Multimed Tools Appl (2018) 77:12871–12899
https://doi.org/10.1007/s11042-017-4921-5

Visual cryptograms of random grids via linear algebra

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

Received: 14 September 2016 / Revised: 10 April 2017 / Accepted: 6 June 2017 /
Published online: 14 June 2017

Abstract Two visual models of image secret sharing have been studied: visual cryptography schemes (VCS), introduced by Naor and Shamir, and visual cryptograms of random grids (VCRG), introduced by Kafri and Keren. VCRG has gained much attention in academia than before to avoid the pixel expansion of VCS. Although there is a strict relation between VCRG and VCS, VCRG can still be improved to achieve a better result. In this paper, based on new insight into linear algebraic technique to construct VCS, where we are able to construct VCS by solving a linear system of more equations at a time, we put forward a new construction of VCRG for general access structures. The effectiveness and advantage of the proposed construction are formally analyzed and experimentally demonstrated. With theoretical and practical interests, our construction exposes new possibilities to the researches of visual models of image secret sharing.

Keywords Image secret sharing · Visual cryptography · Random grid · Linear algebra · General access structure

1 Introduction

With the rapid development and wide application of digital camera, scanner, mobile phone and other digital products, images are easily obtained and transmitted. At the same time, more and more attentions are paid to the secure protection of the image. To protect the secret

✉ 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

image from the malicious behaviors, some technologies have been developed, such as image secret sharing [29, 31] and steganography [1, 11, 23]. Image secret sharing (ISS) is about encoding the secret image while steganography is about concealing the very existence of the encoded image. Obviously, the conjunctive use of steganography and ISS is more secure [18, 39]. In this paper, we focus on ISS.

In a conventional (k, n)-ISS scheme, a secret image is encoded into n different shadows distributed to n participants such that any group of k participants can compute the secret image using their shadows, while that of less than k ones cannot. The secret image is thus tolerant to a loss of $n-k$ shadow images. However, the complicated computations, i.e., Lagrange interpolations, are required in both encoding and decoding. In some circumstances where the cost of computations may not be affordable or the decoding time should be instantly done in a constant time, these computation-based ISS schemes become no longer appropriate.

Two visual models of ISS have been studied: visual cryptography scheme(VCS), introduced by Naor and Shamir [22], and visual cryptograms of random grids (VCRG), introduced by Kafri and Keren [16]. Such a (k, n) scheme is capabl1e of encoding a secret image into n shadows. Any group of k or more shadows can visually recover the secret image by printing the shadows on transparencies and stacking (Boolean OR operation) them together. Whereas, any group of $k-1$ or less shadows give no clue about the secret image. The feature is that the decoding is done via human visual system instead of complicated computations. With such an attractive feature, the above two models can be applied to protect online transactions against manipulation like online money transfers by Trojans [21], realize visual voting while ensuring voter's anonymity without counting process [9], design secure display screen with controllable visual area against malicious peep while avoiding the attacks of virus and electromagnetic leakage [19], and other application scenarios including financial documents [12] and bar codes [36]. In addition, some new technologies, such as google glass and flexible screen, also provide new opportunities for the application of the above two models.

VCS uses whiteness to distinguish black color from white color. Specifically, each pixel of the black-and-white secret image is encoded into m subpixels, referred to as pixel expansion, for each of the n shadows by designing two collections of $n \times m$ Boolean matrices C_0 and C_1. 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 shadows. If any k or more shadows are stacked together, our eyes can perceive the secret information due to the whiteness difference, referred to as contrast, between black pixels and white pixels in the stacked result, while if fewer than k shadows are superimposed it is impossible to perceive the secret information. Inspired by Naor and Shamir's work, many research papers have explored various aspects: general access structure (GAS) [2, 3], pixel expansion [8, 28], contrast [4, 6], multiple secrets [24, 40], cheating prevention [14, 20], meaningful shadows [30, 35], color image [5, 13], aspect ratio invariant [17, 38] and other applications [15, 33, 34]. However, a main drawback of VCS is the large pixel expansion, which will increase storage and transmission bandwidth.

VCRG uses average light transmission to distinguish black areas from white areas. A secret image is encoded into some size invariant random grids, each of which is a transparency comprising a two-dimensional array of pixels that are chosen between white and black with a probability. After VCRG was first introduced, many researchers focused their attentions on it. Shyu gave a formal definition to VCRG to make VCRG applicable [25], and devised algorithms for (k, n)-VCRG [27] and VCRG for GAS [24], respectively. Similar works by other research groups could also be found in [10, 32]. The most essential advantage of VCRG lies in that extra pixel expansion is not needed.

At the same time, the relationship between VCS and VCRG was discussed [7, 37]. Especially, De Prisco and De Santis [7] showed that there is a close relation between deterministic VCS and VCRG, and indicated that it allows to use results known for the deterministic VCS in the VCRG and vice versa. In other words, the future works that deal with VCRG and VCS should not ignore each other in comparison of contrast.

Recently, Adhikari [2] introduced a linear algebraic technique to construct VCS. In addition, a simple and effective way to construct VCRG, as described in [7], is randomly choosing a column from the corresponding encoding matrix of VCS. Hence, exploring the algebraic aspects of VCS is worthy of study. For a future study, as posed in [2], taking more than two equations simultaneously to construct the encoding matrix should be considered.

In this paper, we pay attention to the construction of VCRG and improve VCRG by exploiting the algebraic aspects of VCS. First, we consider the problem of characterizing the set of access structures on n participants and put forward a characterization where we can take more equations simultaneously. Second, based on the above knowledge, we propose a new construction of VCRG for general access structures, where a competitive visual performance is achieved. Finally, we provide some experimental results and comparisons to demonstrate the effectiveness and advantage of our construction.

The rest of the paper is organized as follows. In Section 2, we give some preliminaries including the models of VCS and VCRG. In Section 3, some related works, as well as our motivation, are presented. In Section 4, we provide a characterization of the set of access structures on a set of participants where we are able to take more equations simultaneously. In Section 5, we give a new construction of VCRG for GAS based on the above characterization. Some experimental results and comparisons are presented in Section 6. Lastly we conclude the paper in Section 7.

2 The model

2.1 GAS

Let $P = \{1, 2, \ldots, n\}$ be a set of n participants and 2^P denoting 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 secret image, since the information he has is not needed by any set in P in order to recover the shared image. Therefore, unless otherwise specified, we assume that all participants are essential throughout the paper.

Definition 1 [3] An 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. $\Gamma_{Qual} \cup \Gamma_{Forb} = 2^P$.

For a strong access structure $(\Gamma_{Qual}, \Gamma_{Forb})$, define Γ_0 to consist of all the minimal qualified sets:

$$\Gamma_0 = \{Q \in \Gamma_{Qual} : Q' \notin \Gamma_{Qual} \ for\ all\ Q' \subset Q\} \tag{1}$$

and Z_M to consist of all the maximal forbidden sets:

$$Z_M = \{F \in \Gamma_{Forb} : F \cup \{i\} \in \Gamma_{Qual} \ for\ all\ i \in P \setminus F\}. \tag{2}$$

Because $\Gamma_{Forb} = 2^P - \Gamma_{Qual}$, Γ_0 is termed a basis, which completely determines its corresponding strong access structure by

$$\Gamma_{Qual} = \{Q' \subseteq P : Q \subseteq Q' \ for\ some\ Q \in \Gamma_0\}. \tag{3}$$

As a special access structure, a (k, n) threshold structure is a strong access structure $(\Gamma_{Qual}, \Gamma_{Forb})$ with the following constraints: $\Gamma_0 = \{Q \subseteq P : |Q| = k\}$ and $\Gamma_{Forb} = \{Q \subseteq P : |Q| \leq k-1\}$.

In this paper, unless otherwise specified, all the considered access structures are supposed to be strong.

2.2 VCS and VCRG

Let D be an $n \times m$ Boolean matrix and $X \subseteq P$. Then $D[X]$ denotes the $|X| \times m$ submatrix obtained from D by considering its restriction to rows corresponding to the elements in X. D_X denotes the Boolean "OR" operation to the rows of $D[X]$. $\omega(D_X)$ denotes the whiteness of the row vector D_X, which is the number of 0's in the vector D_X.

Definition 2 [3] 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. If $X = \{i_1, i_2, \ldots, i_p\} \in \Gamma_{Qual}, \omega(S^0_X) > \omega(S^1_X)$.
2. If $X = \{i_1, i_2, \ldots, i_p\} \in \Gamma_{Forb}, \omega(S^0_X) = \omega(S^1_X)$.

For VCRG, a secret image S is encoded into n size invariant random grids $R_1, R_2, \ldots, R_n$. Let $S(0)$ (resp. $S(1)$) denote the area of all the white (resp. black) pixels in the secret image. R_X denotes the Boolean "OR"ed result of the random grids of $X \subseteq P$. Let $R_X[S(0)]$ (resp. $R_X[S(0)]$) denote the corresponding area of all the white (resp. black) pixels in the recovered secret image. The formal definition of VCRG is given by means of the average light transmission.

Definition 3 [25] For a certain pixel s in a secret image S whose size is $M \times N$, the probability for s being transparent, say $Prob(s = 0)$, is represented as the light transmission of s, say $T(s)$. The light transmission of a white (resp. black) pixel is defined as $T(s) = 1$ (resp. $T(s) = 0$). The average light transmission of S is defined as

$$T(S) = \frac{1}{M \times N} \times \sum_{i=1}^{M} \sum_{j=1}^{N} T(S(i, j)), \tag{4}$$

where $S(i, j)$ denotes the secret pixel at position (i, j) of S.

Definition 4 [24] Given an access structure $(\Gamma_{Qual}, \Gamma_{Forb})$ on a set of n participants, n random grids $R_1, R_2, \ldots, R_n$ constitute a $(\Gamma_{Qual}, \Gamma_{Forb})$-VCRG if the following conditions are satisfied:

1. If $X = \{i_1, i_2, \ldots, i_p\} \in \Gamma_{Qual}$, $T(R_X[S(0)]) > T(R_X[S(1)])$.
2. If $X = \{i_1, i_2, \ldots, i_p\} \in \Gamma_{Forb}$, $T(R_X[S(0)]) = T(R_X[S(1)])$.

In Definitions 2 and 4, the first condition is related to the contrast of the reconstructed secret image. It states that when a qualified set of participants stack their shares they can perceive the secret information. The second condition is called security, since it implies that, even by inspecting all their shares, a forbidden set of participants cannot gain any information in deciding whether the shared pixel was white or black.

2.3 Visual performance

For a qualified set of participants, the secret image can be reconstructed and the visual performance of the reconstructed secret image is mainly determined by the contrast.

For VCS, various definitions of contrast have been used. In the original model by Naor and Shamir [22], the contrast is defined as

$$\alpha_{NS} = \frac{\omega(S_X^0) - \omega(S_X^1)}{m}, \tag{5}$$

while Eisen and Stinson [8] have proposed

$$\alpha_{ES} = \frac{\omega(S_X^0) - \omega(S_X^1)}{m + \omega(S_X^1)}. \tag{6}$$

Both measurements favor a larger $\omega(S_X^0) - \omega(S_X^1)$, yet the latter in addition prefers a smaller (darker) $\omega(S_X^1)$ due to the reason that a larger (brighter) $\omega(S_X^1)$ weakens our visual recognition between S_X^1 and S_X^0 (than a smaller (darker) one) under a same $\omega(S_X^0) - \omega(S_X^1)$. Therefore, α_{ES}, as pointed out in [6], is a better choice for measuring the contrast.

