Far East Journal of Mathematical Sciences (FJMS)

http://www.pphmj.com
http://dx.doi.org/10.17654/MS102061223
Volume 102, Number 6, 2017, Pages 1223-1241 **ISSN: 0972-0871**

MATRIX PROBLEMS INDUCED BY VISUAL CRYPTOGRAPHY SCHEMES

Agustín Moreno Cañadas[1], Hernán Giraldo[2] and Robinson-Julian Serna Vanegas[1]

[1]Department of Mathematics
National University of Colombia
Bogotá, Colombia
e-mail: amorenoca@unal.edu.co
rjsernav@unal.edu.co

[2]Institute of Mathematics
University of Antioquia
Medellín, Colombia
e-mail: hernan.giraldo@udea.edu.co

Abstract

In this paper, k-linear representations of posets are used to define lattice-based schemes of visual cryptography for color images.

Received: April 20, 2017; Revised: June 18, 2017; Accepted: July 18, 2017
2010 Mathematics Subject Classification: 68U10, 16G60, 16G30, 11U71.
Keywords and phrases: lattice, matrix problem, poset representation, visual cryptography, indecomposable representation.
This research was partly supported by CODI and Estrategia de Sostenibilidad 2016-2017 (Universidad de Antioquia), and COLCIENCIAS-ECOPETROL (Contrato RC. No. 0266-2013).
This research was supported by COLCIENCIAS- convocatoria 727 Doctorado Nacional.

1. Introduction

Visual cryptography is a kind of cryptography where the decoding process only requires the use of the human visual system without any special computation. This kind of cryptography was introduced by Naor and Shamir in [8]. In this case, a secret is shared between a group of n persons by giving to each of them an image (called *shadow*) with no information about the secret, such images are printed onto a transparency in such a way that the only way to recover the secret is by stacking the transparencies all together [2, 3].

Naor and Shamir analyzed the case of k out n or (k, n)-*threshold visual cryptography schemes* (TVS), in which the secret image is visible if and only if any k transparencies are stacked together. Soon afterwards, this set up was generalized by Blundo et al. [1] Droste [5] and Klein and Wessler [6].

Tsai et al. and Feng et al. proposed sharing methods for multiple secret images in [22] and [13] via XOR computing for embedding and extracting images, and Lagrange's interpolation, respectively, [10]. According to Shyu et al. [20], Wu and Chen might be the first researchers to consider the problem of sharing two secret images in two shares in visual cryptography [23]. Afterwards, Shyu et al. [20] proposed a generalization of the work of Wu and Chen, actually, they defined a visual secret sharing scheme to encode more than two secrets.

Nakajima and Yamaguchi [7] introduced the use of natural images in schemes of visual cryptography (see Figure 1), besides Ross and Othman [18] applied gray-level extended visual cryptography schemes to preserve the privacy of digital images stored in a central database.

We also recall that some visual secret sharing schemes (VSSS) have been introduced by using some mathematical structures. For instance, Cañadas et al. [3] introduced a visual cryptography scheme with a special share T_0 containing sets of nested images, all secrets can be revealed by superimposing some transparencies to this fixed share. These authors also have used some properties of k-linear maps to generate schemes of multiple secret sharing.

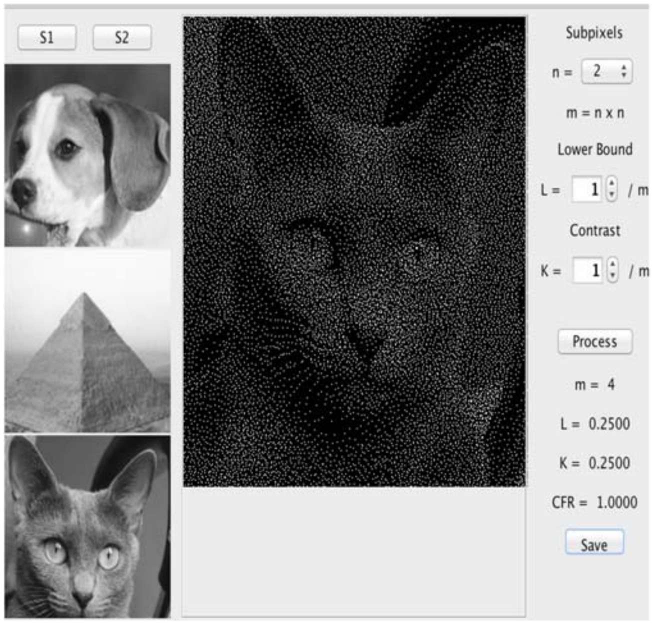

Figure 1. Example of a Nakajima's $(2, 2)$-scheme. In this case, shadows S1 (Dog) and S2 (Pyramid) are used to encrypt the original image (Cat).

In 1998, Koga and Yamamoto [17] proposed a lattice-based TVS for color images, in this case pixels are treated as elements of a suitable lattice S and the stacking process is defined as an operation between elements of the lattice, according to them the commutative and associative laws of such operation allow to (k, n) VSSS to decrypt k shares by stacking up of all them in an arbitrary order. Permitting the existence of inverses for all $s \in S$ leads to pathological VSSS for example, stacking a black subpixel with another subpixel yield to a white or transparent subpixel, finite lattices are one of the simplest structures that meet these requirements. Under these circumstances we generalize this kind of TVS by using k-linear representations in such a way that the VSSS is completely defined by the orbits defined by some admissible transformations between columns and rows of a matrix representation.

