



Polynomial Representation of a Visual Secret Sharing Scheme and Its Application

Kuwakado, Hidenori

Tanaka, Hatsukazu

(Citation)

IEICE transactions on fundamentals of electronics, communications and computer sciences, E85-A(6):1379-1386

(Issue Date)

2002-06-01

(Resource Type)

journal article

(Version)

Version of Record

(Rights)

Copyright (c) 2002 IEICE

(URL)

<https://hdl.handle.net/20.500.14094/90001321>



PAPER

Polynomial Representation of a Visual Secret Sharing Scheme and Its Application

Hidenori KUWAKADO^{†a)} and Hatsukazu TANAKA[†], *Regular Members*

SUMMARY A visual secret sharing scheme (VSSS) is one of secret sharing schemes for images. Droste showed the method for constructing VSSS based on basis matrices whose contrast was high. Koga, Iwamoto, and Yamamoto also proposed the method for constructing a lattice-based VSSS and its polynomial representation. It is known that many good VSSSs are not in the class of lattice-based VSSSs. In this paper, we show the well-defined polynomial representation of a VSSS based on permuting different matrices for black-white images. The necessary and sufficient condition of the existence of a VSSS based on permuting different matrices can be obtained from the proposed polynomial representation. This condition is useful for constructing a good VSSS. We also point out that without additional data, it is possible to achieve member verification by using a VSSS. Using the proposed polynomial representation, the probability of detecting a cheater is analyzed.

key words: information security, visual secret sharing, polynomial representation

1. Introduction

A visual secret sharing scheme (VSSS) that was proposed by Naor and Shamir [10] is a method for sharing black-white images in an unconditionally secure way. In a (k, n) VSSS a secret original image is encoded to n shares. To decode the original image it is necessary to have k shares, print shares on transparencies, and stack them. Then the original image shall be recognizable. Although k shares have sufficient information to reproduce the original image precisely, the reconstructed image is not precisely same as the original image: (i) since one pixel is encoded some subpixels in a share, the size of the reconstructed image is larger than that of the original image, (ii) a white pixel in the original image may not be all white upon reconstruction, and a black pixel may not be all black upon reconstruction.

In order to resolve these issues, the construction of a VSSS with small size and high contrast have been studied [1], [3]–[5]. The concept of contrast on a VSSS was introduced by Naor and Shamir [10], and it represents the recognizability of a reconstructed image. Although their definition of contrast has intuitive appeal, the experimentation in [4] shows that it is insufficient for evaluating the quality of a reconstructed

image. To evaluate the quality of a reconstructed image precisely, different definitions of contrast have been also proposed. We note that the optimality of a VSSS depends on the definition of contrast.

Thus it might be not advisable to optimize only the contrast based on some definition. Eisen and Stinson [4] suggested how to construct VSSS for given parameters that were related to contrast. Using combinatorics and the linear programming, they showed the necessary condition of the existence of a $(2, n)$ VSSS for given parameters that were related to contrast. However, it seems difficult to extend their analysis to a (k, n) VSSS where $k \geq 3$. This paper mainly discusses how to construct a (k, n) VSSS where $k \geq 3$ for given parameters. The results of this paper are as follows.

1. We give the well-defined polynomial representation of a (k, n) VSSS for black-white images. The polynomial representation of subclass of (k, n) VSSSs has been introduced in [5]. However, the previous polynomial representation is not applicable to many good (k, n) VSSSs. The proposed polynomial representation is applicable to wider subclass of (k, n) VSSSs that includes many good (k, n) VSSSs.
2. Using the proposed polynomial representation, we obtain a sufficient condition for the existence of a (k, n) VSSS for given k, n and contrast. If parameters that satisfy the sufficient condition are found, then it is easy to achieve such a (k, n) VSSS from its polynomial representation. Comparing with the analysis in [2], the analysis based on the proposed polynomial representation is clear and does not depend the definition of the contrast.
3. We examined the existence of a high contrast VSSS using the proposed polynomial representation. As a result, we discovered better VSSSs that were not obtained by the previous method.
4. A VSSS can detect the existence of a third party whom a dealer does not distribute a share to. We show the probability of its detection using the proposed polynomial representation.

The organization of this paper is as follows. Section 2 describes the relationship of classes of VSSSs and three kinds of definitions on contrast. In Sect. 3, we study the relationship between a matrix and a polynomial, and propose the definition of a VSSS by poly-

Manuscript received May 23, 2001.

Manuscript revised October 30, 2001.

Final manuscript received January 7, 2002.

[†]The authors are with the Faculty of Engineering, Kobe University, Kobe-shi, 657-8501 Japan.

a) E-mail: kuwakado@eedept.kobe-u.ac.jp

nomials. Then an example of a good VSSS obtained by our polynomial representation is shown. In Sect. 4, we point out that the member verification can be achieved by using a VSSS without additional data. Section 5 concludes this paper.

