Draft

Visual Cryptography Schemes with Dihedral Group Access Structure for Many Images

Miyuki Uno[1] and M. Kano[2]

Department of Computer and Information Sciences,
Ibaraki University, Hitachi, 316-8511, Japan
[1] umyu@mug.biglobe.ne.jp [2] kano@mx.ibaraki.ac.jp
http://gorogoro.cis.ibaraki.ac.jp/

Abstract

A new construction of visual cryptography scheme (VCS) with dihedral group access structure for two shares and many secret images is proposed. Let D_{2n} be a dihedral group of order $2n$, and let $\{Image(\tau) \mid \tau \in D_{2n}\}$ be $2n$ secret images corresponding to D_{2n}. In a VCS with dihedral group access structure, two shares (two transparencies) A and B are constructed so that for any element τ of D_{2n}, A and $\tau(B)$ reconstruct the secret image $Image(\tau)$. This new VCS is perfect and has contrast $1/(6n^2)$.

Keywords: visual cryptography, VCS, visual secret sharing, VSS, diheadral group, many secret images.

1 Introduction

A visual cryptography scheme (VCS), which was proposed by Shamir and Naor [5] ([4]), is a method of encoding a secret image into some shares, which are usually printed on transparencies. In k-out-of-n VCS, the secret image is encoded into n shares. If any k set of n shares are stacked together, then the original secret image is reconstructed, but any set of shares less than k does not leak any information about the secret image.

Droste [1] introduced the following new VCS and gave its construction. Let $\mathcal{F}$ be a family of non-empty subsets of $\{1, 2, \ldots, n\}$, and $\{Image(A) \mid A \in \mathcal{F}\}$ be a set of $|\mathcal{F}|$ different secret images. Then we can make n shares $S(1), S(2), \ldots, S(n)$ so that for any element $A \in \mathcal{F}$, a stack of the shares in $\{S(i) \mid i \in A\}$ reconstructs the secret image $Image(A)$, and we cannot get any information on $Image(B)$ from the set of transparencies if $B \not\subseteq A$. This kind of VCS for many secret images has been studied in some papers including [3], [6], [2].

In this paper we consider a VCS with dihedral group access structure, which is defined below, and give its construction. Let

$$D_{2n} = \{1, \alpha, \ldots, \alpha^{n-1}, \beta, \beta\alpha, \ldots, \beta\alpha^{n-1}\}$$

be a *dihedral group* of order $2n$, where α denotes a rotation with angle $2\pi/n$ and β denotes a horizontal reversion. Let $\{Image(\tau) \mid \tau \in D_{2n}\}$ be a set of $2n$ secret images, each of which corresponds to an element of D_{2n} and is comprised of black

and white pixels. Then two shares A and B, which are printed on transparencies, are constructed so that for any element $\tau \in D_{2n}$, by staking A and $\tau(B)$, the secret image $Image(\tau)$ is obtained (see Figure 1). This VCS is called a *VCS with dihedral group access structure* for two shares and $2n$ secret images. We give a new construction of this *perfect* VCS with contrast $1/(6n^2)$, where a perfect VCS means that a black pixel of a secret image is reconstructed into a pure black region, while a white pixel is translated into a region consisting of white and black subpixels.

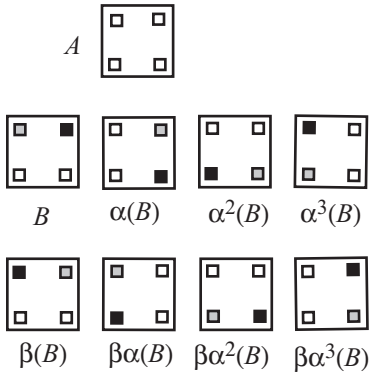

Figure 1: Two shares A and B of VCS with D_8 access structure.

This paper is organized as follows: In Sect. 2, a construction of a VCS with D_{2n} access structure is given, but it has a contrast $1/(8n^2)$. In Sect. 3, we give a revised construction of a perfect VCS with reverse access structure, which is a VCS with $\{1, \beta\}$ access structure. In Sect. 4, by using the construction given in Sect. 3 we obtain an improved construction of a perfect VCS with D_{2n} access structure, whose contrast is $1/(6n^2)$. In appendix, an example of the improved VCS with D_4 access structure is given.

2 A construction of VCS with dihedral group access structure

In this section we give a construction of a VCS with dihedral group D_{2n} access structure for two shares and $2n$ secret images. It has contrast $1/(8n^2)$ though an improved VCS given latter has contrast $1/(6n^2)$. Let D_{2n} be a dihedral group defined in Section 1, which is generated by the rotation α with angle $2\pi/n$ and the horizontally reversion β. Let A and B be two shares, and let $\{Image(\tau) \mid \tau \in D_{2n}\}$ be a set of $2n$ distinct secret images, that is, given $2n$ secret images are assigned to the elements of D_{2n}.

We first define two 2×2 matrices $R1$ and $R2$, which are randomly chosen from the following matrices according to the color of a pixel in an image.

$$R1 \in \left\{ \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \right\}, \quad R2 \in \left\{ \begin{bmatrix} 0 & 1 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 1 & 0 \end{bmatrix} \right\}.$$

Let x and y be pixels of the shares A and B, respectively, such that x and y are in the same position when we stack A and B. Then $\{\tau(x) \mid \tau \in D_{2n}\}$ and $\{\tau(y) \mid \tau \in D_{2n}\}$ are the sets of $2n$ pixels of A and B, respectively, such that they have the same position in some $A+\tau(B)$, $\tau \in D_{2n}$ (Figures 2, 3). Notice that in the following figures, every pixel and subpixel are rectangular, but this condition is not necessary. Actually for some VCS with D_{2n} access structure, triangles and other figures can be used.

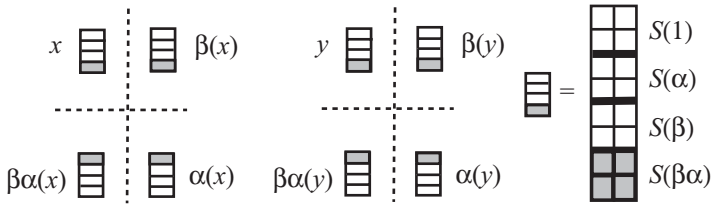

Figure 2: A construction of VCS with D_4 access structure, where x and y denote pixels and are split into 16 subregions each.

