International Journal of Computer Applications (0975 8887)
Volume 83 - No. 7, December 2013

Secret Image Sharing for General Access Structures using Random Grids

Sachin Kumar
Department of Mathematics
Indian Institute of Technology Delhi
Hauz Khas, New Delhi - 110016, India

R. K. Sharma
Department of Mathematics
Indian Institute of Technology Delhi
Hauz Khas, New Delhi - 110016, India

ABSTRACT

This paper presents a visual secret sharing (VSS) scheme for general access structures by using random grids. Compared to the existing VSS schemes for general access structures, the proposed scheme generates the shares of same size as that of the original secret image and does not require any codebook prior to encryption process. With these advantages, the proposed scheme broadens the potential applicability of random-grid based VSS. We prove that the proposed scheme gives the strong access structure. Formal proofs, security analysis and experimental results are given to demonstrate both the feasibility and the correctness of the proposed scheme.

General Terms:

Cryptography, Information Security

Keywords:

Visual secret sharing, Visual cryptography, Random grids, General access structure, Image encryption

1. INTRODUCTION

Shamir [12] and Blakley [3] independently proposed (k, n)-threshold secret sharing (SS) scheme in which a secret is shared among n participants such that the secret can be obtained by at least k $(\leq n)$ participants together, but any $k-1$ or fewer participants cannot obtain any secret information. The SS schemes [3, 12] reconstruct the secret accurately by using complex computation. To share a visual secret information, several visual secret sharing (VSS) schemes [4–9, 11, 13, 14, 16] are developed involving complex, little or no computation in the decryption phase.

In 1995, Naor and Shamir [11] proposed a new technique known as Visual Cryptography (VC), which shares a visual information and removes the problem of computation involved in the decryption phase. Naor and Shamir's scheme is a (k, n)-threshold scheme, which encrypts a black and white secret image into n meaningless shares such that knowledge of less than k shares reveals nothing about the secret image. However, the secret image can be reconstructed by xeroxing at least k $(\leq n)$ shares on transparencies and stacking these transparencies together. The reconstruction is performed by human visual system without any computation. A VC scheme for an access structure splits the secret image into a set of shares such that certain qualified set of participants can visually recover the secret image, but other forbidden set of participants have no information about the secret image. The different construction techniques of VC scheme for general access structures, where an access structure is a specification of all qualified and forbidden sets of participants, were studied in [1, 2]. These schemes generate the shares of the size larger than that of the secret and require collections of basis matrices (codebook) prior to encryption process.

In 1987, Kafri and Keren [6] proposed a random-grid based $(2, 2)$ VSS technique in which a binary secret image is encrypted into two cipher grids without any pixel expansion and codebook requirement. The decryption is same as in traditional VC. Shyu [13] extended Kafri and Keren's scheme to (n, n) scheme for any n (≥ 2). Chen [4] also proposed $(2, n)$ and (n, n) VSS schemes based on random grids. Further, Chen and Tsao [5] proposed a random-grid based (k, n)-threshold VSS scheme, which is limited to threshold access structure and cannot be used for general access structures. Wu and Sun [16] developed a VSS scheme for general access structures. In their scheme original basis matrices, generated by the conventional VC scheme for general access structures [2], are modified to generate the shares. However, Wu and Sun's scheme has no pixel expansion but requires to generate basis matrices prior to encryption process. Recently, Shyu [14] proposed another VSS technique for general access structures without any pixel expansion and codebook requirement. They gave two construction techniques, where one uses the basis and other uses the collection of maximal forbidden sets to generate a set of visual cryptograms of random grids. For a given access structure, both the construction techniques can yield the reconstructed images of different quality.

In this paper, a random-grid based VSS scheme for general access structures is designed having the following merits.

1. No pixel expansion - The size of each share is same as that of the original image. It makes the storage and distribution of shares more efficient.
2. No codebook requirement - The proposed scheme does not require the collections of basis matrices for generating shares.
3. Generalized - The proposed scheme generalizes the existing random-grid based VSS schemes to general access structures.
4. Wide image format - The proposed scheme can be used to encrypt binary as well as color images.

The rest of this paper is organized as follows. Section 2 reviews VC schemes for general access structures, and the traditional random-grid based VSS. Section 3 presents the proposed scheme for binary

and color images. The security and performance analysis of the proposed scheme are discussed in Section 4. Section 5 presents the experimental results and comparison with related work. Finally, the paper is concluded in Section 6.

2. PRELIMINARIES

This section presents the results from VC schemes for general access structures and discusses traditional random-grid based VSS.

2.1 Review of VC schemes for general access structures

Let $\mathcal{P} = \{1, 2, ..., n\}$ be a set of n participants, and $2^{\mathcal{P}}$ denote the set of all subsets of $\mathcal{P}$. Let $\Gamma_{Qual} \subseteq 2^{\mathcal{P}}$ and $\Gamma_{Forb} \subseteq 2^{\mathcal{P}}$, where $\Gamma_{Qual} \cap \Gamma_{Forb} = \emptyset$. The members of Γ_{Qual} are referred as qualified sets, while the members of Γ_{Forb} are referred as forbidden sets. The pair $(\Gamma_{Qual}, \Gamma_{Forb})$ is known as the access structure.
We define Γ_0 as a set consisting of the minimal qualified sets, i.e., $\Gamma_0 = \{Q \in \Gamma_{Qual} : Q' \notin \Gamma_{Qual}, \forall Q' \subset Q\}$. A monotone increasing (respectively monotone decreasing) access structure Γ on $\mathcal{P}$ is a subset $\Gamma \subseteq 2^{\mathcal{P}} \backslash \emptyset$ ($\Gamma \subseteq 2^{\mathcal{P}}$) such that if $Q \in \Gamma$ and $Q \subseteq Q' \subseteq \mathcal{P}$ (respectively $Q' \subseteq Q \subseteq \mathcal{P}$), then $Q' \in \Gamma$. If Γ_{Qual} is monotone increasing, Γ_{Forb} is monotone decreasing, and $\Gamma_{Qual} \cup \Gamma_{Forb} = 2^{\mathcal{P}}$ then the access structure is called strong access structure and Γ_0 is called the basis of the access structure,.
Ateniese et al. [2] were the first to consider VC-based VSS for general access structures. They proposed two constructions for binary images. The first construction uses the cumulative array method to generate shares, while in the second construction smaller schemes are used as building blocks in construction of larger schemes. In [2], both constructions give strong access structure and obtain the pixel expansion as presented by the following results.

Result 1: Let $(\Gamma_{Qual}, \Gamma_{Forb})$ be a strong access structure. Any set $F \in \Gamma_{Forb}$ is said to be maximal forbidden if $F \cup \{p\} \in \Gamma_{Qual}$ for all $p \in \mathcal{P} \backslash F$. Let Z_M denote the collection of the maximal forbidden sets in Γ_{Forb}. Then, for the given access structure, there exists a VC scheme having pixel expansion equals to $2^{|Z_M|-1}$.

Result 2: Let $(\Gamma_{Qual}, \Gamma_{Forb})$ be a strong access structure with the basis Γ_0. Then, for the given access structure, there exists a VC scheme having pixel expansion equals to $\sum_{X \in \Gamma_0} 2^{|X|-1}$.
Adhikari et al. [1] proposed another black and white VC for strong access structures, where basis matrices are constructed by using the fact that the collection of all solutions of a system of linear homogeneous equations over the binary field forms a vector space over the base field.

2.2 Review of traditional random-grid based VSS

A random grid is defined as a transparency comprising a two-dimensional array of pixels, where each pixel is either transparent (0) or opaque (1), chosen randomly similar to a coin-flip procedure. Kafri and Keren [6] proposed three algorithms to encrypt a binary image into two cipher grids, which are regarded as Algorithms 1-3.

Input: Binary secret image A of the size $h \times w$.
Output: Cipher grids R_1 and R_2 of the size $h \times w$.

