IEICE TRANS. FUNDAMENTALS, VOL.E84–A, NO.1 JANUARY 2001

PAPER Special Section on Cryptography and Information Security

An Analytic Construction of the Visual Secret Sharing Scheme for Color Images*

Hiroki KOGA†, ***Regular Member***, **Mitsugu IWAMOTO**††, ***Nonmember***, ***and*** **Hirosuke YAMAMOTO**††, ***Regular Member***

SUMMARY This paper proposes a new construction of the visual secret sharing scheme for the (n, n)-threshold access structure applicable to color images. The construction uses matrices with n rows that can be identified with homogeneous polynomials of degree n. It is shown that, if we find a set of homogeneous polynomials of degree n satisfying a certain system of simultaneous partial differential equations, we can construct a visual secret sharing scheme for the (n, n)-threshold access structure by using the matrices corresponding to the homogeneous polynomials. The construction is easily extended to the cases of the (t, n)-threshold access structure and more general access structures.

key words: *secret sharing, visual secret sharing, visual cryptology, general access structure*

1. Introduction

The visual secret sharing scheme (VSSS) originated from Naor and Shamir [9] provides a unconventional way for secret sharing of digital images. In the VSSS with n participants a secret image is encrypted into n images called *shares*. The n shares are distributed to n respective participants. The VSSS has an important property that no computation is required for decryption of the shares. That is, if the n shares are printed on n respective transparencies, all sets of participants qualified for reproducing the secret image can decrypt their shares only by stacking. For any unqualified sets of participants, the VSSS is designed not to reveal any information on the secret image.

Secret sharing of black-white images for the (t, n)-threshold access structure is discussed in [2]–[5], [7], [9], [14], where t is an integer satisfying $2 \leq t \leq n$. In particular, from viewpoints of the combinatorics and the linear programming, [2], [3], [5] attempt to optimize the contrast of the reproduced image obtained by stacking arbitrary t shares. Construction of the VSSS for general access structures is discussed in [1]. It proposes constructions of the VSSS for various access structures and obtains several combinatorial bounds on the contrast.

On the other hand, there are not many results on secret sharing of color images [6], [8], [10], [11], [14] for the (t, n)-threshold access structure. In addition, there is no study that deals with the VSSS for color images designed for general access structures. A technical difficulty on the VSSS for color images may consist in how we can mathematically express stacking of colored pixels instead of using simple "OR" operation that expresses stacking of black and white pixels. In order to define the VSSS for color images in strict mathematical sense, [8] treats pixels as elements of a bounded lattice of colors. In the framework in [8] stacking of pixels is expressed as the join operation of the bounded lattice, which enables to reproduce a secret image by stacking of shares in an arbitrary order. However, the optimality of the constructions given in [8] is not guaranteed, i.e., brightness of the reproduced image is not maximized in the constructions.

In this paper we propose a new construction of the (n, n)-VSSS for color images defined over a bounded upper semilattice, where the (n, n)-VSSS means the VSSS for the (n, n)-threshold access structure. As is mentioned in [9], the VSSS is obtained if we can construct matrices called the *basis matrices* with certain properties. We construct the basis matrices from concatenations of matrices with n rows belonging to the class each element of which can be identified with a monomial of degree n. The concatenation of such matrices can be expressed in homogeneous polynomials of degree n. We prove that, if a set of homogeneous polynomials of degree n is a solution to a system of simultaneous partial differential equations satisfying a specified initial condition, the set of matrices corresponding to the solution can be used as the basis matrices. In addition, if the solution satisfies the *minimal* condition, the solution turns out to be unique. This property guarantees a certain kind of optimality of the basis matrices corresponding to the minimal solution and enables to search for the globally optimal basis matrices in the class that make the reproduced image as bright as possible.

The new construction has two byproducts. One is a construction of the basis matrices of the (t, n)-VSSS. We can show that it is easy to obtain the basis matrices of the (t, n)-VSSS if we obtain the basis matrices of the (t, t)-VSSS by using the new construction. The

Manuscript received March 24, 2000.
Manuscript revised July 12, 2000.

†The author is with the Institute of Engineering Mechanics and Systems, University of Tsukuba, Tsukuba-shi, 305-8573 Japan.
††The authors are with the Graduate School of Engineering, The University of Tokyo, Tokyo, 113-8656 Japan.

*This papar was presented in part at 2000 Symposium of Cryptography and Information Security.

other is a construction of the VSSS for general access structures. Let Γ_{Qual} and Γ_{Forb} be the sets of all subsets of n participants that are qualified and forbidden to reproduce a secret image, respectively. If Γ_{Qual} and Γ_{Forb} are monotone increasing and decreasing, respectively, and form a partition of all subsets of n participants, then we can construct the basis matrices for such access structure by using the basis matrices of the (t, t)-VSSS, where t is a certain constant determined by Γ_{Forb}. The construction uses the cumulative map [12] and is essentially parallel to the construction proposed in [1].

This paper is organized as follows. Section 2 is devoted to definitions of bounded upper semilattices, general access structures and the VSSS for color images. Pixels with colors are treated as elements belonging to a bounded upper semilattice of colors. In Sect. 3 a new construction of the (n, n)-VSSS for color images is proposed. Several examples are also given. Constructions of the VSSS for the (t, n) access structure and general access structures are described in Sect. 4.

2. Definitions

2.1 A Bounded Upper Semilattice of Colors

A partially ordered set L is called the *upper semilattice* if for any $\mathsf{x}, \mathsf{y} \in L$ the least upper bound of x and y, which is denoted by $\mathsf{x} \sqcup \mathsf{y}$, belongs to L. The operation $\sqcup$ is called the *join* of L. It is known that the idempotent law, the commutative law and the associative law hold with respect to the join. The upper semilattice L is called *bounded* if it contains the least element $\mathsf{0}$ and the greatest element $\mathsf{1}$ satisfying $\mathsf{x} \sqcup \mathsf{0} = \mathsf{x}$ and $\mathsf{x} \sqcup \mathsf{1} = \mathsf{1}$ for any $\mathsf{x} \in L$. Throughout the paper assume that L is an arbitrary bounded upper semilattice with the join $\sqcup$.

For example, the set of eight colors $\mathsf{0}$ (white), C (cyan), M (magenta), Y (yellow), R (red), G (green) B (blue) and $\mathsf{1}$ (black), compose a bounded upper semilattice L_{color} whose Hasse diagram is given in Fig. 1. Figure 1 shows that $\mathsf{Y} \sqcup \mathsf{M} = \mathsf{R}$, $\mathsf{Y} \sqcup \mathsf{C} = \mathsf{G}$, $\mathsf{M} \sqcup \mathsf{C} = \mathsf{B}$ and $\mathsf{R} \sqcup \mathsf{C} = \mathsf{G} \sqcup \mathsf{M} = \mathsf{B} \sqcup \mathsf{Y} = \mathsf{1}$. Physically, $\mathsf{x} \sqcup \mathsf{y}$ means the mixture of two colors x and y. If x is mixed with white, we obtain the same color x. On the other hand, x becomes black when x is mixed with black. If two colors x and y are printed on two respective transparencies, we obtain the color $\mathsf{x} \sqcup \mathsf{y}$ by stacking them in an arbitrary order.

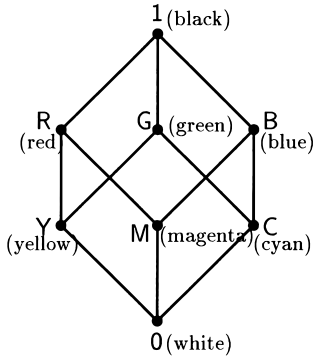

Fig. 1 Hasse diagram of the bounded upper semilattice L_{color}.

It is also important to note that, if L is a bounded upper semilattice, then for an arbitrary integer $q \geq 1$ the Cartesian product L^q is also a bounded upper semilattice. The join $\sqcup_q$ of L^q is defined as

$$(\mathsf{x}_1, \mathsf{x}_2, \ldots, \mathsf{x}_q) \sqcup_q (\mathsf{y}_1, \mathsf{y}_2, \ldots, \mathsf{y}_q) = (\mathsf{x}_1 \sqcup \mathsf{y}_1, \mathsf{x}_2 \sqcup \mathsf{y}_2, \ldots, \mathsf{x}_q \sqcup \mathsf{y}_q), \quad (1)$$

where x_i and y_i belong to L for all $i = 1, 2, \ldots, q$. The least and the greatest elements of L^q are $(\mathsf{0}, \mathsf{0}, \ldots, \mathsf{0})$ and $(\mathsf{1}, \mathsf{1}, \ldots, \mathsf{1})$, respectively.

2.2 General Access Structures

We define access structures for secret sharing scheme according to [1], [13]. Suppose that n is an integer satisfying $n \geq 2$. Let $\mathcal{P} = \{1, 2, \ldots, n\}$ be the set of n participants. Denote by $2^{\mathcal{P}}$ the set of all subsets of $\mathcal{P}$. Throughout the paper the i-th share is distributed to the i-th participant for $i = 1, 2, \ldots, n$. Let Γ_{Qual} and Γ_{Forb} be two disjoint subsets of $2^{\mathcal{P}}$ satisfying $\Gamma_{\mathsf{Qual}} \cup \Gamma_{\mathsf{Forb}} = 2^{\mathcal{P}}$. If $A = \{i_1, i_2, \ldots, i_p\} \subseteq \mathcal{P}$ satisfies $A \in \Gamma_{\mathsf{Qual}}$, then a secret image is reproduced from the i_1-th, the i_2-th, $\ldots$, and the i_p-th shares. Because of this reason members of Γ_{Qual} are called the *qualified sets*. On the other hand, members of Γ_{Forb} are called the *forbidden sets* since no information on the secret image is obtained from the shares corresponding to any $A \in \Gamma_{\mathsf{Forb}}$. The pair $(\Gamma_{\mathsf{Qual}}, \Gamma_{\mathsf{Forb}})$ is called an access structure. Suppose that all participants know the access structure.

We assume that Γ_{Qual} is monotone increasing and Γ_{Forb} is monotone decreasing. That is, Γ_{Qual} and Γ_{Forb} are supposed to satisfy that any $B \in 2^{\mathcal{P}}$ including $A \in \Gamma_{\mathsf{Qual}}$ belongs to Γ_{Qual} and any $B \in 2^{\mathcal{P}}$ included in $A \in \Gamma_{\mathsf{Forb}}$ belongs to Γ_{Forb}, respectively. Denote Γ^*_{Qual} and Γ^*_{Forb} by the *minimal qualified sets* and the *maximal forbidden sets* defined as

$$\Gamma^*_{\mathsf{Qual}} = \{A \in \Gamma_{\mathsf{Qual}} : B \notin \Gamma_{\mathsf{Qual}} \text{ for any } B \subset A\}, \quad (2)$$

$$\Gamma^*_{\mathsf{Forb}} = \{A \in \Gamma_{\mathsf{Forb}} : A \cup \{i\} \notin \Gamma_{\mathsf{Forb}} \text{ for any } i \in \mathcal{P} \backslash A\}, \quad (3)$$

respectively. If Γ_{Qual} satisfies

$$\Gamma^*_{\mathsf{Qual}} = \{A \in 2^{\mathcal{P}} : |A| = t\}$$

for some $2 \leq t \leq n$, then $(\Gamma_{\mathsf{Qual}}, \Gamma_{\mathsf{Forb}})$ is called the (t, n)-*threshold access structure*, where $|A|$ denotes the cardinality of A. Obviously, in the (t, n)-threshold access structure Γ^*_{Forb} can be expressed as

$$\Gamma^*_{\mathsf{Forb}} = \{A \in 2^{\mathcal{P}} : |A| = t - 1\}.$$

2.3 The Lattice-Based $(\Gamma_{\mathsf{Qual}}, \Gamma_{\mathsf{Forb}})$-Visual Secret Sharing Scheme

A visual secret sharing scheme defined over a bounded lattice is firstly proposed by [8] for the (t, n)-threshold access structure. We extend the definition given in [8] for general access structures.