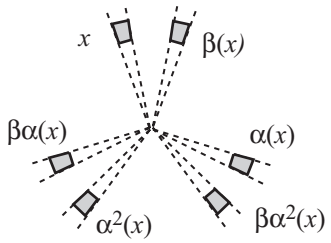

Figure 3: A construction of VCS with D_6 access structure.

Each pixel of A and B is first split into $4n^2$ *subregions*, and latter each of these subregions is split into two *subpixels*, and so finally original pixel is split into $8n^2$ subpixels. The dihedral group D_{2n} acts on the set of subregions of $\{\tau(x) \mid \tau \in D_{2n}\}$, which contains $2n \cdot 4n^2$ subregions. Every orbit of this permutation has length $2n$, and there are $4n^2$ orbits. We divide these $4n^2$ orbits into $2n$ disjoints subsets, each of which contains $2n$ orbits, and label them $\{S(\tau) \mid \tau \in D_{2n}\}$.

Example 1: Our construction of VCS with D_4 access structure, where $D_4 = \{1, \alpha, \beta, \beta\alpha\}$, will be given. In Figure 4, (1) denotes the set of $2n \cdot 4n^2 = 16 \cdot 2^2$ subregions, which consists of $4 \cdot 2^2$ orbits, and each orbit contains four subregions. We mark some subregions with some symbols to emphasis its orbit. Using this example, we explain the rule of determining the color of each subpixel. In order to do so easily, we rearrange all the subregions so that each orbit consists of the subregions lying on the same position (see (2)). Moreover, these orbits are partitioned into four subsets $S(1), S(\alpha), S(\beta), S(\beta\alpha)$. Of course, there is a bijection between the subregions of (1) and those of (2), and thus if we determine the colors of subregions of (2), the colors of original subregions are determined. Let $\tau \in D_4$. For any

element $\rho \in D_4$, choose one subregion $sub(\rho, x, \tau)$ from $\rho(x) \cap S(\tau)$ so that the four subregions $sub(\rho, x, \tau), \rho \in \{1, \alpha, \beta, \beta\alpha\}$, are contained in four distinct orbits of $S(\tau)$. Furthermore, for any fixed ρ, we can choose $sub(\rho, x, \tau)$ so that it is placed at the same position in every $S(\tau), \tau \in D_4$ (see (2)).

For a pixel y of B, which is placed at the same position as x of A, we first split it into $16 \cdot 2^2$ subregions. Then for any $\gamma, \rho \in D_4$, choose a subpixel $sub(\rho, y, \gamma)$ from $\rho(y) \cap S(\gamma)$ of B that is placed at the same positions as

$$sub(\gamma^{-1}\rho, x, \gamma) \quad \text{of } A \ \text{ (see (3))}.$$

Thus, by $\tau \in D_4$, the subregion $sub(\rho, y, \tau)$ in B is moved to the following subregion in $\tau(B)$:

$$sub(\tau\tau^{-1}\rho, x, \tau) = sub(\rho, x, \tau),$$

which is in the same position of $sub(\rho, x, \tau)$ in A. Namely, the subregions $sub(\rho, y, \tau)$ in B and $sub(\rho, x, \tau)$ in A are placed at the same position in $A + \tau(B)$, and so they are used to make a color of the pixel $\rho(z)$ of $Image(\tau)$, which is reconstructed by $A + \tau(B)$.

Consider the secret image $Image(\tau)$. We determine the basis matrix of $sub(\rho, x, \tau)$ and $sub(\rho, y, \tau)$, $\rho \in D_{2n}$, by using matrices $R1$ and $R2$ as follows according to the color of a pixel $\rho(z)$ of $Image(\tau)$, which is placed at the same position as $\rho(x)$.

$$\begin{bmatrix} sub(\rho, x, \tau) \\ sub(\rho, y, \tau) \end{bmatrix} = \begin{cases} R1 & \text{if } \rho(z) \text{ is black,} \\ R2 & \text{if } \rho(z) \text{ is white,} \end{cases}$$
$$\text{and all the non-chosen subregions are } [1, 1],$$

Notice that all the subregions are split into two subpixels each. We repeat the same procedure for every non-chosen pixel $z \in Image(\tau)$ and for all secret images until the colors of all the subpixels of shares A and B are determined. By the definition of $sub(\rho, x, \tau)$ and $sub(\rho, y, \gamma)$, when we stack A and $\tau(B)$, $Image(\tau)$ is reconstructed and its contrast is $1/32$ since each pixel is finally split into 32 subpixels.

Now we explain our construction of VCS with general dihedral group D_{2n} access structure. Each pixel of shares A and B is split into $4n^2$ subregions, and for every $\rho \in D_{2n}$, one subregion $sub(\rho, x, \gamma)$ is chosen from $\rho(x) \cap S(\gamma)$ of A as Example 1, and $sub(\rho, y, \gamma)$ is the subregion placed at the position as $sub(\tau^{-1}\rho, x, \gamma)$. For any image $Image(\tau)$ and any element $\rho \in D_{2n}$, let $\rho(z)$ be a pixel of $Image(\tau)$, and let $\rho(x)$ and $\rho(y)$ be the pixels of A and B being in the same position of $\rho(z)$. We determine $sub(\rho, x, \tau)$ and $sub(\rho, y, \tau)$ as

$$\begin{bmatrix} sub(\rho, x, \tau) \\ sub(\rho, y, \tau) \end{bmatrix} = \begin{cases} R1 & \text{if } \rho(z) \text{ is black,} \\ R2 & \text{if } \rho(z) \text{ is white,} \end{cases}$$
$$\text{and all the non-chosen subregions are } [1, 1],$$

where all the subregions are split into two subpixels each.

