Multimed Tools Appl (2017) 76:14511–14533
DOI 10.1007/s11042-016-3867-3

New insight into linear algebraic technique to construct visual cryptography scheme for general access structure

Gang Shen[1] · Feng Liu[2,3] · Zhengxin Fu[1] · Bin Yu[1]

Received: 23 February 2016 / Revised: 26 June 2016 / Accepted: 12 August 2016/
Published online: 22 August 2016
© Springer Science+Business Media New York 2016

Abstract The most essential advantage of applying linear algebra to construct visual cryptography scheme (VCS) lies in that it only requires solving linear equations in the construction of initial basis matrices, which are the basis matrices before removing the common columns. In this paper, we give some new insight into linear algebraic technique to construct VCS, where we can take more equations simultaneously. Then based on this knowledge, we propose a construction of VCS for general access structure. The construction is efficient in the sense that it gets the smallest initial pixel expansion compared with some well-known constructions. At the same time, by using the technique of deleting common columns from the initial basis matrices, the proposed construction achieves the optimal pixel expansions in most cases according to our experimental results. However, finding exact number of common columns in the initial basis matrices is a challenging issue. Then we deal with this issue and find out that the exact number of common columns is $n-2$ for $(2, n)$ threshold access structures. Finally, we provide some future research directions in the algebraic aspect of VCS.

Keywords Visual cryptography · Basis matrices · Linear algebra · More equations · Common columns

✉ Gang Shen
shengang_zisti@163.com

[1] Zhengzhou Information Science and Technology Institute, Zhengzhou, China

[2] State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, Beijing, China

[3] School of Cyber Security, University of Chinese Academy of Sciences, Beijing, China

1 Introduction

A (k, n) visual cryptography scheme (VCS), where $k \leq n$, for a set of n participants is a method to split a secret image into n shadow images called shares, where each participant receives one share. One can reconstruct the secret image with any k or more than k shares; but, one cannot obtain any information of the secret image from fewer than k shares. The attractiveness of VCS is the stacking-to-see property by which the reconstruction requires neither knowledge of cryptography nor a computer. Any k or more than k participants may photocopy their shares onto transparencies and stack them on an overhead projector to visually decode the secret image through the human visual system.

In some circumstances where the cost of computations may be not affordable, the decoding time should be instantly done in a constant time, or the recognition of the secret shape/pattern is sensitive or meaningful only to the human perception, VCS becomes very appropriate.

The first VCS was proposed by Naor and Shamir [14] and they gave a formal description to (k, n)-VCS. Specifically, each pixel of the secret image is encoded into m subpixels, referred to as pixel expansion, for each of the n shares by designing two collections C_0 and C_1 of $n \times m$ Boolean matrices. To share a white pixel, the dealer randomly chooses one of the matrices in C_0, and to share a black pixel, the dealer randomly chooses one of the matrices in C_1. The chosen matrix defines the color of the m subpixels in each of the shares. If any k or more shares are stacked together, our eyes can perceive the secret information due to the darkness difference, referred to as contrast, between black pixels and white pixels in the stacked result, while if fewer than k shares are superimposed it is impossible to perceive the secret information.

Following Naor and Shamir's work, many related problems of VCS, such as reducing the pixel expansion [14, 16], improving the contrast [3, 4], sharing multiple secrets [15, 24], cheating prevention [10, 12], sharing color image [5, 19], keeping aspect ratio invariant [11, 22], meaningful shares [17, 20], progress recovery [9], region incrementing [23], special access structures [2, 8] and applications [21] were subsequently proposed. Also studies have tried to sacrifice contrast to obtain less pixel expansion [6, 18]. Though VCS has a very rich literature, a very few papers have been published for the construction of VCS for general access structures, which is a specification of all qualified and forbidden sets of participants.

In 1996, Ateniese et al. [2] extended (k, n) threshold access structures to general access structures. They also introduced basis matrices, which save memory requirements, to the model of VCS and presented two techniques to construct basis matrices of VCS for general access structures: cumulative arrays and smaller schemes.

Shyu and Chen [14] applied the skills of integer linear programming (ILP) into constructing basis matrices to acquire the optimal pixel expansion of VCS for threshold access structures. Then they [16] generalized and extended the formulation of ILP to general access structures, where the optimal pixel expansions are obtained. However, the proposed method resorts to an exhaustive search strategy and takes exponential time in the worst case. Therefore, whether there is an efficient construction of VCS with near optimal pixel expansions is still a challenging topic.

Recently, Adhikari [1] proposed a linear algebraic technique to construct VCS for general access structures. He first obtained the initial basis matrices, which are the basis matrices before removing the common columns, by solving some systems of two linear equations. Then he deleted the common columns from the initial basis matrices and obtained the reduced basis matrices with less pixel expansion. This technique is more efficient than ILP

[14, 16] since it mainly requires solving some linear systems. Yet the question of finding exact number of common columns in the initial basis matrices was left open. Towards this end, Dutta et al. [7] found a closed form of the exact number of common columns in the initial basis matrices of $(n-1, n)$-VCS. However, the above works focused on constructing basis matrices by taking two equations at a time. As they pointed out, constructing basis matrices by taking more equations simultaneously to obtain less pixel expansion is worthy of study. Moreover, it is also a challenging problem that finding the exact number of common columns in the initial basis matrices for other access structures.

In this paper, we deal with the above open issues. We first put forward an efficient construction of VCS for general access structures using linear algebra, where we can take more equations at a time. Then we find out the exact number of common columns in the initial basis matrices of $(2, n)$ threshold access structures. Our main contribution is that the proposed construction, in an efficient way, gets the smallest initial pixel expansion compared to some well-known constructions and achieves the optimal pixel expansions in most cases after deleting the common columns from the initial basis matrices.

The rest of the paper is organized as follows. In Section 2 we give some preliminaries including the model of VCS for general access structures and some previous studies. In Section 3 we provide a characterization of the set of access structures on a set of participants where we can exploit the linear algebraic technique to take more equations simultaneously. In Section 4 we give an efficient construction of VCS for general access structures based on the characterization. What's more, we find the exact number of common columns in the initial basis matrices to be $n-2$ for $(2, n)$ threshold access structures. In Section 5, we discuss some interesting examples, which will lead to future research directions. Lastly we conclude the paper in Section 6.

2 Preliminaries

2.1 The model

The model that we describe here is based on basis matrices and similar to the model as described in Ateniese et al. [2].

Let $P = \{1, 2, \ldots, n\}$ be a set of participants and 2^P denote the set of all subsets of P. Let $\Gamma_{Qual} \subseteq 2^P$ and $\Gamma_{Forb} \subseteq 2^P$, where $\Gamma_{Qual} \cap \Gamma_{Forb} = \emptyset$. Members of Γ_{Qual} are referred to as qualified sets and members of Γ_{Forb} are referred to as forbidden sets. The pair $(\Gamma_{Qual}, \Gamma_{Forb})$ is called an access structure on P. A participant $p \in P$ is an essential participant if there exists a set $X \subseteq P$ such that $X \cup \{p\} \in \Gamma_{Qual}$ but $X \notin \Gamma_{Qual}$. In fact, a non-essential participant does not need to participate "actively" in the reconstruction of the image, since the information he has is not needed during recovering the secret image.

In this paper, we mostly deal with strong access structures, which are defined as follows.

Definition 1 [2] The access structure $(\Gamma_{Qual}, \Gamma_{Forb})$ on $P = \{1, 2, \ldots, n\}$ is said to be strong if the following conditions are satisfied:

1. Γ_{Qual} is monotone increasing. Formally, for each $Q \in \Gamma_{Qual}$ and $Q \subseteq Q' \subseteq P$, we have $Q' \in \Gamma_{Qual}$.
2. Γ_{Forb} is monotone decreasing. Formally, for each $F \in \Gamma_{Forb}$ and $F' \subseteq F \subseteq P$, we have $F' \in \Gamma_{Forb}$.
3. $\Gamma_{Qual} \cup \Gamma_{Forb} = 2^P$.

Let $\Gamma_0 = \{Q \in \Gamma_{Qual} : Q' \notin \Gamma_{Qual} forall Q' \subset Q\}$ be the collection of all minimal qualified sets and $Z_M = \{F \in \Gamma_{Forb} : F \cup \{i\} \in \Gamma_{Qual} foralli \in P \setminus F\}$ be the collection of all maximal forbidden sets. Γ_0 is termed a basis, which completely determines its corresponding strong access structure by $\Gamma_{Qual} = \{Q' \subseteq P : Q \subseteq Q' forsome Q \in \Gamma_0\}$.

Let M be an $n \times m$ Boolean matrix and $X \subseteq P$. Then $M[X]$ denotes the $|X| \times m$ submatrix obtained from M by considering its restriction to rows corresponding to the elements in X. M_X denotes the Boolean "OR" operation to the rows of $M[X]$. $\omega(M_X)$ denotes the Hamming weight of the row vector M_X, which is the number of 1's in the vector M_X. For a $1 \times n$ Boolean row vector $\mathbf{v} = \{v_1, v_2, \ldots, v_n\}$, let $\Re_{\mathbf{v}} = \{j | v_j = 1, j = 1, 2, \ldots, n\}$. Given two Boolean row vectors $\mathbf{v}_1$ and $\mathbf{v}_2$, define $\Re_{\mathbf{v}_1} \oplus \Re_{\mathbf{v}_2} = \Re_{\mathbf{v}_1 \oplus \mathbf{v}_2}$. Denote Γ_0^{odd} as the "$\oplus$"ed result of any odd number of elements of Γ_0 and Γ_0^{even} as the "$\oplus$"ed result of any even number of elements of Γ_0.

