Secret Sharing Using Visual Cryptography

Chin-Chen Chang, Bo Li, and Jung-San Lee

(*Invited paper*)

***Abstract*—Compared with the traditional cryptography, visual cryptography (VC) decrypts secret images referring to the characteristics of human vision, rather than the cryptography knowledge or complex computations. Furthermore, seeing to the freeness of the secret key, the whole process of encryption as well as decryption for the visual cryptography meets a fast dealing course. As to the security concern, it is able to guarantee that no one can have access to any clues about the content of a secret image from individual cover images. Thus, owing to the studies on this area, the target of light-weighted cryptography is reached. Now the visual cryptography has been developed from the meaningless shadows to the meaningful ones. Seeing to the highly developed technique, some advanced VC techniques are introduced in this survey, respectively.**

***Index Terms*—Light-weighted, meaningful shares, meaningless shares, progressive, visual cryptography.**

doi: 10.3969/j.issn.1674-862X.2010.04.001

1. Introduction

Corresponding to the highly developed technique in this information age, the security of digital data has become more and more important considering the ease of digital duplication and tampering. Seeing to the traditional cryptography mechanism, it provides a secure environment to guarantee people's surfing over the Internet by encrypting the data transferred online. However, as it is known, all traditional encryption methods, symmetric and asymmetric, such as advanced encryption standard (AES), data encryption standard (DES), and RSA (Rivest, Shamir, and Adleman), need complex knowledge of the cryptography and require a long time to complete the process. Thus, a light-weighted method for encrypting the secrets is in desperate need nowadays[1, 2]. Moreover, in some cases, it is dangerous if a file of secret data is held by only one person without extra copies, for the secret data file may be lost incidentally, modified intentionally or compromised by malicious attackers. Therefore, during these cases, it is necessary for a group of individuals to share a certain secret data file on the purpose of guaranteeing the security of the secret. Therefore, in 1979, Shamir firstly proposed the concept of (k, n) threshold secret sharing to solve this problem. This method is designed to transfer a secret data file into n shares and distribute them to n participants. Subsequently, any k or more than k shares can be collected to recover the secret image, while any k–1 or fewer can only gain no information about the secret[3, 4]. Later, Naor and Shamir proposed the main concept of a (k, k) threshold visual secret sharing in 1994, making the encryption process with low computation come true[5].

Afterwards, in 1995, Naor and Shamir proposed the idea of visual cryptography formally, which provides an easy and fast decryption process generating n shares as transparencies and then stacking them together to reveal the secret image for visual inspection. Similar with traditional ones, visual cryptography is a cryptographic method that allows visual information to be encrypted, while the encryption process can be performed by the human visual system without the aid of computers or the complex cryptography theories. In the visual secret sharing scheme, a secret image is broken up into n shares so that only keepers with all n shares are able to decrypt the image, while any n–1 shares reveal no information about the original secret image. By being printed on separated transparencies, the decryption process is performed just through stacking the shares, with which the original image can appear as the secret[6]. Taking into account the low computation and simple procedure, this technique is quite suitable for encrypting a shared secret image while referring to the human vision to decrypt the secret. Moreover, free from the construction of secret key, visual cryptography is able to enhance the efficiency thanks to its fast and convenient decryption techniques[7, 8].

Compared with traditional encryption mechanisms, visual cryptography experiences a light-weighted decryption process[9]-[11]. Besides, there is no more concern about the loss of keys or the brute-method of trying for the value of the keys in the visual cryptography. Just by

Manuscript received July 28, 2010; revised October 25, 2010. This work was supported by National Science Council under Grant No. NSC98-2218-E-035-001-MY3.

C.-C. Chang and J.-S. Lee are with the Department of Information Engineering and Computer Science, Feng Chia University, Taichung 40724, Taiwan, China (e-mail: alan3c@gmail.com and leejs@fcu.edu.tw).

B. Li is with the Department of Information Security, Tongji University, Shanghai 201804, China (e-mail: lxbosky@live.cn).

Color versions of one or more of the figures in this paper are available online at http://www.intl-jest.com.

stacking the shares owned by a group of people together, the secret images can come out in time securely and efficiently[12].

In addition, seeing to various kinds of images, the visual cryptography has been applied to the binary images, grayscale images, colorful ones, and the progressive mechanism with their shares varying from meaningless to meaningful ones. It is concerned that the meaningless shares always cause suspicion of others, thus leading to the risks during the data transmission. As a result, the meaningful shares come into being referring to the technique of steganography, in which the merged image is called camouflage image in the revealing process. Different from previous visual cryptography schemes, which generate meaningless shares with noises, the idea of generating shares with meaningful contents can achieve a more secure system for secret sharing courses [13].

The remainder of this paper is organized as follows. In Section 2, the visual cryptography methods for the binary, grayscale, and colorful images that are referred to generate meaningless shares as well as the progressive mechanism are introduced. Subsequently, in Section 3, the visual cryptography for meaningful shares is demonstrated, which also consists of the binary, grayscale, colorful images, and the progressive methods. Finally, we make the conclusions in Section 4.

2. Visual Cryptography for Meaningless Shares

In this section, we introduce four techniques for visual cryptography, where the shares are based on binary image, grayscale image, and color image, respectively. And the progressive method is illustrated in the last. These techniques focus on dealing with different types of shares needed to reveal a secret image, and guarantee that the secret image can be transmitted on the Internet securely without heavy computation or complex encoding/decoding process.

2.1 Meaningless Shares for Binary Images

As it is known to all, the binary image is a simple kind of image format, which includes only two levels 0 and 255. Nowadays, this kind of image is occupying an important position in the image handling area corresponding to this visual world. Though the binary image just refers to simple operations, it still can lead to multifarious valuable effects. Thus, within idiographic image dealing systems, it is always necessary to convert original images into the binary ones for further usage.

