PAPER *Special Section on Information Theory and Its Applications*

The Optimal n-out-of-n Visual Secret Sharing Scheme for Gray-Scale Images*

Mitsugu IWAMOTO†a), ***Student Member and*** **Hirosuke YAMAMOTO**†, ***Regular Member***

SUMMARY In this paper, a method is proposed to construct an n-out-of-n visual secret sharing scheme for gray-scale images, for short an (n, n)-VSS-GS scheme, which is optimal in the sense of contrast and pixel expansion, i.e., resolution. It is shown that any (n, n)-VSS-GS scheme can be constructed based on the so-called polynomial representation of basis matrices treated in [15], [16]. Furthermore, it is proved that such construction can attain the optimal (n, n)-VSS-GS scheme.

key words: *visual secret sharing scheme, gray-scale image, polynomial representation, contrast, pixel expansion*

1. Introduction

The visual secret sharing (VSS) scheme proposed by Naor and Shamir [18] is a method to encode a secret image into several shares, each of which does not reveal any information of the secret image. Shares are printed on transparencies for example, and distributed to n participants. The secret image can easily be decrypted only by stacking the shares in an arbitrary order. This property, i.e., the VSS scheme needs no computation in decryption, distinguishes the VSS scheme from ordinary secret sharing schemes.

The VSS scheme originated by Naor and Shamir is the (k, n)-threshold scheme for black-white binary (BW-binary) images, which we call a (k, n)-VSS-BW scheme. The (k, n)-threshold scheme means that any k out of n participants can decrypt the secret, but any $k - 1$ or less participants cannot obtain any information of the secret. The quality of the decrypted image can be evaluated by contrast and pixel expansion that determine the clearness and the resolution of the decrypted image, respectively. The optimizations of such parameters are treated in [3]–[5], [7]–[9], [11], [13], [16], [18], [22].

The (k, n) structure of VSS-BW scheme can be extended to a general access structure which is specified by qualified sets and forbidden sets [1]. The qualified set is a subset of n participants that can decrypt the secret image while a forbidden set is a subset of participants that can gain no information of the secret image.

Some other extensions are proposed in the case of (k, n)-VSS-BW schemes. For example, the method shown in [12] allows participants to reproduce plural secret images as the number of shares is increased, and each share of the method in [2] can have an identification image instead of a random sandstorm-like image. Some applications of VSS schemes are also investigated in [12], [17]. VSS schemes for color secret images are proposed in [3], [10], [14], [15], [19], [21]–[23].

In the previous studies, a secret image is usually assumed to be huge letters and/or simple geometrical shapes, e.g., circles, triangles, etc. But, if we can encrypt gray-scale images, a picture, for instance shown in Fig. 1, can be encrypted as a secret image. In [6], a VSS scheme for gray-scale images, for short a VSS-GS scheme, is studied, and the necessary and sufficient condition is derived to construct the VSS-GS scheme for general access structures. However, concerning the (n, n)-threshold scheme, the consideration for the optimality is not sufficient, and only the minimum contrast is treated. In this paper, we consider average contrast and brightness offset in addition to the minimum contrast, and we give the optimal construction of the VSS-GS scheme for the (n, n)-threshold scheme.

We show that an (n, n)-VSS-GS scheme can be constructed analytically by using polynomials and simultaneous partial differential equations. This method is first derived for color images in [15] and extended to BW-binary images in [16]. In this paper, we extend

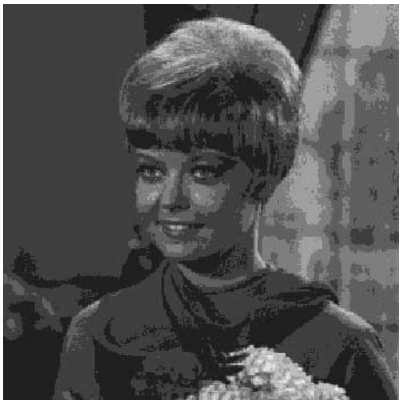


Fig. 1 Original secret image with 8-depths gray-scale.

Manuscript received January 21, 2002.
Manuscript revised April 22, 2002.
Final manuscript received June 6, 2002.

†The authors are with the Department of Mathematical Informatics, Graduate School of Information Science and Technology, The University of Tokyo, Tokyo, 113-8656 Japan.

a) E-mail: mitsugu@sr3.t.u-tokyo.ac.jp

*This paper was presented in part at the Computer Security Symposium at Morioka, 2001.

this method to gray-scale images. Furthermore, we show that the optimal scheme in all the (n, n)-VSS-GS schemes can be constructed by the proposed method.

This paper is organized as follows. In Sect. 2, (n, n)-VSS-GS schemes, average and minimum contrasts, and brightness offset are formally defined, and the polynomial representations of (n, n)-VSS-GS schemes are described. Section 3 is devoted to show that the optimal (n, n)-VSS-GS scheme, in the viewpoint of the pixel expansion, i.e., resolution, can be constructed by using the polynomial representation. Finally in Sect. 4, we derive tight upper bounds of the average and minimum contrasts.

2. Preliminaries

2.1 Definitions

A secret image is assumed to be a gray-scale image with t-depths, $t \geqq 2$, which is encrypted to n images called *shares*. Each share is distributed to each participant in $\mathcal{P}$, which is the set of n participants. In VSS-GS schemes, each pixel on the secret image is expanded to m subpixels. Parameter m is called *pixel expansion*, which should be as small as possible in the viewpoint of resolution for the decrypted image. Each subpixel consists of white or black, and a gray depth of a pixel is represented by a composition of white and black subpixels. We denote white and black by $\mathsf{0}$ and $\mathsf{1}$, respectively, and the mixture of them is expressed by the *OR* operation $\circ$, which is defined as $\mathsf{0} \circ \mathsf{0} = \mathsf{0}$, $\mathsf{1} \circ \mathsf{0} = \mathsf{0} \circ \mathsf{1} = \mathsf{1} \circ \mathsf{1} = \mathsf{1}$.

An (n, n)-VSS scheme for gray-scale images with t-depths, for short an (n, n)-VSS-GS-t scheme, can be expressed by a set of $n \times m$ matrices $T^{(k)}$, $k = 1, 2, \ldots, t$. The (i, j) element of $T^{(k)}$ takes $\mathsf{0}$ or $\mathsf{1}$ when the j-th subpixel of the i-th share for the k-th gray depth is white or black, respectively.

Let $\boldsymbol{x}_i^{(k)}$ be the i-th row vector in $T^{(k)}$. Then for a given set $\mathcal{A} = \{i_1, i_2, \ldots, i_q\} \subseteqq \mathcal{P}$, define $T^{(k)}[\mathcal{A}]$ as

$$T^{(k)}[\mathcal{A}] = \begin{bmatrix} \boldsymbol{x}_{i_1}^{(k)} \\ \boldsymbol{x}_{i_2}^{(k)} \\ \vdots \\ \boldsymbol{x}_{i_q}^{(k)} \end{bmatrix}. \tag{1}$$

Furthermore, we define a map h from $T^{(k)}[\mathcal{A}]$ to an m-dimensional row vector as

$$h(T^{(k)}[\mathcal{A}]) = \boldsymbol{x}_{i_1}^{(k)} \overset{m}{\circ} \boldsymbol{x}_{i_2}^{(k)} \overset{m}{\circ} \cdots \overset{m}{\circ} \boldsymbol{x}_{i_q}^{(k)}, \tag{2}$$

where the operator $\overset{m}{\circ}$ means the element-wise *OR* operation of m-dimensional vectors.

