Visual Cryptography for General Access Structure Using Pixel-block Aware Encoding

Haibo Zhang
[1]College of Computer Science and Technology, Harbin Engineering University, Harbin, Heilongjiang, 150001, China
[2]Wuhan Digital Engineering Institute, Wuhan, Hubei, 430074, China
Email: zhanghb412@yahoo.com.cn

Xiaofei Wang, Wanhua Cao and Youpeng Huang
[1]College of Computer Science and Technology, Harbin Engineering University, Harbin, Heilongjiang, 150001, China
[2]Wuhan Digital Engineering Institute, Wuhan, Hubei, 430074, China

***Abstract*—Multi-pixel encoding is an emerging method in visual cryptography for that it can encode more than one pixel for each encoding run. Nevertheless, in fact its encoding efficiency is still low because of that the encoding length is invariable and very small for each run. This paper presents a novel multi-pixel encoding called pixel-block aware encoding. It scans the secret image by zigzag and perceives a pixel block with as many pixels as possible to encode for each run. A pixel-block consists of consecutive pixels of same type during the scanning. The proposed scheme has advantage in encoding efficiency over single-pixel encoding and other known multi-pixel encoding methods. Furthermore, this scheme can work well for both threshold access structure and general access structure and well for both gray-scale and chromatic images without pixel expansion. The experimental results also show that it can achieve good quality for overlapped images.**

***Index Terms*—Visual secret sharing (VSS), general access structure, multi-pixel encoding, pixel-block aware encoding, zigzag scanning**

I. INTRODUCTION

In 1994, Naor and Shamir [1] first presented a novel secret sharing scheme called visual cryptography that differs extremely from the traditional cryptography. It divides a black-white image into n shares. Among those shares, any k or more ones are stacked and then a discernable image appears; otherwise any less than k ones together can reveal nothing about the original secret. The advantages of this visual secret sharing (VSS) scheme are very clear in that those complex computations needed in traditional cryptography are redundant and the decryption even does not need any knowledge of cryptography or any help with computer; it only depends on the humankind's visual system.

A. The Model of VSS

Usually we assume that the secret image is composed of a collection of black and white pixels. The model of VSS consists of two phases: (1) distribution and (2) reconstruction. At the first phase, the secret image is encoded pixel by pixel into n shadows and then distributed to n participants. Generally, a pixel of the original image is encoded into m black and white sub pixels of each shadow. Those sub pixels are printed in close proximity to each other, so that the human visual system averages their individual black/white contributions and a gray level forms. Usually two basis matrices, M_0 and M_1, are required to encode the secret image. They are both the $n \times m$ Boolean matrix $M = [a_{ij}]$ where $a_{ij} = 1$ if and only if the j-th sub pixel in the i-th shadow is black, otherwise $a_{ij} = 0$. When encoding a white (resp. black) pixel in the secret image, the dealer randomly permutes the columns of M_0 (resp. M_1), and then chooses the i-th row of the permuted matrix to fill into the corresponding positions of the i-th shadow. After all pixels in the secret image are encoded, n shadows are formed. Obviously, each shadow has the size m times as that of the original image. Therefore, we call the parameter m pixel expansion.

At reconstruction, any k or more shadows are stacked, and then a secret image with gray level is reconstructed. The gray level is proportional to the Hamming weight of the ORed m-vector V, which is usually denoted as $H(V)$. This gray level is interpreted by the visual system of the users as black or as white according to some rule of contrast. Generally, in the reconstructed image, if $H(V) \geq (m - l)$, the gray level is interpreted by our visual system as black, and $H(V) \leq (m - h)$ as white, where h and l are the whiteness of the white and black secret pixel such that $m > h > l \geq 0$ [2]. Especially, if $l = 0$ in a VSS scheme, a black secret pixel is totally reconstructed by m black sub pixels, so we call it perfect black VSS scheme.

B. Related Works

After the Naor-Shamir VSS scheme appears, many related researches and some extended VSS schemes come forth. Some of which can be used for gray-scale or chromatic images [3, 4 and 5], general access structure [5 and 6], ideal contrast [7], cheating immune [8 and 9], anonymity [10] and multiple images hiding [6, 11 and 12]. However, all these schemes introduce pixel expansion, which leads to an expansion even distortion of the

revealed image; meanwhile, more storage capacity and more transmission delay are needed for shares.