2. Preliminaries

2.1 Different Permuting Matrix

A matrix $M_{n,h}$ is called a *different permuting matrix* if it consists of different permutations of a vector $[a_1, a_2, \dots, a_n]^t$ where $a_i \in \{0, 1\}$ and the Hamming weight of the vector is h . We do not distinguish between $M_{n,h}$ and its column-permuted matrix.

The size of a different permuting matrix $M_{n,h}$ is n rows and $\binom{n}{h}$ columns. The following is an example of a different permuting matrix.

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

Let $M_{n,h}$ be a different permuting matrix. Consider the reduced matrix such that a row is removed from $M_{n,h}$, denoted by $M_{n,h}^{(-1)}$. We obtain the following theorem from the structure of a different permuting matrix.

Theorem 1: The reduced matrix $M_{n,h}^{(-1)}$ is a different permuting matrix, or the concatenation of different permuting matrices. Precisely speaking,

$$M_{n,h}^{(-1)} = M_{n-1,h-1} | M_{n-1,h}. \quad (1)$$

for $0 < h \leq n$.

We notice that $M_{n,h}^{(-1)}$ is independent on the removed row. The following example is the case of removing the second row or the third row from $M_{3,2}$.

$$M_{3,2} = \begin{pmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix} \xrightarrow{\text{removing the 2nd row}} \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix} \xrightarrow{\text{removing the 3rd row}} \begin{pmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \end{pmatrix}$$

$$\xrightarrow{\text{column permutation}} M_{3,2}^{(-1)} = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix} = M_{2,1} | M_{2,2}$$

Similar to the order of columns, the order of the concatenation of different permuting matrices is ignored.

2.2 Definitions of a VSSS

Naor and Shamir [10] defined a VSSS as follows.

Definition 1: Let us consider two sets of $n \times m$

Boolean matrices C_w and C_b . To share a white pixel, the dealer randomly chooses one of the matrices in C_w , and to share a black pixel, the dealer randomly chooses one of the matrices in C_b . The chosen matrix defines the color of the m subpixels in each of the n transparencies. If the following three conditions are met, C_w and C_b are called a (k, n, h, ℓ, m) VSSS.

1. For any $S \in C_w$, the “or” of any k of the n rows has a Hamming weight of at most $m - h$.
2. For any $S \in C_b$, the “or” of any k of the n rows has a Hamming weight of at least $m - \ell$, where $h > \ell$.
3. For any subset $\{i_1, i_2, \dots, i_q\} \subset \{1, 2, \dots, n\}$ with $q < k$, the two sets obtained by restricting each matrix C_w (resp. C_b) to rows $i_1, i_2, \dots, i_q$ contain the same matrices with same frequencies.

When there is no misunderstanding, the parameter (k, n, h, ℓ, m) is often omitted.

Usually, C_w (resp. C_b) consists of all matrices obtained by permuting the column of a matrix S_w (resp. S_b) called *basis matrices*. The definition of a VSSS based on basis matrices (called a *BM-VSSS*) is as follows [4].

Definition 2: If the following conditions are satisfied, two $n \times m$ matrices S_w, S_b are called a (k, n, h, ℓ, m) BM-VSSS.

1. The “or” vector of any k of the n rows in S_w satisfies that its Hamming weight is at most $m - h$.
2. The “or” vector of any k of the n rows in S_b satisfies that its Hamming weight is at least $m - \ell$. To guarantee that reconstructed white pixels appear lighter than reconstructed black pixels, we have $h > \ell$.
3. For any subset $\{i_1, i_2, \dots, i_q\} \subset \{1, 2, \dots, n\}$ with $q < k$, the matrices obtained by restricting S_w and S_b to rows $i_1, i_2, \dots, i_q$ are equal up to column permutation.

If S_w and S_b are different permuting matrices or the concatenation of different permuting matrices, it is called a (k, n, h, ℓ, m) *DPBM-VSSS*. We observe that the Hamming weight of the “or” vector of any k of the n rows in S_w of DPBM-VSSS is precisely $m - h$, and that of the “or” vector of any k of the n rows in S_b of DPBM-VSSS is precisely $m - \ell$. The class of DPBM-VSSSs is very important because many good VSSSs shown in [3], [10] are in the class of DPBM-VSSSs.

Koga, Iwamoto, and Yamamoto [6] introduced the concept of a finite lattice in the framework of a VSSS (called a *lattice-based VSSS*). Their idea is useful for constructing a VSSS for color images. Moreover, they also showed that a lattice-based VSSS was able to be represented by polynomials, and the construction of a lattice-based VSSS was reduced to solving partial differential equations [5].

However, several DPBM-VSSSs do not satisfy the

definition of lattice-based VSSS. For example, the following $(2, 3, 2, 1, 3)$ DPBM-VSSS is not a lattice-based VSSS [6]. Notice that this $(2, 3)$ DPBM-VSSS is optimal in the sense that contrast of Naor and Shmiar is the highest.

$$S_w = \begin{pmatrix} 1 & 0 & 0 \\ 1 & 0 & 0 \\ 1 & 0 & 0 \end{pmatrix}, \quad S_b = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}. \quad (2)$$

Conversely, a lattice-based VSSS is a DPBM-VSSS.

