Visual Secret Sharing Schemes with Cyclic Access Structure for Many Images

Miyuki Uno and Mikio Kano

Department of Computer and Information Sciences
Ibaraki University, Hitachi, Ibaraki, 316-8511 Japan
uno.miyuki@gmail.com kano@mx.ibaraki.ac.jp
http://gorogoro.cis.ibaraki.ac.jp/

Abstract. We consider a visual secret sharing scheme with cyclic access structure for n secret images and n shares, where two consecutive shares decode one secret image. This secret sharing scheme can be constructed by using Droste's method. However the contrast of its scheme is $1/(2n)$. In this paper, it is shown that for every integer $n \geq 4$, there exists no construction of such a visual secret sharing scheme having a perfect black reconstruction and contrast at least $1/4$. Also for every even integer $n \geq 4$, a new construction of such a visual sharing scheme that satisfies a slightly weaker condition and has a contrast $1/4$ is given.

1 Introduction

A visual secret sharing scheme (VSS scheme), which is also called a visual cryptography scheme (VCS), was introduced by Naor and Shamir [9]. Since then, it have been studied in many papers including [1,2,3,6]. A VSS scheme is a special kind of secret sharing scheme in which the secret is an image comprised of black and white pixels and encoded into n shares, where each share is usually printed on a transparency. In k-out-of-n VSS scheme, the secret image can be obtained only by stacking k of the shares, but we cannot get any information about the secret image from fewer than k shares.

Droste [5] introduced the following generalized VSS scheme and gave its construction. Let $\mathcal{F}$ be a family of non-empty subsets of $\{1, 2, \ldots, n\}$, and $\{Image(X) \mid X \in \mathcal{F}\}$ be a set of $|\mathcal{F}|$ secret images, each of which corresponds to an element of $\mathcal{F}$. Then we can construct n shares $Share(1)$, $Share(2)$, $\ldots$, $Share(n)$ so that for any element $X \in \mathcal{F}$, a stack of the shares in $\{Share(i) \mid i \in X\}$ recovers the secret image $Image(X)$, and we cannot get any information about $Image(X)$ from a set $\{Share(i) \mid i \in Y\}$ for $X \not\subseteq Y \subset \{1, 2, \ldots, n\}$. The family $\mathcal{F}$ is called the access structure of the VSS scheme.

If we apply this construction to a VSS scheme with cyclic access structure given below, then each pixel is split into $2n$ subpixels and its contrast is $1/(2n)$. Thus this VSS scheme loses a lot of contrast in reconstructed images when n is large.

In this paper, we first prove that for every $n \geq 4$, there exists no construction of a VSS scheme with cyclic access structure that has a perfect black reconstruction and contrast greater than or equal to 1/4. Next, for every even $n \geq 4$, we give a new construction of a VSS scheme with cyclic access structure that satisfies a slightly weaker condition and has a contrast 1/4. For $n = 3$, we give a similar results with contrast 1/6.

We now explain a VSS scheme with cyclic access structure and another such a VSS scheme satisfying a slightly weaker condition. They consist of n shares $Share(1), \ldots, Share(n)$ and n secret images $Image(1), \ldots, Image(n)$ and posses the following properties either (a),(b),(c) or (a),(b*),(c):

(a) for every $1 \leq i \leq n$, a stack of $Share(i)$ and $Share(i+1)$ reconstructs $Image(i)$, where $Share(n+1) = Share(1)$;
(b) for every $1 \leq k \leq n$, a set $\{Share(i) \mid 1 \leq i \leq n, i \neq k\}$ of $n-1$ shares gives us no information about $Image(k-1)$ and $Image(k)$;
(b*) for every $1 \leq k \leq n$, a set $\{Share(i) \mid 1 \leq i \leq n,\ i \neq k, k+1\}$ of $n-2$ shares gives us no information about $Image(k-1)$, $Image(k)$, $Image(k+1)$; and
(c) this VSS scheme is *perfect*, that is, it has a perfect black reconstruction. So every black pixel of a secret image is recovered into a pure black region in the reconstructed image.

The condition (b*) says that if two consecutive shares $Share(k)$ and $Share(k+1)$ are missing, then any information about three images $Image(k-1)$, $Image(k)$, $Image(k+1)$ cannot be obtained. It is obvious that a VSS scheme having the property (b) satisfies (b*), and so in this sense, we say that the condition (b*) is slightly weaker than (b). As we shall show, it is impossible to construct a VSS scheme with cyclic access structure satisfying (a), (b), (c) and having contrast at least 1/4 for every $n \geq 4$. Keeping a high contrast 1/4, we give a new construction of a VSS scheme with cyclic access structure satisfying (a), (b*), (c) for every even $n \geq 4$.