Let L be a bounded upper semilattice of colors. Define $\mathcal{C} = \{\mathsf{c}_1, \mathsf{c}_2, \ldots, \mathsf{c}_K\}$ as a subset of L that a secret image contains. The subset $\mathcal{C}$ itself is not necessarily an upper bounded semilattice. Let $\mathcal{P} = \{1, 2, \ldots, n\}$ be a set of n participants. For an integer $q \geq 1$ we express an element of $(L^q)^n$ in the form of $n \times q$ matrix S, where

$$S = \begin{bmatrix} \mathsf{s}_{11} & \mathsf{s}_{12} & \cdots & \mathsf{s}_{1q} \\ \mathsf{s}_{21} & \mathsf{s}_{22} & \cdots & \mathsf{s}_{2q} \\ \vdots & \vdots & \ddots & \vdots \\ \mathsf{s}_{n1} & \mathsf{s}_{n2} & \cdots & \mathsf{s}_{nq} \end{bmatrix} \tag{4}$$

and $\mathsf{s}_{ij} \in L$ for all $i = 1, 2, \ldots, n$ and $j = 1, 2, \ldots, q$. For $1 \leq p \leq n$ and $A = \{i_1, i_2, \ldots, i_p\} \subseteq \mathcal{P}$ define $S[A]$ as the $p \times q$ matrix

$$S[A] = \begin{bmatrix} \mathsf{s}_{i_1 1} & \mathsf{s}_{i_1 2} & \cdots & \mathsf{s}_{i_1 q} \\ \mathsf{s}_{i_2 1} & \mathsf{s}_{i_2 2} & \cdots & \mathsf{s}_{i_2 q} \\ \vdots & \vdots & \ddots & \vdots \\ \mathsf{s}_{i_p 1} & \mathsf{s}_{i_p 2} & \cdots & \mathsf{s}_{i_p q} \end{bmatrix}, \tag{5}$$

which is obtained by picking up the i_1-th, the i_2-th, ..., and the i_p-th rows of S. For such p and A define the mapping $h : (L^q)^p \to L^q$ as

$$\begin{aligned} &h(S[A]) \\ &\quad = (\mathsf{s}_{i_1 1}, \mathsf{s}_{i_1 2}, \ldots, \mathsf{s}_{i_1 q}) \sqcup_q (\mathsf{s}_{i_2 1}, \mathsf{s}_{i_2 2}, \ldots, \mathsf{s}_{i_2 q}) \\ &\qquad \sqcup_q \cdots \sqcup_q (\mathsf{s}_{i_p 1}, \mathsf{s}_{i_p 2}, \ldots, \mathsf{s}_{i_p q}), \end{aligned} \tag{6}$$

where $\sqcup_q$ denotes the join of L^q defined in (1). That is, for given $S \in (L^q)^n$ and $A \subseteq \mathcal{P}$, $h(S[A])$ means the join of all rows of S specified by A.

The lattice-based visual secret sharing for an access structure $(\Gamma_{\mathsf{Qual}}, \Gamma_{\mathsf{Forb}})$ is defined as follows:

Definition 1: Let $(\Gamma_{\mathsf{Qual}}, \Gamma_{\mathsf{Forb}})$ be an access structure of n participants. Let L be a bounded upper semilattice of colors and $\mathcal{C} = \{\mathsf{c}_1, \mathsf{c}_2, \ldots, \mathsf{c}_K\}$ a subset of L. If there exists $q \geq 1$ and $\mathcal{X}_{\mathsf{c}_k} \subset (L^q)^n$, $1 \leq k \leq K$, satisfying the following two properties, the collection of $\mathcal{X}_{\mathsf{c}_k}$, $1 \leq k \leq K$, is called the lattice-based $(\Gamma_{\mathsf{Qual}}, \Gamma_{\mathsf{Forb}})$-visual secret sharing scheme (the lattice-based $(\Gamma_{\mathsf{Qual}}, \Gamma_{\mathsf{Forb}})$-VSSS) with $\mathcal{C}$.

(i) For each $k = 1, 2, \ldots, K$, if $A \in \Gamma^*_{\mathsf{Qual}}$, then for all $S \in \mathcal{X}_{\mathsf{c}_k}$ $h(S[A]) \in L^q$ contains only $\mathsf{1}$s and at least one c_k, where Γ^*_{Qual} means the minimal qualified sets of Γ_{Qual} defined in (2).

(ii) If $A \in \Gamma^*_{\mathsf{Forb}}$, then $\mathcal{X}_{\mathsf{c}_k}[A]$, $1 \leq k \leq K$, defined as

$$\mathcal{X}_{\mathsf{c}_k}[A] = \{S[A] \,:\, S \in \mathcal{X}_{\mathsf{c}_k}\} \tag{7}$$

are indistinguishable in the sense that they contain the same elements with the same frequencies, where Γ^*_{Forb} means the maximal forbidden sets of Γ_{Forb} defined in (3).

Notice that, if $\mathsf{1} \in \mathcal{C}$, then (i) in Definition 1 means that $h(S[A])$ contains q $\mathsf{1}$s for any $A \in \Gamma_{\mathsf{Qual}}$ and $S \in \mathcal{X}_{\mathsf{1}}$. If (ii) in Definition 1 is satisfied, $\mathcal{X}_{\mathsf{c}_k}[A]$, $1 \leq k \leq K$, become indistinguishable for all $A \in \Gamma_{\mathsf{Forb}}$. In case that $(\Gamma_{\mathsf{Qual}}, \Gamma_{\mathsf{Forb}})$ is the (t, n)-threshold access structure for some $2 \leq t \leq n$, the lattice-based $(\Gamma_{\mathsf{Qual}}, \Gamma_{\mathsf{Forb}})$-VSSS is simply called the *the lattice-based* (t, n)*-VSSS*.

When a secret image is encrypted into n shares, for each pixel of the secret image we choose $S \in \mathcal{X}_{\mathsf{c}_k}$ randomly with the uniform distribution according to its color c_k. The i-th row of S is used for generating q pixels of the i-th share corresponding to the original pixel. The q pixels are called the *subpixels* of the i-th share. This step is repeated until all pixels in the secret image are encrypted. As a result, we obtain n shares that are q times larger than the secret image.

For any $A \in \Gamma_{\mathsf{Qual}}$ the secret image is reproduced as follows. All should be done are finding $A^* \subseteq A$ satisfying $A^* \in \Gamma^*_{\mathsf{Qual}}$ arbitrarily and stacking the $|A^*|$ shares indicated by A^*. Here, we use the assumption that all participants know the access structure. Note that the $|A^*|$ shares can be stacked in an arbitrary order since the join of L^q satisfies the commutative law and the associative law. Property (i) in Definition 1 guarantees that for each pixel in the secret image we can find at least one subpixel with the same color in its corresponding stacked q subpixels. On the other hand, for any $A \in \Gamma_{\mathsf{Forb}}$ property (ii) in Definition 1 guarantees that no information on colors of pixels of the secret image is obtained from the $|A|$ shares indicated by A. Figure 3 in [8] gives examples of a secret image, two shares and a reproduced image in the lattice-based $(2, 2)$-VSSS.

In the following sections we construct $\mathcal{X}_{\mathsf{c}_k}$ from all permutations of columns of an $n \times q$ matrix X_{c_k} for $k = 1, 2, \ldots, K$. Such X_{c_k} is called the *basis matrix* of $\mathcal{X}_{\mathsf{c}_k}$. If X_{c_k}, $1 \leq k \leq K$, are the basis matrices of $\mathcal{X}_{\mathsf{c}_k}$, then (ii) in Definition 1 can be replaced by

$$\mathcal{X}_{\mathsf{c}_1}[A] = \mathcal{X}_{\mathsf{c}_2}[A] = \cdots = \mathcal{X}_{\mathsf{c}_K}[A] \tag{8}$$

for any $A \in \Gamma^*_{\mathsf{Forb}}$. Here, we consider that $|\mathcal{X}_{\mathsf{c}_k}|$ always equals $q!$ even if more than two columns of its basis matrix X_{c_k} are the same.

Brightness of the reproduced image can be evaluated by the parameter α defined as

$$\alpha = \min_{A \in \Gamma^*_{\mathsf{Qual}}} \min_{\mathsf{c}_k \in \mathcal{C}, \mathsf{c}_k \neq \mathsf{1}} \frac{N_k(A)}{q}, \tag{9}$$

where $N_k(A)$ means the number of components in $h(X_{\mathsf{c}_k}[A])$ equal to c_k. The number of subpixels q is

also an important parameter on the performance of the lattice-based $(\Gamma_{\mathsf{Qual}}, \Gamma_{\mathsf{Forb}})$-VSSS since q determines the size of n shares. However, in this paper we try to maximize α instead of minimizing q. It is not q but α that is crucial to the lattice-based $(\Gamma_{\mathsf{Qual}}, \Gamma_{\mathsf{Forb}})$-VSSS if we use pixels of small size or apply a technique proposed in [6] for reducing the size of subpixels by random selection of columns.

3. Construction of the Lattice-Based (n, n)-VSSS

3.1 The Column-Permuting Matrices and Their Polynomial Representations

In this section we construct the basis matrices of the lattice-based (n, n)-VSSS by concatenating matrices belonging to a certain class. Fix a bounded upper semilattice L. We use the convention that all symbols expressed in the sans serif font are elements in L. A matrix $M_n(\mathsf{a}_1, \mathsf{a}_2, \ldots, \mathsf{a}_n)$ is called the *n-th order column-permuting matrix* if $M_n(\mathsf{a}_1, \mathsf{a}_2, \ldots, \mathsf{a}_n)$ consists of all permutations of a vector ${}^t[\mathsf{a}_1, \mathsf{a}_2, \ldots, \mathsf{a}_n]$. Then, $M_n(\mathsf{a}_1, \mathsf{a}_2, \ldots, \mathsf{a}_n)$ has n rows and $n!$ columns. For example, $M_3(\mathsf{a}, \mathsf{b}, \mathsf{c})$ is the 3×6 matrix expressed as

$$M_3(\mathsf{a}, \mathsf{b}, \mathsf{c}) = \begin{bmatrix} \mathsf{a} & \mathsf{b} & \mathsf{b} & \mathsf{c} & \mathsf{c} & \mathsf{a} \\ \mathsf{b} & \mathsf{a} & \mathsf{c} & \mathsf{b} & \mathsf{a} & \mathsf{c} \\ \mathsf{c} & \mathsf{c} & \mathsf{a} & \mathsf{a} & \mathsf{b} & \mathsf{b} \end{bmatrix}. \tag{10}$$

Note that the join of all rows of $M_n(\mathsf{a}_1, \mathsf{a}_2, \ldots, \mathsf{a}_n)$ is composed by $n!$ $(\mathsf{a}_1 \sqcup \mathsf{a}_2 \sqcup \cdots \sqcup \mathsf{a}_n)$s.