This paper is organized as follows: Basic notations, facts, and definitions are included in Section 2, the main results of this paper are given in Section 3 actually in this section, we interpret visual cryptography schemes as some matrix representations of some color-lattices. Finally, in Section 4, we give some concluding remarks.

2. Preliminaries

In this section, we introduce basic definitions, and notations to be used throughout the paper [1-5].

2.1. Visual cryptography schemes

A *visual cryptography scheme* (*VCS*) is based on the fact that each pixel of an image is divided into a certain number m of subpixels. This number m is called the *pixel expansion* of the image. If the number of black subpixels needed to represent a white pixel in an image is l, and the number of black subpixels needed to represent a black pixel is h, then we call the number $\alpha = \frac{h - l}{m}$ the *contrast* of the image [2, 3].

Here we present the definition of a VSSS according to Cañadas et al. [2, 3, 12].

Formally, let $\mathcal{P} = \{1, 2, ..., n\}$ be a set of elements called *participants* and let $2^{\mathcal{P}}$ denote the set of all subsets of $\mathcal{P}$. Let $\Gamma_{\text{Qual}} \subseteq 2^{\mathcal{P}}$ and $\Gamma_{\text{Forb}} \subseteq 2^{\mathcal{P}}$, where $\Gamma_{\text{Qual}} \cap \Gamma_{\text{Forb}} = \varnothing$. Members of Γ_{Qual} (respectively, Γ_{Forb}) are called *qualified sets* (respectively, *forbidden sets*). The pair $(\Gamma_{\text{Qual}}, \Gamma_{\text{Forb}})$ is called the *access structure* of the scheme [12].

$(\Gamma_{\text{Qual}}, \Gamma_{\text{Forb}})$ is an access structure on a set of n participants. Two collections (multisets) of $n \times m$ Boolean matrices C_0, C_1 constitute a visual cryptography scheme with pixel expansion m if there exist integers l and h such that $h > l$ satisfying:

(1) Any qualified set $X = \{i_1, i_2, ..., i_p\} \in \Gamma_{\text{Qual}}$ can recover the shared image by stacking their transparencies (i.e., for any $M \in C_0$, the "or" of rows $\bigvee, i_1, i_2, ..., i_p$ satisfies $w_H(\bigvee) \le m - h$, whereas, for any $M \in C_1$, it results that $w_H(\bigvee) \ge m - h$, where $w_H(\bigvee)$ is then Hamming weight of $\bigvee$).

(2) Any (forbidden) set $X = \{i_1, i_2, ..., i_p\} \in \Gamma_{\text{Forb}}$ has no information on the shared image (i.e., the two collections of D_t matrices with $t \in \{0, 1\}$ obtained by restricting each $n \times m$ matrix in C_t to rows $i_1, i_2, ..., i_p$ are indistinguishable in the sense that they contain the same matrices with the same frequencies).

Several visual cryptography schemes have been realized by using two $n \times m$ matrices, S^0 and S^1 called *basis matrices*. The collections C_0 and C_1 are obtained by permuting the columns of the corresponding basis matrix [12].

In [12], it is described a VCS with perfect reconstruction of black pixels (where all the subpixels associated in a reconstructed image with a black pixel are black), in this case, for $i = 1, 2, ..., q$, let $(\Gamma^i_{\text{Qual}}, \Gamma^i_{\text{Forb}})$ be an access structure on a set $\mathcal{P}$ of n participants. If a participant $j \in \mathcal{P}$ is not essential for the ith structure, it is assumed that $j \notin \Gamma^i_{\text{Forb}}$ and that j does not receive any share. Suppose there exists a $(\Gamma^i_{\text{Qual}}, \Gamma^i_{\text{Forb}})$-VCS with a pixel expansion m_i and basis matrices S^0_i and S^1_i, for $i = 1, 2, ..., q$. The basis matrix S^0 (S^1, resp.) of a VCS for the access structure $(\Gamma_{\text{Qual}}, \Gamma_{\text{Forb}})$, where $\Gamma_{\text{Qual}} = \sum_{i=1}^{q} \Gamma^i_{\text{Qual}}$ and $\Gamma_{\text{Forb}} = \bigcap_{i=1}^{q} \Gamma^i_{\text{Forb}}$ is constructed as the concatenation of some auxiliary matrices $\hat{T}^0_i$ ($\hat{T}^1_i$, resp.), for each $i = 1, 2, ..., q$. Such matrices are obtained as follows: for each $j = 1, 2, ..., n$, the jth row of $\hat{T}_i^0$ ($\hat{T}_i^1$, resp.) has all ones as entries if the participant j is not essential for $(\Gamma_{\text{Qual}}^i, \Gamma_{\text{Forb}}^i)$, otherwise it is the row of S_i^0 (S_i^1, resp.) corresponding to participant j. Hence, $S^0 = \hat{T}_1^0 \oplus \hat{T}_2^0 \oplus \cdots \oplus \hat{T}_q^0$ and $S^1 = \hat{T}_1^1 \circ \hat{T}_2^1 \oplus \cdots \oplus \hat{T}_q^1$, where $\oplus$ denotes the concatenation of matrices. The resulting VCS has a pixel expansion $m = \sum_{i=1}^{q} m_i$.

