\ \vdots & \cdots & \cdots & \ddots & \vdots \\ 0 & \cdots & \cdots & 0 & 1 \end{bmatrix}_{n \times n}$	$C_3 = \begin{bmatrix} 1 & 1 & \cdots & \cdots & 1 \\ 1 & 1 & \cdots & \cdots & 1 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 1 & 1 & \cdots & \cdots & 1 \end{bmatrix}_{n \times n}$

In matrix C_0, there is only one 1 in each column. It means that when applying C_0 to generate shares, every participant has only a $1/n$ chance of being assigned the black pixel. Also, since all 1's appear in the same row, these black spots will all appear at the same pixel position on each share. Therefore, after superimposing the shares, there remains a chance of $1/n$ for a pixel to appear as black on the restored image if pixels are dispatched from matrix C_0. For matrices C_1 and C_2, every participant also has a $1/n$ chance to be assigned the black pixel, but this time, all black pixels appear in different pixel positions on each share. As more and more shares are superimposed, the chance of black spots appearing in these pixel positions will gradually increase. When all shares are stacked, these spots, dispatched from matrices C_1 and C_2, will all be black. Matrix C_3 shows that each participant has a 100% chance to get a black spot on the share during dispatching. Hence, these positions will certainly appear black during share stacking.

Four sharing matrices (M^0-M^3), each with a size of $2n \times n$, are composed of C_0-C_3 (Table 3). The black part in the camouflage image has a higher chance of appearing black on the shadow images than the white part. Therefore, matrices C_2 and C_3 are used to control the contrast in the shadow image. We place C_2 in the related matrices (M^0, M^2) to produce the white parts of the camouflage image, and C_3 in the related matrices (M^1, M^3) to produce the black parts of the camouflage image. In the result, there are only 2 ones in each column of M^0 and M^2, but there are n+1 ones in each column of M^1 and M^3. When the pixel on the camouflage image is white, the corresponding pixel on each shadow image has a $2/2n$ chance of being black, regardless of whether it is derived from a black or white secret pixel. Likewise, when the pixel of the camouflage image is black, the chance of being a black spot on each shadow will increase to $(n+1)/2n$ regardless of whether it is derived from M^1 or M^3. This indistinguishable property ensures the security of the shadow images. The commonly used definition for the black-white contrast is α = "the average blackness in the black region" – "the average blackness in the white region" [11]. Therefore, each share will have a contrast of $(n-1)/2n$ (= $(n+1)/2n$-$2/2n$) that allows the production of some lighter parts and some darker parts in the shadow images, revealing the outlines of the camouflage image.

Table 3. Four $2n \times n$ dispatching matrices.

		Camouflage image	
		White	Black
Secret image	White	$M^0 = \begin{bmatrix} C_2 \\ C_0 \end{bmatrix}_{2n \times n}$	$M^1 = \begin{bmatrix} C_3 \\ C_0 \end{bmatrix}_{2n \times n}$
	Black	$M^2 = \begin{bmatrix} C_2 \\ C_1 \end{bmatrix}_{2n \times n}$	$M^3 = \begin{bmatrix} C_3 \\ C_1 \end{bmatrix}_{2n \times n}$

To be able to see the content of the confidential image clearly, the black regions of the secret image should have a greater chance of having black pixels on the corresponding locations of the superimposed image than that for the white regions. Matrices C_0 and C_1 are used to control the color difference on the superimposed image. That is, C_0 is placed in the related matrices (M^0, M^1) to reveal the white parts of the confidential image, and C_1 is placed in the related matrices (M^2, M^3) to reveal the black parts of the confidential image. Every row of matrix M^i represents a different way of dispatching. There are only n+1 rows having 1s in matrices M^0 and M^1, but there are 1s in every row of matrices M^2 and M^3. Therefore, pixels dispatched from M^0 and M^1 to each share image will have a smaller chance to appear black compared to

those dispatched from M^2 and M^3. Consequently, when composing k shadow images, the white part of the secret image has $(k+1)/2n-(n+1)/2n$ chances of appearing as black pixels on the stacked image, while the black spots on the secret image have $2k/2n - (n+k)/2n$ chances of being black. As the number of superimposed shares increases, the ratio of black appearing in the black regions of the confidential image will be greater, making the black-and-white contrast more and more obvious. The outlines of the confidential image will be shown on the stacked shares. After superimposing all shares, white pixels on the restored secret image will have a $(n+1)/2n$ chance of appearing black, while the black pixels will be totally black. Furthermore, the restored image will display a black-and-white color difference of $(n-1)/2n$ $(=1-(n+1)/2n)$, which makes the contour of the secret image distinguishable.