Definition 2 [2] Let $(\Gamma_{Qual}, \Gamma_{Forb})$ be an access structure on a set of n participants. Two $n \times m$ basis matrices S^0 and S^1, which generate the two collections of $n \times m$ Boolean matrices C_0 and C_1 by permuting the columns of the corresponding basis matrix (S^0 for C_0, and S^1 for C_1) in all possible ways, constitute a $(\Gamma_{Qual}, \Gamma_{Forb}, m)$-VCS if the following conditions are satisfied:

1. (Contrast) If $X = \{i_1, i_2, \ldots, i_p\} \in \Gamma_{Qual}$, $\omega(S_X^0) < \omega(S_X^1)$.
2. (Security) If $X = \{i_1, i_2, \ldots, i_p\} \in \Gamma_{Forb}$, the $p \times m$ matrices obtained by restricting S^0 and S^1 to rows $i_1, i_2, \ldots, i_p$ are identical up to a column permutation.

Then, for constructing VCS by cumulative arrays, the following lemma is presented by Ateniese et al. [2].

Lemma 1 [2] *For a strong access structure $(\Gamma_{Qual}, \Gamma_{Forb})$ with Z_M, there exists a VCS with $m = 2^{|Z_M|-1}$.*

Before giving the construction of VCS from smaller schemes, the following lemma is described without a proof.

Lemma 2 [2] *Let $(\Gamma'_{Qual}, \Gamma'_{Forb})$ and $(\Gamma''_{Qual}, \Gamma''_{Forb})$ be two access structures on a set P of n participants. If a participant $i \in P$ is non-essential for $(\Gamma'_{Qual}, \Gamma'_{Forb})$, we assume that $i \in \Gamma'_{Forb}$ and that i receives a share completely "white". Analogously for $(\Gamma''_{Qual}, \Gamma''_{Forb})$. Suppose there exist a $(\Gamma'_{Qual}, \Gamma'_{Forb}, m')$-VCS and a $(\Gamma''_{Qual}, \Gamma''_{Forb}, m'')$-VCS constructed using basis matrices. Then there exists a $(\Gamma'_{Qual} \cup \Gamma''_{Qual}, \Gamma'_{Forb} \cap \Gamma''_{Forb}, m' + m'')$-VCS. If the original access structures are both strong, then so is the resulted access structure.*

Based on Lemma 2, the following lemma is presented immediately.

Lemma 3 [2] *For a strong access structur $(\Gamma_{Qual}, \Gamma_{Forb})$ with Γ_0, there exists a VCS with $m = \sum_{X \in \Gamma_0} 2^{|X|-1}$.*

Furthermore, we present the following lemma, illustrating why we can delete the common columns in the initial basis matrices. In other words, if there exist two initial basis matrices having common columns, then we can delete the common columns and obtain two reduced basis matrices with less pixel expansion, where the conditions of Definition 2 are still hold.

Lemma 4 [2] *Let $(\Gamma_{Qual}, \Gamma_{Forb})$ be an access structure. Let S^0 and S^1 be the basis matrices in a $(\Gamma_{Qual}, \Gamma_{Forb}, m)$-VCS and let D be any $n \times p$ Boolean matrix. The two matrices $S'^0 = S^0 \circ D$ and $S'^1 = S^1 \circ D$, where $\circ$ denotes the operator "concatenation" of two matrices, comprise a $(\Gamma_{Qual}, \Gamma_{Forb}, m+p)$-VCS.*

2.2 VCS and linear equations

Adhikari [1] introduced a construction procedure for the two $n \times m$ basis matrices S^0 and S^1 of $(\Gamma_{Qual}, \Gamma_{Forb}, m)$-VCS using linear algebraic technique. He started with the following two associated systems of linear equations over the binary field,

$$A\mathbf{x} = \mathbf{0} \tag{1}$$
$$A\mathbf{x} = \mathbf{1} \tag{2}$$

where, A is an $r \times n$ known Boolean matrix of rank r, $0 < r < n$; $\mathbf{x}$ is an $n \times 1$ vector of unknowns; $\mathbf{0}$ and $\mathbf{1}$ are $r \times 1$ vectors of 0's and 1's respectively. Since A is full of row rank, both the systems (1) and (2) are consistent. Let S^0 (resp. S^1) be an $n \times 2^{n-r}$ Boolean matrix whose columns are all possible solutions of the system (1) (resp. (2)). Then, to show S^0 and S^1 can form the basis matrices of a $(\Gamma_{Qual}, \Gamma_{Forb}, 2^{n-r})$-VCS, he proved the following lemma which plays an important role in our new insight into the linear algebraic technique to construct visual cryptography schemes.

Lemma 5 [1] *Let $X = \{i_1, i_2, \ldots, i_p\} \subseteq P = \{1, 2, \ldots, n\}$. Then $X \in \Gamma_{Qual}$ (resp. $X \in \Gamma_{Forb}$) if and only if the system of equations*

$$\begin{pmatrix} A \\ B_X \end{pmatrix} \boldsymbol{x} = \begin{pmatrix} \boldsymbol{1} \\ \boldsymbol{0} \end{pmatrix} \tag{3}$$

is inconsistent (resp. consistent), where B_X is a column permutation of the $p \times n$ Boolean matrix $(\boldsymbol{I}_p | \boldsymbol{0}_{p \times (n-p)})$ with unit vectors of the identity matrix $\boldsymbol{I}_p$, which is of order p, occupying columns indexed by $i_1, i_2, \ldots, i_p$ in B_X.

Then based on the above knowledge, Adhikari [1] proposed a construction of VCS for any strong access structure by taking two equations simultaneously, where the pixel expansion is less than that of Lemma 3. The following lemma presents the result.

Lemma 6 [1] *For any given strong access structure $(\Gamma_{Qual}, \Gamma_{Forb})$ on a set $P = \{1, 2, \ldots, n\}$ of n participants with $\Gamma_0 = \{Q_1, Q_2, \ldots, Q_t\}$ where $Q_i \subseteq P$, $\forall i = 1, 2, \ldots, t$ and for any permutation $\sigma \in SG_t$, the symmetric group of degree t, there exists a strong $(\Gamma_{Qual}, \Gamma_{Forb})$-VCS with m_σ, where m_σ is given as follows:*

$$m_\sigma = \begin{cases} \sum_{i=1}^{l} 2^{|Q_{\sigma(2i-1)} \cup Q_{\sigma(2i)}|-2} & if t = 2l, l \geq 1 \\ \sum_{i=1}^{l} 2^{|Q_{\sigma(2i-1)} \cup Q_{\sigma(2i)}|-2} + 2^{|Q_{\sigma(2l+1)}|-1} & if t = 2l+1, l \geq 0. \end{cases}$$

3 New insight into linear algebraic technique to construct VCS

In this section, we give some new insight into the linear algebraic technique to construct VCS, where we can take more equations simultaneously to reduce the pixel expansion. First, we also start with the following two systems of linear equations over the binary field,

$$A\mathbf{x} = \mathbf{0} \tag{4}$$

$$A\mathbf{x} = \mathbf{1} \tag{5}$$

where, A is a $t \times n$ known Boolean matrix of rank r, $0 < r \leq t < n$; $\mathbf{x}$ is an $n \times 1$ vector of unknowns; $\mathbf{0}$ and $\mathbf{1}$ are $t \times 1$ vectors of 0's and 1's respectively; both the systems (4) and (5) are consistent. The difference from Adhikari's systems [1] is the coefficient matrix A, which does not have to be of full row rank.

Also, let S^0 (resp. S^1) be an $n \times 2^{n-r}$ Boolean matrix whose columns are all possible solutions of the system (4) (resp. (5)). Then, to prove S^0 and S^1 can form the basis matrices of a $(\Gamma_{Qual}, \Gamma_{Forb}, 2^{n-r})$-VCS, the following lemma is immediate since the proof of Lemma 5 also works for this lemma.

Lemma 7 *Let $X = \{i_1, i_2, \ldots, i_p\} \subseteq P = \{1, 2, \ldots, n\}$. Build a system of equations as follows:*

$$\begin{pmatrix} A \\ B^X \end{pmatrix} \boldsymbol{x} = \begin{pmatrix} \boldsymbol{1} \\ \boldsymbol{0} \end{pmatrix} \tag{6}$$

where B^X is a column permutation of the $p \times n$ Boolean matrix $(\boldsymbol{I}_p | \boldsymbol{0}_{p\times(n-p)})$ with unit vectors of the identity matrix $\boldsymbol{I}_p$, which is of order p, occupying columns indexed by $i_1, i_2, \ldots, i_p$ in B^X. Then, for an access structure $(\Gamma_{Qual}, \Gamma_{Forb})$, S^0 and S^1 form the basis matrices of a $(\Gamma_{Qual}, \Gamma_{Forb}, m = 2^{n-r})$-OVCS if the following conditions are satisfied:

1. *For $X \in \Gamma_{Qual}$, the system (6) is inconsistent;*
2. *For $X \in \Gamma_{Forb}$, the system (6) is consistent.*

Next we are going to explore the conditions for consistency or inconsistency of the system (6). Let rows of A_1 (resp. A_2) represent all possible sum of odd (resp. even) number of rows in A. Then we have the following lemma.