We now explain the contrast of a VSS scheme with perfect black reconstruction. Consider such a VSS scheme in which each pixel of secret images is split into m subpixels in a share. We say that such a perfect VSS scheme has a contrast δ if for every white pixel of secret images, at least δm subpixels of the corresponding pixel in the reconstructed images are white, and for a certain white pixel of a secret image, exactly δm subpixels of the corresponding pixel in the reconstructed images are white.

This paper is organized as follows: In Sect. 2, a construction of cyclic VSS scheme that satisfies (a), (b), (c) is given where $n = 3$. In Sect. 3, it is proved that for every $n \geq 4$, non-existence of the VSS scheme that satisfies (a),(b),(c) and has contrast greater than or equal to 1/4. In Sect. 4, for every even $n \geq 4$, a construction of the VSS scheme satisfying (a), (b*), (c) and having contrast 1/4 is proposed. In appendix A, it is proved that for $n = 3$ non-existence of the VSS scheme satisfying (a), (b), (c) and having contrast greater than 1/6. In appendix B, an example of the VSS scheme for $n = 6$ and with contrast 1/4 is shown.

Other results on VSS scheme with many secret images can be found in [6], [10] and etc.

2 Preliminaries and a VSS Scheme with Cyclic Access Structure for $n = 3$

We first introduce some notations and definitions used throughout this paper. Consider a VSS scheme with cyclic access structure consisting of n secret images $Image(1), \ldots, Image(n)$ and n shares $Share(1), \ldots, Share(n)$. All the secret images are comprised of black and white pixels. Each pixel of secret images is split into m subpixels in a share.

Hereafter we consider any fixed pixel x of secret images, and denote its color in $Image(i)$ by $img(i) = img_x(i)$, and by $S(i) = S_x(i)$ the set of subpixels of $Share(i)$ corresponding to the pixel x. Then the pixel x corresponds to the $m \times n$ subpixels $S(1) \cup S(2) \cup \cdots \cup S(n)$. These $m \times n$ subpixels can be expressed by a $m \times n$ $(0,1)$-matrix $B = [b_{ij}]$, where $b_{ij} = 1$ if the i-th subpixel of $S(j)$ is black, otherwise $b_{ij} = 0$. Namely, the j-th column vector of B corresponds to $S(j)$, and we also use $S(j)$ to denote the j-th column vector of B. The matrix B is called a *basis matrix* of the VSS scheme, which is the transposed matrix of usually used basis matrix. For convenience, this matrix is used in this paper. A 2×2 $(0,1)$-matrix

$$M(i) = \begin{bmatrix} m_{i1}\ m_{i3} \\ m_{i2}\ m_{i4} \end{bmatrix}$$

is randomly chosen from the two matrices of the following (1) if the pixel of a secret image is black, and otherwise it is randomly chosen from (2).

$$\left\{ \begin{bmatrix} 1\ 0 \\ 0\ 1 \end{bmatrix}, \quad \begin{bmatrix} 0\ 1 \\ 1\ 0 \end{bmatrix} \right\}, \tag{1}$$

$$\left\{ \begin{bmatrix} 0\ 0 \\ 1\ 1 \end{bmatrix}, \quad \begin{bmatrix} 1\ 1 \\ 0\ 0 \end{bmatrix} \right\}. \tag{2}$$

A VSS scheme with cyclic access structure for three secret images and three shares is presented as Fig. 1.

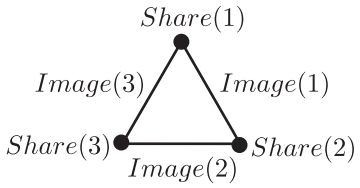

Fig. 1. The secret images and the shares correspond to the edges and the vertices, respectively.

We adopt the Droste's method. Each pixel is split into six subpixels, and the 6×3 $(0,1)$-matrix $B = [b_{ij}]$ is defined as follows:

$$B = \begin{bmatrix} m_{11} & m_{13} & 1 \\ m_{12} & m_{14} & 1 \\ 1 & m_{21} & m_{23} \\ 1 & m_{22} & m_{24} \\ m_{33} & 1 & m_{31} \\ m_{34} & 1 & m_{32} \end{bmatrix} = [S(1), S(2), S(3)],$$

which contains $M(1)$, $M(2)$ and $M(3)$ as submatrices.