Algorithm 1

Step 1.1 Generate R_1 randomly, i.e., $R_1[i,j] = random(0,1)$, where $1 \le i \le h$ and $1 \le j \le w$

Step 1.2 Generate R_2 by R_1 and A as follows
for (each pixel $A[i,j]$, $1 \le i \le h$ and $1 \le j \le w$)
{
if ($A[i,j] = 0$) $R_2[i,j] = R_1[i,j]$
else $R_2[i,j] = \overline{R_1[i,j]}$
}

Step 1.3 output (R_1, R_2)

Algorithm 2

Step 2.1 Generate R_1 randomly, i.e., $R_1[i,j] = random(0,1)$, where $1 \le i \le h$ and $1 \le j \le w$

Step 2.2 Generate R_2 by R_1 and A as follows
for (each pixel $A[i,j]$, $1 \le i \le h$ and $1 \le j \le w$)
{
if ($A[i,j] = 0$) $R_2[i,j] = R_1[i,j]$
else $R_2[i,j] = random(0,1)$
}

Step 2.3 output (R_1, R_2)

Algorithm 3

Step 3.1 Generate R_1 randomly, i.e., $R_1[i,j] = random(0,1)$, where $1 \le i \le h$ and $1 \le j \le w$

Step 3.2 Generate R_2 by R_1 and A as follows
for (each pixel $A[i,j]$, $1 \le i \le h$ and $1 \le j \le w$)
{
if ($A[i,j]$ = 0) $R_2[i,j] = random(0,1)$
else $R_2[i,j] = \overline{R_1[i,j]}$
}

Step 3.3 output (R_1, R_2)

$random(0,1)$ is a function that returns a value (0 or 1) randomly. $\overline{R}$ is defined as an inverse grid of a binary grid R of the size $h \times w$ obtained by bitwise complementing of R, i.e., $\overline{R[i,j]} = 1 - R[i,j]$ for $1 \le i \le h$ and $1 \le j \le w$. The cipher grids R_1 and R_2 do not reveal any secret information. However, the image obtained by stacking R_1 and R_2 visually reveals the secret image.

3. THE PROPOSED SCHEME

This section presents the proposed scheme for general access structures based on random grids. The proposed scheme encrypts a secret image into n (≥ 2) cipher grids such that each cipher grid is meaningless, and stacking result of the cipher grids corresponding to participants of any forbidden set reveals no secret information. However, the secret image can be recognized visually by stacking the cipher grids corresponding to participants of any qualified set.

3.1 Scheme for binary images

Some notations are given before presenting the proposed scheme. Let $(\Gamma_{Qual}, \Gamma_{Forb})$ be a strong access structure defined on a set of n participants $\mathcal{P} = \{1, 2, ..., n\}$ with the basis Γ_0. Let $|\Gamma_0| = N$ and Γ_0 contains the subsets of $\mathcal{P}$ of different cardinalities $m_1, m_2, ..., m_r$, where $m_1 < m_2 < ... < m_r$ and $m_j \in \{2, 3, ..., n\}$ for $1 \le j \le r$. Let n_j $(1 \le j \le r)$ denote the number of subsets of cardinality m_j in Γ_0, where $n_j \in \{1, 2, ..., \binom{n}{m_j}\}$ and $n_1 + n_2 + ... + n_r = N$. We define $\Gamma_0 = \{B^1_{m_1}, ..., B^{n_1}_{m_1}, B^1_{m_2}, ..., B^{n_2}_{m_2}, ..., B^1_{m_r}, ..., B^{n_r}_{m_r}\}$, where $B^t_{m_k}$ denotes t^{th} subset of cardinality m_k, $1 \le t \le n_k$ and $1 \le k \le r$. Let $B^t_{m_k}$ be the set of participants $p^t_1, p^t_2, ..., p^t_{m_k} \in \{1, 2, ..., n\}$, i.e., $B^t_{m_k} = \{p^t_1, p^t_2, ..., p^t_{m_k}\}$. The

procedure for sharing a secret image into n cipher grids for any general access structure is given in Algorithm 4. Here, $\oplus$ denotes the Boolean exclusive OR operation.
Input: Binary secret image A of the size $h \times w$ and a strong access structure $(\Gamma_{Qual}, \Gamma_{Forb})$ with the basis Γ_0.
Output: Cipher grids $R_1, R_2, ..., R_n$ of the size $h \times w$.

Algorithm 4

Step 4.1 Select a pixel $A[i,j] \in A$ and encrypt it into n random values $R_1[i,j], R_2[i,j], ..., R_n[i,j]$ by following Steps 4.2 to 4.6

Step 4.2 Select randomly one set from the basis Γ_0. Let us assume that the selected set is $B^t_{m_k}$, where $t \in \{1, 2, ..., n_k\}$ and $k \in \{1, 2, ..., r\}$

Step 4.3 For the selected pixel $A[i,j]$ generate binary values $a_1, a_2, ..., a_{m_k}$ by using the traditional random-grid based VSS as follows

Step 4.3.1 Generate $a_1, a_2, ..., a_{m_k-1}$ independently by the function $random(0,1)$

Step 4.3.2 Select one algorithm from Algorithms 1-3 and generate a_{m_k} from $a_1, a_2, ..., a_{m_k-1}$ as follows

$b_1 = a_1$
for $(2 \le l \le m_k - 1)$
{
$b_l = b_{l-1} \oplus a_l$
}

Case 1: Algorithm 1 is selected
if $(A[i,j] = 0)$ $a_{m_k} = b_{m_k-1}$
else $a_{m_k} = \overline{b_{m_k-1}}$

Case 2: Algorithm 2 is selected
if $(A[i,j] = 0)$ $a_{m_k} = b_{m_k-1}$
else $a_{m_k} = random(0,1)$

Case 3: Algorithm 3 is selected
if $(A[i,j] = 0)$ $a_{m_k} = random(0,1)$
else $a_{m_k} = \overline{b_{m_k-1}}$

Step 4.4 Generate the binary values $a_{m_{k+1}}, a_{m_{k+2}}, ..., a_n$ independently by the function $random(0,1)$, i.e., $a_u = random(0,1)\ \forall u \in \{m_{k+1}, m_{k+2}, ..., n\}$

Step 4.5 Assign $a_1, a_2, ..., a_{m_k}$ at the location $[i,j]$ of the random grids corresponding to the participants of selected set $B^t_{m_k}$, i.e.,

$$R_{p^t_1}[i,j] = a_1$$
$$R_{p^t_2}[i,j] = a_2$$
$$\vdots$$
$$\vdots$$
$$R_{p^t_{m_k}}[i,j] = a_{m_k}$$

Step 4.6 Assign $a_{m_{k+1}}, a_{m_{k+2}}, ..., a_n$ randomly at the location $[i,j]$ of the remaining $(n - m_k)$ random grids

Step 4.7 Repeat Step 4.1 until all the pixels $A[i,j]$ of the secret image A are encrypted

Step 4.8 output $(R_1, R_2, ..., R_n)$

3.2 Scheme for color images

The proposed scheme can be easily extended to color images by adopting a similar procedure as discussed in [4, 5]. A color model, which is either additive (RGB) or subtractive (CMY), is employed to decompose the color image into three channels. The procedure to encrypt a color secret image B for general access structures is given as follows:

Step 5.1 Decompose the color secret image B into three color components Cyan, Magenta and Yellow (CMY), i.e., B^C, B^M and B^Y

Step 5.2 By using error diffusion halftone techniques [10, 15], transform the color components B^C, B^M and B^Y into halftone images, i.e., HB^C, HB^M and HB^Y

Step 5.3 Generate n cipher grids for each of halftone color components HB^C, HB^M and HB^Y by using the proposed scheme for binary images, i.e., R^C_i, R^M_i and R^Y_i where $1 \le i \le n$

Step 5.4 The color components of the cipher grids R^C_i, R^M_i and R^Y_i are combined to form eight color cipher grid R_i, i.e., $R_i = (R^C_i, R^M_i, R^Y_i)$ where $1 \le i \le n$

Step 5.5 output $(R_1, R_2, ..., R_n)$

4. PERFORMANCE ANALYSIS

The performance of the proposed scheme is measured in terms of the security of the original image and the visual quality of the reconstructed image.