By the definition of $sub(\rho, x, \tau)$ and $sub(\rho, y, \tau)$, the color of the region $\rho(z)$ in $A + \tau(B)$ is determined by $sub(\rho, x, \tau)$ and $\tau(sub(\rho, y, \tau))$, and thus $Image(\tau)$ is reconstructed. It is easy to see that its contrast is $1/(8n^2)$ and we cannot get any

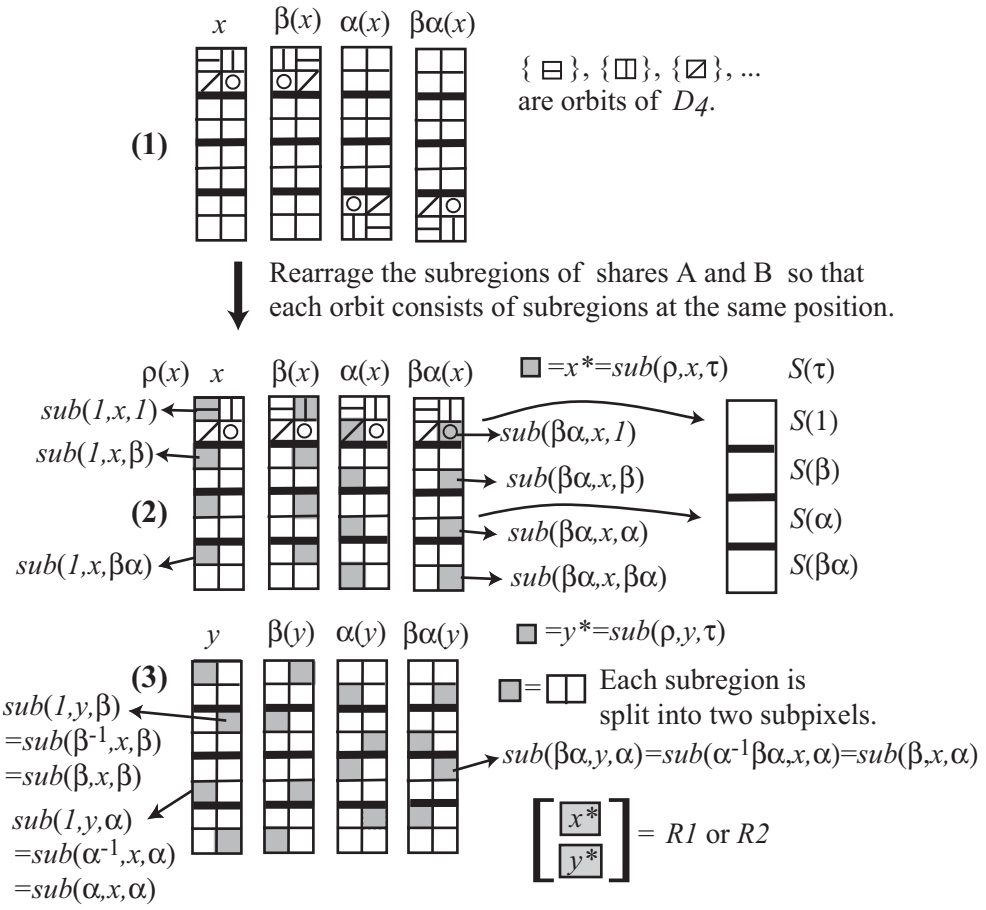

Figure 4: A construction of VCS with D_4 access structure. Gray squares denote $sub(\rho, x, \tau)$ of A and $\rho(\rho, y, \tau)$ of B.

information about the secret images from one of $\{A, B\}$ since (i) each $sub(\rho, x, \tau)$ in A is $[0, 1]$, $[1, 0]$ or $[1, 1]$, (ii) $[1, 1]$ means that the color of the pixel is determined by other subregion, and (iii) there is no difference between white pixel and black pixel of the image; and the same conditions hold for B. Consequently we can construct a VCS with dihedral group access structure.

3 A revised construction of VCS with reverse access structure

We give a new construction of VCS with reverse access structure, which will play important role in the next section. Our method of constructing VCS with reverse access structure is different from the method given in the previous section. The contrast of our construction is 1/6, but that of the preceding construction is 1/8. Moreover, it will be shown that the construction given here is best possible in some sense. Namely, we will prove in the appendex that it is impossible to construct a

perfect VCS with reverse access structure with contrast 1/5 or more.

For a share X, we briefly denote by $\tilde{X}$ the share $\beta(X)$, which is obtained by horizontally reversing X (Figures 5, 6). Suppose that two distinct secret images $Image1$ and $Image2$ are given. We want to encode these two secret images into two shares A and B so that we can reconstruct $Image1$ and $Image2$ by stacking A and B, and by A and $\tilde{B}$, respectively (see Figures 5, 6). We call this VCS a *VCS with reverse access structure*.

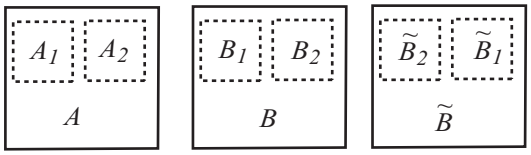

Figure 5: A VCS with reverse access structure.

We now explain our construction of VCS with reverse access structure. Let A_1 and A_2 be two pixels of A, and B_1 and B_2 be the two pixels of B such that A_i covers B_i in orderly stacking, and A_i covers $\tilde{B}_j$ in reversely stacking, where $\{i, j\} = \{1, 2\}$ (Figures 5, 6). We split each of these pixels into six subpixels. Then A_i and B_i are expressed as $A_i = (x_{ij})$ and $B_i = (y_{ij})$, where x_{ij} and y_{ij} denote subpixels. For convenience, we also regard $A_i = (x_{ij})$ and $B_i = (y_{ij})$ as their basis matrices, that is, we assume that x_{ij} and y_{ij} express subpixels and their colors $x_{ij}, y_{ij} \in \{0, 1\} = \{white, black\}$. Let us write $A_i = (x_{ij})$ and $B_i = (y_{ij})$ as Figure 6, where the suffixes of A_2 and B_2 are reversed.

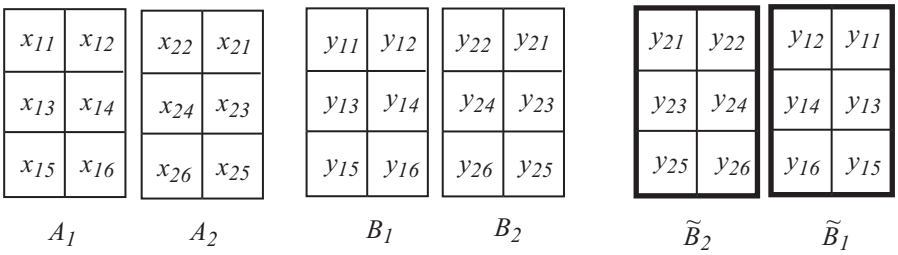

Figure 6: Subpixels of A, B, and $\tilde{B}$.