Lemma 8 *For an access structure $(\Gamma_{Qual}, \Gamma_{Forb})$, S^0 and S^1 form the basis matrices of a $(\Gamma_{Qual}, \Gamma_{Forb}, m = 2^{n-r})$-OVCS if the following conditions are satisfied:*

1. *For $X \in \Gamma_{Qual}$, any row vector of A_1 belongs to the row space of B^X.*
2. *For $X \in \Gamma_{Forb}$, A and B^X are independent, or, any row vector of A_2 belongs to the row space of B^X.*

Proof In light of the system (6), there are two possibilities: the coefficient matrix A and B^X are either linearly independent or linearly dependent.

If they are independent, since the system (5) is consistent and $B^X\mathbf{x} = \mathbf{0}$ is consistent (B^X is of full row rank), the system (6) is consistent.

If they are linearly dependent, then there exists a vector $\mathbf{u} = (\mathbf{u}_1, \mathbf{u}_2) \neq \mathbf{0}$, where $\mathbf{u}_1$ and $\mathbf{u}_2$ are $1 \times t$ and $1 \times p$ vectors respectively, such that $\mathbf{u}\begin{pmatrix} A \\ B^X \end{pmatrix} = \mathbf{0} \Leftrightarrow \mathbf{u}_1 A + \mathbf{u}_2 B^X = \mathbf{0}$.

Note that $\mathbf{u}_1$ is nonzero, otherwise this will imply linear dependence of the rows of B^X. Now $\mathbf{u}_1 A + \mathbf{u}_2 B^X = \mathbf{0} \Leftrightarrow \mathbf{u}_1 A \in$ the row space of B^X. Also note that if $\mathbf{u}_1$ has an odd (resp. even) number of 1's then $\mathbf{u}_1 A$ will be a row of A_1 (resp. A_2). Then we have that any row of A_1 or A_2 belongs to the row space of B^X. On the right of the system (6), $\mathbf{u}\begin{pmatrix}\mathbf{1}\\ \mathbf{0}\end{pmatrix} = \mathbf{u}_1\mathbf{1}$. If $\mathbf{u}_1$ has an odd (resp. even) number of 1's then the system (6) is inconsistent (resp. consistent).

Based on the above discussions and Lemma 7, this lemma is proved. □

Until now, we have seen that given a suitable binary matrix A and a suitable access structure $(\Gamma_{Qual}, \Gamma_{Forb})$, which satisfy the conditions of Lemma 8, we can construct a VCS by solving the two systems (4) and (5). In other words, we have concluded the sufficient conditions for constructing VCS by using linear equations. Then, we are now in a position to give a concrete structure of the coefficient matrix A. Towards this end, we prove the following lemma.

Lemma 9 *For an access structure $(\Gamma_{Qual}, \Gamma_{Forb})$ with $\Gamma_0 = \{Q_1, Q_2, \ldots, Q_t\}$, let $A = (\boldsymbol{v}_1, \boldsymbol{v}_2, \ldots, \boldsymbol{v}_t)^T$ of rank r and $\Re_{\boldsymbol{v}_i} = Q_i$, $i = 1, 2, \ldots, t$. S^0 and S^1 form the basis matrices of a $(\Gamma_{Qual}, \Gamma_{Forb}, m = 2^{n-r})$-OVCS if the following conditions are satisfied:*

1. *For any row $\boldsymbol{v}$ of A_1, $\Re_{\boldsymbol{v}} \in \Gamma_{Qual}$;*
2. *For any row $\boldsymbol{v}$ of A_2, $\Re_{\boldsymbol{v}} = \emptyset$ or $\Re_{\boldsymbol{v}} \not\subseteq Q \in \Gamma_0$.*

Proof For $X \in \Gamma_{Qual}$, because $\Re_{\mathbf{v}} \in \Gamma_{Qual}$ for any row $\mathbf{v}$ of A_1, $\mathbf{v}$ obviously belongs to the row space of B^X.

For $X \in \Gamma_{Forb}$, there are three cases to be considered:

Case 1 For any row $\mathbf{v}$ of A_1, $\Re_{\mathbf{v}} \in \Gamma_{Qual}$; for any row $\mathbf{v}$ of A_2, $\Re_{\mathbf{v}} = \emptyset$.

In this case, any row vector of A_2 belongs to the row space of B^X immediately.

Case 2 For any row $\mathbf{v}$ of A_1, $\Re_{\mathbf{v}} \in \Gamma_{Qual}$; for any row $\mathbf{v}$ of A_2, $\Re_{\mathbf{v}} \not\subset Q \in \Gamma_0$ and $\Re_{\mathbf{v}} \in \Gamma_{Forb}$.

In this case, any row vector of A_2 also belongs to the row space of B^X immediately.

Case 3 For any row $\mathbf{v}$ of A_1, $\Re_{\mathbf{v}} \in \Gamma_{Qual}$; for any row $\mathbf{v}$ of A_2, $\Re_{\mathbf{v}} \notin \Gamma_0$ and $\Re_{\mathbf{v}} \in \Gamma_{Qual}$.

In this case, no row vector of A_1 and A_2 belongs to the row space of B^X, namely, A and B^X are independent. □

It should be noted that the sum operation "+" over the binary field is actually the Boolean XOR operation "⊕". Therefore, the sum of a number of row vectors, say $\mathbf{v}_1, \cdots, \mathbf{v}_i$, of the coefficient matrix A equals to $\mathbf{v}_1 \oplus \cdots \oplus \mathbf{v}_i$. Since $Q_i = \Re_{\mathbf{v}_i}$, we have $\Re_{\mathbf{v}_1 \oplus \cdots \oplus \mathbf{v}_i} = Q_1 \oplus \cdots \oplus Q_i$. So, for clarity, we restate Lemma 9 as follows, and hence omit its proof.

Theorem 1 *For an access structure $(\Gamma_{Qual}, \Gamma_{Forb})$ with $\Gamma_0 = \{Q_1, Q_2, \ldots, Q_t\}$, if Γ_0 satisfies the following two conditions:*

1. *The "⊕"ed result of any odd number of elements of Γ_0 is an element of Γ_{Qual}. Formally, $\Gamma_0^{odd} \in \Gamma_{Qual}$.*
2. *The "⊕"ed result of any even number of elements of Γ_0 is an empty set, or not a subset of any element of Γ_0. Formally, $\Gamma_0^{even} = \emptyset$ or $\Gamma_0^{even} \not\subseteq Q \in \Gamma_0$.*

Then the basis matrices S^0 and S^1 of a $(\Gamma_{Qual}, \Gamma_{Forb}, m = 2^{n-r})$-OVCS are composed of all possible solutions of the systems (4) *and* (5) *respectively, where $A = (\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_t)^T$ of rank r and $\Re_{\mathbf{v}_i} = Q_i$, $i = 1, 2, \ldots, t$.*

Remark 1 Theorem 1 helps us to prove Lemma 3 on the existence of a VCS for any given strong access structure with the basis Γ_0, since we can construct a VCS by taking one equation at a time regarding each element, satisfying the conditions of Theorem 1 obviously, of Γ_0. Analogously for Lemma 6 since we can construct a VCS by taking two equation at a time regarding any two elements, satisfying the conditions of Theorem 1 obviously, of Γ_0. Therefore, our Theorem 1 is a generalization of Lemma 3 and Lemma 6.

Let us try to illustrate the above theory through the following example.

Example 1 Consider the following strong access structure $(\Gamma_{Qual}, \Gamma_{Forb})$ on a set of four participants having $\Gamma_0 = \{\{1, 2\}, \{1, 3\}, \{1, 4\}\}$. Obviously, this access structure satisfies the conditions of Theorem 1. Then we can construct a $(\Gamma_{Qual}, \Gamma_{Forb})$-VCS with basis matrices S^0 and S^1, which are obtained by solving the following two systems of three linear equations over the binary field:

$$\begin{cases} x_1 + x_2 = 0 \\ x_1 + x_3 = 0 \\ x_1 + x_4 = 0 \end{cases} \tag{7}$$

and

$$\begin{cases} x_1 + x_2 = 1 \\ x_1 + x_3 = 1 \\ x_1 + x_4 = 1 \end{cases} \tag{8}$$

Let S^0 and S^1 be the Boolean matrices whose columns are just all possible solutions of (7) and (8), respectively. Thus, $S^0 = \begin{bmatrix} 0 & 1 \\ 0 & 1 \\ 0 & 1 \\ 0 & 1 \end{bmatrix}$ and $S^1 = \begin{bmatrix} 0 & 1 \\ 1 & 0 \\ 1 & 0 \\ 1 & 0 \end{bmatrix}$. Clearly, S^0 and S^1 satisfy the properties of basis matrices for the strong access structure $(\Gamma_{Qual}, \Gamma_{Forb})$ determined by Γ_0. It gives pixel expansion 2, which is less than pixel expansion 4 obtained by taking two equations simultaneously as proposed by Theorem 4.2 of [1] (described in Appendix A).

