Joint Conference of 1996 International Computer Symposium
December 19~21, Kaohsiung, Taiwan, R.O.C.

Some Visual Secret Sharing Schemes and Their Share Size

Taku Katoh and Hideki Imai

Institute of Industrial Science, University of Tokyo
7-22-1, Roppongi, Minato, Tokyo, 106 Japan
Tel : +81-3-3402-6231 (Ext 2327), FAX : +81-3-3402-7365
E-mail: taku@imailab.iis.u-tokyo.ac.jp and imai@iis.u-tokyo.ac.jp

Abstract

Visual secret sharing scheme[1] permits a secret to be shared among participants using transparencies. In this paper, we show a general share construction method, and share sizes which is constructed by the method. Furthermore, we consider an improved constructing method of visual secret sharing scheme that can conceal some images in a series of transparencies, in such a way that different images are seen as the number of stacking transparencies increases. We also introduce a type of $(2, n)$ visual secret sharing scheme which has smaller number of the columns than [1] when the numbers of the rows are the same.

1 Introduction

When important secret information is managed by individuals, secrets may leak out by not enough management or personal malice, and there is also the possibility of abuse. As a result, constructions of secret management that allow access to secret shared among group member by mutual agreement have been investigated. The (k, n) threshold scheme for secret sharing was proposed by A.Shamir [3], and since then various researches have further investigated.

A secret sharing scheme is a method of distributing a secret among a set of participants in such a way that qualified subsets of participants can reconstruct the value of the secret by combining their shares, whereas any non-qualified subset of participants cannot determine anything about the value of the secret by any way. In the basic secret sharing scheme, however, cryptographic computations using computer are necessary to share a secret and decode the secret from shared data. In many secret sharing schemes, a great deal of complexity is necessary to encrypt and decode a secret, and therefore computers are essential.

A new type of secret sharing in which images are used as secret information, and the shared secret image can be decoded directly by the human sight was proposed by M.Naor, A.Shamir [1]. In this scheme, the decoder of a (k, n) threshold scheme is replaced by the human eye, and the original secret image is shared and printed on n materials, as transparencies, which can be stacked, and can be revealed by stacking any k (or more) materials together.

This paper is organized as follows. The visual secret sharing scheme proposed by M.Naor et al. is reviewed in section 2. We show a general share construction method for a visual secret sharing scheme in section 3, and consider the size of constructed share matrix, and construct visual $(2, 3, 3)$ secret sharing scheme. In section 4, we consider a new type visual $(2, n)$ threshold scheme which is constructed by using a constant weight code.

2 Visual secret sharing scheme

The visual secret sharing scheme [1] can securely share image information (printed text, handwritten notes, pictures, etc.) and it is possible to decode shared secrets by the human sight. This visual secret sharing scheme can be extended into a visual variant of the (k, n) secret sharing scheme: Given an original secret image, we would like to generate n transparencies so that the original image is visible if any k (or more) of them are stacked together, but totally invisible if fewer than k transparencies are stacked together (or analyzed by any other method).

The original image consists of a collection of black and white pixels and each pixel is handled separately. Each original pixel appears in n modified versions (called shares), one for each transparency. Each share is a collection of m black and white subpixels, which are printed in close proximity to each other so that the human visual system averages their individual black/white contributions. The resulting structure can be described by an $n \times m$ Boolean matrix $S = [s_{ij}]$ where $s_{ij} = 1$ iff the jth subpixel in the ith transparency is black. When transparencies $i_1, i_2, \ldots, i_r$ are stacked together in a way which properly aligns the subpixels, we see a combined share whose black subpixels are represented by the Boolean "or"of rows $i_1, i_2, \ldots, i_r$ in S. The Gray level of this combined share is proportional to the Hamming weight $H(V)$ of the "or"ed m dimensional vector V. This gray level is interpreted by the visual system of the users as black if $H(V) \geq d$ and as white if $H(V) < d - \alpha m$ for some fixed threshold $1 \leq d \leq m$ and relative difference $\alpha > 0$. The α represents the loss in contrast and is desired to be as large as possible.