On the purpose of applying visual cryptography to the binary image domain, the dealer firstly extends a secret pixel into a block of 2×2 sub-pixels, which contains a group of two white pixels and two black pixels. Additionally, the white pixels are denoted as transparent, while the black ones are just black as shown in Table 1. It is obvious that if a stacked image is constructed by two same shares, it shall contain two white pixels and two black ones whose result comes out as white, shown as share 1 in Table 1. On the other hand, if a stacked image is generated by the opposite shares, it comes out as black containing four black pixels, which is displayed as share 2.

Here an example of (2, 2)-method is given to illustrate the visual cryptography in the binary image domain[1]. During the encryption, every pixel is turned into two blocks, each of which belongs to the corresponding share image. In this way, the two shares are gained successfully. To reveal the secret image, two corresponding blocks are stacked together to retrieve the secret pixel, where both share blocks of a white secret pixel are the same while those of a black secret pixel are complementary as listed in Table 2. As a consequence, the white pixel here is represented by a block with the stacked result of half white sub-pixels, and a black secret pixel is all black as shown in Table 2.

Moreover, the effect of the (2, 2) method is shown in Fig. 1, where the middle two images are the shares of the secret image with letters. When stacking the two transparencies together, the secret image can be extracted owing to the rules for binary images mentioned above. Just referring to the human vision system, the content of secret can be decrypted faultlessly.

Table 1: Stacking pixel process

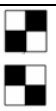
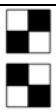
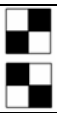
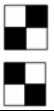
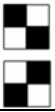
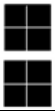
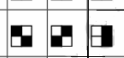
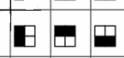
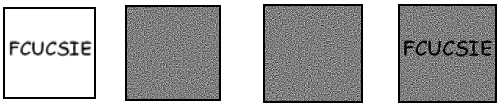
Secret pixel	Share 1	Share 2	Stacked result
			
			

Table 2: Share blocks of the (2, 2)-VSS

Secret pixel color / Share blocks	White	Black
2×2 block of the first share		
2×2 block of the second share		
Stacked 2×2 block		



(a) (b) (c) (d)

Fig. 1. Visual cryptography in binary image domain: (a) original secret image, (b) the first share image, (c) the second share image, and (d) the stacked result of (b) and (c).

In addition, Chen and Wu proposed a (2, 2) VSS scheme for two secret images to guarantee the multiple secrets embedding[14]. During the revealing process, the first secret image is decrypted only by stacking two shares. In succession, the second secret image is revealed by stacking two shares while one share is rotated. Note that the rotating angle can be 90˚, 180˚, or 270˚, allowing that the images are in rectangular form. For each secret pixel, it is turned into two share blocks b_{i_1} and b_{i_2} in the share images S_1 and S_2, in which the size of blocks is 2×2. Moreover, there is only one white sub-pixel in b_{i_1}, where p_i represents the corresponding position of the white sub-pixel in b_{i_1}, and p_i' represents the white one in the rotated sub-pixel. The detailed construction mechanism for it can be seen in Table 3. As it is shown, if the second secret image is decrypted by rotating the first share image with 90° clockwise and p_i is in the bottom right, then p_i' is in the bottom left. During the encryption process, the two sub-pixels of b_{i_2} are firstly set for the directors of p_i and p_i', following the denoting colors of secret pixels. Later on, the other sub-pixel colors are defined satisfying the block b_{i_2} with half black and half white. What is more, if the secret pixels are both white (W) before and after rotation, the positions p_i and p_i' belong to the bottom sub-pixels in b_{i_2} shall be white; while the others belong to the upper ones shall be black (B). As a result, a white sub-pixel comes into being both before and after rotation in the stacking results. Thus for the decryption process, the stacked results of b_{i_1} and b_{i_2} are determined just corresponding to the colors of the sub-pixels within the positions p_i and p_i'. In this system, two secret images can be hided faultlessly referring to the rotation. In addition, the rotation has to be focused on the angle of 90˚, 180˚, and 270˚, by which the color of the sub-pixels can be decided following the instructions shown in Table 3.

Table 3: Instruction table

Block	Two secret pixels with/without rotating			
	W/W	W/B	B/W	B/B
Share 1				
Share 2				
Stacked image				
Stacked image with rotating share 1 for 90˚				

A basic example for the mechanism of Chen and Wu is illustrated in Fig. 2, where two secrets are extracted after rotating the first share by 90˚ clockwise. Thus, two secret images can be hidden with only two shares. Note that Fig. 2 (f) is the rotated result of Fig. 2 (c), while Fig. 2 (d) and (g) are the share 2. Owing to this mechanism, the number of secret images can be largely extended. Therefore, the visual cryptography can be applied to the key management, message concealment, authorization, identification, and the entertainment domains with low storage requirement.

Considering the convenience visual cryptography has brought, numerous fields in the real world can meet a challenge of applying this technique to their current studies. For example, as to the military affairs, it is possible to embed more secret information into limited shares to transfer the secrets securely and guarantee the rights of the whole group of people with the help of visual cryptography.

2.2 Meaningless Shares for Grayscale Images

Grayscale image is an image where the value of each pixel is an independent pattern, that is to say, it carries the intensity information only in the photography and computing domains. This kind of image is also known as black-and-white image, composed exclusively of shades of gray, varying from black at the weakest intensity to white at the strongest part. Different from the binary images, which in the context of computer imaging are images with only two colors, black and white, the grayscale images have many shades of gray levels between the exact black and white. In addition, the grayscale images are regarded as monochromatic, representing their absence of any chromatic variation. As a result of measuring the intensity of light at each pixel in a single band of the electromagnetic spectrum, the intensity of a pixel in the grayscale images is expressed within a given range from 0 to 255.

For the grayscale images have been widely applied nowadays, the visual cryptography for the grayscale domain shall be demonstrated as below, whose experimental result is shown in Fig. 3.