Consider any fixed pixel x of images. If $img(1)$ is black, then $M(1)$ is chosen from (1), and so perfect black region is reconstructed by $S(1)$ and $S(2)$, otherwise $M(1)$ is chosen from (2), and thus one common subpixels of $S(1)$ and $S(2)$ are white, and hence a white region is reconstructed. For other images, the colors are reconstructed in the same way by using $M(2)$ and $M(3)$. The security condition (b) is proved in [5].

We will prove in the appendix that it is impossible to construct a cyclic VSS scheme satisfying (a), (b), (c) and having contrast greater than 1/6.

3 Non-existence of the VSS with Contrast at Least 1/4

In this section we shall show that if $n \geq 4$, then the contrast of a VSS scheme with cyclic access structure for n images satisfying the conditions (a), (b), (c) is less than 1/4. Namely, we prove the following theorem.

Theorem 1. *Let $n \geq 4$ be an integer. Then there exists no construction of a VSS scheme with cyclic access structure for n secret images that satisfies (a), (b), (c) and has contrast greater than or equal to* 1/4.

Proof. Assume that there exists a construction of a VSS scheme with cyclic access structure for n images which satisfies (a), (b), (c) and whose contrast is greater than or equal to 1/4. We consider a fixed pixel x of images, and use the same notation as in the previous section. Namely, we write $img(i)$ for the color of x in $Image(i)$, and $S(i)$ for the set of subpixels of $Share(i)$ corresponding to x. Suppose that each pixel is split into m subpixels. Let $W_i,\ B_i \subseteq \{1, 2, \cdots, m\}$ denote the indices of white subpixels and black subpixels of $S(i)$, respectively, as follows (Fig. 2):

$$W_i = \{k \mid \text{the } k\text{-th subpixel of } S(i) \text{ is white}\},$$
$$B_i = \{k \mid \text{the } k\text{-th subpixel of } S(i) \text{ is black}\}.$$

Put $|W_i| = w_i$ and $|B_i| = b_i$. Then $m = w_i + b_i$ for every i.

Let λ denote the minimum number of $|W_i \cap W_{i+1}|$ such that $img(i)$ is white and $1 \leq i \leq n$. Since the contrast is greater than or equal to 1/4, we have $\lambda/m \geq 1/4$, and thus

$$m \leq 4\lambda. \tag{3}$$

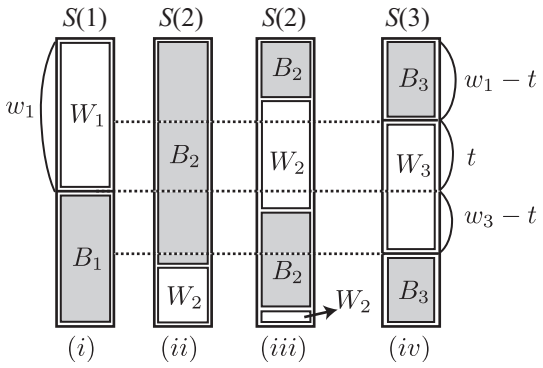

Fig. 2. The sets $S(1), S(2), S(3)$ of pixels.

First consider the case that n is even. Without loss of generality, we may assume that w_1 is maximum among all $w_1, w_3, \ldots, w_{n-1}$ with odd suffixes. Take a triple $(S_1(1), S_1(2), S_1(3))$ so that $|W_1 \cap W_3|$ is maximum among all triples $(S(1), S(2), S(3))$. Let $t = |W_1 \cap W_3|$ for the $(S_1(1), S_1(2), S_1(3))$ (Fig. 2 (i), (iv)). Assume $w_3 - t < \lambda$. If $img(2)$ is white, then $|W_2 \cap W_3| \geq \lambda$ and so $W_1 \cap W_2 \cap W_3 \neq \emptyset$. Since our VSS scheme is perfect, this implies that $S_1(1)$ and $S_1(2)$ must decode a white pixel. Namely, from $(S_1(1), S_1(3))$, we can obtain the information that $(img(1), img(2)) = (black, white)$ never occurs. This contradicts the security condition (b). Hence $w_3 - t \geq \lambda$. By the choice of w_1, we obtain

$$w_1 \geq w_3 \geq \lambda + t. \tag{4}$$

Consider a triple $(S_2(1), S_2(2), S_2(3))$ decoding $(img(1), img(2)) = (white, white)$ (Fig. 2 (i), (iii), (iv)). Then for these $S_2(i)$, it follows that $|W_1 \cap W_2| \geq \lambda$ and $|W_2 \cap W_3| \geq \lambda$, and so