Definition 1 A solution to the (k, n) visual secret

sharing scheme consists of two collections of $n \times m$ Boolean matrices C_0 and C_1. To share a white pixel, the dealer randomly chooses one of the matrices in C_0, and to share a black pixel, the dealer randomly chooses one of the matrices in C_1. The chosen matrix defines the color (white or black) of the m subpixels in each one of the n transparencies.

3 A general share construction method

The previous (k, n) scheme shares one secret image among n transparencies, and can reveal the secret by stacking k (or more) transparencies. In this section, we show a method which constructs not only the (k, n) threshold schemes, but various secret sharing schemes, such as the one where more than one secret image can be kept on one series of n transparencies.

3.1 A share construction method for visual (3,3) threshold scheme

We explain the proposed construction method using an example for $n = 3$, and generalize this method afterwards.

First, we generate unit matrices $M_{n,i}$ $(i = 0, 1, \ldots, n)$ which have n rows and a set of ${}_nC_i$ columns obtained by all permutations of i 1s and $n-i$ 0s. For example, in the case of $n = 3$,

$$M_{3,0} = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix}, M_{3,1} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

$$M_{3,2} = \begin{bmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{bmatrix}, M_{3,3} = \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix}$$

We generate the matrices, which construct the shares respectively, by concatenating $M_{n,i}$ $(i = 0, 1, \ldots, n)$, suitably. In each matrix $M_{n,i}$ $(n = 3)$, when the number of the stacked shares (rows) increases, the number of the black subpixels changes as shown in Table 1.

From Table 1, we generate a matrix

$$T_3 = \begin{pmatrix} 1 & 2 & 1 \\ 2 & 3 & 1 \\ 3 & 3 & 1 \end{pmatrix} \quad (1)$$

where (i, j) component is the number of the black subpixels when j rows of $M_{3,i}$ are stacked. The $M_{3,0}$ is excluded, however, because this matrix does not affect the transition of the number of the black subpixels.

Furthermore, we define a vector $X_3 = (x_1, x_2, x_3)$ whose ith $(i = 1, 2, 3)$ component is the number of the $M_{3,i}$'s which compose the share generating matrix, and a vector $Y_3 = (y_1, y_2, y_3)$ whose ith $(i = 1, 2, 3)$ component is the number of the black subpixels in the stacked shares when i shares are stacked. Then, T_3, X_3 and Y_3 are related by the following equations.

$$\begin{aligned} Y_3 &= T_3 X_3 \\ X_3 &= T_3^{-1} Y_3 \end{aligned} \quad (2)$$

$$= \begin{pmatrix} 0 & -1 & 1 \\ -1 & 2 & -1 \\ 3 & -3 & 1 \end{pmatrix} Y_3 \quad (3)$$

In case of a (3,3) visual secret sharing scheme, we can define Y_{W3} and Y_{B3} for white share and black share, respectively as shown in Table 2, where we select that the relative difference $\alpha = 1/m$ in order to make m (the number of subpixels in a share) as small as possible.

And we define two vectors, which are composed of the numbers of $M_{3,i}s$ $(i = 1, 2, 3)$ for constructing the white and black share matrices, $X_{W3} = (x_{w1}, x_{w2}, x_{w3})$ and $X_{B3} = (x_{b1}, x_{b2}, x_{b3})$, respectively.