Suppose that $\mathcal{M}^n$ is a set of matrices with n rows, each element of which consists of $\mathsf{0}$ or $\mathsf{1}$. We introduce an equivalence relation $\sim$ into matrices in $\mathcal{M}^n$. For matrices $A, B \in \mathcal{M}^n$, $A \sim B$ means that matrices A and B have the same set of column vectors. In other word, it holds that for any permutation $\sigma : \{1, 2, \ldots, m\} \to \{1, 2, \ldots, m\}$,

$$[\boldsymbol{a}_1, \boldsymbol{a}_2, \ldots, \boldsymbol{a}_m] \sim [\boldsymbol{a}_{\sigma(1)}, \boldsymbol{a}_{\sigma(2)}, \ldots, \boldsymbol{a}_{\sigma(m)}], \tag{3}$$

where $\boldsymbol{a}_i$'s are column vectors. It is easy to check that the relation $\sim$ satisfies the conditions of equivalence relation, i.e., the reflective law, the symmetric law, and the transitive law. For the equivalence relation $\sim$, we can consider the quotient set $\mathcal{M}^n/\!\sim$, which consists of equivalence classes. An equivalence class is represented as $\langle R \rangle$ by a representative R of the class.

Now, we define the (n, n)-VSS-GS-t scheme as follows:

Definition 1: A VSS-GS scheme is called the (n, n)-VSS-GS-t scheme if each pixel with the k-th gray depth is determined by matrix $T^{(k)}$ which is randomly selected for each pixel from the following equivalence class $\langle B^{(k)} \rangle$.

(i) The representatives $B^{(k)}$, which are called the *basis matrices*, satisfy that

$$w(h(B^{(t)}[\mathcal{P}])) = m - d^{(t)}, \tag{4}$$

and for $k = 1, 2, \ldots, t-1$,

$$w(h(B^{(k+1)}[\mathcal{P}])) - w(h(B^{(k)}[\mathcal{P}])) = d^{(k)}, \tag{5}$$

where $w(\boldsymbol{v})$ stands for the Hamming weight of $\boldsymbol{v}$ and $d^{(k)}$ is the *relative difference* between the k-th and $(k+1)$-th gray depths. $d^{(k)}$ is an integer which satisfies $d^{(t)} \geqq 0$ and $d^{(k)} \geqq 1$ for $k = 1, 2, \ldots, t-1$.

(ii) For any set $\mathcal{F} \subset \mathcal{P}$ satisfying $|\mathcal{F}| \leqq n-1$, all $B^{(k)}[\mathcal{F}]$, $k = 1, 2, \ldots, t$, belong to the same equivalence class in $\mathcal{M}^{|\mathcal{F}|}/\!\sim$. □

We note from the above definition that basis matrix $B^{(1)}$ corresponds to the brightest pixel while $B^{(t)}$ expresses the darkest one in the decrypted image.

Next we consider *contrasts* and *brightness offset* which guarantee the clearness and the brightness of decrypted images, respectively.

Definition 2: Let $B^{(k)}$ be the basis matrices of an (n, n)-VSS-GS-t scheme. Then the *relative contrasts* are defined as $\alpha^{(k)} = \frac{d^{(k)}}{m}$ for $k = 1, 2, \ldots, t-1$, where m is the pixel expansion, i.e., the number of subpixels expanded from one pixel. Furthermore, the *minimum contrast*, the *average contrast*, and the *brightness offset* of a decrypted image are defined as

$$\alpha_{\min} = \min_{1 \leqq k \leqq t-1} \alpha^{(k)}, \tag{6}$$

$$\alpha_{\text{ave}} = \frac{\sum_{k=1}^{t-1} \alpha^{(k)}}{t-1}, \tag{7}$$

$$\beta = \frac{d^{(t)}}{m}, \tag{8}$$

respectively[†]. □

$\alpha_{\min}$ represents the worst clearness in two adjacent gray-depths while α_{ave} gives the average clearness of a decrypted image.

In the case of the BW-binary images, i.e., $t = 2$, these contrasts $\alpha_{\min}$ and α_{ave} coincide with each other and they are equal to a contrast

$$\alpha_{NS} = \frac{d^{(1)}}{m}, \tag{9}$$

which is defined by Naor and Shamir [18] for BW-binary secret images. Hence, $\alpha_{\min}$ and α_{ave} can be considered as extensions of α_{NS}. Since α_{NS} does not consider the effect of the brightness offset, Verheul and Van Tilborg [22] proposed another contrast

$$\alpha_{VV} = \frac{d^{(1)}}{m\left(d^{(1)} + 2d^{(2)}\right)}. \tag{10}$$

But it is pointed out in [8] that α_{VV} has a defect such that α_{VV} is equal to $1/m$ when $d^{(2)} = 0$. Instead of α_{VV}, Eisen and Stinson [8] proposed a new contrast

$$\alpha_{ES} = \frac{d^{(1)}}{m + d^{(2)}} = \frac{\alpha_{NS}}{1 + \beta}, \tag{11}$$

where two effects of α_{NS} and β are included in the contrast α_{ES}. In [8], [22], it is shown for the BW-binary case that β effects the clearness, and the larger the value of $d^{(1)}$ is and the smaller the value of $d^{(2)}$ is, the clearer the decrypted image is. In other words, large α_{NS} and small β are desirable. However, such consequences cannot be applied to the case of gray-scale generally.

In the case of VSS-GS schemes, the brightest pixel on decrypted images cannot become complete white while complete black can be realized. In addition, the darkest pixel on the decrypted image is not always complete black. Hence, even if two VSS-GS schemes have the same relative contrasts $\alpha^{(k)}$, the brightness offset β may be different. The larger β is, the brighter the decrypted image is. When $\beta = 0$, i.e., $d^{(t)} = 0$, then the darkest pixel is complete black. For instance, Fig. 2(a) has $\beta = 0$ and $\alpha^{(k)} = 1/16$ for $k = 1, 2, \ldots, 7$, which means $\alpha_{\min} = \alpha_{\text{ave}} = 1/16$. Figure 2(b) has the same relative differences $\alpha^{(k)}$ as Fig. 2(a), but Fig. 2(b) has $\beta = 1/16$. In Fig. 2, (b) is more natural than (a) because the complete black areas on (a) are much more conspicuous than other areas. But if the share size is smaller, Fig. 2(a) may look clearer than (b). These facts mean that it is difficult to determine the optimal value of β because it depends on the size and/or contents of the image, and hence β should be treated separately from $\alpha_{\min}$ or α_{ave}. In this paper, we derive the maximum $\alpha_{\min}$ and α_{ave} for a given β.

We note that gray-scale secret images are treated in [6] and [14]. But, [14] does not consider the contrast for gray-scale secret images. Although the relative contrasts and the minimum contrast are introduced in [6], the average contrast and the brightness offset are not considered.