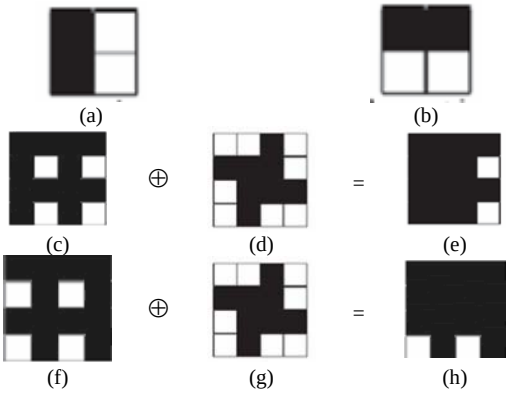


Fig. 2. An example for the mechanism of Chen and Wu: (a) secret image 1, (b) secret image 2, (c) share 1, (d) share 2, (e) stacked image 1, (f) share 1 rotated by 90° clockwise, (g) share 2, and (h) stacked image 2.

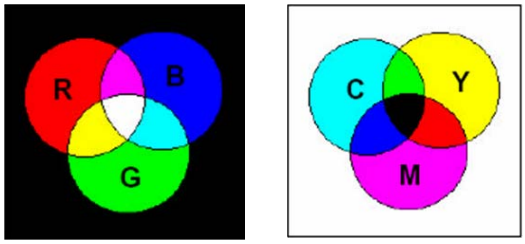
(a) (b) (c)

Fig. 3. An experimental result: (a) and (b) meaningless shares for grayscale image and (c) stacked image.

When dealing with the grayscale image, it is always firstly changed into the halftone one. Moreover, the transformed halftone image is black-and-white only, whose format is quite suitable for generating the shares of visual cryptography. Therefore, in the method of Hou[15], the grayscale image is at the beginning transformed into the halftone one, and then the shares for gray-level images are generated.

After the grayscale image is converted into a black-and-white halftone one, each black or white pixel is extended into 2×2 blocks for the two transparencies following the principles in Fig. 1. Along with this course, if the pixel is white, one combination is chosen from the upper two rows randomly to construct blocks in share 1 and share 2. On the other hand, if the pixel is black, one combination is selected from either two rows optionally to form the transparencies in the blocks of both shares. According to this way, each pixel in the halftone image has been decomposed and as a result two transparencies can be generated to share the secret image, which is in the grayscale domain.

Besides, to improve the quality of the reconstructed secret block, Chen *et al*. proposed a (*t*, *t*) VSS scheme for grayscale images in 2007[16]. In their scheme, a secret image is first partitioned into several blocks with size $b = h \times c$ pixels. Then the secret block shall be encoded into *t* share blocks. Based on the concept of pattern density, for each secret block, the dealer can generate *t* share blocks. For example, the patterns with higher density of black pixels can be replaced with darker regions. On the contrary, the patterns with higher density of white pixels can be represented by brighter regions. Thus, the quality of the reconstructed secret block is improved. As is seen, the scheme works out the average intensity of each grayscale block and maps all the possible intensities into the $b/2+1$ levels. For each secret block, the dealer constructs *t* share blocks containing $b/2$ black pixels and $b/2$ white pixels. In succession, each secret block corresponds to a reconstructed secret block with $b/2+v$ black pixels, where $v=0, 1, \cdots, b/2$. The scheme also presents two techniques named histogram width-equalization and histogram depth-equalization. These techniques are utilized to adjust a secret block to its corresponding share blocks. However, when the information is only a small part of the histogram area within the secret image, the loss of the information may occur. Thus, this method is somehow limited on the information detriment issues.



(a) (b)

Fig. 4. Additive and subtractive models: (a) additive model (Monitors) and (b) subtractive model (color printing press).

2.3 Meaningless Shares for Colorful Images

Seeing to the advantages of visual cryptography, it is needed to apply this method to the colorful images instead of the binary image only to achieve a more efficient mechanism and enhance the wide usage of this technique. Hou has proposed the method for visual cryptography in 2002, which focuses on the decomposition colorful images[15].

The additive and subtractive models shown in Fig. 4 are used to describe the constitutions of colors in the method of Hou[15]. In the additive system, the primaries are red, green, and blue (RGB), while in the subtractive model, colors are represented by applying the combinations of colored-lights just reflected from the surface of a certain object.

As human eyes cannot identify color pixels which are too tiny, the nearby color pixels shall be mixed up in the view of human eyes and form an average color. Since the halftone and color-decomposition techniques can be used to display various colors, Hou offered a scheme for color visual cryptography construction. In the method, every pixel of a halftone image is expanded into a 2×2 block on two sharing images, and the block is filled with cyan (C), magenta (M), yellow (Y), and transparent color, respectively. Referring to these four colors, two stacked images can generate various colors with different permutations. As is seen in Table 4, the distribution of colors in share 1 and share 2 of the first row is the same, thus the human vision perception can mix up and equalize the effect of the four stacked pixels mentioned above. Subsequently, a white-like color is laid out. As to the color intensity, cyan, magenta, and yellow, each occupies a quarter of the block, saying (1/4, 1/4, 1/4).

Besides, share 1 and share 2 of the second row exchange the positions of cyan and transparent color to reveal two cyan pixels: one magenta pixel and one yellow pixel within the four pixels after stacking. Therefore, the color intensity is (1/2, 1/4, 1/4), showing a cyan-like color. We can follow the construction rule shown in Table 4 to select a distribution of colors for generating the blocks in share 1 and share 2 to obtain two colorful shares. After stacking the two shares, a secret image can be gained, whose color intensity is able to range from (1/4, 1/4, 1/4) to (1/2, 1/2, 1/2). The experimental result is shown in Fig. 5.