We substitute these vectors in equation (3) to obtain.

$$\begin{cases} x_{w1} = 0 \cdot y_{w1} + (-1) \cdot y_{w2} + 1 \cdot y_{w3} \\ x_{w2} = (-1) \cdot y_{w1} + 2 \cdot y_{w2} + (-1) \cdot y_{w3} \\ x_{w3} = 3 \cdot y_{w1} + (-3) \cdot y_{w2} + 1 \cdot y_{w3} \end{cases}$$

$$\begin{cases} x_{b1} = 0 \cdot y_{w1} + (-1) \cdot y_{w2} + 1 \cdot (y_{w3} + 1) \\ x_{b2} = (-1) \cdot y_{w1} + 2 \cdot y_{w2} + (-1) \cdot (y_{w3} + 1) \\ x_{b3} = 3 \cdot y_{w1} + (-3) \cdot y_{w2} + 1 \cdot (y_{w3} + 1) \end{cases}$$

Then,

$$\begin{cases} x_{w1} - x_{b1} = -1 \\ x_{w2} - x_{b2} = 1 \\ x_{w3} - x_{b3} = -1 \end{cases}$$

We choose the minimum non-negative integers, which satisfy above equations, to let m be as small as possible.

$$\begin{cases} X_{B3} = (1, 0, 1) \\ X_{W3} = (0, 1, 0) \end{cases}$$

Finally, $M_{3,0}$ is concatenated to the white share matrix to construct a matrix of the size as the black share matrix. The (3,3) visual secret sharing problem can be solved by the following scheme :

C_0 = {all the matrices obtained by permuting the columns of $\begin{bmatrix} 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{bmatrix}$}

C_1 = {all the matrices obtained by permuting the columns of $\begin{bmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{bmatrix}$}

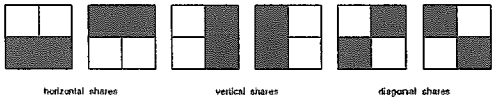

Figure 1: Shares of the visual (3,3) secret sharing scheme

Table 1: Transition of the number of black subpixels according to stacking rows of $M_{3,i}$

	1	2	3
$M_{3,0}$	0	0	0
$M_{3,1}$	1	2	3
$M_{3,2}$	2	3	3
$M_{3,3}$	1	1	1

Table 2: Transition of the number of black subpixels according to stacking shares of a (3,3) scheme

	1	2	3
Y_{W3}	y_{w1}	y_{w2}	y_{w3}
Y_{B3}	$y_{b1} = y_{w1}$	$y_{b2} = y_{w2}$	$y_{b3} = y_{w3} + 1$

3.2 A general share construction method for visual (k,n) threshold scheme

To construct various visual threshold schemes, first, we properly choose the vectors X_n and Y_n.

As previously stated, the (i,j) component of the matrix T_n is the number of the black subpixels when j rows of $M_{n,i}$ are stacked. We generalize the matrix T_n. The size of $M_{n,i}$ is $n \times {}_nC_i$, and each row has $\frac{i}{n} \times {}_nC_i = {}_{n-1}C_{i-1}$ 1s and ${}_nC_i - {}_{n-1}C_{i-1} = {}_{n-1}C_i$ 0s.

Here, we show the transition of the number of black subpixels using the transition of the number of white subpixels. To keep a subpixel in the stacked shares white when j shares have been stacked, it is necessary that the component of row "or"ed j rows of $M_{n,i}$ is 0. This event occurs with probability $P_W(n,i,j)$.

$$P_W(n,i,j) = \begin{cases} \frac{{}_{n-i}C_j}{{}_nC_j} & (n \geq i+j) \\ 0 & (n < i+j) \end{cases} \quad (4)$$