If we orderly stack A and B, then the subpixels of the resulting region are

$$x_{ij} + y_{ij} \quad \text{for} \quad 1 \le i \le 2, \quad 1 \le j \le 6,$$

where $+$ denotes OR of two elements, and if we reverse B and stack it and A together, then the the subpixels of the resulting region are

$$x_{ij} + y_{i'j}, \quad \text{where} \quad \{i, i'\} = \{1, 2\}, \quad 1 \le j \le 6.$$

The pairs of this operation " $+$ " between elements of A_i and those of B_i or $\tilde{B}_{i'}$ are represented by the diagram given in Figure 7. Thus, for example, if the pixel of

$Image1$ placed at A_1 is black, then the basis matrices should satisfy

$$\begin{aligned} & x_{11}+y_{11}=x_{12}+y_{12}=x_{13}+y_{13} \\ = \;& x_{14}+y_{14}=x_{15}+y_{15}=x_{16}+y_{16}=1 \end{aligned}$$

because our VCS is perfect. Similarly, if the pixel of $Image2$ placed at A_1 is white, then at least one of the following six elements is equal to 0 because the contrast of our VCS is 1/6.

$$\begin{aligned} & x_{11}+y_{21},\ x_{12}+y_{22},\ x_{13}+y_{23}, \\ & x_{14}+y_{24},\ x_{15}+y_{25},\ x_{16}+y_{26}. \end{aligned}$$

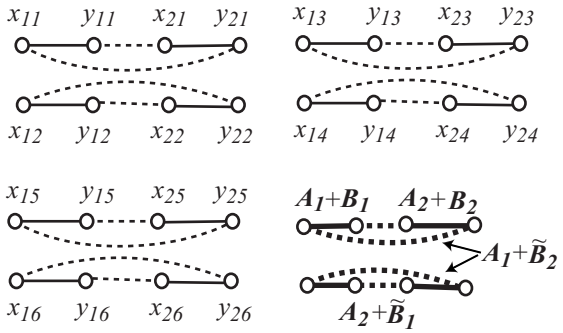

Figure 7: The diagram representing the pairs of " + ".

We now define the three 2×2 matrices as follows:

$$M1=\begin{bmatrix} 0 & 0 \\ 1 & 1 \end{bmatrix},\ M2=\begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix},\ \text{ and }\ M3=\begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix} \tag{1}$$

Then we tentatively define the two basis matrices A_1 and A_2 as follows:

$$[A_1, A_2]=\begin{bmatrix} x_{11} & x_{21} \\ x_{12} & x_{22} \\ x_{13} & x_{23} \\ x_{14} & x_{24} \\ x_{15} & x_{25} \\ x_{16} & x_{26} \end{bmatrix}=\begin{bmatrix} M1 \\ M2 \\ M3 \end{bmatrix}=\begin{bmatrix} 0 & 0 \\ 1 & 1 \\ 0 & 1 \\ 1 & 1 \\ 1 & 1 \\ 1 & 0 \end{bmatrix}. \tag{2}$$

We next define the matrices B_1 and B_2 according to the set of colors $\{A_1+B_1,\ A_2+\tilde{B}_1,\ A_2+B_2,\ A_1+\tilde{B}_2\}$. For example, if their colors are

$$\begin{aligned} & A_1+B_1=black,\ A_2+\tilde{B}_1=black, \\ & A_2+B_2=white,\ A_1+\tilde{B}_2=black, \end{aligned} \tag{3}$$

then by considering Figure 7, we define

$$[B_1, B_2] = \begin{bmatrix} y_{11} & y_{21} \\ y_{12} & y_{22} \\ y_{13} & y_{23} \\ y_{14} & y_{24} \\ y_{15} & y_{25} \\ y_{16} & y_{26} \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 0 & 1 \\ 1 & 1 \\ 0 & 0 \\ 1 & 1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} M2^* \\ M1^* \\ M3 \end{bmatrix},$$

where Mi^* is obtained from Mi only by exchanging the first and the second rows. Then it is clear that these matrices satisfy the color condition (3).

In fact, when we distribute subpixels, we randomly permute the six rows of (A_1, A_2) and (B_1, B_2) simultaneously. Thus there are no difference between the above two matrices $[A_1, A_2]$ and $[B_1, B_2]$.

We shall show that for any set of colors, we can define the basis matrices B_1 and B_2 that satisfy the given color condition and posses the following properties: (i) (B_1, B_2) consists of the three matrices choosing one from each $\{M1, M1^*\}, \{M2, M2^*\}, \{M3, M3*\}$; (ii) the VCS is perfect; and (iii) the VCS has contrast 1/6. By the property (i) and symmetry, our construction guarantees that the VCS is secure, that is, we cannot get any information about secret images from one of $\{(A_1, A_2),\ (B_1, B_2)\}$.

We prove that for any set of colors, we can always define the matrices (B_1, B_2) possessing the above properties. We consider the following three cases.

Case 1. *Two consecutive colors in* $(A_1 + B_1,\ A_2 + \tilde{B}_1,\ A_2 + B_2,\ A_1 + \tilde{B}_2)$ *are white.*

Suppose first $A_1 + B_1 = A_2 + \tilde{B}_1 = white$. In this case we define the first and second rows of (B_1, B_2) as follows:

$$[B_1, B_2] \supset \begin{bmatrix} y_{11} & y_{21} \\ y_{12} & y_{22} \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix} = M2,$$

Then $A_1 + B_1 = A_2 + \tilde{B}_1 = white$, and the other colors $A_2 + B_2$ and $A_1 + \tilde{B}_2$ are determined by the remaining rows of (B_1, B_2). We define the remaining rows of (B_1, B_2) as follows according to $(A_2 + B_2,\ A_1 + \tilde{B}_2) = (black, black)$, $(black, white)$, $(white, black)$, $(white, white)$.