4 On construction of VCS for general access structures

In this section, we give a construction of VCS for any strong access structure to obtain less pixel expansion. To begin with, the following definition is presented.

Definition 3 A strong access structure $(\Gamma_{Qual}, \Gamma_{Forb})$ is called feasible if it satisfies the conditions of Theorem 1. The Γ_0 obtained from the feasible $(\Gamma_{Qual}, \Gamma_{Forb})$ is called a feasible basis.

Obviously, for any given strong access structure, the conditions of Theorem 1 are not always satisfied. A comprehensive idea to construct a VCS for any given strong access structure is to group the access structure into some feasible access structures, and then to realize a VCS by Lemma 2. We are now in a position to describe such a grouping algorithm.

Then, we need to give a sorting method for a basis Γ_0. For a $1 \times n$ Boolean row vector $\mathbf{v}_i$, define $Dec_{\mathbf{v}_i}$ as the decimal number corresponding to $\mathbf{v}_i$, then a sorting method for a basis Γ_0 is defined as follows.

Definition 4 A basis Γ_0 is sorted such that for any two different elements $Q_i, Q_{i'} \in \Gamma_0$, if $i < i'$, then $Dec_{\mathbf{v}_i} < Dec_{\mathbf{v}_{i'}}$, where $\Re_{\mathbf{v}_i} = Q_i$ and $\Re_{\mathbf{v}_{i'}} = Q_{i'}$.

Then, we describe a grouping algorithm for any strong access structure in Algorithm 1. Note that Steps 2–8 guarantee that each of $\Gamma_0^1, \Gamma_0^2, \ldots, \Gamma_0^d$ is feasible since the conditions of Theorem 1 are satisfied.

Algorithm 1 Grouping algorithm for general access structure.

```
Require:
 1: $\Gamma_0$ obtained from any given $(\Gamma_{Qual}, \Gamma_{Forb})$;
Ensure:
 2: Feasible bases $\Gamma_0^1, \Gamma_0^2, \ldots, \Gamma_0^d$;
 3: Initially set a counting variable $l = 1$;
 4: Sort the basis $\Gamma_0$ and assign two sets $Q = F = \emptyset$.
 5: Select and delete the first element $X$ from $\Gamma_0$, and put $X$ into the set $Q$;
 6: If $\Gamma_0 \neq \emptyset$, select the next element $Y$ of $\Gamma_0$ in sequence and put $Y$ into the set $Q$; else
    go to the step 10;
 7: For the "$\oplus$"ed result $Z_o$ of any odd number of elements of $Q$, if $Z_o \in \Gamma_0$, put $Z_o$ into
    $Q$;
 8: If $Q$ does not satisfy the conditions of Theorem , delete $Y$, $Z_o$ from $Q$, delete $Y$ from
    $\Gamma_0$, and put $Y$ into $F$;
 9: For the "$\oplus$"ed result $Z_e$ of any even number of elements of $Q$, if $Z_e \in \Gamma_0$, delete $Z_e$
    from $\Gamma_0$, put $Z_e$ into $F$, and then go to the step 6;
10: Assign $\Gamma_0^l = Q$.
11: If $F \neq \emptyset$, $\Gamma_0 = F$, $l = l + 1$, and then go to the step 4;
12: If $F = \emptyset$, $d = l$; return $\Gamma_0^1, \Gamma_0^2, \ldots, \Gamma_0^d$;
```

For any given strong access structure, we can apply Algorithm 1 to group the access structure and construct a VCS for each feasible access structure based on Theorem 1, and then realize a final VCS by Lemma 2. Let us try to illustrate the proposed algorithm through the following example.

Example 2 Consider the following strong access structure $(\Gamma_{Qual}, \Gamma_{Forb})$ on a set of four participants having $\Gamma_0 = \{\{1, 2\}, \{1, 3\}, \{2, 3\}, \{1, 4\}\}$. Obviously, this access structure is not feasible. By Algorithm 1, we can obtain the following two feasible bases $\Gamma_0^1 = \{\{1, 2\}, \{1, 3\}, \{1, 4\}\}$ and $\Gamma_0^2 = \{\{2, 3\}\}$. For Γ_0^1, consider the following two systems of three linear equations over the binary field:

$$\begin{cases} x_1 + x_2 = 0 \\ x_1 + x_3 = 0 \\ x_1 + x_4 = 0 \end{cases} \tag{9}$$

and

$$\begin{cases} x_1 + x_2 = 1 \\ x_1 + x_3 = 1 \\ x_1 + x_4 = 1 \end{cases} \tag{10}$$

Let S_1^0 and S_1^1 be the Boolean matrices whose columns are just all possible solutions of the above two systems (9) and (10), respectively. Thus, $S_1^0 = \begin{bmatrix} 0 & 1 \\ 0 & 1 \\ 0 & 1 \\ 0 & 1 \end{bmatrix}$ and $S_1^1 = \begin{bmatrix} 0 & 1 \\ 1 & 0 \\ 1 & 0 \\ 1 & 0 \end{bmatrix}$.

For Γ_0^2, let us consider the two following systems of one linear equation over the binary field:

$$x_2 + x_3 = 0 \tag{11}$$

and

$$x_2 + x_3 = 1 \tag{12}$$

Let S_2^0 and S_2^1 be the Boolean matrices whose columns are just all possible solutions of the above two linear systems (11) and (12), respectively. Thus, $S_2^0 = \begin{bmatrix} 0 & 0 \\ 0 & 1 \\ 0 & 1 \\ 0 & 0 \end{bmatrix}$ and $S_2^1 = \begin{bmatrix} 0 & 0 \\ 0 & 1 \\ 1 & 0 \\ 0 & 0 \end{bmatrix}$. Note that the first and fourth participants are non-essential for the strong access structure determined by Γ_0^2, so we assign both of them the values (00) for the two Boolean matrices.

Finally, by Lemma 2 we construct a $(\Gamma_{Qual}, \Gamma_{Forb})$-VCS on a set of four participants having $\Gamma_0 = \{\{1, 2\}, \{1, 3\}, \{2, 3\}, \{1, 4\}\}$, where the basis matrices $S^0 = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 \end{bmatrix}$ and $S^1 = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 \end{bmatrix}$.

Remark 2 Based on Theorem 1, Algorithm 1 groups any given strong access structure so that we can take more than two equations simultaneously to obtain the basis matrices. In Example 2, we obtain the pixel expansion 4, which is less than the pixel expansion 5 obtained by taking $\Gamma_0^1 = \{\{1, 2\}, \{1, 3\}\}$ and $\Gamma_0^2 = \{\{2, 3\}, \{1, 4\}\}$ according to Lemma 6 (described in Appendix B). Moreover, in Lemma 6, the role of σ is very important for the reduction of pixel expansion. Different σ may give rise to different pixel expansion. For example, if we take $\Gamma_0^1 = \{\{1, 2\}, \{2, 3\}\}$ and $\Gamma_0^2 = \{\{1, 3\}, \{1, 4\}\}$ (described in Appendix C), then the pixel expansion will be 4, which is the same as ours. Therefore, our construction is more efficient than Lemma 6.

4.1 Finding common columns of (2, n)-VCS

Though there are many dedicated nice constructions available for the (2, n)-VCS which even achieve the optimal pixel expansion, in this subsection we are going to provide an efficient construction of (2, n)-VCS, which comes as a direct consequence of Algorithm 1, by finding the exact number of common columns in the initial basis matrices.

Algorithm 2 Grouping algorithm for (2, n) threshold access structure.

```
Require:
1: $\Gamma_0 = \{X \subseteq P : |X| = 2\}$;
Ensure:
2: $n - 1$ feasible bases $\Gamma_0^1, \Gamma_0^2, \ldots, \Gamma_0^{n-1}$;
3: Initially set $n - 1$ sets $\Gamma_0^1 = \Gamma_0^2 = \cdots = \Gamma_0^{n-1} = \emptyset$ and a counting variable $l = 1$;
4: Put the $n - l$ subsets $\{l, l + 1\}, \{l, l + 2\}, \ldots, \{l, n - 1\}, \{l, n\}$ into the set $\Gamma_0^l$;
5: Assign $l = l + 1$;
6: If $l \neq n$, go to the step 4; return $\Gamma_0^1, \Gamma_0^2, \ldots, \Gamma_0^{n-1}$;
```

Let us apply Algorithm 1 to $(2, n)$ threshold access structure, then Algorithm 1 is reduced to a simple grouping algorithm for (2, n) threshold access structure, which is illustrated in Algorithm 2. Note that, for any basis Γ_0^l of Algorithm 2, $l = 1, 2, \ldots, n - 1$, there are a total of $n - l$ elements and they have a common participant l. The "$\oplus$"ed result of any odd number of elements of Γ_0^l consists a common participant l and an odd number of participants of $\{l + 1, l + 2, \ldots, n\}$, so the first condition of Theorem 1 is met. The "$\oplus$"ed result of any even number of elements of Γ_0^l is an even number of participants of $\{l + 1, l + 2, \ldots, n\}$, so the second condition of Theorem 1 is met. Then, we have the following lemma.