In [2], the definition of a canonical (k, n) VSSS has been given. The class of canonical (k, n) VSSSs is located between the class of lattice-based VSSSs and that of DPBM-VSSSs. For example, Eq. (2) is the DPBM-VSSS, but neither the canonical VSSS nor the lattice-based VSSS. Equation (14) stated in Sect. 3.3 is the DPBM-VSSS and the canonical VSSS, but not the lattice-based VSSS.

Summarizing the discussion above, we see the following relationship among classes of VSSSs.

$$\begin{aligned} \text{Lattice-based VSSS} &\subset \text{Canonical VSSS} \\ &\subset \text{DPBM-VSSS} \\ &\subset \text{BM-VSSS} \\ &\subset \text{VSSS} \end{aligned}$$

Hence, the polynomial representation of a lattice-based VSSS is not always applicable to a DPBM-VSSS. One of the objectives of this paper is to give the well-defined polynomial representation of a DPBM-VSSS.

2.3 Definitions of Contrast

The parameter called contrast is probably the most important because it represents recognizability of a reconstructed image. Naor and Shamir defined the contrast as

$$\alpha_{NS} = \frac{h - \ell}{m}, \quad (3)$$

where ℓ (resp. h) is the number of white subpixels when an original pixel is white (resp. black) [10]. To obtain a clearer reconstructed image, we would like to h to be as large as possible, and ℓ to be as small as possible. Moreover, to reduce the amount of data of a share, it is desirable that the value of m is as small as possible. Thus the definition of α_{NS} has intuitive appeal. However the experimentation in [4] shows that it is insufficient for evaluating the quality of a reconstructed image. Hence different definitions of contrast have been proposed; Verhael and Van Tilborg's contrast is

$$\alpha_{VV} = \frac{h - \ell}{m(h + \ell)}, \quad (4)$$

and Eisen and Stinson's contrast is

$$\alpha_{ES} = \frac{h - \ell}{m + \ell}. \quad (5)$$

Generally speaking, it seems difficult to estimate the quality of a reconstructed image only by contrast. Eisen and Stinson also suggest that what is important is the minimum value of m for given k, n, h and ℓ . According to this idea, they show the necessary condition for the existence of a $(2, n, h, \ell, m)$ BM-VSSS in [4]. In order to obtain the necessary condition, they examined the property of basis matrices of a $(2, n, h, \ell, m)$ BM-VSSS in detail. In the case of a $(2, n, h, \ell, m)$ BM-VSSS, it is sufficient to consider all combination of two rows of a basis matrix. However, it seems difficult that Eisen and Stinson's analysis is extended to a necessary condition for the existence of a (k, n, h, ℓ, m) BM-VSSS where $k \geq 3$ because we have to consider all combination of k rows of basis matrices.

3. New Construction of a DPBM-VSSS

3.1 Polynomial Representation

First let us consider the relationship between a different permuting matrix and a polynomial. A different permuting matrix $M_{n,h}$ corresponds to the following polynomial with two variables b, w .

$$M_{n,h} \Leftrightarrow \frac{1}{h!(n-h)!} b^h w^{n-h} \quad (6)$$

In this paper Eq. (6) is called the *polynomial representation* of $M_{n,h}$. We observe that the polynomial representation is uniquely decided from a different permuting matrix, and vice versa. Appendix states the intuitive interpretation of this polynomial representation, and compares this polynomial representation with the polynomial representation of [5].

The number of columns of $M_{n,h}$ is computed by multiplying coefficient $1/(h!(n-h)!)$ by $n!$, where n is the sum of the degrees of b and w . As mentioned in Sect. 3.2, the number of columns is one of important parameters for a VSSS because it is closely related with contrast.

For example, the polynomial representation of $M_{3,2}$ is as follows.

$$M_{3,2} = \begin{pmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix} \Leftrightarrow \frac{1}{2} b^2 w \quad (7)$$

The number of columns is $(2+1)!/2 = 3$.

The concatenation of different permuting matrices corresponds to the addition of their polynomial representations. For example,

$$\begin{aligned} M_{3,1} | M_{3,2} &= \left(\begin{array}{ccc|ccc} 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 \end{array} \right) \\ &\Leftrightarrow \frac{1}{2} b w^2 + \frac{1}{2} b^2 w \end{aligned}$$

Notice that $M_{3,1}|M_{3,1}$ corresponds to bw^2 . That is, a usual addition of polynomials is available.