$$|W_2| \geq 2\lambda - |W_1 \cap W_3| \geq 2\lambda - t \tag{5}$$

by the maximality of t. By considering a triple $(S_3(1), S_3(2), S_3(3))$ decoding $(img(1), img(2)) = (black, black)$ (Fig. 2 (i),(ii),(iv)), we have $W_2 \subseteq B_1 \cap B_3$ since the VSS scheme is perfect. Therefore it follows from Fig. 2 (iv), (4), (5) and the maximality of t that

$$\begin{aligned} m = |S_3(3)| &\geq |W_1 \cap B_3| + |B_1 \cap B_3| + |W_3| \\ &\geq |W_1 \cap B_3| + |W_2| + |W_3| \\ &\geq (w_1 - t) + (2\lambda - t) + (\lambda + t) \\ &\geq \lambda + 2\lambda - t + \lambda + t = 4\lambda. \end{aligned}$$

This inequality together with (3) implies $m = 4\lambda$, $|W_1 \cap B_3| = w_1 - t = \lambda$, $|B_1 \cap B_3| = |W_2| = 2\lambda - t$ and $|W_3| = \lambda + t$. Hence the following equality (6)

and statement (7) hold.

$$w_1 = w_3 = \lambda + t, \quad w_2 = 2\lambda - t. \tag{6}$$

If $(img(1), img(2)) = (black, black)$ then

$$|W_1 \cap W_3| = t \quad \text{and} \quad B_1 \cap B_3 = W_2. \tag{7}$$

Notice that if the contrast is greater than $1/4$, then $m > 4\lambda$ in (3), and so we derive a contradiction. Namely, hereafter we consider the case that the contrast is exactly $1/4$.

By applying the same argument to $(S(3), S(4), S(5))$, we obtain

$$w_3 = w_5 = \lambda + t', \quad w_4 = 2\lambda - t', \tag{8}$$

where t' is the maximum value of $|W_3 \cap W_5|$. Hence it follows from (6) and (8) that $t = t'$ and

$$w_1 = w_3 = w_5 = \lambda + t, \quad w_2 = w_4 = 2\lambda - t.$$

By repeating the above argument for $(S(j), S(j+1), S(j+2))$, where $j = 5, \ldots, n-1$, we have

$$w_1 = w_3 = \cdots = w_{n-1} = \lambda + t, \tag{9}$$

$$w_2 = w_4 = \cdots = w_n = 2\lambda - t. \tag{10}$$

Let $s = |W_2 \cap W_4|$ be the maximum value among all triples $(S(2), S(3), S(4))$. Then by the same argument as above, we obtain

$$w_2 = w_4 = \cdots = w_n = \lambda + s, \tag{11}$$

$$w_1 = w_3 = \cdots = w_{n-1} = 2\lambda - s. \tag{12}$$

Moreover, it follows from (7) and the symmetry of t and s that if $(img(2), img(3)) = (black, black)$ then

$$|W_2 \cap W_4| = s \quad \text{and} \quad B_2 \cap B_4 = W_3. \tag{13}$$

Therefore it follows from (9), (10), (11) and (12) that for every integer $1 \leq i \leq n/2$,

$$\lambda = s + t, \quad w_{2i-1} = \lambda + t, \quad w_{2i} = \lambda + s.$$

By $m = 4\lambda = 4(s + t)$ and the symmetry of s and t, we may assume that $t \geq 1$. Consider a sequence $(S(1), S(2), S(3), S(4))$ decoding $(img(1), img(2), img(3)) = (white, black, black)$ (Fig. 3). If $|W_1 \cap W_3| \neq t$, then by (7) we can get the information from $S(1)$ and $S(3)$ without $S(2)$ that $(img(1), img(2)) = (black, black)$ does not occur. This contradicts the condition (b). Hence

$$|W_1 \cap W_3| = t. \tag{14}$$

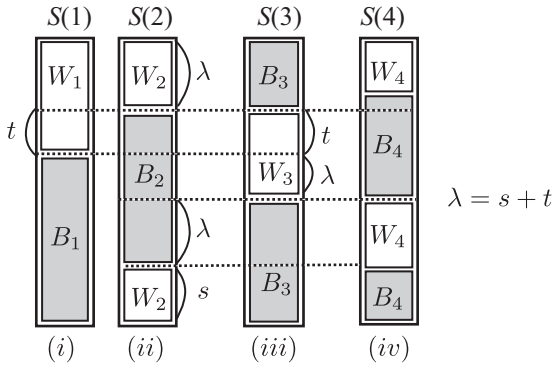

Fig. 3. $(S(1), S(2), S(3), S(4))$ for ($img(1)$, $img(2)$, $img(3)$)=($white$, $black$, $black$).