For VCRG, the contrast depends on the difference of the average light transmission between the white and the black areas of the secret image. Papers [10, 25–27, 32] that dealt with VCRG have used the following definition of contrast

$$\alpha_{RG} = \frac{T(R_X[S(0)]) - T(R_X[S(1)])}{1 + T(R_X[S(1)])}. \tag{7}$$

Clearly, the use of the average light transmission is not restricted to reconstructions obtained with VCRG but can be used also to evaluate VCS. In fact, it should not be hard to see that

$$T(R_X[S(0)]) = \frac{\omega(S_X^0)}{m} \tag{8}$$

and

$$T(R_X[S(1)]) = \frac{\omega(S_X^1)}{m}. \tag{9}$$

Hence, we have that

$$\begin{aligned}\alpha_{ES} &= \frac{\omega(S_X^0) - \omega(S_X^1)}{m + \omega(S_X^1)} \\ &= \frac{T(R_X[S(0)]) - T(R_X[S(1)])}{1 + T(R_X[S(1)])} \\ &= \alpha_{RG}. \end{aligned} \tag{10}$$

This equivalence opens up a door between VCRG and VCS. As De Prisco and De Santis [7] pointed out, the future works that deal with VCRG and VCS should not ignore each other in comparison of contrast, which is defined by α_{ES} and α_{RG} respectively.

The contrast α determines how well human visual system can recognize the recovered secret image. It is lucid that for a valid scheme, $\alpha = 0$ if $X \in \Gamma_{Forb}$ and $\alpha > 0$ where $X \in \Gamma_{Qual}$. The contrast is expected to be as large as possible.

3 Related work and our motivation

In terms of the construction of VCRG for GAS, Wu and Sun [32] proposed one, which is restated as Algorithm 1.

Algorithm 1 VCRG for GAS

Input:
A binary secret image S whose size is $M \times N$, and an access structure $(\Gamma_{Qual}, \Gamma_{Forb})$;
Output:
n random grids $R_1, R_2, \ldots, R_n$;
1: Obtain the basis Γ_0 of access structure $(\Gamma_{Qual}, \Gamma_{Forb})$;
2: For each secret pixel $S(i, j)$, where $1 \le i \le M$, $1 \le j \le N$, repeat the steps 3–7;
3: Randomly select a minimal qualified set $Q = \{i_1, i_2, \ldots, i_p\} \in \Gamma_0$ where $p \le n$;
4: Generate $p - 1$ bits $b_{i_1}, b_{i_2}, \ldots, b_{i_{p-1}}$ by assigning them the value 0 or 1 randomly;
5: Compute b_{i_p} by $b_{i_1} \oplus \cdots \oplus b_{i_{p-1}} \oplus b_{i_p} = S(i, j)$;
6: Assign the p bits $b_{i_1}, b_{i_2}, \ldots, b_{i_p}$ to the associated random grids $R_{i_1}, R_{i_2}, \ldots, R_{i_p}$, respectively;
7: Generate $n - p$ bits by assigning them the value 0 or 1 randomly and assign them to the left $n - p$ random grids, respectively;
8: **return** n random grids $R_1, R_2, \ldots, R_n$;

In Algorithm 1, it is easy to see that the steps 4–6 are the core that certifies the security and contrast requirements for p random grids to constitute a (p, p)-VCRG [27]. The left $n - p$ random grids are randomly assigned. As proved in [32], any qualified set containing the chosen minimal qualified set Q can recover the secret. When a set X is randomly chosen from 2^P, the chance for X being able to recover the secret (namely, $X \supseteq Q$) does exist ($\frac{d}{|\Gamma_0|}$, where d denotes the number of minimal qualified sets that elements in X can form). Moreover, Wu and Sun [32] gave an accurate equation expressing the relation between the contrast and the chance (please refer to [32] for details). The equation concludes that a larger chance will lead to a better contrast of the recovered secret image. However, the chance for X being able to recover the secret is small when $|\Gamma_0|$ is large, and then the contrast becomes quite small.

In this paper, we try to improve the contrast by increasing the chance for X being able to recover the secret. A comprehensive idea to improve such a probability is to choose more minimal qualified sets in the step 3 and assign them in the steps 4–6. This method undoubtedly works since the value d is increased.

For the assignment to random grids of Q, Algorithm 1 actually accomplishes it by solving the following two linear equations over the binary field: $x_{i_1} + \cdots + x_{i_{p-1}} + x_{i_p} = 0$ for the white secret pixel ($S(i, j) = 0$) and $x_{i_1} + \cdots + x_{i_{p-1}} + x_{i_p} = 1$ for the black secret pixel ($S(i, j) = 1$). Thereinto, Algorithm 1 randomly choose one from all possible solutions of the first (resp. second) equation and assign it to the corresponding random grids of Q when the shared secret pixel is white (resp. black).

Similar to Algorithm 1, we can accomplish the assignment to random grids of more chosen minimal qualified sets by solving the following two systems of linear equations over the binary field: $A\mathbf{x} = \mathbf{0}$ for the white secret pixel and $A\mathbf{x} = \mathbf{1}$ for the black secret pixel, where A is a Boolean matrix of t rows determining t chosen minimal qualified sets, $\mathbf{x}$ is a vector denoting an assignment to random grids of the t chosen minimal qualified sets, and $\mathbf{0}$ and $\mathbf{1}$ are $t \times 1$ vectors of 0's and 1's respectively. If both systems are consistent, we can randomly choose one from all possible solutions of the first (resp. second) system and assign it to the corresponding random grids of the chosen minimal qualified sets when the shared secret pixel is white (resp. black). Therefore, to explore the conditions for consistency or inconsistency of both systems is the problem to be solved.

Recently, Adhikari [2] systematically explored the consistency or inconsistency of the above systems. He utilized this linear algebraic technique to construct VCS, where all possible solutions of the first (resp. second) system form the basis matrix S^0 (resp. S^1). In other words, to construct VCRG for the chosen minimal qualified sets, we can randomly choose a column from the above basis matrices. If the number of chosen minimal qualified sets is two, then we could solve a linear system of two equations to obtain the basis matrices in accordance with Adhikari's method [2]. However, Adhikari's method is confined to taking a system of two equations and cannot deal with more than two chosen minimal qualified sets.

Inspired by the above analysis, we are going to propose a new construction of VCRG via the linear algebraic technique, where we are able to take a system of more than two equations simultaneously.

4 New insight into linear algebraic technique to construct VCS

In this section, we propose an improved linear algebraic technique to construct basis matrices of VCS for some specific access structures, where the access structure should meet some constraints. Given such a specific access structure on a set of n participants, we construct some suitable systems of linear equations over the binary field and the solutions of these systems of linear equations will construct the basis matrices for the given access structure. However, to understand what constraints the access structure should meet, we build our theory from the reverse direction in this section. First, we start with the following two systems of linear equations over the binary field,

$$A\mathbf{x} = \mathbf{0} \tag{11}$$

$$A\mathbf{x} = \mathbf{1} \tag{12}$$

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 (11) and

(12) are consistent. The difference from Adhikari's systems [2] is the coefficient matrix A, which does not have to be of full row rank.

Let S^0 (resp. S^1) be an $n \times 2^{n-r}$ Boolean matrix whose columns are all possible solutions of the system (11) (resp. (12)). Then, to prove S^0 and S^1 can form the basis matrices of a $(\Gamma_{Qual}, \Gamma_{Forb}, m = 2^{n-r})$-VCS, the following lemma is first given immediately since the proof of Lemma 5 in Adhikari [2] also works for this lemma.

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

$$\begin{pmatrix} A \\ B^X \end{pmatrix} \boldsymbol{x} = \begin{pmatrix} \mathbf{1} \\ \mathbf{0} \end{pmatrix} \tag{13}$$

where B^X is a column permutation of the $p \times n$ Boolean matrix $(\boldsymbol{I}_p | \mathbf{0}_{p\times(n-p)})$ 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 $(\Gamma_{Qual}, \Gamma_{Forb}, m = 2^{n-r})$-VCS if the following conditions are satisfied:

1. *For $X \in \Gamma_{Qual}$, the system (13) is inconsistent.*
2. *For $X \in \Gamma_{Forb}$, the system (13) is consistent.*

Next we are going to explore the conditions for consistency or inconsistency of the system (13). Let rows of A_1 (resp. A_2) represent all possible sum of odd (resp. even) number of rows in A. 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. Then we have the following lemma.

Lemma 2 *For an access structure $(\Gamma_{Qual}, \Gamma_{Forb})$, S^0 and S^1 form the basis matrices of a $(\Gamma_{Qual}, \Gamma_{Forb}, m = 2^{n-r})$-VCS 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 (13), 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 (12) is consistent and $B^X\mathbf{x} = \mathbf{0}$ is consistent (B^X is of full row rank), the system (13) 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 $\mathbf{u}\begin{pmatrix} A \\ B^X \end{pmatrix} = \mathbf{0} \Leftrightarrow \mathbf{u}_1 A + \mathbf{u}_2 B^X = \mathbf{0}$ over the binary field. 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 (13), $\mathbf{u}\begin{pmatrix} \mathbf{1} \\ \mathbf{0} \end{pmatrix} = \mathbf{u}_1\mathbf{1}$. If $\mathbf{u}_1$ has an odd (resp. even) number of 1's, then the system (13) is inconsistent (resp. consistent).

Based on the above discussions and Lemma 1, 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 2, we can construct a VCS by solving the two linear systems (11) and (12). In other words, we have concluded the sufficient conditions for constructing VCS by solving 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 3 *For an access structure* $(\Gamma_{Qual}, \Gamma_{Forb})$ *with* $\Gamma_0 = \{Q_1, Q_2, \ldots, Q_t\}$, *let* $A = (\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_t)^T$ *of rank* r *and* $\Re_{\mathbf{v}_i} = Q_i$, $i = 1, 2, \ldots, t$. S^0 *and* S^1 *form the basis matrices of a* $(\Gamma_{Qual}, \Gamma_{Forb}, m = 2^{n-r})$*-VCS if the following conditions are satisfied:*

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

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, $\Re_{\mathbf{v}} \not\subseteq Q \in \Gamma_0$ 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 3 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* $(\Gamma_{Qual}, \Gamma_{Forb}, m = 2^{n-r})$*-VCS are composed of all possible solutions of the systems* (11) *and* (12) *respectively, where* $A = (\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_t)^T$ *of rank* r *and* $\Re_{\mathbf{v}_i} = Q_i$, $i = 1, 2, \ldots, t$.

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

Example 1 Consider the following access structure $(\Gamma_{Qual}, \Gamma_{Forb})$ on a set of 4 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 $(\Gamma_{Qual}, \Gamma_{Forb}, m = 2)$-VCS with basis matrices S^0

and S^1, which are obtained by solving the two systems of three linear equations over the binary field as follows:

$$\begin{cases} x_1 + x_2 = 0 \\ x_1 + x_3 = 0 \\ x_1 + x_4 = 0 \end{cases} \tag{14}$$

and

$$\begin{cases} x_1 + x_2 = 1 \\ x_1 + x_3 = 1 \\ x_1 + x_4 = 1 \end{cases} \tag{15}$$

Let S^0 and S^1 be the Boolean matrices whose columns are just all possible solutions of the above two systems of (14) and (15) respectively. Thus, $S^0 = \begin{bmatrix} 0 & 1 \\ 0 & 1 \\ 0 & 1 \\ 0 & 1 \end{bmatrix}$ and $S^1 = \begin{bmatrix} 0 & 1 \\ 1 & 0 \\ 1 & 0 \\ 1 & 0 \end{bmatrix}$. Obviously, S^0 and S^1 satisfy the properties of basis matrices for the access structure $(\Gamma_{Qual}, \Gamma_{Forb})$ determined by Γ_0.

5 General construction of VCRG via linear algebraic technique

Based on the above knowledge, we are able to construct the basis matrices of VCS for more chosen minimal qualified sets. Hence, we can construct VCRG for more chosen minimal qualified sets by randomly choosing a column from the corresponding basis matrix. But the conditions of Theorem 1 are not always met by any given strong access structure. Therefore, we can only construct VCRG for some restricted access structures to share a secret pixel at a time. As described in the motivation of this paper, to share a secret pixel, at least one minimal qualified set should be randomly chosen from Γ_0 and more minimal qualified sets should be chosen at the same time. Meanwhile, the conditions of Theorem 1 should be satisfied by the chosen minimal qualified sets so that we can apply the proposed linear algebra technique to construct the corresponding basis matrices. Towards this end, we give a choosing algorithm for GAS, which is described as Algorithm 2.