In order to overcome above-mentioned disadvantages, many researches aim at non-expanded schemes. Bai [13] proposed such scheme based on random number concept, but its shortcoming is clear in that it is only suitable for (n, n) threshold access structure. Ito et al. [14] put forward another non-expanded scheme that is suitable for (k, n) threshold structure. However, the quality of stacked image is very poor and there needs complex encoding and operations when it extends to encode gray-scale or chromatic images. A similar scheme proposed by Hou et al. [15] improves the quality of revealed image, but it only can be utilized to encrypt gray-scale images.

C. Multi-pixel Encoding Methods

No matter that the pixel expansion exists in all above-mentioned schemes or not, they all use so-called single-pixel encoding method by which there is only one pixel can be encrypted at each encoding run. It is obvious that the encoding efficiency is very low for such methods. In 2004, Hou et al. [16] first proposed a multi-pixel encoding method by which at each run there are m consecutive pixels joining encoding, where m is pixel expansion and equal to the number of columns of the basis matrix. Despite the improvement for encoding efficiency, this scheme exhibits poor quality of stacked image for most access structures other than (2, 2) threshold access structure. Afterwards, they proposed another multi-pixel encoding method in [17] to win an improvement for the quality of revealed image. This scheme also encodes m pixels at each run nevertheless the m pixels are of same type. On the other hand, it has disadvantages that less than m consecutive same pixels in the input sequence induce the encoder to trace backward or forward so as to collect just m pixels of same type for one run and that more than m consecutive same pixels induce the redundant parts need to stay for the next run.

The common feature of the multi-pixel encoding schemes in [16 and 17] is that the length of the encoded pixels for each run is a constant value m. In fact, this feature leads to two shortcomings. On one hand, the parameter m is pixel expansion and hence the value of m is usually limited into a very small range, which implies that the actual improvement of encoding efficiency is not attractive. On the other hand, it is a usual thing in applications that the number of the consecutive pixels of same type in a meaningful image is remarkably larger than the value of m. This means that the fixed value of m is not preferably suitable for the real cases of the input sequence.

D. General Access Structure

Actually, an access structure is a rule, which defines how to share a secret. The most familiar examples are (n, n) and (t, n) threshold access structures. A (t, n) threshold access structure rules that any t or more out of n participants can cooperate to reveal the secret image and any less than t participants together get nothing about the secret image. Obviously, a (n, n) threshold access structure is one instance of the (t, n) threshold access structure. It demands all participants to cooperate for a secret recovery and hence nothing can be seen even if only one attendee is absent. It is easy to know that a (t, n) threshold access structure is tolerant because the final secret still can be restored from the other t shares even though up to ($n - t$) shares are corrupted.

However, threshold access structure is only one special case of the so-called general access structure. Usually, a general access structure is denoted as $\Gamma = \{\mathcal{A}_0, \mathcal{A}_1\}$, where $\mathcal{A}_0$ and $\mathcal{A}_1$ are sets of subsets of all participants and $\mathcal{A}_0 \cap \mathcal{A}_1 = \varnothing$. Furthermore, $\mathcal{A}_0$ denotes a collection of forbidden sets and $\mathcal{A}_1$ denotes a collection of qualified sets. It is easily known that stacking all the shares held by the participants of any qualified set can recover the secret image; but stacking all the shares held by the participants of any forbidden set cannot reveal any information about the secret image. For example, in a system with four participants, we let $\mathcal{A}_1$ = {{1, 2}, {2, 3}, {3, 4}, {1, 2, 3}, {1, 2, 4}, {1, 3, 4}, {2, 3, 4}, {1, 2, 3, 4}}, which implies that $\mathcal{A}_0$ = {{1}, {2}, {3}, {4}, {1, 3}, {1, 4}, {2, 4}}. Therefore, we can learn that stacking share 1 and share 2 can recover the secret image; however, stacking share 1 and share 4 can reveal nothing about the secret image.

It is easy to know that a general access structure should follow the monotone property: if $\gamma \in \mathcal{A}_1$ and $\gamma \subseteq \gamma'$, then $\gamma' \in \mathcal{A}_1$; if $\lambda \in \mathcal{A}_0$ and $\lambda \supseteq \lambda'$, then $\lambda' \in \mathcal{A}_0$. So we can learn that the fact $\{1, 2\} \in \mathcal{A}_1$ implies it is truly sure that $\{1, 2, 3\} \in \mathcal{A}_1$, $\{1, 2, 4\} \in \mathcal{A}_1$ and $\{1, 2, 3, 4\} \in \mathcal{A}_1$; the fact $\{1, 4\} \in \mathcal{A}_0$ implies that $\{1\} \in \mathcal{A}_0$ and $\{4\} \in \mathcal{A}_0$. Furthermore, we also can let $\mathcal{A}_1^-$ = {{1, 2}, {2, 3}, {3, 4}} and $\mathcal{A}_0^+$ = {{1, 3}, {1, 4}, {2, 4}} to represent above mentioned $\mathcal{A}_1$ and $\mathcal{A}_0$ respectively in terms of the monotone property. In fact, $\mathcal{A}_1^-$ is usually named the family of minimal qualified sets and $\mathcal{A}_0^+$ is the family of maximal forbidden sets. In many situations, it is more convenient to refer to them instead of $\mathcal{A}_1$ and $\mathcal{A}_0$.