Since $|W_1 \cap W_2| \geq \lambda$, $W_2 \cap W_3 = \emptyset$, (14) and $|W_1| = \lambda + t$, we have $|W_1 \cap W_2| = \lambda$ (Fig. 3 (ii)). By (13), we have $B_2 \cap B_4 = W_3$ and $|W_2 \cap W_4| = s$. Hence

$$|W_1 \cap W_4| = |W_1 \cap W_2 \cap W_4| \leq |W_2 \cap W_4| = s. \tag{15}$$

Next consider a sequence $(S(1), S(2), S(3), S(4))$ decoding ($img(1)$, $img(2)$, $img(3)$) = ($black$, $black$, $black$) (Fig. 4). Then $|W_1 \cap W_3| = t$ and $B_1 \cap B_3 = W_2$ by (7). Hence the structure of $(S(1), S(2), S(3))$ is determined as Fig. 4. Since

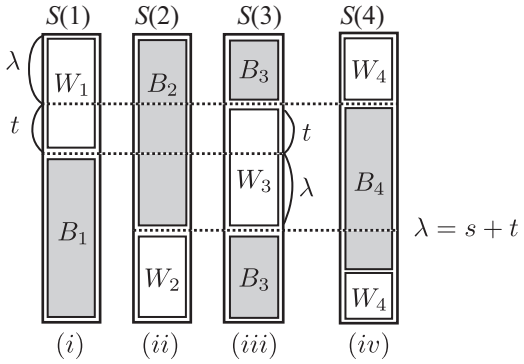

Fig. 4. $(S(1), S(2), S(3), S(4))$ for $(img(1), img(2), img(3)) = (black, black, black)$.

$t \geq 1$ and $B_2 \cap B_4 = W_3$ by (13), we obtain

$$|W_1 \cap W_4| = \lambda = s + t > s. \tag{16}$$

Therefore by (15) and (16), we can get the information from ($S(1)$, $S(4)$) that if $|W_1 \cap W_4| = \lambda$, then ($img(1)$, $img(2)$, $img(3)$) = ($white$, $black$, $black$) does

not occur. This contradicts the security condition. Hence the proof is complete in this case.

Suppose that n is odd. By the same argument as (9) and (10), we can show that the following holds.

$$\lambda + t = w_1 = w_3 = \ldots = w_n \tag{17}$$
$$= w_2 = w_4 = \ldots = w_{n-1} = 2\lambda - t. \tag{18}$$

By applying the same argument as above, we can derive a contradiction. Consequently the theorem is proved.

4 A New Construction of VSS Scheme with Cyclic Access Structure for Even $n \geq 4$

In this section, for every even integer $n \geq 4$, a new construction of VSS scheme with cyclic access structure for n images that satisfies (a), (b*) and (c) is given. It has contrast 1/4, and every pixel of the images is split into four subpixels in each share.

Let $n = 2r \geq 4$. Hereafter, for any fixed pixel x of images, we consider the colors $img(1), \cdots, img(n)$ and the sets $S(1), \cdots, S(n)$ of subpixels corresponding to x. For every $1 \leq i \leq r$, let $A(i)$ and $B(i)$ denote two column vectors consisting of four entries. For convenience, let $A(r+1) = A(1)$ and $B(r+1) = B(1)$. Then by these $A(i)$ and $B(i)$, $S(i)$'s are randomly determined in one of the following two ways (Fig. 5).

$$(S(1), S(2), \cdots, S(n)) = \begin{cases} (A(1), B(1), A(2), B(2), \cdots, A(r), B(r)) \text{ or,} \\ (B(r), A(1), B(1), A(2), \cdots, A(r)). \end{cases}$$

For every $1 \leq i \leq r$, the four row vectors of $[A(i)A(i+1)]$ consist of

$$[0\ 0],\ [0\ 1],\ [1\ 0],\ [1\ 1]. \tag{19}$$

Namely, $[A(i)A(i+1)]$ is obtained from the following matrix by a permutation on the four row vectors:

$$\begin{bmatrix} 0\ 0 \\ 0\ 1 \\ 1\ 0 \\ 1\ 1 \end{bmatrix}.$$

On the other hand, $B(i)$ is a column vector consisting of one 0 entry and three 1's entries, and is determined by the colors of two consecutive colors $(img(2i-1), img(2i))$ or $(img(2i), img(2i+1))$ according to the decision of $S(i)$'s.