Furthermore, the number of the black subpixels when j shares generated from $M_{n,i}$ are stacked is described as follows :

$$N_B(n,i,j) = (1 - P_W(n,i,j)) \cdot {}_nC_i \quad (5)$$

Then, for any n, the matrices T_n and T_n^{-1} are described as follows :

$$\begin{aligned} T_n &= \left[\; t_{ji} \; \right] \\ t_{ji} &= (1 - P_W(n,i,j)) \cdot {}_nC_i \end{aligned}$$

$$T_n^{-1} = \begin{bmatrix} 0 & \cdots & 0 & 0 & 0 & 0 & -1 & 1 \\ 0 & \cdots & 0 & 0 & 0 & -1 & 2 & -1 \\ 0 & \cdots & 0 & 0 & -1 & 3 & -3 & 1 \\ 0 & \cdots & 0 & -1 & 4 & -6 & 4 & -1 \\ 0 & \cdots & -1 & 5 & -10 & 10 & -5 & 1 \\ & \cdots & & & & & & \end{bmatrix}$$

$$= \left[\; s_{ij} \; \right] \quad (6)$$

$$s_{ij} = \begin{cases} (-1)^{(n-j)+(i-1)} \cdot {}_iC_{n-j} & i \geq n-j \\ 0 & i < n-j \end{cases} \quad (7)$$

In a visual (k,n) threshold scheme, two share matrices for black pixel and white pixel of the secret image are necessary, and the contrast between black share and white share is necessary to realize a concealed image on stacked k shares. In other words, the number of black subpixels in the stacked black shares has to be much more than in the stacked white shares, when k or more shares are stacked. In this paper, let the differences of the number of the black subpixels $\alpha_i (\geq 0)$, where i means the number of the stacked shares, and $\alpha_i = 0$ for $i < k$. Then,

$$\begin{cases} y_{b1} = y_{w1} + \alpha_1 \\ y_{b2} = y_{w2} + \alpha_2 \\ \quad \vdots \\ y_{bn} = y_{wn} + \alpha_n, \end{cases} \quad (8)$$

where y_{wi}, y_{bi} mean the number of the black subpixels in the stacked white and black shares respectively, when i shares are stacked. Furthermore, by using following equations,

$$\begin{cases} x_{w1} = s_{11}y_{w1} + s_{12}y_{w2} + \cdots + s_{1n}y_{wn} \\ x_{w2} = s_{21}y_{w1} + s_{22}y_{w2} + \cdots + s_{2n}y_{wn} \\ \quad \vdots \\ x_{wn} = s_{n1}y_{w1} + s_{n2}y_{w2} + \cdots + s_{nn}y_{wn}, \end{cases} \quad (9)$$

$$\begin{cases} x_{b1} = s_{11}y_{b1} + s_{12}y_{b2} + \cdots + s_{1n}y_{bn} \\ x_{b2} = s_{21}y_{b1} + s_{22}y_{b2} + \cdots + s_{2n}y_{bn} \\ \quad \vdots \\ x_{bn} = s_{n1}y_{b1} + s_{n2}y_{b2} + \cdots + s_{nn}y_{bn}, \end{cases} \quad (10)$$

the following equations are derived.

Table 3: Size of black share matrices of (k, n) threshold schemes

k	n						
	2	3	4	5	6	7	8
2	2 (1)	3 (1,1) (1,2)	4 (1,1,1) (1,2,3)	5 (1,1,1,1) (1,2,3,4)	6 (1,1,1,1,1) (1,2,3,4,5)	7 (1,1,1,1,1,1) (1,2,3,4,5,6)	8 (1,1,1,1,1,1,1) (1,2,3,4,5,6,7)
3		4 (1)	6 (1,2)	8 (1,2,3)	10 (1,2,3,4)	12 (1,2,3,4,5)	14 (1,2,3,4,5,6)
4			8 (1)	15 (1,2) (1,3)	24 (1,2,3) (1,3,6)	35 (1,2,3,4) (1,3,6,10)	48 (1,2,3,4,5) (1,3,6,10,15)
5				16 (1)	30 (1,3)	48 (1,3,6)	70 (1,3,6,10)
6					32 (1)	70 (1,3) (1,4)	128 (1,3,6) (1,4,10)
7						64 (1)	140 (1,4)
8	the numbers in () mean $(\alpha_k, \alpha_{k+1}, \cdots, \alpha_n)$ $(\alpha_i = 0\ (i < k))$						128 (1)

$$\begin{cases} x_{b1} &= x_{w1} + \sum_{i=1}^{n} s_{1i}\alpha_i \\ x_{b2} &= x_{w2} + \sum_{i=1}^{n} s_{2i}\alpha_i \\ &\vdots \\ x_{bn} &= x_{wn} + \sum_{i=1}^{n} s_{ni}\alpha_i \end{cases} \tag{11}$$