E. Our Contributions

In this paper, we propose a new multi-pixel encoding method called *pixel-block aware encoding*, which can encode variable number of pixels for each run. For those known encoding schemes including both single-pixel and multi-pixel encoding ones, how to scan the secret image is totally excluded from consideration and row-by-row scanning is taken for a natural thing without a moment's thought. However, a well-chosen scanning mode will bring us a better profit. In this novel scheme, we pay attentions to the choosing of scanning mode and adopt zigzag scanning for it. For most images, a zigzag scanning is more suitable to reveal the space relationships of pixel organization and hence producing a cluster of more pixels with same type. In this scheme, the encoding length at each run is equal to the size of the cluster, in other words, to the length of the consecutive same pixels during scanning the secret image. Additionally, tracing

backward or forward is redundant in this scheme. Therefore, the proposed scheme has advantages in encoding efficiency over single-pixel encoding and other known multi-pixel encoding methods. Furthermore, this scheme is a non-expansive encoding scheme. The experimental results demonstrate that it can work well for both threshold access structure and general access structure and work well for both gray-scale and chromatic images.

F. Organization of This Paper

The rest of this paper is organized as follows. Firstly, section 2 discusses different ways to scan an image, gives a description of the novel encoding method and analyzes the security as well as complexity of this scheme. Subsequently, section 3 illustrates how to apply the proposed scheme to chromatic images under the control of general access structure. At the same time, three experimental results are shown in section 4. The first one is for the comparison of the proposed scheme with other typical schemes; the second one is an application of this novel scheme to chromatic image and general access structure; the third one is a statistics about the contributions of different scanning modes. At last, section 5 concludes our works.

II. THE PROPOSED SCHEME

Generally, we suppose the basis matrices M_0 and M_1 are used to encode white and black pixels, respectively. They have the same dimension $n \times m$. Suppose the secret image is SI with $L \times H$ pixels and the n share are S_1, S_2, …, S_n, respectively. In gray-scale or chromatic images, the white pixel usually means *blank* and black pixel means *non-blank*.

A. Scanning Mode

During the encryption of a secret image, the encoder needs to scan one or more pixels in the original image and then encrypts them for each encoding run. Usually, we are accustomed to scanning an image row by row and indeed pay no attention to the fact that an alternative scanning mode maybe exist.

In the proposed scheme, we first focus on the analysis and choosing of scanning mode. It is easy to know that the secret image to be encrypted is usually a significant image, which means that there exist some relationships among pixels of the secret image. If an encoder gives further consideration on those relationships, it will obtain a better adaptability. For example, a more adaptable scanning mode will bring more pixels to be encoded for one run and hence a higher encoding efficiency is easily returned. Here we mainly consider three scanning modes as follows.

(1) Row-by-row scanning: it is the most used scanning mode. It scans the pixels along a row of an image and then scans along the next row. A fact is obvious that this scanning mode is very suitable for those images with plenty of horizontal stripes;

(2) Column-by-column scanning: this mode scans the pixels along a column of an image and then scans along the next column. It is clear that this scanning mode is very suitable for those images with plenty of vertical stripes;

(3) Zigzag scanning: its scanning order is shown in Fig. 1. It is very different from above two scanning modes that at most situations the next pixel to be scanned is adjacent to the current one with both different row and different column. Therefore, to some extend this scanning mode can be suitable for more kinds of images. It is noticeable that an image is not always square. When it is rectangular, the zigzag scanning will still work well.

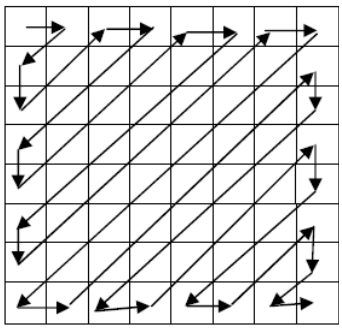


Figure 1. Zigzag scanning order

For a comprehensive consideration, our proposed scheme will adopt zigzag scanning mode to scan the original image.