Algorithm 2 Choosing algorithm for GAS

Input:
An access structure $(\Gamma_{Qual}, \Gamma_{Forb})$;
Output:
A collection of chosen minimal qualified sets Γ;
1: Obtain the basis Γ_0 of the access structure $(\Gamma_{Qual}, \Gamma_{Forb})$;
2: Randomly choose a minimal qualified set Q from Γ_0;
3: Choose λ collections of minimal qualified sets $\Gamma_m^1, \ldots, \Gamma_m^\lambda$ from Γ_0, where $1 \le \lambda \le |\Gamma_0|$ (the number of minimal qualified sets of Γ_0) and the following conditions are met:
  1: $Q \in \Gamma_m^i, i = 1, \ldots, \lambda$;
  2: Each of $\Gamma_m^1, \ldots, \Gamma_m^\lambda$ satisfies the conditions of Theorem 1;
  3: $|\Gamma_m^1| = \cdots = |\Gamma_m^\lambda| = N_{max}$, where $N_{max} \le |\Gamma_0|$ is the largest number of chosen minimal qualified sets;
4: Randomly select a collection Γ from $\Gamma_m^1, \ldots, \Gamma_m^\lambda$;
5: **return** Γ;

In Algorithm 2, we choose collections of the largest number of minimal qualified sets satisfying the conditions of Theorem 1. For $|\Gamma_0| \geq 2$, the worst case is that we can always choose two minimal qualified sets from the basis since any two minimal qualified sets satisfy the conditions of Theorem 1. Therefore, it is always possible to choose the collection of sets needed to construct the scheme.

Then we construct VCRG for GAS (GAS-VCRG) based on the above choosing algorithm. Diagram of the proposed VCRG for GAS is depicted in Fig. 1. The random grid generation is a pixel-wise operation, and n random grids are constructed via the proposed scheme for every given secret pixel. Simply, the proposed scheme consists of three components: the selection of minimal qualified sets, the construction of basis matrices and the assignment of random grids. In the selection of minimal qualified sets, Step 3 of Algorithm 2 is executed for every pixel, which will become time-consuming during encoding all pixels. However, for each chosen minimal qualified set Q from Γ_0, the generated λ collections

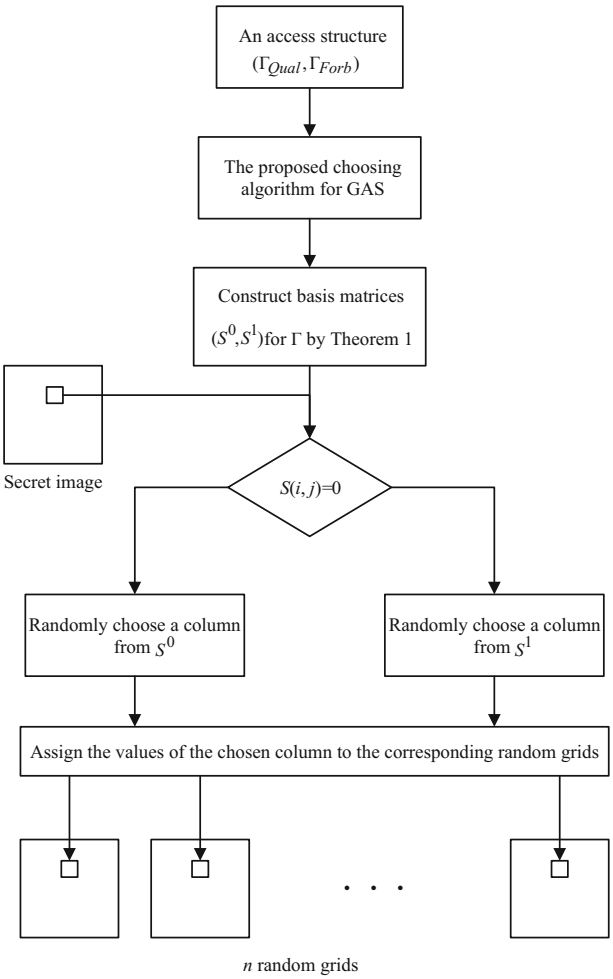


Fig. 1 Diagram of the proposed VCRG for GAS

of minimal qualified sets $\Gamma_m^1, \ldots, \Gamma_m^\lambda$ from Γ_0 are fixed since they are of the largest number of minimal qualified sets. Therefore, after the λ collections of minimal qualified sets $\Gamma_m^1, \ldots, \Gamma_m^\lambda$ for a randomly chosen Q are first generated, we can store them so that we can reuse them, instead of generating them again, when the same Q is chosen in next time. In the construction of basis matrices, we are able to obtain the basis matrices S^0 and S^1 for the collection Γ of chosen minimal qualified sets by solving the corresponding systems of linear equations. It should be noted that we could assign the non-essential participants shares completely white (the value 0) and this assignment would not have an influence on the contrast and security conditions of the corresponding basis matrices (please refer to the paper [3]). In the assignment of random grids, we assign the values to n random grids according to the randomly chosen column from the corresponding S^0 and S^1. Detailed information on the proposed scheme is described as Algorithm 3.

Algorithm 3 The proposed VCRG for GAS

Input:
A binary secret image S whose size is $M \times N$, and an access structure $(\Gamma_{Qual}, \Gamma_{Forb})$;
Output:
n random grids $R_1, R_2, \ldots, R_n$;
1: For each secret pixel $S(i, j)$, where $1 \le i \le M$, $1 \le j \le N$, repeat the steps 2-7;
2: Apply Algorithm 2 and get a collection of minimal qualified sets Γ;
3: For Γ, build the two corresponding systems of linear equations by Theorem 1;
4: Solve the two built linear systems and let S^0 and S^1 be the Boolean matrices whose columns are just all possible solutions of the above two systems (for the non-essential participants, we assign them shares completely white);
5: If $S(i, j) = 0$, randomly choose a column from S^0;
6: If $S(i, j) = 1$, randomly choose a column from S^1;
7: Assign the values of the chosen column to the corresponding n random grids $R_1(i, j), R_2(i, j), \ldots, R_n(i, j)$;
8: **return** n random grids $R_1, R_2, \ldots, R_n$;

Participants of any qualified set can visually reconstruct the secret image by stacking their random grids together without the aid of any computational devices. Theoretical analysis on the proposed construction is formulated as follows.

Lemma 4 *Given a secret pixel s, an access structure* (Γ_Q, Γ_F) *is determined by the collection* Γ *of chosen minimal qualified sets. For* $X \in \Gamma_Q$*, we have* $T(R_X[s = 0]) > T(R_X[s = 1])$*. For* $X \in \Gamma_F$*, we have* $T(R_X[s = 0]) = T(R_X[s = 1])$.

Proof Given the collection Γ satisfying the conditions of Theorem 1, we could construct the basis matrices S^0 and S^1 of (Γ_Q, Γ_F)-VCS according to Theorem 1. Because a column is randomly chosen from the corresponding basis matrices and assigned to the corresponding random grids, we have $T(R_X[s = 0]) = \frac{\omega(S_X^0)}{m}$ and $T(R_X[s = 1]) = \frac{\omega(S_X^1)}{m}$. For $X \in \Gamma_Q$, we have $\omega(S_X^0) > \omega(S_X^1)$ and therefore $T(R_X[s = 0]) > T(R_X[s = 1])$. For $X \in \Gamma_F$, we have $\omega(S_X^0) = \omega(S_X^1)$ and therefore $T(R_X[s = 0]) = T(R_X[s = 1])$. □

Theorem 2 *Given a secret image S and a strong access structure* $(\Gamma_{Qual}, \Gamma_{Forb})$*, n random grids are generated by the proposed Algorithm 3. Algorithm 3 is a valid construction for a* $(\Gamma_{Qual}, \Gamma_{Forb})$*-VCRG for GAS.*

Proof Given a secret image S and a strong access structure $(\Gamma_{Qual}, \Gamma_{Forb})$, let (Γ_Q, Γ_F) be an access structure determined by the set Γ of chosen minimal qualified sets when sharing a secret pixel s. S^0 and S^1 denotes basis matrices of the corresponding (Γ_Q, Γ_F)-VCS. Obviously, we have $\Gamma_Q \subseteq \Gamma_{Qual}$ and $\Gamma_F \supseteq \Gamma_{Forb}$. For $X = \{i_1, i_2, \ldots, i_p\} \in \Gamma_{Qual}$, suppose that the chance for $X \in \Gamma_Q$ is ϕ. We can conclude $\phi > 0$ since the step 2 of Algorithm 2 guarantees that at least one minimal qualified set is randomly chosen from Γ_0 when sharing a secret pixel s. By Lemma 4, we have $T(R_X[s = 0]) - T(R_X[s = 1]) = \phi(\frac{\omega(S_X^0)}{m} - \frac{\omega(S_X^1)}{m}) > 0$. For $X \in \Gamma_{Forb}$, we immediately obtain $X \in \Gamma_F$ and then we have $T(R_X[s = 0]) - T(R_X[s = 1]) = 0$ by Lemma 4. According to Definitions 3 and 4, it

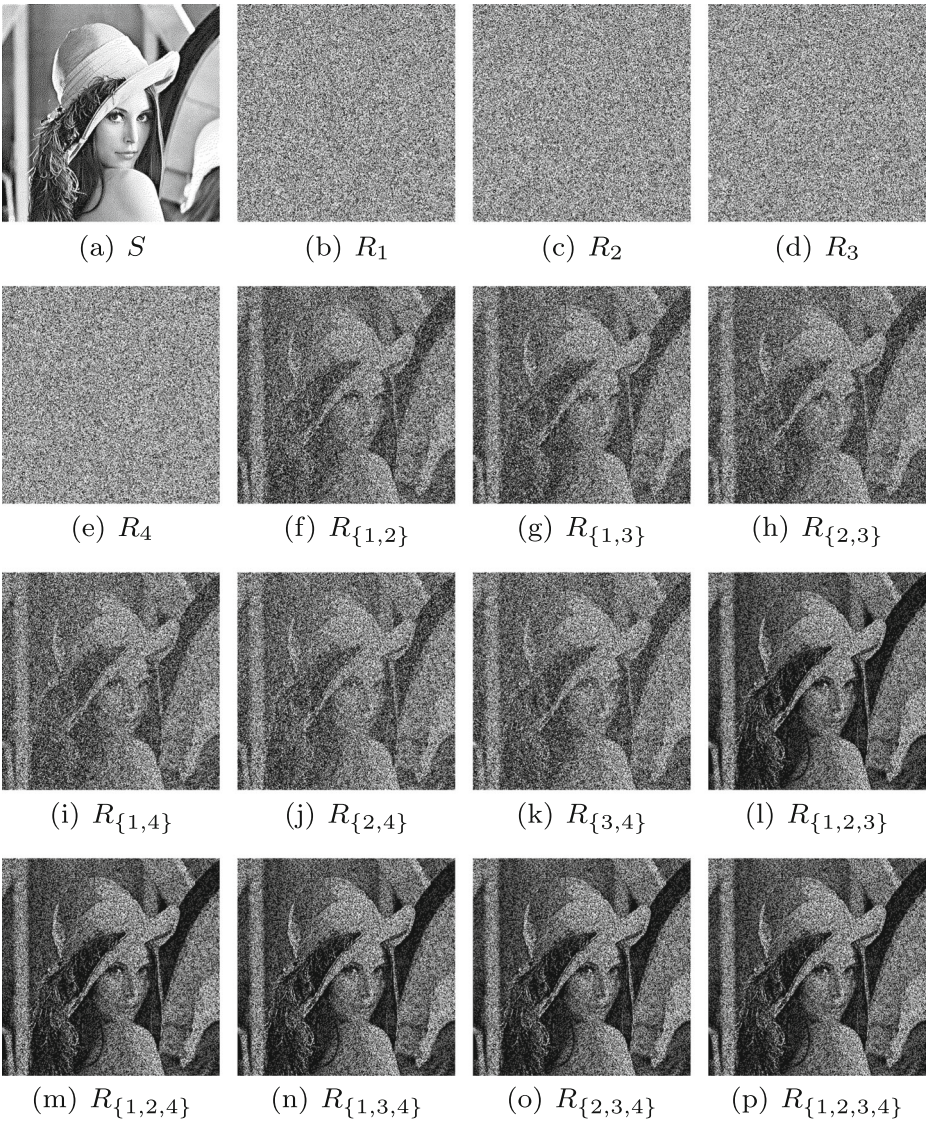


Fig. 2 Experimental results of our (2, 4)-VCRG

is easy to conclude that $T(R_X[S(0)]) > T(R_X[S(1)])$ for $X \in \Gamma_{Qual}$ and $T(R_X[S(0)]) = T(R_X[S(1)])$ for $X \in \Gamma_{Forb}$. □

6 Experiment and comparison

Extensive experimental results by the proposed VCRG are presented in this section. Moreover, some comparisons and further discussions among the proposed VCRG and related schemes are provided as well. Note that, it is quite complicated to choose collections of of the largest number of minimal qualified sets satisfying the conditions of Theorem 1 in Algorithm 2. Here we only give the choosing algorithm by computing search. The computer programs are coded in Matlab 7.0 and run in a PC with MS windows.