Because x_{wi} and x_{bi} are the number of the unit matrices $M_{n,i}$s, and each unit matrices $M_{n,i}$ has ${}_nC_i$ columns, the minimum size of the share matrices for (k, n) threshold schemes are shown as follows :

$$S_{\text{column}} = \left(\sum_{i=k}^{n} s_{1i}\alpha_i\right) {}_nC_1 + \left(\sum_{i=k}^{n} s_{2i}\alpha_i\right) {}_nC_2 + \cdots + \left(\sum_{i=k}^{n} s_{ni}\alpha_i\right) {}_nC_n, \tag{12}$$

where let $\sum_{i=k}^{n} s_{ji}\alpha_i \equiv 0$ if $\sum_{i=k}^{n} s_{ji}\alpha_i > 0$ for white share matrix, and let $\sum_{i=k}^{n} s_{ji}\alpha_i \equiv 0$ if $\sum_{i=k}^{n} s_{ji}\alpha_i < 0$ for black share matrix.

Although the size of black share matrix found from (12) is invariably bigger than the size of white share matrix, it is easy to make the size of white and black share matrices equal by connecting some matrices $M_{n,0}$ to the white share matrix.

We show the size of black share matrices and coefficients α_i for some visual (k, n) threshold schemes in Table.3

In a visual (k, n) threshold scheme, it is to be desired that α_i is as big as possible, because the contrast between white shares and black shares is improved. Then, we should construct visual (k, n) threshold schemes with care about coefficients α_i.

To construct any visual threshold scheme, we should

1. describe the weight hierarchies of each required share (in other words, we define the vector $\boldsymbol{Y}_{n_i}$),
2. calculate $\boldsymbol{X}_{n_i} = T_n^{-1}\boldsymbol{Y}_{n_i}$,
3. construct the matrix S_i for each case.

3.3 A visual $(2, 3, 3)$ secret sharing scheme

In this section, we construct a visual $(2, 3, 3)$ secret sharing scheme. The scheme can share two secret image on series of three shares, and first secret image appears when two transparencies are stacked and second secret image appears when three transparencies are stacked.

In a similar way as for the $(3, 3)$ visual secret sharing scheme, this scheme can be constructed.

We define four vectors $\boldsymbol{Y}_{WW}, \boldsymbol{Y}_{BW}, \boldsymbol{Y}_{WB}$ and $\boldsymbol{Y}_{BB}$ as shown in Table 4, where we select that the relative difference $\alpha = 1/m$ in order to make m (the number of subpixels in a share) as small as possible.

A share matrix derived from $\boldsymbol{Y}_{BB}$ reconstructs a white pixel of first secret image and second secret image, and a share matrix derived from $\boldsymbol{Y}_{BW}$ reconstructs a black pixel of first secret image and a white pixel of second secret image, and a share matrix derived from $\boldsymbol{Y}_{WB}$ reconstructs a white pixel of first secret image and a black pixel of second secret image, and a share matrix derived from $\boldsymbol{Y}_{BB}$ reconstructs

Table 4: Transition of the number of black pixels according to stacking shares of a visual $(2,3,3)$ secret sharing scheme

	1	2	3	
Y_{WW}	y_1	y_2	y_3	stack two shares = white, three shares = white
Y_{BW}	y_1	y_2+1	y_3	stack two shares = black, three shares = white
Y_{WB}	y_1	y_2	y_3+1	stack two shares = white, three shares = black
Y_{BB}	y_1	y_2+1	y_3+1	stack two shares = black, three shares = black

a black pixel of first secret image and second secret image.