B. Encoding

Same to the traditional Naor-Shamir scheme [1], the proposed scheme also includes two phases: distribution and reconstruction. At reconstruction phase, the thing is very simple that we only need to stack those legal shares and thereby the secret image is revealed. Therefore, we only give the distribution description shown in Fig. 2.

C. Security

Here we give the following theorems to show the security of the proposed scheme.

Theorem 1. The security of the proposed scheme is equivalent to that of the traditional Naor-Shamir scheme.

Proof. In the traditional Naor-Shamir scheme [1], one pixel in secret image is mapped into m sub pixels for each share. In the proposed scheme, for each run, the pixels to encode are same and can be divided into some pixel blocks with length of m. We suppose the real length of every block is b, so there are two cases:

(1) if $b = m$, the pixel block can be regarded as one entire "pixel" and mapped into m sub pixels for each share. The mapping method in this situation is same to that of the Naor-Shamir scheme and accordingly the security is equivalent to that of Naor-Shamir scheme;

(2) if $b < m$, we can first encode this block into m sub pixels, and then pick out the front-standing b sub pixels as the final mapped code. We have known that those m sub pixels have enough security, so the part of them, namely the b sub pixels, is also secure; otherwise, if the part is not secure, the entireness including it is certainly not secure too. This means that the traditional Naor-Shamir scheme is insecure. However, the Naor-Shamir

scheme is secure; accordingly, the security of the proposed scheme is also equivalent to that of Naor-Shamir scheme in this situation.

The proof is completed.

INPUT: SI with $L \times H$ pixels; M_0 and M_1 with size of $n \times m$, respectively.
OUTPUT: $S_1, S_2, \ldots, S_n$ with $L \times H$ pixels, respectively.
step1: scan the secret image SI using zigzag mode till meeting different pixel or reaching the end of SI, and then two values are known: r, the span of this run, and p, the pixel type. There is $p = 0$ for white pixel, otherwise $p = 1$.
step2: $\boldsymbol{L} = \emptyset$;
step3: while ($|\boldsymbol{L}| < r$)
{
step3.1: randomly rearrange (1, 2, …, m) and write the result as ($l_1, l_2, \ldots, l_m$);
step3.2: $\boldsymbol{L} = \boldsymbol{L} \,||\, (l_1, l_2, \ldots, l_m)$; /* "||" means vector concatenation operation */
}
step4: if ($|\boldsymbol{L}| > r$)
{
step4.1: truncate the tail of $\boldsymbol{L}$ to make sure that $|\boldsymbol{L}| = r$;
}
step5: fill the pixels at line i and the columns indicated by $\boldsymbol{L}$ of M_p into S_i, where $i = 1, 2, \ldots, n$, using the same mode during scanning.
step6: if scanning does not reach the end of SI, go to *step1*; otherwise terminate.

Figure 2. Algorithm of pixel-block aware encoding

Theorem 2. The security of the proposed scheme has nothing to do with the scanning or fill-in mode.

Proof. The proposed scheme does three things — scanning, encoding and fill-in — to finish the encryption for an image. The encoder first scans the input image in order to fetch the pixels, which are encrypted and then filled in each share to form a new image. Therefore, it is easy to learn that the encryption only acts on those pixels no matter how they organize as long as the way to fill-in is same to the way to fetch. In other words, the encryption only occurs during the pixel encoding procedure and pays no attention to the positions of pixels. Furthermore, similar to the traditional Naor-Shamir scheme [1], the security of the proposed scheme is also uniquely determined by the pixel encoding procedure. Therefore, the proposed scheme's security has nothing to do with the scanning or fill-in mode. The proof is completed.

D. Complexity

Compared with those known multi-pixel encoding methods [16 and 17] and most single-pixel encoding methods, the complexity of the proposed scheme is in the same situation even lower in terms of the following facts. Firstly, the proposed scheme scans the original image instead of temporarily storing the image; it only remembers two values, r and p, and the encoder need not to trace backward or forward. Secondly, during encoding the proposed scheme randomly rearranges the m integers, i.e., 1, 2, …, m, to indirectly achieve the rearranging of the entire basis matrices, so the storage for the rearranged basis matrices is redundant; it only need to store an integer array. However, in most schemes including multi-pixel and single-pixel encoding methods, the directly rearranging of basis matrices and the storage for the rearranged basis matrices are inevitable, so the time and space complexity is usually higher than our scheme. On the other hand, the proposed scheme is a non-expansion encoding scheme, so the storage for all shares produced during encoding needs much less than that of the schemes based on expansion encoding.