DEFINITION 1. *For a certain pixel r in a binary image R of the size $h \times w$, the light transmission of r $(t(r))$ is defined as the probability of r to be transparent (i.e., $Prob(r = 0)$). Thus, the light transmission of a transparent (respectively opaque) pixel $r \in R$ is $t(r) = 1$ (respectively $t(r) = 0$). Additionally, the average light transmission of R is defined as $T(R) = \frac{1}{h \times w} \sum_{i=1}^{h} \sum_{j=1}^{w} t(R[i,j])$.*

In random-grid based VSS, the visual quality of the reconstructed image is measured by the contrast [13], which is defined as follows.

DEFINITION 2. *The contrast of the image S reconstructed for the binary image A is defined as $\alpha = \frac{T(S[A(0)]) - T(S[A(1)])}{1 + T(S[A(1)])}$. $A(0)$ (respectively $A(1)$) denotes the area of all transparent (respectively opaque) pixels in A, with $A = A(0) \cup A(1)$ and $A(0) \cap A(1) = \emptyset$. $S[A(0)]$ (respectively $S[A(1)]$) denotes the area of all pixels in S corresponding to $A(0)$ (respectively $A(1)$).*

DEFINITION 3. *For the contrast $\alpha > 0$, the reconstructed image S visually reveals the original image A. Precisely, $\alpha > 0$ implies $T(S[A(0)]) > T(S[A(1)])$ and S is visually recognizable as A. For $\alpha = 0$ (i.e. $T(S[A(0)]) = T(S[A(1)])$), S is meaningless and reveals no information about A.*

If R is a random grid, then for $r \in R$, the probability of r to be transparent (0) is equal to the probability of r to be opaque (1), i.e., $Prob(r = 0) = Prob(r = 1) = \frac{1}{2}$. Since the number of transparent pixels is probabilistically equal to that of opaque pixels in R, we have $T(R) = \frac{1}{2}$. Let $\otimes$ denote Boolean OR operation, which simulates the human visual system.

LEMMA 4. *If $r_1, r_2, ..., r_n$ are n random pixels generated independently by the function $random(0,1)$, then $Prob(r_1 \otimes r_2 \otimes ... \otimes r_n = 0) = \frac{1}{2^n}$.*

PROOF. We prove by mathematical induction on n. We have $Prob(r_1 \otimes r_2 = 0) = Prob(r_1 = 0) \times Prob(r_2 = 0) = \frac{1}{2} \times \frac{1}{2} = \frac{1}{2^2}$, i.e., the result is true for $n = 2$.
Assume that the result holds for $n-1$, i.e., $Prob(r_1 \otimes ... \otimes r_{n-1} = 0) = \frac{1}{2^{n-1}}$. We have to prove that it holds for n also. We know that $Prob(r_1 \otimes ... \otimes r_{n-1} \otimes r_n = 0) = Prob(r_1 \otimes ... \otimes r_{n-1} = 0) \times Prob(r_n = 0) = \frac{1}{2^{n-1}} \times \frac{1}{2} = \frac{1}{2^n}$. $\square$

LEMMA 5. *If $r_1, r_2, ..., r_n$ are n random pixels generated independently by the function $random(0,1)$, then $Prob(r_1 \oplus r_2 \oplus ... \oplus r_n = 0) = \frac{1}{2}$.*

PROOF. We prove by mathematical induction on n. We have $Prob(r_1 \oplus r_2 = 0) = Prob(r_1 = 0) \times Prob(r_2 = 0) + Prob(r_1 = 1) \times Prob(r_2 = 1) = (\frac{1}{2} \times \frac{1}{2}) + (\frac{1}{2} \times \frac{1}{2}) = \frac{1}{2}$, i.e., the result is true for $n = 2$.
Assume that the result holds for $n-1$, i.e., $Prob(r_1 \oplus ... \oplus r_{n-1} = 0) = \frac{1}{2}$. We have to prove that it holds for n also. We know that $Prob(r_1 \oplus ... \oplus r_{n-1} \oplus r_n = 0) = Prob(r_1 \oplus ... \oplus r_{n-1} = 0) \times Prob(r_n = 0) + Prob(r_1 \oplus ... \oplus r_{n-1} = 1) \times Prob(r_n = 1) = (\frac{1}{2} \times \frac{1}{2}) + (\frac{1}{2} \times \frac{1}{2}) = \frac{1}{2}$. □

THEOREM 6. *In the proposed random-grid based VSS scheme for general access structures, each cipher grid is meaningless and reveals no information about the secret image A.*

PROOF. In the proposed scheme, each pixel $A[i,j] \in A$ is encrypted corresponding to a minimal qualified set randomly selected from the basis Γ_0. Let $A[i,j]$ be encrypted corresponding to a minimal qualified set of cardinality m_k, where $k \in \{1, 2, ..., r\}$. Therefore, the pixel values at location $[i,j]$ of the cipher grids $R_1, R_2, ..., R_n$ (i.e., $R_1[i,j], R_2[i,j], ..., R_n[i,j]$) are selected among the binary values $a_1, a_2, ..., a_{m_k-1}, a_{m_k}, a_{m_k+1}, ..., a_n$ that are generated by Steps 4.3 to 4.4 of the proposed scheme. Since the binary values $a_1, a_2, ..., a_{m_k-1}, a_{m_k+1}, ..., a_n$ are generated independently by the function $random(0,1)$, $Prob(a_l = 0) = \frac{1}{2}$ for $1 \le l \le m_{k-1}$ and $m_{k+1} \le l \le n$.
From Step 4.3.2 of the proposed scheme, we have $b_{m_k-1} = a_1 \oplus a_2 \oplus ... \oplus a_{m_k-1}$. By Lemma 5, we obtain

$$Prob(b_{m_k-1} = 0) = \frac{1}{2}.$$

As a_{m_k} depends on the algorithm selected from Algorithms 1-3, three cases are considered as follows.
In Algorithm 1, for $A[i,j] = 0$, $a_{m_k} = b_{m_k-1}$, i.e, $Prob(a_{m_k} = 0) = Prob(b_{m_k-1} = 0) = \frac{1}{2}$. While for $A[i,j] = 1$, $a_{m_k} = \overline{b_{m_k-1}}$, i.e., $Prob(a_{m_k} = 0) = 1 - Prob(b_{m_k-1} = 0) = \frac{1}{2}$. Therefore, $Prob(a_{m_k} = 0) = \frac{1}{2}$.
In Algorithm 2, for $A[i,j] = 0$, $a_{m_k} = b_{m_k-1}$, i.e., $Prob(a_{m_k} = 0) = Prob(b_{m_k-1} = 0) = \frac{1}{2}$. While for $A[i,j] = 1$, $a_{m_k} = random(0,1)$, i.e., $Prob(a_{m_k} = 0) = \frac{1}{2}$. Therefore, $Prob(a_{m_k} = 0) = \frac{1}{2}$.
In Algorithm 3, for $A[i,j] = 0$, $a_{m_k} = random(0,1)$, i.e., $Prob(a_{m_k} = 0) = \frac{1}{2}$. While for $A[i,j] = 1$, $a_{m_k} = \overline{b_{m_k-1}}$, i.e., $Prob(a_{m_k} = 0) = 1 - Prob(b_{m_k-1} = 0) = \frac{1}{2}$. Therefore, $Prob(a_{m_k} = 0) = \frac{1}{2}$.
Precisely, no matter if $A[i,j] = 0$ or 1, we obtain $Prob(R_l[i,j] = 0) = \frac{1}{2}$, i.e., $t(R_l[i,j]) = \frac{1}{2}$ for $1 \le l \le n$. Therefore,

$$T(R_l[A(0)]) = T(R_l[A(1)]) = \frac{1}{2},$$

where $1 \le l \le n$. Hence, each cipher grid is meaningless and does not reveal any information about the secret image A. □