Example Assume that $n = 2r = 6$ and $(S(1), \cdots, S(6)) = (A(1), B(1), A(2), B(2), A(3), B(3))$. Then we first determine three column vectors $A(1), A(2), A(3)$

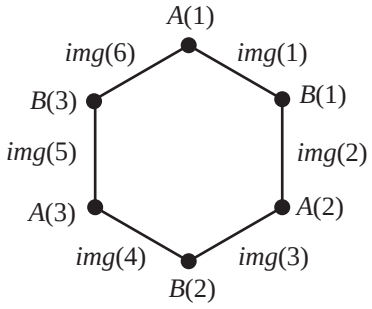

Fig. 5. The graph representing a VSS scheme with cyclic access structure for 6 images.

so that every $[A(i)A(i+1)]$ consisting of four row vectors of (19). For example, the following three column vectors satisfy this condition.

$$[A(1)A(2)A(3)] = \begin{bmatrix} 0\,0\,1 \\ 0\,1\,0 \\ 1\,1\,1 \\ 1\,0\,0 \end{bmatrix}.$$

Assume that $(img(1), img(2), \cdots, img(6))$ are ($white$, $black$, $black$, $black$, $black$, $white$). Then $B(1)$ is determined by a pair ($white$, $black$) of colors so that the second row vector $[0, 1]$ of $[A(1), A(2)]$ works in the reconstruction of $img(1)$ and $img(2)$. Namely,

$$B(1) = \begin{bmatrix} 1 \\ 0 \\ 1 \\ 1 \end{bmatrix} \quad \text{and} \quad [A(1)B(1)A(2)] = \begin{bmatrix} 0\,1\,0 \\ 0\,0\,1 \\ 1\,1\,1 \\ 1\,1\,0 \end{bmatrix}$$

Similarly, $B(2)$ and $B(3)$ are determined to reconstruct ($black$, $black$) and ($black$, $white$) by $[A(2), B(2), A(3)]$ and $[A(3), B(3), A(1)]$, respectively.
Hence

$$[A(1)B(1)A(2)B(2)A(3)B(3)] = \begin{bmatrix} 0\,1\,0\,1\,1\,0 \\ 0\,0\,1\,1\,0\,1 \\ 1\,1\,1\,0\,1\,1 \\ 1\,1\,0\,1\,0\,1 \end{bmatrix},$$

and thus the desired colors are reconstructed.

We now prove that a similar construction is always possible for every even integer $n \geq 4$. In order to do so, we need the next lemma.

Lemma 1. *Let $r \geq 2$ be an integer. Then a sequence $(X_1, X_2, \cdots, X_r)$ of r column vectors having the following properties can be constructed.*

(i) Each $X(i)$ consists of two 0 entries and two 1 entries.
(ii) For every $1 \le i \le r$, $[X(i)X(i+1)]$ consist of

$$[0\ 0],\ [0\ 1],\ [1\ 0],\ [1\ 1].$$

(iii) For any integer $1 \le k \le r$, we cannot guess $X(k)$ from the set $\{X(i) \mid 1 \le i \le r, i \ne k\}$ of $r-1$ vectors.

Proof. We first take $X(1)$ as

$$X(1) = \begin{bmatrix} 0 \\ 0 \\ 1 \\ 1 \end{bmatrix}.$$

If $r = 2$, then $X(2)$ is determined as one of the following four vectors :

$$X(2) = \begin{bmatrix} a \\ b \\ c \\ d \end{bmatrix},\ \text{where } \{a, b\} = \{c, d\} = \{0, 1\}.$$

Assume $r \ge 3$. If $X(j)$, $j \ge 1$, is given, then $X(j+1)$ is obtained from $X(j)$ by independently and randomly replacing

$$\begin{bmatrix} 0 \\ 0 \end{bmatrix} \text{ and } \begin{bmatrix} 1 \\ 1 \end{bmatrix} \text{ by } \begin{bmatrix} 0 \\ 1 \end{bmatrix} \text{ or } \begin{bmatrix} 1 \\ 0 \end{bmatrix}.$$

Thus there exist four distinct $X(j+1)$. By this method, we can obtain $X(1)$, $X(2)$, $\cdots$, $X(r-1)$. The last vector $X(r)$ is randomly determined as follows depending on both $X(r-1)$ and $X(1)$. By symmetry, we may assume that $X(r-1)$ is one of the following vectors

$$X(r-1) = \begin{bmatrix} 0 \\ 0 \\ 1 \\ 1 \end{bmatrix},\ \begin{bmatrix} 0 \\ 1 \\ 1 \\ 0 \end{bmatrix} \text{ or } \begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \end{bmatrix}.$$

Then determine

$$X(r) = \begin{bmatrix} a \\ b \\ c \\ d \end{bmatrix},\ \begin{bmatrix} a \\ b \\ a \\ b \end{bmatrix} \text{ or } \begin{bmatrix} a \\ b \\ c \\ d \end{bmatrix},\ \text{respectively,}$$

where $\{a, b\} = \{c, d\} = \{0, 1\}$. Finally permute all the entries of all $X(i)$ simultaneously by any permutation on $\{1, 2, 3, 4\}$.