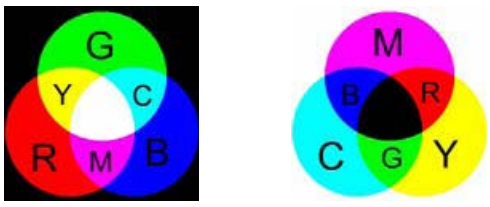
III. The Proposed Scheme Applied to Chromatic Images

A chromatic image is usually composed of three-dimensional parts. Each dimensional part is a gray-scale image. However, like the traditional Naor-Shammir scheme, most VSS schemes are initially designed for binary black-and-white images. In order to work for gray-scale or chromatic images, many researches try to design respective basis matrices for different colors on a secret image [18 and 19]. In this paper, we introduce a technology called halftoning, which can transform a continuous-tone image into a binary one, to make the proposed scheme smoothly work for gray-scale and chromatic images.

A. The Model of Color

A color model is a way to specify colors. It is usually represented as a three-dimensional space. There are many kinds of color model; the most common models are RGB and CMY shown in Fig. 3.

In terms of RGB model, each color is mixed with red, green, and blue, which are the three primary colors of light. This model is commonly used for on-screen display. Mixtures of pure red, pure green and pure blue light produce white light. Therefore, RGB model is also called additive model.



(a) RGB color model (b) CMY color model

Figure 3. Two most common color models

On the other hand, CMY model is called subtractive model. For CMY model, each color is mixed with cyan, magenta, and yellow, which are the three primary colors

of pigments. This model is commonly used for color printing. Generally speaking, the more colors of pigments are mixed, the more wavelengths of light are absorbed. The mixtures of pure cyan, pure magenta and pure yellow absorb all wavelengths of light and hence produce black.

In fact, the RGB model and CMY model are mutually complementary, which can be easily learnt from Fig. 3. For example, the mixture of pure magenta and pure yellow in CMY model produces pure red in RGB model; the mixture of pure green and pure blue produces pure cyan in CMY model.

B. Halftoning

The main idea of halftoning is to utilize the density of printed dots to simulate the grey scale of pixels. For human eyes, the denser the dots are, the darker the image is; on the contrary, the sparser the dots are, the lighter the image is. For example, if the black dot densities of two areas with same size are 90% and 50% respectively, the human visual system can perceive the difference between them: the former is darker than the latter and the latter lighter than the former. Therefore, we can learn that the black dot density can simulate the gray-scale value of an area. Just by dominating the black dot density of an area, halfoning transforms a continuous-tone image into a binary one.

C. Encryption for Chromatic Image

Since the secret image is revealed by stacking those legal shares and the stacking produces color mixing as color printing, we adopt CMY model to decompose a chromatic image into three monochromatic ones. Each one is a gray-scale image whose intensity ranges from zero to 255. We can transform each gray-scale image into a binary image by halftoning. Then each halftoned image can be encrypted by the proposed scheme under the control of an appointed access structure. Finally, the three encrypted monochromatic images are again combined to form an intact share. When constructing, we only need to stack all the legal shares to reveal the secret image. The whole encryption procedure of the proposed scheme for chromatic images is concluded and illustrated in Fig. 4. By the way, how to encrypt a gray-scale image can be easily inferred from the encryption procedure shown in Fig. 4 and the details are omitted here.

IV. Experimental Results

Three experimental results are shown in this section. The first one is used to compare the proposed scheme with other typical schemes such as the traditional Naor-Shammir scheme [1], Ito et al's scheme [14] and Hou et al's scheme [17]. The second one is the result of the proposed scheme used for chromatic image and general access structure. Finally, the last one shows the statistics about the contributions of three scanning modes including row-by-row scanning, column-by-column scanning and zigzag scanning.

A. Experimental Result for Comparisons

Take the basis matrices in (1) for a (2, 3) threshold access structure. The matrix M_0 is used to encrypt white pixels and M_1 is to encrypt black pixels. For such threshold structure, an original secret image is encrypted into three shares of which any two or three can be stacked to recover the discernable secret image; any single share cannot reveal any information about the secret image. Fig. 5 shows a secret image and Fig. 6 presents the comparison results.

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

Among the schemes joining the comparison, Naor-Shammir scheme [1] is the first VSS scheme that is also a representative of VSS schemes with expansion. Ito et al's scheme [14] is a typical representative of early non-expanded VSS schemes and it is usually cited for a comparison by many researches. Hou et al's scheme [17] is the representative of VSS schemes using multi-pixel encoding with a fixed encoding length for each run. The proposed scheme uses a new multi-pixel encoding method called pixel-block aware encoding that encrypts different amount of pixels for each run where the amount of encoded pixels lies on the number of consecutive pixels with same type during the original image scanning.