Next, let us consider the polynomial representation of $M_{n,h}^{(-1)}$. As shown in Sect. 2.1, $M_{3,2}^{(-1)}$ is equal to $M_{2,1}|M_{2,2}$. Accordingly, we have

$$M_{3,2}^{(-1)} = M_{2,1}|M_{2,2} \Leftrightarrow bw + \frac{1}{2}b^2. \quad (8)$$

From Eq. (1), the polynomial representation of $M_{n,h}^{(-1)}$ is given as

$$M_{n,h}^{(-1)} \Leftrightarrow \frac{1}{(h-1)!(n-h)!} b^{h-1} w^{n-h} + \frac{1}{h!(n-1-h)!} b^h w^{n-1-h}. \quad (9)$$

Here, we observe that Eq. (9) is total differential of Eq. (6). For instance, Eq. (8) is total differential of Eq. (7), that is,

$$\left(\frac{\partial}{\partial b} + \frac{\partial}{\partial w} \right) \frac{1}{2} b^2 w = bw + \frac{1}{2} b^2.$$

Thus removing a row from a different permuting matrix corresponds to the total differential of the first order of its polynomial representation.

In general removing d rows from a different permuting matrix corresponds to total differential of the d -th order of its polynomial representation. Moreover, such a relationship holds for the concatenation of any different permuting matrices. Notice that the resulting polynomial representation depends on only the number of removed rows. Consequently, the polynomial representation of $M_{n,h}^{(-d)}$ is given as follows.

$$M_{n,h}^{(-d)} \Leftrightarrow \left(\frac{\partial}{\partial b} + \frac{\partial}{\partial w} \right)^d \frac{1}{h!(n-h)!} b^h w^{n-h}.$$

For simplicity, we denote by ψ^d the d -th total differential operator, i.e.,

$$\psi^d = \left(\frac{\partial}{\partial b} + \frac{\partial}{\partial w} \right)^d.$$

The relationship between removing rows and total differentiation was originally stated in [5]. Note that the definition of their polynomial representation is different from our definition.

3.2 DPBM-VSSS Using the Polynomial Representation

We apply the polynomial representation to a DPBM-VSSS. The polynomial representation of a different permuting basis matrix is called a *different permuting basis polynomial*. By using different permuting basis polynomials, the definition of a DPBM-VSSS is rewritten as follows. Let polynomial representations of different

permuting basis matrices S_w, S_b be

$$P_w(b, w) = \sum_{i=0}^n \frac{s_i}{i!(n-i)!} b^i w^{n-i},$$

$$P_b(b, w) = \sum_{i=0}^n \frac{t_i}{i!(n-i)!} b^i w^{n-i},$$

respectively. Then the parameter m , which is the number of columns of a basis matrix, is computed as

$$m = n! \cdot P_w(1, 1) = n! \cdot P_b(1, 1).$$

The matrix that consists of any $k-1$ rows of S_w is represented by $\psi^{n-k+1} P_w(b, w)$. Similarly for S_b . Since $k-1$ shares do not reveal any information on the original image, the following equation must hold.

$$\psi^{n-k+1} P_w(b, w) = \psi^{n-k+1} P_b(b, w) \quad (10)$$

Equation (10) corresponds to the third condition of Definition 2. The matrix that consists of any k rows of S_w is represented by $\psi^{n-k} P_w(b, w)$. Similarly for S_b . In order to recognize the original image by stacking k shares, the following equation must hold.

$$\psi^{n-k} P_w(b, w) \neq \psi^{n-k} P_b(b, w) \quad (11)$$

Since the parameter h is the number of all zero columns of a matrix that consists of any k rows of S_w , h is obtained by multiplying a coefficient of w^k of $\psi^{n-k} P_w(b, w)$ by $k!$, i.e.,

$$h = k! \cdot \psi^{n-k} P_w(0, 1), \quad (12)$$

where $\psi^{n-k} P_w(0, 1)$ implies substituting 0 and 1 after totally differentiating $P_w(b, w)$. Similarly, the parameter ℓ , which is less than h , is computed as

$$\ell = k! \cdot \psi^{n-k} P_b(0, 1). \quad (13)$$

Summarizing the discussion above, we obtain the following definition of a DPBM-VSSS.

Definition 3: Let $P_w(b, w)$ and $P_b(b, w)$ be polynomials as

$$P_w(b, w) = \sum_{i=0}^n \frac{s_i}{i!(n-i)!} b^i w^{n-i},$$

$$P_b(b, w) = \sum_{i=0}^n \frac{t_i}{i!(n-i)!} b^i w^{n-i},$$

where s_i and t_i are non-negative integers. A pair of $P_w(b, w)$ and $P_b(b, w)$ satisfying the following conditions is a (k, n, h, ℓ, m) DPBM-VSSS.

$$\begin{cases} \psi^{n-k+1} P_w(b, w) = \psi^{n-k+1} P_b(b, w), \\ \psi^{n-k} P_w(b, w) \neq \psi^{n-k} P_b(b, w), \\ h = k! \cdot \psi^{n-k} P_w(0, 1), \\ \ell = k! \cdot \psi^{n-k} P_b(0, 1) < h, \\ m = n! \cdot P_w(1, 1) = n! \cdot P_b(1, 1). \end{cases}$$

Definition 3 immediately leads the necessary and sufficient condition for the existence of a (k, n, h, ℓ, m) DPBM-VSSS. The following theorem is obtained by rearranging coefficients of $P_w(b, w)$, $P_b(b, w)$ in Definition 3.