$$[B_1, B_2] \supset \begin{bmatrix} y_{13} & y_{23} \\ y_{14} & y_{24} \\ y_{15} & y_{25} \\ y_{16} & y_{26} \end{bmatrix} = \begin{bmatrix} 1 & 1^* \\ 0 & 0 \\ 1 & 0 \\ 1 & 1^* \end{bmatrix},$$

$$\begin{bmatrix} 0 & 0^* \\ 1 & 1 \\ 1 & 0 \\ 1 & 1^* \end{bmatrix}, \begin{bmatrix} 1 & 1^* \\ 0 & 0 \\ 1 & 1 \\ 1 & 0^* \end{bmatrix}, \text{ or } \begin{bmatrix} 0 & 0^* \\ 1 & 1 \\ 1 & 1 \\ 1 & 0^* \end{bmatrix},$$

where only 0^* and 1^* guarantee the desired colors, and the remaining elements are determined so that two matrices coming from each of $\{M1,\ M1^*\}$ and $\{M3,\ M3^*\}$ appear.

By the symmetry of the diagram in Figure 7, we can similarly construct the desired basis matrices (A_1, A_2, B_1, B_2) in the other cases. For example, in the case of $A_2 + \tilde{B}_1 = A_2 + B_2 = white$, $A_1 + \tilde{B}_2 = X$, and $A_1 + B_1 = Y$, where $X, Y \in \{white, black\}$, we first define $\tilde{B}_1$ and $\tilde{B}_2$ as (2) then define the remaining matrix A_2 and A_1, which correspond to B_1 and B_2 in the above construction. Hence in this case we obtain the desired basis matrices A_1, A_2, B_1, B_2.

Case 2. *Two consecutive colors in* $(A_1 + B_1,\ A_2 + \tilde{B}_1,\ A_2 + B_2,\ A_1 + \tilde{B}_2)$ *are* $(white, black)$.

Suppose first $A_1 + B_1 = white$ and $A_2 + \tilde{B}_1 = black$. We define (A_1, A_2) by (2), and B_1 by

$$B_1 = \begin{pmatrix} y_{11} \\ y_{12} \\ y_{13} \\ y_{14} \\ y_{15} \\ y_{16} \end{pmatrix} = \begin{pmatrix} 1 \\ y_{12} \\ 0 \\ y_{14} \\ y_{15} \\ 1 \end{pmatrix}.$$

Then $A_1 + B_1 = white$ and $A_2 + \tilde{B}_1 = black$. We can easily determined the matrix B_2 and the remaining elements y_{12}, y_{14}, y_{15} of B_1 so that the desired colors of $A_2 + B_2$ and $A_1 + \tilde{B}_2$ are reconstructed and the three matrices $M1$, $M2$ and $M3$ appear.

By the symmetry of the diagram in Figure 7, we can similarly construct the desired basis matrices (A_1, A_2, B_1, B_2) in the other cases.

Case 3. $A_1 + B_1 = A_2 + \tilde{B}_1 = A_2 + B_2 = A_1 + \tilde{B}_2 = black$.

The (A_1, A_2) of (2) and the following (B_1, B_2) have the desired colors and properties.

$$(B_1, B_2) = \begin{bmatrix} 1 & 1 \\ 0 & 0 \\ 1 & 0 \\ 1 & 1 \\ 0 & 1 \\ 1 & 1 \end{bmatrix}.$$

Since Cases 1,2,3 covers all the cases, the proof is complete. Therefore we can construct a perfect VCS with reverse access structure with contrast 1/6.

4 An improved construction of VCS with dihedral group access structure

We present an improved construction of VCS with dihedral group access structure for two shares and $2n$ secret images by applying the VCS with reverse access structure

given in the previous section. Let D_{2n} be the dihedral group defined in the preceding sections. In our construction the contrast is $1/(6n^2)$.

First let $\Omega = \{(1, \beta), (\alpha, \beta\alpha), \ldots, (\alpha^{n-1}, \beta\alpha^{n-1})\}$ be the set of pairs of elements in D_{2n}. We construct a VCS in such a way that we apply the construction of VCS with reverse access structure to two secret images $Image(\rho)$ and $Image(\beta\rho)$ and some regions of two shares A and $\rho(B)$ for every $(\rho, \beta\rho) \in \Omega$. Namely, we split each pixel of shares A and B into $2n$ subregions, then for every $(\rho, \beta\rho) \in \Omega$, we encode two images $Image(\rho)$ and $Image(\beta\rho)$ into one subregion of every pixel of A and B so that $A+\rho(B)$ and $A+\beta\rho(B)$ reconstruct $Image(\rho)$ and $Image(\beta\rho)$, respectively. We begin with an example of this construction before giving a construction in general case.

Example 2: We construct a VCS with D_4 access structure. Let D_4=$\{1, \alpha, \beta, \beta\alpha\}$. Then $\Omega = \{(1, \beta), (\alpha, \beta\alpha)\}$. Let x and y be pixels of the shares A and B, respectively, such that x and y are in the same position when we stack A and B (Figure 8).

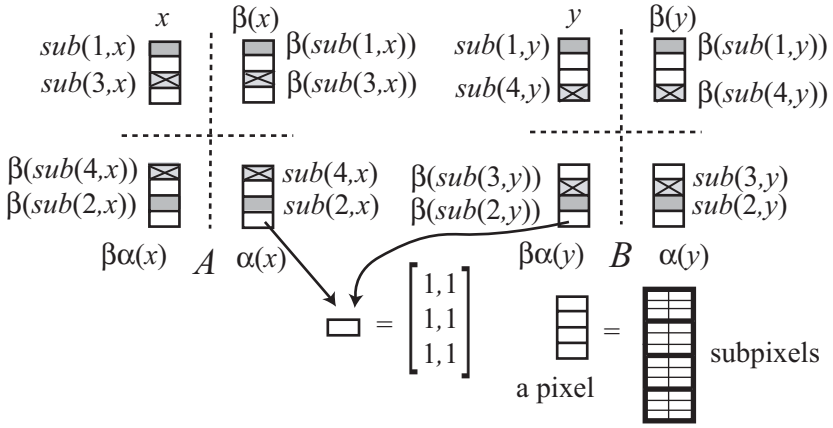

Figure 8: A construction of VCS with D_4 access structure. Every pixel is split into four subregions, and each subregion is split into six subpixels. Gray subregions reconstruct $Image(1)$ and $Image(\beta)$, and regions with cross reconstruct $Image(\alpha)$ and $Image(\beta\alpha)$.