THEOREM 7. *In the proposed random-grid based VSS scheme for general access structures, stacking the cipher grids corresponding to the participants of any forbidden set cannot reveal the secret image A.*

PROOF. Let $F = \{p_1, p_2, \ldots, p_s\}$ be any forbidden set and S denote the stacking result of the cipher grids corresponding to the participants of F, i.e., $S[i,j] = R_{p_1}[i,j] \otimes R_{p_2}[i,j] \otimes \ldots \otimes R_{p_s}[i,j]$, where $1 \le i \le h$ and $1 \le j \le w$. We define

$$C_F = \{Q \in \Gamma_0 \ : \ F \subset Q\}.$$

In the proposed scheme, each pixel $A[i,j] \in A$ is encrypted corresponding to a minimal qualified set, which is selected from the basis Γ_0 randomly. Let $A[i,j]$ be encrypted corresponding to a minimal qualified set $Q_1 \in \Gamma_0$. Two cases are considered, where Case 1 is for $Q_1 \notin C_F$ or $C_F = \emptyset$, and Case 2 is for $Q_1 \in C_F$.
Case 1: In this case, for $A[i,j] = 0$ or 1, the pixels $R_{p_1}[i,j], R_{p_2}[i,j], \ldots, R_{p_s}[i,j]$ are generated independently as random values. By Lemma 4, no matter if $A[i,j] = 0$ or 1, we obtain $Prob(S[i,j] = 0) = \frac{1}{2^s}$, i.e., $t(S[i,j]) = \frac{1}{2^s}$. Therefore,

$$T(S[A(0)]) = T(S[A(1)]) = \frac{1}{2^s}. \quad (1)$$

Case 2: Let $|Q_1| = m_k$ for some $k \in \{1, 2, \ldots, r\}$. Since $F \subset Q_1$ and $Q_1 \in \Gamma_0$, the pixel values at any location $[i,j]$ of the cipher grids corresponding to the participants of F will be assigned from the set $\{a_1, a_2, \ldots, a_{m_k}\}$ generated as in Step 4.3 of the proposed scheme. If $D = \{R_{p_1}[i,j], R_{p_2}[i,j], \ldots, R_{p_s}[i,j]\}$, then $D \subset \{a_1, a_2, \ldots, a_{m_k}\}$. Considering a_{m_k} as the last value generated based on selection from Algorithms 1-3, we have either $a_{m_k} \notin D$ or $a_{m_k} \in D$.
If $a_{m_k} \notin D$, then $D \subseteq \{a_1, a_2, \ldots, a_{m_k-1}\}$. We know that $a_1, a_2, \ldots, a_{m_k-1}$ are generated independently by the function $random(0,1)$. By using Lemma 4, for $A[i,j] = 0$ or 1, we obtain $Prob(S[i,j] = 0) = \frac{1}{2^s}$, i.e., $t(S[i,j]) = \frac{1}{2^s}$. Therefore,

$$T(S[A(0)]) = T(S[A(1)]) = \frac{1}{2^s}. \quad (2)$$

If $a_{m_k} \in D$, then consider $R_{p_u}[i,j] = a_{m_k}$ for some $u \in \{1, 2, ..., s\}$. If $D_1 = D \setminus \{R_{p_u}[i,j]\} = \{R_{y_1}[i,j], \ldots, R_{y_{s-1}}[i,j]\}$, then each pixel $R_{y_v}[i,j] \in D_1$ is generated independently by the function $random(0,1)$, i.e., $Prob(R_{y_v}[i,j] = 0) = \frac{1}{2}$ for $1 \le v \le s-1$. By Lemma 4, we obtain

$$Prob(R_{y_1}[i,j] \otimes \ldots \otimes R_{y_{s-1}}[i,j] = 0) = \frac{1}{2^{s-1}}.$$

We know that $R_{y_1}[i,j] \otimes \ldots \otimes R_{y_{s-1}}[i,j]$ will be transparent (0) only if

$$R_{y_1}[i,j] = \ldots\ldots = R_{y_{s-1}}[i,j] = 0.$$

If $R_{y_v}[i,j] = 0$ $(1 \le v \le s-1)$, then $b_{m_k-1} = R_{z_1}[i,j] \oplus \ldots \oplus R_{z_{m_k-s}}[i,j]$, where $\{R_{z_1}[i,j], \ldots, R_{z_{m_k-s}}[i,j]\} = \{a_1, a_2, \ldots, a_{m_k-1}\} \setminus D_1$. By using Lemma 5, we obtain

$$Prob(b_{m_k-1} = 0) = \frac{1}{2}.$$

We have $Prob(S[i,j] = 0) = Prob(R_{y_1}[i,j] \otimes \ldots \otimes R_{y_{s-1}}[i,j] = 0) \times Prob(R_{p_u}[i,j] = 0)$. Therefore,

$$Prob(S[i,j] = 0) = \frac{1}{2^{s-1}} \times Prob(R_{p_u}[i,j] = 0). \quad (3)$$

The pixel $R_{p_u}[i,j]$ $(= a_{m_k})$ depends upon b_{m_k-1} and the algorithm selected from Algorithms 1-3.
In Algorithm 1, for $A[i,j] = 0$, we have $R_{p_u}[i,j] = b_{m_k-1}$, i.e., $Prob(R_{p_u}[i,j] = 0) = Prob(b_{m_k-1} = 0) = \frac{1}{2}$. From (3), we obtain $Prob(S[i,j] = 0) = \frac{1}{2^{s-1}} \times \frac{1}{2} = \frac{1}{2^s}$, i.e., $t(S[i,j]) = \frac{1}{2^s}$. Therefore,

$$T(S[A(0)]) = \frac{1}{2^s}. \quad (4)$$

In addition, for $A[i,j] = 1$, we have $R_{p_u}[i,j] = \overline{b_{m_k-1}}$, i.e., $Prob(R_{p_u}[i,j] = 0) = 1 - Prob(b_{m_k-1} = 0) = \frac{1}{2}$. From (3), we obtain $Prob(S[i,j] = 0) = \frac{1}{2^{s-1}} \times \frac{1}{2} = \frac{1}{2^s}$, i.e., $t(S[i,j]) = \frac{1}{2^s}$. Therefore,

$$T(S[A(1)]) = \frac{1}{2^s}. \quad (5)$$

From (4) and (5), we have

$$T(S[A(0)]) = T(S[A(1)]) = \frac{1}{2^s}. \quad (6)$$

In Algorithm 2, for $A[i,j] = 0$, we have $R_{p_u}[i,j] = b_{m_{k-1}}$. We obtain

$$T(S[A(0)]) = \frac{1}{2^s}. \quad (7)$$

In addition, for $A[i,j] = 1$, we have $R_{p_u}[i,j] = random(0,1)$, i.e., $Prob(R_{p_u}[i,j] = 0) = \frac{1}{2}$. From (3), we obtain $Prob(S[i,j] = 0) = \frac{1}{2^{s-1}} \times \frac{1}{2} = \frac{1}{2^s}$, i.e., $t(S[i,j]) = \frac{1}{2^s}$. Therefore,

$$T(S[A(1)]) = \frac{1}{2^s}. \quad (8)$$

From (7) and (8), we have

$$T(S[A(0)]) = T(S[A(1)]) = \frac{1}{2^s}. \quad (9)$$

In Algorithm 3, for $A[i,j] = 0$, we have $R_{p_u}[i,j] = random(0,1)$, i.e., $Prob(R_{p_u}[i,j] = 0) = \frac{1}{2}$. From (3), we obtain $Prob(S[i,j] = 0) = \frac{1}{2^{s-1}} \times \frac{1}{2} = \frac{1}{2^s}$, i.e., $t(S[i,j]) = \frac{1}{2^s}$. Therefore,

$$T(S[A(0)]) = \frac{1}{2^s}. \quad (10)$$

In addition, for $A[i,j] = 1$, we have $R_{p_u}[i,j] = \overline{b_{m_k-1}}$. We obtain

$$T(S[A(1)]) = \frac{1}{2^s}. \quad (11)$$

From (10) and (11), we have

$$T(S[A(0)]) = T(S[A(1)]) = \frac{1}{2^s}. \quad (12)$$

Precisely in Case 2, from (6), (9) and (12), we have

$$T(S[A(0)]) = T(S[A(1)]) = \frac{1}{2^s}. \quad (13)$$

By considering both cases (1) and (13), we obtain

$$T(S[A(0)]) = T(S[A(1)]).$$

By Definition 3, we obtain $\alpha = 0$. Thus, S is meaningless and reveals no information about A. □