Theorem 2: Let different permuting basis polynomials for a white pixel and a black one be

$$P_w(b, w) = \sum_{i=0}^n \frac{s_i}{i!(n-i)!} b^i w^{n-i},$$

$$P_b(b, w) = \sum_{i=0}^n \frac{t_i}{i!(n-i)!} b^i w^{n-i},$$

respectively. Given k, n, h, ℓ , and m , a (k, n, h, ℓ, m) DPBM-VSSS exists if and only if there are s_i and t_i ($i = 0, 1, \dots, n$) satisfying the following equations. This is also a sufficient condition for the existence of a (k, n, h, ℓ, m) BM-VSSS.

$$\left\{ \begin{array}{l} \sum_{i=0}^{n-k+1} \binom{n-k+1}{i} s_{i+j} = \sum_{i=0}^{n-k+1} \binom{n-k+1}{i} t_{i+j} \\ \quad \text{for } \forall j = 0, 1, \dots, k-1, \\ \sum_{i=0}^{n-k} \binom{n-k}{i} s_{i+j} \neq \sum_{i=0}^{n-k} \binom{n-k}{i} t_{i+j} \\ \quad \text{for } \exists j = 0, 1, \dots, k, \\ h = \sum_{i=0}^{n-k} \binom{n-k}{i} s_i, \\ \ell = \sum_{i=0}^{n-k} \binom{n-k}{i} t_i, \\ m = \sum_{i=0}^n \binom{n}{i} s_i = \sum_{i=0}^n \binom{n}{i} t_i. \end{array} \right.$$

The essential part of previous constructing methods of VSSS is how to combine various matrices [1]–[3], [10]. However, using polynomial representation, we can reduce the construction of VSSS to the problem of determining the coefficients of polynomials.

In [2], the condition of basis matrices for the optimal contrast of Naor and Shamir has been given. Specializing Theorem 2 to maximum Naor and Shamir's contrast, we obtain the condition of [2]. As stated in Sect. 1, the definition of Naor and Shamir's contrast is not always best for indicating the recognizability of a reconstructed image. In the case of other contrasts, the condition of [2] is not available.

3.3 Example

To construct a $(2, 4, h, \ell, m)$ DPBM-VSSS where $m \leq$

50, we searched s_i and t_i satisfying the following equations.

$$\left\{ \begin{array}{l} \sum_{i=0}^3 \binom{3}{i} s_{i+j} = \sum_{i=0}^3 \binom{3}{i} t_{i+j} \quad \text{for } \forall j = 0, 1, \\ \sum_{i=0}^2 \binom{2}{i} s_{i+j} \neq \sum_{i=0}^2 \binom{2}{i} t_{i+j} \quad \text{for } \exists j = 0, 1, 2, \\ h = \sum_{i=0}^2 \binom{2}{i} s_i, \\ \ell = \sum_{i=0}^2 \binom{2}{i} t_i, \\ m = \sum_{i=0}^4 \binom{4}{i} s_i = \sum_{i=0}^4 \binom{4}{i} t_i. \end{array} \right.$$

As a result, a $(2, 4, h, \ell, m)$ DPBM-VSSS with the largest contrast of Naor and Shamir α_{NS} and the smallest m is

$$P_w(b, w) = \frac{1}{8}w^4 + \frac{1}{8}b^4, \quad P_b(b, w) = \frac{1}{4}b^2w^2, \quad (14)$$

that is, $h = 3$, $\ell = 1$, $m = 6$, and $\alpha_{NS} = 1/3$. It seems difficult to find this $(2, 4, 3, 1, 6)$ DPBM-VSSS by using Droste's method because Droste's method is for finding VSSS with the smallest m ; the $(2, 4, h, \ell, m)$ DPBM-VSSS with the smallest m is

$$P_w(b, w) = \frac{1}{24}w^4 + \frac{1}{8}b^4, \quad P_b(b, w) = \frac{1}{6}b^3w, \quad (15)$$

that is, $h = 1$, $\ell = 0$, $m = 4$, and $\alpha_{NS} = 1/4$. We note that the VSSS with the smallest m is not always the optimal VSSS in the sense that the value of α_{NS} is the largest.

Next, One of $(2, 4, h, \ell, m)$ DPBM-VSSSs with the largest α_{VV} is given by Eq. (15), where $\alpha_{VV} = 1/4$. One of $(2, 4, h, \ell, m)$ DPBM-VSSSs with the largest α_{ES} is also given by Eq. (14), where $\alpha_{ES} = 2/7$.

Remark The examples above are optimal for each of contrasts under the condition $m \leq 50$. Although the better VSSS with $m > 50$ might exist, it is not practical because the size is too large.