2.2. Posets

An *ordered set* (or *partially ordered set* or *poset*) is an ordered pair of the form $(\mathcal{P}, \leq)$ of a set $\mathcal{P}$ and a binary relation $\leq$ contained in $\mathcal{P} \times \mathcal{P}$, called the *order* (or the *partial order*) on $\mathcal{P}$, such that $\leq$ is reflexive, antisymmetric and transitive [11]. The elements of $\mathcal{P}$ are called the *points* of the ordered set. We will write $x < y$ for $x \leq y$ and $x \neq y$, in this case we will say x is *strictly less than* y. An ordered set will be called *finite* (*infinite*) if and only if the underlying set is finite (infinite). Usually we shall be a little slovenly and say simply $\mathcal{P}$ *is an ordered set*. Where it is necessary to specify the order relation overtly we write $(\mathcal{P}, \leq)$.

Let $\mathcal{P}$ be an ordered set and let $x, y \in \mathcal{P}$. Then we say x is *covered* by y if $x < y$ and $x \leq z < y$ imply $z = x$.

An ordered set C is called a *chain* (or a *totally ordered set* or a *linearly ordered set*) if and only if for all $p, q \in C$ we have $p \leq q$ or $q \leq p$ (i.e., p and q are comparable). On the other hand, an ordered set $\mathcal{P}$ is called an *antichain* if $x \leq y$ in $\mathcal{P}$ only if $x = y$ [11]. We let $\mathcal{P}_2$ denote the set of all antichains with two points in $\mathcal{P}$.

$$w(\mathcal{P}) = \max_{\substack{C \subseteq \mathcal{P} \\ C \text{ antichain}}} |C| \text{ is called the } \textit{width} \text{ of the poset } \mathcal{P}.$$

Let $\mathcal{P}$ be an ordered set. A chain C in $\mathcal{P}$ will be called a *maximal chain* if and only if for all chains $K \subseteq \mathcal{P}$ with $C \subseteq K$ we have $C = K$. If for every $y \in \mathcal{P}$ comparable with $x \in \mathcal{P}$, we have that $y \leq x$ (respectively, $x \leq y$), then x is a maximal point (respectively, minimal point) of $\mathcal{P}$.

If n is a positive integer, we let $\mathbf{n}$ denote the n-element poset with the special property that any two elements are comparable [19]. We also define a subposet Q of a poset P to be *convex* if $y \in Q$ whenever $x < y < z$ in P and $x, z \in Q$.

Let $\mathcal{P}$ be a finite ordered set. We can represent $\mathcal{P}$ by a configuration of circles (representing the elements of $\mathcal{P}$) and interconnecting lines (indicating the covering relation). The construction goes as follows:

(1) To each point $x \in \mathcal{P}$, associate a point $p(x)$ of the Euclidean plane $\mathbb{R}^2$, depicted by a small circle with center at $p(x)$.

(2) For each covering pair $x < y$ in $\mathcal{P}$, take a line segment $l(x, y)$ joining the circle at $p(x)$ to the circle at $p(y)$.

(3) Carry out (1) and (2) in such a way that

(a) if $x < y$, then $p(x)$ is lower than $p(y)$,

(b) the circle at $p(z)$ does not intersect the line segment $l(x, y)$ if $z \neq x$ and $z \neq y$.

A configuration satisfying (1)-(3) is called a *Hasse diagram* or *diagram* of $\mathcal{P}$. In the other direction, a diagram may be used to define a finite ordered set; an example is given below, for a poset $(\mathcal{M}_3, \preceq) = \{(i, j) \mid 0 \leq i \leq 3, 0 \leq j \leq 3\} \subset \mathbb{N}^2$ whose points satisfy the following condition:

$$(i, j) \preceq (i', j') \text{ if and only if } i \leq i' \text{ and } j \leq j'$$
$$\text{for all } (i, j), (i', j') \in \mathcal{M}_3. \tag{1}$$

In this case, $\mathbb{N}$ has been equipped with its natural ordering.

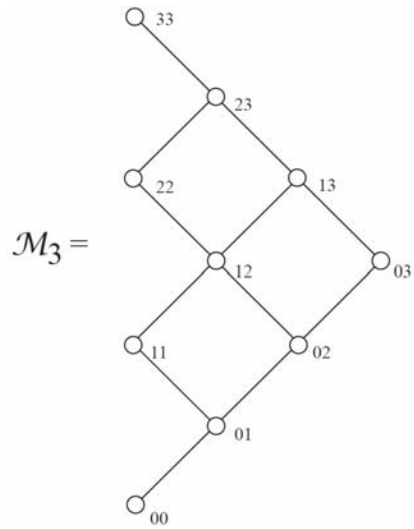

Figure 2. Hasse diagram of poset $\mathcal{M}_3$.