We split every pixel in $\{\rho(x) \mid \rho \in D_4\}$ of A into four subregions. Then D_4 acts on the set of these subregions, and every orbit of this permutation has length four. We choose two subregions from each orbit such that they are transformed each other by β and exactly two subregions are chosen from each pixel, and denote these subregions by $sub(i, x), \beta(sub(i, x))$ $(1 \leq i \leq 4)$ (Figure 8). We also choose eight subregions $sub(i, y), \beta(sub(i, y))$ $(1 \leq i \leq 4)$ that are placed at the same positions as

$$sub(1, x),\ \beta(sub(1, x)),$$
$$sub(2, x),\ \beta(sub(2, x)),$$
$$\alpha^{-1}(sub(3, x)),\ \alpha^{-1}\beta(sub(3, x)),$$

$$\alpha^{-1}(sub(4,x)),\ \alpha^{-1}\beta(sub(4,x)),\ \text{respectively.}$$

By using the construction of VCS with reverse access structure, we can encode two secret images $Image(1)$ and $Image(\beta)$ into the eight subregions

$$\begin{aligned} & sub(1,x),\ \beta(sub(1,x)),\ sub(2,x),\ \beta(sub(2,x)) \quad \text{of } A \\ \text{and} \quad & sub(1,y),\ \beta(sub(1,y)),\ sub(2,y),\ \beta(sub(2,y)) \quad \text{of } B. \end{aligned}$$

Of course, we split each subregion into six subpixels. Next we encode two secret images $Image(\alpha)$ and $Image(\beta\alpha)$ into eight subregions

$$\begin{aligned} & sub(3,x),\ \beta(sub(3,x)),\ sub(4,x),\ \beta(sub(4,x)) \quad \text{of } A \\ \text{and} \quad & sub(3,y),\ \beta(sub(3,y)),\ sub(4,y),\ \beta(sub(4,y)) \quad \text{of } B. \end{aligned}$$

Then, for example, we can reconstruct $Image(1)$ by stacking A and B, and $Image(\alpha)$ by stacking A and $\alpha(B)$. The contrast of this VCS is $1/24 = 1/(6 \cdot 2^2)$.

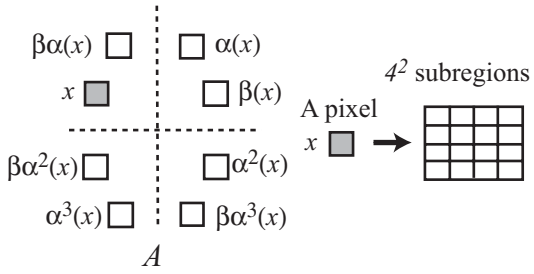

Figure 9: A construction of VCS with D_8 access structure.

We can similarly construct a VCS with general dihedral group D_{2n} access structure as Example 2. We first consider the share A. We split every pixel of A into n^2 subregions. Then D_{2n} acts on the set of subregions of pixels in $\{\rho(x) \mid \rho \in D_{2n}\}$, where every orbit has length $2n$ and there are n^2 orbits (Figures 9, 10). We divide these n^2 orbits into n disjoints subsets, each of which contains n orbits, and label them $\{T(j) \mid 0 \le j \le n-1\}$ (Figure 10). For every α^k $(0 \le k \le n-1)$, we choose the n subregions of $T(k) \cap \alpha^k(x)$, and the n subregions of $T(k) \cap \beta\alpha^k(x)$ (Figure 10).

We next consider the share B. First split every pixel of B into n^2 subregions. For every $0 \le h \le n-1$, choose the n subregions from $\alpha^h(y)$ that are placed at the same positions as the following subregions of A.

$$\{\alpha^{-j}(sub(h,j,x)) \text{ in } A \quad | \quad \text{the } (j+1)\text{-th chosen subregion } sub(h,j,x) \text{ of } \alpha^{j+h}(x),\ \ j = 0,1,\ldots,n-1\}\ ,$$

where the indexes of $T(h+j)$ are expressed module $2n$.

Similarly, we next choose the n subregions from $\beta\alpha^h(y)$ that are placed at the same positions as the following subregions in A.

$$\{\alpha^{-j}(sub(h,j,x)) \text{ in } A \quad | \quad \text{the } (j+1)\text{-th chosen subregion } sub(h,j,x) \text{ of } \alpha^j\beta\alpha^h(x) = \beta\alpha^{h-j}(x),\ \ j = 0,1,\ldots,n-1\}\ .$$

For every $0 \leq k \leq n-1$, the two secret images $Image(\alpha^k)$ and $Image(\beta\alpha^k)$ corresponding to $(\alpha^k, \beta\alpha^k) \in \Omega$ are encoded into the above $(k+1)$-th chosen subregions of A and B by using the construction of VCS with reverse access structure given in Section 4. Namely, we can reconstruct $Image(\alpha^k)$ by stacking A and $\alpha^k(B)$, and $Image(\beta\alpha^k)$ by A and $\beta\alpha^k(B)$. The first reconstruction follows from the fact that when we stack A and $\alpha^k(B)$, for every $0 \leq h \leq n-1$, the $(k+1)$-th chosen subregion of $\alpha^{k+h}(x)$ of A is $sub(h, k, x)$, and the subregions of B corresponding this subregion is placed at the $(k+1)$-th subregion of $\alpha^h(y)$ in B. Hence they are matched in $A + \alpha^k(B)$. Similarly, the subregion of $\beta\alpha^h(x)$ of A and its corresponding subregion of B are matched.