To generate shares, we first obtain a random number l ranging from 1 to $2n$. When the pixels in the secret and camouflage images are (white, white), take the l-th row vector from matrix M^0, then allocate the first value $M^0(l, 1)$ to share 1, the second value $M^0(l, 2)$ to share 2, …, and the n-th value $M^0(l, n)$ to share n. Similarly, if the pixels in the secret and camouflage images are (white, black), (black, white) or (black, black), take the l-th row vector of the corresponding matrices (M^1, M^2, or M^3), then each value of the l-th row will be allocated to the corresponding shares, respectively. The detailed dispatching algorithm is shown in Algorithm 1.

Algorithm 1: Dispatching Algorithm:

Input：

1. *A halftone secret image P whose size is $H\times W$*
2. *A halftone camouflage image C whose size is $H\times W$*
3. *Four $2n\times n$ secret sharing matrices M^0 - M^3*

Output：*n shares S^m with the same camouflage image on them, $m = 1, 2, \ldots, n$*

Process：

1. *For (each $P(i, j) \in P$ and $C(i, j) \in C$, where $1 \le i \le H, 1 \le j \le W$)DO*
2. *Get a random index l, where $1 \le l \le 2n$*
3. *For (each m, $1 \le m \le n$) DO*
   - 3.1. *if $P(i, j) = 0, C(i, j) = 0$ then $S^m(i, j) = M^0(l, m)$*
   - 3.2. *else if $P(i, j) = 0, C(i, j) = 1$ then $S^m(i, j) = M^1(l, m)$*
   - 3.3. *else if $P(i, j) = 1, C(i, j) = 0$ then $S^m(i, j) = M^2(l, m)$*

   else $S^m(i, j) = M^3(l, m)$

According to the Dispatching Algorithm, for each pixel of the secret image, every share is assigned one pixel at a time. This means that our method can be classified as a pixel non-expansion scheme. This is an improvement on Fang's method [4] which expands every pixel 2×2 times. As to the security aspect, since each column in matrices M^0 and M^2 has two "1s", whether the pixel in the confidential image is black or white, there is a chance of $2/2n$ for the pixel in the share to be black. For the black pixels in the shares, since each row in matrices M^1 and M^3 has $(n+1)$ "1s", no matter what the secret pixel is, there is a chance of $(n+1)/2n$ that black pixels will be assigned in the shares. In addition, since all of the dispatching processes are based on random variables, no information can be gained from any shadow image as to whether the shared secret pixel is white or black. Hence, the shadow images will only reveal the content of the camouflage image. No clues of the confidential image will be leaked. Therefore, the shares can be regarded as safe. In addition, the shares display a camouflage image, giving the false impression that this is just an ordinary picture. The viewer will not think that a confidential image is concealed inside. It reduces the possibility of being attacked, and greatly improves the security of the confidential image. In the restored image, regardless of whether the white spots on the confidential images are formed from black spots or white spots on the cover image, there is a chance of $(n+1)/2n$ that they will be superimposed as black. In contrast, the pixels on the black spots of the restored image must be fully black. For the restored image, not only we cannot see the outline of the camouflage image, but also a contrast as high as $(n-1)/2n$ can be reached, which can produce good visual quality in the restored image.