Let $(\mathcal{P}, \preceq)$ and $(\mathcal{Q}, \trianglelefteq)$ be ordered sets and let $f : \mathcal{P} \to \mathcal{Q}$ be a map. Then *f* is called an *order-preserving function* if and only if for all $x, y \in \mathcal{P}$ we have:

$$x \preceq y \Rightarrow f(x) \trianglelefteq f(y).$$

We shall say that two posets *P* and *Q* are *isomorphic* if there exists an order-preserving bijection $f : P \to Q,$ whose inverse is order-preserving. In such a case, we shall write $P \cong Q.$

Let $(\mathcal{P}, \preceq)$ and $(\mathcal{Q}, \trianglelefteq)$ be ordered sets. Then $f : \mathcal{P} \to \mathcal{Q}$ is called an (*order*) *embedding* if and only if *f* is injective, and for all $x, y \in \mathcal{P}$ we have:

$$x \preceq y \Leftrightarrow f(x) \trianglelefteq f(y).$$

If $(P, \leq)$ and $(Q, \trianglelefteq)$ are posets, then the *direct* (or Cartesian) *product* of *P* and *Q* is the poset $(P \times Q, \preceq)$ on the set $\{(x, y) : x \in P \text{ and } y \in Q\}$ such that $(x, y) \preceq (x', y')$ in $P \times Q$ if $x \leq x'$ in *P* and $y \trianglelefteq y'$ in *Q*. To draw the Hasse diagram of $P \times Q$ (when *P* and *Q* are finite), draw the Hasse diagram of *P*, replace each element *x* of *P* by a copy Q_x of *Q* and connect corresponding elements of Q_x and Q_y (with respect to some isomorphism $Q_x \cong Q_y$) if x and y are connected in the Hasse diagram of P.

If x, y belong to a poset $\mathcal{P}$, then an *upper bound* of x and y is an element $z \in \mathcal{P}$, satisfying $x \leq z$ and $y \leq z$. A *least upper bound* of x and y is an upper bound z of x and y such that every upper bound w of x and y satisfies $z \leq w$. If a least upper bound of x and y exists, then it is clearly unique and is denoted $x \vee y$. Dually one can define the greatest lower bound $x \wedge y$, when it exists. A *lattice* is a poset L for which every pair of elements has a least upper bound and greatest lower bound. We say that a poset $\mathcal{P}$ *has a* $\hat{0}$ if there exists an element $\hat{0} \in \mathcal{P}$ such that $\hat{0} \leq x$ for all $x \in \mathcal{P}$. Similarly, $\mathcal{P}$ *has a* $\hat{1}$ if there exists $\hat{1} \in \mathcal{P}$ such that $x \leq \hat{1}$ for all $x \in \mathcal{P}$. Clearly all finite lattices have $\hat{0}$ and $\hat{1}$.

An *order ideal* of a poset $(\mathcal{P}, \leq)$ is a subset I of $\mathcal{P}$ such that if $x \in I$ and $y \leq x$, then $y \in I$. We let $J(\mathcal{P})$ denote the set of all order ideals of $\mathcal{P}$, ordered by inclusion. In particular, we define the order ideal or *down-set* of $a \in \mathcal{P}$ to be $a_{\triangle} = \{q \in \mathcal{P} : q \leq a\}$. Dually, $a^{\triangledown} = \{q \in \mathcal{P} : a \leq q\}$ is the *filter* or *up-set* of a [19]. $a^{\blacktriangledown} = a^{\triangledown} \setminus \{a\}$, $a_{\blacktriangle} = a_{\triangle} \setminus \{a\}$.

2.3. Matrix representations

The poset representation theory was introduced in 1972 by Nazarova Roiter and their students in Kiev. The main goal of its investigations was to obtain a complete classification of the indecomposable objects of the additive category rep $\mathcal{P}$ of a given poset $\mathcal{P}$. In this case, a representation U of a given poset $(\mathcal{P}, \leq)$ over a commutative ring k is a system of the form:

$$U = (U_0, U_x \mid x \in \mathcal{P}), \tag{2}$$

where U_0 is a k-module and for each $x \in \mathcal{P}$, U_x is a submodule of U_0 such that $U_x \subseteq U_y$ provided $x \leq y$ [4, 14, 15, 21]. Attached to each representation U there exists its matrix representation with dimension vector

$d = [d_0 d_1 \cdots d_t]^T \in \mathbb{N}^{1+t}$ is by definition a pair (d, A), where $A \in k^{d_0 \times \overline{d}}$ and $\overline{d} = d_1 + \cdots + d_t$. The datum of d provides a partition of $A = [A_1 | A_2 | \cdots | A_t]$ into t vertical stripes $A_i \in k^{d_0 \times d_i}$ and permits us to define the following equivalence relation: Two representations (d, A) and (e, B) are equivalent if $d = e$ and if B can be obtained from A by performing the following transformations:

(a) Arbitrary row-transformations.

(b) Arbitrary column-transformations within each vertical stripe.

(c) Additions of columns of stripe i to columns of stripe j if $x_i < x_j$.