Example 1: A $(3, 3)$-VSS-GS-3 scheme with $d^{(1)} = 1$, $d^{(2)} = 2$, and $d^{(3)} = 1$ is constructed by the following basis matrices

$$B^{(1)} = \begin{bmatrix} \mathsf{0000011011011} \\ \mathsf{0000101101101} \\ \mathsf{0000110110110} \end{bmatrix}, \tag{12}$$

$$B^{(2)} = \begin{bmatrix} \mathsf{0000011101101} \\ \mathsf{0000101011011} \\ \mathsf{0001000110111} \end{bmatrix}, \tag{13}$$

$$B^{(3)} = \begin{bmatrix} \mathsf{0001001001111} \\ \mathsf{0010010010111} \\ \mathsf{0100100100111} \end{bmatrix}, \tag{14}$$

which have pixel expansion $m = 13$. Since $w(h(B^{(1)}[\mathcal{P}])) = 9$, $w(h(B^{(2)}[\mathcal{P}])) = 10$, and $w(h(B^{(3)}[\mathcal{P}])) = 12$ hold, we note from Eqs. (4) and (5) that the basis matrices attain relative differences $d^{(1)} = 1$, $d^{(2)} = 2$, $d^{(3)} = 1$. From Def. 2, the contrasts and brightness offset become $\alpha^{(1)} = 1/13$, $\alpha^{(2)} = 2/13$, $\alpha_{\min} = 1/13$, $\alpha_{\text{ave}} = 3/26$, and $\beta = 1/13$. Since the first and second rows of $B^{(1)}$, $B^{(2)}$, and $B^{(3)}$ satisfy the following equivalence relation

$$\begin{aligned} &B^{(1)}[\{1,2\}] \sim B^{(2)}[\{1,2\}] \sim B^{(3)}[\{1,2\}] \\ &\quad \sim \begin{bmatrix} \mathsf{0000010101111} \\ \mathsf{0000101010111} \end{bmatrix} \end{aligned} \tag{15}$$

and the similar argument holds for other combinations of two rows, the security condition Def. 1 (ii) is also satisfied. □

Next, for two matrices A and B in $\mathcal{M}^n$, we define concatenation $A \odot B$ as, for example,

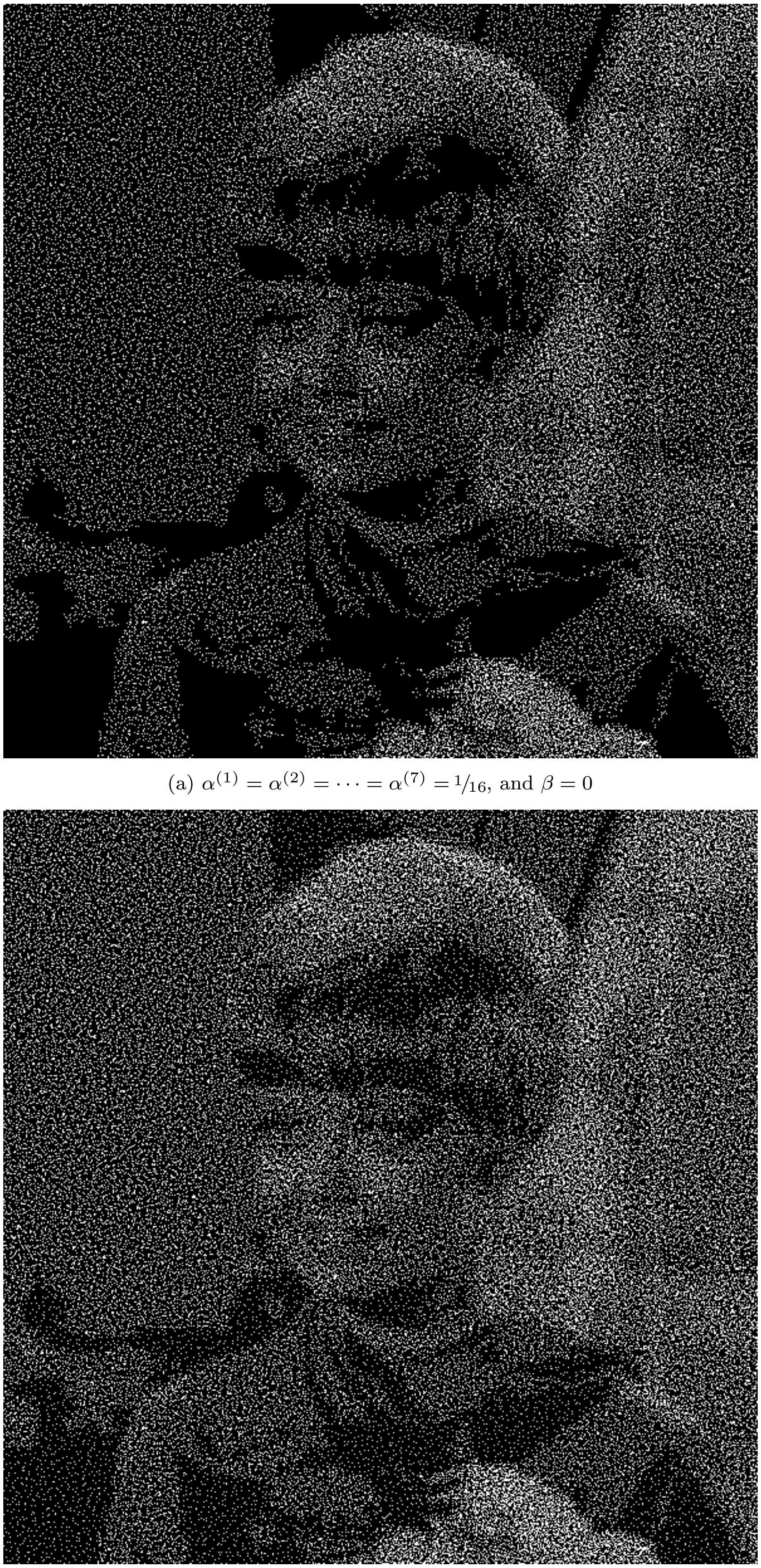
$$\begin{bmatrix} \mathsf{000} \\ \mathsf{000} \\ \mathsf{000} \end{bmatrix} \odot \begin{bmatrix} \mathsf{11} \\ \mathsf{11} \\ \mathsf{11} \end{bmatrix} = \begin{bmatrix} \mathsf{00011} \\ \mathsf{00011} \\ \mathsf{00011} \end{bmatrix}. \tag{16}$$

Furthermore, we can introduce naturally the operator $\odot$ into a quotient set $\mathcal{M}^n/\!\sim$ as $\langle A \rangle \odot \langle B \rangle \overset{\text{def}}{=} \langle A \odot B \rangle$. Note that this operator $\odot$ is not commutative in $\mathcal{M}^n$ but is commutative in $\mathcal{M}^n/\!\sim$ because it holds that $A \odot B \sim B \odot A$.

2.2 Polynomial Representation of VSS-GS Schemes

In [15], Koga, Iwamoto and Yamamoto proposed that a

[†] In [6], $\alpha^{(k)} = \frac{d^{(k)}}{m}$ is called as "relative differences" rather than "relative contrasts."



(a) $\alpha^{(1)} = \alpha^{(2)} = \cdots = \alpha^{(7)} = {}^{1}\!/_{16}$, and $\beta = 0$

(b) $\alpha^{(1)} = \alpha^{(2)} = \cdots = \alpha^{(7)} = {}^{1}\!/_{16}$, and $\beta = {}^{1}\!/_{16}$

Fig. 2 Comparison between two decrypted images with $\beta = 0$ and $\beta = {}^{1}\!/_{16}$.

simple and efficient method to construct VSS schemes for color secret images. In their method, the basis matrices are represented by polynomials, and it is shown that the basis matrices are derived analytically by solving some simultaneous partial differential equations for the polynomials. Kuwakado and Tanaka [16] modified the method to apply to VSS-BW schemes. In this subsection, we extend the method to VSS-GS schemes.