3.2. Other Designs

The upper half of the M^0-M^3 matrices (C_2, C_3) is used to control the contrast between the black and white regions in the shares. In addition to the design shown in Table 2, other designs may also be possible (Table 4) in order to get varying degrees of black-and-white contrast in the shares. Assume that the new sharing matrices C_2^i and C_3^i are $i\times n$, and that i stands for an integer between 2 and n. C_2^i means that the matrix will have i groups of same columns. Each group has n/i columns (if n/i is indivisible, some groups will have one more column or $\lceil n/i \rceil$ columns and some will have one less, or $\lfloor n/i \rfloor$ columns). The values of the i-th row in the i-th group are all set to 1, and the remaining values in C_2^i are all set to 0. In the C_3^i matrix, all of the values are set to 1. That is, there is only one opportunity for a black spot to appear in each column of matrix C_2^i. According to C_3^i, there are i opportunities for black spots to appear in each column. Based on the concepts mentioned above, new dispatching matrices (Table 5) using C_2^i and C_3^i to control the black-and-white contrast in the shadow image are created, and the size of the matrices is $(i+n)\times n$.

Table 4. Two $i \times n$ elementary matrices.

$C_2^i = \begin{bmatrix} 1\cdots1 & 0\cdots0 & \cdots & \cdots & 0\cdots0 \\ 0\cdots0 & 1\cdots1 & 0\cdots0 & \cdots & 0\cdots0 \\ \vdots & 0\cdots0 & \ddots & \vdots & \vdots \\ \vdots & \cdots & \cdots & \ddots & \vdots \\ 0\cdots0 & \cdots & \cdots & 0\cdots0 & 1\cdots1 \end{bmatrix}_{i\times n}$
$C_3^i = \begin{bmatrix} 1 & 1 & \cdots & \cdots & 1 \\ 1 & 1 & \cdots & \cdots & 1 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 1 & 1 & \cdots & \cdots & 1 \end{bmatrix}_{i\times n}$

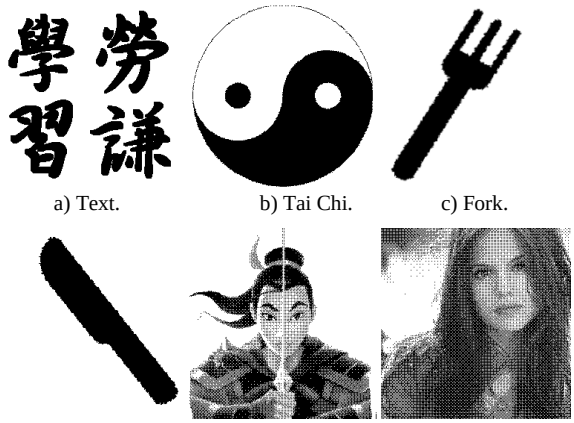
Table 5. Four $(i+n)\times n$ dispatching matrices.

		Camouflage image	
		White	Black
Secret image	White	$M^0 = \begin{bmatrix} C_2^i \\ C_0 \end{bmatrix}_{(i+n)\times n}$	$M^1 = \begin{bmatrix} C_3^i \\ C_0 \end{bmatrix}_{(i+n)\times n}$
	Black	$M^2 = \begin{bmatrix} C_2^i \\ C_1 \end{bmatrix}_{(i+n)\times n}$	$M^3 = \begin{bmatrix} C_3^i \\ C_1 \end{bmatrix}_{(i+n)\times n}$

According to Table 5, there is a probability of $2/(n+i)$ that the white pixels in the shares will be assigned to be black spots, while the black pixels will have a chance of $(i+1)/(n+i)$ to be assigned as black spots. Therefore, the black and white contrast in the shadow image is $(i+1)/(n+i)-2/(n+i) = (i-1)/(n+i)$, i=2, 3, ..., and n. The larger the number i is, the greater the black-and-white contrast is and the clearer the outline of the camouflage image in the shares will be. Hence, we obtain better visual quality in the camouflage image in the shares. In contrast, when the value of i is small, the black-and-white contrast in the shares is also small. As a result, the difference between the black and white regions will not be as clear, leading to a shadow image with less clear visual quality. On the other hand, when n shares are superimposed, the white pixels in the secret image have a chance of $(i+1)/(n+i)$ to appear as black spots, and the black pixels are fully black. So the contrast of the restored image is $1-(i+1)/(n+i)=(n-1)/(n+i)$, i = 2, 3, ..., and n. Therefore, when the value of i is small, the restored image will have a larger black-and-white contrast, which means that the quality of the reconstructed secret image is better. On the other hand, when the value of i is large, the contrast in the restored image will be smaller and the visual quality will not be as clear. Following from the above observations, we can use i to control the contrasts in both the shares and the stacked image to satisfy different needs. Some experimental results will be presented in section 4.3.