6.1 Experimental results

To demonstrate the effectiveness of our VCRG, two experiments are conducted: Experiment 1 focuses on threshold access structure, while Experiment 2 focuses on general access structure.

Experiment 1 An experiment of the proposed (2,4)-VCRG is presented in Fig. 2, where the basis of (2, 4) threshold access structure is

$$\Gamma_0 = \{\{1, 2\}, \{1, 3\}, \{1, 4\}, \{2, 3\}, \{2, 4\}, \{3, 4\}\}$$

and the set of forbidden sets is $\Gamma_{Forb} = \{\{1\}, \{2\}, \{3\}, \{4\}\}$. The secret image is shown in Fig. 2a and the four generated shares are exhibited in Fig. 2b–e. The stacked results of two random grids are exhibited in Fig. 2f–k. The stacked results of three random grids are exhibited in Fig. 2l–o. The stacked results of four random grids are exhibited in Fig. 2p. Furthermore, the contrast for this experiment is listed in Table 1.

Experiment 2 An experiment of the proposed GAS-VCRG is presented in Fig. 3, where $\Gamma_0 = \{\{1, 2, 3\}, \{1, 4\}, \{3, 4\}\}$ and the set of forbidden sets is $\Gamma_{Forb} = \{\{1\}, \{2\}, \{3\}, \{4\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, \{2, 4\}\}$. The secret image is shown in Fig. 3a and the four generated shares are exhibited in Fig. 3b–e. The stacked results of two random grids are exhibited in Fig. 3f–k. The stacked results of three random grids are exhibited in Fig. 3l–o. The stacked results of four random grids are exhibited in Fig. 3p. Furthermore, the contrast for this experiment is listed in Table 2.

As seen from the above experimental results, visually and quantitatively, the stacked results of random grids owned by forbidden sets of participants reveal nothing about

Table 1 Contrast for Experiment 1

	R_1	R_2	R_3	R_4	$R_{\{1,2\}}$
Contrast	0	0	0	0	0.287
	$R_{\{1,3\}}$	$R_{\{2,3\}}$	$R_{\{1,4\}}$	$R_{\{2,4\}}$	$R_{\{3,4\}}$
Contrast	0.28	0.284	0.283	0.289	0.286
	$R_{\{1,2,3\}}$	$R_{\{1,2,4\}}$	$R_{\{1,3,4\}}$	$R_{\{2,3,4\}}$	$R_{\{1,2,3,4\}}$
Contrast	0.499	0.499	0.499	0.499	0.499

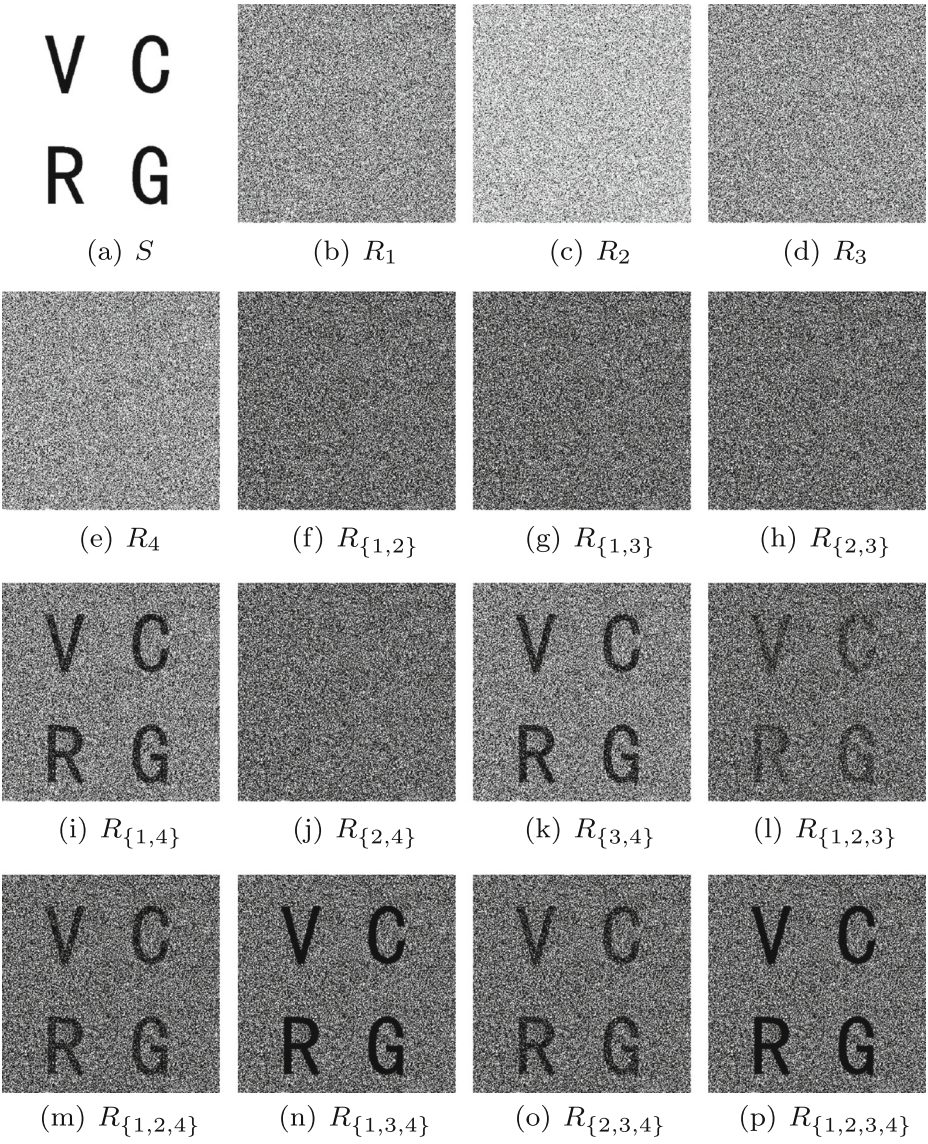


Fig. 3 Experimental results of our VCRG for an access structure determined by $\Gamma_0 = \{\{1, 2, 3\}, \{1, 4\}, \{3, 4\}\}$

Table 2 Contrast for Experiment 2

	R_1	R_2	R_3	R_4	$R_{\{1,2\}}$
Contrast	0	0	0	0	0
	$R_{\{1,3\}}$	$R_{\{2,3\}}$	$R_{\{1,4\}}$	$R_{\{2,4\}}$	$R_{\{3,4\}}$
Contrast	0	0	0.303	0	0.307
	$R_{\{1,2,3\}}$	$R_{\{1,2,4\}}$	$R_{\{1,3,4\}}$	$R_{\{2,3,4\}}$	$R_{\{1,2,3,4\}}$
Contrast	0.141	0.226	0.331	0.229	0.331

the secret image while the stacked results of random grids owned by qualified sets of participants reveal the secret information to our eyes.

6.2 Visual performance

Contrast is a measurement to evaluate the visual performance of the recovered secret image. Because De Prisco and De Santis [7] pointed out the future works that deal with VCRG and

Table 3 Comparison of contrast among the proposed (k, n)-VCRG, Shyu's Algorithm 4 [27] and Guo et al.'s VCRG [10] for $2 \leq k \leq n \leq 7$

No.	(k, n)	Our	Shyu's Algorithm 4 [27]	Guo et al.'s VCRG [10]
1	(2, 2)	$\alpha_2 = 0.5$	$\alpha_2 = 0.5$	$\alpha_2 = 0.5$
2	(2, 3)	$\alpha_2 = 0.288, \alpha_3 = 0.499$	$\alpha_2 = 0.288, \alpha_3 = 0.501$	$\alpha_2 = 0.146, \alpha_3 = 0.25$
3	(2, 4)	$\alpha_2 = 0.287, \alpha_3 = 0.499$	$\alpha_2 = 0.282, \alpha_3 = 0.5$	$\alpha_2 = 0.141, \alpha_3 = 0.25$
		$\alpha_4 = 0.499$	$\alpha_4 = 0.5$	$\alpha_4 = 0.25$
4	(2, 5)	$\alpha_2 = 0.246, \alpha_3 = 0.426$	$\alpha_2 = 0.252, \alpha_3 = 0.432$	$\alpha_2 = 0.085, \alpha_3 = 0.145$
		$\alpha_4 = 0, 5, \alpha_5 = 0.5$	$\alpha_4 = 0, 5, \alpha_5 = 0.5$	$\alpha_4 = 0.151, \alpha_5 = 0.126$
5	(2, 6)	$\alpha_2 = 0.251, \alpha_3 = 0.425$	$\alpha_2 = 0.247, \alpha_3 = 0.428$	$\alpha_2 = 0.087, \alpha_3 = 0.144$
		$\alpha_4 = 0.5, \alpha_5 = 0.5$	$\alpha_4 = 0.498, \alpha_5 = 0.498$	$\alpha_4 = 0.15, \alpha_5 = 0.125$
		$\alpha_6 = 0.5$	$\alpha_6 = 0.498$	$\alpha_6 = 0.125$
6	(2, 7)	$\alpha_2 = 0.237, \alpha_3 = 0.404$	$\alpha_2 = 0.234, \alpha_3 = 0.402$	$\alpha_2 = 0.062, \alpha_3 = 0.1$
		$\alpha_4 = 0.479, \alpha_5 = 0.5$	$\alpha_4 = 0.479, \alpha_5 = 0.5$	$\alpha_4 = 0.105, \alpha_5 = 0.089$
		$\alpha_6 = 0.5, \alpha_7 = 0.5$	$\alpha_6 = 0.5, \alpha_7 = 0.5$	$\alpha_6 = 0.071, \alpha_7 = 0.062$
7	(3, 3)	$\alpha_3 = 0.25$	$\alpha_3 = 0.25$	$\alpha_3 = 0.25$
8	(3, 4)	$\alpha_3 = 0.112, \alpha_4 = 0.25$	$\alpha_3 = 0.111, \alpha_4 = 0.249$	$\alpha_3 = 0.055, \alpha_4 = 0.125$
9	(3, 5)	$\alpha_3 = 0.09, \alpha_4 = 0.191$	$\alpha_3 = 0.082, \alpha_4 = 0.187$	$\alpha_3 = 0.023, \alpha_4 = 0.048$
		$\alpha_5 = 0.251$	$\alpha_5 = 0.249$	$\alpha_5 = 0.061$
10	(3, 6)	$\alpha_3 = 0.09, \alpha_4 = 0.190$	$\alpha_3 = 0.086, \alpha_4 = 0.191$	$\alpha_3 = 0.022, \alpha_4 = 0.05$
		$\alpha_5 = 0.249, \alpha_6 = 0.249$	$\alpha_5 = 0.251, \alpha_6 = 0.251$	$\alpha_5 = 0.064, \alpha_6 = 0.064$
11	(3, 7)	$\alpha_3 = 0.073, \alpha_4 = 0.16$	$\alpha_3 = 0.073, \alpha_4 = 0.161$	$\alpha_3 = 0.014, \alpha_4 = 0.027$
		$\alpha_5 = 0.222, \alpha_6 = 0.25$	$\alpha_5 = 0.223, \alpha_6 = 0.251$	$\alpha_5 = 0.036, \alpha_6 = 0.036$
		$\alpha_7 = 0.25$	$\alpha_7 = 0.251$	$\alpha_7 = 0.031$
12	(4, 4)	$\alpha_4 = 0.125$	$\alpha_4 = 0.125$	$\alpha_4 = 0.125$
13	(4, 5)	$\alpha_4 = 0.044, \alpha_5 = 0.124$	$\alpha_4 = 0.047, \alpha_5 = 0.125$	$\alpha_4 = 0.023, \alpha_5 = 0.064$
14	(4, 6)	$\alpha_4 = 0.028, \alpha_5 = 0.077$	$\alpha_4 = 0.032, \alpha_5 = 0.079$	$\alpha_4 = 0.005, \alpha_5 = 0.018$
		$\alpha_6 = 0.124$	$\alpha_6 = 0.125$	$\alpha_6 = 0.031$
15	(4, 7)	$\alpha_4 = 0.031, \alpha_5 = 0.072$	$\alpha_4 = 0.024, \alpha_5 = 0.066$	$\alpha_4 = 0.003, \alpha_5 = 0.01$
		$\alpha_6 = 0.108, \alpha_7 = 0.125$	$\alpha_6 = 0.103, \alpha_7 = 0.125$	$\alpha_6 = 0.013, \alpha_7 = 0.016$
16	(5, 5)	$\alpha_5 = 0.063$	$\alpha_5 = 0.063$	$\alpha_5 = 0.063$
17	(5, 6)	$\alpha_5 = 0.02, \alpha_6 = 0.062$	$\alpha_5 = 0.021, \alpha_6 = 0.062$	$\alpha_5 = 0.009, \alpha_6 = 0.031$
18	(5, 7)	$\alpha_5 = 0.011, \alpha_6 = 0.036$	$\alpha_5 = 0.009, \alpha_6 = 0.033$	$\alpha_5 = 0.003, \alpha_6 = 0.008$
		$\alpha_7 = 0.063$	$\alpha_7 = 0.062$	$\alpha_7 = 0.016$
19	(6, 6)	$\alpha_6 = 0.031$	$\alpha_6 = 0.031$	$\alpha_6 = 0.031$
20	(6, 7)	$\alpha_6 = 0.009, \alpha_7 = 0.032$	$\alpha_6 = 0.009, \alpha_7 = 0.032$	$\alpha_6 = 0.004, \alpha_7 = 0.016$
21	(7, 7)	$\alpha_7 = 0.016$	$\alpha_7 = 0.016$	$\alpha_7 = 0.016$

