

# Visual Crystal for Access Structure by Multi-pixel Encoding with Variable Block Size

Alaudeen.B.M\*., Dr.G.Tholkappia Arasu.\*\*

\*Research Scholar, \*\* Professor

\*Manonmaniam Sundaranar University, Tirunelveli., \*\*A.V.S.College of Technology , Salem

---

**Abstract:** Multi-pixel encoding is an emerging method in visual Krystal for that it can encode more than one pixel for each run. However, in fact its encoding efficiency is still low. This paper presents a novel multi- pixel encoding which can encode variable number of pixels for each run. The length of encoding at one run is equal to the number of the consecutive same pixels met during scanning the secret image. The proposed scheme can work well for general access structure and chromatic images without pixel expansion. The experimental results also show that it can achieve high efficiency for encoding and good quality for overlapped images.

**Keywords:** Visual secret sharing, cheating immune, anonymity.

---

## 1. INTRODUCTION

In 1994, Naor and Shamir <sup>[1]</sup> first presented a novel secret sharing scheme called visual cryptography which 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 doesn't need any knowledge of cryptography or any help with computer; it only depends on the mankind's visual system.

Actually, the Naor-Shamir scheme implements a  $(t, n)$  threshold access structure. Generally speaking, 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 structure rules that any  $t$  or more out of  $n$  participants can cooperate to reveal the secret image and any less than  $t$  participants get nothing about the secret image.

However, threshold structure is only one special case of the so-called general access structure. Usually, a general access structure is denoted as  $\Gamma = \{A0, A1\}$ , where  $A0$  and  $A1$  are sets of subsets of all participants and  $A0 \cap A1 = \emptyset$

Furthermore,  $A0$  denotes a collection of forbidden sets and  $A1$  denotes a collection of qualified sets. It is easily known that stacking all the shares held by the participants of a qualified set can recover the secret image; but stacking all the shares held by the participants of a forbidden set cannot reveal any information about the secret image.

For example, in a system with four participants, we can let  $A1 = \{\{1, 2\}, \{2, 3\}, \{3, 4\}, \{1, 2, 3\}, \{1, 2, 4\},$

$\{1, 3, 4\}, \{2, 3, 4\}, \{1, 2, 3, 4\}\}$ , which implies that  $A0 = \{\{1\}, \{2\}, \{3\}, \{4\}, \{1, 3\}, \{1, 4\}, \{2, 4\}\}$ . 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.

## 2. PREVIOUS WORKS

After the Naor-Shamir scheme appears, many related researches and some extended VSS schemes come forth. Some of which can be used for gray-scale or chromatic images <sup>[2, 3]</sup>, general access structure <sup>[3, 4]</sup>, ideal contrast <sup>[5]</sup>, cheating immune <sup>[6, 7]</sup>, anonymity <sup>[8]</sup> and multiple images hiding.

However, all these schemes introduce pixel expansion, which leads to an expansion even distortion of the revealed image; meanwhile, more storage capacity and transmission delay are needed for shares. In order to overcome above mentioned disadvantages, many researches are aimed at pixel non-expanded schemes. Bai<sup>[11]</sup> proposed such scheme based on random number concept, but its shortcoming is clear in that it is only suitable for the  $(n, n)$  threshold access structure. Ito et al.<sup>[12]</sup> put forward another non-expanded scheme which is suitable for  $(k, n)$  threshold structure. However, the quality of stacked image is very poor and moreover their needs complex encoding and operations when it extends to encode gray-scale or chromatic images.

A similar scheme proposed by Hou et al.<sup>[13]</sup> improves the quality of revealed image, but it only can be utilized to encrypt gray-scale images. No matter 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 method. In 2004, Hou et al.<sup>[14]</sup> first proposed a multi-pixel encoding method by which at each run there are  $m$  consecutive pixels joining encoding, where  $m$  is 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 structure. Afterwards, they proposed another multi-pixel encoding method in<sup>[15]</sup> 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 have disadvantage 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 more than  $m$  consecutive same pixels induce the redundant parts need to stay for the next run. The common feature of the schemes in<sup>[14, 15]</sup> is that the length of the encoded pixels for each run is a constant value  $m$ . In fact, this feature leads to two short comings.

On one hand, the parameter  $m$  is usually also called the expansion rate of most VSS schemes; therefore, the value of  $m$  is usually limited into a very small range, which implies that the improvement of encoding efficiency is not attractive.

On the other hand, it is a usual thing in applications that the number of the consecutive same pixels is remarkably more than the value of  $m$ . This means that the fixed value of  $m$  is not preferably suit to the real cases of the input sequence. In this paper, we propose a new multi-pixel encoding method which can encode variable number of pixels for each run. The length of encoding at one run is equal to the number of the consecutive pixels of same type during scanning the secret image.