The set $\mathrm{Mat}_{\mathcal{P}}$ of all matrix representations of $\mathcal{P}$ is closed under the direct sum defined by the formula

$$A \oplus A' = \begin{array}{|c|c|c|} \hline A_1 \ \vdots \ 0 & \cdots & A_t \ \vdots \ 0 \\ \hline 0 \ \vdots \ A'_1 & \cdots & 0 \ \vdots \ A'_t \\ \hline \end{array}$$

The direct sum of the k-linear representations U, V is defined by the formula

$$U \oplus V = (U_0 \oplus V_0; U_x \oplus V_x \,|\, x \in \mathcal{P}).$$

A k-linear representation U of a poset $\mathcal{P}$ is said to be *indecomposable* if U is non-zero and is not a direct sum of two non-zero k-linear representations. The *dimension* of a representation $U = (U_0, U_x \,|\, x \in \mathcal{P})$ is a vector $(d_0; d_x \,|\, x \in \mathcal{P})$, where $d_x = \dim U_x / \underline{U_x}$ and $\underline{U_x} = \sum_{y<x} U_y$ is the *radical subspace* of U_x. U is a representation *sincere* if $d_x \neq 0$ for all $x \in \mathcal{P}$.

A k-linear representation U of a poset $\mathcal{P}$ is called *trivial* if $\dim_k U_0 = 1$. For any subset $S \subseteq \mathcal{P}$, we define a trivial representation $k(S) = k(S^{\triangledown}) = k(\min S) = (k; U_x \,|\, x \in \mathcal{P})$ with $U_x = k$ if $x \in S^{\triangledown}$, $U_x = 0$ otherwise.

For example, if

$$\mathcal{P} = \begin{matrix} \circ & \circ & \circ \\ a_1 & a_2 & a_3 \end{matrix}$$

is a poset consisting of three incomparable elements, then the following is a complete list of indecomposable representations:

$$k(a_i),\ k(a_i, a_j),\ k(a_1, a_2, a_3), \quad \text{and} \quad U_{a_3} = \boxed{\begin{array}{|c|c|c|} 1 & 0 & 1 \\ \hline 0 & 1 & 1 \end{array}},$$

where $i \in \{1, 2, 3\}$, and $i < j$.

2.4. Lattice-based VSSS

Now, we present the definition of a lattice-based TVS in accordance with Koga and Yamamoto [17]:

Let $m > 0$ be given and $\mathcal{L}$ be a finite lattice of a finite number of colors that can be physically realized. Suppose that $\mathcal{C} = \{c_1, c_2, ..., c_J\}$ is a subset of elements in $\mathcal{L}$, which is not necessarily a sublattice of $\mathcal{L}$. For all q satisfying $1 \leq q \leq k$ and distinct $i_1, i_2, ..., i_q \subseteq \{1, 2, ..., n\}$ define a mapping $h^{(i_1, i_2, ..., i_q)} : (\mathcal{L}^m)^n \to \mathcal{L}^m$ by

$$h^{(i_1, i_2, ..., i_q)}(x) = x_{i_1} \vee x_{i_2} \cdots \vee x_{i_q}, \tag{3}$$

where $x = (x_1, x_2, ..., x_n) \in (\mathcal{L}^m)^n$. If there exists $(\mathcal{X}_{c_j}, \mathcal{Y}_{c_j})_{1 \leq j \leq J}$ is called the *lattice-based* (k, n) *VSSS* with colors $\mathcal{C}$.

(1) For all $j = 1, 2, ..., J$ and distinct $\{i_1, i_2, ..., i_k\} \subseteq \{1, 2, ..., n\}$, all $x \in \mathcal{X}_{c_j}$ satisfy

$$h^{(i_1, i_2, ..., i_k)}(x) \in \mathcal{Y}_{c_j}.$$

(2) For all $q < k$ and $\{i_1, i_2, ..., i_k\} \subset \{1, 2, ..., n\}$, define

$$\mathcal{X}_{c_j}^{(i_1, i_2, ..., i_q)} = \{(x_{i_1}, x_{i_2}, ..., x_{i_q}) : (x_1, x_2, ..., x_n) \in \mathcal{X}_{c_j}\}.$$

Then $\mathcal{X}_{c_j}^{(i_1, i_2, \ldots, i_q)}$, $j = 1, 2, \ldots, J$ are indistinguishable in the sense that they contain the same elements with the same frequencies.

(3) For all $c_j \in \mathcal{C}$ satisfying $c_j \neq 1 \in \mathcal{L}$ all the elements in $\mathcal{Y}_{c_j}$ are composed by 1's and at least one c_j. In case that $c_j = 1$, $\mathcal{Y}_{c_j}$ has only one element composed by m 1's.

3. A Matrix Problem Induced by a Lattice-based VSSS

In this section, we interpret the Koga-Yamamoto scheme as a matrix problem. To do that, we consider matrix representations (d, A) of a lattice $\mathcal{L}$ induced by a finite number of colors. In this case, for a (k, n) VSSS we have that $A \in \mathcal{L}^{d_0 \times \overline{d}}$ with $d_0 = m$ is the pixel expansion, $d_i = d_j = n$ for any $i, j \in \mathcal{L}$ is the size of the set of participants and k is the number of qualified participants. In other words, each vertical stripe consists of n generators (of the corresponding module U_{c_j} for each color $c_j \in \mathcal{L}$) with $k < n$ linear independent columns. Besides a *lattice-color matrix representation* of $\mathcal{L}$ is an $m \times \overline{d}$ rectangular matrix separated into vertical stripes with the same number c of columns. In this case, columns in each stripe M_x are indistinguishable (i.e., they have the same elements appearing with the same frequency) and constitute a composition (i.e., a partition where the order matters) of a given vector $F_x \in \mathcal{L}^m$ for any $x \in \mathcal{C}$.