There are generally $(n!)!$ ways to express $M_n(\mathsf{a}_1, \mathsf{a}_2, \ldots, \mathsf{a}_n)$ in a form of $n \times n!$ matrix. However, we regard two column-permuting matrices as equal if one matrix can be transformed into the other only by an adequate permutation of its columns. In other words, $M_n(\mathsf{a}_1, \mathsf{a}_2, \ldots, \mathsf{a}_n)$ is supposed to be equal to $M_n(\mathsf{a}'_1, \mathsf{a}'_2, \ldots, \mathsf{a}'_n)$ if and only if $\{\mathsf{a}_1, \mathsf{a}_2, \ldots, \mathsf{a}_n\} = \{\mathsf{a}'_1, \mathsf{a}'_2, \ldots, \mathsf{a}'_n\}$ is satisfied. We identify $M_n(\mathsf{a}_1, \mathsf{a}_2, \ldots, \mathsf{a}_n)$ with a monomial $a_1 a_2 \cdots a_n$, where a_i is the symbol corresponding to a_i used in the monomial. For example, the monomial expressions of $M_3(\mathsf{a}, \mathsf{b}, \mathsf{c})$ and $M_3(\mathsf{a}, \mathsf{a}, \mathsf{b})$ are abc and a^2b, respectively, where a, b and c are the symbols corresponding to a, b and c, respectively. Clearly, the degree of monomials expressing n-th order column-permuting matrices are always equal to n.

The concatenation of two column-permuting matrices $M_n(\mathsf{a}_1, \mathsf{a}_2, \ldots, \mathsf{a}_n)$ and $M_n(\mathsf{a}'_1, \mathsf{a}'_2, \ldots, \mathsf{a}'_n)$ is denoted by $M_n(\mathsf{a}_1, \mathsf{a}_2, \ldots, \mathsf{a}_n) \odot M_n(\mathsf{a}'_1, \mathsf{a}'_2, \ldots, \mathsf{a}'_n)$. Concatenated column-permuting matrices are regarded to be equal if they contain the same matrices in the same frequencies. We identify $M_n(\mathsf{a}_1, \mathsf{a}_2, \ldots, \mathsf{a}_n) \odot M_n(\mathsf{a}'_1, \mathsf{a}'_2, \ldots, \mathsf{a}'_n)$ with a polynomial $a_1 a_2 \cdots a_n + a'_1 a'_2 \cdots a'_n$, where $+$ denotes a formal addition expressing the concatenation. The polynomial $a_1 a_2 \cdots a_n + a'_1 a'_2 \cdots a'_n$ is called the *polynomial representation* of $M_n(\mathsf{a}_1, \mathsf{a}_2, \ldots, \mathsf{a}_n) \odot M_n(\mathsf{a}'_1, \mathsf{a}'_2, \ldots, \mathsf{a}'_n)$. For example, the polynomial expression of $M_3(\mathsf{a}, \mathsf{a}, \mathsf{a}) \odot M_3(\mathsf{b}, \mathsf{b}, \mathsf{c}) \odot M_3(\mathsf{b}, \mathsf{b}, \mathsf{c})$ is $a^3 + 2b^2c$. Notice that there is a one-to-one correspondence between all finite concatenations of n-th order column-permuting matrices and homogeneous polynomials of degree n. The sum of all coefficients in a polynomial expression means the number matrices included in the concatenation.

Now, consider the $(n-1) \times n!$ matrix $M'_n(\mathsf{a}_1, \mathsf{a}_2, \ldots, \mathsf{a}_n)$ obtained by eliminating the n-th row of $M_n(\mathsf{a}_1, \mathsf{a}_2, \ldots, \mathsf{a}_n)$. For example, $M'_3(\mathsf{a}, \mathsf{b}, \mathsf{c})$ means the 2×6 matrix obtained by eliminating the third row of the matrix given in (10). Clearly, (10) implies that $M'_3(\mathsf{a}, \mathsf{b}, \mathsf{c})$ can be expressed as

$$M'_3(\mathsf{a}, \mathsf{b}, \mathsf{c}) = M_2(\mathsf{a}, \mathsf{b}) \odot M_2(\mathsf{b}, \mathsf{c}) \odot M_2(\mathsf{c}, \mathsf{a}). \tag{11}$$

It is interesting to notice that $ab + bc + ca$, the polynomial expression of the right hand side of (11), is obtained by applying a partial differential operator $(\frac{\partial}{\partial a} + \frac{\partial}{\partial b} + \frac{\partial}{\partial c})$ to abc, the monomial expression of $M_3(\mathsf{a}, \mathsf{b}, \mathsf{c})$. More generally, the operation obtaining $M'_n(\mathsf{a}_1, \mathsf{a}_2, \ldots, \mathsf{a}_n)$ from $M_n(\mathsf{a}_1, \mathsf{a}_2, \ldots, \mathsf{a}_n)$ can be described by using the polynomial representation as

$$\psi[a_1 a_2 \cdots a_n] = \sum_{i=1}^{n} \prod_{\substack{j=1 \\ j \neq i}}^{n} a_j,$$

where ψ is the partial differential operator corresponding to $L = \{\mathsf{x}_1, \mathsf{x}_2, \ldots, \mathsf{x}_J\}$ defined as

$$\psi = \frac{\partial}{\partial x_1} + \frac{\partial}{\partial x_2} + \cdots + \frac{\partial}{\partial x_J}, \tag{12}$$

where $x_k, 1 \leq k \leq K$, denote the symbol used in the polynomial expression corresponding to x_k. Notice that $\{a_1, a_2, \ldots, a_n\} \subseteq \{x_1, x_2, \ldots, x_J\}$ from the convention. The same argument is still valid for the concatenated column-permuting matrices. That is, if F is the polynomial representation of a concatenated column-permuting matrix X over L, then the polynomial representation of X' can be expressed as ψF.

3.2 Basis Matrices for the Lattice-Based (n, n)-VSSS

In this subsection we unveil a basic property on the basis matrices of the lattice-based (n, n)-VSSS with $\mathcal{C} = \{\mathsf{c}_1, \mathsf{c}_2, \ldots, \mathsf{c}_K\}$. Let X_{c_k} be the basis matrix of $\mathcal{X}_{\mathsf{c}_k}$ for $k = 1, 2, \ldots, K$. In order to guarantee (8) for the (n, n)-threshold access structure, it is sufficient to choose X_{c_k}, $1 \leq k \leq K$, satisfying

$$X_{\mathsf{c}_1}[A] = X_{\mathsf{c}_2}[A] = \cdots = X_{\mathsf{c}_K}[A] \tag{13}$$

for all $A \in 2^{\mathcal{P}}$ satisfying $|A| = n - 1$, where $\mathcal{P} = \{1, 2, \ldots, n\}$ is a set of n participants. If X_{c_k}, $1 \leq k \leq K$, are concatenated column-permuting matrices, (13) can be expressed as

$$X'_{\mathsf{c}_1} = X'_{\mathsf{c}_2} = \cdots = X'_{\mathsf{c}_K} \tag{14}$$

or

$$\psi F_{\mathsf{c}_1} = \psi F_{\mathsf{c}_2} = \cdots = \psi F_{\mathsf{c}_K} \tag{15}$$

from a property of the column-permuting matrices, where F_{c_k} is the polynomial expressions of X_{c_k} for $k = 1, 2, \ldots, K$. We call K homogeneous polynomials F_{c_k}, $1 \le k \le K$, the *basis polynomials* if their corresponding concatenated column-permuting matrices are the basis matrices of the lattice-based (n, n)-VSSS with $\mathcal{C} = \{\mathsf{c}_1, \mathsf{c}_2, \ldots, \mathsf{c}_K\}$. It is obvious that the basis polynomials must be homogeneous polynomials of degree n satisfying (15).

There is one more requirement that F_{c_k}, $1 \le k \le K$, satisfying (15) can be regarded as the basis polynomials. Notice that, if F_{c_k} contains a term $a_1 a_2 \cdots a_n$, then the term results in the color $\mathsf{a}_1 \sqcup \mathsf{a}_2 \sqcup \cdots \sqcup \mathsf{a}_n \in L$ in a reproduced image. Let z be the symbol corresponding to the greatest element $\mathsf{1} \in L$ and assume that $\mathsf{1} \notin \mathcal{C}$. Since $h(X_{\mathsf{c}_k}[\mathcal{P}])$ contains only 1s and at least one c_k, all terms of F_{c_k} result in either c_k or $\mathsf{1}$ in the reproduced image. Throughout the paper we focus on the case that the terms resulting in $\mathsf{1}$ contain at least one z. Since such terms vanish if we substitute $z = 0$ into F_{c_k}, we can consider that F_{c_k} satisfies

$$F_{\mathsf{c}_k}|_{z=0} = N_k c_k \tag{16}$$

for each $k = 1, 2, \ldots, K$, where c_k is the symbol corresponding to c_k and N_k, $1 \le k \le K$, are positive integers. Notice that c_k in (16) is equal to $a_1 a_2 \cdots a_n$ if c_k is represented as $\mathsf{c}_k = \mathsf{a}_1 \sqcup \mathsf{a}_2 \sqcup \cdots \sqcup \mathsf{a}_n$.

Summarizing, we have the following theorem:

Theorem 1: Let $\mathcal{C} = \{\mathsf{c}_1, \mathsf{c}_2, \ldots, \mathsf{c}_K\}$, $\mathsf{1} \notin \mathcal{C}$ be a subset of a bounded upper semilattice L. Let F_{c_k}, $1 \le k \le K$, be K homogeneous polynomials of degree n. If F_{c_k}, $1 \le k \le K$, satisfy the following two conditions, they can be regarded as the basis polynomials of the lattice-based (n, n)-VSSS with a set of colors $\mathcal{C}$.

(a) $\psi F_{\mathsf{c}_1} = \psi F_{\mathsf{c}_2} = \cdots = \psi F_{\mathsf{c}_K}$, where ψ is the partial differential operator defined in (12),
(b) there exist positive integers N_k, $1 \le k \le K$, satisfying $F_{\mathsf{c}_k}|_{z=0} = N_k c_k$ for $k = 1, 2, \ldots, K$, where z and c_k are the symbols corresponding to $\mathsf{1}$ and c_k, respectively.