Lemma 10 *For (2, n)-VCS on a set* $P = \{1, 2, \ldots, n\}$ *of n participants with* $\Gamma_0 = \{X \subseteq P : |X| = 2\}$*, there exists a strong (2, n)-VCS with* $m_{ini} = 2(n - 1)$.

Proof By Algorithm 2, we can group (2, n) threshold access structures into $n - 1$ feasible bases $\Gamma_0^1, \Gamma_0^2, \ldots, \Gamma_0^{n-1}$. The number of elements of Γ_0^l is $n - l$, $l = 1, 2, \ldots, n - 1$. For any Γ_0^l, its set of participants is $\{l, l + 1, \ldots, n\}$, and then there exists a VCS on it with $m = 2^{n-l+1-(n-l)} = 2$ by Theorem 1. Since there are $n - 1$ feasible bases, there exists a strong (2, n)-VCS with $m_{ini} = 2(n - 1)$ by Lemma 2. □

In Lemma 10, m_{ini} denotes the initial pixel expansion obtained without deleting the common columns in the initial basis matrices of (2, n)-VCS. Hence, we need to find the exact number of common columns and obtain the reduced basis matrices with less pixel expansion. We are now going to determine the exact number of common columns occurring in the initial basis matrices for different feasible bases and find the exact value of the reduced pixel expansion of the scheme. Towards finding the results, let us explore the structure of initial basis matrices of the (2, n)-VCS constructed by our linear algebraic method.

For any feasible basis Γ_0^l output by Algorithm 2, $l = 1, 2, \ldots, n-1$, let us consider the following two systems of $n - l$ linear equations over the binary field:

$$\begin{cases} x_l + x_{l+1} = 0 \\ x_l + x_{l+2} = 0 \\ \vdots \\ x_l + x_{n-1} = 0 \\ x_l + x_n = 0 \end{cases} \tag{13}$$

and

$$\begin{cases} x_l + x_{l+1} = 1 \\ x_l + x_{l+2} = 1 \\ \vdots \\ x_l + x_{n-1} = 1 \\ x_l + x_n = 1 \end{cases} \tag{14}$$

Let S_l^0 and S_l^1 be the Boolean matrices whose columns are just all possible solutions of the above two systems (13) and (14) respectively. Thus,

$$S_l^0 = \begin{array}{cc} \begin{bmatrix} 0 & 0 \\ \vdots & \\ 0 & 0 \\ 0 & 1 \\ 0 & 1 \\ \vdots & \\ 0 & 1 \end{bmatrix} & \begin{array}{c} x_1 \\ \vdots \\ x_{l-1} \\ x_l \\ x_{l+1} \\ \vdots \\ x_n \end{array} \end{array} \text{ and } S_l^1 = \begin{array}{cc} \begin{bmatrix} 0 & 0 \\ \vdots & \\ 0 & 0 \\ 0 & 1 \\ 1 & 0 \\ \vdots & \\ 1 & 0 \end{bmatrix} & \begin{array}{c} x_1 \\ \vdots \\ x_{l-1} \\ x_l \\ x_{l+1} \\ \vdots \\ x_n \end{array} \end{array}.$$

Note that the participants $\{1, 2, \ldots, l-1\}$ is non-essential for the strong access structure determined by Γ_0^l, so we assign all of them the values (00).

Finally, by Lemma 2 we construct (2, n)-VCS with the initial basis matrices $S^0 = S_1^0 \circ S_2^0 \circ \cdots \circ S_{n-1}^0$ and $S^1 = S_1^1 \circ S_2^1 \circ \cdots \circ S_{n-1}^1$. Obviously, there exists one common column $\begin{array}{ccccccc} (0 & \cdots & 0 & 0 & 1 & \cdots & 1)^T \\ x_1 & \cdots & x_{1-1} & x_1 & x_{1+1} & \cdots & x_n \end{array}$ in the two matrices S_l^1 and S_{l+1}^0. As a result, there exist $n-2$ common columns in the initial basis matrices S^0 and S^1.

So, based on the above discussions and Lemma 10, the following theorem is given immediately to obtain the reduced pixel expansion m_{red}.

Theorem 2 *For (2, n)-VCS on a set* $P = \{1, 2, \ldots, n\}$ *of n participants with* $\Gamma_0 = \{X \subseteq P : |X| = 2\}$*, there exists a strong (2, n)-VCS with* $m_{red} = n$.

4.2 Comparison of pixel expansion between our construction and some well-known constructions

We deal with any strong access structures by taking more equations at a time. In [1] the author pointed out [Remark 4, Sect. 3] that one may take more than two equations at a time to reduce pixel expansion. In this subsection we will show that our construction, where more equations are taken at a time, can get the smallest initial pixel expansion compared to some well-known constructions. At the same time, by using the technique of deleting the common columns from the initial basis matrices, it can also achieve the optimal pixel expansions in most cases according to our experimental results.

Tables 1 and 2 summarize the comparisons of pixel expansion, including initial pixel expansion and reduced pixel expansion, between our construction and some well-known constructions for different access structures with up to four participants. In Table 1, m_{ini} stands for the initial pixel expansion of our construction, m_{ini}^{A} denotes the initial pixel expansion obtained by taking two equations simultaneously of [1], m_{ini}^{CA} denotes the initial pixel expansion obtained by cumulative arrays of [2], m_{ini}^{SS} denotes the initial pixel expansion obtained by smaller schemes of [2]. In Table 2, m_{red} stands for the reduced pixel expansion of our construction, m_{red}^{A} denotes the reduced pixel expansion obtained by taking two equations simultaneously of [1], m_{red}^{CA} denotes the reduced pixel expansion by cumulative arrays of [2], m_{red}^{SS} denotes the reduced pixel expansion by smaller schemes of [2], m^{ILP} denotes the optimal pixel expansion by ILP of [14, 16]. Table 3 lists the reduced pixel expansions of our (k, n)-VCS for $2 \leq k \leq n \leq 8$, where the optimal pixel expansions by ILP of [14, 16] are given in parentheses.

From Table 1, it is easy to see that our construction gets the smallest initial pixel expansion compared to some well-known constructions. From Tables 2 and 3, we conclude that the proposed construction achieves the optimal pixel expansions in most cases after deleting the common columns from the initial basis matrices.

5 Open problems

In Table 2, our proposed construction for four access structures ($\Gamma_0 = \{\{1, 2\}, \{1, 3\}, \{2, 3\}, \{1, 4\}\}$, $\Gamma_0 = \{\{1, 2\}, \{1, 3\}, \{1, 4\}, \{2, 3, 4\}\}$, $\Gamma_0 = \{\{1, 2\}, \{1, 3\}, \{2, 4\}\}$, $\Gamma_0 = \{\{1, 2\}, \{1, 3, 4\}, \{2, 3, 4\}\}$) does not achieve the optimal pixel expansion. In this section, based on Theorem 1 we are going to present constructions case by case and finally achieve the optimal pixel expansions for the above four access structures.

Example 3 Let us start with the strong access structure $(\Gamma_{Qual}, \Gamma_{Forb})$ with $\Gamma_0 = \{\{1, 2\}, \{1, 3\}, \{2, 3\}, \{1, 4\}\}$. Apply Algorithm 1 to group the collection Γ_0 into two collections, namely $\Gamma_0^1 = \{\{1, 2\}, \{1, 3\}, \{1, 4\}\}$ and $\Gamma_0^2 = \{\{2, 3\}\}$. After this grouping operation, we construct the initial basis matrices for Γ_0^1 just like Example 2, and hence $S_1^0 = \begin{bmatrix} 0 & 1 \\ 0 & 1 \\ 0 & 1 \\ 0 & 1 \end{bmatrix}$ and $S_1^1 = \begin{bmatrix} 0 & 1 \\ 1 & 0 \\ 1 & 0 \\ 1 & 0 \end{bmatrix}$. For Γ_0^2, the first and fourth participants are non-essential. Different from Example 2, we assign the first participant the values (11) and the fourth participant the values (00). Thus, $S_2^0 = \begin{bmatrix} 1 & 1 \\ 0 & 1 \\ 0 & 1 \\ 0 & 0 \end{bmatrix}$ and $S_2^1 = \begin{bmatrix} 1 & 1 \\ 0 & 1 \\ 1 & 0 \\ 0 & 0 \end{bmatrix}$. Finally, by concatenating the initial basis matrices respectively, we construct a $(\Gamma_{Qual}, \Gamma_{Forb})$-VCS with