First, for any integer p satisfying $p \leqq n$, we define *constant-column-weight* (CCW) *matrix* $M_{p,n}$ with weight p as the $n \times \binom{n}{p}$ matrix that have all kinds of column vectors with Hamming weight p. For instance, $M_{2,4}$ is given by

$$M_{2,4} \sim \begin{bmatrix} \mathtt{001110} \\ \mathtt{011001} \\ \mathtt{110010} \\ \mathtt{100101} \end{bmatrix}. \tag{17}$$

Note that there are $\binom{n}{p}!$ matrices that are equivalent to $M_{p,n}$. But, by the benefit of the equivalence class, it suffices to consider only the representative, which is any one of the matrices.

Let $M'_{p,n}$ be an $(n-1) \times \binom{n}{p}$ matrix obtained by deleting a row from $M_{p,n}$. Then, it can easily be checked that $M_{p,n}$ and $M'_{p,n}$ satisfy $M'_{p,n} \sim M_{p-1,n-1} \odot M_{p,n-1}$, i.e.,

$$\langle M'_{p,n} \rangle = \langle M_{p-1,n-1} \rangle \odot \langle M_{p,n-1} \rangle \tag{18}$$

independently from the deleted row. Now we identify the equivalence class $\langle M_{p,n} \rangle$ with the monomial $\frac{b^p w^{n-p}}{p!(n-p)!}$ where p and $n-p$ represent the number of $\mathtt{1}$ (black) and $\mathtt{0}$ (white), respectively, in each column of $M_{p,n}$. We also represent formally the concatenation operator $\odot$ with plus operator $+$. If we use these representations, $\langle M_{p-1,n-1} \rangle \odot \langle M_{p,n-1} \rangle$ can be identified with a homogeneous polynomial $\frac{b^{p-1} w^{n-p}}{(p-1)!(n-p)!} + \frac{b^p w^{n-p-1}}{p!(n-p-1)!}$, which is equal to $(\frac{\partial}{\partial b} + \frac{\partial}{\partial w}) \frac{b^p w^{n-p}}{p!(n-p)!}$. This fact means from Eq. (18) that the partial differential operator $\frac{\partial}{\partial b} + \frac{\partial}{\partial w}$ represents the deletion of an arbitrary row from representative $M_{p,n}$, and hence all matrices in $\langle M_{p,n} \rangle$.

Example 2: For $M_{2,4}$ given by Eq. (17), the polynomial representation of $\langle M_{2,4} \rangle$ is $\frac{b^2 w^2}{2!2!}$. If any one row is deleted from $M_{2,4}$, the deleted matrix $M'_{2,4}$ satisfies from Eq. (17) that

$$M'_{2,4} \sim \begin{bmatrix} \mathtt{001110} \\ \mathtt{011001} \\ \mathtt{110010} \end{bmatrix} \sim \begin{bmatrix} \mathtt{001110} \\ \mathtt{010101} \\ \mathtt{100011} \end{bmatrix} = \begin{bmatrix} \mathtt{001} \\ \mathtt{010} \\ \mathtt{100} \end{bmatrix} \odot \begin{bmatrix} \mathtt{110} \\ \mathtt{101} \\ \mathtt{011} \end{bmatrix}.$$

Hence, by the polynomial representation, $\langle M'_{2,4} \rangle$ can be described as a homogeneous polynomial $\frac{b^1 w^2}{1!2!} + \frac{b^2 w^1}{2!1!}$, which is equal to $(\frac{\partial}{\partial b} + \frac{\partial}{\partial w}) \frac{b^2 w^2}{2!2!}$. □

In the polynomial representation, there is one-to-one correspondence between all equivalence classes in $\mathcal{M}^n/\!\sim$, which are generated from finite concatenations of CCW matrices in $\mathcal{M}^n$, and all homogeneous polynomials with degree n. Now, assume that a basis matrix $B^{(k)}$ is constructed by the concatenation of CCW matrices given by

$$B^{(k)} = \bigodot_{p=0}^{n} M_{p,n}^{\left[\mu_p^{(k)}\right]}, \tag{19}$$

where $\mu_p^{(k)}$ are nonnegative integers and $M^{[\ell]}$ stands for the ℓ-times concatenation of matrix M, i.e., $\underbrace{M \odot M \odot \cdots \odot M}_{\ell \text{ times}}$. Then the equivalence class of the basis matrix $B^{(k)}$ in Eq. (19) can be represented by the corresponding homogeneous polynomials $F^{(k)}(b,w)$ such as

$$F^{(k)}(b,w) = \sum_{p=0}^{n} \mu_p^{(k)} \frac{b^p w^{n-p}}{p!(n-p)!}, \tag{20}$$

which we call a *basis polynomial.* Hence, the properties in Def.1 that (n,n)-VSS-GS schemes must satisfy can be described by basis polynomials as follows.

Theorem 1: Let $F^{(k)}(b,w)$, $k = 1, 2, \ldots, t$, be basis polynomials which are identified with basis matrices $B^{(k)}$ of an (n,n)-VSS-GS-t scheme. Then the construction of basis matrices satisfying Def.1 is equivalent to solve the following simultaneous partial differential equations.

$$F^{(k)}(0,1) - F^{(k+1)}(0,1) = \frac{d^{(k)}}{n!}, \tag{21}$$

$$\psi F^{(1)}(b,w) = \cdots = \psi F^{(t)}(b,w), \tag{22}$$

where $\psi = \frac{\partial}{\partial b} + \frac{\partial}{\partial w}$ and $F^{(t+1)}(0,1) = 0$. Furthermore, the pixel expansion m is given by

$$m = n! F^{(k)}(1,1), \tag{23}$$

for any k. □

Proof of Theorem 1: In the same way as [15], [16], it is easy to check that Eqs. (21) and (22) correspond to Def. 1 (i) and (ii), respectively. Equation (23) holds because the column number of the CCW matrix $M_{p,n}$ is given by $n! \left. \frac{b^p w^{n-p}}{p!(n-p)!} \right|_{\substack{b=1 \\ w=1}}$. □

3. Minimum Pixel Expansion of (n,n)-VSS-GS schemes

In this section, based on the polynomial representation, we show how to construct the (n,n)-VSS-GS scheme that achieves the minimum pixel expansion for given relative differences.

3.1 Generality of Polynomial Representation in (n, n)-VSS-GS Schemes

If the basis matrix consists of the concatenation of CCW matrices, it can be represented by the corresponding basis polynomial. But we further show in the next theorem that the basis matrices of any (n, n)-VSS-GS scheme can be represented by the basis polynomials.

Theorem 2: For any (n, n)-VSS-GS-t scheme, the basis matrices $B^{(1)}, B^{(2)}, \ldots, B^{(t)}$, can be constructed by the concatenation of CCW matrices in the case that all the basis matrices contain no common column vectors except the zero column vector. □

We can assume that all the basis matrices contain no column vectors except the column zero vector because such common vectors play no role, and hence such common vectors can be removed or changed to the zero vectors to make a pixel bright.