THEOREM 8. *In the proposed random-grid based VSS scheme for general access structures, the secret image A can be visually revealed by stacking the cipher grids corresponding to the participants of any qualified set.*

PROOF. Let $Q = \{p_1, p_2, \ldots, p_t\}$ be any qualified set consisting of t participants and S denote the stacking result of the cipher grids corresponding to the participants of Q. We have $S[i,j] = R_{p_1}[i,j] \otimes R_{p_2}[i,j] \otimes \ldots \otimes R_{p_t}[i,j]$, where $1 \le i \le h$ and $1 \le j \le w$. Let C_Q be the set of minimal qualified sets which are the subsets of Q and belong to the basis Γ_0, i.e.,

$$C_Q = \{Q_1 \subseteq Q \ : \ Q_1 \in \Gamma_0\},$$

and $c = |C_Q|$.
In the proposed scheme, each pixel $A[i,j] \in A$ is encrypted corresponding to a minimal qualified set, which is selected from the basis Γ_0 randomly. Let $A[i,j]$ be encrypted corresponding to a minimal qualified set $Q_1 \in \Gamma_0$. Two cases are considered, where Case 1 is for $Q_1 \notin C_Q$ and Case 2 is for $Q_1 \in C_Q$. In Case 2, we have

$$Prob(Q_1 \in C_Q) = \frac{c}{N},$$

and in Case 1, we have

$$Prob(Q_1 \notin C_Q) = 1 - \frac{c}{N},$$

where $N = |\Gamma_0|$. By considering Case 1 and Case 2, we have

$$Prob(S[i,j] = 0) = (1 - \tfrac{c}{N}) \times Prob(S[i,j] = 0 \mid Case\ 1) + (\tfrac{c}{N}) \times Prob(S[i,j] = 0 \mid Case\ 2).$$

Case 1: In this case, the pixels $R_{p_1}[i,j], R_{p_2}[i,j], \ldots, R_{p_t}[i,j]$ are generated randomly so that they are independent of corresponding secret pixel $A[i,j]$, i.e., $Prob(R_{p_l}[i,j] = 0) = \frac{1}{2}$ for $1 \le l \le t$. By using Lemma 4, for $A[i,j] = 0$ or 1, we obtain

$$Prob(S[i,j] = 0 \mid Case\ 1) = \frac{1}{2^t}. \quad (14)$$

Case 2: Let $D = \{R_{p_1}[i,j], R_{p_2}[i,j], \ldots, R_{p_t}[i,j]\}$ and $|Q_1| = m_k$ for some $k \in \{1, 2, \ldots, r\}$. The pixels $R_{p_1}[i,j], R_{p_2}[i,j], \ldots, R_{p_t}[i,j]$ will be selected from the set $\{a_1, a_2, \ldots, a_{m_k}, a_{m_{k+1}}, \ldots, a_n\}$ generated as in Steps 4.3 to 4.4 of the proposed scheme. Let us assume that

$$D_1 = \{R_{y_1}[i,j], \ldots, R_{y_{m_k}}[i,j]\} = \{a_1, \ldots, a_{m_k}\},$$

and

$$D_2 = \{R_{z_1}[i,j], \ldots, R_{z_{t-m_k}}[i,j]\} \subseteq \{a_{m_k+1}, \ldots, a_n\},$$

where $D_1 \subseteq D$, $D_2 \subseteq D$, $D_1 \cap D_2 = \emptyset$ and $D = D_1 \cup D_2$. We have $Prob(S[i,j] = 0 \mid Case\ 2) = Prob(R_{p_1}[i,j] \otimes R_{p_2}[i,j] \otimes \ldots \otimes R_{p_t}[i,j] = 0) = Prob(R_{y_1}[i,j] \otimes \ldots \otimes R_{y_{m_k}}[i,j] = 0) \times Prob(R_{z_1}[i,j] \otimes \ldots \otimes R_{z_{t-m_k}}[i,j] = 0)$.
The binary values $a_{m_k+1}, a_{m_k+2}, \ldots, a_n$ are generated independently by the function $random(0,1)$. By Lemma 4, we obtain

$$Prob(R_{z_1}[i,j] \otimes \ldots \otimes R_{z_{t-m_k}}[i,j] = 0) = \frac{1}{2^{t-m_k}}.$$

In addition, we have $Prob(R_{y_1}[i,j] \otimes \ldots \otimes R_{y_{m_k}}[i,j] = 0) = Prob(a_1 \otimes a_2 \otimes \ldots \otimes a_{m_k-1} \otimes a_{m_k} = 0) = Prob(a_1 \otimes a_2 \otimes \ldots \otimes a_{m_k-1} = 0) \times Prob(a_{m_k} = 0)$.
The binary values $a_1, a_2, \ldots, a_{m_k-1}$ are generated independently by the function $random(0,1)$. By Lemma 4,

$$Prob(a_1 \otimes a_2 \otimes \ldots \otimes a_{m_k-1} = 0) = \frac{1}{2^{m_k-1}}.$$

We know that $a_1 \otimes a_2 \otimes \ldots \otimes a_{m_k-1}$ will be transparent (0) only if $a_1, a_2, \ldots, a_{m_k-1}$ are transparent, i.e., $a_1 = a_2 = \ldots = a_{m_k-1} = 0$. By Step 4.3.2 of the proposed scheme, for $a_v = 0$ $(1 \le v \le m_k - 1)$, we obtain $b_{m_k-1} = 0$. The value of a_{m_k} depends on b_{m_k-1} and the algorithm selected from Algorithms 1-3.
In Algorithm 1, for $A[i,j] = 0$, we have $a_{m_k} = b_{m_k-1} = 0$, i.e., $Prob(a_{m_k} = 0) = 1$. Therefore,

$$Prob(R_{y_1}[i,j] \otimes \ldots \otimes R_{y_{m_k}}[i,j] = 0) = \frac{1}{2^{m_k-1}} \times 1 = \frac{1}{2^{m_k-1}}.$$

We obtain

$$Prob(S[i,j] = 0 \mid Case\ 2) = \frac{1}{2^{m_k-1}} \times \frac{1}{2^{t-m_k}} = \frac{1}{2^{t-1}}. \quad (15)$$

For $A[i,j] = 0$, by considering both cases (14) and (15), we have

$$Prob(S[i,j] = 0) = (1 - \tfrac{c}{N}) \times \tfrac{1}{2^t} + (\tfrac{c}{N}) \times \tfrac{1}{2^{t-1}} = (1 + \tfrac{c}{N}) \times \tfrac{1}{2^t},$$

i.e., $t(S[i,j]) = (1 + \frac{c}{N}) \times \frac{1}{2^t}$. Therefore,

$$T(S[A(0)]) = (1 + \tfrac{c}{N}) \times \tfrac{1}{2^t}.$$

In addition, for $A[i,j] = 1$ we have $a_{m_k} = \overline{b_{m_k-1}} = 1$, i.e., $Prob(a_{m_k} = 0) = 0$. Therefore,

$$Prob(R_{y_1}[i,j] \otimes \ldots \otimes R_{y_{m_k}}[i,j] = 0) = \frac{1}{2^{m_k-1}} \times 0 = 0.$$