VCS should not ignore each other in comparison of contrast defined by α_{ES} for VCS and α_{RG} for VCRG, we are going to provide comparison of contrast between our VCRG and other schemes to demonstrate the advantage of our construction. Furthermore, to make the comparison clearer, we give the definition of average contrast $\overline{\alpha}$ as follows:

$$\overline{\alpha} = \frac{\sum_{X \in \Gamma_{Qual}} \alpha_X}{|\Gamma_{Qual}|}, \tag{16}$$

where α_X denotes the contrast of recovered secret image by the qualified set X.

For threshold access structures, Table 3 presents the contrasts of Shyu's Algorithm 4 [27], Guo et al.' scheme [10] and the proposed construction, where $2 \leq k \leq n \leq 7$. Note that, α_p denotes the contrast of recovered secret image by stacking p random grids since any p random grids achieve the same contrast. Figure 4 illustrates the average contrast for Table 3. From Table 3 and Fig. 4, we find that our contrast is larger than Guo et al.'s contrast [10]. Moreover, our contrast is almost the same as the contrast achieved by Shyu's Algorithm 4 [27]. However, Shyu's Algorithm 4 [27] is confined to threshold schemes. Also note that, Shyu compared his method with the existing VCSs in contrast, and concluded that the contrast of his (k, n)-VCRG is competitive to that of the existing (k, n)-VCSs (please refer to the paper [27]). Hence, we herein omit the comparison of contrast between our VCRG and the existing (k, n)-VCSs.

For general access structures, Table 4 presents the comparison of contrast among the proposed VCRG, Wu and Sun's GAS-VCRG [32] and Shyu's VCRG [26], and Table 5 presents the comparison of contrast among the proposed VCRG, Ateniese et al.'s GAS-VCS [3] and Adhikari's GAS-VCS [2]. In the above two tables, different access structures are adopted, the contrast of recovered secret image by the qualified set $\{i_1, i_2, \ldots, i_p\}$ is represented by $\alpha_{i_1,i_2,\ldots,i_p}$, CA denotes the Ateniese et al.'s construction using cumulative array and SS denotes the Ateniese et al.'s construction using smaller schemes [3]. Note that, because both of Shyu's method [26] and Ateniese et al.'s CA [3] achieve a constant contrast for an access structure, we omit the subscript $\{i_1, i_2, \ldots, i_p\}$ in $\alpha_{i_1,i_2,\ldots,i_p}$. Figures 5 and 6 illustrate the average contrast for Tables 4 and 5, respectively. From Table 4 and Fig. 5, we find that our contrast is larger than those of Wu and Sun's method [32] and Shyu's two

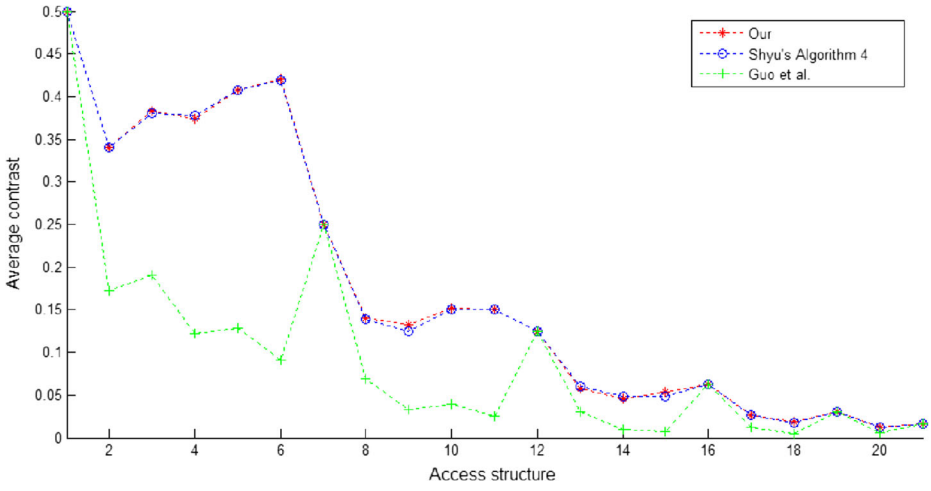


Fig. 4 Average contrast for Table 3

Table 4 Comparison of contrast among the proposed VCRG, Wu and Sun's GAS-VCRG [32] and Shyu's GAS-VCRG [26]

No.	Basis Γ_0	Our	Wu and Sun [32]	Shyu [26]	
				Algorithm 2	Algorithm 3
1	{1, 2}, {1, 3}	$\alpha_{1,2} = 0.5, \alpha_{1,3} = 0.5,$ $\alpha_{1,2,3} = 0.5$	$\alpha_{1,2} = 0.224, \alpha_{1,3} = 0.223,$ $\alpha_{1,2,3} = 0.25$	$\alpha_{1,2} = 0.25, \alpha_{1,3} = 0.25,$ $\alpha_{1,2,3} = 0.25$	$\alpha = 0.5$
2	{1, 2}, {2, 3}	$\alpha_{1,2} = 0.5, \alpha_{2,3} = 0.5,$ $\alpha_{1,2,3} = 0.5$	$\alpha_{1,2} = 0.221, \alpha_{2,3} = 0.222,$ $\alpha_{1,2,3} = 0.249$	$\alpha_{1,2} = 0.25, \alpha_{2,3} = 0.25,$ $\alpha_{1,2,3} = 0.25$	$\alpha = 0.5$
3	{1, 3}, {2, 3}	$\alpha_{1,3} = 0.5, \alpha_{2,3} = 0.5,$ $\alpha_{1,2,3} = 0.5$	$\alpha_{1,3} = 0.222, \alpha_{2,3} = 0.221,$ $\alpha_{1,2,3} = 0.25$	$\alpha_{1,3} = 0.25, \alpha_{2,3} = 0.25,$ $\alpha_{1,2,3} = 0.25$	$\alpha = 0.5$
4	{1, 2}, {1, 3}, {2, 3}	$\alpha_{1,2} = 0.288, \alpha_{1,3} = 0.288,$ $\alpha_{2,3} = 0.288, \alpha_{1,2,3} = 0.499$	$\alpha_{1,2} = 0.141, \alpha_{1,3} = 0.145,$ $\alpha_{2,3} = 0.140, \alpha_{1,2,3} = 0.25$	$\alpha_{1,2} = 0.125, \alpha_{1,3} = 0.125,$ $\alpha_{2,3} = 0.125, \alpha_{1,2,3} = 0.125$	$\alpha = 0.25$
5	{1, 2}, {2, 3}, {3, 4}	$\alpha_{1,2} = 0.284, \alpha_{2,3} = 0.309,$ $\alpha_{3,4} = 0.282, \alpha_{1,2,3} = 0.417,$ $\alpha_{1,2,4} = 0.212, \alpha_{1,3,4} = 0.211,$ $\alpha_{2,3,4} = 0.417, \alpha_{1,2,3,4} = 0.417$	$\alpha_{1,2} = 0.141, \alpha_{2,3} = 0.142,$ $\alpha_{3,4} = 0.144, \alpha_{1,2,3} = 0.159,$ $\alpha_{1,2,4} = 0.077, \alpha_{1,3,4} = 0.079,$ $\alpha_{2,3,4} = 0.159, \alpha_{1,2,3,4} = 0.125$	$\alpha_{1,2} = 0.250, \alpha_{2,3} = 0.125,$ $\alpha_{3,4} = 0.250, \alpha_{1,2,3} = 0.125,$ $\alpha_{1,2,4} = 0.125, \alpha_{1,3,4} = 0.125,$ $\alpha_{2,3,4} = 0.125, \alpha_{1,2,3,4} = 0.125$	$\alpha = 0.25$
6	{1, 2}, {1, 3}, {1, 4}	$\alpha_{1,2} = 0.5, \alpha_{1,3} = 0.5,$ $\alpha_{1,4} = 0.5, \alpha_{1,2,3} = 0.5,$ $\alpha_{1,2,4} = 0.5, \alpha_{1,3,4} = 0.5,$ $\alpha_{1,2,3,4} = 0.5$	$\alpha_{1,2} = 0.145, \alpha_{1,3} = 0.144,$ $\alpha_{1,4} = 0.143, \alpha_{1,2,3} = 0.162,$ $\alpha_{1,2,4} = 0.159, \alpha_{1,3,4} = 0.161,$ $\alpha_{1,2,3,4} = 0.126$	$\alpha_{1,2} = 0.125, \alpha_{1,3} = 0.125,$ $\alpha_{1,4} = 0.125, \alpha_{1,2,3} = 0.125,$ $\alpha_{1,2,4} = 0.125, \alpha_{1,3,4} = 0.125,$ $\alpha_{1,2,3,4} = 0.125$	$\alpha = 0.5$
7	{1, 2}, {1, 4}, {2, 3}, {3, 4}	$\alpha_{1,2} = 0.5, \alpha_{1,4} = 0.5,$ $\alpha_{2,3} = 0.5, \alpha_{3,4} = 0.5,$ $\alpha_{1,2,3} = 0.5, \alpha_{1,2,4} = 0.5,$ $\alpha_{1,3,4} = 0.5, \alpha_{2,3,4} = 0.5,$ $\alpha_{1,2,3,4} = 0.5$	$\alpha_{1,2} = 0.105, \alpha_{1,4} = 0.105,$ $\alpha_{2,3} = 0.103, \alpha_{3,4} = 0.102,$ $\alpha_{1,2,3} = 0.117, \alpha_{1,2,4} = 0.118,$ $\alpha_{1,3,4} = 0.117, \alpha_{2,3,4} = 0.115,$ $\alpha_{1,2,3,4} = 0.124$	$\alpha_{1,2} = 0.125, \alpha_{1,4} = 0.125,$ $\alpha_{2,3} = 0.125, \alpha_{3,4} = 0.125,$ $\alpha_{1,2,3} = 0.063, \alpha_{1,2,4} = 0.063,$ $\alpha_{1,3,4} = 0.063, \alpha_{2,3,4} = 0.063,$ $\alpha_{1,2,3,4} = 0.063$	$\alpha = 0.5$