Table 4: Colorful shares for visual cryptography

Stacked color (C, M, Y)	Share 1	Share 2	Stacked image	Procedure	Stacked result	Color intensity
(0, 0, 0)				The same permutetion for Share 1 and Share 2		(1/4, 1/4, 1/4)
(1, 0, 0)				Exchange cyan and transparent color for Share 2		(1/2, 1/4, 1/4)
(0, 1, 0)				Exchange magenta and transparent color for Share 2		(1/4, 1/2, 1/4)
(0, 0, 1)				Exchange yellow and transparent color for Share 2		(1/4, 1/4, 1/2)
(1, 1, 0)				Exchange cyan and magenta for Share 2		(1/2, 1/2, 1/4)
(0, 1, 1)				Exchange yellow and magenta for Share 2		(1/4, 1//2, 1/2)
(1, 0, 1)				Exchange cyan and yellow for Share 2		(1/2, 1/4, 1/2)
(1, 1, 1)				Exchange two in pair for Share 2		(1/2, 1/2, 1/2)

(a) (b) (c)

Fig. 5. Experimental result: (a) and (b) meaningless colorful shares and (c) the stacked image.

Furthermore, when considering the security of the system, we can see that there are 3! = 6 combinations of each color distribution within a 2×2 block on share 1, which then can be used as the basis for generating the corresponding share 2 in turn. As for a 512×512 secret image, the probability for figuring out the real content is $1/2^{20.585}$. This has led to the fact that it is difficult to crack visual cryptograms, so that the robust transmission of the data files on the Internet can be guaranteed.

Owing to this efficient mechanism in the colorful image domain, two meaningless transparencies can be stacked together to generate the secret image as in Fig. 5 without complex computation. As a result, this technique can be used to protect the authorization of certain art works or digital materials by embedding the shares into them. Moreover, with various colors within the images increasing the vision enjoyment, this technique has already been employed on the entertainment affairs, such like games and movies, which attract lots of human beings.

2.4 Meaningless Shares for Progressive Images

The secret images are not allowed to be viewed progressively in the traditional visual cryptography, for the secret images concerned in the previous methods are generally the one-meaning secret images, whose viewing system can only output either complete recovered-view images or with-nothing-but-noise ones. However, the one-meaning secret images are not suitable within all the fields in reality. Sometimes the secret images are slightly sensitive, while they still need to be recovered frequently, thus the progressive method is required to show the secret step by step. To make up the inconvenience of the traditional visual mechanism, the progressive method for visual cryptography is brought forward to achieve that each time one more share is stacked the secret image can be clearer on different levels. By offering the fuzzy viewing, Fang and Lin[2] as well as Jin *et al.*[17] proposed progressive mechanisms for viewing the secret image step by step on different levels, the result of which is shown in Fig. 6.

This study employs a 256×256 half-tone image as the input image, where the threshold n is set to 6. In succession, a user who can collect all transparencies without doubt is able to reveal the content of original half-tone image. On the contrary, the participant who only owns a single transparency and has no access to other transparencies from

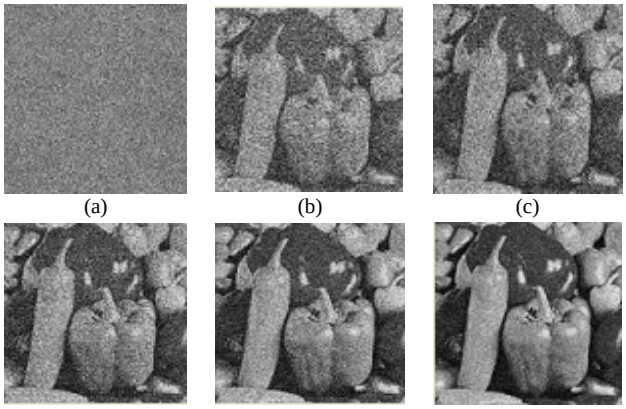


Fig. 6. Progressive mechanisms for viewing the secret image step by step on different levels: (a) meaningless share, (b) two shares, (c) three shares, (d) four shares, (e) five shares, and (f) six shares.

any other participants cannot obtain the original secret image. Conversely, if the user is able to collect several transparencies from other participants, then the stacked result develops progressively along with the increasing numbers of the stacked shares.

In the method of Jin[17], the shares are revealed by each resolution layer to construct a hierarchical structure. Thus the secret image of different resolutions can be restored by stacking the different numbers of shares. In this way, the decryption process is flexible enough to achieve the sensitive image recovering. Considering this method, it is divided into three parts. Firstly, the original images are converted into the grayscale images on the purpose of enabling applying the traditional visual cryptography here. Secondly, the grayscale/color space is transformed to the monochrome space, which guarantees the perfect restoration of the original image. Finally, the multi-resolution mechanism is employed to decrypt images of varying quality.

In the traditional (k, n) visual cryptography, the secret image of single resolution is constructed only when the number of shares that are available just meets the threshold k. Evenly, if more than k shares are stacked, it does not add any new information to the revealed image. However, in the new progressive one, not only the reconstructed image is built by stacking the threshold number of shares, but also the resolution of the final image is enhanced by adding the other images.

Generally, shares are created randomly in order to obtain the maximum security. In the scheme of Jin[17], a single share is allowed to be shared across, while still retains the security request. This is really useful when a set of images requires to be shared and the security has to be guaranteed firmly. In this method, each pixel of the secret image is expanded into 4 sub-pixels for each share. Based on the $(2, 2)$ visual cryptography scheme or other extensions, including common share visual cryptography methods or perfect visual cryptography methods, the multi-resolution visual cryptography is realized. At first, n shares are created, among which one is picked in advance to act as the common share for the latter resolution. Then any of the n–1 shares remained together with the common share is used to reconstruct the secret image at a certain resolution. Within the (2, n) method, I denotes the secret image, while S_c is the common share. Therefore, given any k for k =0, 1, ···, n–2, I^k is gained by stacking S_c and S_k together, where I^k denotes I with different quality. That is to say, $\text{Resolution}(I^0) \le \text{Resolution}(I^1) \le, \cdots, \text{Resolution}(I^{n-2}) \le \text{Resolution}(I)$, which means that with the addition of shares, the stacked image can be meaningful with growing quality. What is more, for other secret images, the common share S_c can still be used to generate the embedded private image in this system. Therefore, a mechanism that displays sensitive images by advancing gradually is provided.