3.3 Examples

In this section we construct the basis polynomials of the lattice-based (n, n)-VSSS over $\tilde{L}_{\text{color}}$, where $\tilde{L}_{\text{color}}$ is the sublattice of L_{color} composed by $\mathsf{0}, \mathsf{Y}, \mathsf{C}, \mathsf{G}$ and $\mathsf{1}$. Hereafter, let a, y, c, g and z be the symbols in the polynomial representations corresponding to $\mathsf{0}, \mathsf{Y}, \mathsf{C}, \mathsf{G}$ and $\mathsf{1}$. The partial differential operator ψ can be expressed as $\psi = \frac{\partial}{\partial a} + \frac{\partial}{\partial y} + \frac{\partial}{\partial c} + \frac{\partial}{\partial g} + \frac{\partial}{\partial z}$.

Example 1: (*The lattice-based* $(2, 2)$*-VSSS with* $\{\mathsf{Y}, \mathsf{C}, \mathsf{G}\}$) The basis matrices of this case can be written as follows [8]:

$$\begin{aligned} X_{\mathsf{Y}} &= M_2(\mathsf{0}, \mathsf{Y}) \odot M_2(\mathsf{C}, \mathsf{1}), \\ X_{\mathsf{C}} &= M_2(\mathsf{0}, \mathsf{C}) \odot M_2(\mathsf{Y}, \mathsf{1}), \\ X_{\mathsf{G}} &= M_2(\mathsf{Y}, \mathsf{C}) \odot M_2(\mathsf{0}, \mathsf{1}). \end{aligned}$$

Then, the polynomial representations of $X_{\mathsf{Y}}, X_{\mathsf{C}}$ and X_{G} become $F_{\mathsf{Y}} = ay + cz, F_{\mathsf{C}} = ac + yz$ and $F_{\mathsf{G}} = cy + az$, respectively. It is easy to check that $F_{\mathsf{Y}}, F_{\mathsf{C}}$ and F_{G} are homogeneous polynomials of degree 2 satisfying conditions (a) and (b) in Theorem 1. In fact, all of $\psi F_{\mathsf{Y}}, \psi F_{\mathsf{C}}$ and ψF_{G} are equal to $a + c + y + z$. This construction yields $q = 4$ and $\alpha = \frac{1}{2}$. □

Example 2: (*The lattice-based* $(3, 3)$*-VSSS with* $\{\mathsf{Y}, \mathsf{C}\}$) Here, we construct X_{Y} and X_{C} without using G. First, define F_{Y} and F_{C} by

$$\begin{aligned} F_{\mathsf{Y}} &= a^2 y + A_1(a, c, y) z + A_2(a, c, y) z^2, \\ F_{\mathsf{C}} &= a^2 c + B_1(a, c, y) z + B_2(a, c, y) z^2, \end{aligned}$$

where A_1, B_1, A_2 and B_2 are homogeneous polynomials composed by only a, c and y. Since F_{Y} and F_{C} are homogeneous polynomials of degree 3, the degrees of A_1 and B_1 must be 2 and the degrees of A_2 and B_2 must be 1. In addition, notice that $F_{\mathsf{Y}}|_{z=0} = a^2 y$ and $F_{\mathsf{C}}|_{z=0} = a^2 c$ result in $\mathsf{0} \sqcup \mathsf{0} \sqcup \mathsf{Y} = \mathsf{Y}$ and $\mathsf{0} \sqcup \mathsf{0} \sqcup \mathsf{C} = \mathsf{C}$ in a reproduced image, respectively.

By applying ψ to F_{Y} and F_{C} and setting $\psi F_{\mathsf{Y}} = \psi F_{\mathsf{C}}$, it follows that

$$\begin{aligned} &(a^2 + 2ay + A_1) + (\tilde{\psi} A_1 + 2A_2) z + (\tilde{\psi} A_2) z^2 \\ &\quad = (a^2 + 2ac + B_1) + (\tilde{\psi} B_1 + 2B_2) z \\ &\qquad + (\tilde{\psi} B_2) z^2, \end{aligned} \tag{17}$$

where $\tilde{\psi} = \frac{\partial}{\partial a} + \frac{\partial}{\partial y} + \frac{\partial}{\partial c}$. We choose A_1, A_2, B_1 and B_2 in the simplest way that (17) holds as an identity. That is, we choose A_1, A_2, B_1 and B_2 satisfying the following three equations:

$$a^2 + 2ay + A_1 = a^2 + 2ac + B_1, \tag{18}$$

$$\tilde{\psi} A_1 + 2A_2 = \tilde{\psi} B_1 + 2B_2, \tag{19}$$

$$\tilde{\psi} A_2 = \tilde{\psi} B_2. \tag{20}$$

From (18) we have $A_1 = 2ac$ and $B_1 = 2ay$. By using these A_1, B_1 and (19), A_2 and B_2 can be chosen as $A_2 = y$ and $B_2 = c$. Such A_2 and B_2 trivially satisfy (20). Therefore, we obtain

$$\begin{aligned} F_{\mathsf{Y}} &= a^2 y + 2acz + yz^2, \\ F_{\mathsf{C}} &= a^2 c + 2ayz + cz^2, \end{aligned}$$

which can be regarded as the basis polynomials corresponding to the basis matrices X_{Y} and X_{C} with

$q = 4 \times 3! = 24$ and $\alpha = 1/4$. □

Example 3: (*The lattice-based* $(3,3)$*-VSSS with* $\{\mathsf{Y}, \mathsf{C}, \mathsf{G}\}$) We can construct the basis matrices X_{Y}, X_{C} and X_{G} similarly to Example 2. The basis polynomials $F_{\mathsf{Y}}, F_{\mathsf{C}}$ and F_{G} satisfying $F_{\mathsf{Y}}|_{z=0} = a^2y, F_{\mathsf{C}}|_{z=0} = a^2c$ and $F_{\mathsf{G}}|_{z=0} = acy$ are expressed as

$$\begin{aligned} F_{\mathsf{Y}} &= a^2y + (2ac + cy)z + (a + y)z^2, \\ F_{\mathsf{C}} &= a^2c + (2ay + cy)z + (a + c)z^2, \\ F_{\mathsf{G}} &= acy + (a^2 + ac + ay)z + (c + y)z^2. \end{aligned}$$

In this example, $q = 6 \times 3! = 36$ and $\alpha = 1/6$. □

3.4 Basis Polynomials for the Lattice-Based (n, n)-VSSS with K Colors

This subsection is devoted to a construction of the lattice-based (n, n)-VSSS with a set of colors $\mathcal{C} = \{\mathsf{c}_1, \mathsf{c}_2, \ldots, \mathsf{c}_K\}$. First, we consider the case when c_k, $1 \le k \le K$, satisfy

$$\mathsf{c}_k = \mathsf{c}_{k,1} \sqcup \mathsf{c}_{k,2} \sqcup \cdots \sqcup \mathsf{c}_{k,n}, \tag{21}$$

where $\mathsf{c}_{k,i}$, $1 \le k \le K, 1 \le i \le n$, are distinct elements in L not equal to the greatest element $\mathsf{1} \in L$.

Let c_k and $c_{k,i}$ be the symbols corresponding to c_k and $\mathsf{c}_{k,i}$ in the polynomial expressions, respectively. For each $k = 1, 2, \ldots, K$ and $p = 0, 1, \ldots, n$ define $s_{k,p}$ by

$$s_{k,p} = \begin{cases} \displaystyle\sum_{\substack{\{i_1, i_2, \ldots, i_p\} \subseteq \mathcal{P} \\ i_1 < i_2 < \cdots < i_p}} c_{k,i_1} c_{k,i_2} \cdots c_{k,i_p}, & \text{if } 1 \le p \le n, \\ 1, & \text{if } p = 0. \end{cases} \tag{22}$$

It is clear that $s_{k,1} = c_{k,1} + c_{k,2} + \cdots + c_{k,n}$ and $s_{k,n} = c_{k,1}c_{k,2} \cdots c_{k,n} = c_k$.

The basis polynomials F_{c_k}, $1 \le k \le K$, can be found in the following theorem.

Theorem 2: In the lattice-based (n, n)-VSSS with $\mathcal{C} = \{\mathsf{c}_1, \mathsf{c}_2, \ldots, \mathsf{c}_K\}$ satisfying (21), the basis polynomial F_{c_k} can be expressed as

$$F_{\mathsf{c}_k} = \sum_{\substack{i=0 \\ i:\text{even}}}^{n-1} s_{k,n-i} z^i + \sum_{\substack{i=1 \\ i:\text{odd}}}^{n-1} \sum_{\substack{j=1 \\ j \ne k}}^{K} s_{j,n-i} z^i \tag{23}$$

for all $k = 1, 2, \ldots, K$.

Proof: Since $F_{\mathsf{c}_k}|_{z=0} = s_{k,n} = c_k$ is clear from (23), we only prove that F_{c_k}, $1 \le k \le K$, in (23) satisfy condition (a) in Theorem 1. For each $k = 1, 2, \ldots, K$ ψF_{c_k} is evaluated in the following way:

$$\begin{aligned} &\psi F_{\mathsf{c}_k} \\ &\overset{1)}{=} \left(\sum_{l=1}^{n} \frac{\partial}{\partial c_{k,l}} + \frac{\partial}{\partial z} \right) F_{\mathsf{c}_k} \\ &= \sum_{\substack{i=0 \\ i:\text{even}}}^{n-1} \left(\sum_{l=1}^{n} \frac{\partial}{\partial c_{k,l}} + \frac{\partial}{\partial z} \right) s_{k,n-i} z^i \\ &\quad + \sum_{\substack{i=1 \\ i:\text{odd}}}^{n-1} \sum_{\substack{j=1 \\ j \ne k}}^{K} \left(\sum_{l=1}^{n} \frac{\partial}{\partial c_{j,l}} + \frac{\partial}{\partial z} \right) s_{j,n-i} z^i \\ &\overset{2)}{=} \sum_{\substack{i=0 \\ i:\text{even}}}^{n-1} (i+1) s_{k,n-i-1} z^i + \sum_{\substack{i=2 \\ i:\text{even}}}^{n-1} i s_{k,n-i} z^{i-1} \\ &\quad + \sum_{\substack{i=1 \\ i:\text{odd}}}^{n-1} \sum_{\substack{j=1 \\ j \ne k}}^{K} (i+1) s_{j,n-i-1} z^i + \sum_{\substack{i=1 \\ i:\text{odd}}}^{n-1} \sum_{\substack{j=1 \\ j \ne k}}^{K} i s_{j,n-i} z^{i-1} \\ &= \sum_{\substack{i=1 \\ i:\text{odd}}}^{n} i s_{k,n-i} z^{i-1} + \sum_{\substack{i=2 \\ i:\text{even}}}^{n-1} i s_{k,n-i} z^{i-1} \\ &\quad + \sum_{\substack{i=2 \\ i:\text{even}}}^{n} \sum_{\substack{j=1 \\ j \ne k}}^{K} i s_{j,n-i} z^{i-1} + \sum_{\substack{i=1 \\ i:\text{odd}}}^{n-1} \sum_{\substack{j=1 \\ j \ne k}}^{K} i s_{j,n-i} z^{i-1} \\ &= \sum_{i=1}^{n-1} \sum_{j=1}^{K} i s_{j,n-i} z^{i-1} \\ &\quad + \begin{cases} n z^{n-1}, & \text{if } n \text{ is odd}, \\ (K-1) n z^{n-1}, & \text{otherwise}, \end{cases} \end{aligned} \tag{24}$$

where the marked equalities follow since
1): F_{c_k} contains only z and $c_{k,i}$, $i = 1, 2, \ldots, n$,
2): for all $i = 0, 1, \ldots, n-1$ and $j = 1, 2, \ldots, K$

$$\sum_{l=1}^{n} \frac{\partial}{\partial c_{j,l}} s_{j,n-i} = (i+1) s_{j,n-i-1}$$

holds from the definition of $s_{j,p}$ in (22).