4. Member Verification in DPBM-VSSS

Before discussing the member verification with a VSSS, we consider the existence of a dishonest user in ordinary secret sharing schemes. The dealer keeps the original secret information, and distributes n shares generated with a (k, n) secret sharing scheme to n users. Suppose that just k users participates in the information reconstruction and a user who does not receive a share from the dealer is included. Hereafter, we call a user who does not receive a share from the dealer a dishonest user. For example, let us consider $(3, 3)$

Shamir's threshold scheme over $GF(p)$ [11]. The dealer distributes a share $(i, f(i))$ to User i ($i = 1, 2, 3$), where f is a randomly chosen polynomial with degree 2 over $GF(p)$. Assume that User 1, User 2, and User 4 take part in the information reconstruction. Although the dealer did not distribute a share to User 4, User 4 can take part in the information reconstruction because it is easy for User 4 to forge share $(4, y)$ if p is known, that is, User 4 may choose a value of y ($\in GF(p)$) at random. In such a case, it is impossible for User 1 and User 2 to detect the existence of dishonest User 4. Although the reconstructed information might be equal to the original information accidentally, it is different from the original information in almost all cases. Regardless of the validity of the reconstructed information, User 1 and User 2 cannot detect the existence of the dishonest user.

In order to detect the existence of the dishonest user, we have two methods; one is that $k+1$ (or more) users participate in the information reconstruction, and the other is that authenticated data is added to shares. The former method is not available when just k users participate. Using the latter method, it is possible to detect the existence of the dishonest user. The disadvantage of the latter method is the increase of the size of a share. Including the case of the dishonest act of the users who received the shares from the dealer, the relationship between the probability of the detection and the size of a share is studied in [7], [8]. From these previous works, it is impossible to detect the existence of the dishonest user by just k users without auxiliary authenticated data in ordinary secret sharing schemes.

We discuss how to detect the existence of the dishonest user in a (k, n) DPBM-VSSS. From the following discussion, it is possible to detect the existence of the dishonest user by just k users without auxiliary authenticated data. For example, consider the $(3, 3, 1, 0, 4)$ DPBM-VSSS such as

$$\begin{aligned} P_w(b, w) &= \frac{1}{6}w^3 + \frac{1}{2}b^2w, \\ P_b(b, w) &= \frac{1}{2}bw^2 + \frac{1}{3}b^3. \end{aligned} \quad (16)$$

From Eq. (16), User 4 learns that the size of a share is 4, and the number of "0" in a share is always 2. Assuming that User 4 takes part in image reconstruction with share "0011," we consider the following typical cases.

case 1 If shares of User 1 and User 2 are "0110" and "0101," then the reconstructed image is recognized as a white pixel. User 1 and User 2 cannot detect the existence of the dishonest user.

case 2 If shares of User 1 and User 2 are "0101" and "1001," then the reconstructed image is recognized as a black pixel. User 1 and User 2 cannot detect the existence of the dishonest user.

case 3 If shares of User 1 and User 2 are "0011" and

"0101," then they are aware of the existence of the dishonest user because the following matrix, which consists of their shares, is not a different permuting matrix represented by Eq. (16). However, it is unknown who is dishonest.

$$\begin{pmatrix} 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{pmatrix}$$

The number of possible pairs of shares of User 1, 2 is 24. The number of pairs of shares of User 1, 2 that a different permuting matrix is obtained by adapting them to User 4's share "0011" is 8. Therefore, the probability that User 1, 2 cannot detect the existence of the dishonest user is $1/3$. In other words, the existence of the dishonest user is detectable with probability $2/3$. Even if User 4 chooses any vector with size 4 and Hamming weight 2, this probability is not changed. Notice that it is unknown who is dishonest even if the existence of the dishonest user can be detected.

In the (k, n) DPBM-VSSS with basis polynomials $P_w(b, w)$, $P_b(b, w)$, suppose that k_d ($< k$) dishonest users to whom the dealer did not distribute shares take part in image reconstruction. In order that their existence cannot be detected, the dishonest users need to find a different permuting matrix $Y(b, w)$ satisfying the following conditions. Notice that the size m of a share is given as $n! \cdot P_w(1, 1)$.

$$\begin{aligned} Y(b, w) &= \sum_{i=0}^k \frac{\lambda_i}{i!(k-i)!} b^i w^{k-i} \\ m &= k! \cdot Y(1, 1) \\ \psi^{k_d} Y(b, w) &= \psi^{n-k+k_d} P_w(b, w) \end{aligned} \quad (17)$$

Namely, when the honest users' vectors are combined the dishonest users' ones together, it has to become a $k \times m$ different permuting matrix. Equation (17) means that vectors of the $k - k_d$ honest users appear in the forged different permuting matrix. Here, $\psi^{n-k} P_w(b, w)$ and $\psi^{n-k} P_b(b, w)$ are trivial solutions of $Y(b, w)$. In addition, we observe that there is no other solution because of the property of a different permuting matrix. Accordingly, if dishonest users do not show a matrix represented by $\psi^{n-k_d} P_w(b, w)$ to honest users, the k shares do not become a different permuting matrix.