We substitute these vectors in equation (3), and take the following solutions.

$$S_{WW} = [M_{3,0}\ M_{3,1}\ M_{3,2}\ M_{3,3}^3] = \begin{bmatrix} 0&1&0&0&0&1&1&1&1&1 \\ 0&0&1&0&1&0&1&1&1&1 \\ 0&0&0&1&1&1&0&1&1&1 \end{bmatrix},$$

$$S_{BW} = [M_{3,0}\ M_{3,2}^3] = \begin{bmatrix} 0&0&1&1&0&1&1&0&1&1 \\ 0&1&0&1&1&0&1&1&0&1 \\ 0&1&1&0&1&1&0&1&1&0 \end{bmatrix},$$

$$S_{WB} = [M_{3,1}^2\ M_{3,3}^4] = \begin{bmatrix} 1&0&0&1&0&0&1&1&1&1 \\ 0&1&0&0&1&0&1&1&1&1 \\ 0&0&1&0&0&1&1&1&1&1 \end{bmatrix},$$

$$S_{BB} = [M_{3,1}\ M_{3,2}^2\ M_{3,3}] = \begin{bmatrix} 1&0&0&0&1&1&0&1&1&1 \\ 0&1&0&1&0&1&1&0&1&1 \\ 0&0&1&1&1&0&1&1&0&1 \end{bmatrix},$$

where M^p means concatenation of p matrices M ($M^p = [M \cdots M]$) The $(2,3,3)$ visual secret sharing problem can be solved by the following scheme :

C_{WW} = {all the matrices obtained by permuting the columns of S_{WW}}
C_{BW} = {all the matrices obtained by permuting the columns of S_{BW}}
C_{WB} = {all the matrices obtained by permuting the columns of S_{WB}}
C_{BB} = {all the matrices obtained by permuting the columns of S_{BB}}

The dealer randomly chooses one of the matrices in C_{WW}, C_{BW}, C_{WB}, or C_{BB} while taking account of the colors of pixels in both the first and second secret images. We show a example of visual $(2,3,3)$ secret sharing scheme using these share matrices in Fig.2

In the $(2,3,3)$ visual secret sharing scheme, the image made by any two transparencies is used for the group authentication, and the image made by three ones gives important information. And, if a fake transparency and two legitimate one are included in the group, the fake transparency can be found out by stacking every two ones out of the three.

4 Another type of $(2,n)$ scheme

The security of the (k,n) visual secret sharing scheme is kept by the following condition : For any subset $\{i_1, i_2, \ldots i_q\}$ of $\{1,2,\ldots,n\}$ with $q < k$, the two collections $\mathcal{D}_t$ for $t \in \{0,1\}$ obtained by restricting each $n \times m$ matrix in C_t (where $t = 0,1$) to rows $i_1, i_2, \ldots, i_q$ are indistinguishable in the sense that they contain the same matrices with the same frequencies.

In other words, if the Hamming weights of stacked white shares and stacked black ones of $q < k$ transparencies are equal, then the security of the visual secret sharing is warranted. It follows that in a $(2,n)$ visual secret sharing scheme, it is only necessary for security that the Hamming weights of rows of matrices for black share and white share in one transparency are equal.

In this section, we show a new type of $(2,n)$ visual secret sharing scheme which uses the codewords of a *constant weight code* [4, 5, 6, 7] for rows of black share matrix S_1. The codewords have same Hamming weight, and therefore suitable for the above security condition.

It is possible to get a larger number of rows n of the share matrix than the previous $(2,n)$ scheme for the same number of the columns m in the case when number of columns is large.