Since (24) no longer depends on k, $\psi F_{\mathsf{c}_1} = \psi F_{\mathsf{c}_2} = \cdots = \psi F_{\mathsf{c}_K}$ is established. □

By using the formula

$$\sum_{\substack{i=0 \\ i:\text{even}}}^{n} \binom{n}{i} = \sum_{\substack{i=1 \\ i:\text{odd}}}^{n} \binom{n}{i} = 2^{n-1} \quad \text{for all } n \ge 1,$$

it is not hard to verify that the basis matrices corresponding to F_{c_k}, $1 \le k \le K$, in (23) satisfy $\alpha = 1/(K \cdot 2^{n-1} - K + 1)$ if n is odd and $\alpha = 1/(K \cdot 2^{n-1} - 1)$ otherwise.

For constructing the lattice-based (n, n)-VSSS with $\mathcal{C} = \{\mathsf{c}_1, \mathsf{c}_2, \ldots, \mathsf{c}_K\}$ satisfying $\mathsf{0} \notin \mathcal{C}$ and $\mathsf{1} \notin \mathcal{C}$, it is often convenient to find the basis polynomials F_{c_k}, $1 \le k \le K$, satisfying

$$F_{\mathsf{c}_k}|_{z=0} = a^{n-1} c_k \quad \text{for all } k = 1, 2, \ldots, K, \tag{25}$$

where a and c_k denote the symbols corresponding to $\mathsf{0}$ and c_k, respectively. The following theorem describes such basis polynomials yielding $\alpha = 1/(K \cdot 2^{n-2})$.

Theorem 3: The basis polynomials of the lattice-based (n, n)-VSSS with $\mathcal{C} = \{\mathsf{c}_1, \mathsf{c}_2, \ldots, \mathsf{c}_K\}$ satisfying

$\mathsf{0} \notin \mathcal{C}, \mathsf{1} \notin \mathcal{C}$ and (25) can be written as

$$F_{\mathsf{c}_k} = \sum_{\substack{i=0 \\ i:\text{even}}}^{n-1} \binom{n-1}{i} a^{n-1-i} c_k z^i + \sum_{\substack{i=1 \\ i:\text{odd}}}^{n-1} \sum_{\substack{j=1 \\ j \neq k}}^{K} \binom{n-1}{i} a^{n-1-i} c_j z^i \quad (26)$$

for all $k = 1, 2, \ldots, K$.

Proof: Since F_{c_k} in (26) clearly satisfy (25), we have only to prove that ψF_{c_k}, $1 \le k \le K$, do not depend on k. However, by using techniques used in the proof of Theorem 2, it is not hard to verify that $\psi F_{\mathsf{c}_k} = (\frac{\partial}{\partial a} + \frac{\partial}{\partial c_k} + \frac{\partial}{\partial z}) F_{\mathsf{c}_k}$ is independent of k. □

If the basis polynomials F_{c_k}, $1 \le k \le K$, contain a homogeneous polynomial $f \neq 0$ of degree n in common, we can use $F_{\mathsf{c}_k} - f$, $1 \le k \le K$, as the new basis polynomials that require less subpixels than F_{c_k}. For example, if F_{c_k}, $1 \le k \le K$, contain z^n in common, we can drop z^n from F_{c_k}, $1 \le k \le K$, without violating conditions (a) and (b) in Theorem 1. The basis polynomials F_{c_k}, $1 \le k \le K$, are called *minimal* if such f does not exist. As is easily checked, the basis polynomials given in Examples 1–3 and Theorems 2–3 are minimal. The following theorem claims that minimal basis polynomials are unique in a certain sense.

Theorem 4: Let $\mathcal{C} = \{\mathsf{c}_1, \mathsf{c}_2, \ldots, \mathsf{c}_K\} \subseteq L$ be a set of colors and F_{c_k}, $1 \le k \le K$, be the minimal basis polynomials of the lattice-based (n, n)-VSSS satisfying

$$F_{\mathsf{c}_k}|_{z=0} = N_k c_k, \quad (27)$$

where for $k = 1, 2, \ldots, K$ N_k is a positive integer and c_k denotes the symbol corresponding to c_k. Let $L' = \{\mathsf{c}'_1, \mathsf{c}'_2, \ldots, \mathsf{c}'_I, \mathsf{1}\}$ be a subset of L whose corresponding symbols $\{c'_1, c'_2, \ldots, c'_I, z\}$ are contained in at least one F_{c_k}. Then, F_{c_k}, $1 \le k \le K$, are unique in the sense that they satisfy

$$\varphi F_{\mathsf{c}_1} = \varphi F_{\mathsf{c}_2} = \cdots = \varphi F_{\mathsf{c}_K} \quad (28)$$

and (27), where φ is the partial differential operator defined as

$$\varphi = \frac{\partial}{\partial c'_1} + \frac{\partial}{\partial c'_2} + \cdots + \frac{\partial}{\partial c'_I} + \frac{\partial}{\partial z}. \quad (29)$$

Proof: Suppose that there exist another basis polynomials $\tilde{F}_{\mathsf{c}_k}$, $1 \le k \le K$, satisfying

$$\varphi \tilde{F}_{\mathsf{c}_1} = \varphi \tilde{F}_{\mathsf{c}_2} = \cdots = \varphi \tilde{F}_{\mathsf{c}_K} \quad (30)$$

and $\tilde{F}_{\mathsf{c}_k}|_{z=0} = N_k c_k$ for all $k = 1, 2, \ldots, K$. Assume that $\tilde{F}_{\mathsf{c}_k}$, $1 \le k \le K$, are minimal. From (28) and (30) we have

$$\varphi f_{\mathsf{c}_1} = \varphi f_{\mathsf{c}_2} = \cdots = \varphi f_{\mathsf{c}_K}, \quad (31)$$

where f_{c_k} is defined as $f_{\mathsf{c}_k} = \tilde{F}_{\mathsf{c}_k} - F_{\mathsf{c}_k}$ for all $k = 1, 2, \ldots, K$. Notice that $f_{\mathsf{c}_k}|_{z=0} = \tilde{F}_{\mathsf{c}_k}|_{z=0} - F_{\mathsf{c}_k}|_{z=0} = N_k c_k - N_k c_k = 0$ for all $k = 1, 2, \ldots, K$.

Hereafter, we prove that $f_{\mathsf{c}_1} = f_{\mathsf{c}_2} = \cdots = f_{\mathsf{c}_K}$. Fix j and k satisfying $1 \le j, k \le I$ arbitrarily and define $g = f_{\mathsf{c}_j} - f_{\mathsf{c}_k}$. Since f_{c_j} and f_{c_k} satisfy $f_{\mathsf{c}_j}|_{z=0} = f_{\mathsf{c}_k}|_{z=0} = 0$, g becomes a homogeneous polynomial of degree n expressed as $g = g_1 z + g_2 z^2 + \cdots + g_{n-1} z^{n-1}$, where for each $j = 1, 2, \ldots, n-1$ g_j is a homogenous polynomial of c'_i, $1 \le i \le I$, of degree $n-j$. By noticing that g is a solution to $\varphi g = 0$, it follows that

$$g_1 + (\tilde{\varphi} g_1 + 2g_2) z + (\tilde{\varphi} g_2 + 3g_3) z^2 + \cdots + (\tilde{\varphi} g_{n-2} + (n-1) g_{n-1}) z^{n-2} + (\tilde{\varphi} g_{n-1}) z^{n-1} = 0,$$

where $\tilde{\varphi} = \sum_{i=1}^{I} \frac{\partial}{\partial c'_i}$, which implies $g_1 = g_2 = \cdots = g_{n-1} = 0$ and therefore $g = 0$. This fact leads to the existence of a homogeneous polynomial f of degree n satisfying $f_{\mathsf{c}_1} = f_{\mathsf{c}_2} = \cdots = f_{\mathsf{c}_K} = f$. Such f must satisfy $f = 0$ since F_{c_k}, $1 \le k \le K$, are minimal and $\tilde{F}_{\mathsf{c}_k}$, $1 \le k \le K$, are assumed to be minimal. That is, if such f not equal to 0 exists, the definition of f_{c_k} implies that $\tilde{F}_{\mathsf{c}_k} = F_{\mathsf{c}_k} + f$ holds for all $k = 1, 2, \ldots, K$, which conflicts with the assumption that $\tilde{F}_{\mathsf{c}_k}$, $1 \le k \le K$, are minimal. This completes the proof of this theorem. □

Example 4: (*The lattice-based* $(3,3)$*-VSSS with* $\{\mathsf{R}, \mathsf{G}, \mathsf{B}\}$) Here, we demonstrate how Theorem 2 can be applied to construction of the lattice-based $(3,3)$-VSSS with $\{\mathsf{R}, \mathsf{G}, \mathsf{B}\}$ over L_{color}. We construct the basis polynomial $F_{\mathsf{R}}, F_{\mathsf{G}}$ and F_{B} by using only $\mathsf{0}, \mathsf{Y}, \mathsf{M}, \mathsf{C}$ and $\mathsf{1}$. Though we can also construct $F_{\mathsf{R}}, F_{\mathsf{G}}$ and F_{B} in a way similar to Example 2, we construct them by using Theorem 2.

