Improved Contrast for Threshold Random-grid-based Visual Cryptography

Hao Hu[1*], Gang Shen[2], Zhengxin Fu[2] and Bin Yu[2]
[1] China National Digital Switching System Engineering and Technological Research Center, Zhengzhou 450000, China
[2] Zhengzhou Information Science and Technology Institute, Zhengzhou 450000, China
[e-mail: wjjhh_908@163.com]
[e-mail: shengang_zisti@163.com]
[e-mail: fzx2515@163.com]
[e-mail: byu2009@163.com]
*Corresponding author: Hao Hu

Received August 11, 2017; revised October 19, 2017; accepted February 13, 2018; published July 31, 2018

Abstract

Pixel expansion and contrast are two major performance parameters for visual cryptography scheme (VCS), which is a type of secret image sharing. Random Grid (RG) is an alternative approach to solve the pixel expansion problem. Chen and Tsao proposed the first (*k*, *n*) RG-based VCS, and then Guo et al., Wu et al., Shyu, and Yan et al. significantly improved the contrast in recent years. However, the investigations on improving the contrast of threshold RG-based VCS are not sufficient. In this paper, we develop a contrast-improved algorithm for (*k*, *n*) RG-based VCS. Theoretical analysis and experimental results demonstrate that the proposed algorithm outperformers the previous threshold algorithms with better visual quality and a higher accuracy of contrast.

Keywords: Secret image sharing, visual cryptography, random grid, threshold, contrast

1. Introduction

A (k, n) visual cryptography scheme (VCS), which is a type of secret image sharing, encodes a secret image (confined to a binary image in this paper) into n meaningless shares in such a way that stacking any more than or equal to k shares can recover the secret image visually, while any less than k shares can't get any information about the secret image. Its beauty is that the decoding process is directly done via human visual system instead of complex cryptographic computation. There are two ways to realize a VCS: encode matrix (EM), introduced by Naor and Shamir [1], and random grid (RG), introduced by Kafri and Keren [2].

EM-based VCS encodes each pixel of a secret image into m subpixels, referred to as the pixel expansion, for each of the n shares 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 one of the shares. Based on the above principle, many papers have explored various aspects: general access structure [3-4], pixel expansion [5-6], contrast [7], randomness [8], multiple secrets [9], color image [10], cheating prevention [11-12], meaningful shares [13-14] and other issues [15-16]. Different from the above-mentioned schemes, which are now called deterministic schemes, a probabilistic scheme, which was introduced by Yang [17] to relieve the concern of pixel expansion, recover the secret pixel with a certain probability instead of a deterministic difference. Later, Cimato et al. [18] generalized the probabilistic scheme to show how to trade pixel expansion for the probability of a good reconstruction and proved that there exists a one-to-one mapping between a probabilistic scheme with no pixel expansion and a deterministic scheme. However, EM-based VCSs always need matrices to support encoding. The matrices are not easily generated for some specific cases in [3].

RG-based VCS encodes a secret image into several size invariant random grids. Each random grid is a transparency comprising a two-dimensional array of pixels that are either transparent or opaque determined in a totally random way. Compared to EM-based VCS, RG-based VCS has merits such as no encode matrix and no pixel expansion. After RG-based VCS is first introduced, its development is not significant for a long period [19-21]. Until recently, Chen and Tsao gave a general construction for (k, n) RG-based VCS [22]. Schemes for general access structure (GAS) were described in [23-25]. Constructing RG-based VCS with abilities of both OR and XOR decryptions was introduced in [26]. Furthermore, generating meaningful random grids was proposed in [27]. A novel quality-adaptive threshold RG-based VCS with progressive visual property was proposed in [28]. Yan et al. [29] proposed a (k, n) threshold random grids based visual cryptography with the function of participants increment in further. In essence, which is still a progressive scheme. On this basis, Chao et al. [30] improved the progressive visual cryptography scheme with adaptive priority, wherein the priority weighting of each share can be adjusted. More deeply, the relationship between probabilistic EM-based VCS and RG-based VCS is analyzed in [31-32] and they concluded that a RG-based VCS is a subset of a probabilistic EM-based VCS and improving the contrast of RG-based VCS is the future work.