Under this environment, the secrets that are needed to be revealed frequently or sensitively in some cases can be extracted referring to this method. For example, in the message concealment and identification domains, if the secret image is only needed by some of the group members, the progressive mechanism can offer a chance for revealing the secret just with low quality, which can still be figured out anyway. Compared with the traditional complete one-meaning secret image mechanism, the progressive one furnishes a more flexible and convenient system for sharing secret securely.

3. Visual Cryptography for Meaningful Shares

Even the visual cryptography can enjoy various advantages such as the low computation, free from the complex cryptography theories, and the without-key mechanism, its shares which are meaningless shall be suspicious to invaders. Thus, this technique can experience the malicious attacks, and the shares may be destroyed by the attackers. Therefore, instead of the noise-like shares, the meaningful shares are in great need to protect the security of the transmitted images. Owing to the steganography technique, which offers a way of secure protection for digital image, the meaningful shares are proposed to prevent malicious attackers from suspecting about the delivered image. It is achieved by embedding secret image in pre-selected meaningful ones called camouflage images.

3.1 Meaningful Shares for Binary Images

To deal with the meaningful shares for binary images in case of malicious attacks coming from the noisy shares, Hsu *et al*. proposed a screen based method to achieve this target[18]. The scheme is composed of three steps: the generation of basic screen blocks, the generation of screen

block group, and the generation of screen images. During the whole process, the basic screen pairs are firstly obtained and then the target screen block is revealed. In succession, the secret image is combined with the target screen blocks to engender the final stego-image.

In the mechanism of Hsu *et al.*, the first screen block of size $m \times m$ is selected as S_1 from a pool of screen blocks for generating a pair of basic screens. Note that the initial screen is always designed with a character that larger threshold values intersect with smaller ones for consideration of good image quality. Referring to this interleaving structure, it is helpful to generate uniformly distributed white and black pixels in order to show good quality of resultant images. By exploiting this property, the two basic screen blocks are combined to generate extended screen blocks of size $2m \times 2m$. The extended blocks can be used to screen a cover image to perform secret embedding. At last, for a given group of extended screen blocks and a secret message, which is embedded into a cover image to make up the share, a secret-dependent screen image with the size that is the same as the cover one shall be generated. Then based on the traditional visual cryptography, the meaningful binary shares are gained, and the experimental results are given in Fig. 7.

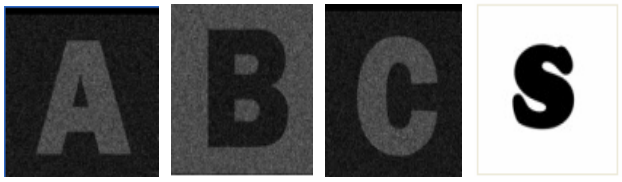
Considering the convenience of the decoding process and binary images, the visual cryptography with meaningful shares can be applied to the authentication for the wireless communication, Internet verification, and other registration phases. It could be quite efficient because of its freedom of the password transferring, the special equipment, and the complicated decoding algorithm or steps. What is more, more contributions can be achieved by enlarging the capacity of the secret images within this mechanism.

3.2 Meaningful Shares for Grayscale Images

Seeing to the wide applications of the grayscale images, ensuring the meaningful shares to be applied to the visual cryptography in the grayscale domain is in demand. In 2003, Lin and Tsai[10] proposed a method to achieve this requirement faultlessly. Based on the previous mechanism of the visual cryptography, whose shares are meaningless, the new method can refer to a cover image to generate the meaningful shares by combining it with the original shares. As shown in Fig. 8, the secret "FCUCSIE" can be figured out by stacking the shares which are meaningful by embedding the cover image.

The embedding rule is stated in Table 5, in which the varying process of stacked images with shares is illustrated in detail.

Along with the characters of the cover image and the embedding rules, the meaningful shares are then obtained. In Fig. 9, an example is taken to demonstrate the whole mechanism of generating meaningful shares. As it is seen, firstly the sub-blocks of the meaningless original share, which have been extended, are compared with those of the cover image. If it is "1" in the meaningless original share, then the corresponding block is set to be the same value with the cover image. Otherwise, if it is a "0" in the original share block, then the corresponding block of the final share is still 0.



(a) (b) (c) (d)

Fig. 7. Experimental results of the mechanism of Hsu *et al.*: (a), (b), and (c) the meaningful binary shares and (d) the stacked result image.

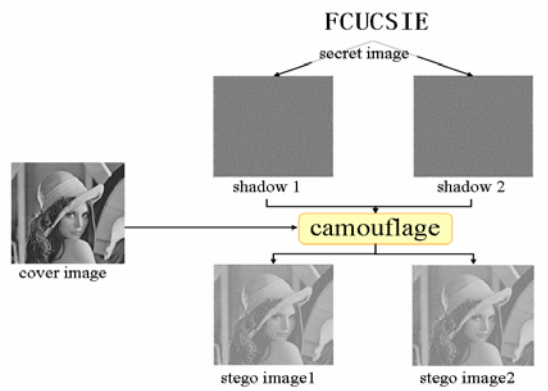


Fig. 8. Meaningful shares for grayscale image.

Table 5: Rules of stacking images

Secret image	Share 1	Share 2	Stacked image

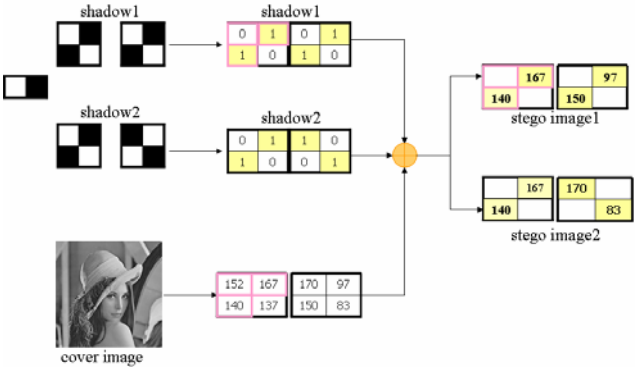


Fig. 9. Construction of meaningful shares.