Let a, y, m, c and z be the symbols corresponding to $\mathsf{0}, \mathsf{Y}, \mathsf{M}, \mathsf{C}$ and $\mathsf{1}$, respectively. It is important to notice that basis matrices corresponding to monomials amy, acy and acm result in R, G and B in a reproduced image, respectively. In order to apply Theorem 2 we first *split* the symbols corresponding to $\mathsf{0}, \mathsf{Y}, \mathsf{M}$ and C. That is, we split $\mathsf{0}$ into $\mathsf{0}_1, \mathsf{0}_2$ and $\mathsf{0}_3$, Y into Y_1 and Y_2, M into M_1 and M_2 and C into C_1 and C_2, and express amy, acy and acm as $a_1 m_1 y_1, a_2 c_1 y_2$ and $a_3 c_2 m_2$, respectively. Then, Theorem 2 guarantees that $F_{\mathsf{R}}, F_{\mathsf{G}}$ and F_{B} can be written as follows:

$$F_{\mathsf{R}} = a_1 m_1 y_1 + (a_2 c_1 + a_2 y_2 + c_1 y_2 + a_3 c_2 + a_3 m_2 + c_2 m_2) z + (a_1 + m_1 + y_1) z^2, \quad (32)$$

$$F_{\mathsf{G}} = a_2 c_1 y_2 + (a_1 m_1 + a_1 y_1 + m_1 y_1 + a_3 c_2 + a_3 m_2 + c_2 m_2) z + (a_2 + c_1 + y_2) z^2, \quad (33)$$

$$F_{\mathsf{B}} = a_3 c_2 m_2 + (a_1 m_1 + a_1 y_1 + m_1 y_1 + a_2 c_1 + a_2 y_2 + c_1 y_2) z + (a_3 + c_2 + m_2) z^2. \quad (34)$$

Next, we drop all subscripts of the symbols in (32)–(34) and find all the terms included in $F_{\mathsf{R}}, F_{\mathsf{G}}$ and F_{B} in common. In this example, it is easy to see that $(c + m + y) az$ and az^2 are included in all of (32)–(34).

By eliminating such terms from (32)–(34), we obtain the following *minimal* basis polynomials:

$$F_{\mathsf{R}} = amy + (a+m+y)cz + (m+y)z^2, \quad (35)$$
$$F_{\mathsf{G}} = acy + (a+c+y)mz + (c+y)z^2, \quad (36)$$
$$F_{\mathsf{B}} = acm + (a+c+m)bz + (c+m)z^2. \quad (37)$$

These basis polynomials yield the basis matrices with $q = 6 \times 3! = 36$ and $\alpha = 1/6$. Theorem 4 guarantees that $F_{\mathsf{R}}, F_{\mathsf{G}}$ and F_{B} given in (35)–(37) are unique in the sense that they are composed by $\{a, y, m, c, z\}$ and satisfy $F_{\mathsf{R}}|_{z=0} = amy, F_{\mathsf{G}}|_{z=0} = acy$ and $F_{\mathsf{B}}|_{z=0} = acm$. The uniqueness guarantees that α cannot be larger than $1/6$ in this construction. □

Remark: We can regard the requirement $F_{\mathsf{R}}|_{z=0} = amy, F_{\mathsf{G}}|_{z=0} = acy$ and $F_{\mathsf{B}}|_{z=0} = acm$ as an initial condition of the partial differential equation $\psi F_{\mathsf{R}} = \psi F_{\mathsf{G}} = \psi F_{\mathsf{B}}$ and the basis polynomials in (35)–(37) as the minimal solution. On the other hand, Theorem 3 guarantees that, under another initial condition $F_{\mathsf{R}}|_{z=0} = a^2 r, F_{\mathsf{G}}|_{z=0} = a^2 g$ and $F_{\mathsf{B}}|_{z=0} = a^2 b$, the minimal solution are expressed as

$$F_{\mathsf{R}} = a^2 r + 2(b+g)az + rz^2, \quad (38)$$
$$F_{\mathsf{G}} = a^2 g + 2(b+r)az + gz^2, \quad (39)$$
$$F_{\mathsf{B}} = a^2 b + 2(g+r)az + bz^2, \quad (40)$$

where r, g and b denote the symbols corresponding to R, G and B, respectively. Since the basis polynomials in (38)–(40) also yield $\alpha = 1/6$ and $q = 36$, we cannot mention which of the two initial conditions is better for the lattice-based $(3,3)$-VSSS with $\{\mathsf{R}, \mathsf{G}, \mathsf{B}\}$ from the viewpoint of brightness of the reproduced image. However, difference of initial conditions appears in construction of the lattice-based $(3,3)$-VSSS with $\{\mathsf{Y}, \mathsf{M}, \mathsf{C}, \mathsf{R}, \mathsf{G}, \mathsf{B}\}$. If we set the initial conditions as

$$F_{\mathsf{Y}}|_{z=0} = a^2 y, F_{\mathsf{M}}|_{z=0} = a^2 m, F_{\mathsf{Y}}|_{z=0} = a^2 c,$$
$$F_{\mathsf{R}}|_{z=0} = amy, F_{\mathsf{G}}|_{z=0} = acy, F_{\mathsf{B}}|_{z=0} = acm, \quad (41)$$

then we obtain the following minimal basis polynomials with $\alpha = 1/10$:

$$\begin{aligned}
F_{\mathsf{Y}} &= a^2y+(2ac+2am+cm+cy+my)z+(a+y)z^2,\\
F_{\mathsf{M}} &= a^2m+(2ac+2ay+cm+cy+my)z+(a+m)z^2,\\
F_{\mathsf{C}} &= a^2c+(2am+2ay+cm+cy+my)z+(a+c)z^2,\\
F_{\mathsf{R}} &= amy+(a^2+2ac+am+ay+cm+cy)z+(m+y)z^2,\\
F_{\mathsf{G}} &= acy+(a^2+ac+2am+ay+cm+my)z+(c+y)z^2,\\
F_{\mathsf{B}} &= acm+(a^2+ac+am+2ay+cy+my)z+(c+m)z^2.
\end{aligned}$$

On the other hand, if we use

$$F_{\mathsf{Y}}|_{z=0} = a^2 y, F_{\mathsf{M}}|_{z=0} = a^2 m, F_{\mathsf{Y}}|_{z=0} = a^2 c,$$
$$F_{\mathsf{R}}|_{z=0} = a^2 r, F_{\mathsf{G}}|_{z=0} = a^2 g, F_{\mathsf{B}}|_{z=0} = a^2 b \quad (42)$$

instead of (41), we obtain the basis polynomials with $\alpha = 1/12$ from Theorem 3 (Notice that they are minimal under the initial condition (42)). Generally, in the construction of the lattice-based (n,n)-VSSS with $\mathcal{C} = \{\mathsf{c}_1, \mathsf{c}_2, \ldots, \mathsf{c}_K\}$ over L, if K is large, it will be better to use small number of elements in L for representing all of c_k. For constructing the basis matrices with the largest α, we need to search for the initial conditions yielding the maximal α. The assumption that L is a bounded upper semilattice provides various ways of giving initial conditions and enables to find the optimal initial condition yielding the maximal α.

3.5 Discussion

Here, we show that the basis matrices obtained from Theorem 3 lead to the basis matrices of the lattice-based (n,n)-VSSS given in Sect. 4 of [8]. Note that, however, this fact does not mean the optimality of the basis matrices in [8].

Consider the lattice-based $(3,3)$-VSSS with $\{\mathsf{R}, \mathsf{G}, \mathsf{B}\}$ whose basis polynomials are given in (38)–(40) as an example. By using the definitions of the column-permuting matrix and its polynomial representation, it is easy to check that the basis matrix X_{R} corresponding to F_{R} can be expressed as follows:

$$X_{\mathsf{R}} = \tilde{X}_{\mathsf{R}} \odot \tilde{X}_{\mathsf{R}},$$

where

$$\tilde{X}_{\mathsf{R}} = \begin{bmatrix}
\mathsf{R}\,0\,0 & \mathsf{G}\,0\,\mathsf{G}\,0\,1\,1 & \mathsf{B}\,0\,\mathsf{B}\,0\,1\,1 & \mathsf{R}\,1\,1\\
0\,\mathsf{R}\,0 & 0\,\mathsf{G}\,1\,1\,\mathsf{G}\,0 & 0\,\mathsf{B}\,1\,1\,\mathsf{B}\,0 & 1\,\mathsf{R}\,1\\
0\,0\,\mathsf{R} & 1\,1\,0\,\mathsf{G}\,0\,\mathsf{G} & 1\,1\,0\,\mathsf{B}\,0\,\mathsf{B} & 1\,1\,\mathsf{R}
\end{bmatrix}.$$

Defining $M_n^*(\mathsf{a}_1, \mathsf{a}_2, \ldots, \mathsf{a}_n)$ as the matrix obtained from all the *different* permutations of the vector ${}^t[\mathsf{a}_1, \mathsf{a}_2, \ldots, \mathsf{a}_n]$, $\tilde{X}_{\mathsf{R}}$ is written as

$$\begin{aligned}
\tilde{X}_{\mathsf{R}} = {} & M_3^*(0,0,\mathsf{R}) \odot M_3^*(0,1,\mathsf{G})\\
& \odot M_3^*(0,1,\mathsf{B}) \odot M_3^*(1,1,\mathsf{R}). \quad (43)
\end{aligned}$$

Similarly, X_{G} and X_{B} corresponding to F_{G} and F_{B} can be expressed as $X_{\mathsf{G}} = \tilde{X}_{\mathsf{G}} \odot \tilde{X}_{\mathsf{G}}$ and $X_{\mathsf{B}} = \tilde{X}_{\mathsf{B}} \odot \tilde{X}_{\mathsf{B}}$, respectively, where

$$\begin{aligned}
\tilde{X}_{\mathsf{G}} = {} & M_3^*(0,0,\mathsf{G}) \odot M_3^*(0,1,\mathsf{B})\\
& \odot M_3^*(0,1,\mathsf{R}) \odot M_3^*(1,1,\mathsf{G}), \quad (44)
\end{aligned}$$

$$\begin{aligned}
\tilde{X}_{\mathsf{B}} = {} & M_3^*(0,0,\mathsf{B}) \odot M_3^*(0,1,\mathsf{R})\\
& \odot M_3^*(0,1,\mathsf{G}) \odot M_3^*(1,1,\mathsf{B}). \quad (45)
\end{aligned}$$

Equations (43)–(45) guarantee that $\tilde{X}_{\mathsf{R}}$, $\tilde{X}_{\mathsf{G}}$ and $\tilde{X}_{\mathsf{B}}$ can be used as the basis matrices of the lattice-based $(3,3)$-VSSS with $\{\mathsf{R}, \mathsf{G}, \mathsf{B}\}$ with the same brightness parameter $\alpha = 1/6$ as X_{R}, X_{G} and X_{B}. The number of subpixels required by $\tilde{X}_{\mathsf{R}}$, $\tilde{X}_{\mathsf{G}}$ and $\tilde{X}_{\mathsf{B}}$ is 12, while X_{R}, X_{G} and X_{B} require 24 subpixels.