From the experimental results associating with some analyses, some facts can be learnt as follows.

(1) For Naor-Shamir scheme [1], an expansion even a distortion occurs in shares and reconstructed images. Concretely, the pixel expansion is that m = 3. Moreover, this scheme scans the secret image row by row and encrypts pixel by pixel;

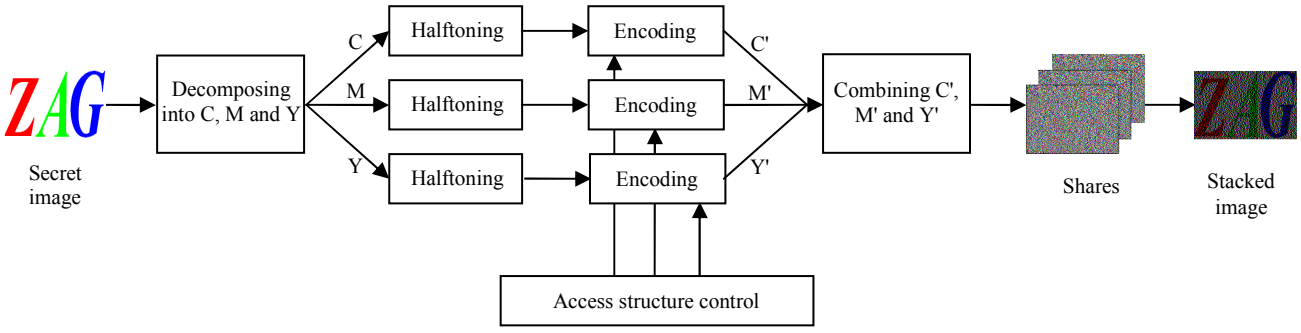


Figure 4. Encryption procedure for chromatic images

(2) For Ito et al's scheme [14], the quality of recovered images is worse than that of the other two schemes. This scheme also scans the secret image row by row and encrypts pixel by pixel;

(3) For Hou et al's scheme [17], only three (m = 3) pixels are encoded at each run where tracings backward or forward exists. Additionally, this scheme also scans the secret image row by row in despite of that it encodes block by block;

(4) For the proposed scheme, the quality of the shares and reconstructed images is same as that of the traditional Naor-Shamir scheme. A statistics during the experiment demonstrates that the proposed scheme encodes at most 1016 pixels at one run. What is more, no tracing backward or forward occurs during encoding. This new scheme encodes block by block and especially scans the secret image using zigzag mode;

(5) This experiment further shows that the stacking of all shares brings us an example of perfect black VSS mentioned in section 1: every black pixel in secret image is reconstructed by black pixel and hence the stacked image has a better visual quality.

Figure 5. The secret image (125×125 pixels)

	Naor-Shamir scheme	Ito et al's scheme	Hou et al's scheme	The proposed scheme
Share 1				
Share 2				
Share 3				
Stacking share 1 and share 2				
Stacking share 1 and share 3				
Stacking share 2 and share 3				
Stacking all the three shares				
size	375×125 pixels	125×125 pixels	125×125 pixels	125×125 pixels

Figure 6. Experimental results by the proposed scheme and other typical schemes

B. Experimental Result for General Access Structure

We take the general structure $\Gamma = \{\mathcal{A}_0, \mathcal{A}_1\}$ mentioned in section 1 for instance. Since $\mathcal{A}_1$ = {{1, 2}, {2, 3}, {3, 4}, {1, 2, 3}, {1, 2, 4}, {1, 3, 4}, {2, 3, 4}, {1, 2, 3, 4}} and $\mathcal{A}_0$ = {{1}, {2}, {3}, {4}, {1, 3}, {1, 4}, {2, 4}}, we can adopt the basis matrices in (2).

$$M_0 = \begin{bmatrix} 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 \end{bmatrix}, M_1 = \begin{bmatrix} 1 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \end{bmatrix}. \quad (2)$$

Fig. 7 shows a chromatic secret image and the image shown in Fig. 8 is its halftoned version. Fig. 9 demonstrates the experimental results under the control of above-mentioned general access structure $\Gamma = \{\mathcal{A}_0, \mathcal{A}_1\}$.