(a) (b) (c)

Fig. 10. Embedding of the intended cover image: (a) and (b) the grayscale shares and (c) the stacked image.

After the embedding of the intended cover image, shares of the secret images are represented as meaningful ones in the grayscale domain. It is obvious that, by applying the construction method, the secret image is preserved well all the same, the effect of which is shown in Fig. 10.

Furthermore, most of the previous (*t*, *n*) VC techniques can not reveal the secret completely. Recently, Lin and Chan[19] have proposed a visual cryptography method which achieves reversibility. It means whenever the involved participants collect *t* shares, the secret as well as the cover image can be reconstructed without any distortion. More securely, the scheme allows dealer to derive a set of *n* meaningful shares by employing the concept of steganography techniques.

In Lin and Chan's scheme, given a secret image, the dealer firstly converts it into an *m*-based representation. Without loss of generality, *m* can be chosen as 7. To reconstruct the cover image, for each pixel p_i of the cover image, dealer computes

$$d = p_i \bmod m .$$

Afterwards, the secret digits and parameter *d* are used as coefficients of the polynomial function:

$$F(x) = (s_1 + s_2 x^1 + \cdots + s_{t-1} x^{t-2} + d x^{t-1}) \bmod m$$

where s_1, s_2, …, s_{t-1} are the (*t*–1) secret digits. Therefore, the shares can be constructed by feeding secret keys k_i into $F(x)$, where $y_1=F(k_1)$, $y_2=F(k_2)$, ⋯ , and $y_n=F(k_n)$.

Since the embedding step may decrease the quality of camouflage images, dealer needs to perform the quantized step, in which dealer firstly computes the quantized value:

$$Q = \lfloor p / m \rfloor \times m .$$

After that, dealer adds the quantized value and data y_i to obtain the camouflage images by the equation

$$p_i = Q + y_i .$$

In the revealing process, involved participants collect *t*-out-of-*n* shares to gain the secret image, reconstruct the cover image, and derive the polynomial function $F(x)$ from the camouflage images. In succession, the participants obtain the share y_i' by computing $y_i' = p_i' \bmod m$, and the secret image can be extracted from the (*t*–1) coefficients of $F(x)$. To obtain the pixel of the cover image, involved participants need to apply the quantized step to compute value *Q* firstly:

$$Q = \lfloor p_i' / m \rfloor \times m .$$

Consequently, the pixel of cover image is restored by employing the equation:

$$p_i = Q + d.$$

To avoid the suspicions of malicious attackers, which are caused by the noise-like shares, the meaningful shares can enhance the security of the whole secret transferring process. Thus, this method can be made use of in the identification and key management domains, during which the shares cannot avoid being seen by others.

3.3 Meaningful Shares for Colorful Images

Besides the images themselves, the color can also deliver more information in certain cases. Therefore, it is indeed necessary to make full use of the colorful images to transfer secret images among a group of people, which requests the application of meaningful shares for colorful images.

In 2008, Wu *et al*. proposed a color visual cryptography scheme to generate meaningful shares[20]. To achieve the secure process, the meaningful shares are produced to avoid arousing the attention of hackers. In the proposed scheme, halftone technique, cover coding table, and secret coding table are utilized to generate two meaningful shares. There are four main procedures in this scheme. The first one is color halftone transformation, where the color image is transformed into a colorful halftone image. The second procedure is the pixel extraction process, where the pixels are retrieved from the color halftone image. Following it, there come the encoding and decoding procedures, respectively. On the purpose of generating shares, two $N\times N$ cover images are employed to encode the $N\times N$ secret image and make two $2N\times 2N$ shares called share 1 and share 2. As it is concerned, share 1 is a meaningful share that appears just like the cover image 1, while share 2 is a meaningful share similar with the cover image 2. In the last, within the decoding procedure, the secret image can be easily figured out by stacking share 1 and share 2. Furthermore, in this scheme, there are two coding tables referred to in the encoding procedure, naming the cover coding table and the secret coding table. The cover coding table is responsible for the encoding process of cover image; on the other hand, the secret coding table is used to encode the secret image. Moreover, the secret coding table works in a color recognition way. For example, if one pixel of the transferred halftone image is green, then the ratio of pixel color must be 100%, 0%, and 100% for C, M, and Y, respectively. By this way, each block in share 1 comes as the permutation of pixels: cyan, magenta, yellow, and white.

Subsequently, the above rules are applied, and the coding table is used to produce block of share 2, where the permutation of the pixels is yellow, magenta, cyan, and white. When all the pixels have been processed, two shares are produced faultlessly. Each block of the two shares consists of C, M, Y, and W. Therefore, the secret image can be rapidly recognized according to the human visual system when the two shares are stacked.

The experimental results in Fig. 11 display the secret image obtained when stacking the two color meaningful shares. Following the illustrated mechanism offered by Wu *et al.*, the visual cryptography system is made up, which demonstrates that the meaningful-share-scheme for colorful images is perfectly applicable and can build a high secure environment for the digital world.

Additionally, seeing to the attracting colorful images coming out as friendly to persons, this method has been widely used to make vision games or movies with high quality to entertain human life as well as accelerate the development of business affairs.

3.4 Meaningful Shares on Progressive Visual Cryptography

Here the method with meaningful shares for progressive visual cryptography is introduced to simplify the management of the shares and enhance the security of the secret image[21]. Fang proposed a mechanism of generating meaningful shares for progressive visual cryptography in 2007 based on the cover-image-embedding concept, which is illustrated in Fig. 12.

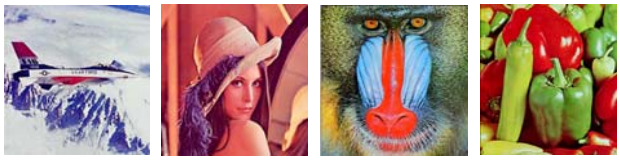


Fig. 11. Secret image obtained by stacking the two color meaningful shares: (a), (b), and (c) the meaningful shares for color images; (d) the stacked image.