The correct k shares are $\psi^{n-k} P_w(b, w)$ or $\psi^{n-k} P_b(b, w)$. We denote them by

$$\begin{aligned} \psi^{n-k} P_w(b, w) &= \sum_{i=0}^k \frac{\zeta_i}{i!(k-i)!} b^i w^{k-i}, \\ \psi^{n-k} P_b(b, w) &= \sum_{i=0}^k \frac{\eta_i}{i!(k-i)!} b^i w^{k-i}. \end{aligned} \quad (18)$$

When we distinguish between the different permuting matrix of Eq. (18) and its column-permuted matrix, the

numbers of different matrices are computed as

$$N_{w,k} = \frac{m!}{\prod_{i=0}^k \zeta_i^{\binom{k}{i}}}, \quad N_{b,k} = \frac{m!}{\prod_{i=0}^k \eta_i^{\binom{k}{i}}}.$$

Similarly, the $k - k_d$ shares of honest users are denoted by

$$\psi^{n-k+k_d} P_w(b, w) = \psi^{n-k+k_d} P_b(b, w) = \sum_{i=0}^{k-k_d} \frac{\theta_i}{i!(k-k_d-i)!} b^i w^{k-i}, \quad (19)$$

and the number of different matrices represented by Eq. (19) is obtained by

$$N_{k-k_d} = \frac{m!}{\prod_{i=0}^{k-k_d} \theta_i^{\binom{k-k_d}{i}}}.$$

From discussion above, the k_d shares of dishonest users are denoted by

$$\psi^{n-k_d} P_w(b, w) = \psi^{n-k_d} P_b(b, w) = \sum_{i=0}^{k_d} \frac{\lambda_i}{i!(k_d-i)!} b^i w^{k-i}, \quad (20)$$

and the number of different matrices represented by Eq. (20) is obtained by

$$N_{k_d} = \frac{m!}{\prod_{i=0}^{k_d} \lambda_i^{\binom{k_d}{i}}}.$$

For the $k - k_d$ shares of honest users, since there are $(N_{w,k} + N_{b,k})/N_{k-k_d}$ matrices for dishonest act to be successful, the probability of success of dishonest act is obtained by

$$Pr_{suc} = \frac{N_{w,k} + N_{b,k}}{N_{k-k_d} N_{k_d}}.$$

From this equation, it is desirable that m is large in order to improve the probability of detection of the existence of the dishonest user. This requirement contradicts requirement to improve contrast of the reconstructed image. Finally, in the case of $k = 2$, the existence of the dishonest user even if a large m is employed.

5. Concluding Remarks

In this paper we have proposed the construction of a DPBM-VSSS by using polynomials. Although the polynomial representation of [5] is applicable to only the class of lattice-based VSSSs, our polynomial representation is applicable to the wider class of DPBM-VSSSs. Using the polynomial representation, the construction of the optimal DPBM-VSSS is reduced to the

problem of determining the coefficients of polynomials. It remains an open problem to find an efficient algorithm for solving the problem of determining the coefficients of polynomials. In addition, we showed that a DPBM-VSSS was useful for preventing an illegal user from joining in the image reconstruction.

This paper discussed the class of DPBM-VSSSs. A (k, n) DPBM-VSSS guarantees that the reconstructed image by any k shares has same recognizability, i.e., contrast. However, in the case of a (k, n) VSSS which is not a DPBM-VSSS, the recognizability of a reconstructed image depends on the combination of k shares. If we consider the average recognizability of the reconstructed image, then there might exist a better VSSS outside of the class of DPBM-VSSSs. We will study the efficient construction for the wider class of VSSSs.

Acknowledgment

The authors thank to the anonymous reviewers for their useful comments.

References

- [1] G. Ateniese, C. Blundo, A. De Santis, and D.R. Stinson, "Visual cryptography for general access structures," *Information and Computation*, vol.129, no.86, pp.86-106, 1996.
- [2] C. Blundo, P. D'Arco, A. De Santis, and D.R. Stinson, "Contrast optimal threshold visual cryptography schemes," <http://cacr.math.uwaterloo.ca/~dstinson/papers/COTVCS.ps>, 1998.
- [3] S. Droste, "New results on visual cryptography," *Advances in Cryptology—CRYPTO'96*, Lecture Notes in Computer Science, vol.1109, pp.401-415, 1996.
- [4] P.A. Eisen and D.R. Stinson, "Threshold visual cryptography schemes with specified whiteness levels of reconstructed pixels," Submitted to *Design, Codes and Cryptography*, <http://cacr.math.uwaterloo.ca/~dstinson/>, 1999.
- [5] H. Koga, M. Iwamoto, and H. Yamamoto, "An analytic construction of the visual secret sharing scheme for color images," *IEICE Trans. Fundamentals*, vol.E84-A, no.1, pp.262-272, Jan. 2001.
- [6] H. Koga and H. Yamamoto, "Proposal of a lattice-based visual secret sharing scheme for color and gray-scale images," *IEICE Trans. Fundamentals*, vol.E81-A, no.6, pp.1262-1269, June 1998.
- [7] K. Kurosawa, S. Obana, and W. Ogata, "t-cheater identifiable (k, n) threshold secret sharing schemes," *Advances in Cryptology—CRYPTO'95*, Lecture Notes in Computer Science, vol.963, pp.410-423, 1995.
- [8] H. Kuwakado and H. Tanaka, "Improvement on the cheater identifiable threshold scheme," *IEICE Trans. Fundamentals*, vol.E84-A, no.4, pp.957-960, April 2001.
- [9] R.J. McEliece and D.V. Sarwate, "On sharing secrets and Reed-Solomon codes," *Commun. ACM*, vol.24, no.9, pp.583-584, 1981.
- [10] M. Naor and A. Shamir, "Visual cryptography," *Advances in Cryptology—EUROCRYPT'94*, Lecture Notes in Computer Science, vol.950, pp.1-12, 1994.
- [11] A. Shamir, "How to share a secret," *Commun. ACM*, vol.22, no.11, pp.612-613, 1979.