We obtain

$$Prob(S[i,j]=0 \mid Case\ 2) = 0 \times \frac{1}{2^{t-m_k}} = 0. \quad (16)$$

For $A[i,j]=1$, by considering both cases (14) and (16), we have $Prob(S[i,j]=0) = (1-\frac{c}{N}) \times \frac{1}{2^t} + (\frac{c}{N}) \times 0 = (1-\frac{c}{N}) \times \frac{1}{2^t}$, i.e., $t(S[i,j]) = (1-\frac{c}{N}) \times \frac{1}{2^t}$. Therefore,

$$T(S[A(1)]) = (1-\frac{c}{N}) \times \frac{1}{2^t}.$$

Thus, the contrast of S is

$$\alpha = \frac{T(S[A(0)])-T(S[A(1)])}{1+T(S[A(1)])} = \frac{(1+\frac{c}{N})\times\frac{1}{2^t}-(1-\frac{c}{N})\times\frac{1}{2^t}}{1+(1-\frac{c}{N})\times\frac{1}{2^t}} = \frac{2\times c}{N\times 2^t+N-c}. \quad (17)$$

In Algorithm 2, for $A[i,j]=0$, we have $a_{m_k} = b_{m_k-1} = 0$. By the following similarly as in case of Algorithm 1, we obtain

$$T(S[A(0)]) = (1+\frac{c}{N}) \times \frac{1}{2^t}.$$

For $A[i,j]=1$, we have $a_{m_k} = random(0,1)$, i.e., $Prob(a_{m_k} = 0) = \frac{1}{2}$. Therefore,

$$Prob(R_{y_1}[i,j] \otimes \ldots \otimes R_{y_{m_k}}[i,j] = 0) = \frac{1}{2^{m_k-1}} \times \frac{1}{2} = \frac{1}{2^{m_k}}.$$

We obtain

$$Prob(S[i,j]=0 \mid Case\ 2) = \frac{1}{2^{m_k}} \times \frac{1}{2^{t-m_k}} = \frac{1}{2^t}. \quad (18)$$

For $A[i,j]=1$, by considering both cases (14) and (18), we have

$$Prob(S[i,j]=0) = (1-\frac{c}{N}) \times \frac{1}{2^t} + (\frac{c}{N}) \times \frac{1}{2^t} = \frac{1}{2^t},$$

i.e., $t(S[i,j]) = \frac{1}{2^t}$. Therefore,

$$T(S[A(1)]) = \frac{1}{2^t}.$$

Thus, the contrast of S is

$$\alpha = \frac{T(S[A(0)])-T(S[A(1)])}{1+T(S[A(1)])} = \frac{(1+\frac{c}{N})\times\frac{1}{2^t}-\frac{1}{2^t}}{1+\frac{1}{2^t}} = \frac{c}{N\times 2^t+N}. \quad (19)$$

In Algorithm 3, for $A[i,j]=0$, we have $a_{m_k} = random(0,1)$, i.e., $Prob(a_{m_k}=0) = \frac{1}{2}$. Therefore,

$$Prob\ (R_{y_1}[i,j] \otimes \ldots \otimes R_{y_{m_k}}[i,j] = 0) = \frac{1}{2^{m_k-1}} \times \frac{1}{2} = \frac{1}{2^{m_k}}.$$

We obtain

$$Prob(S[i,j]=0 \mid Case\ 2) = \frac{1}{2^{m_k}} \times \frac{1}{2^{t-m_k}} = \frac{1}{2^t}. \quad (20)$$

For $A[i,j]=0$, by considering both cases (14) and (20), we obtain

$$Prob(S[i,j]=0) = (1-\frac{c}{N}) \times \frac{1}{2^t} + (\frac{c}{N}) \times \frac{1}{2^t} = \frac{1}{2^t},$$

i.e., $t(S[i,j]) = \frac{1}{2^t}$. Therefore,

$$T(S[A(0)]) = \frac{1}{2^t}.$$

For $A[i,j]=1$, we have $a_{m_k} = \overline{b_{m_k-1}} = 1$. By the following similarly as in case of Algorithm 1, we obtain

$$T(S[A(1)]) = (1-\frac{c}{N}) \times \frac{1}{2^t}.$$

Thus, the contrast of S is

$$\alpha = \frac{T(S[A(0)])-T(S[A(1)])}{1+T(S[A(1)])} = \frac{\frac{1}{2^t}-(1-\frac{c}{N})\times\frac{1}{2^t}}{1+(1-\frac{c}{N})\times\frac{1}{2^t}} = \frac{c}{N\times 2^t+N-c}. \quad (21)$$

From (17), (19) and (21), we have $\alpha > 0$ (i.e. $T(S[A(0)]) > T(S[A(1)])$) in the proposed scheme based on Algorithms 1-3. Thus by Definition 3, the stacked image S visually reveals the original secret image A. □

5. EXPERIMENTAL RESULTS AND COMPARISON WITH RELATED WORK

For experiments and comparison, Algorithm 1 is selected from Algorithms 1-3 as required in Step 4.3.2 of the proposed scheme. The proposed scheme is experimented for binary and color images by considering two access structures defined on a set $\mathcal{P} = \{1,2,3,4\}$ of four participants.

Access structure 1: Basis $\Gamma_0 = \{\{1,2\},\{1,3\},\{2,3\}\}$, $\Gamma_{Qual} = \{\{1,2\},\{1,3\},\{2,3\},\{1,2,3\},\{1,2,4\},\{1,3,4\},\{2,3,4\},\{1,2,3,4\}\}$ and $\Gamma_{Forb} = \{\{1\},\{2\},\{3\},\{4\},\{1,4\},\{2,4\},\{3,4\}\}$.

Access structure 2: Basis $\Gamma_0 = \{\{1,4\},\{2,3,4\}\}$, $\Gamma_{Qual} = \{\{1,4\},\{1,2,4\},\{1,3,4\},\{2,3,4\},\{1,2,3,4\}\}$ and $\Gamma_{Forb} = \{\{1\},\{2\},\{3\},\{4\},\{1,2\},\{1,3\},\{2,3\},\{2,4\},\{3,4\},\{1,2,3\}\}$.

5.1 Experiment 1

This experiment is conducted for the secret image of size 1024×1024 shown in Fig. 1(a). The secret image is encrypted into four cipher grids (Figs. 1(b)-1(e)) for the access structure 1. Each cipher grid is meaningless and does not reveal the secret information. By the stacked images for the forbidden sets (Figs. 1(h), 1(j), 1(k)), no secret information can be revealed. The stacked images for the qualified sets (Figs. 1(f), 1(g), 1(i), 1(l)-1(p)) can visually reveal the secret image. Table 1 shows the contrast of the stacked images for the qualified sets of the access structure 1.

5.2 Experiment 2

In this experiment, a color image of size 1024×1024 shown in Fig. 2(a) is encrypted into four cipher grids (Figs. 2(b)-2(e)) for the access structure 2. Each cipher grid is meaningless and reveals no secret information. The stacked images for the forbidden sets (Figs. 2(f), 2(g), 2(i)-2(l)) do not reveal any information about the secret image. The secret image can be easily recognized by the stacked images for the qualified sets (Figs. 2(h), 2(m)-2(p)).