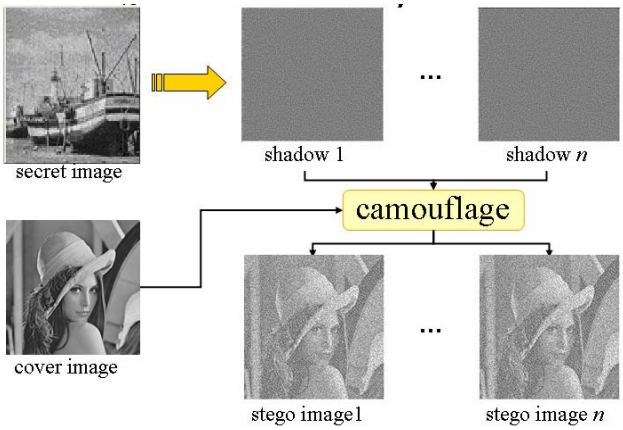


Fig. 12. Construction of meaningful shares for progressive mechanism.

Within this proposed method, there are two phases, of which the first one expands the original image, thus every pixel corresponds to a 2×2 block. That is to say, if the size of the original image is 256×256, then the size of the expanded one is 512×512. Referring to Table 2, if the pixel value is black, then all pixels of the corresponding block are black; on the contrary, if the pixel is white, the corresponding block contains two white and two black pixels. After finishing this, the second phase of creating shares is carried out. In this process, each block of shares is generated by checking the stego-image.

As it is deduced in Table 6, $S(x, y)$ denotes the pixel with coordinate (x, y) of the secret image, which is defined as white and black. While S' represents the real type of the homologous pixel. $C(x, y)$ shows the type of the cover image, which is classified as white and black. Then P_i provides the choices for the corresponding combination of the secret and cover images. For example, if the secret pixel value is black and the cover image pixel value is white, the block type can be randomly selected just by satisfying the fourth column P_i.

Table 6: Possibilities for paring the share pattern

$S(x, y)$	S'	$C(x, y)$	P_i
B	(1, 1, 1, 1)	B	(1, 1, 0, 0)(1, 0, 1, 0)(1, 0, 0, 1) (0, 1, 1, 0)(0, 1, 0, 1)(0, 0, 1, 1)
		W	(0, 0, 0, 0)(1, 0, 0, 0)(0, 1, 0, 0) (0, 0, 1, 0)(1, 1, 0, 0)
W	(1, 1, 0, 0)	B	(1, 1, 0, 0)
		W	(0, 0, 0, 0)(1, 0, 0, 0)(0, 1, 0, 0)
	(1, 0, 1, 0)	B	(1, 0, 1, 0)
		W	(0, 0, 0, 0)(1, 0, 0, 0)(0, 1, 0, 0)
	(1, 0, 0, 1)	B	(1, 0, 1, 0)
		W	(0, 0, 0, 0)(1, 0, 0, 0)(0, 0, 1, 0)
	(0, 1, 1, 0)	B	(0, 1, 1, 0)
		W	(0, 0, 0, 0)(0, 1, 0, 0)(0, 0, 0, 1)
	(0, 1, 0, 1)	B	(0, 1, 0, 1)
		W	(0, 0, 0, 0)(0, 1, 0, 0)(0, 0, 0, 1)
	(0, 0, 1, 1)	B	(0, 0, 1, 1)
		W	(0, 0, 0, 0)(0, 0, 1, 0)(0, 0, 0, 1)

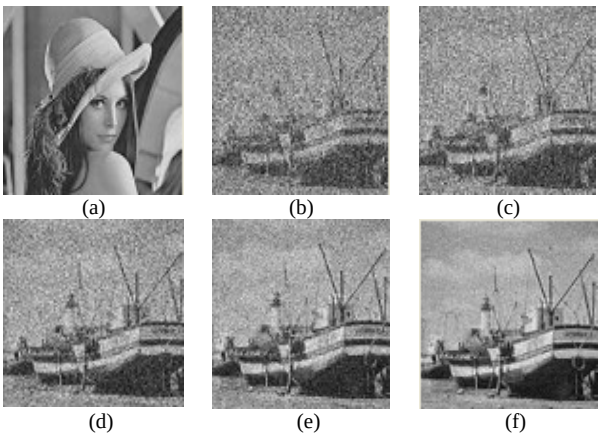


Fig. 13. Experimental result comparison: (a) the meaningful share and (b), (c), (d), (e), and (f) the progressive stacked images.

Compared with the previous method for progressive visual cryptography with meaningless shares, this method employing the meaningful shares can withstand the malicious attacks coming from the suspicious invaders caused by the noise-like shares. Following this mechanism, the meaningful shares can moreover be used to generate the secret step by step without being influenced by the cover image itself. The experimental result is shown in Fig. 13, demonstrating that the progressive visual cryptography mechanism with meaningful shares can be achieved perfectly.

By preserving the meaningful shares, no one can easily figure out which is the share and which is the pure image. Therefore, when dealing with the sensitive secret image sharing issues, the secret provider can take this mechanism to reveal the real secret gradually without having to collect all the shares or causing the suspicions of attackers. Corresponding to these advantages, the meaningful shares visual cryptography can be used in the key management, the authorization, and login systems, which can be conveniently and quickly completed by low computation.

4. Conclusions

Owing to the wide applications of the Internet technology, the security of data has become a pivotal factor nowadays. Compared with traditional cryptography methods, the visual cryptography mechanism which is based on the human vision system can achieve low computation and get rid of the complex encryption knowledge. In addition, without perplexing procedure for constructing keys, the visual cryptography method can withstand the danger of losing session keys, brute-force attacks for trying the session keys, and the intercepting attacks which aim at compromising the information for generating keys. Therefore, considering the advantages of this light-weight cryptography method, secret images of binary, grayscale, and colorful ones can be applied to this field to achieve the group keeping mechanism, during which no one can have access to the secret, thus enhancing the security of the transferred data. Seeing to the progressive mechanism, the sensitive secret images can achieve the convenient recovering process without having to gather all the shares together when it is needed to reveal the secret frequently. Along with the characteristics discussed, visual cryptography can be applied to the key management, message concealment, authorization, identification, and entertainment fields. Owing to this efficient and robust mechanism, many complex applications in the past can meet a new age.