From the experimental results shown in Fig. 9, we can easily learn that the general access structure $\Gamma = \{\mathcal{A}_0, \mathcal{A}_1\}$ is correctly implemented and the recovered images have good visual quality. On the other hand, there are at most 10251 pixels encoded at one run, which further show that the proposed scheme wins good encoding efficiency.

C. Experimental Result for Scanning modes

Aiming at evaluating different scanning modes, we still take the black-and-white image in Fig. 5 and the chromatic image in Fig. 8. The former has totally 15625 black and white pixels; the latter has three halftoned monochromatic gray-scale images of which each one has totally 23276 black and white pixels that are actually non-blanks and blanks.

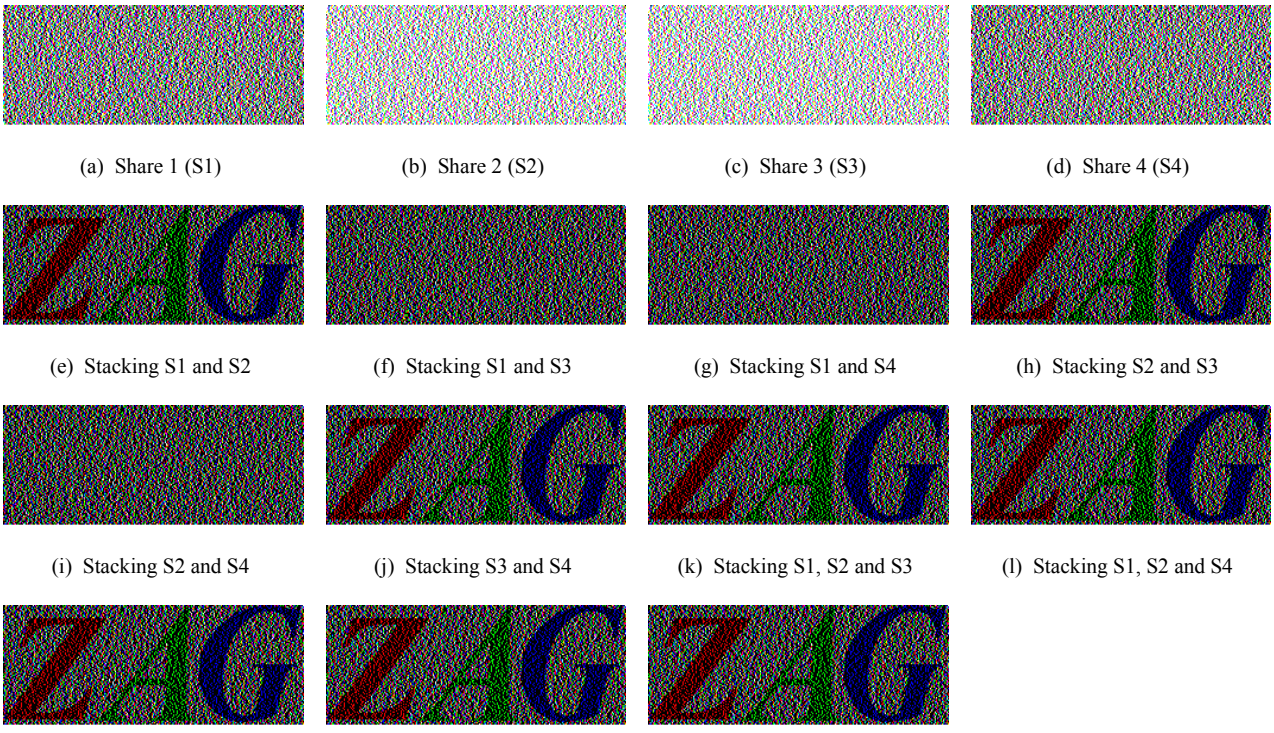
For the image in Fig. 5, different scanning modes demonstrate distinct capacities. The statistics during the experiment shows that for row-by-row scanning, column-by-column scanning and zigzag scanning, the maximum values among the numbers of scanned pixels of same type at one scanning run are 416, 308 and 1016, respectively.

On the other hand, for the image in Fig. 8, the maximum values among the numbers of scanned pixels of same type at one scanning run contributed by row-by-row scanning, column-by-column scanning and zigzag scanning are 851, 8376 and 10251, respectively.

It is clear from above statistics that zigzag scanning mode has an evident advantage over the other two modes. This experiment further illuminates the significance of the properly choosing of scanning mode.