Proof of Theorem 2: We first prove that for any column vector $\boldsymbol{v}$ in any $B^{(i)}$, $B^{(i)}$ must also contain all vectors with the same Hamming weight as $\boldsymbol{v}$.

In the case that $\boldsymbol{v}$ is a zero column vector, Theorem 2 holds obviously. Hence, assume that $\boldsymbol{v}$ with $w(\boldsymbol{v}) \geqq 1$ is a nonzero column vector of basis matrix $B^{(i)}$. Then there is at least one basis matrix $B^{(j)}$, $j \neq i$, that does not contain the vector $\boldsymbol{v}$. Although $B^{(j)}$ does not contain $\boldsymbol{v}$, it is possible that $B^{(i)}$ and $B^{(j)}$ have the same column vectors. In such cases, $B^{(i)}$ and $B^{(j)}$ can be represented as $B^{(i)} \sim \hat{B}^{(i)} \odot X$, $B^{(j)} \sim \hat{B}^{(j)} \odot X$, where $\hat{B}^{(i)}$ and $\hat{B}^{(j)}$ contain no common column vectors. Obviously, $\boldsymbol{v}$ is contained in $\hat{B}^{(i)}$. Since it must satisfy from the Def. 1 (ii) that any $n-1$ rows in $\hat{B}^{(i)}$ are equivalent to the corresponding $n-1$ rows in $\hat{B}^{(j)}$, $\hat{B}^{(j)}$ must contain all n column vectors $\boldsymbol{v}_1, \boldsymbol{v}_2, \ldots, \boldsymbol{v}_n$ that differ one Hamming distance from $\boldsymbol{v}$. On the other hand, for each $\boldsymbol{v}_\ell$, $\ell = 1, 2, \ldots, n$, $\hat{B}^{(i)}$ also must have all n column vectors that differ one Hamming distance from $\boldsymbol{v}_\ell$. These facts mean that $\hat{B}^{(i)}$ must have all the column vectors that differ even Hamming distances from $\boldsymbol{v}$.

Since the Hamming distance between any two vectors having the same Hamming weight is even, all the vectors with Hamming weight $w(\boldsymbol{v})$ must also be contained in $\hat{B}^{(i)}$.

We can also show by the similar argument that if $B^{(i)}$ contains the same column vector $\boldsymbol{v}$ ℓ-times, then each vector with Hamming weight $w(\boldsymbol{v})$ is also included in $B^{(i)}$ ℓ-times. Hence, in the case of (n, n)-VSS-GS schemes, any basis matrix can be represented by the concatenation of CCW matrices, i.e., the basis polynomials. □

3.2 Minimum Pixel Expansion of (n, n)-VSS-GS Schemes

In this subsection, we derive the optimal (n, n)-VSS-GS scheme in the viewpoint of the pixel expansion m, i.e., resolution for given relative differences $d^{(k)}$, $k = 1, 2, \ldots, t$.

Theorem 3: Let m be the pixel expansion of an (n, n)-VSS-GS-t scheme which has relative differences $d^{(k)}$, $k = 1, 2, \ldots, t$. Then the minimum pixel expansion m^* is given by

$$m^* = 2^{n-1} D + d, \tag{24}$$

where $d = d^{(t)}$ and $D = \sum_{k=1}^{t-1} d^{(k)}$. The basis matrices that attain m^* are given by

$$\begin{aligned} B^{(k)} = {} & M_{0,n}^{[d]} \\ & \odot \left[\bigodot_{\substack{p=0 \\ p:\mathrm{even}}}^{n} M_{p,n}^{[D^{(k)}]} \right] \odot \left[\bigodot_{\substack{p=1 \\ p:\mathrm{odd}}}^{n} M_{p,n}^{[D-D^{(k)}]} \right], \end{aligned} \tag{25}$$

where $D^{(k)} = \sum_{\ell=k}^{t-1} d^{(\ell)}$. □

Proof of Theorem 3: From Theorems 1 and 2, we can use the basis polynomials shown in Eq. (19) instead of the basis matrices in the construction of (n, n)-VSS-GS schemes. From Eqs. (20) and (21), $\mu_0^{(k)}$ must satisfy that

$$\mu_0^{(k)} = \sum_{\ell=k}^{t} d^{(\ell)} = d + D^{(k)}, \tag{26}$$

and

$$d = \mu_0^{(t)} < \mu_0^{(t-1)} < \cdots < \mu_0^{(1)} = d + D. \tag{27}$$

Since it holds that

$$\begin{aligned} & \psi F^{(k)}(b, w) \\ & \quad = \sum_{p=0}^{n-1} \left(\mu_p^{(k)} + \mu_{p+1}^{(k)} \right) \frac{b^p w^{n-p-1}}{p!(n-p-1)!} \end{aligned} \tag{28}$$

and $\psi F^{(k)}(b, w)$ must satisfy Eq. (22), $\mu_p^{(k)} + \mu_{p+1}^{(k)}$ must be independent of k. Hence, for some nonnegative integers μ_p, $\mu_p^{(k)}$ must satisfy that for any k

$$\mu_p = \mu_p^{(k)} + \mu_{p+1}^{(k)}. \tag{29}$$

Since all μ_p and $\mu_p^{(k)}$ are nonnegative integers, we have that

$$\mu_p \geqq \max_{1 \leqq k \leqq t} \mu_p^{(k)} \tag{30}$$

for any p. Letting $F'(b, w)$ be

$$\begin{aligned} &F'(b,w) \\ &\quad = \psi F^{(1)}(b,w) = \psi F^{(2)}(b,w) = \cdots = \psi F^{(t)}(b,w) \\ &\quad = \sum_{p=0}^{n-1} \mu_p \frac{b^p w^{n-p-1}}{p!(n-p-1)!}, \end{aligned} \tag{31}$$

the pixel expansion m is given from Eq. (23) as follows.

$$m = (n-1)!\ F'(1,1) = \sum_{p=0}^{n-1} \mu_p \binom{n-1}{p} \tag{32}$$

In order to minimize the pixel expansion m, we must minimize all μ_p. In the following, we show that such minimization is possible.

Since it holds from Eqs. (27) and (30) that $\mu_0 \geqq \max_{1 \leqq k \leqq t} \mu_0^{(k)} = \mu_0^{(1)} = d + D$, μ_0 can be represented as $\mu_0 = \varepsilon_0 + d + D$ for some nonnegative parameter $\varepsilon_0 \geqq 0$. Substituting μ_0 into Eq. (29), we have $\mu_1^{(k)} = \varepsilon_0 + d + D - \mu_0^{(k)}$. Then μ_1 can be represented as $\mu_1 = \varepsilon_0 + \varepsilon_1 + D$ for another nonnegative parameter $\varepsilon_1 \geqq 0$ because it is obtained from Eqs. (27) and (30) that $\mu_1 \geqq \max_{1 \leqq k \leqq t} \mu_1^{(k)} = \varepsilon_0 + d + D - \min_{1 \leqq k \leqq t} \mu_0^{(k)} = \varepsilon_0 + d + D - \mu_0^{(t)} = \varepsilon_0 + D$. Next we have from Eq. (29) that $\mu_2^{(k)} = \mu_1 - \mu_1^{(k)} = \varepsilon_1 - d + \mu_0^{(k)}$. Hence, it is also obtained from Eqs. (27) and (30) that $\mu_2 \geqq \max_{1 \leqq k \leqq t} \mu_2^{(k)} = \varepsilon_1 - d + \max_{1 \leqq k \leqq t} \mu_0^{(k)} = \varepsilon_1 - d + \mu_0^{(1)} = \varepsilon_1 + D$. Repeating the similar procedure, we have that $\mu_0 = \varepsilon_0 + d + D$ and for $p = 1, 2, \ldots, n$,

$$\mu_p = \varepsilon_p + \varepsilon_{p-1} + D, \tag{33}$$

$$\mu_p^{(k)} = \varepsilon_{p-1} + \begin{cases} \mu_0^{(k)} - d & \text{if } p \text{ is even} \\ D + d - \mu_0^{(k)} & \text{if } p \text{ is odd,} \end{cases} \tag{34}$$

where $\varepsilon_p \geqq 0$ are parameters and $\mu_0^{(k)}$ is given by Eq. (26). Since μ_p should be as small as possible, the optimal μ_p is obtained by letting $\varepsilon_p = 0$ for all p as follows.