Table 4 (continued)

No.	Basis Γ_0	Our	Wu and Sun [32]	Shyu [26]	
				Algorithm 2	Algorithm 3
8	{1, 2}, {2, 3}, {2, 4}, {3, 4}	$\alpha_{1,2} = 0.385, \alpha_{2,3} = 0.397, \alpha_{2,4} = 0.388, \alpha_{3,4} = 0.095, \alpha_{1,2,3} = 0.430, \alpha_{1,2,4} = 0.417, \alpha_{1,3,4} = 0.079, \alpha_{2,3,4} = 0.479, \alpha_{1,2,3,4} = 0.479$	$\alpha_{1,2} = 0.104, \alpha_{2,3} = 0.105, \alpha_{2,4} = 0.103, \alpha_{3,4} = 0.105, \alpha_{1,2,3} = 0.117, \alpha_{1,2,4} = 0.116, \alpha_{1,3,4} = 0.058, \alpha_{2,3,4} = 0.181, \alpha_{1,2,3,4} = 0.125$	$\alpha_{1,2} = 0.125, \alpha_{2,3} = 0.063, \alpha_{2,4} = 0.063, \alpha_{3,4} = 0.125, \alpha_{1,2,3} = 0.063, \alpha_{1,2,4} = 0.063, \alpha_{1,3,4} = 0.063, \alpha_{2,3,4} = 0.063, \alpha_{1,2,3,4} = 0.063$	$\alpha = 0.25$
9	{1, 2}, {1, 3}, {1, 4}, {2, 3}, {2, 4}, {3, 4}	$\alpha_{1,2} = 0.287, \alpha_{1,3} = 0.287, \alpha_{1,4} = 0.287, \alpha_{2,3} = 0.287, \alpha_{2,4} = 0.287, \alpha_{3,4} = 0.287, \alpha_{1,2,3} = 0.499, \alpha_{1,2,4} = 0.499, \alpha_{1,3,4} = 0.499, \alpha_{2,3,4} = 0.499, \alpha_{1,2,3,4} = 0.499$	$\alpha_{1,2} = 0.066, \alpha_{1,3} = 0.069, \alpha_{1,4} = 0.071, \alpha_{2,3} = 0.07, \alpha_{2,4} = 0.067, \alpha_{3,4} = 0.07, \alpha_{1,2,3} = 0.118, \alpha_{1,2,4} = 0.116, \alpha_{1,3,4} = 0.119, \alpha_{2,3,4} = 0.117, \alpha_{1,2,3,4} = 0.125$	$\alpha_{1,2} = 0.031, \alpha_{1,3} = 0.031, \alpha_{1,4} = 0.031, \alpha_{2,3} = 0.031, \alpha_{2,4} = 0.031, \alpha_{3,4} = 0.031, \alpha_{1,2,3} = 0.016, \alpha_{1,2,4} = 0.016, \alpha_{1,3,4} = 0.016, \alpha_{2,3,4} = 0.016, \alpha_{1,2,3,4} = 0.016$	$\alpha = 0.125$
10	{1, 2, 3}, {1, 4}	$\alpha_{1,4} = 0.5, \alpha_{1,2,3} = 0.25, \alpha_{1,2,4} = 0.25, \alpha_{1,3,4} = 0.25, \alpha_{1,2,3,4} = 0.25$	$\alpha_{1,4} = 0.225, \alpha_{1,2,3} = 0.119, \alpha_{1,2,4} = 0.119, \alpha_{1,3,4} = 0.119, \alpha_{1,2,3,4} = 0.125$	$\alpha_{1,4} = 0.251, \alpha_{1,2,3} = 0.125, \alpha_{1,2,4} = 0.125, \alpha_{1,3,4} = 0.125, \alpha_{1,2,3,4} = 0.125$	$\alpha = 0.25$
11	{1, 2, 3}, {1, 4}, {3, 4}	$\alpha_{1,4} = 0.303, \alpha_{3,4} = 0.307, \alpha_{1,2,3} = 0.141, \alpha_{1,2,4} = 0.226, \alpha_{1,3,4} = 0.331, \alpha_{2,3,4} = 0.229, \alpha_{1,2,3,4} = 0.331$	$\alpha_{1,4} = 0.145, \alpha_{3,4} = 0.145, \alpha_{1,2,3} = 0.076, \alpha_{1,2,4} = 0.077, \alpha_{1,3,4} = 0.161, \alpha_{2,3,4} = 0.077, \alpha_{1,2,3,4} = 0.125$	$\alpha_{1,4} = 0.125, \alpha_{3,4} = 0.125, \alpha_{1,2,3} = 0.062, \alpha_{1,2,4} = 0.062, \alpha_{1,3,4} = 0.062, \alpha_{2,3,4} = 0.062, \alpha_{1,2,3,4} = 0.062$	$\alpha = 0.125$
12	{1, 3, 4}, {1, 2}, {2, 3}, {2, 4}	$\alpha_{1,2} = 0.4, \alpha_{2,3} = 0.403, \alpha_{2,4} = 0.401, \alpha_{1,2,3} = 0.409, \alpha_{1,2,4} = 0.407, \alpha_{1,3,4} = 0.051, \alpha_{2,3,4} = 0.411, \alpha_{1,2,3,4} = 0.438$	$\alpha_{1,2} = 0.108, \alpha_{2,3} = 0.106, \alpha_{2,4} = 0.110, \alpha_{1,2,3} = 0.119, \alpha_{1,2,4} = 0.120, \alpha_{1,3,4} = 0.058, \alpha_{2,3,4} = 0.121, \alpha_{1,2,3,4} = 0.126$	$\alpha_{1,2} = 0.063, \alpha_{2,3} = 0.063, \alpha_{2,4} = 0.063, \alpha_{1,2,3} = 0.032, \alpha_{1,2,4} = 0.032, \alpha_{1,3,4} = 0.032, \alpha_{2,3,4} = 0.032, \alpha_{1,2,3,4} = 0.032$	$\alpha = 0.125$

Table 4 (continued)

No.	Basis Γ_0	Our	Wu and Sun [32]	Shyu [26]	
				Algorithm 2	Algorithm 3
13	{1, 2, 3}, {1, 2, 4}	$\alpha_{1,2,3} = 0.25, \alpha_{1,2,4} = 0.25,$ $\alpha_{1,2,3,4} = 0.25$	$\alpha_{1,2,3} = 0.119, \alpha_{1,2,4} = 0.118,$ $\alpha_{1,2,3,4} = 0.125$	$\alpha_{1,2,3} = 0.062, \alpha_{1,2,4} = 0.062,$ $\alpha_{1,2,3,4} = 0.062$	$\alpha = 0.25$
14	{1, 2, 4}, {1, 3, 4}, {2, 3}	$\alpha_{2,3} = 0.284, \alpha_{1,2,3} = 0.153,$ $\alpha_{1,2,4} = 0.158, \alpha_{1,3,4} = 0.154,$ $\alpha_{2,3,4} = 0.153, \alpha_{1,2,3,4} = 0.251$	$\alpha_{2,3} = 0.144, \alpha_{1,2,3} = 0.077,$ $\alpha_{1,2,4} = 0.079, \alpha_{1,3,4} = 0.077,$ $\alpha_{2,3,4} = 0.079, \alpha_{1,2,3,4} = 0.127$	$\alpha_{2,3} = 0.126, \alpha_{1,2,3} = 0.031,$ $\alpha_{1,2,4} = 0.031, \alpha_{1,3,4} = 0.031,$ $\alpha_{2,3,4} = 0.031, \alpha_{1,2,3,4} = 0.031$	$\alpha = 0.063$
15	{1, 2, 3}, {1, 2, 4}, {1, 3, 4}	$\alpha_{1,2,3} = 0.152, \alpha_{1,2,4} = 0.154,$ $\alpha_{1,3,4} = 0.152, \alpha_{1,2,3,4} = 0.251$	$\alpha_{1,2,3} = 0.077, \alpha_{1,2,4} = 0.079,$ $\alpha_{1,3,4} = 0.075, \alpha_{1,2,3,4} = 0.125$	$\alpha_{1,2,3} = 0.016, \alpha_{1,2,4} = 0.016,$ $\alpha_{1,3,4} = 0.016, \alpha_{1,2,3,4} = 0.016$	$\alpha = 0.125$
16	{1, 2, 3}, {1, 2, 4}, {1, 3, 4}, {2, 3, 4}	$\alpha_{1,2,3} = 0.112, \alpha_{1,2,4} = 0.112,$ $\alpha_{1,3,4} = 0.112, \alpha_{2,3,4} = 0.112,$ $\alpha_{1,2,3,4} = 0.25$	$\alpha_{1,2,3} = 0.057, \alpha_{1,2,4} = 0.058,$ $\alpha_{1,3,4} = 0.057, \alpha_{2,3,4} = 0.058,$ $\alpha_{1,2,3,4} = 0.126$	$\alpha_{1,2,3} = 0.008, \alpha_{1,2,4} = 0.008,$ $\alpha_{1,3,4} = 0.008, \alpha_{2,3,4} = 0.008,$ $\alpha_{1,2,3,4} = 0.008$	$\alpha = 0.031$

Table 5 Comparison of contrast among the proposed VCRG, Ateniese et al.'s GAS-VCS [3] and Adhikari's GAS-VCS [2]