4. Experimental Results

Our experiment runs in the environment of an AMD Athlon™ X2 240 2.81GHz CPU with 1.75 GB of memory. The operating system is Windows XP, and Java (JDK 1.6.14) is used as the development tool. The superiority of our approach is demonstrated by the results of the two methods described in Sections 3.1 and 3.2. There are six 256×256 images used in our experiment, as shown in Figure1.Figure 1-a to 1-d show binary images. Figure1-e shows a gray-scale image with few colors. Figure1-f illustrates a gray-scale image with 256 colors.



a) Text. b) Tai Chi. c) Fork.

d) Knife. e) Knight. f) Mena.

Figure 1. Six test images used in this experiment.

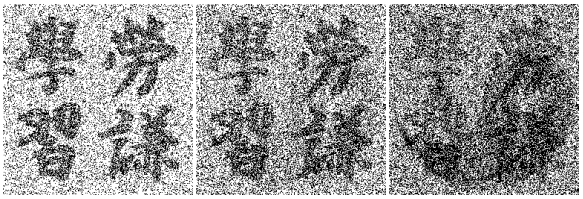
4.1. Experiment 1: Meaningful Cover Image

The experimental results of the method discussed in section 3.1 are shown in Figures 2 and 3. The number of participants are set to five and seven, respectively, and the dispatching matrices used are shown in Tables 2 and 3 with n=5 and 7. The execution time for the whole dispatching process is 0.500 and 0.594 seconds, respectively.

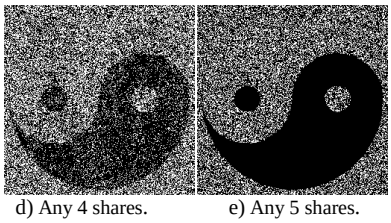
The secret image and the camouflage image used in Figure 2 are Tai Chi and Text, respectively. Five shares are generated in this experiment. Figure 2-a is one of the shares. The probabilities of black spots appearing in the white and black regions on the share are 2/10 and 6/10, respectively. The different densities of black pixels among white and black regions on the shares cause 40% black-and-white contrast. Consequently, the disguised contents of the camouflage image can be seen on the shares. As we can see, no confidential information can be obtained from any single share. When k shares are superimposed, the probability of white pixels in the secret image being black ranges from $(k+1)/10$ (superimposed by all white pixels) to 6/10 (superimposed by all black pixels) while black pixels in the secret image have a $2k/10$ (superimposed by all white pixels)-$(k+5)/10$ (superimposed by all black pixels) chance of being black.

As a result, if the number of overlapping shares are few (Figures 2-b to 2-c), some of the black pixels on the secret image, which are superimposed by white pixels in the shares, have less chance to be black than some part of the white pixels in the secret image, which are superimposed by black pixels from the shares. Hence, the outlines of the secret image on the

stacked shares may not be so obvious. Nevertheless, as more shares are superimposed, the rate of accumulation of black pixels in the black areas is faster than that in the white areas. The image gradually becomes clearer with the stacking of more shares (Figure 2-b to 2-e). When all shares are superimposed (Figure 2-e), the white pixels of the secret image have a chance of 6/10 to be black, while the black pixels of the secret image are fully black. Therefore, the contrast of the restored image is 4/10 (40%), which is enough for clear identification of the secret image. Figure 3 shows the experiment with seven shares.



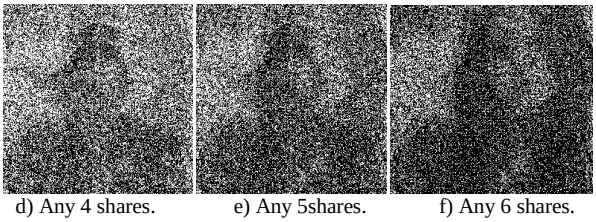
a) Any one share. b) Any 2 shares. c) Any 3 shares.