Appendix

The polynomial representation is based on the following intuitive idea. The Hamming weight of a column in a different permuting matrix is important, but the order of columns is meaningless. Roughly speaking, the term " $b^h w^{n-h}$ " means the n -dimensional column vector with the Hamming weight h . The number of such a vector is $n!/(h!(n-h)!)$. When we consider a (k, n) BM-VSSS including a (k, n) DPBM-VSSS, the number of rows of the basis matrix must be n . Hence we omit the numerator $n!$ which does not depend on k, h . The another reason why we ignore the numerator $n!$ is that the polynomial representation is well-defined when one row is removed from the basis matrix. Conversely, we define the polynomial representation in such a way that Eq. (9) holds.

We compare our polynomial representation with the polynomial representation of [5] (called the *KIY polynomial representation*). The KIY polynomial representation is defined for a column-permuting matrix. A matrix $M_n[a_1, a_2, \dots, a_n]$ is called the column-permuting matrix if it consists of all permutation of a vector $[a_1, a_2, \dots, a_n]^t$. For example,

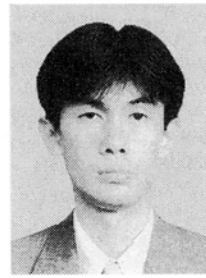
$$M_3[b, b, w] = \begin{pmatrix} b & b & b & b & w & w \\ b & w & b & w & b & b \\ w & b & w & b & b & b \end{pmatrix}$$

Considering $b = 1$ and $w = 0$, the class of VSSSs whose two basis matrices are column-permuting is a lattice-based VSSS. We see that the $(2, 3, 2, 1, 3)$ DPBM-VSSS shown in Sect. 2.2 is not a lattice-based VSSS.

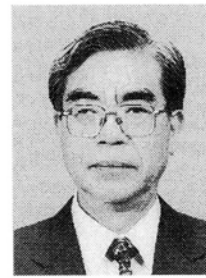
In addition, the KIY polynomial representation of $M_n[a_1, a_2, \dots, a_n]$ is a monomial $a_1 a_2 \cdots a_n$. For example, the KIY polynomial representation of $M_3[b, b, w]$ is $b^2 w$. The KIY polynomial representation is not applicable to a different permuting matrix. For example, the following different permuting matrix cannot be represented with the KIY polynomial representation.

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

Using our polynomial representation, $M_{3,2}$ is represented as $b^2 w/2$. As shown above, the KIY polynomial representation is not suitable for constructing a VSSS of black-white images. However, we should note that our polynomial representation is closely related with the KIY polynomial representation. For example, $M_{3,2}$ appears in $M_3[b, b, w]$ $2!(3-2)!$ times, which is the value of the denominator of the coefficient in our polynomial representation. We can interpret our polynomial representation as follows: the repeated columns in the column-permuting matrix are represented as the denominator of the coefficient of the polynomial.



Hidenori Kuwakado received the B.E., M.E. and D.E. degrees from Kobe University in 1990, 1992, and 1999 respectively. He worked for Nippon Telegraph and Telephone Corporation from 1992 to 1996. Since 1996, he has been a Research Associate in the Faculty of Engineering, Kobe University. His research interests are in cryptography and information security.



Hatsukazu Tanaka was born in Hyogo, Japan, on September 30, 1941. He received the B.E. degree from Kobe University, Kobe, Japan in 1964, the M.E. degree in 1966, and the D.E. degree in 1969, both from Osaka University, Osaka, Japan. He was appointed as a Research Associate in the Faculty of Engineering, University of Osaka Prefecture in 1969. From 1972 through 1987 he was an Associate Professor in the Department of Electrical Engineering, Kobe University. Since 1988 he has been a Professor in the Department of Electrical and Electronics Engineering, Kobe University. From 1980 through 1981 he was a member of the Communication Group of the University of Toronto, Toronto, Ontario, Canada, as a Visiting Scientist. His main work is on the basic theory of Information Engineering such as Information Theory, Coding Theory, Cryptography and Information Security, Image Processing, etc. Dr. Tanaka is a Fellow member of IEEE and a member of IACR.