$$\mu_p = \begin{cases} d + D & \text{if } p = 0 \\ D & \text{if } p \geqq 1. \end{cases} \tag{35}$$

This optimal case can be attained from Eqs. (26) and (34) by

$$\mu_p^{(k)} = \begin{cases} D^{(k)} & \text{if } p \geqq 2 \text{ is even} \\ D - D^{(k)} & \text{if } p \geqq 1 \text{ is odd,} \end{cases} \tag{36}$$

and the minimum pixel expansion m^* is obtained from Eqs. (32) and (35) by

$$\begin{aligned} m^* &= \mu_0 + \sum_{p=1}^{n-1} \mu_p \binom{n-1}{p} \\ &= d + D + D \sum_{p=1}^{n-1} \binom{n-1}{p} \\ &= d + D + D(2^{n-1} - 1) \\ &= 2^{n-1} D + d. \end{aligned} \tag{37}$$

Finally, the optimal basis matrices shown in Eq. (25) are obtained from Eqs. (19),(26) and (36). □

We note from the proof of Theorem 3 that in case of $m \geqq 2^{n-1}D + d$, the basis matrices can be constructed by selecting $\varepsilon_p \geqq 0$ adequately. Hence we have the following corollary.

Corollary 1: An (n,n)-VSS-GS-t scheme with relative differences $d^{(k)}$ and pixel expansion m can be constructed if and only if it holds that

$$m \geqq 2^{n-1} D + d. \tag{38}$$

□

Theorem 3 gives the minimum pixel expansion m^* for given relative differences $d^{(k)}$. But, when we can select the minimum values of $d^{(k)}$, i.e., $d^{(t)} = 0$, $d^{(k)} = 1$ for $k = 1, 2, \ldots, t-1$, we have that $D = t - 1$ and $d = 0$. This case attains the overall minimum of pixel expansion m^* in all allowable $d^{(k)}$.

Corollary 2 ([6], [18]): The minimum pixel expansion m^* in all (n,n)-VSS-GS-t schemes is given by $2^{n-1}(t-1)$. □

This corollary coincides with the results shown in [6] and, in case of $t = 2$, [18].

Remark: We note that an (n,n)-VSS-GS scheme can be constructed in a different way. We first transform a gray-scale secret image into a BW-binary image with t-depth halftones, e.g., by the dither method [20]. Then we encrypt the binary image by the basis matrices of an (n,n)-VSS-BW scheme. If the differences of the k-th and $(k+1)$-th halftones are $d^{(k)}$ which are determined by a dither matrix, each pixel must be expanded to at least D subpixels in the case of $d^{(t)} = 0$. Since 2^{n-1} subpixels are required to realize any (n,n)-VSS-BW scheme, the total pixel expansion becomes $2^{n-1}D$, which coincides with Eq. (24) in the case of $d^{(t)} = 0$. Hence, such construction of (n,n)-VSS-GS-t schemes is also optimal. □

4. Maximum Contrasts and Minimum Pixel Expansion

In Sect. 2.1, we pointed out that the optimal brightness offset β may depend on the size or contents of a secret image. However, for a given β, the contrasts should be maximized. Hence, for a given β, we derive the maximum $\alpha_{\min}$ and α_{ave} in Sect. 4.1 and the minimum pixel expansion that attains the maximum average contrast α_{ave} in Sect. 4.2.

4.1 Maximum $\alpha_{\rm min}$ and $\alpha_{\rm ave}$

Blundo, De Santis and Naor [6] showed that a VSS-GS-t scheme with a given access structure Γ exists if and only if it holds that $\sum_{k=1}^{t-1} \alpha^{(k)} \leqq \alpha_{NS}^*$, where α_{NS}^* is the maximum α_{NS} defined in Eq. (9) for the VSS-BW schemes with the access structure Γ. In the case of the (n,n)-VSS-GS schemes, the above inequality becomes

$$\sum_{k=1}^{t-1} \alpha^{(k)} \leqq 2^{-(n-1)} \tag{39}$$

because the maximum contrast α_{NS}^* is given by $\alpha_{NS}^* = 2^{-(n-1)}$ as shown in [18]. This condition given by Eq. (39) can also be derived directly from Corollary 1 by dividing both sides of Eq. (38) by m and letting $d=0$. Furthermore, we can also obtain the condition in the case of $d \neq 0$, i.e., $\beta \neq 0$ from Eq. (38) as follows.

Corollary 3: An (n,n)-VSS-GS-t scheme with relative contrasts $\alpha^{(1)}, \alpha^{(2)}, \ldots, \alpha^{(t-1)}$ and brightness offset β can be constructed if and only if it holds that

$$\sum_{k=1}^{t-1} \alpha^{(k)} \leqq 2^{-(n-1)}(1-\beta), \tag{40}$$

and $\alpha^{(k)}$ and β are rational numbers. □

Corollary 3 can be derived from Corollary 1. But we have from Corollary 3 only that

$$m \geqq K\left(2^{n-1}D + d\right) \tag{41}$$

for some integer $K \geqq 1$. Hence, Corollary 1 cannot be derived directly from Corollary 3. In [6], it is described that Eq. (41) with $(K=1, D=t-1, d=0)$ is obtained directly from Eq. (40) with $\beta=0$ in the (n,n)-threshold case although $K=2^{n-1}$ is assumed in their proof of [6, Theorem 3.2]. Therefore, their proof for the (n,n)-VSS-GS schemes is not rigorous.

Note that the case of $\beta=0$ does not always give a clear image. Corollary 3 gives how the value of β effects the relative contrasts.

Next, from Corollary 3 and Theorem 3, we derive the maximum $\alpha_{\rm ave}$ and $\alpha_{\rm min}$.