No.	Basis Γ_0	Our	Ateniese et al. [3]		Adhikari [2]
			CA	SS	
1	$\{1,2\},\{1,3\}$	$\alpha_{1,2}=0.5, \alpha_{1,3}=0.5,$ $\alpha_{1,2,3}=0.5$	$\alpha=0.5$	$\alpha_{1,2}=0.2, \alpha_{1,3}=0.2,$ $\alpha_{1,2,3}=0.5$	$\alpha_{1,2}=0.5, \alpha_{1,3}=0.5,$ $\alpha_{1,2,3}=0.5$
2	$\{1,2\},\{2,3\}$	$\alpha_{1,2}=0.5, \alpha_{2,3}=0.5,$ $\alpha_{1,2,3}=0.5$	$\alpha=0.5$	$\alpha_{1,2}=0.2, \alpha_{2,3}=0.2,$ $\alpha_{1,2,3}=0.5$	$\alpha_{1,2}=0.5, \alpha_{2,3}=0.5,$ $\alpha_{1,2,3}=0.5$
3	$\{1,3\},\{2,3\}$	$\alpha_{1,3}=0.5, \alpha_{2,3}=0.5,$ $\alpha_{1,2,3}=0.5$	$\alpha=0.5$	$\alpha_{1,3}=0.2, \alpha_{2,3}=0.2,$ $\alpha_{1,2,3}=0.5$	$\alpha_{1,3}=0.5, \alpha_{2,3}=0.5,$ $\alpha_{1,2,3}=0.5$
4	$\{1,2\},\{1,3\},\{2,3\}$	$\alpha_{1,2}=0.288, \alpha_{1,3}=0.288,$ $\alpha_{2,3}=0.288, \alpha_{1,2,3}=0.499$	$\alpha=0.25$	$\alpha_{1,2}=0.125, \alpha_{1,3}=0.125,$ $\alpha_{2,3}=0.125, \alpha_{1,2,3}=0.5$	$\alpha_{1,2}=0.25, \alpha_{1,3}=0.25,$ $\alpha_{2,3}=0.25, \alpha_{1,2,3}=0.5$
5	$\{1,2\},\{2,3\},\{3,4\}$	$\alpha_{1,2}=0.284, \alpha_{2,3}=0.309,$ $\alpha_{3,4}=0.282, \alpha_{1,2,3}=0.417,$ $\alpha_{1,2,4}=0.212, \alpha_{1,3,4}=0.211,$ $\alpha_{2,3,4}=0.417, \alpha_{1,2,3,4}=0.417$	$\alpha=0.25$	$\alpha_{1,2}=0.111, \alpha_{2,3}=0.111,$ $\alpha_{3,4}=0.111, \alpha_{1,2,3}=0.286,$ $\alpha_{1,2,4}=0.125, \alpha_{1,3,4}=0.125,$ $\alpha_{2,3,4}=0.286, \alpha_{1,2,3,4}=0.5$	$\alpha_{1,2}=0.167, \alpha_{2,3}=0.2,$ $\alpha_{3,4}=0.2, \alpha_{1,2,3}=0.2,$ $\alpha_{1,2,4}=0.2, \alpha_{1,3,4}=0.2,$ $\alpha_{2,3,4}=0.5, \alpha_{1,2,3,4}=0.5$
6	$\{1,2\},\{1,3\},\{1,4\}$	$\alpha_{1,2}=0.5, \alpha_{1,3}=0.5,$ $\alpha_{1,4}=0.5, \alpha_{1,2,3}=0.5,$ $\alpha_{1,2,4}=0.5, \alpha_{1,3,4}=0.5,$ $\alpha_{1,2,3,4}=0.5$	$\alpha=0.5$	$\alpha_{1,2}=0.125, \alpha_{1,3}=0.125,$ $\alpha_{1,4}=0.125, \alpha_{1,2,3}=0.286,$ $\alpha_{1,2,4}=0.286, \alpha_{1,3,4}=0.286,$ $\alpha_{1,2,3,4}=0.5$	$\alpha_{1,2}=0.2, \alpha_{1,3}=0.2,$ $\alpha_{1,4}=0.2, \alpha_{1,2,3}=0.2,$ $\alpha_{1,2,4}=0.5, \alpha_{1,3,4}=0.5,$ $\alpha_{1,2,3,4}=0.5$
7	$\{1,2\},\{1,4\},\{2,3\},\{3,4\}$	$\alpha_{1,2}=0.5, \alpha_{1,4}=0.5,$ $\alpha_{2,3}=0.5, \alpha_{3,4}=0.5,$ $\alpha_{1,2,3}=0.5, \alpha_{1,2,4}=0.5,$ $\alpha_{1,3,4}=0.5, \alpha_{2,3,4}=0.5,$ $\alpha_{1,2,3,4}=0.5$	$\alpha=0.5$	$\alpha_{1,2}=0.083, \alpha_{1,4}=0.083,$ $\alpha_{2,3}=0.083, \alpha_{3,4}=0.083,$ $\alpha_{1,2,3}=0.25, \alpha_{1,2,4}=0.25,$ $\alpha_{1,3,4}=0.25, \alpha_{2,3,4}=0.25,$ $\alpha_{1,2,3,4}=0.5$	$\alpha_{1,2}=0.2, \alpha_{1,4}=0.2,$ $\alpha_{2,3}=0.2, \alpha_{3,4}=0.2,$ $\alpha_{1,2,3}=0.5, \alpha_{1,2,4}=0.2,$ $\alpha_{1,3,4}=0.5, \alpha_{2,3,4}=0.2,$ $\alpha_{1,2,3,4}=0.5$

Table 5 (continued)

No.	Basis Γ_0	Our	Ateniese et al. [3]		Adhikari [2]
			CA	SS	
8	$\{1,2\},\{2,3\},\{2,4\},\{3,4\}$	$\alpha_{1,2}=0.385, \alpha_{2,3}=0.397,$ $\alpha_{2,4}=0.388, \alpha_{3,4}=0.095,$ $\alpha_{1,2,3}=0.430, \alpha_{1,2,4}=0.417,$ $\alpha_{1,3,4}=0.079, \alpha_{2,3,4}=0.479,$ $\alpha_{1,2,3,4}=0.479$	$\alpha=0.25$	$\alpha_{1,2}=0.083, \alpha_{2,3}=0.091,$ $\alpha_{1,2,3}=0.2, \alpha_{1,2,4}=0.2,$ $\alpha_{1,3,4}=0.091, \alpha_{2,3,4}=0.333,$ $\alpha_{1,2,3,4}=0.5$	$\alpha_{1,2}=0.2, \alpha_{2,3}=0.2,$ $\alpha_{2,4}=0.2, \alpha_{3,4}=0.2,$ $\alpha_{1,2,3}=0.2, \alpha_{1,2,4}=0.5,$ $\alpha_{1,3,4}=0.2, \alpha_{2,3,4}=0.5,$ $\alpha_{1,2,3,4}=0.5$
9	$\{1,2\},\{1,3\},\{1,4\},\{2,3\},\{2,4\},\{3,4\}$	$\alpha_{1,2}=0.287, \alpha_{1,3}=0.287,$ $\alpha_{1,4}=0.287, \alpha_{2,3}=0.287,$ $\alpha_{2,4}=0.287, \alpha_{3,4}=0.287,$ $\alpha_{1,2,3}=0.499, \alpha_{1,2,4}=0.499,$ $\alpha_{1,3,4}=0.499, \alpha_{2,3,4}=0.499,$ $\alpha_{1,2,3,4}=0.499$	$\alpha=0.125$	$\alpha_{1,2}=0.056, \alpha_{1,3}=0.056,$ $\alpha_{2,4}=0.056, \alpha_{3,4}=0.056,$ $\alpha_{1,2,3}=0.2, \alpha_{1,2,4}=0.2,$ $\alpha_{1,3,4}=0.2, \alpha_{2,3,4}=0.2,$ $\alpha_{1,2,3,4}=0.5$	$\alpha_{1,2}=0.1, \alpha_{1,3}=0.1,$ $\alpha_{1,4}=0.1, \alpha_{2,3}=0.1,$ $\alpha_{2,4}=0.1, \alpha_{3,4}=0.1,$ $\alpha_{1,2,3}=0.222, \alpha_{1,2,4}=0.375,$ $\alpha_{1,3,4}=0.375, \alpha_{2,3,4}=0.222,$ $\alpha_{1,2,3,4}=0.375$
10	$\{1,2,3\},\{1,4\}$	$\alpha_{1,4}=0.5, \alpha_{1,2,3}=0.25,$ $\alpha_{1,2,4}=0.25, \alpha_{1,3,4}=0.25,$ $\alpha_{1,2,3,4}=0.25$	$\alpha=0.25$	$\alpha_{1,4}=0.125, \alpha_{1,2,3}=0.143,$ $\alpha_{1,2,4}=0.143, \alpha_{1,3,4}=0.143,$ $\alpha_{1,2,3,4}=0.333$	$\alpha_{1,4}=0.5, \alpha_{1,2,3}=0.25,$ $\alpha_{1,2,4}=0.25, \alpha_{1,3,4}=0.25,$ $\alpha_{1,2,3,4}=0.25$
11	$\{1,2,3\},\{1,4\},\{3,4\}$	$\alpha_{1,4}=0.303, \alpha_{3,4}=0.307,$ $\alpha_{1,2,3}=0.141, \alpha_{1,2,4}=0.226,$ $\alpha_{1,3,4}=0.331, \alpha_{2,3,4}=0.229,$ $\alpha_{1,2,3,4}=0.331$	$\alpha=0.125$	$\alpha_{1,4}=0.091, \alpha_{3,4}=0.091,$ $\alpha_{1,2,3}=0.1, \alpha_{1,2,4}=0.1,$ $\alpha_{1,3,4}=0.222, \alpha_{2,3,4}=0.1,$ $\alpha_{1,2,3,4}=0.375$	$\alpha_{1,4}=0.143, \alpha_{3,4}=0.143,$ $\alpha_{1,2,3}=0.143, \alpha_{1,2,4}=0.143,$ $\alpha_{1,3,4}=0.333, \alpha_{2,3,4}=0.143,$ $\alpha_{1,2,3,4}=0.333$
12	$\{1,3,4\},\{1,2\},\{2,3\},\{2,4\}$	$\alpha_{1,2}=0.4, \alpha_{2,3}=0.403,$ $\alpha_{2,4}=0.401, \alpha_{1,2,3}=0.409,$ $\alpha_{1,2,4}=0.407, \alpha_{1,3,4}=0.051,$ $\alpha_{2,3,4}=0.411, \alpha_{1,2,3,4}=0.438$	$\alpha=0.125$	$\alpha_{1,2}=0.071, \alpha_{2,3}=0.071,$ $\alpha_{2,4}=0.071, \alpha_{1,2,3}=0.167,$ $\alpha_{1,2,4}=0.167, \alpha_{1,3,4}=0.077,$ $\alpha_{2,3,4}=0.167, \alpha_{1,2,3,4}=0.4$	$\alpha_{1,2}=0.286, \alpha_{2,3}=0.143,$ $\alpha_{2,4}=0.143, \alpha_{1,2,3}=0.333,$ $\alpha_{1,2,4}=0.333, \alpha_{1,3,4}=0.143,$ $\alpha_{2,3,4}=0.143, \alpha_{1,2,3,4}=0.333$

Table 5 (continued)

No.	Basis Γ_0	Our	Ateniese et al. [3]		Adhikari [2]
			CA	SS	
13	{1, 2, 3}, {1, 2, 4}	$\alpha_{1,2,3} = 0.25, \alpha_{1,2,4} = 0.25,$ $\alpha_{1,2,3,4} = 0.25$	$\alpha = 0.25$	$\alpha_{1,2,3} = 0.111, \alpha_{1,2,4} = 0.111,$ $\alpha_{1,2,3} = 0.25,$	$\alpha_{1,2,3,4} = 0.25\alpha_{1,2,4} = 0.25,$ $\alpha_{1,2,3,4} = 0.25$
14	{1, 2, 4}, {1, 3, 4}, {2, 3}	$\alpha_{2,3} = 0.284, \alpha_{1,2,3} = 0.153,$ $\alpha_{1,2,4} = 0.158, \alpha_{1,3,4} = 0.154,$ $\alpha_{2,3,4} = 0.153, \alpha_{1,2,3,4} = 0.251$	$\alpha = 0.063$	$\alpha_{2,3} = 0.071, \alpha_{1,2,3} = 0.083,$ $\alpha_{1,2,4} = 0.083, \alpha_{1,3,4} = 0.083,$ $\alpha_{2,3,4} = 0.083, \alpha_{1,2,3,4} = 0.3$	$\alpha_{2,3} = 0.125, \alpha_{1,2,3} = 0.143,$ $\alpha_{1,2,4} = 0.143, \alpha_{1,3,4} = 0.143,$ $\alpha_{2,3,4} = 0.143, \alpha_{1,2,3,4} = 0.333$
15	{1, 2, 3}, {1, 2, 4}, {1, 3, 4}	$\alpha_{1,2,3} = 0.152, \alpha_{1,2,4} = 0.154,$ $\alpha_{1,3,4} = 0.152, \alpha_{1,2,3,4} = 0.251$	$\alpha = 0.125$	$\alpha_{1,2,3} = 0.071, \alpha_{1,2,4} = 0.071,$ $\alpha_{1,3,4} = 0.071, \alpha_{1,2,3,4} = 0.25$	$\alpha_{1,2,3} = 0.111, \alpha_{1,2,4} = 0.111,$ $\alpha_{1,3,4} = 0.111, \alpha_{1,2,3,4} = 0.25$
16	{1, 2, 3}, {1, 2, 4}, {1, 3, 4}, {2, 3, 4}	$\alpha_{1,2,3} = 0.112, \alpha_{1,2,4} = 0.112,$ $\alpha_{1,3,4} = 0.112, \alpha_{2,3,4} = 0.112,$ $\alpha_{1,2,3,4} = 0.25$	$\alpha = 0.031$	$\alpha_{1,2,3} = 0.053, \alpha_{1,2,4} = 0.053,$ $\alpha_{1,3,4} = 0.053, \alpha_{2,3,4} = 0.053,$ $\alpha_{1,2,3,4} = 0.25$	$\alpha_{1,2,3} = 0.111, \alpha_{1,2,4} = 0.111,$ $\alpha_{1,3,4} = 0.111, \alpha_{2,3,4} = 0.111,$ $\alpha_{1,2,3,4} = 0.25$