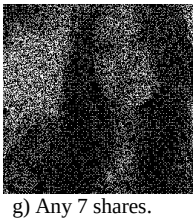
d) Any 4 shares. e) Any 5 shares.

Figure 2. Results of five shares with the same meaningful feature.

a) Any one share. b) Any 2 shares. c) Any 3shares.



d) Any 4 shares. e) Any 5shares. f) Any 6 shares.



g) Any 7 shares.

Figure 3. Results of seven shares with the same meaningful feature.

For restoration of the secret image, the probability of black spots occurring in the black regions of the secret image must be greater than that in the white regions of the secret image. However, the white parts of the secret image may be superimposed by the black parts in the shares (after superimposing k shadow images, the chance of having black spots is $(n+1)/2n$). On the other hand, the black parts of the secret image may be stacked with the white parts in the shadow images (after superimposing k shares, the chance of having black spots is $2k/2n$). As a result, when fewer shares overlap, we may not have enough chance for black pixels to accumulate in some black regions of the secret image. Thus, the degree of blackness appearing in certain black areas may be even less than some white areas in the secret image. This causes the contours of the secret image to appear less obvious when fewer shares are overlapped. When $2k/2n > (n+1)/2n$ holds, or $k > (n+1)/2$, the superimposition of more than k shares will reveal the secret content increasingly clearer. This is also confirmed from Figs. 2-3.

4.2. Experiment 2: Comparisons with Fang's Work

The superiority of our matrices over those used in Fang's [4] sharing model is confirmed by taking a camouflage image of "Fork" and a secret image of "Knife" as an example. Five meaningful shares are produced. A comparison of our results with Fang's appears in Table 6. Since Fang used pixel expansion techniques, their shares are four times larger than the original images. In contrast, the non-expanded share technique used in our study improves on this. As a result, every share's size is the same as that of the secret image. Therefore, our approach saves both storage space and transmission time.

Secondly, no matter what the pixel content of the secret image is, in our matrices, the probabilities of the appearance of black pixels in the white and black regions in the shares are always 1/5 and 3/5, respectively. This creates the necessary contrast in the shares. Therefore, every share we generate is a meaningful image, and an attacker cannot find any secret information from these shares. In contrast, in Fang's model, there are different opportunities for black pixels to appear in the white regions in the camouflage images. When the secret pixel is black, the expected probability of black appearing at the corresponding location on the shares is 4/5, greater than the situation where the expectation value is 2/3 when the secret pixel is white. It created a contrast of $2/15 = 4/5 - 2/3$ just because the secret pixels have different colors. Consequently, the outlines of the secret image are exposed in these shares, which lead to a severe security problem. Take Table 6-a as an example. One can see the vague image of a knife from the upper-left hand side to the bottom-right hand side on the share.

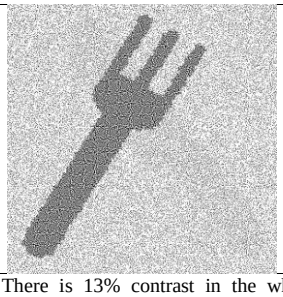
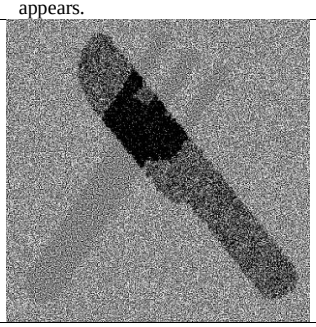
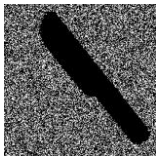
Besides, when the pixels of the secret image are white, the probabilities of black spots appearing in the white and black regions of the camouflage image on the shares are not the same (Table 1). When the camouflage pixel is black, it has a 100% probability to be distributed as a block with 2-black pixels. On the

other hand, when the camouflage pixel is white, it has 1/3 (or 2/3) chance to be distributed as a block with 0-black (or 1-black) pixels. Consequently, after stacking all 5 shares, the white regions on the restored image may be displayed as a block with 2-black pixels with 100% probability if they are superimposed by black pixels from the camouflage image. They also have a chance of 1/243, 62/243 or 180/243 to be displayed as a block with 0-, 1- or 2-black pixels, respectively, if they are superimposed by white pixels from the camouflage image. In this case, the expectation of black pixels in every 2×2 block is 422/243 (≈ 1.74). This difference means that we can clearly see the Fork in the stacked image (Table 6-c).