For $\{x_1, x_2, \ldots, x_j\} = \mathcal{C}$, let M and M' be lattice-color matrix representations with associated vectors $F_{x_1} \cdots F_{x_t}$ and $F'_{x_1} \cdots F'_{x_t}$, respectively. Then M and M' are called *equivalent* if and only if there exists some permutation $\pi \in S_m$ such that

$$F'_{x_j} = (x_j^{\pi(1)}, \ldots, x_j^{\pi(m)}) \text{ if } F_{x_j} = (x_j^1, \ldots, x_j^m)$$

for each chosen $x_j \in \mathcal{L}$.

The following result establishes the existence of matrix representations whose columns within each vertical stripe M_x constitute compositions of a given set of fixed vectors F_x.

Theorem 1. *If* $x \in \mathcal{C}$ *and* F_x *consists of* k_1 1'*s and* k_x x'*s with* $k_1 + k_x = m$, *then there exist* n *indistinguishable vectors* $g_x^1, \ldots, g_x^n$ *such that* $F(x) = \sum_{i=1}^{n} g_x^i$.

Proof. Let $F(x)$ be such that $F_x = (a_1, \ldots, a_m) \in \mathcal{L}^m$ with k_1 1's, k_x x's and $k_1 + k_x = m$, and a permutation $\pi \in S_m$ such that $\overline{F}_x = (a_{\pi(1)} \cdots a_{\pi(m)}) = (x, \ldots, x, 1, \ldots, 1)$. We fix points $y \in \mathcal{L} \cap x_\triangle$, $z \in \mathcal{L}$, and an $m \times n$ matrix R_x such that the entries of the first $k(x)$ rows are y's and the entries of the remain rows are z's. Then there exist integers q_1 and r_1 such that $k_1 = nq_1 + r_1$ with $0 \le r_1 < n$, $k_x = nq_x + r_x$ with $0 \le r_x < n$.

Let us consider the matrix block

$$\overline{M}_x = R_x - \begin{array}{|c|}\hline yI_n \\ \hline \vdots \\ \hline yI_n \\ \hline yA \\ \hline zI_n \\ \hline \vdots \\ \hline zI_n \\ \hline zB \\ \hline \end{array} \bigvee \begin{array}{|c|}\hline xI_n \\ \hline \vdots \\ \hline xI_n \\ \hline A \\ \hline I_n \\ \hline \vdots \\ \hline I_n \\ \hline B \\ \hline \end{array},$$

where I_n denotes an $n \times n$ matrix, the number of matrix blocks $xI_n(I_n)$ in $\overline{M}_x$ is given, respectively, by nq_x (nq_1), in this case A is an $r_x \times n$ matrix with the form. Besides, $-A$ is a matrix such that $A \vee (-A) = 0$.

$$A = \left[\begin{array}{c|c} I_{r_x} & \\ \cline{2-2} & x, \ldots, x \end{array}\right]$$

B is an $r_1 \times n$ matrix with the form

$$B = \left[\begin{array}{c|c} I_{r_1} & \\ \cline{2-2} & 1, \ldots, 1 \end{array}\right]$$

It is worth noting that empty blocks in A and B denote matrices whose entries are all zeroes.

By construction columns of matrix $\overline{M}_x$ constitute an n-elements set of indistinguishable vectors associated to the fixed vector $\overline{F}_x$. If matrix M_x is obtained from $\overline{M}_x$ by applying permutation π to the rows then columns of M_x correspond to n indistinguishable vectors which define a composition of the fixed vector F_x. $\square$

The following result defines admissible transformations which guarantee the existence of equivalent lattice-color matrix representations. Therefore, it guarantees the construction of different types of (k, n) lattice-based VSSS.

Theorem 2. *Let M and M' be two lattice matrix representations of a given lattice $\mathcal{L}$. Then M and M' are equivalent if M and M' can be turned one into each other by applying the following transformations*:

(a) *Row permutations of the whole matrix*.

(b) *Column permutations within a given vertical stripe*.

(c) *Multiplication of a given column j in the stripe M_x by some scalar $z \in (\lambda_j^x)^{\triangledown}$, where λ_j^x is the maximum of all entries in such a column*.

(d) *Addition of a given jth column in the stripe M_x to the jth column in the stripe M_y with coefficients in $(\delta_j^y)_{\vartriangle}$, where δ_j^y is the minimum of all entries in the column of M_y. If $x \leq y$ in $\mathcal{L}$.*

Proof. Row permutations of M determine same indistinguishable vectors up to permutations. That is, if $F_{x_1}, ..., F_{x_t}$ are fixed vectors attached to the representation M and $F'_{x_1}, ..., F'_{x_t}$ are corresponding fixed vectors attached to the matrix M' obtained from M by row permutations then there exists a permutation $\pi \in S_t$ such that if

$$F_{x_i} = (x_j^1, ..., x_j^m), \text{ then } F'_{x_j} = (x_j^{\pi(1)}, ..., x_j^{\pi(m)});$$

thus M is equivalent to M'. Besides, column permutations in a given vertical stripe M_x keep invariant vectors $F_{x_1}, ..., F_{x_t}$. Therefore, if M' is obtained from M by transformations of type (a), then M is equivalent to M'.