In order to show that X_{c_k} corresponding to F_{c_k} in Theorem 3 is written in the concatenated form of a single matrix, we make use of the following property:

$$M_n(\underbrace{\mathsf{0},\ldots,\mathsf{0}}_{n-1-i},\mathsf{c}_k,\underbrace{\mathsf{1},\ldots,\mathsf{1}}_{i}) = M_n^*(\underbrace{\mathsf{0},\ldots,\mathsf{0}}_{n-1-i},\mathsf{c}_k,\underbrace{\mathsf{1},\ldots,\mathsf{1}}_{i})^{[(n-1-i)!\cdot i!]}, \quad (46)$$

where for a matrix S $S^{[\alpha]}$ denotes the concatenation of S for α times. Then, it easily follows from (46) that for all $i = 1, 2, \ldots, n-1$ $\binom{n-1}{i} a^{n-1-i} c_k z^i$ corresponding to

$$M_n(\underbrace{\mathsf{0},\ldots,\mathsf{0}}_{n-1-i},\mathsf{c}_k,\underbrace{\mathsf{1},\ldots,\mathsf{1}}_{i})^{[\binom{n-1}{i}]}$$

can be expressed as

$$M_n^*(\underbrace{\mathsf{0},\ldots,\mathsf{0}}_{n-1-i},\mathsf{c}_k,\underbrace{\mathsf{1},\ldots,\mathsf{1}}_{i})^{[(n-1)!]}.$$

This means that for each $k = 1, 2, \ldots, K$ there exists a matrix $\tilde{X}_{\mathsf{c}_k}$ satisfying $X_{\mathsf{c}_k} = \tilde{X}_{\mathsf{c}_k}^{[(n-1)!]}$. We can use $\tilde{X}_{\mathsf{c}_k}$, $1 \le k \le K$, as the basis matrices of the lattice-based (n, n)-VSSS. It is not hard to see that $\tilde{X}_{\mathsf{c}_k}$ contains $K \cdot n \cdot 2^{n-2}$ columns, while X_{c_k} contains $K \cdot n! \cdot 2^{n-2}$ columns. These $\tilde{X}_{\mathsf{c}_k}$, $1 \le k \le K$, are equal to the basis matrices of the lattice-based (n, n)-VSSS in [8].

Note that we can never obtain the basis matrices corresponding to the basis polynomials in Examples 3–4 and Remark (with $\alpha = 1/10$) from the construction given in [8]. In general, the construction proposed in this section uses $M_n(\mathsf{a}_1, \mathsf{a}_2, \ldots, \mathsf{a}_n)$ and therefore requires more subpixels than the construction in [8] using $M_n^*(\mathsf{a}_1, \mathsf{a}_2, \ldots, \mathsf{a}_n)$. Nevertheless, the proposed construction enables us to easily obtain various basis matrices that use properties of colors such as $\mathsf{G} = \mathsf{Y} \sqcup \mathsf{C}$. In addition, it is important to notice that reproduced images can be brighter. For example, in the lattice-based $(3, 3)$-VSSS with $\{\mathsf{Y}, \mathsf{M}, \mathsf{C}, \mathsf{R}, \mathsf{G}, \mathsf{B}\}$, the basis matrices corresponding to F_{Y}–F_{B} satisfying (41) yield $q = 60$ and $\alpha = 1/10$ while the basis matrices constructed via the method in [8], which can be obtained from F_{Y}–F_{B} satisfying (42), yield $q = 36$ and $\alpha = 1/12$.

4. Extensions

4.1 The Lattice-Based (t, n)-VSSS

We can obtain the basis polynomials of the lattice-based (t, n)-VSSS from the basis polynomials of the lattice-based (t, t)-VSSS. Let X_{c_k}, $1 \le k \le K$, be the basis matrices of the lattice-based (t, t)-VSSS with a set of colors $\mathcal{C} = \{\mathsf{c}_1, \mathsf{c}_2, \ldots, \mathsf{c}_K\}$ constructed from column-permuting matrices. All should be done are to replace all contained column-permuting matrices $M_t(\mathsf{a}_1, \mathsf{a}_2, \ldots, \mathsf{a}_t)$ by $M_n(\mathsf{a}_1, \mathsf{a}_2, \ldots, \mathsf{a}_t, \mathsf{1}, \ldots, \mathsf{1})$. For example, by using the basis matrices in Example 1 in Sect. 3.3 we obtain the following basis matrices for the lattice-based $(2, 3)$-VSSS with $\{\mathsf{Y}, \mathsf{C}, \mathsf{G}\}$:

$$\begin{aligned} X_{\mathsf{Y}} &= M_3(\mathsf{0}, \mathsf{Y}, \mathsf{1}) \odot M_3(\mathsf{C}, \mathsf{1}, \mathsf{1}), \\ X_{\mathsf{C}} &= M_3(\mathsf{0}, \mathsf{C}, \mathsf{1}) \odot M_3(\mathsf{Y}, \mathsf{1}, \mathsf{1}), \\ X_{\mathsf{G}} &= M_3(\mathsf{Y}, \mathsf{C}, \mathsf{1}) \odot M_3(\mathsf{0}, \mathsf{1}, \mathsf{1}). \end{aligned}$$

It is clear that $\mathcal{X}_{\mathsf{Y}}, \mathcal{X}_{\mathsf{C}}$ and $\mathcal{X}_{\mathsf{G}}$ obtained from all permutations of the columns of $X_{\mathsf{Y}}, X_{\mathsf{C}}$ and X_{G}, respectively, satisfy Definition 1. The polynomial representations of $X_{\mathsf{Y}}, X_{\mathsf{C}}$ and X_{G} are $F_{\mathsf{Y}} = (ay + cz)z, F_{\mathsf{C}} = (ac + yz)z$ and $F_{\mathsf{G}} = (cy + az)z$, respectively, where a, y, c and z are symbols corresponding to $\mathsf{0}, \mathsf{Y}, \mathsf{C}$ and $\mathsf{1}$, respectively. More generally, the following theorem holds:

Theorem 5: Let $F_{\mathsf{c}_k}^{(t)}$, $1 \le k \le K$, be the basis polynomials of the lattice-based (t, t)-VSSS with a set of colors $\mathcal{C} = \{\mathsf{c}_1, \mathsf{c}_2, \ldots, \mathsf{c}_K\}$. Then, for all integers $n \ge t$ the basis polynomials F_{c_k}, $1 \le k \le K$, of the lattice-based (t, n)-VSSS can be written as $F_{\mathsf{c}_k} = F_{\mathsf{c}_k}^{(t)} \cdot z^{n-t}$.

Proof: Let F be a homogeneous polynomial of degree n and X the concatenated column-permuting matrix corresponding to F. It is important to note that for each $j = 1, 2, \ldots, n-1$ $\psi^j F$ implies the polynomial representation of the matrix obtained by eliminating the n-th, the $(n-1)$-th, ..., and the $(n-j+1)$-th columns of from X, where $\psi^j F$ means applying ψ to F repeatedly for j times. Therefore, for proving the claim of the theorem it is sufficient to establish

$$\psi^{n-t+1} F_{\mathsf{c}_1} = \psi^{n-t+1} F_{\mathsf{c}_2} = \cdots = \psi^{n-t+1} F_{\mathsf{c}_K} \quad (47)$$

and show the existence of integers $N_k > 0$, $1 \le k \le K$, such that

$$\psi^{n-t} F_{\mathsf{c}_k}|_{z=0} = N_k \cdot F_{\mathsf{c}_k}^{(t)}|_{z=0}. \quad (48)$$

Equations (47) and (48) correspond to the conditions (ii) and (i) in Definition 1, respectively.

Equation (47) is proved first. Since $F_{\mathsf{c}_k}^{(t)}$, $1 \le k \le K$, are the basis polynomials satisfying $\psi F_{\mathsf{c}_1}^{(t)} = \psi F_{\mathsf{c}_2}^{(t)} = \cdots = \psi F_{\mathsf{c}_K}^{(t)}$, it is clear that

$$\psi^j F_{\mathsf{c}_1}^{(t)} = \psi^j F_{\mathsf{c}_2}^{(t)} = \cdots = \psi^j F_{\mathsf{c}_K}^{(t)} \quad (49)$$

holds for all $j \ge 1$. In addition, if we note that ψ is a linear partial differential operator, for each $k = 1, 2, \ldots, K$ $\psi^{n-t+1} F_{\mathsf{c}_k}$ is evaluated in the following way:

$$\begin{aligned} &\psi^{n-t+1} F_{\mathsf{c}_k} \\ &= \psi^{n-t+1}(F_{\mathsf{c}_k}^{(t)} \cdot z^{n-t}) \\ &= \sum_{i=0}^{n-t+1} \binom{n-t+1}{i} (\psi^{n-t+1-i} F_{\mathsf{c}_k}^{(t)}) \cdot (\psi^i z^{n-t}) \\ &= \sum_{i=0}^{n-t} \binom{n-t+1}{i} \frac{(n-t)!}{(n-t-i)!} \\ &\quad \cdot (\psi^{n-t+1-i} F_{\mathsf{c}_k}^{(t)}) \cdot z^{n-t-i}, \end{aligned} \quad (50)$$

where the last equality in (50) follows from

$\psi^{n-t+1}z^{n-t} = 0$. Combining (49) with (50) immediately implies (47).

Next, we prove that (48) with setting $N_k = (n-t)!$ is satisfied for all $k = 1, 2, \ldots, K$. Similarly to (50) we obtain

$$\begin{aligned}\psi^{n-t}F_{\mathsf{C}_k} &= \sum_{i=0}^{n-t}\binom{n-t}{i}(\psi^{n-t-i}F^{(t)}_{\mathsf{C}_k})\cdot(\psi^i z^{n-t}) \\ &= \sum_{i=0}^{n-t}\binom{n-t}{i}\frac{(n-t)!}{(n-t-i)!} \\ &\quad\cdot(\psi^{n-t-i}F^{(t)}_{\mathsf{C}_k})\cdot z^{n-t-i}. \qquad (51)\end{aligned}$$

Then, we have $N_k = (n-t)!$ by setting $z = 0$ in (51). □

If the basis polynomials in Theorem 3 are used as $F^{(t)}_{\mathsf{C}_k}$ in Theorem 5, its corresponding basis matrix X_{C_k} contains $K\cdot 2^{n-2}$ column-permuting matrices and hence contains $K\cdot 2^{n-2}\cdot n!$ columns. In addition, such X_{C_k} contains $(n-t)!\cdot t!$ columns that result in c_k, where $(n-t)!$ follows from (48). Hence, $\alpha = 1/(K\cdot 2^{n-2}\cdot\binom{n}{t})$. It is important to notice that Theorem 5 does not guarantee the optimality of these basis matrices.

4.2 The Lattice-Based $(\Gamma_{\mathsf{Qual}}, \Gamma_{\mathsf{Forb}})$-VSSS

Let $(\Gamma_{\mathsf{Qual}}, \Gamma_{\mathsf{Forb}})$ be an arbitrary access structure of n participants $\mathcal{P}$. In this subsection we show that the basis matrices of the lattice-based $(\Gamma_{\mathsf{Qual}}, \Gamma_{\mathsf{Forb}})$-VSSS with a set of colors $\mathcal{C} = \{\mathsf{c}_1, \mathsf{c}_2, \ldots, \mathsf{c}_K\}$ can be constructed by using the basis matrices of X_{C_k}, $1 \le k \le K$, of the lattice-based (t,t)-VSSS with $\mathcal{C}$, where $t = |\Gamma^*_{\mathsf{Forb}}|$ and Γ^*_{Forb} means the maximal forbidden sets defined in (3). This construction is essentially parallel to the construction given Sect. 4 in [1].