If we use the set of codewords of the optimal constant weight code with a minimum semi-distance 2 for the black share matrix, the size of matrix (n,m) becomes $(7,7)$, $(14,8)$, $(18,9)$ and so on. For white share, we can use the same matrix as in the previous scheme. In the case of $m = 8$, the share matrices S_0 and S_1 are constructed as follows :
$m = 8$

$$S_0 = \begin{bmatrix} 1&1&1&1&0&0&0&0 \\ 1&1&1&1&0&0&0&0 \\ 1&1&1&1&0&0&0&0 \\ 1&1&1&1&0&0&0&0 \\ 1&1&1&1&0&0&0&0 \\ 1&1&1&1&0&0&0&0 \\ 1&1&1&1&0&0&0&0 \\ 1&1&1&1&0&0&0&0 \\ 1&1&1&1&0&0&0&0 \\ 1&1&1&1&0&0&0&0 \\ 1&1&1&1&0&0&0&0 \\ 1&1&1&1&0&0&0&0 \\ 1&1&1&1&0&0&0&0 \\ 1&1&1&1&0&0&0&0 \end{bmatrix}$$

$$S_1 = \begin{bmatrix} 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{bmatrix}$$

The $(2, n)$ visual secret sharing problem can be solved by the following collections of $(7, 7)$ matrices :

$$\begin{aligned} \mathcal{C}_0 &= \{\text{all the matrices obtained by permuting the columns of } S_0\} \\ \mathcal{C}_1 &= \{\text{all the matrices obtained by permuting the columns of } S_1\} \end{aligned}$$

In some cases, however, weights of the "or"ed rows of the matrix for black share are different, in other words, there is a contrast among black shares in one image. But the weight of black share is always larger than white share's, and the revealed image can always be recognized.

The advantage of this scheme is not only a smaller matrix size, but also that the relative difference in weight between stacked black share and stacked white share is larger than the previous scheme. In other words, the revealed image in the proposed scheme can be recognized easier than in the previous scheme[1].

5 Conclusions

We have introduced a generalized share construction method for the visual secret sharing scheme, and we show share sizes of some visual (k, n) threshold schemes which is able to be constructed by using the share construction methods. We presented a $(2, 3, 3)$ visual secret sharing scheme as a example. Furthermore, we show a new type of the $(2, n)$ visual secret sharing scheme which allows the size of share matrices to be smaller. This characteristic is desirable for practical construction and use of shares.

References

[1] M.Naor and A.Shamir, "Visual cryptography, " Advances in Cryptology – EUROCRYPT'94, Lecture Notes in Computer Science No.950, pp.1-12, Springer, 1995.

[2] S. Droste , "New results on visual cryptography, " Advances in Cryptology – CRYPTO'96, Lecture Notes in Computer Science, No.1109, pp401-415, Springer, 1996.

[3] A.Shamir, "How to share a secret," Commun. of the ACM, vol.22, pp. 612-613, Nov. 1979.

[4] R.L.Graham and N.J.A.Sloane, "Lower bounds for constant weight codes," *IEEE Trans. Inform. Theory*, vol.IT-26, pp.37-43, Jan. 1980.

[5] R.E.Kibler, "Some new constant weight codes," *IEEE Trans. Inform. Theory*, vol.IT-26, pp.364-365, May 1980.

[6] A.E.Brouwer, "A few new constant weight codes, " *IEEE Trans. Inform. Theory*, vol.IT-26, p.366, May 1980.

[7] N.Ikeno and G.Nakamura, "Constant-weight codes (in Japanese), " IEICE Trans.,54-A, vol.7, pp. 410-417, July 1971.

[8] T.Katoh and H.Imai , "On extension and applications of visual secret sharing (in Japanese), " Tech. rept. IEICE, ISEC95-9, pp. 41-48, Sep. 1995.

[9] T.Katoh and H.Imai , "An extended construction method of visual secret sharing scheme (in Japanese), " Trans. IEICE, vol.J79-A, pp. 1344-1351, Aug. 1996.