The proposed scheme can work well for general access structure and chromatic images without pixel expansion. Tracing backward or forward is redundant for this scheme. Compared with those known multi-pixel encoding methods, it wins higher efficiency for encoding.

### 3. PROPOSED SCHEME

Generally, we suppose the basis matrices  $M0$  and  $M1$  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  $S1, S2, \dots, Sn$ , respectively. In gray-scale or chromatic images, the white pixel usually means blank and black pixel means non-blank. Same to the traditional Naor- Shamir scheme<sup>[1]</sup>, 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 then the secret image is revealed. Therefore, we only give the distribution description as follows.

#### Multi-pixel Encoding with Variable Block Size:

**INPUT:**  $SI$  with  $L \times H$  pixels;  $M0$  and  $M1$  with size of  $n \times m$ , respectively.

**OUTPUT:**  $S1, S2, \dots, Sn$  with  $L \times H$  pixels, respectively.

**step1:** scan the secret image  $SI$  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:** for  $(i = 1$  to  $\lceil L/r/m \rceil)$

{

**step2.1:** randomly rearrange  $(1, 2, \dots, m)$  and write the result as  $L_i = (l_1, l_2, \dots, l_m)$

;}

**step3:** concatenate all the  $L_i$ s into  $L$ . Namely,  $L = L_1 || L_2 || \dots || r/m L_i ||$ ;

**step4:** if  $(|L| > r)$

{

**step4.1:** truncate the tail of  $L$  to make sure that  $|L| = r$ ;

}

**step5:** fill the pixels at line  $i$  and the columns indicated by  $L$  of  $M_p$  into  $S_i$ , where  $i = 1, 2, \dots, n$ .

An encoding run is finished from step1 to step5, and then repeat above procedure to encode all the pixels of SI

Compared with those known multi-pixel encoding methods<sup>[14, 15]</sup> 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 sequentially scans the original image instead 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.,  $1, 2, \dots, m$ , to indirectly achieve the rearranging of the entire basis matrix, so the storage for the rearranged basis matrix is redundant.

However, in most schemes including multi-pixel and single-pixel encoding methods, the directly rearranging of basis matrix and the storage for the rearranged basis matrix 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 need much less than that of the schemes based on expansion encoding.

Application to chromatic image and general access structure A chromatic image is usually composed of three dimensional parts. Each dimensional part is a gray-scale image. However, like the traditional Naor-Shamir scheme, most VSS schemes are initially designed for binary black-and-white images. In order to work for grayscale or chromatic images, many researches try to design respective basis matrices for different colors on a secret image<sup>[16, 17]</sup>.

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 work for gray-scale and chromatic images.

### Halftoning and color model

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 40% 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, halftoning transforms a continuous-tone image into a binary one.

A color model is a way to specify colors. There are many kinds of color model such as RGB and CMY model. 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. So RGB model is also called additive model. On the other hand, CMY model is 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. Usually, 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.

### Encryption procedure

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

which can be transformed 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 a whole 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 figure 1. By the way, how to encrypt a gray-scale image can be easily inferred from figure 1.

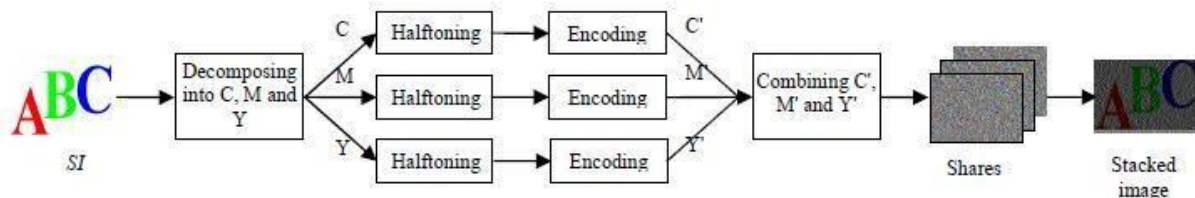


Figure 1 Encryption procedure for chromatic images

#### 4. EXPERIMENTAL RESULTS

Two experimental results are shown in this section. One is used to compare the proposed scheme with other typical schemes such as the traditional Naor-Shamir scheme,

Ito et al's scheme and Hou et al's scheme. The other one is the result of the proposed scheme for chromatic image and general access structure. Firstly, we take the basis matrices in equation (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 can not reveal any information about the secret image. Figure 2 shows a secret image and figure 3 demonstrates the results.

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

Because the stacked images from any two shares are very similar, figure 3 only shows one of them as a representative. We can learn from the experimental results and some analyses that (1) the recovered image is expanded even distorted in Naor-Shamir scheme; (2) the quality of recovered image by

Ito et al's scheme is worse than that of the other schemes; (3) Hou et al's scheme only encodes three ( $m = 3$ ) pixels for each run; (4) the proposed scheme encodes at most 602 pixels at one run and on average 29.0 pixels for each run. What is more, no tracing backward or forward occurs during encoding.