On the other hand, if λ_j^x is the maximum of all entries in a column $j \in M_x$ and $z \in (\lambda_j^x)^{\nabla}$, then $z \geq \lambda_j^x$ and $\lambda_j^x \geq g_{kj}^x$, where $g_j^x = (g_{1j}^x, ..., g_{mj}^x)$ is the jth column of the stripe M_x, then $zg_j^x = g_j^x$. Therefore, if M' has attached fixed vectors as defined above and M is obtained via transformations of type (b), then $F'_{x_i} = F_{x_i}$ for any $1 \leq i \leq t$ therefore M is equivalent to M'.

Finally, let us suppose that δ_j^y is the minimum of the set of entries of the jth column in a vertical stripe $M_y(g_j^y = (g_{1j}^y, ..., g_{mj}^y))$, that is, $\delta_j^y \leq g_{kj}^y$ for all $1 \leq k \leq m$ and if $g_i^x = (g_{1i}^x, ..., g_{mi}^x)$ is the ith column in M_x and we add $z \wedge g_i^x$ to the column g_j^y with $z \in (\delta_j^y)_{\triangle}$, then $z \leq g_{kj}^y$ for all $1 \leq k \leq m$ thus $(z \wedge g_{ki}^x) \vee g_{kj}^y = g_{kj}^y$ which means that $(z \wedge g_i^x) \vee g_j^y$. Therefore, if M' is obtained from M via transformations of type (c), then $M = M'$. □

The following result establishes the structure of vectors F_x with $x \in \mathcal{C}$.

Theorem 3. *If* $x \in \mathcal{C}$ *with* $x \neq a \vee b$ *for any* $x \neq a$ *and* $x \neq b$ *and* F_x *consists of* k_1 1*'s and* k_x x*'s with* $k_1 + k_x = m$, *then an indistinguishable vector* g_x *consists of at least* $\left\lceil \frac{k_1}{n} \right\rceil$ x*'s and at least* $\left\lceil \frac{k_1}{n} \right\rceil$ 1*'s, where n is the number of generators in* M_x. *Moreover, if* m_x *is the number of* x*'s in* g_x *and* m_1 *is the number of* 1*'s in* g_x, *then there exist* $m - (m_1 + m_x)$ *elements in* $x_\blacktriangle$ *in* g_x.

Proof. Let us suppose that $F_x = (x, \ldots, x, 1, \ldots, 1)$ without loss of generality, where k_1 is the number of 1's and k_x is the number of x*'s* with $k_1 + k_x = m$ and $x \in \mathcal{C}$. Since x cannot be obtained as a supremum of two points y and z with $y \neq x$ and $z \neq x$, the number of x's must be at least $\left\lceil \frac{k_x}{n} \right\rceil$. Indeed, for each occurrence of x each part of the partition of the vector F_x contains at least an x if they are ordered in the last k_x rows of the vertical stripe the result is obtained by using as few x's as possible. Similarly, the result can be obtained for a minimal number of 1's if it is considered that $1 \in \mathcal{C}$. That there exist $m - (m_1 + m_x)$ elements in $x_\blacktriangle$ follows from arguments used in Theorem 1. □

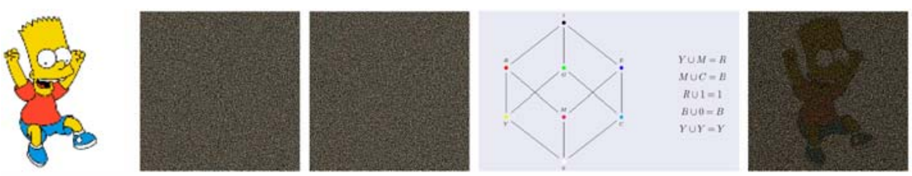

Figure 3. Example of a $(2, 2)$ lattice-based encryption. In this case, two color-shadows and an eight color-lattice are used to encrypt an original image of Bart.

We note that structure of the form $(\Gamma^i_{\text{Qual}}, \Gamma^i_{\text{Forb}})$ can be interpreted from this point of view as indecomposable lattice-color matrix representations (see Figure 4).

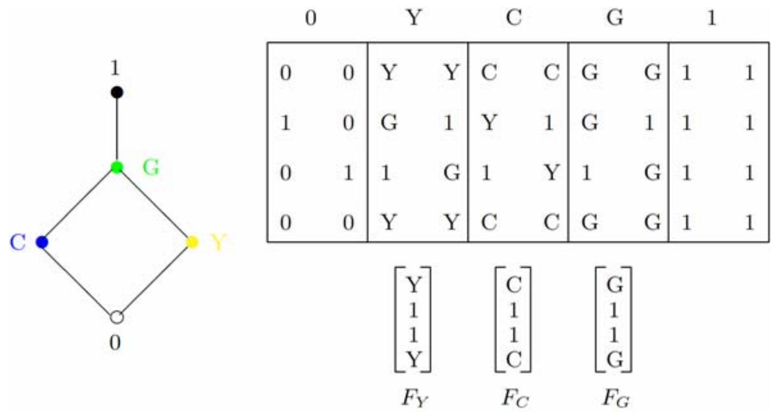

Figure 4. Example of a matrix representation induced by a $(2, 2)$ lattice-based VSSS.