Table 1 Comparison of initial pixel expansion between our construction and some well-known constructions for different access structures having four participants at most

n	Γ_0	Z_M	m_{ini}	m_{ini}^{A}	m_{ini}^{CA}	m_{ini}^{SS}
3	$\{\{1,2\},\{1,3\}\}$	$\{\{1\},\{2,3\}\}$	2	2	2	4
	$\{\{1,2\},\{1,3\},\{2,3\}\}$	$\{\{1\},\{2\},\{3\}\}$	4	4	4	6
	$\{\{1,2,3\}\}$	$\{\{1,2\},\{1,3\},\{2,3\}\}$	4	4	4	4
4	$\{\{1,2\},\{1,3\},\{2,3\},\{1,4\}\}$	$\{\{1\},\{2,4\},\{3,4\}\}$	4	6	4	8
	$\{\{1,2\},\{1,3\},\{2,3\},\{1,4\},\{2,4\}\}$	$\{\{1\},\{2\},\{3,4\}\}$	4	8	4	10
	$\{\{1,2\},\{1,3\},\{2,3\},\{1,4\},\{2,4\},\{3,4\}\}$	$\{\{1\},\{2\},\{3\},\{4\}\}$	6	8	8	12
	$\{\{1,2\},\{1,3\},\{1,4\}\}$	$\{\{1\},\{2,3,4\}\}$	2	4	2	6
	$\{\{1,2\},\{1,3\},\{1,4\},\{2,3,4\}\}$	$\{\{1\},\{2,3\},\{2,4\},\{3,4\}\}$	6	6	8	10
	$\{\{1,2\},\{1,3\},\{2,4\}\}$	$\{\{2,3\},\{1,4\},\{3,4\}\}$	4	4	4	6
	$\{\{1,2\},\{1,3\},\{2,4\},\{3,4\}\}$	$\{\{2,3\},\{1,4\}\}$	2	4	2	8
	$\{\{1,2\},\{1,3\},\{2,3,4\}\}$	$\{\{2,3\},\{1,4\},\{2,4\},\{3,4\}\}$	6	6	8	8
	$\{\{1,2\},\{3,4\}\}$	$\{\{1,3\},\{2,3\},\{1,4\},\{2,4\}\}$	4	4	8	4
	$\{\{1,2\},\{1,3,4\}\}$	$\{\{1,3\},\{1,4\},\{2,3,4\}\}$	4	4	4	6
	$\{\{1,2\},\{1,3,4\},\{2,3,4\}\}$	$\{\{1,3\},\{2,3\},\{1,4\},\{2,4\},\{3,4\}\}$	8	8	16	10
	$\{\{1,2,3\},\{1,2,4\}\}$	$\{\{1,2\},\{1,3,4\},\{2,3,4\}\}$	4	4	4	8
	$\{\{1,2,3\},\{1,2,4\},\{1,3,4\}\}$	$\{\{1,2\},\{1,3\},\{1,4\},\{2,3,4\}\}$	8	8	8	12
	$\{\{1,2,3\},\{1,2,4\},\{1,3,4\},\{2,3,4\}\}$	$\{\{1,2\},\{1,3\},\{2,3\},\{1,4\},\{2,4\},\{3,4\}\}$	8	8	32	16
	$\{\{1,2,3,4\}\}$	$\{\{1,2,3\},\{1,2,4\},\{1,3,4\},\{2,3,4\}\}$	8	8	8	8

$\Gamma_0 = \{\{1,2\},\{1,3\},\{2,3\},\{1,4\}\}$, where the basis matrices are $S^0 = \begin{bmatrix} 0&1&1&1\\ 0&1&0&1\\ 0&1&0&1\\ 0&1&0&0 \end{bmatrix}$ and $S^1 = \begin{bmatrix} 0&1&1&1\\ 1&0&0&1\\ 1&0&1&0\\ 1&0&0&0 \end{bmatrix}$. By deleting the common column $(1000)^T$ from the initial basis matrices S^0 and S^1, we obtain the optimal pixel expansion 3.

Table 2 Comparison of reduced pixel expansion between our construction and some well-known constructions for different access structures having four participants at most

n	Γ_0	Z_M	m_{red}	m^{A}_{red}	m^{CA}_{red}	m^{SS}_{red}	m^{ILP}
3	{{1, 2}, {1, 3}}	{{1}, {2, 3}}	2	2	2	4	2
	{{1, 2}, {1, 3}, {2, 3}}	{{1}, {2}, {3}}	3	3	3	6	3
	{{1, 2, 3}}	{{1, 2}, {1, 3}, {2, 3}}	4	4	4	4	4
4	{1, 2}, {1, 3}, {2, 3}, {1, 4}	{{1}, {2, 4}, {3, 4}}	4	5	3	8	3
	{1, 2}, {1, 3}, {2, 3}, {1, 4}, {2, 4}	{{1}, {2}, {3, 4}}	3	6	3	10	3
	{1, 2}, {1, 3}, {2, 3}, {1, 4}, {2, 4}, {3, 4}	{{1}, {2}, {3}, {4}}	4	7	4	12	4
	{{1, 2}, {1, 3}, {1, 4}}	{{1}, {2, 3, 4}}	2	4	2	6	2
	{1, 2}, {1, 3}, {1, 4}, {2, 3, 4}	{1}, {2, 3}, {2, 4}, {3, 4}	6	5	4	10	4
	{{1, 2}, {1, 3}, {2, 4}}	{{2, 3}, {1, 4}, {3, 4}}	4	4	3	6	3
	{1, 2}, {1, 3}, {2, 4}, {3, 4}	{{2,3},{1,4}}	2	4	2	8	2
	{1, 2}, {1, 3}, {2, 3, 4}	{2, 3}, {1, 4}, {2, 4}, {3, 4}	5	5	5	8	5
	{{1, 2}, {3, 4}}	{1, 3}, {2, 3}, {1, 4}, {2, 4}	4	4	5	4	4
	{{1, 2}, {1, 3, 4}}	{1, 3}, {1, 4}, {2, 3, 4}	4	4	4	6	4
	{1, 2}, {1, 3, 4}, {2, 3, 4}	{1, 3}, {2, 3}, {1, 4}, {2, 4}, {3, 4}	6	6	7	10	5
	{{1, 2, 3}, {1, 2, 4}}	{1, 2}, {1, 3, 4}, {2, 3, 4}	4	4	4	8	4
	{1, 2, 3}, {1, 2, 4}, {1, 3, 4}	{1, 2}, {1, 3}, {1, 4}, {2, 3, 4}	6	6	6	12	6
	{1, 2, 3}, {1, 2, 4}, {1, 3, 4}, {2, 3, 4}	{1, 2}, {1, 3}, {2, 3}, {1, 4}, {2, 4}, {3, 4}	6	6	9	16	6
	{{1, 2, 3, 4}}	{1, 2, 3}, {1, 2, 4}, {1, 3, 4}, {2, 3, 4}	8	8	8	8	8

Example 4 For the strong access structure $(\Gamma_{Qual}, \Gamma_{Forb})$ with $\Gamma_0 = \{\{1, 2\}, \{1, 3\}, \{1, 4\}, \{2, 3, 4\}\}$, apply Algorithm 1 to group the collection Γ_0 into two collections, namely $\Gamma_0^1 = \{\{1, 2\}, \{1, 3\}, \{1, 4\}\}$ and $\Gamma_0^2 = \{\{2, 3, 4\}\}$. We can construct the initial basis matrices for Γ_0^1 like Example 2, and hence $S_1^0 = \begin{bmatrix} 0 & 1 \\ 0 & 1 \\ 0 & 1 \\ 0 & 1 \end{bmatrix}$ and $S_1^1 = \begin{bmatrix} 0 & 1 \\ 1 & 0 \\ 1 & 0 \\ 1 & 0 \end{bmatrix}$. For Γ_0^2, the first participant is non-essential. We assign the first participant the values (11). Thus, $S_2^0 =$

Table 3 Reduced pixel expansions of our (k, n)-VCS

$k\backslash n$	2	3	4	5	6	7	8
2	2(2)	3(3)	4(4)	5(4)	6(4)	7(5)	8(5)
3		4(4)	6(6)	8(8)	10(10)	12(12)	14(14)
4			8(8)	15(15)	24(23)	35(28)	48(32)
5				16(16)	30(30)	48(48)	70(70)
6					32(32)	70(70)	128(120)
7						64(64)	140(140)
8							128(128)

$\begin{bmatrix}1&1&1&1\\0&0&1&1\\0&1&0&1\\0&1&1&0\end{bmatrix}$ and $S_2^1 = \begin{bmatrix}1&1&1&1\\0&0&1&1\\0&1&0&1\\1&0&0&1\end{bmatrix}$. Finally, by concatenating the initial basis matrices respectively, we construct a $(\Gamma_{Qual}, \Gamma_{Forb})$-VCS with $\Gamma_0 = \{\{1,2\}, \{1,3\}, \{1,4\}, \{2,3,4\}\}$, where the basis matrices are $S^0 = \begin{bmatrix}0&1&1&1&1&1\\0&1&0&0&1&1\\0&1&0&1&0&1\\0&1&0&1&1&0\end{bmatrix}$ and $S^1 = \begin{bmatrix}0&1&1&1&1&1\\1&0&0&0&1&1\\1&0&0&1&0&1\\1&0&1&0&0&1\end{bmatrix}$. By deleting the common columns $(1111)^T$ and $(1000)^T$ from the initial basis matrices S^0 and S^1, we obtain the optimal pixel expansion 4.