Define $\mathcal{T} = \{1, 2, \ldots, t\}$ and $\Gamma^*_{\mathsf{Forb}} = \{B_1, B_2, \ldots, B_t\}$. Denote by $2^{\mathcal{T}}$ all of the subsets of $\mathcal{T}$. We define $\beta : \mathcal{P} \to 2^{\mathcal{T}}$ as the mapping that maps $i \in \mathcal{P}$ to $\{j \in \mathcal{T} : i \notin B_j\} \in 2^{\mathcal{T}}$. Such mapping is called the *cumulative map* [12]. It is known that β satisfies

(P1) $\bigcup_{i\in A}\beta(i) = \mathcal{T}$ for all $A \in \Gamma^*_{\mathsf{Qual}}$,

(P2) $\bigcup_{i\in A}\beta(i) \subset \mathcal{T}$ for all $A \in \Gamma^*_{\mathsf{Forb}}$, where the inclusion holds in the strict sense.

Now, we construct the basis matrices X_{C_k}, $1 \le k \le K$, in the following way. Let $X^{(t)}_{\mathsf{C}_k}$, $1 \le k \le K$, be the basis matrices of the lattice-based (t,t)-VSSS. For each $k = 1, 2, \ldots, K$ define the i-th row of X_{C_k} as $h(X^{(t)}_{\mathsf{C}_k}[\beta(i)])$ for all $i = 1, 2, \ldots, n$, where $X^{(t)}_{\mathsf{C}_k}[\beta(i)]$ is defined in the same manner as (5) and h is the mapping defined in (6). If X_{C_k}, $1 \le k \le K$, contain the same column in common, remove the column from all X_{C_k}. Hence, the number of columns of X_{C_k} is less than or equal to that of $X^{(t)}_{\mathsf{C}_k}$. Define $\mathcal{X}_{\mathsf{C}_k}$, $1 \le k \le K$, as the set obtained from all the permutations of the columns of X_{C_k}.

The reason why such $X_{\mathsf{C}_k}, 1 \le k \le K$, become the basis matrices of the lattice-based $(\Gamma_{\mathsf{Qual}}, \Gamma_{\mathsf{Forb}})$-VSSS is deeply related to the properties (P1) and (P2). Suppose that $A \in \Gamma^*_{\mathsf{Qual}}$. Then, (P1) guarantees that

$$\begin{aligned}h(X_{\mathsf{C}_k}[A]) &= h\left(X^{(t)}_{\mathsf{C}_k}\left[\bigcup_{i\in A}\beta(i)\right]\right) \\ &= h(X^{(t)}_{\mathsf{C}_k}[\mathcal{T}]), \qquad (52)\end{aligned}$$

where the idempotent law on the join of L^q is used for obtaining the first equality in (52). Since for each $k = 1, 2, \ldots, K$ $h(X^{(t)}_{\mathsf{C}_k}[\mathcal{T}])$ is designed to contain 1s and at least one c_k from its definition, $\mathcal{X}_{\mathsf{C}_k}$ obtained from X_{C_k} satisfies (i) in Definition 1. On the other hand, suppose that $A \in \Gamma_{\mathsf{Forb}}$ and define B as $B = \bigcup_{i\in A}\beta(i)$. Since (P2) implies $|B| < t$, the definitions of $X^{(t)}_{\mathsf{C}_k}$, $1 \le k \le K$, lead to $\mathcal{X}_{\mathsf{C}_1}[B] = \mathcal{X}_{\mathsf{C}_2}[B] = \cdots = \mathcal{X}_{\mathsf{C}_K}[B]$, where $\mathcal{X}_{\mathsf{C}_k}[B]$ is defined in (7), which establishes (ii) in Definition 1.

Summarizing, we obtain the following theorem.

Theorem 6: Let $(\Gamma_{\mathsf{Qual}}, \Gamma_{\mathsf{Forb}})$ be an arbitrary access structure of n participants. Let $X^{(t)}_{\mathsf{C}_k}$, $1 \le k \le K$, be the basis matrices of the lattice-based (t,t)-VSSS with a set of colors $\mathcal{C} = \{\mathsf{c}_1, \mathsf{c}_2, \ldots, \mathsf{c}_K\}$, where $t = |\Gamma^*_{\mathsf{Forb}}|$. If for each $k = 1, 2, \ldots, K$ the i-th row of X_{C_k} is defined as $h(X^{(t)}_{\mathsf{C}_k}[\beta(i)])$ for all $i = 1, 2, \ldots, n$, then X_{C_k}, $1 \le k \le K$, become the basis matrices of the lattice-based $(\Gamma_{\mathsf{Qual}}, \Gamma_{\mathsf{Forb}})$-VSSS with $\mathcal{C}$.

Example 5: Suppose that $\mathcal{P} = \{1, 2, 3, 4\}$ and $\Gamma^*_{\mathsf{Qual}} = \{\{1,2\}, \{2,3\}, \{3,4\}\}$. This is the access structure given in Example 4.1 in [1]. It is easy to see that $\Gamma^*_{\mathsf{Forb}} = \{\{1,4\}, \{1,3\}, \{2,4\}\}$. We construct the basis matrices of the lattice-based $(\Gamma_{\mathsf{Qual}}, \Gamma_{\mathsf{Forb}})$-VSSS with $\{\mathsf{Y}, \mathsf{C}, \mathsf{G}\}$.

Define $B_1 = \{1,4\}, B_2 = \{1,3\}$ and $B_3 = \{2,4\}$. Since $|\Gamma^*_{\mathsf{Forb}}| = 3$, we define $\mathcal{T}$ as $\mathcal{T} = \{1,2,3\}$. Let $\beta : \mathcal{P} \to 2^{\mathcal{T}}$ be the cumulative map satisfying $\beta(1) = \{3\}, \beta(2) = \{1,2\}, \beta(3) = \{1,3\}$ and $\beta(4) = \{2\}$. That is, β maps $i \in \mathcal{T}$ to the set of indices of elements in Γ^*_{Forb} not containing i. Denote by $X^{(3)}_{\mathsf{Y}}, X^{(3)}_{\mathsf{C}}$ and $X^{(3)}_{\mathsf{G}}$ the basis matrices of the lattice-based $(3,3)$-VSSS with $\{\mathsf{Y}, \mathsf{C}, \mathsf{G}\}$ given in Example 3 in Sect. 3.3. Then, the basis matrices $X_{\mathsf{Y}}, X_{\mathsf{C}}$ and X_{G} are obtained from $X^{(3)}_{\mathsf{Y}}, X^{(3)}_{\mathsf{C}}, X^{(3)}_{\mathsf{G}}$ and β. For example, $\beta(2) = \{1,2\}$ indicates that the second rows of $X_{\mathsf{Y}}, X_{\mathsf{C}}$ and X_{G} are obtained from the joins of the first and the second rows of $X^{(3)}_{\mathsf{Y}}, X^{(3)}_{\mathsf{G}}$ and $X^{(3)}_{\mathsf{G}}$, respectively. We obtain $X_{\mathsf{Y}}, X_{\mathsf{C}}$ and X_{G} with $q = 36 - 4 = 32$ and $\alpha = 3/16$ since we can remove four ${}^t[1,1,1,1]$s commonly contained in the matrices obtained from $X^{(3)}_{\mathsf{Y}}, X^{(3)}_{\mathsf{C}}, X^{(3)}_{\mathsf{G}}$ and β. □

5. Conclusion

In this paper we propose a new construction of the basis matrices of the lattice-based (n, n)-VSSS that can be applied to color images. We show that, if we find homogeneous polynomials of degree n satisfying a certain system of simultaneous partial differential equations, we can obtain the basis matrices corresponding to the homogenous polynomials. The obtained basis matrices turns out to have a certain kind of optimality. We also show that the basis matrices of the (t, n)-VSSS or VSSS for general access structures are easily obtained from the new construction. Developing another construction of the basis matrices of the (t, n)-VSSS yielding brighter reproduced images remains as an open problem.

References

[1] G. Ateniese, C. Blundo, A. De Santis, and D.R. Stinson, "Visual cryptography for general access structures," Information and Computation, vol.129, pp.86–106, 1996.
[2] C. Blundo, A. De Santis, and D.R. Stinson, "On the contrast in visual cryptography schemes," J. Cryptology, vol.12, no.4, pp.261–289, 1999.
[3] C. Blundo, P. D'Arco, A. De Santis, and D.R. Stinson, "Contrast optimal threshold visual cryptography schemes," submitted to SIAM J. Discrete Mathematics. (Available from `http://cacr.math.uwaterloo.ca/~dstin son`)
[4] S. Droste, "New results on visual cryptography," Advance in Cryptography-CRYPT'96, Lecture Notes in Computer Science 1109, pp.401–415, Springer Verlag, 1996.
[5] T. Hofmeister, M. Krause, and H.U. Simon, "Contrast-optimal k out of n secret sharing schemes in visual cryptography," Cocoon'97, Lecture Note in Computer Science 1276, pp.176–185, Springer-Verlag, 1997.
[6] 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.
[7] T. Kato and H. Imai, "An extended construction method of visual secret sharing scheme," IEICE Trans., vol.J79-A, no.8, pp.1344–1351, Aug. 1996.
[8] 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.
[9] M. Naor and A. Shamir, "Visual cryptography," Advance in Cryptography-EUROCRYPT'94, Lecture Notes in Computer Science 950, pp.1–12, Springer-Verlag, 1994.
[10] M. Naor and A. Shamir, "Visual cryptography II: Improving the contrast via the cover base," Security Protocols, Lecture Notes in Computer Science 1189, pp.197–202, Springer-Verlag, 1997.
[11] V. Rijmen and B. Preneel, "Efficient color visual encryption or 'shared colors of Benetton'," presented at the Rump session of Eurocrypt'96. (Available from `http://www.esat.kuleuven.ac.be/~rijmen/vc`)
[12] G.J. Simmons, W. Jackson, and K.M. Martin, "The geometry of shared secret schemes," Bulletin of the Institute of Combinatorics and its Applications, vol.1, pp.71–88, 1991.
[13] D.R. Stinson, Cryptography: theory and practice, CRC Press, 1995.
[14] E.R. Verheul and H.C.A. van Tilborg, "Constructions and properties of k out of n visual secret sharing schemes," Designs, Codes, and Cryptography, vol.11, no.2, pp.179–196, 1997.

Hiroki Koga was born in Fukuoka, Japan, on November 2, 1967. He received the B.E., M.E. and Dr.E. degrees from University of Tokyo, Japan, in 1990, 1992 and 1995, respectively. He was an Assistant Professor at University of Tokyo during 1995–1999. From April 1999 he is a lecturer at Institute of Engineering Mechanics and Systems, University of Tsukuba. His research interest includes the Shannon theory, data compression and information security.

Mitsugu Iwamoto was born in Fukuoka, Japan on July 29, 1976. He received the B.E. degree from University of Tokyo, Japan, in 1999. He is currently a master course student of Graduate School of Engineering, University of Tokyo. His research interest includes high-performance computing and information security.

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