4. Concluding Remarks

Lattice-based VSSS can be seen as particular cases of some matrix problems. Since permutations are part of the corresponding admissible transformations, matrix representations allow to define multiple schemes of visual cryptography.

Acknowledgment

Authors are grateful with the anonymous referee for his/her useful suggestions and comments.

References

[1] C. Blundo, A. de Santis and D. R. Stinson, On the contrast in visual cryptography schemes, J. Cryptology 12(4) (1999), 261-289.

[2] A. M. Cañadas and N. P. P. Vanegas, Extended visual cryptography scheme with an artificial cocktail party effect, IEEE Digital Library, 2011. DOI: 10.1049/ic.2011.0114.

[3] A. M. Cañadas, N. P. P. Vanegas and M. H. Quitian, Visual cryptography schemes based in *k*-linear maps, Lecture Notes in Computer Science, Vol. 8389, Springer-Verlag, 2014, pp. 288-302. doi: 10.1007/978-3-662-43886-2_21

[4] A. M. Cañadas, M. H. Quitian and N. P. Palma Vanegas, Algorithms of differentiation of posets to analyze tactics of war, Far East J. Math. Sci. (FJMS) Special Volume Part V (2013), 501-525.

[5] S. Droste, New Results on Visual Cryptography, Advances in Cryptology – CRYPTO'96, Lecture Notes in Computer Science 1109 (1998), 401-415.

[6] A. Klein and M. Wessler, Extended visual cryptography schemes, Information and Computation 205(5) (2007), 716-732.

[7] M. Nakajima and Y. Yamaguchi, Extended visual cryptography for natural images, WSCG 10(2) (2002), 303-310.

[8] M. Naor and A. Shamir, Visual cryptogrzaphy, Advances in Cryptology Eurocrypt' 94, Lecture Notes in Computer Science 950, 1995, pp. 1-12.

[9] S. Cimato and C.-N. Yang, Visual Cryptography and Secret Image Sharing, CRC Press, 2011.

[10] S.-K. Chen, A visual cryptography based system for sharing multiple secret images, Proc. 7th WSEAS Int. Conf. on Signal Processing, Computational Geometry and Artificial Vision, Athens, Greece 40, 2007, pp. 117-121.

[11] B. A. Davey and H. A. Priestley, Introduction to Lattices and Order, Cambridge University Press, 2002.

[12] A. De Santis, A. L. Ferrara and B. Masucci, Visual Cryptography Schemes with Reversing, S. Cimato and C.-N. Yang, eds., Visual Cryptography and Secret Image Sharing, CRC Press, 2011, pp. 255-278.

[13] J. B. Feng, H. C. Wu, C. S. Tsai and Y. P. Chu, A new multi-secret images sharing scheme using Lagrange's interpolation, The Journal of Systems and Software 76(3) (2005), 327-339.

[14] P. Gabriel and A. V. Roiter, Representations of Finite Dimensional Algebras, Algebra VIII, Encyclopedia of Math. Sc., Springer-Verlag, 73, 1992, pp. 177.

[15] M. Hazewinkel, N. Gubareni and V. V. Kirichenko, Algebras, Rings and Modules, First Edition, Springer 2, 2007.

[16] A. Klein and M. Wessler, Extended visual cryptography schemes, Information and Computation 205(5) (2007), 716-732.

[17] H. Koga and H. Yamamoto, Proposal of a lattice-based visual secret sharing scheme for color and gray scale images, IEICE Trans. Fundamentals E 81-A(6) (1998), 1262-1269.

[18] A. Ross and A. A. Othman, Visual Cryptography for Face Privacy, SPIE Conference on Biometrics Technology for Human Identification VII, April, 2010.

[19] B. S. W. Schröder, Ordered Sets: An Introduction, Birkhäuser, 2002.

[20] S. J. Shyu, S. Y. Huang, Y. K. Lee, R. Z. Wang and K. Cheng, Sharing multiple secrets in visual cryptography, Pattern Recognition 40 (2007), 3633-3651.

[21] D. Simson, Linear Representations of Partially Ordered Sets and Vector Space Categories, Gordon and Breach, London, 1992.

[22] C. S. Tsai, C. C. Chang and T. S. Chen, Sharing multiple secrets in digital images, Journal of Systems and Software 64(2) (2002), 163-170.

[23] C. C. Wu and L. H. Chen, A study on visual cryptography, Master Thesis, National Chiao Tung University, Taiwan, R.O.C., 1998.

[24] H. C. Wu and C.-C. Chang, Sharing visual multi-secrets using circle shares, Comput. Stand. Interfaces 134(28) (2005), 123-135.