Theorem 4: In all (n,n)-VSS-GS-t schemes, the average and minimum contrasts, $\alpha_{\rm ave}$ and $\alpha_{\rm min}$, are bounded by

$$\alpha_{\rm ave}, \alpha_{\rm min} \overset{\rm (a)}{\leqq} \frac{1-\beta}{2^{n-1}(t-1)} \overset{\rm (b)}{\leqq} \frac{1}{2^{n-1}(t-1)} \tag{42}$$

for $t \geqq 2$. There always exist the basis matrices that attain the equality of (a), and inequality (b) holds with equality when $\beta=0$. □

Proof of Theorem 4: From Corollary 3 and Eq. (7), it is obvious that inequality (a) holds with respect to $\alpha_{\rm ave}$. On the other hand, for $\alpha_{\rm min}$, inequality (a) follows from that $(t-1)\alpha_{\rm min} \leqq \sum_{k=1}^{t-1} \alpha^{(k)} \leqq 2^{-(n-1)}(1-\beta)$, where the first inequality holds with equality if and only if

$$d^{(1)} = d^{(2)} = \cdots = d^{(t-1)}. \tag{43}$$

Finally, inequality (b) holds because of $0 \leqq \beta < 1$. □

We note from the proof of Theorem 4 that both $\alpha_{\rm min}$ and $\alpha_{\rm ave}$ can be maximized at the same time in all (n,n)-VSS-GS-t schemes by letting $d^{(k)}$ satisfy Eq. (43) and $d=0$. The next example attains the maximum $\alpha_{\rm min}$ and $\alpha_{\rm ave}$ in all $(3,3)$-VSS-GS-4 schemes.

Example 3: Letting $d^{(1)} = d^{(2)} = d^{(3)} = 1$ and $d^{(4)} = 0$, the basis polynomials of the optimal $(3,3)$-VSS-GS scheme with the maximum $\alpha_{\rm min}$ and $\alpha_{\rm ave}$ is given from Eqs. (20),(26) and (36) by

$$\begin{aligned}
F^{(1)}(b,w) &= 3\frac{b^0w^3}{0!3!} + 0\frac{b^1w^2}{1!2!} + 3\frac{b^2w^1}{2!1!} + 0\frac{b^3w^0}{3!0!},\\
F^{(2)}(b,w) &= 2\frac{b^0w^3}{0!3!} + 1\frac{b^1w^2}{1!2!} + 2\frac{b^2w^1}{2!1!} + 1\frac{b^3w^0}{3!0!},\\
F^{(3)}(b,w) &= 1\frac{b^0w^3}{0!3!} + 2\frac{b^1w^2}{1!2!} + 1\frac{b^2w^1}{2!1!} + 2\frac{b^3w^0}{3!0!},\\
F^{(4)}(b,w) &= 0\frac{b^0w^3}{0!3!} + 3\frac{b^1w^2}{1!2!} + 0\frac{b^2w^1}{2!1!} + 3\frac{b^3w^0}{3!0!},
\end{aligned}$$

which achieve $\alpha_{\rm min} = \alpha_{\rm ave} = {}^1\!/_{12}$, $\beta=0$ and $m=12$. □

4.2 Minimum Pixel Expansion with Maximum Average Contrast

In this subsection we consider the minimum pixel expansion that attains the maximum average contrast $\alpha_{\rm ave}$ for a given brightness offset β. From Corollary 3, the relative contrast $\alpha^{(k)}$ and the brightness offset β must satisfy Eq. (40), and the equality case in Eq. (40) maximizes the average contrast $\alpha_{\rm ave}$. Therefore, we consider such a case.

Theorem 5: In an (n,n)-VSS-GS-t scheme, assume that the relative contrasts $\alpha^{(1)}, \alpha^{(2)}, \ldots, \alpha^{(t-1)}$ and the brightness offset β satisfy Eq. (40) with equality, and each $\alpha^{(k)}$ and β are given by rational number $\alpha^{(k)} = \frac{p_k}{q_k}$ for $k=1,2,\ldots,t-1$ and $\beta = \frac{p_t}{q_t}$, where p_k and q_k are relatively prime. In case of $\beta=0$, $p_t=0$ and $q_t=1$. Then, the minimum pixel expansion m^* is given by the least common multiple of $q_1, q_2, \ldots, q_t$. □

Proof of Theorem 5: Let ℓ be the least common multiple of $q_1, q_2, \ldots, q_t$. Then, $\alpha^{(k)}$ and β satisfy that

$$\alpha^{(k)} = \frac{d^{(k)}}{m} = \frac{p_k}{q_k} = \frac{p_k \dfrac{\ell}{q_k}}{\ell}, \tag{44}$$

$$\beta = \frac{d^{(t)}}{m} = \frac{p_t}{q_t} = \frac{p_t \dfrac{\ell}{q_t}}{\ell}. \tag{45}$$

Since p_k and q_k are relatively prime, m must be a multiple of q_k for every k and, hence, it cannot become smaller than ℓ. Since $p_k \frac{\ell}{q_k}$ is an integer, we can set $d^{(k)}$ as $d^{(k)} = p_k \frac{\ell}{q_k}$. In this case, it holds from Eq. (24) that

$$\begin{aligned} m^* &= 2^{n-1} \sum_{k=1}^{t-1} d^{(k)} + d^{(t)} = 2^{n-1} \ell \sum_{k=1}^{t-1} \frac{p_k}{q_k} + p_t \frac{\ell}{q_t} \\ &= \ell \left(2^{n-1} \sum_{k=1}^{t-1} \alpha^{(k)} + \beta \right) = \ell, \end{aligned} \tag{46}$$

where the last equality follows from the equality case of Eq. (40). Hence, ℓ is the minimum pixel expansion. □

We note from the proof of Theorem 4 that the minimum pixel expansion m^* given in Theorem 5 also attains the maximum $\alpha_{\min}$ if $\alpha^{(k)}$ and β satisfy Eq. (40) with equality and $\alpha^{(1)} = \alpha^{(2)} = \cdots = \alpha^{(t-1)}$.

Example 4: We construct the $(3,3)$-VSS-GS-4 scheme with relative contrasts $\alpha^{(1)} = 1/16$, $\alpha^{(2)} = 3/32$, $\alpha^{(3)} = 1/16$ and brightness offset $\beta = 1/8$ which satisfy $\sum_{k=1}^{4-1} \alpha^{(k)} = 2^{-(3-1)}(1 - \frac{1}{8})$. Since the least common multiple of denominators of $\alpha^{(k)}$ and β is given by $\ell = 32$, we can attain $m^* = 32$. Actually, we can realize this m^* by letting $d^{(k)} = \ell\alpha^{(k)}$ and $d^{(t)} = \ell\beta$, i.e., $d^{(1)} = 2$, $d^{(2)} = 3$, $d^{(3)} = 2$, and $d^{(4)} = 4$, which derive the following basis polynomials.

$$\begin{aligned} F^{(1)}(b,w) &= 11\frac{b^0w^3}{0!3!} + 0\frac{b^1w^2}{1!2!} + 7\frac{b^2w^1}{2!1!} + 0\frac{b^3w^0}{3!0!}, \\ F^{(2)}(b,w) &= 9\frac{b^0w^3}{0!3!} + 2\frac{b^1w^2}{1!2!} + 5\frac{b^2w^1}{2!1!} + 2\frac{b^3w^0}{3!0!}, \\ F^{(3)}(b,w) &= 6\frac{b^0w^3}{0!3!} + 5\frac{b^1w^2}{1!2!} + 2\frac{b^2w^1}{2!1!} + 5\frac{b^3w^0}{3!0!}, \\ F^{(4)}(b,w) &= 4\frac{b^0w^3}{0!3!} + 7\frac{b^1w^2}{1!2!} + 0\frac{b^2w^1}{2!1!} + 7\frac{b^3w^0}{3!0!}. \end{aligned}$$

□

Finally we consider the minimum pixel expansion m^* in the case that both $\alpha_{\min}$ and α_{ave} are maximized at the same time for $\beta = 0$. From Theorem 4, the maximum of $\alpha_{\min}$ and α_{ave} can be achieved when $\alpha^{(k)} = \frac{1}{(t-1)2^{n-1}}$ for all $k = 1, 2, \ldots, t-1$. In this case, the pixel expansion is given by $2^{n-1}(t-1)$ from Theorem 5. We note from Corollary 2 that this m^* is equal to the minimum pixel expansion in all (n,n)-VSS-GS-t schemes.