Secondly, we take the general structure  $\Gamma =$

$\{A_0, A_1\}$  mentioned in section 1 for instance. Since  $A_1 = \{\{1, 2\}, \{2, 3\}, \{3, 4\}, \{1, 2, 3\}, \{1, 2, 4\}, \{1,$

$3, 4\}, \{2, 3, 4\}, \{1, 2, 3, 4\}\}$  and  $A_0 = \{\{1\}, \{2\}, \{3\},$

$\{4\}, \{1, 3\}, \{1, 4\}, \{2, 4\}\}$ ,

We can adopt the basis matrices in equation(2)

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

From the experimental results shown in figure 4, we can easily learn that the general access structure  $\Gamma = \{A0, A1\}$  is correctly implemented and the recovered images have good visual quality. On the other hand, there are at most 8976 pixels encoded at one run and on average 56.9 pixels for each run, which further show that the proposed scheme wins good encoding efficiency.



Figure 2: Secret image with 100 X 100 pixel





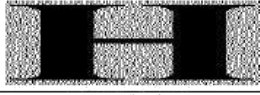




















	Naor-Shamir scheme	Ito et al's scheme	Hou et al's scheme	The proposed scheme
Stacking two shares (S1 and S2)				
Stacking all shares				
size	300×100 pixels	100×100 pixels	100×100 pixels	100×100 pixels

Figure 3 Experimental results by the proposed scheme and other typical schemes

Original image	Halftoned image	S1	S2	S3	S4
					
S1 + S2	S1 + S3	S1 + S4	S2 + S3	S2 + S4	S3 + S4
					
S1 + S2 + S3	S1 + S2 + S4	S1 + S3 + S4	S2 + S3 + S4	S1 + S2 + S3 + S4	
					

Note: "+" means stacking operation.

Figure 4 Experimental results for chromatic image and general access structure by the proposed scheme

## 5. CONCLUSION

The multi-pixel encoding with variable block size proposed in this paper is a novel VSS 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] Naor M, Shamir A (1995). "Visual cryptography". Advances in Cryptology- EUROCRYPT'94, pp.1-12.
- [2] Cimato S, Prisco R D, Santis A D (2007). "Colored visual cryptography without color darkening". Theoretical Computer Science, Vol.374, No.1-3, pp.261-276.
- [3] MacPherson L A (2003). "Grey level visual cryptography for general access structures". Dissertation, University of Waterloo.
- [4] Yi F, Wang D S, Luo P, et al (2006). "Multi secret image color visual cryptography schemes for general access structures". Progress in Natural Science, Vol.16, No.4, pp.431- 436.
- [5] Zhang H B, Wang X F, Huang Y P (2008). "General construction for ideal contrast visual secret sharing scheme with reversing". Proceedings of Information Technology and Environmental System Sciences, pp.212-216.
- [6] Gan Z, Chen K F (2005). "Cheater identifiable visual secret sharing scheme". Journal of Systems Engineering and Electronics, Vol.16, No.1, pp.233-236.



- [7] Hu C M, Tzeng W G (2007). "Cheating prevention in visual cryptography". IEEE Transactions on Image Processing, Vol.16, No.1, pp.36-45.
- [8] Deng Y P, Guo L F, Liu M L (2007). "Constructions for Anonymous secret sharing schemes using combinatorial designs". Acta Mathematicae Applicatae Sinica, English Series, Vol.23, No.1, pp.67-78.
- [9] Tsai P F, Wang M S (2006). "An (3,3)- visual secret sharing scheme for hiding three secret data". Proceedings of the 2006 Joint Conference on Information Sciences.
- [10] Shyu S J, Huang S Y, Lee Y K, et al (2007). "Sharing multiple secrets in visual cryptography". Pattern Recognition, Vol.40, pp.3633-3651.
- [11] Bai J L (2005). "Images secret sharing based upon random numbers". Dissertation, MingChuan University.
- [12] Ito R, Kuwakado H, Tanaka H (1999). "Image size invariant visual cryptography". IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, Vol.E82-A, No.10, pp.2172- 2177.
- [13] Hou Y C, Hsu C S (2004). "An unexpanded visual cryptography method for gray- level images". Journal of Information Management, Vol.13, pp.107-125.
- [14] Hou Y C, Tu S F (2004). "Visual cryptography techniques for color images without pixel expansion". Journal of Information, Technology and Society, Vol.1, pp.95- 110.
- [15] Hou Y C, Tu S F (2005). "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.
- [16] Blundo C, De Santis A, Van Tilborg H C A (2000). "Visual cryptography for grey level images" Information Processing Letters, Vol.75, pp.255-259.
- [17] Yang C N, Laih C S (2000). "New colored visual secret sharing schemes". Designs, Codes and Cryptography, Vol.20, pp.325-335.