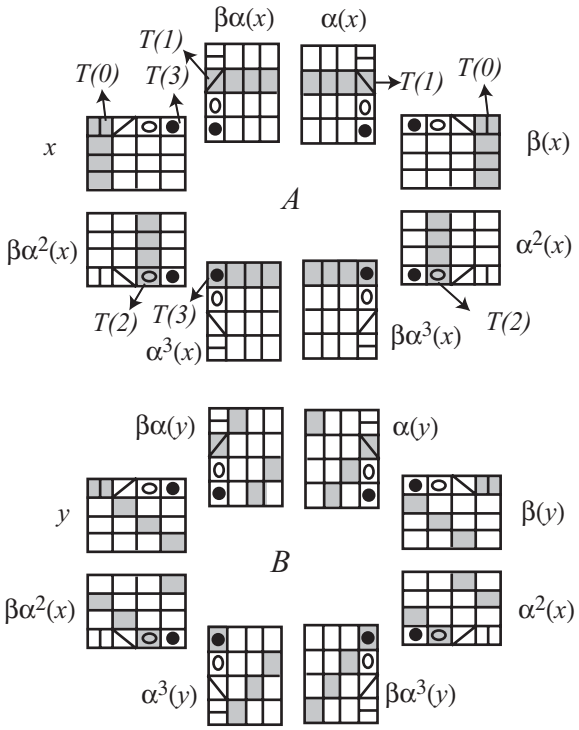

Figure 10: A construction of VCS with D_8 access structure. Gray rectangles denote the chosen subregions of A and B.

The similar situation holds when we stack A and $\beta\alpha^k(B)$, and so we can reconstruct $Image(\beta\alpha^k)$ by staking A and $\beta\alpha^k(B)$.

Consequently, we can construct the desired perfect VCS with dihedral group D_{2n} access structure having contrast $1/(6n^2)$.

5 Conclusions

In this paper, we consider constructions of perfect VCS with dihedral group D_{2n} access structure for two shares and $2n$ secret images. We first give a construction by using orbits of a permutation group. Next we give a revised construction of VCS

with reverse access structure, which is essentially different from the previous one. Then by using this new method, we give an improved construction of perfect VCS with dihedral group D_{2n} access structure, whose contrast is $1/(6n^2)$. It is difficult to find a construction with higher contrast, and so it might be possible to show that our new construction is best possible for some n.

References

[1] S. Droste, New results on visual cryptography, *Advances in Cryptology-CRYPTO'96, LNCS*, **1109** (1996) 401–415.

[2] M. Iwamoto and H. Yamamoto, A construction method of visual secret sharing schemes for plural secret images, *IEICE Trans. Fundamentals*, **E86-A** (2003) 2577-2588.

[3] T. Kato and H. Imai, An extended construction method of visual secret sharing scheme, *IEICE Trans. Fundamentals (in Japanese)*, **J79-A** (1996) 1344-1351.

[4] H. Koga, A general formula of the (t, n)-threshold visual secret sharing scheme, *Advances in cryptology–ASIACRYPT 2002*, LNCS **2501** (2002) 328–345.

[5] M. Naor and A. Shamir, Visual cryptography, *Advances in Cryptology, Eurocrypt'94, LNCS*, **950** (1995) 1–12.

[6] Y. Suga, K. Iwama, K. Sakurai and H. Imai, Extended graph-type visual secret sharing schemes with embedded plural images, *Inf. Process. Sco. Japan*, **42** (2001) 2106–2113.

Appendix A: A proof of sharpness of improved VCS with reverse access structure

We prove that it is impossible to construct a perfect VCS with reverse access structure of contrast 1/5. It is easy to prove the non-existence of such a VCS with higher contrast in the same way. We shall use the same notation of Section 3. Let

$$A_i = (x_{i1}, x_{i2}, x_{i3}, x_{i4}, x_{i5}) \text{ and } B_i = (y_{i1}, y_{i2}, y_{i3}, y_{i4}, y_{i5}), \quad i \in \{1, 2\}.$$

Then the colors of $A_i + B_i$ and $A_i + \tilde{B}_i$ are determined by $\{x_{ij} + y_{ij}\}$ and $\{x_{ij} + y_{i'j}\}$, respectively, where $\{i, i'\} = \{1, 2\}$ and $1 \le j \le 5$. Because of security, the sets $\{(x_{1j}, x_{2j}), 1 \le j \le 5\}$ and $\{(y_{1j}, y_{2j}), 1 \le j \le 5\}$ must consist of the same elements, respectively, for any colors of $\{A_i + B_i,\ A_i + \tilde{B}_i,\ i \in \{1, 2\}\}$. We consider the following two cases. Case 1 $(x_{1j}, x_{2j}) = (0, 0)$ for some j; and Case 2 neither (x_{1j}, x_{2j}) nor (y_{1j}, y_{2j}) is $(0, 0)$. Here we consider only Case 1 since Case 2 can be considered in a similar way. Without loss of generality, we may assume that $(x_{11}, x_{21}) = (0, 0)$.

Consider the case that the colors of $(A_1 + B_1,\ A_2 + \tilde{B}_1,\ A_2 + B_2,\ A_1 + \tilde{B}_2)$ are $(0, 1, 0, 1)$, where $1 = black$ and $0 = white$. Then for some $a, b \in \{1, 2, 3, 4, 5\}$, $a \neq b$, we have

$$(x_{1a}x_{1b}) = (01),\ (y_{1a}y_{1b}) = (01),\ (x_{2a}x_{2b}) = (10),\ (y_{2a}y_{2b}) = (10).$$

Hence we may assume that $\{(x_{1j}x_{2j}), j = 1, 2, 3\} = \{(00), (01), (10)\}$. By considering the case that the colors of $(A_1 + B_1,\ A_2 + \tilde{B}_1,\ A_2 + B_2,\ A_1 + \tilde{B}_2)$ are $(1, 1, 1, 1)$, we have

$$(y_{11}y_{12}y_{13}y_{14}y_{15}) = (11101),\ (y_{21}y_{22}y_{23}y_{24}y_{25}) = (11110),$$

where $(y_{14}y_{15}) = (y_{1a}y_{1b}) = (01)$ and $(y_{24}y_{25}) = (y_{2a}y_{2b}) = (10)$. By considering the case that the colors of $(A_1 + B_1,\ A_2 + \tilde{B}_1,\ A_2 + B_2,\ A_1 + \tilde{B}_2)$ are $(0, 0, 0, 0)$, we have

$$(x_{14}x_{15}) = (00),\ (x_{24}x_{25}) = (00).$$

Hence we may assume $\{(x_{1j}, x_{2j}), 1 \leq j \leq 5\} \supset \{(00), (00), (01), (10)\}$. Finally again by considering the case that the colors of $(A_1 + B_1,\ A_2 + \tilde{B}_1,\ A_2 + B_2,\ A_1 + \tilde{B}_2)$ are $(1, 1, 1, 1)$, we have $\{(y_{1j}, y_{2j}), 1 \leq j \leq 5\} \supset \{(11), (11), (11), (11)\}$, which contradicts the above fact that $(y_{1a}y_{1b}) = (01)$ and $(y_{2a}y_{2b}) = (10)$. Consequently the statement is proved.