Example 5 For the strong access structure $(\Gamma_{Qual}, \Gamma_{Forb})$ with $\Gamma_0 = \{\{1,2\}, \{1,3\}, \{2,4\}\}$, apply Algorithm 1 to group the collection Γ_0 into two collections, namely $\Gamma_0^1 = \{\{1,2\}, \{1,3\}\}$ and $\Gamma_0^2 = \{\{2,4\}\}$. For Γ_0^1, the fourth participant is non-essential. We assign the fourth participant the values (00). Thus, we have $S_1^0 = \begin{bmatrix}0&1\\0&1\\0&1\\0&0\end{bmatrix}$ and $S_1^1 = \begin{bmatrix}0&1\\1&0\\1&0\\0&0\end{bmatrix}$. For Γ_0^2, the first and third participants are non-essential. We assign the first participant the values (11) and the third participant the values (00). Thus, $S_2^0 = \begin{bmatrix}1&1\\0&1\\0&0\\0&1\end{bmatrix}$ and $S_2^1 = \begin{bmatrix}1&1\\0&1\\0&0\\1&0\end{bmatrix}$. Finally, by concatenating the initial basis matrices respectively, we construct a $(\Gamma_{Qual}, \Gamma_{Forb})$-VCS with $\Gamma_0 = \{\{1,2\}, \{1,3\}, \{2,4\}\}$, where the basis matrices are $S^0 = \begin{bmatrix}0&1&1&1\\0&1&0&1\\0&1&0&0\\0&0&0&1\end{bmatrix}$ and $S^1 = \begin{bmatrix}0&1&1&1\\1&0&0&1\\1&0&0&0\\0&0&1&0\end{bmatrix}$. By deleting the common column $(1000)^T$ from the initial basis matrices S^0 and S^1, we obtain the optimal pixel expansion 4.

Example 6 For the strong access structure $(\Gamma_{Qual}, \Gamma_{Forb})$ with $\Gamma_0 = \{\{1,2\},\{1,3,4\},\{2,3,4\}\}$, apply Algorithm 1 to group the collection Γ_0 into two collections, namely $\Gamma_0^1 = \{\{1,2\},\{1,3,4\}\}$ and $\Gamma_0^2 = \{\{2,3,4\}\}$. For Γ_0^1, we construct the initial basis matrices by solving the corresponding linear equations, and we have $S_1^0 = \begin{bmatrix} 0&0&1&1\\ 0&0&1&1\\ 0&1&0&1\\ 0&1&1&0 \end{bmatrix}$ and $S_1^1 = \begin{bmatrix} 0&0&1&1\\ 1&1&0&0\\ 0&1&0&1\\ 1&0&0&1 \end{bmatrix}$. For Γ_0^2, the first participant is non-essential and we construct the initial basis matrices by assigning the first participant the values (0100) for S_2^0 and (0001) for S_2^1, thus $S_2^0 = \begin{bmatrix} 0&1&0&0\\ 0&0&1&1\\ 0&1&0&1\\ 0&1&1&0 \end{bmatrix}$ and $S_2^1 = \begin{bmatrix} 0&0&0&1\\ 0&0&1&1\\ 0&1&0&1\\ 1&0&0&1 \end{bmatrix}$. Finally, by concatenating the initial basis matrices respectively, we construct a $(\Gamma_{Qual}, \Gamma_{Forb})$-VCS with $\Gamma_0 = \{\{1,2\},\{1,3,4\},\{2,3,4\}\}$, where the basis matrices are $S^0 = \begin{bmatrix} 0&0&1&1&0&1&0&0\\ 0&0&1&1&0&0&1&1\\ 0&1&0&1&0&1&0&1\\ 0&1&1&0&0&1&1&0 \end{bmatrix}$ and $S^1 = \begin{bmatrix} 0&0&1&1&0&0&0&1\\ 1&1&0&0&0&0&1&1\\ 0&1&0&1&0&1&0&1\\ 1&0&0&1&1&0&0&1 \end{bmatrix}$. By deleting the common column $(1011)^T$, $(0101)^T$ and $(0110)^T$ from the initial basis matrices S^0 and S^1, we obtain the optimal pixel expansion 5.

Remark 3 In general, we construct a VCS based on Lemma 2, where the non-essential participants are assigned the value 0. However, the above examples do not follow Lemma 2 and achieve the optimal pixel expansions. A natural question for future studies may be asked. For the non-essential participants, how to assign them the values 0 or 1 to achieve the optimal pixel expansion, especially for $(2, n)$ threshold access structure in Table 3. This question may lead to another problem that how to assign the non-essential participants the values 0 or 1 to guarantee that we can construct a VCS for the corresponding strong access structure by the concatenation of matrices.

6 Conclusion

In this paper we mainly deal with the following two issues: taking more equations simultaneously to construct the initial basis matrices and finding exact number of common columns in the initial basis matrices. For the first issue, we give a useful theory (Theorem 1), by which we could exploit the linear algebraic technique to construct efficient VCS for general access structures. For the second issue, we obtain the exact number of common columns in the initial basis matrices of $(2, n)$-VCS. Though our proposed construction based on Theorem 1 may not achieve the optimal pixel expansions for some cases, our theory lays a sound and constructive foundation for the minimization of pixel expansion for general access structures in the algebraic aspect of VCS.

Acknowledgments The authors would like to thank the anonymous reviewers for their helpful and constructive comments that improved the clarity and quality of this paper. This work was supported by the National Natural Science Foundation of China (Grant No.61602513 and No.61671448) and the Strategic Priority Research Program of the Chinese Academy of Sciences (Grant No.XDA06010701).

Appendix A

Let us first group the set $\Gamma_0 = \{\{1,2\},\{1,3\},\{1,4\}\}$ into two collections, namely $\Gamma_0^1 = \{\{1,2\},\{1,3\}\}$ and $\Gamma_0^2 = \{\{1,4\}\}$. For Γ_0^1, consider the following two systems of two linear equations over the binary field:

$$\begin{cases} x_1 + x_2 = 0 \\ x_1 + x_3 = 0 \end{cases} \tag{15}$$

and

$$\begin{cases} x_1 + x_2 = 1 \\ x_1 + x_3 = 1 \end{cases} \tag{16}$$

Let S_1^0 and S_1^1 be the Boolean matrices whose columns are just all possible solutions of (15) and (16), respectively. Thus, $S_1^0 = \begin{bmatrix} 0 & 1 \\ 0 & 1 \\ 0 & 1 \\ 0 & 0 \end{bmatrix}$ and $S_1^1 = \begin{bmatrix} 0 & 1 \\ 1 & 0 \\ 1 & 0 \\ 0 & 0 \end{bmatrix}$. Note that the fourth participant is non-essential for the strong access structure determined by Γ_0^1, so we assign it the values (00).

For Γ_0^2, consider the following two systems of one linear equations over the binary field:

$$x_1 + x_4 = 0 \tag{17}$$

and

$$x_1 + x_4 = 1 \tag{18}$$

Let S_2^0 and S_2^1 be the Boolean matrices whose columns are just all possible solutions of (17) and (18), respectively. Thus, $S_2^0 = \begin{bmatrix} 0 & 1 \\ 0 & 0 \\ 0 & 0 \\ 0 & 1 \end{bmatrix}$ and $S_2^1 = \begin{bmatrix} 0 & 1 \\ 0 & 0 \\ 0 & 0 \\ 1 & 0 \end{bmatrix}$. Note that the second and third participants are non-essential for the strong access structure determined by Γ_0^2, so we assign both of them the values (00).

Finally, by Lemma 2 we construct a $(\Gamma_{Qual}, \Gamma_{Forb})$-VCS on a set of four participants having $\Gamma_0 = \{\{1,2\},\{1,3\},\{1,4\}\}$ with the basis matrices $S^0 = \begin{bmatrix} 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$ and $S^1 = \begin{bmatrix} 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{bmatrix}$. It gives the pixel expansion 4.

Appendix B

Let us first group the collection $\Gamma_0 = \{\{1,2\},\{1,3\},\{2,3\},\{1,4\}\}$ into two collections, namely $\Gamma_0^1 = \{\{1,2\},\{1,3\}\}$ and $\Gamma_0^2 = \{\{2,3\},\{1,4\}\}$. For Γ_0^1, consider the following two systems of two linear equations over the binary field:

$$\begin{cases} x_1 + x_2 = 0 \\ x_1 + x_3 = 0 \end{cases} \tag{19}$$

and

$$\begin{cases} x_1 + x_2 = 1 \\ x_1 + x_3 = 1 \end{cases} \tag{20}$$

Let S_1^0 and S_1^1 be the Boolean matrices whose columns are just all possible solutions of (19) and (20), respectively. Thus, $S_1^0 = \begin{bmatrix} 0 & 1 \\ 0 & 1 \\ 0 & 1 \\ 0 & 0 \end{bmatrix}$ and $S_1^1 = \begin{bmatrix} 0 & 1 \\ 1 & 0 \\ 1 & 0 \\ 0 & 0 \end{bmatrix}$. Note that the fourth participant is non-essential for the strong access structure determined by Γ_0^1, so we assign it the values (00).

For Γ_0^2, consider the following two systems of two linear equations over the binary field:

$$\begin{aligned} x_2 + x_3 = 0 \\ x_1 + x_4 = 0 \end{aligned} \tag{21}$$

and

$$\begin{aligned} x_2 + x_3 = 1 \\ x_1 + x_4 = 1 \end{aligned} \tag{22}$$

Let S_2^0 and S_2^1 be the Boolean matrices whose columns are just all possible solutions of (21) and (22), respectively. Thus, $S_2^0 = \begin{bmatrix} 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{bmatrix}$ and $S_2^1 = \begin{bmatrix} 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 \end{bmatrix}$.