Table 1. Contrast of the stacked images for the qualified sets of the access structure 1

Qualified set	Contrast α	Qualified set	Contrast α
{1,2}	1/7	{1,2,4}	1/13
{1,3}	1/7	{1,3,4}	1/13
{2,3}	1/7	{2,3,4}	1/13
{1,2,3}	1/4	{1,2,3,4}	1/8

Table 2. Comparison of the contrast between the proposed scheme and random-grid based VSS schemes

Scheme	$(2,2)$	(n,n)	(k,n)	Access structure
Kafri and Keren [6]	$\frac{1}{2}$	-	-	-
Shyu [13]	$\frac{1}{2}$	$\frac{1}{2^{n-1}}$	-	-
Chen and Tsao [4]	$\frac{1}{2}$	$\frac{1}{2^{n-1}}$	-	-
Chen and Tsao [5]	$\frac{1}{2}$	$\frac{1}{2^{n-1}}$	$\frac{2\times\binom{t}{k}}{(2^t+1)\times\binom{n}{k}-\binom{t}{k}}$	-
Ours	$\frac{1}{2}$	$\frac{1}{2^{n-1}}$	$\frac{2\times\binom{t}{k}}{(2^t+1)\times\binom{n}{k}-\binom{t}{k}}$	$\frac{2\times c}{N\times 2^t+N-c}$

$k \le t \le n$.

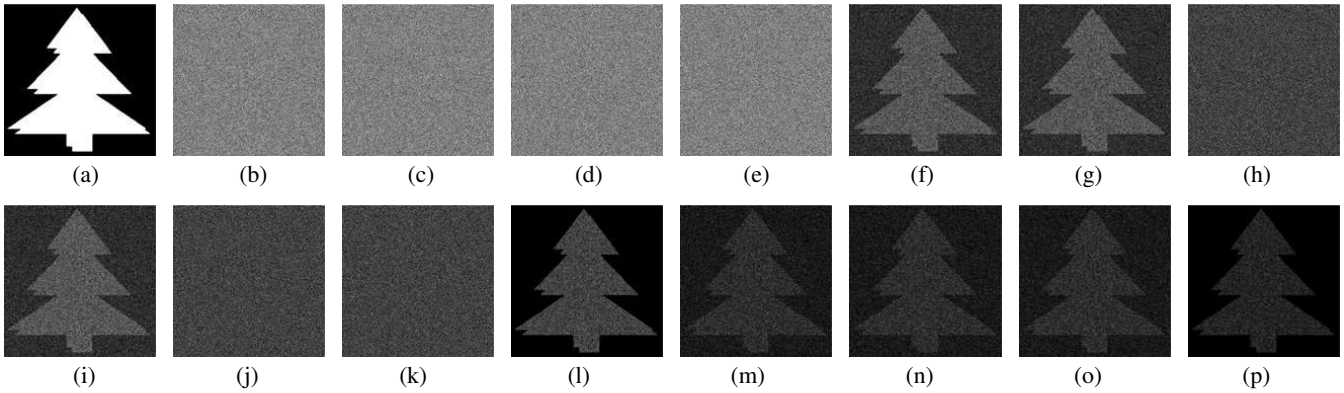

Fig. 1 The experimental results of the proposed scheme for the access structure 1: (a) Binary secret image; (b) $\mathbf{R_1}$; (c) $\mathbf{R_2}$; (d) $\mathbf{R_3}$; (e) $\mathbf{R_4}$; (f) $\mathbf{R_1 \otimes R_2}$; (g) $\mathbf{R_1 \otimes R_3}$; (h) $\mathbf{R_1 \otimes R_4}$; (i) $\mathbf{R_2 \otimes R_3}$; (j) $\mathbf{R_2 \otimes R_4}$; (k) $\mathbf{R_3 \otimes R_4}$; (l) $\mathbf{R_1 \otimes R_2 \otimes R_3}$; (m) $\mathbf{R_1 \otimes R_2 \otimes R_4}$; (n) $\mathbf{R_1 \otimes R_3 \otimes R_4}$; (o) $\mathbf{R_2 \otimes R_3 \otimes R_4}$; (p) $\mathbf{R_1 \otimes R_2 \otimes R_3 \otimes R_4}$.

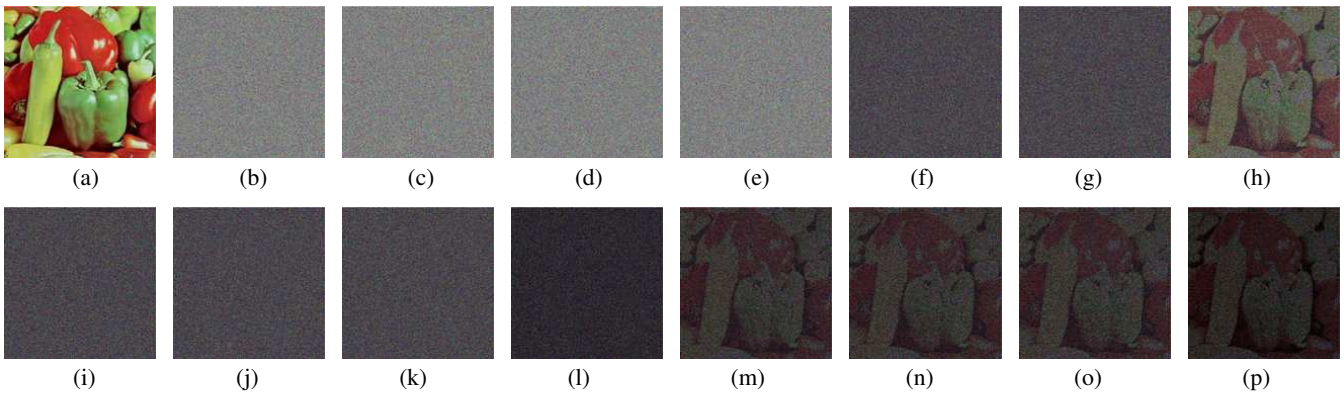

Fig. 2 The experimental results of the proposed scheme for the access structure 2: (a) Color secret image; (b) $\mathbf{R_1}$; (c) $\mathbf{R_2}$; (d) $\mathbf{R_3}$; (e) $\mathbf{R_4}$; (f) $\mathbf{R_1 \otimes R_2}$; (g) $\mathbf{R_1 \otimes R_3}$; (h) $\mathbf{R_1 \otimes R_4}$; (i) $\mathbf{R_2 \otimes R_3}$; (j) $\mathbf{R_2 \otimes R_4}$; (k) $\mathbf{R_3 \otimes R_4}$; (l) $\mathbf{R_1 \otimes R_2 \otimes R_3}$; (m) $\mathbf{R_1 \otimes R_2 \otimes R_4}$; (n) $\mathbf{R_1 \otimes R_3 \otimes R_4}$; (o) $\mathbf{R_2 \otimes R_3 \otimes R_4}$; (p) $\mathbf{R_1 \otimes R_2 \otimes R_3 \otimes R_4}$.

Table 3. Comparison of the contrast between the proposed scheme and Wu and Sun's scheme [16]

Qualified set	The proposed scheme	Wu and Sun's scheme [16]
{1,2}	1/7	1/19
{2,4}	1/7	1/19
{1,2,3}	1/13	1/17
{1,2,4}	4/25	1/19
{2,3,4}	1/13	1/17
{1,3,4}	1/13	1/17
{1,2,3,4}	1/8	1/17

Table 4. Comparison of the contrast between the proposed scheme and Shyu's scheme [14]

Qualified set	The proposed scheme	Shyu's method by using Γ_0 [14]	Shyu's method by using Z_M [14]
{1,2,3}	2/35	1/256	1/32
{1,2,4}	2/35	1/256	1/32
{1,3,4}	2/35	1/256	1/32
{2,3,4}	2/35	1/256	1/32
{1,2,3,4}	1/8	1/256	1/32

5.3 Comparison with related work

A random-grid based (k, n)-threshold VSS scheme with $2 \leq k \leq n$ can be obtained as a special case of the proposed scheme by taking the basis $\Gamma_0 = \{Q \subseteq \mathcal{P} : |Q| = k\}$. In this case, we have $c = \binom{t}{k}$ and $N = \binom{n}{k}$ for any qualified set of t ($\geq k$) participants. Thus, the contrast (in Algorithm 4 based on Algorithm 1) of the image obtained by stacking any t shares is $\frac{2\times\binom{t}{k}}{(2^t+1)\times\binom{n}{k}-\binom{t}{k}}$. This is same as the contrast obtained in random-grid based (k, n)-threshold VSS scheme [5]. If we take $t = n$, then the contrast of the decoded image will be $\frac{1}{2^{n-1}}$, which is again same as obtained in random-grid based (n, n) VSS scheme [4, 13]. The proposed scheme reconstructs the secret image with visual quality similar to random-grid based VSS schemes [4–6, 13] as shown in Table 2.