Appendix B: An example of improved VCS with D_4 access structure

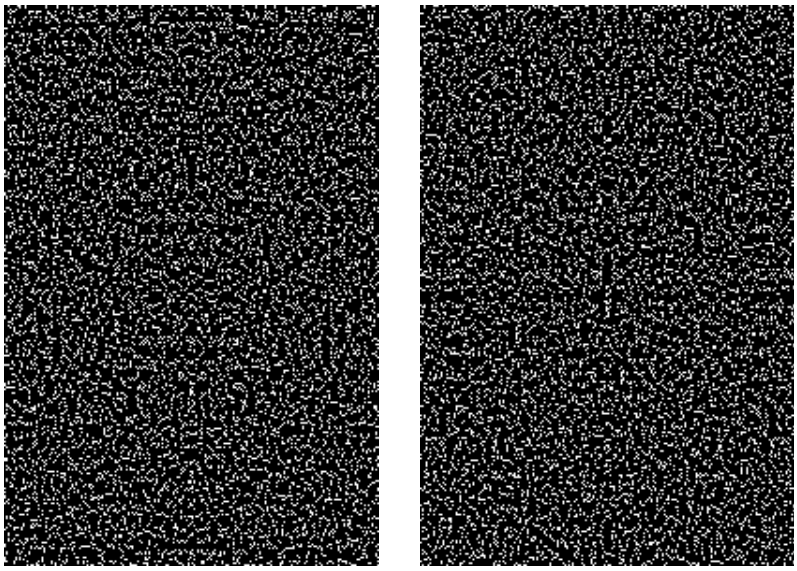

Figure 11: An example of improved VCS with D_4 access structure ($shareA$ and $shareB$).

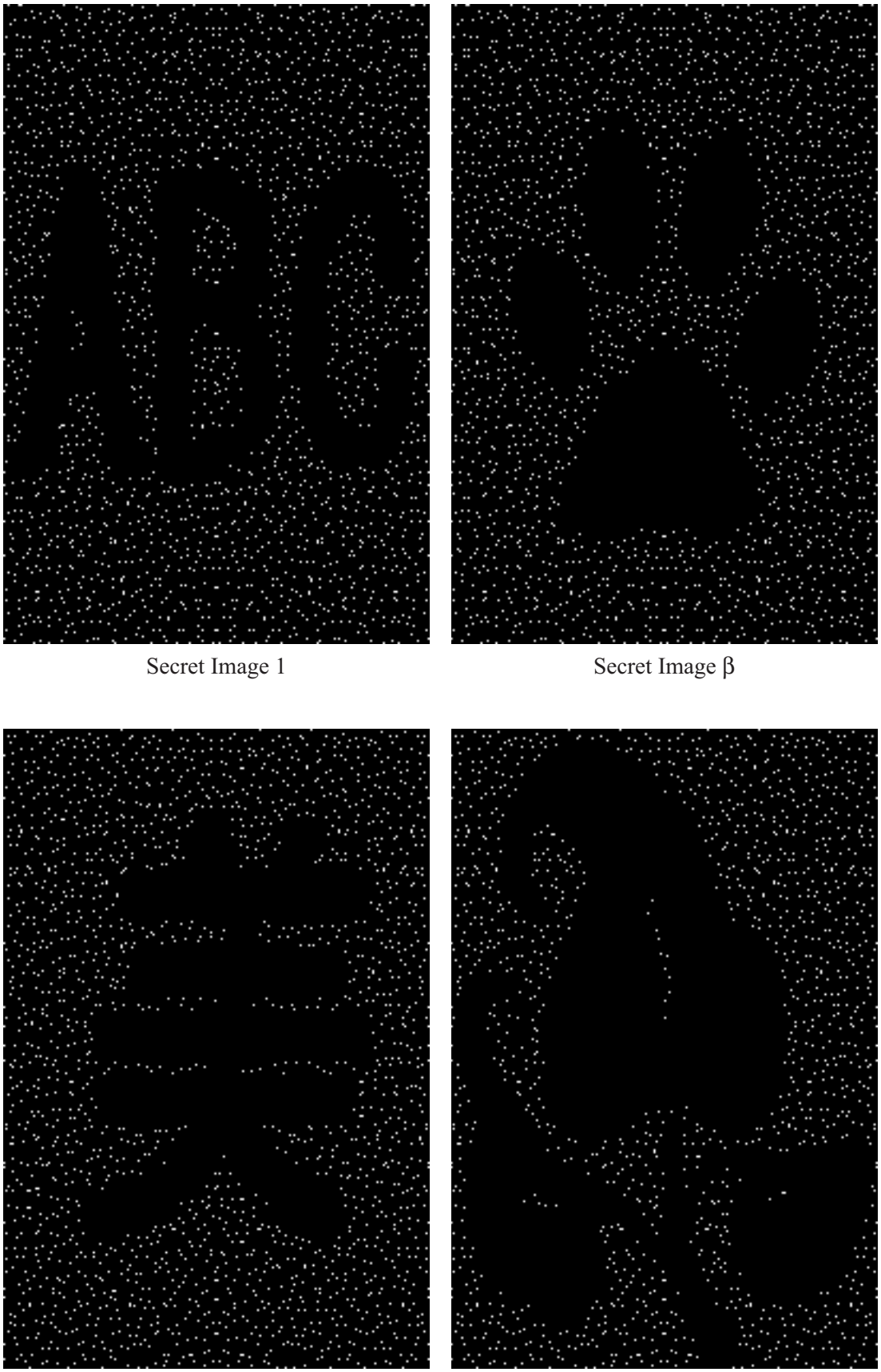

Figure 12: An example of improved VCS with D_4 access structure (reconstructed images).