We now prove the condition (iii). For any integer $1 \leq k \leq r$, consider the set $\{X(i) \mid 1 \leq i \leq r, i \neq k\}$. Without loss of generality, we may assume that

$$X(k-1) = \begin{bmatrix} 0 \\ 0 \\ 1 \\ 1 \end{bmatrix} \quad \text{and}$$

$$X(k+1) = \begin{bmatrix} 0 \\ 0 \\ 1 \\ 1 \end{bmatrix}, \quad \begin{bmatrix} 0 \\ 1 \\ 1 \\ 0 \end{bmatrix} \quad \text{or} \quad \begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \end{bmatrix}.$$

Then

$$X(k) = \begin{bmatrix} a \\ b \\ c \\ d \end{bmatrix}, \quad \begin{bmatrix} a \\ b \\ a \\ b \end{bmatrix} \quad \text{or} \quad \begin{bmatrix} a \\ b \\ c \\ d \end{bmatrix}, \text{respectively,}$$

where $\{a, b\} = \{c, d\} = \{0, 1\}$. Hence we cannot guess $X(k)$ from $\{X(i) \mid 1 \leq i \leq r, i \neq k\}$.

We are now ready to give a construction of the whole sequence. By Lemma 1, first take a random sequence $(A(1), A(2), \ldots, A(r))$. Then each $B(i)$ is chosen from the following four vectors so that $(A(i), B(i), A(i+1))$ reconstructs $(img(2i-1), img(2i))$ or $(img(2i), img(2i+1))$ according to the decision of $S(i)$'s. Namely, we apply the same procedure in the case of $n = 6$.

$$\begin{bmatrix} 0 \\ 1 \\ 1 \\ 1 \end{bmatrix}, \begin{bmatrix} 1 \\ 0 \\ 1 \\ 1 \end{bmatrix}, \begin{bmatrix} 1 \\ 1 \\ 0 \\ 1 \end{bmatrix}, \begin{bmatrix} 1 \\ 1 \\ 1 \\ 0 \end{bmatrix}.$$

We now discuss the security. Assume that $(A(1), B(1), A(2), \ldots, B(r)) = (S(1), S(2), \ldots, S(n))$. It is easy to see that if $B(i)$ is missing, then we cannot get any information about $img(2i-1)$ and $img(2i)$. So we shall next show that if two consecutive shares $A(k), B(k)$ or $B(k), A(k+1)$ are missing, then we cannot get any information about the three secret images ($Image(2k-2)$, $img(2k-1)$, $img(2k)$) or ($img(2k-1)$,$img(2k)$, $img(2k+1)$). By symmetry, we may assume that $A(k)$ and $B(k)$ are missing. It is clear that no information about ($img(2k-1)$, $img(2k)$) leaks because of a missing of $B(k)$. By the statement (iii) of Lemma 1, we cannot guess $A(k)$ from $\{A(i) \mid 1 \leq i \leq r, i \neq k\}$, which implies no information about $img(2k-2)$) leaks. Consequently, the construction of VSS scheme with cycle access structure for even number images is secure in the sense (b*).

We conclude the paper with the following problem.

Problem For every odd integer $n \geq 5$, can we construct a VSS scheme with cyclic access structure for n images that satisfies (a), (b*), (c) and has contrast 1/4?