Similar to our scheme, the VSS schemes [14, 16] can also handle general access structures. To compare the proposed scheme with Wu and Sun's scheme [16], an access structure defined on a set

Table 5. Comparison of the proposed scheme with related VSS schemes

Scheme	Encoding based on	Type	Pixel expansion	Codebook requirement	Secret image format
Naor and Shamir [11]	Basis matrices	(n, n) and (k, n)	Yes	Yes	Binary
Ateniese et al. [2]	Basis matrices	Access structure	Yes	Yes	Binary
Adhikari et al. [1]	Basis matrices	Access structure	Yes	Yes	Binary
Wu and Sun [16]	Basis matrices	Access structure	No	Yes	Binary and Color
Kafri and Keren [6]	Random-grid	$(2, 2)$	No	No	Binary
Shyu [13]	Random-grid	(n, n)	No	No	Binary and Color
Chen and Tsao [4]	Random-grid	$(2, n)$ and (n, n)	No	No	Binary and Color
Chen and Tsao [5]	Random-grid	(k, n)	No	No	Binary and Color
Ours	Random-grid	Access structure	No	No	Binary and Color

$\mathcal{P} = \{1, 2, 3, 4\}$ with the basis $\Gamma_0 = \{\{1, 2\}, \{2, 4\}, \{1, 3, 4\}\}$ and $Z_M = \{\{1, 3\}, \{1, 4\}, \{2, 3\}, \{3, 4\}\}$ is taken. The following modified basis matrices are obtained by using the method discussed in [16], which are used to generate the shares.

$$B_0^M = \begin{bmatrix} 0\,0\,1\,1\,1\,1\,1\,1\,1\,0\,0\,0\,0\,0 \\ 0\,1\,1\,1\,1\,1\,1\,1\,0\,0\,0\,0\,0\,0 \\ 0\,1\,0\,0\,1\,1\,0\,1\,1\,1\,1\,0\,0\,0 \\ 0\,1\,1\,1\,1\,0\,1\,1\,1\,0\,0\,0\,0\,0 \end{bmatrix}, B_1^M = \begin{bmatrix} 0\,0\,1\,1\,1\,1\,1\,1\,1\,0\,0\,0\,0\,0 \\ 1\,1\,0\,1\,1\,1\,1\,1\,0\,0\,0\,0\,0\,0 \\ 0\,1\,0\,0\,1\,1\,0\,1\,1\,1\,1\,0\,0\,0 \\ 1\,0\,1\,0\,1\,1\,1\,1\,1\,0\,0\,0\,0\,0 \end{bmatrix}.$$

Table 3 shows the contrast of the decoded images in the proposed scheme and Wu and Sun's scheme [16] for the given access structure. It is obvious that the proposed scheme can achieve higher contrast compared to Wu and Sun's scheme [16]. Shyu's scheme [14] adopts two different algorithms for encrypting a secret image into general access structures, i.e., by using the construction based on either basis Γ_0 or collection of maximal forbidden sets Z_M. For comparison between the proposed scheme and Shyu's scheme [14], the access structure defined on a set $\mathcal{P} = \{1, 2, 3, 4\}$ with the basis $\Gamma_0 = \{\{1, 2, 3\}, \{1, 2, 4\}, \{1, 3, 4\}\{2, 3, 4\}\}$ and $Z_M = \{\{1, 2\}, \{1, 3\}, \{1, 4\}, \{2, 3\}, \{2, 4\}, \{3, 4\}\}$ is considered. Table 4 confirms that the proposed scheme can achieve higher contrast while comparing to algorithms proposed in [14].

In Table 5, the proposed scheme is compared with the related VSS schemes in terms of the pixel expansion, codebook requirement, type of the scheme and the secret image format. Compared to VSS schemes [1, 2, 11], the proposed scheme benefits by sharing binary as well as color images without any pixel expansion and codebook requirement. Compared to the proposed scheme, Wu and Sun's scheme [16] can share the secret image for general access structures without any pixel expansion, but requires the basis matrices before encryption process. The proposed scheme generalizes the existing random-grid based VSS schemes [4–6, 13] to share a secret image for general access structures. Precisely, the proposed scheme for general access structures is obtained by extending the random-grid based algorithm and attains the security conditions perfectly, i.e., only qualified sets can recover the secret image while the forbidden sets cannot gain any information about the secret image.

6. CONCLUSION

In this paper, a VSS scheme for general access structures is designed based on random grids. The proposed scheme can be used to share a secret image into general access structures without any pixel expansion and codebook requirement. The security analysis and experimental results are given to confirm that the proposed scheme performs well. The potential applications of the proposed scheme may include image sharing, visual authentication, digital watermarking, image hiding, etc.

References

[1] A. Adhikari, T. K. Dutta, and B. Roy. A new black and white visual cryptographic scheme for general access structures. In *Indocrypt'04*, volume 3348, pages 399–413. LNCS, Springer-Verlag, 2004.

[2] G. Ateniese, C. Blundo, A. De Santis, and D. R. Stinson. Visual cryptography for general access structures. *Information and Computation*, 129:86–106, 1996.

[3] G. R. Blakley. Safeguarding cryptographic keys. *AFIPS Conference Proceedings*, 48:313–317, 1979.

[4] T. H. Chen and K. H. Tsao. Visual secret sharing by random grids revisited. *Pattern Recognition*, 42:2203–2217, 2009.

[5] T. H. Chen and K. H. Tsao. Threshold visual secret sharing by random grids. *The Journal of Systems and Software*, 84:1197–1208, 2011.

[6] O. Kafri and E. Keren. Encryption of pictures and shapes by random grids. *Optics Letters*, 12(6):377–379, 1987.

[7] S. Kumar and R. K. Sharma. Improving contrast in random grids based visual secret sharing. *International Journal of Security and Its Application*, 6:9–28, 2012.

[8] S. Kumar and R. K. Sharma. Recursive information hiding of secrets by random grids. *Cryptologia*, 37:154–161, 2013.

[9] S. Kumar and R. K. Sharma. Threshold visual secret sharing based on boolean operations. *Security and Communication Networks*, 2013. dOI:10.1002/sec.769.

[10] D. L. Lau and G. R. Arce. *Modern Digital Halftoning*. Marcel Dekker, New York, 2000.

[11] M. Naor and A. Shamir. Visual cryptography. In *Proceedings of Advances in Cryptology (EUROCRYPT 94)*, volume 950, pages 1–12. LNCS,Springer-Verlag, 1995.

[12] A. Shamir. How to share a secret. *Communication of the ACM*, 22(11):612–613, 1979.

[13] S. J. Shyu. Image encryption by multiple random grids. *Pattern Recognition*, 42:1582–1596, 2009.

[14] S. J. Shyu. Visual cryptograms of random grids for general access structures. *IEEE Trans. on Circuits and Systems for Video Technology*, 23:414–424, 2013.

[15] R. Ulichney. *Digital Halftoning*. The MIT Press, Cambridge, 1987.

[16] X. Wu and W. Sun. Random grid-based visual secret sharing for general access structures with cheat-preventing ability. *The Journal of Systems and Software*, 85:1119–1134, 2012.