References

[1] M. Naor and A. Shamir, "Visual cryptography," in *Proc. of Advances in Eurocrypt 94'*, Perugia, Italy, 1994, pp. 1-12.

[2] W.-P. Fang and J.-C. Lin, "Progressive viewing and sharing of sensitive images," *Pattern Recognition Image Analysis*, vol. 16, no. 4, pp. 638-642, 2006.

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

[4] S.-K. Chen and J.-C. Lin, "Fault-tolerant and progressive transmission of images," *Pattern Recognition*, vol. 38, no. 12, pp. 2466-2471, 2005.

[5] T. Hofmeister, M. Krause, and H. U. Simon, "Contrast-optimal *k* out of *n* secret sharing schemes in visual cryptography," *Theoretical Computer Science*, vol. 240, no. 3, pp. 471-485, 2000.

[6] W.-P. Fang and J.-C. Lin, "Visual cryptography with extra ability of hiding confidential data," *Journal of Electronic Imaging*, vol. 15, no. 2, pp. 1-7, 2006.

[7] A. Shamir, "How to share a secret," *Communications of the ACM*, vol. 22, pp. 612-613, 1979.

[8] Y.-C. Hou, F. Lin, and C.-Y. Chang, "A new approach on 256 color secret image sharing technique," *MIS Reviews*, no. 9, pp. 89-105, Dec. 1999.

[9] G. Ateniese, C. Blundo, A. D. Santis, and D. R. Stinson, "Visual cryptography for general access structures," *Information and Computation*, vol. 129, no. 2, pp. 86-106, 1996.

[10] C.-C. Lin and W.-H. Tsai, "Visual cryptography for gray-level images by dithering techniques," *Pattern Recognition Letters*, vol. 24, no. 1-3, pp. 349-358, 2003

[11] W. Stalling, *Cryptography and Network Security: Principles and Practices*, New Jersey: Prentice Hall, 2010.

[12] R. Lukac and K. N. Plataniotis, "Bi-level based secret sharing for image encryption," *Pattern Recognition*, vol. 38, no. 5, pp. 767-772, 2005.

[13] R. Lukac and K. N. Plataniotis, "Digital image indexing using secret sharing schemes: a unified framework for single-sensor consumer electronics," *IEEE Trans. on Consumer Electronics*, vol. 51, no. 3, pp. 908-916, 2005.

[14] L.-H. Chen and C.-C. Wu, "A study on visual cryptography," *Master Thesis, National Chiao Tung University*, Taiwan, 1998.

[15] Y.-C. Hou, "Visual cryptography for color image," *Pattern Recognition*, vol. 36, no. 7, pp. 1619-1629, 2003.

[16] Y.-F. Chen, Y.-K. Chan, C.-C. Huang, M.-H. Tsai, and Y.-P. Chu, "A multiple-level visual secret-sharing scheme without image size expansion," *Information Sciences*, vol. 177, pp. 4696-4710, Nov. 2007.

[17] D. Jin, W.-Q. Yan, and M. S. Kankanhalli, "Progressive color visual cryptography," *Journal of Electronic Imaging*, vol. 14, no. 3, pp. 1-13, 2005.

[18] C.-Y. Hsu, C.-S. Lu, and S.-C. Pei, "Joint screening halftoning and visual cryptography for image protection," in *Proc. of International Workshop on Digital Watermarking*, Jeju Island, Korea, 2006, pp. 212-225.

[19] P.-Y. Lin and C.-S. Chan, "Invertible secret image sharing with steganography," *Pattern Recognition Letters*, doi:10.1016/j.patrec.2010.01.019, 2010.

[20] H.-C. Wu, H.-C. Wang, and R.-W. Yu, "Color visual cryptography scheme using meaningful shares," in *Proc. of the 8th International Conf. on Intelligent Systems Design and Applications*, Washington, DC, USA, 2008, vol. 3, pp. 173-178.

[21] W.-P. Fang, "Multi-layer progressive secret image sharing," in *Proc. of the 7th WSEAS International Conf. on Signal Processing, Computational Geometry & Artificial Vision*, Athens, Greece, 2007, pp. 112-116.

Chin-Chen Chang received his B.S. degree in applied mathematics in 1977 and his M.S. degree in computer and decision sciences in 1979, both from the National Tsing Hua University, Hsinchu, Taiwan. He received his Ph.D. degree in computer engineering in 1982 from the National Chiao Tung University, Hsinchu, Taiwan. During the academic years of 1980 to 1983, he was on the faculty of the Department of Computer Engineering at the National Chiao Tung University. From 1983 to 1989, he was on the faculty of the Institute of Applied Mathematics, National Chung Hsing University, Taichung, Taiwan. From 1989 to 2004, he has worked as a professor with the Institute of Computer Science and Information Engineering at National Chung Cheng University, Chiayi, Taiwan. Since 2005, he has worked as a professor with the Department of Information Engineering and Computer Science at Feng Chia University, Taichung, Taiwan. His research interests include information security, computer cryptography, data engineering, and image compression. Dr. Chang is a fellow of IEEE, a fellow of IEE, and a member of the Chinese Language Computer Society, the Chinese Institute of Engineers, and the Phi Tau Phi Society.

Bo Li is currently pursuing the degree of Bachelor of Computer Science in Tongji University, Shanghai. Her current research interests include electronic commerce, information security, image processing, and cloud computing.

Jung-San Lee received the B.S. degree in computer science and information engineering in 2002 and the Ph.D. degree in computer science and information engineering in 2008, both from National Chung Cheng University, Chiayi, Taiwan. Since 2008, he has worked as an assistant professor with the Department of Information Engineering and Computer Science at Feng Chia University, Taichung, Taiwan. His current research interests include electronic commerce, information security, image processing, and mobile communications.