Finally, since Fang's model is based on a stochastic process to dispatch blocks to each share, each participant is considered independently. Therefore, it is not guaranteed that every candidate block in Table 1 will be selected. If some candidates are not selected by any share, the desired pattern will not be restored. For example, the white regions of the restored image may not be a 2-black-and-2-white block if they are superimposed by the white portions of the shares. Nevertheless, they will surely have 2 black pixels if they are superimposed by the black portions of the shares. This difference means that we may differentiate between the black and white regions of the camouflage image from the restored image (See Table 6-c). The fork is revealed from the upper-right to the bottom-left). On the other hand, the chance is much lower that fully black blocks will be stacked with the white portions in the shares than the black portions (See Table 6-c). Note the difference between both ends and the middle of the knife).

Although pixels are dispatched randomly to every share, our dispatching matrices are designed to consider all participants at the same time. This is the reason we can improve on the drawbacks in Fang's studies. In this comparison, there are six rows with 1s in matrices M^0 and M^1, but there are 1s in every row of matrices M^2 and M^3. Each row of matrix M^i represents a different way of sharing. After stacking all shares, the black regions will be entirely black and the white regions will have a 60% chance of being black, regardless of whether they are superimposed by the white or black regions of the shares. This will create 40% contrast in the restored image, which is better than that in Fang's model (25% contrast). Therefore, our model can generate better reconstruction quality.

Table 6. Comparison between Fang's method and our method.

	Fang's study [4]	Our study
Image size	512×512(4 times larger)	256×256 (original)
Share		
	(a) There is 13% contrast in the white regions of the share. So a vague outline of the secret Knife image appears.	(b) No secret information appears in a meaningful share at all.
Restored image		
	(c) The black regions of the secret image cannot be guaranteed to produce 100% black pixels. The white regions also cannot be guaranteed to be 50% black. Both the stego and secret images appear in the restored image.	(d) The black regions of the secret image are reconstructed as fully black, and no stego image appears in the restored image.

4.3. Experiment 3: Other Designs

As can be seen from Table 5, the black-and-white color on the share is primarily controlled by matrices C_2^i and C_3^i. When the pixel in the camouflage image is white, the chance of having a black pixel at the corresponding location in each share is $2/(n+i)$, where i=2 to n. When the pixel is black, the chance of it appearing black increases to $(i+1)/(n+i)$. This will create a contrast of $(i-1)/(n+i)$ on each share. This contrast makes the black regions look darker than the white ones on shares, revealing the outline of the camouflage image.

This experiment is designed to explore how different i values may affect both the shares and the restored image. In Figure 4, we set the number of participants to seven and set i values to 3, 5, and 7. The upper parts of Figure 4 are shares generated based on the matrices given in Table 5; the lower parts of Figure 5 show the restored secret image after superimposition of all n shares.

Regarding Figure 4, when i gets larger, the black-and-white contrast becomes more apparent on the shares. In the meantime, the black-and-white outlines of the camouflage image (Figure 4-c) become more pronounced, leading to better visual quality in the shares. On the other hand, when i is smaller, the black-and-white contrast is also lower in the shares. This will cause the black-and-white outlines of the

disguised image to be less clear (Figure 4-a). So the shares with a smaller *i* will have inferior visual quality.

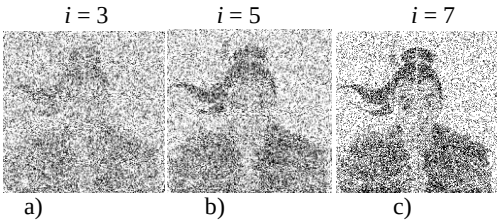


Figure 4. Shadow images.