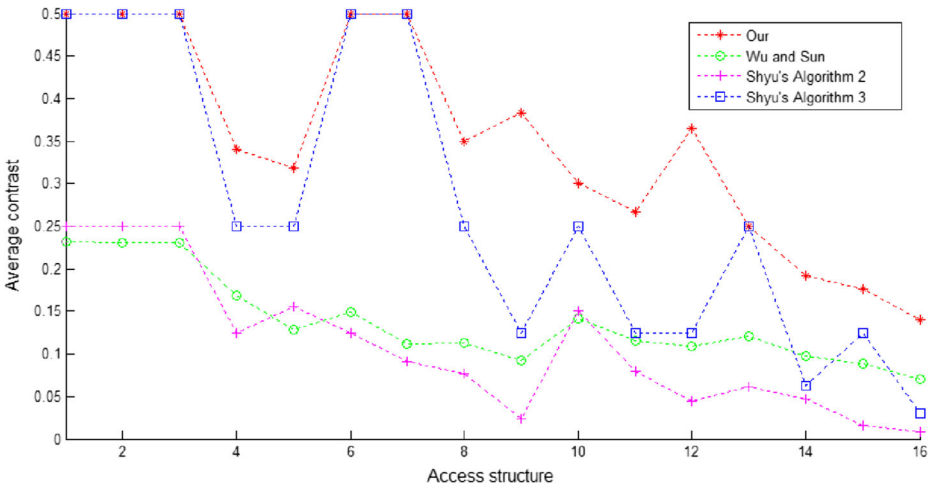


Fig. 5 Average contrast for Table 4

methods [26]. From Table 5 and Fig. 6, we also find that our contrast is larger than those of Ateniese et al.'s CA and SS [3] and Adhikari's contrast [2]. Moreover, the constant contrast achieved by Shyu's Algorithm 3 [26] and Ateniese et al.'s CA [3] is $\frac{1}{2^{|Z_m|-1}}$, so the contrast is too small when $|Z_m|$ is large. For example, when the access structure is $(3, 5)$ threshold case, the contrast of Shyu's Algorithm 3 [26] and Ateniese et al.'s CA [3] is $\frac{1}{512} \approx 0.002$ while our average contrast is 0.132. Therefore, our construction is preferable when $|Z_m|$ is large. In summary, we achieve a better visual performance in the sense that the contrast of our VCRG is larger than those of the existing schemes for GAS.

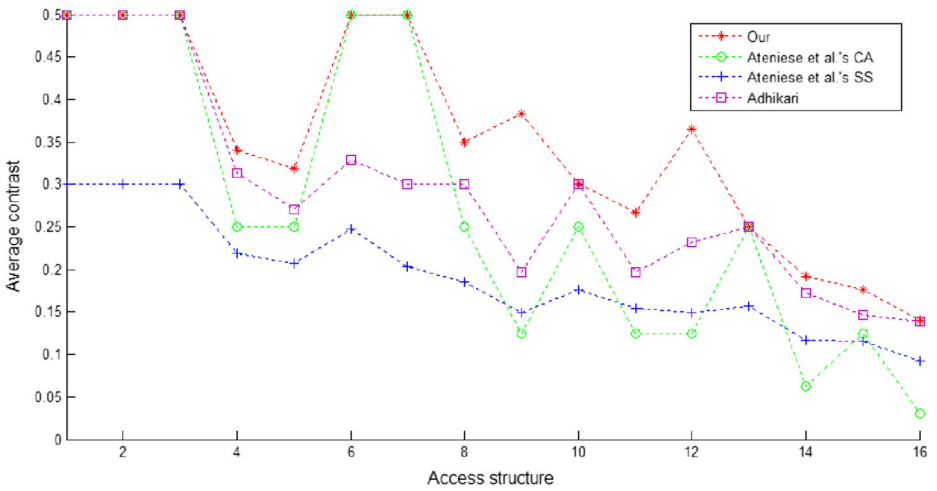


Fig. 6 Average contrast for Table 5

Table 6 Comparison of functionality among the proposed construction and related methods

Methods	Functionalities			
	Pixel expansion	Access structure	Enhanced contrast	Utility
Our	No	GAS	Yes	VCS and VCRG
Shyu [27]	No	(k,n)	Yes	VCRG
Shyu [26]	No	GAS	No	VCRG
Guo et al. [10]	No	(k,n)	No	VCRG
Wu and Sun [32]	No	GAS	No	VCRG
Ateniese et al. [3]	Yes	GAS	No	VCS
Adhikari [2]	Yes	GAS	No	VCS

6.3 Functionality

Functionality comparison among the proposed construction and related methods is demonstrated in Table 6. According to Table 6, major advantages of our construction are

- Flexible sharing strategy. General access structure can be implemented by the proposed construction, more complicated sharing strategy in real world can be conducted. It is superior to the threshold methods [10, 27].
- Enhanced contrast. Contrast is expected to be as large as possible so that human eyes can identify the visual information easily. Our contrast is enhanced in comparison with the methods [2, 3, 10, 26, 32].
- No pixel expansion. Our construction does not expand any pixel while the conventional VCSs [2, 3] take large pixel expansions which will increase storage and transmission bandwidth.
- Wide utility. The methods [10, 26, 27, 32] are elaborately designed for VCRG while the methods [2, 3] are elaborately designed for VCS. However, Theorem 1, supporting our construction, can be better applied to not only VCRG but also VCS. For example, any given access structure can be divided into several certain access structures, each of which satisfies the conditions of Theorem 1. Then we can construct VCS for every access group through solving linear equations and all constructed VCSs constitute a final VCS for the given access structure. The above method to construct VCS, as pointed out in [2], may minimize the pixel expansion of VCS.

7 Conclusion

In this paper, we exploit the algebraic aspects of VCS and propose an construction of VCRG based on the proposed linear algebraic technique. The experimental results demonstrate the feasibility and advantage of our construction. Moreover, our theory lays a sound and innovate foundation for the construction of VCS and VCRG from the theoretical point of view. There are some further researches including could we put forward an accurate expression of contrast, how does the content of the image affect the visual performance besides the

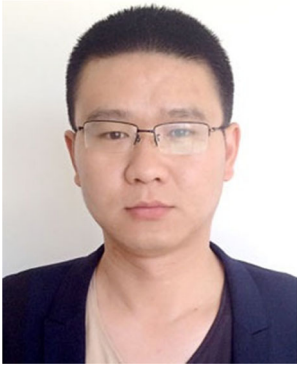
contrast, and so on. For practical applications, our construction would be very useful to develop a good contrast progressive scheme like [15].

Acknowledgements We would like to thank the anonymous reviewers for their important and helpful comments. This work was supported by the National Natural Science Foundation of China with No.61602513 and No.61671448, the Strategic Priority Research Program of the Chinese Academy of Sciences with No.XDA06010701, and the National Key R&D Program of China with No.2016YFB0800100.

References

1. Abu-Marie W, Gutub A, Abu-Mansour H (2010) Image based steganography using truth table based and determinate array on RGB indicator. Int J Signal Image Process 1(3):196–204
2. 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
3. Ateniese G, Blundo C, De Santis A, Stinson DR (1996) Visual cryptography for general access structures. Inf Comput 129(2):86–106
4. Blundo C, De Santis A, Stinson DR (1999) On the contrast in visual cryptography schemes. J Cryptol 12(4):261–289
5. Cimato S, De Prisco R, De Santis A (2005) Optimal colored threshold cisual cryptography schemes. Des Codes Crypt 35:311–335
6. D'Arco P, De Prisco R, De Santis A (2014) Measure-independent characterization of contrast optimal visual cryptography schemes. J Syst Softw 95:89–99
7. De Prisco R, De Santis A (2014) On the relation of random grid and deterministic visual cryptography. IEEE Trans Inf Forensics Secur 9(4):653–665
8. Eisen PA, Stinson DR (2002) Threshold visual cryptography schemes with specified whiteness levels of reconstructed pixels. Des Codes Crypt 25(1):15–61
9. Guo T, Liu F, Wu CK (2013) Visual cryptography for natural images and visual voting. In: Information security and cryptology. Lecture Notes in Computer Science, vol 7763. Springer, Berlin, pp 90–101
10. Guo T, Liu F, Wu CK (2013) Threshold visual secret sharing by random grids with improved contrast. J Syst Softw 86:2094–2109
11. Gutub A, Al-Qahtani A, Tabakh A (2009) Triple-A: secure RGB image steganography based on randomization. In: The 7th ACS/IEEE international conference on computer systems and applications (AICCSA-2009). IEEE, Morocco, pp 400–403
12. Hawkes LW, Yasinsac A, Cline C (2000) An application of visual cryptography to financial documents. Technical Report TR001001. Florida State University, Tallahassee, pp 1–7
13. Hou YC (2003) Visual cryptography for color images. Pattern Recogn 36(7):1619–1629
14. Hu CM, Tzeng WG (2007) Cheating prevention in visual cryptography. IEEE Trans Image Process 16(1):36–45
15. Jin D, Yan WQ, Kankanhalli MS (2005) Progressive color visual cryptography. J Electron Imaging 14(3):033019
16. Kafri O, Keren E (1987) Encryption of pictures and shapes by random grids. Optics Lett 12(6):377–379
17. Li P, Ma PJ, Li D (2012) Aspect ratio invariant visual cryptography scheme with exible size expansion. ICIC Express Lett 6(8):2033–2038
18. Lin CC, Tsai WH (2004) Secret image sharing with steganography and authentication. J Syst Softw 73(3):405–414
19. Liu F, Guo T (2015) Privacy protection display implementation method based on visual passwords. CN Patent App CN 201410542752
20. Liu F, Wu C, Lin X (2011) Cheating immune visual cryptography scheme. IET Inf Secur 5(1):51–59
21. Naor M, Pinkas B (1997) Visual authentication and identification. In: Advances in cryptology. Lecture Notes in Computer Science, vol 1294. Springer, Berlin, pp 322–336
22. Naor M, Shamir A (1995) Visual cryptography. In: Advances in cryptology. Lecture Notes in Computer Science, vol 950. Springer, Berlin, pp 1–12

23. Parvez MT, Gutub A (2008) RGB intensity based variable-bits image steganography. In: IEEE Asia-pacific services computing conference. IEEE, Taiwan, pp 1322–1327
24. Shyu S, Jiang H (2013) General constructions for threshold multiple-secret visual cryptographic shcemes. IEEE Trans Inf Forensics Secur 8(5):733–743
25. Shyu SJ (2007) Image encryption by random grids. Pattern Recogn 40(3):1014–1031
26. Shyu SJ (2013) Visual cryptograms of random grids for general access structures. IEEE Trans Circuits Syst Video Technol 23(3):414–424
27. Shyu SJ (2015) Visual cryptograms of random grids for threshold access structures. Theor Comput Sci 565:30–49
28. Shyu SJ, Chen MC (2011) Optimum pixel expansions for threshold visual secret sharing schemes. IEEE Trans Inf Forensics Secur 6(3):960–969
29. Thien CC, Lin JC (2002) Secret image sharing. Comput Graph 26(5):765–770
30. Wang DS, Yi F, Li X (2009) On general construction for extended visual cryptography schemes. Pattern Recogn 42(11):3071–3082
31. Wang RZ, Su CH (2006) Secret image sharing with smaller shadow images. Pattern Recogn Lett 27(6):551–555
32. Wu X, Sun W (2012) Visual secret sharing for general access structures by random grids. IET Inf Secur 6(4):299–309
33. Yamaguchi Y (2012) An extended visual cryptography scheme for continuous-tone images. Springer Trans Digit Forensics Watermarking 7128:228–242
34. Yan WQ, Jin D, Kankanhalli MS (2004) Visual cryptography for print and scan applications. In: IEEE international symposium on circuits and systems, vol 5. IEEE, Canada, pp 572–575
35. 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
36. Yang C, Chen T, Ching M (2006) Embed additional private information into two-dimensional bar codes by the visual secret sharing scheme. Integr Comput-Aided Eng 13(2):189–199
37. Yang C, Wu C, Wang D (2014) A discussion on the relationship between probabilistic visual cryptography and random grid. Inf Sci 278:141–173
38. 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
39. Yang CN, Chen TS, Yu KH, Wang CC (2007) Improvements of image sharing with steganography and authentication. J Syst Softw 80(7):1070–1076
40. Yu B, Shen G (2014) Multi-secret visual cryptography with deterministic contrast. Multimed 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.