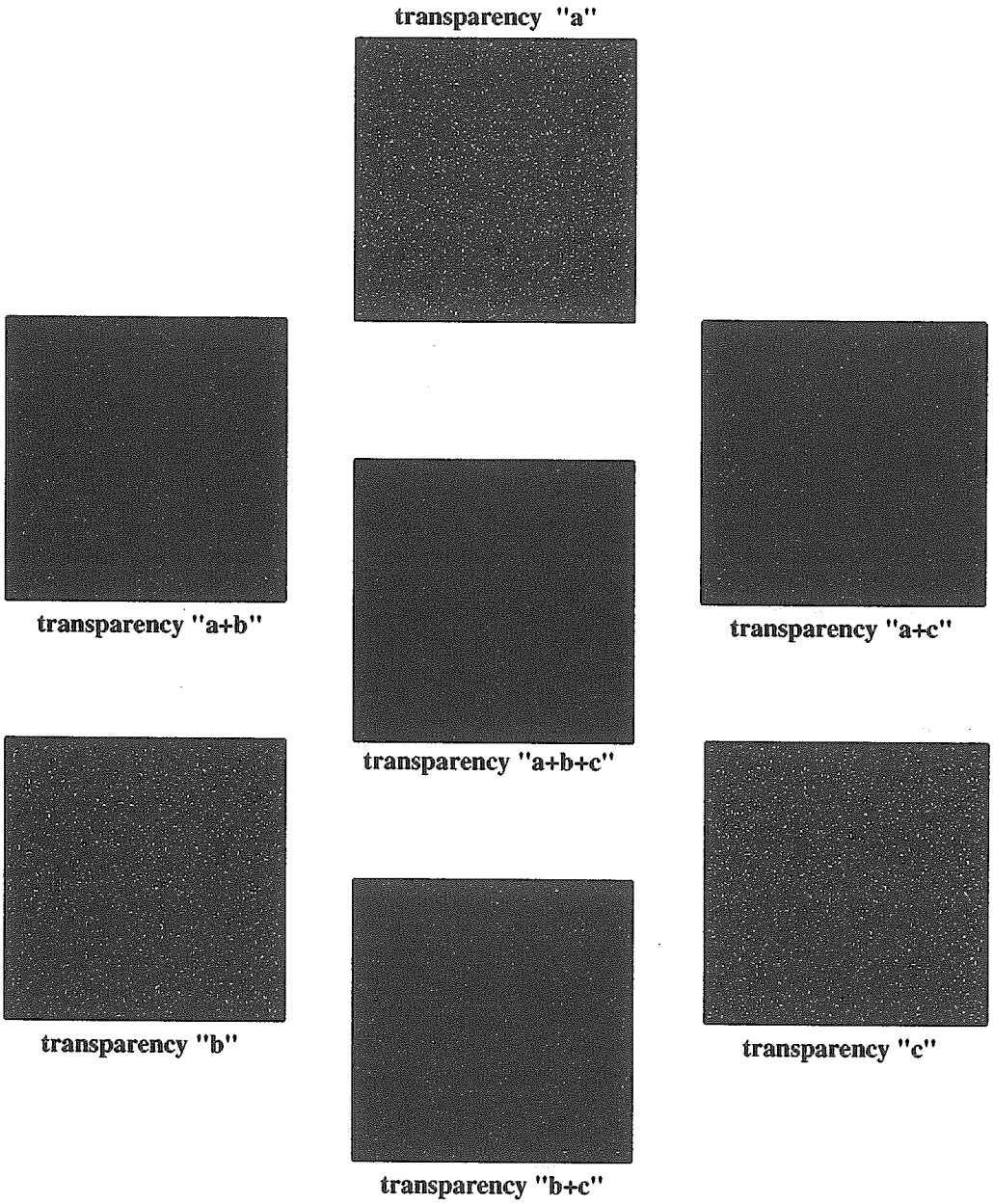

Figure 2: An example of visual $(2, 3, 3)$ secret sharing scheme