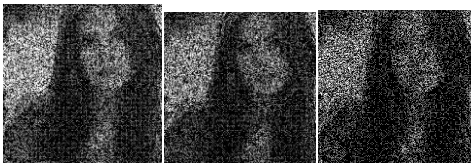


Figure 5. Restored images with n=7 for different i.

When all n shares are superimposed, the probability of black spots appearing on white pixels in the secret image is $(i+1)/(n+i)$ while the black pixels are fully black (100% black). After superimposing all the shares, the black-and-white contrast is $(n-1)/(n+i)$, where i=2, 3, ..., and n, Therefore, the black-and-white contrast in the superimposed image is larger when i is smaller, which leads to a better quality of the restored secret image (Figure 5-a). On the other hand, when i is larger, the black-and-white contrast is lower (Figure 5-c).

Take six shares for instance. The contrasts of the shares and the restored image for different i are shown in Table 7, in which W_1 and B_1 stand for the probability of appearing black spots for the white and black pixels in the shares; and W_2 and B_2 represent the chances of appearing black for the white and black pixels in the secret image when all shares are superimposed.

Table 7. Contrast of shares and stacked images.

n	i	W_1	B_1	Contrast in share	W_2	B_2	Contrast in restored image
6	2	2/8	3/8	12.25%	3/8	1	62.50%
	3	2/9	4/9	22.22%	4/9	1	55.55%
	4	2/10	5/10	30.00%	5/10	1	50.00%
	5	2/11	6/11	36.36%	6/11	1	45.45%
	6	2/12	7/12	41.67%	7/12	1	41.67%

According to the results in Table 7, if we want to obtain better visual quality in the shares, i should be relatively large in order to obtain greater contrast. On the other hand, if we need a clearer restored secret image, then i should be relatively small to obtain better contrast in the restored image. With the aim of having enough contrast to achieve better visual quality in both the camouflage shares and the restored secret image, we set $i=n$ and propose the size of the matrix to be $2n\times n$, as shown in Table 3. Section 3.1 is a special case of section 3.2 when $i=n$.

5. Conclusions

We propose a method of pixel non-expansion progressive visual cryptography with meaningful camouflage images on the shares. Matrices C_2 and C_3 are designed to control the black-and-white contrast of the shares while matrices C_0 and C_1 are designed to control the black and white contrast on the stacked shares. The results of our study and those obtained in other studies are shown in Table 8.

Table 8. Comparison of related research.

Authors	Share (Shadow Image)				Restored Image		Matrix Extensibility
	Size	Content	Contrast	Leakage of Secret	Contrast	Quality	
Fang & Lin [3]	2×2	Noise-like	—	Yes	50%	Poor	No
Fang [4]	2×2	Meaningful	25%	Yes	50%	Poor	No
Hou and Quan [6]	the same	Noise-like	—	No	$(n-1)/n$	Very good	No
Our method	the same	Meaningful	$(i1)/(n+i)$	No	$(n1)/(n+i)$	Good	Yes

Our proposed progressive scheme has the following advantages:

1. It uses a non-expansion technique to dispatch confidential information. So the size of the share is equal to that of the secret image. This reduces the need for extra storage space and transmission time.
2. The dispatching matrices (Table 5) are designed to be adjustable, with i=2, 3, ..., n. The contrasts in the shares and the restored image are $(i-1)/(n+i)$ and $(n-1)/(n+i)$, respectively. Users can adjust the white and black contrasts in the shares and in the restored image to meet their own needs. In the case of $i=n$, each share and restored image has a high contrast of $(n-1)/2n$. The camouflage images and the secret image are clearly displayed.
3. Although we also used the concept of random dispatching, the black pixels in the secret image revert to fully black. Therefore, the restored image has better visual quality than is obtained with other methods.
4. The dispatching matrices will leak out neither the secret image in any single share, nor the camouflage image in the restored image. They meet the requirements of better security and quality.

Acknowledgments

This research was partly supported by National Science Council of Republic of China under contract NSC-97-2221-E-032-024. We gratefully acknowledge the valuable comments provided by Twricy Hsu and Shih-Chieh Wei on earlier drafts of this paper.