References

1. G. Ateniese, C. Blundo, A. De Santis, and D.R. Stinson, "Visual Cryptography for General Access Structures," Information and Computation, vol.129 (1996) pp.86-106.
2. C. Blundo, A. De. Bonis and A. De. Santis, "Improved schemes for visual cryptography," Designs, Codes and Cryptography," vol. 24 (2001) 255–278.
3. C. Blundo, A.De Santis, and D.R. Stinson, "On the Contrast in Visual Cryptography Schemes," J. Cryptology, vol. 12 (1999) 261–289.
4. C. Blundo and A. De Santis, "Visual cryptography schemes with perfect reconstruction of black pixels," Computer and Graphics, vol.22, no.4, (1998) pp.449-455.
5. S. Droste, "New results on visual cryptography," Advances in Cryptology-CRYPTO'96, LNCS, vol. 1109 (1996), 401–415.
6. M. Iwamoto and H. Yamamoto, "A construction method of visual secret sharing schemes for plural secret image," IEICE Trans. Fundamentals, vol. E86-A, no.10 (2003), 2577–2588.
7. H. Koga and E. Ueda, "The optimal (t, n)-threshold visual secret sharing scheme with perfect reconstruction of black pixels," Designs, Codes and Cryptography, vol.40 Issue 1 (2006) 81–102.
8. H. Koga, "A general formula of the (t, n)-threshold visual secret sharing scheme," Advances in cryptology–ASIACRYPT 2002, LNCS vol. 2501 (2002) 328–345.
9. M. Naor and A. Shamir, "Visual cryptography," Advances in Cryptology, Eurocrypt'94, LNCS, vol. 950 (1994) 1–12.
10. M. Uno and M. Kano, " Visual Cryptography Schemes with Dihedral Group Access Structure for Many Images," ISPEC2007, LNCS, vol.464, (2007) 344–359.
11. F. Yi, D. Wang, P. Luo, L. Huang, Y. Dai, "Multi secret image color visual cryptography schemes for general access structures," Progr. Natur. Sci. (English Ed.) 16 (2006), no. 4, 431–436.

A Appendix A : Non-existence of the VSS Scheme with Contrast Greater than 1/6 where $n = 3$

We now prove that for the VSS of three secret images, the contrast 1/6 is best possible. Consider any construction of a perfect VSS scheme with cyclic access structure for three shares and three secret images. We shall use the same notations as in Section 3. Assume that $S(i)$ consists of m subpixels, namely, each pixel is split into m subpixels, where $m \geq 2$. Let us define two subsets $W_i,\ B_i \subseteq \{1, 2, \cdots, m\}$ as in Section 3. Put $|W_i| = w_i$ and $|B_i| = b_i$. Then $m = w_i + b_i$ for every $i \in \{1, 2, 3\}$. Let λ denote the minimum number of $|W_i \cap W_{i+1}|$ such that $img(i)$ is white and $1 \leq i \leq 3$.

By considering the colors $(img(1), img(2), img(3)) = (black, black, black)$, we have that W_i and W_j are disjoint for $i \neq j$, that is, $S(i)$ and $S(j)$ have no white subpixels in common (Fig. 6 (i),(ii),(iv)). Thus

$$m = |S(i)| \geq |W_1| + |W_2| + |W_3|. \tag{20}$$

Similarly, by considering the colors $(img(1), img(2), img(3)) = (white, white, black)$, we have that $|W_1 \cap W_2| \geq \lambda$, $|W_2 \cap W_3| \geq \lambda$ and $W_3 \cap W_1 = \emptyset$ (Fig. 6

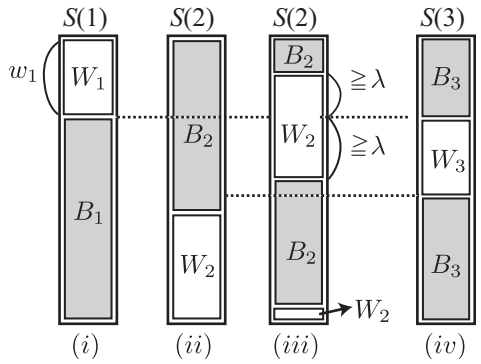

Fig. 6. W_i and B_i denote the indices of white and black subpixels of $S(i)$, respectively.

(i),(iii),(iv)). Hence $|W_2| \geq 2\lambda$. By considering other similar colors, we can obtain that $|W_1| \geq 2\lambda$ and $|W_3| \geq 2\lambda$. Therefore it follows from (20) that $m = |S(i)| \geq 6\lambda$, which implies that $\lambda/m \leq 1/6$. Hence the contrast of a VSS scheme for three images satisfying the conditions (a), (b), (c) is less than or equal to 1/6.

A Appendix B : An example of cyclic VSS scheme where $n = 6$

An example of VSS scheme with cyclic access structure for six shares and six secret images are shown below. Here we encode secret images of 100×100 pixels. Two shares $Share(i)$ and $Share(i+1)$ recover $Image(i)$, where $Share(1) = Share(7)$.

Fig. 7. The secret image $Image(2)$.

Fig. 8. A reconstructed image $Image(1)$

Fig. 9. A reconstructed image $Image(2)$