5. Conclusion

In this paper, we considered the optimal construction of the (n,n)-VSS-GS schemes to minimize the pixel expansion for given relative differences $d^{(k)}$, relative contrasts $\alpha^{(k)}$, or the minimum and average contrasts $\alpha_{\min}$ and α_{ave} with a brightness offset β.

First we showed that the basis polynomials can represent any (n,n)-VSS-GS scheme. Then we derived analytically the attainable minimum pixel expansion for given relative differences $d^{(k)}$ by using the polynomial representation of VSS-GS schemes. Furthermore, we clarified the maximum value of contrasts $\alpha_{\min}$ and α_{ave}, and we derived the minimum pixel expansion for given relative contrasts $\alpha^{(k)}$ and brightness offset β.

(n,n)-VSS-GS schemes can easily be extended to general (k,n)-VSS-GS schemes or VSS-GS schemes with a general access structures in the same way as shown in, for example, [1], [15]. But it is difficult to derive the optimal (k,n)-VSS-GS scheme in the case of $k < n$. We note that Theorem 3 does not hold for the (k,n)-threshold case. For instance, the optimal construction of the $(2,n)$-VSS-BW scheme shown in [5] cannot be represented by any basis polynomials.

Acknowledgments

The authors thank Dr. Hiroki Koga and Dr. Tomohiro Ogawa for their helpful comments. This study is supported in part by Grants-in-Aid for Science Research 13224028 and 14019028 in Japan.

References

[1] G. Ateniese, C. Blundo, A.D. Santis, and D.R. Stinson, “Visual cryptography for general access structures,” Information and Computation, vol.129, pp.86–106, 1996.

[2] G. Ateniese, C. Blundo, A.D. Santis, and D.R. Stinson, “Extended capabilities for visual cryptography,” Theoretical Computer Science, vol.250, nos.1–2, pp.143–161, 2001.

[3] C. Blundo, A.D. Bonis, and A.D. Santis, “Improved schemes for visual cryptography,” Designs, Codes and Cryptography, vol.24, no.3, pp.255–278, 2001.

[4] C. Blundo, P. D’Arco, A.D. Santis, and D.R. Stinson, “Contrast optimal threshold visual cryptography schemes,” SIAM J. Discrete Mathematics, to appear.

[5] C. Blundo, P. D’Arco, A.D. Santis, and D.R. Stinson, “On the contrast in visual cryptography schemes,” J. Cryptology, vol.12, issue 4, pp.261–289, 1999.

[6] C. Blundo, A.D. Santis, and M. Naor, “Visual cryptography for gray-level images,” Inf. Process. Lett., vol.75, issue 6, pp.255–259, 2001.

[7] S. Droste, “New results on visual cryptography,” Advances in Cryptology-CRYPTO’96, LNCS–1109, pp.401–415, Springer-Verlag, 1996.

[8] P.A. Eisen and D.R. Stinson, “Threshold visual cryptography schemes with specified whiteness levels of reconstructed pixels,” Designs, Codes and Cryptography, vol.25, no.1, pp.15–61, 2002.

[9] T. Hofmeister, M. Krause, and H.U. Simmon, “Contrast-optimal k out of n secret sharing schemes in visual cryptology,” COCOON’97, LNCS–1276, pp.176–185, Springer-Verlag, 1997.

[10] T. Ishihara and H. Koga, “New constructions of the lattice-based visual secret sharing using mixture of colors,” IEICE

Trans. Fundamentals, vol.E85–A, no.1, pp.158–166, Jan. 2002.

[11] R. Ito, H. Kuwakado, and H. Tanaka, "Image size invariant visual cryptography," IEICE Trans. Fundamentals, vol.E82–A, no.10, pp.2172–2177, Oct. 1999.

[12] T. Kato and H. Imai, "An extended construction method of visual secret sharing scheme," IEICE Trans. Fundamentals (Japanese Edition), vol.J81–A, no.6, pp.1344–1351, June 1996.

[13] M. Krause and H.U. Simon, "Determining the optimal contrast for secret sharing schemes in visual cryptology," LATIN'00, LNCS–1776, pp.280–291, Springer-Verlag, 2000.

[14] 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.

[15] 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.

[16] H. Kuwakado and H. Tanaka, "Polynomial representation of a visual secret sharing scheme and its application," IEICE Trans. Fundamentals, vol.E85–A, no.6, pp.1379–1386, June 2002.

[17] M. Naor and B. Pinkas, "Visual authentication and identification," Advances in Cryptology-CRYPTO'97, LNCS–1294, pp.322–336, Springer-Verlag, 1997.

[18] M. Naor and A. Shamir, "Visual cryptography," Advances in Cryptology-EUROCRYPT'94, LNCS–950, pp.1–12, Springer-Verlag, 1994.

[19] M. Naor and A. Shamir, "Visual cryptography II: Improving the contrast via the cover base," Security Protocols, LNCS–1189, pp.197–202, Springer Verlag, 1997.

[20] A.N. Netravali and B.G. Haskell, Digital Pictures: Representation, Computation, and Standards, 2nd ed., Plenum Press, 1994.

[21] V. Rijmen and B. Preneel, "Efficient color visual encryption or 'shared colors of Benetton'," presented at the rump session of EUROCRYPT'96, 1996.

[22] E.R. Verheul and H.C.A. van Tilborg, "Constructions and properties of *k* out of *n* visual secret sharing scheme," Designs, Codes, and Cryptography, vol.1, no.2, pp.179–196, 1997.

[23] C.-N. Yang and C.-S. Laih, "New colored visual secret sharing scheme," Designs, Codes, and Cryptography, vol.20, no.3, pp.325–335, 2000.

Mitsugu Iwamoto was born in Fukuoka, on 29 July, 1976. He received the B.E. and M.E. degrees from the University of Tokyo, Japan, in 1999 and 2001, respectively. Currently, he is a doctor course student in the Department of Mathematical Informatics, Graduate School of Information Science and Technology, the University of Tokyo. His research interest includes information security and cryptography.

Hirosuke Yamamoto was born in Wakayama, Japan, on 15 November, 1952. He received the B.E. degree from Shizuoka University, Shizuoka, Japan, in 1975 and M.E. and Dr.E. degrees from the University of Tokyo, Japan, 1977 and 1980, respectively, all in electrical engineering. In 1980, he joined the Tokushima University, Tokushima, Japan. He was an Associate Professor in Tokushima University, University of Electro-Communications, and the University of Tokyo, during 1983–1987, 1987–1993, and 1993–1999, respectively. Since March 1999, he is a professor in the University of Tokyo. Currently, he is with the Department of Mathematical Informatics, Graduate School of Information Science and Technology, the University of Tokyo. In 1989–1990, he was a Visiting Scholar at the Information Systems Laboratory, Stanford University. His research interests are Shannon theory, coding theory, cryptology, and communication theory.