References

[1] Ateniese G., Blundo C., Santis A., and Stinson D., "Extended Capabilities for Visual

Cryptography," *Theoretical Computer Science*, vol. 250, no. 1-2, pp.143-161, 2001.
[2] Chen S. and Lin J., "Fault-tolerant and Progressive Transmission of Images," *Pattern Recognition*, vol. 38, no.12, pp. 2466-2471, 2005.
[3] Fang W. and Lin J., "Progressive Viewing and Sharing of Sensitive Images," *Pattern Recognition Image Analysis*, vol. 16, no. 4, pp. 632-636, 2006.
[4] Fang W., "Friendly Progressive Visual Secret Sharing," *Pattern Recognition*, vol. 41, no. 4, pp. 1410-1414, 2008.
[5] Hou Y., "Visual Cryptography for Color Images," *Pattern Recognition*, vol. 36, no.7, pp.1619-1629, 2003.
[6] Hou Y. and Quan Z., "Progressive Visual Cryptography with Unexpanded Shares," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 21, no. 11, pp. 1760-1764, 2011.
[7] Hou Y., Quan Z., Tsai C., and Tseng A., "Block-based Progressive Visual Secret Sharing," *Information Sciences*, vol. 233, pp. 290-304, 2013.
[8] Hou Y. and Wu J., "An Extended Visual Cryptography Scheme for Concealing Color Images," *in Proceeding of the 5th Conference on Information Management and Police Administrative Practice*, Taoyuan, pp. 62-69, 2001.
[9] Ito R., Kuwakado H., and Tanaka H., "Image Size Invariant Visual Cryptography," *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, vol. E82-A, no. 10, pp. 2172-2177, 1999.
[10] Jin D., Yan W., and Kankanhalli M., "Progressive Color Visual Cryptography," *Journal of Electronic Imaging*, vol. 14, no. 3, pp. 033019-1-033019-13, 2005.
[11] Naor M. and Shamir A., "Visual Cryptography," *Advances in Cryptology-Eurpocrypt'94*, *Lecture Notes in Computer Science*, vol. 950, pp. 1-12, 1995.
[12] Shamir A., "How to Share a Secret," *Communications of the ACM*, vol. 22, no. 11, pp. 612-613, 1979.
[13] Thien C. and Lin J., "Secret Image Sharing," *Computers & Graphics*, vol. 26, no. 5 pp. 765-770, 2002.
[14] Tu S. and Hou Y., "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.
[15] Tu S. and Hsu C., "A Joint Ownership Protection Scheme for Digital Images based on Visual Cryptography," *The International Arab Journal of Information Technology*, vol. 9, no. 3, pp. 276-283, 2012.
[16] Wang R. and Shyu S., "Scalable Secret Image Sharing," *Signal Processing: Image Communication*, vol. 22, no.4, pp. 363-373, 2007.

Young-Chang Hou received his B.S. degree in atmospheric physics from National Central University, Taiwan 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 in 1990. From 1976 to 1987, he was a senior engineer with Air Navigation and Weather Services, Civil Aeronautical Administration, Taiwan, where his work 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 with the Department of Information Management, Tamkang University, Taiwan. His research interests include digital watermarking, information hiding, fuzzy logic, genetic algorithms, and visual cryptography.

Zen-Yu Quan received his B.S. degree in Information management from Tatung University, Taiwan in 2007, his M.S. degree in information management from Tamkang University, Taiwan in 2009. He is currently a PhD student at the Department of Information Management, National Central University, Taiwan. His research interests cover secret sharing, digital watermark, and image retrieval.

Chih-Fong Tsai received a PhD at School of Computing and Technology from the University of Sunderland, UK in 2005. He is now a professor at the Department of Information Management, National Central University, Taiwan. His current research focuses on data mining and machine learning. He has published more than 50 professional publications and received the Emerald Literati Network 2008 Awards for Excellence from Online Information Review ("A Review of Image Retrieval Methods for Digital Cultural Heritage Resources") and the award for top 10 cited articles in 2008 from Expert Systems with Applications ("Using Neural Network Ensembles for Bankruptcy Prediction and Credit Scoring").