Finally, by Lemma 2 we construct a $(\Gamma_{Qual}, \Gamma_{Forb})$-VCS on a set of four participants having $\Gamma_0 = \{\{1,2\},\{1,3\},\{2,3\},\{1,4\}\}$ with the basis matrices $S^0 = \begin{bmatrix} 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 \end{bmatrix}$ and $S^1 = \begin{bmatrix} 0 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 \end{bmatrix}$. It gives the pixel expansion 5, obtained by deleting the common column $(0110)^T$ from the initial basis matrices S^0 and S^1.

Appendix C

Let us first group the set $\Gamma_0 = \{\{1,2\},\{1,3\},\{2,3\},\{1,4\}\}$ into two collections, namely $\Gamma_0^1 = \{\{1,2\},\{2,3\}\}$ and $\Gamma_0^2 = \{\{1,3\},\{1,4\}\}$. For Γ_0^1, consider the following two systems of two linear equations over the binary field:

$$\begin{cases} x_1 + x_2 = 0 \\ x_2 + x_3 = 0 \end{cases} \tag{23}$$

and

$$\begin{cases} x_1 + x_2 = 1 \\ x_2 + x_3 = 1 \end{cases} \tag{24}$$

Let S_1^0 and S_1^1 be the Boolean matrices whose columns are just all possible solutions of (23) and (24), respectively. Thus, $S_1^0 = \begin{bmatrix} 0 & 1 \\ 0 & 1 \\ 0 & 1 \\ 0 & 0 \end{bmatrix}$ and $S_1^1 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \\ 1 & 0 \\ 0 & 0 \end{bmatrix}$. Note that the fourth participant is non-essential for the strong access structure determined by Γ_0^1, so we assign it the values (00).

For Γ_0^2, consider the following two systems of two linear equations over the binary field:

$$\begin{aligned} x_1 + x_3 &= 0 \\ x_1 + x_4 &= 0 \end{aligned} \tag{25}$$

and

$$\begin{aligned} x_1 + x_3 &= 1 \\ x_1 + x_4 &= 1 \end{aligned} \tag{26}$$

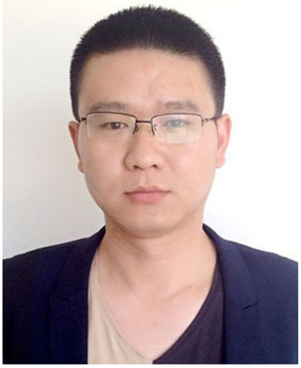
Let S_2^0 and S_2^1 be the Boolean matrices whose columns are just all possible solutions of (25) and (26), respectively. Thus, $S_2^0 = \begin{bmatrix} 0 & 1 \\ 0 & 0 \\ 0 & 1 \\ 0 & 1 \end{bmatrix}$ and $S_2^1 = \begin{bmatrix} 0 & 1 \\ 0 & 0 \\ 1 & 0 \\ 1 & 0 \end{bmatrix}$. Note that the second participant is non-essential for the strong access structure determined by Γ_0^2, so we assign it the values (00).

Finally, by Lemma 2 we construct a $(\Gamma_{Qual}, \Gamma_{Forb})$-VCS on a set of four participants having $\Gamma_0 = \{\{1,2\},\{3,4\},\{2,3\},\{2,4\}\}$ with the basis matrices $S^0 = \begin{bmatrix} 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 \end{bmatrix}$ and $S^1 = \begin{bmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 \end{bmatrix}$. It gives the pixel expansion 4.

References

1. Adhikari A (2014) Linear algebraic techniques to construct monochrome visual cryptographic schemes for general access structure and its applications to color images. Des Codes Crypt 73(3):865–895
2. Ateniese G, Blundo C, De Santis A, Stinson DR (1996) Visual cryptography for general access structures. Inf Comput 129:86–106
3. Blundo C, De Santis A, Stinson DR (1999) On the contrast in visual cryptography schemes. J Cryptol 12(4):261–289
4. Blundo C, Darco P, De Santis A, Stinson DR (2003) Contrast optimal threshold visual cryptography. SIAM J Discret Math 16(2):224–261
5. Cimato S, De Prisco R, De Santis A (2005) Optimal colored threshold cisual cryptography schemes. Des Codes Crypt 35:311–335
6. Cimato S, De Prisco R, De Santis A (2006) Probabilistic Visual Cryptography Schemes. Comput J 49:97–107
7. Dutta S, Rohit RS, Adhikari A (2016) Constructions and analysis of some efficient t-(k, n)*-visual cryptographic schemes using linear algebraic techniques. Des Codes Cryptc 80(1):165–196
8. Guo T, Liu F, Wu C, Ren YW, Wang W (2014) On (k, n) visual cryptography scheme with t essential parties. In: ICITS 2013. Lecture Notes in Computer Science, vol. 8317, pp. 56–68. Springer, Berlin

9. Hou YC, Quan ZY, Tsai CF, Tseng AY (2013) Block-based progressive visual secret sharing. Inf Sci 233:290–304
10. Hu CM, Tzeng WG (2007) Cheating Prevention in Visual Cryptography. IEEE Trans Image Process 16(1):36–45
11. Li P, Ma PJ, Li D (2012) Aspect ratio invariant visual cryptography scheme with flexible size expansion. ICIC Express Letters 6(8):2033–2038
12. Liu F, Wu CK, Lin XJ (2011) Cheating immune visual cryptography scheme. IET Inf Secur 5(1):51–59
13. Naor M, Shamir A (1994) Visual cryptography. In: Advance in Cryptography, Eurocrypt. Lecture Notes in Computer Science, vol. 950, pp. 1–12. Springer, Berlin
14. Shyu SJ, Chen MC (2011) Optimum pixel expansions for threshold visual secret sharing schemes. IEEE Trans Inf Forensics Secur 6(3):960–969
15. Shyu SJ, Jiang HW (2013) General constructions for threshold multiple-secret visual cryptography schemes. IEEE Trans Inf Forensics Secur 8(5):733–743
16. Shyu SJ, Chen MC (2015) Minimizing Pixel Expansion in Visual Cryptographic Scheme for General Access Structures. IEEE Trans Circuits Syst Video Technol 25(9):1557–1561
17. Wang DS, Yi F, Li X (2009) On general construction for extended visual cryptography schemes. Pattern Recogn 42(11):3071–3082
18. Wu XT, Sun W (2013) Generalized Random Grid and Its Applications in Visual Cryptography. IEEE Trans Inf Forensics Secur 8(9):1541–1553
19. Yamaguchi Y (2012) An Extended Visual Cryptography Scheme for Continuous-Tone Images. Springer Trans Digital Forensics and Watermarking 7128:228–242
20. Yan XH, Shen W, Niu XM, Yang CN (2015) Halftone visual cryptography with minimum auxiliary black pixels and uniform image quality. Digital Signal Process 38:53–65
21. Yan WQ, Jin D, Kankanhalli MS (2004) Visual cryptography for print and scan applications. In: ISCAS 2004. Proceedings of IEEE international symposium on circuits and systems, vol. 5, pp. 572–575. IEEE, Canada
22. Yang CN, Chen TS (2006) Reduce shadow size in aspect ratio invariant visual secret sharing schemes using a square block-wise operation. Pattern Recogn 39:1300–1314
23. Yang CN, Shih HW, Wu CC, Harn L (2012) k out of n region incrementing scheme in visual cryptography. IEEE Trans Circuits Syst Video Technol 22:779–810
24. Yu B, Shen G (2014) Multi-secret visual cryptography with deterministic contrast. Multi Tools Appl 72(2):1867–1886



Gang Shen received the B.S. degree and M.S. degree from Zhengzhou Information Science and Technology Institute in 2010 and 2013, respectively. He is studying the Ph.D. degree in Zhengzhou Information Science and Technology Institute and a visiting Ph.D. student in State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences. His research interests include: visual security and cryptography, image security.

Feng Liu received the B.S. degree in computer science from Shandong University, in 2003, and the Ph.D. degree in information security from the Institute of Software, Chinese Academy of Sciences, in 2009. He is currently a professor and Ph.D. supervisor of State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences. His current research interests include: strategic and economic aspects of information security, visual security and cryptography, network security and security protocols.

Zhengxin Fu received the M.S. and Ph.D. degree from Zhengzhou Information Science and Technology Institute in 2010 and 2014, respectively. His research interests include: visual cryptography, image security.

Bin Yu received the B.S. degree in Dept. of Electronic Engineering from the University of Shanghai Jiaotong in 1986, the M.S. degree in Dept. of Automatic Engineering from South China University of Technology in 1991 and the Ph.D. degree in 1999. From 1997 to 1999, he worked as a research assistant at Hong Kong University of Science and Technology. From 2003 to 2004, he worked as a vice professor at in the University of Waterloo, ON, Canada. Currently, he is a professor of the Department of Computer Science and Information Engineering at Zhengzhou Information Science and Technology Institute, China. His research interests include the design and analysis of algorithms, visual secret sharing and network security.