Figure 7. The original image (253×92 pixels)

Figure 8. The halftoned image (253×92 pixels)



(a) Share 1 (S1) (b) Share 2 (S2) (c) Share 3 (S3) (d) Share 4 (S4)

(e) Stacking S1 and S2 (f) Stacking S1 and S3 (g) Stacking S1 and S4 (h) Stacking S2 and S3

(i) Stacking S2 and S4 (j) Stacking S3 and S4 (k) Stacking S1, S2 and S3 (l) Stacking S1, S2 and S4

(m) Stacking S1, S3 and S4 (n) Stacking S2, S3 and S4 (o) Stacking S1, S2, S3 and S4

Figure 9. Experimental results for general access structure by the proposed scheme (Each image has 253×92 pixels)

V. CONCLUSION

The pixel-block aware encoding method proposed in this paper is a novel multi-pixel encoding method. From the experimental results, we easily know that it works well for chromatic images and general access structure. It also can achieve good quality for overlapped images and high efficiency for encoding. All these merits will bring it into wider applications in reality.

REFERENCES

[1] M. Naor and A. Shamir, "Visual cryptography," *Advances in Cryptology-Eurocrypt'94*, pp. 1–12, 1995.

[2] P. A. Eisen and D. R. Stinson, "Threshold visual cryptography schemes with specified whiteness levels of reconstructed pixels," *Designs, Codes and Cryptography*, vol. 25, no. 1, pp. 15–61, 2002.

[3] S. Cimato, R. D. Prisco, and A. D. Santis, "Colored visual cryptography without color darkening," *Theoretical Computer Science*, vol. 374, no. 1–3, pp. 261–276, 2007.

[4] R. Lukac, K. N. Plataniotis, B. Smolka, and A. N. Wenetsanopoulos, "A new approach to color image secret sharing," *Proceedings of the 12th European Signal Processing Conference*, pp. 1493–1496, 2004.

[5] L. A. MacPherson, "Grey level visual cryptography for general access structures," Dissertation, University of Waterloo, 2003.

[6] F. Yi, D. S. Wang, P. Luo, L. S. Huang, and Y. Q. Dai, "Multi secret image color visual cryptography schemes for general access structures," *Progress in Natural Science*, vol. 16, no. 4, pp. 431–436, 2006.

[7] H. B. Zhang, X. F. Wang, and Y. P. Huang, "General construction for ideal contrast visual secret sharing scheme with reversing," *Proceedings of Information Technology and Environmental System Sciences*, pp. 212–216, 2008.

[8] Z. Gan and K. F. Chen. "Cheater identifiable visual secret sharing scheme," *Journal of Systems Engineering and Electronics*, vol. 16, no. 1, pp. 233–236, 2005.

[9] C. M. Hu and W. G. Tzeng, "Cheating prevention in visual cryptography," *IEEE Transactions on Image Processing*, vol. 16, no. 1, pp. 36–45, 2007.

[10] Y. P. Deng, L. F. Guo, and M. L. Liu, "Constructions for Anonymous secret sharing schemes using combinatorial designs," *Acta Mathematicae Applicatae Sinica*, English Series, vol. 23, no. 1, pp. 67–78, 2007.

[11] P. F. Tsai and M. S. Wang, "An (3,3)-visual secret sharing scheme for hiding three secret data," *Proceedings of the 2006 Joint Conference on Information Sciences*, 2006.

[12] S. J. Shyu, S. Y. Huang, Y. K. Lee, R. Z. Wang, and K. Chen, "Sharing multiple secrets in visual cryptography," *Pattern Recognition*, vol. 40, pp. 3633–3651, 2007.

[13] J. L. Bai, "Images secret sharing based upon random numbers," Dissertation, MingChuan University, 2005.

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

[15] Y. C. Hou and C. S. Hsu, "An unexpanded visual cryptography method for gray-level images," *Journal of Information Management*, vol. 13, pp. 107–125, 2004.

[16] Y. C. Hou and S. F. Tu, "Visual cryptography techniques for color images without pixel expansion," *Journal of Information, Technology and Society*, vol. 1, pp. 95–110, 2004.

[17] Y. C. Hou and S. F. Tu, "A visual cryptographic technique for chromatic images using multi-pixel encoding method," *Journal of Research and Practice in Information Technology*, vol. 37, no. 2, pp. 179–191, 2005.

[18] C. Blundo, A. De Santis, and H. C. A. Van Tilborg, "Visual cryptography for grey level images," *Information Processing Letters*, vol. 75, pp. 255–259, 2000.

[19] C. N. Yang and C. S. Laih, "New colored visual secret sharing schemes," *Designs, Codes and Cryptography*, vol. 20, pp. 325–335, 2000.