Since then, many interesting schemes were proposed in recent years i.e. Guo et al [33], Wu and Sun [34], Shyu [35] and Yan et al [36] to improve the first scheme by Chen and Tsao [22]. They all focused on the threshold RG-based VCS, regarded as the basis for GAS-

VCS and other applications. In detail, Chen and Tsao [22] proposed the first (*k*, *n*) case by applying (*k*, *k*) RG-based VCS to generate the first *k* pixels and generating the last *n*-*k* pixels randomly. For the (*k*, *k*)-VCS, the first *k*-1 pixels $r_1, r_2, \cdots, r_{k-1}$ are randomly generated, and the last pixel is further generated by the secret pixel *s* and first *k*-1 pixels using $r_k = s \oplus r_1 \oplus r_2 \oplus \cdots \oplus r_{k-1}$, where $\oplus$ is the Boolean XOR operation. Then Guo et al. [33] improved the contrast in another approach. They repeat the (*k*, *k*)-VCS $\lfloor n/k \rfloor$ times to generate the first $k \cdot \lfloor n/k \rfloor$ pixels and assign the last $n - k \cdot \lfloor n/k \rfloor$ pixels randomly. Almost at the same time, Wu and Sun [34] enhanced the visual performance of (*k*, *n*) case by replacing the last *n*-*k* pixels equal to the *k*-th pixel. Afterwards, Shyu [35] found that the first *k* pixels in the (*k*, *n*)-VCS are generated in the same way by applying (*k*, *k*)-VCS, and meanwhile, the contrast performance is obtained through the first *k* pixels while the last *n*-*k* pixels cannot make any contributions to the contrast. Based on this observation, he improved the contrast by using some pixels in the first *k* pixels to replace the last *n*-*k* pixels, leading to increase the chance for the participants to hold the pixels in the (*k*, *k*)-VCS. Furthermore, Yan et al. [36] enhanced the visual quality by changing the last *n*-*k* pixels from selecting the first *k* pixels one by one, through which the probability of covering the first *k* pixels in the recovered image is improved.

At present, although many schemes have been proposed to improve the contrast, the contrast for certain case of (*k*, *n*) is computed through the specific statistics given by experiments, which is an approximate value essentially. The theoretical contrast by a formal formula is not given yet. As explained in section “Conclusion” in Yan et al. [36], “However, the contrast of the proposed scheme is not given directly by *k*, *t* and *n*, which is left as an open problem for further studies.”

In this paper, the further improvement on contrast of (*k*, *n*) RG-based VCS is obtained. Besides, the general formula of contrast is provided. In our design, based on the finding that the amount of first *k* pixels (generated by (*k*, *k*)-VCS) in the total *n* pixels is related with the contrast, we better arranged the last *n*-*k* pixels by utilizing the first *k* pixels. In the process of decoding, by dividing the *n* empty share pixels into *k* groups, guaranteeing that all the pixels in the same group are the same, and the different pixels in different groups are distinct. The distinct pixels in the *k* different groups are generated using (*k*, *k*)-VCS. By calculating the number of (*k*, *k*)-VCS the user can obtain when stacking *t* shares, the general formula of contrast can be computed. It helps one gain more precise knowledge about the contrast and calculate the contrast easily without implementing complex experiments.

The rest of this paper is organized as follows. In section 2, we give a brief review of the previous (*k*, *n*) RG-based VCSs. The proposed contrast-improved algorithm and its theoretical analysis are described in Section 3. The experimental results and discussions are shown in Section 4 and the paper is concluded in Section 5.

2. Related Works

In a (*k*, *n*) RG-based VCS, a secret image *S* is encoded into *n* random grids $R_1, \cdots, R_n$. Let $\otimes$ denote the Boolean OR operation and the stacking result of any *t* ($t \geq k$) of the *n* random grids $R_1, \cdots, R_n$ can be represented by $R_{i_1 \otimes \cdots \otimes i_t} = R_{i_1} \otimes \cdots \otimes R_{i_t}$. The visual quality of the recovered secret image is reflected by the contrast, which is defined by means of the average light transmission. In addition, let digit 0 (resp. 1) denote a white (resp. black) pixel and $\oplus$ denote the Boolean XOR operation in this paper.

Definition 1 (Average light transmission [19]). For a certain pixel p in a binary image P whose size is $M\times N$, the probability for p being transparent, say $Prob(p=0)$, is represented as the light transmission of p, say $T(p)$. The light transmission of a white (resp. black) pixel is defined as $T(p)=1$ (resp. $T(p)=0$). The average light transmission of P is defined as

$$T(P)=\frac{1}{M\times N}\times\sum_{i=1}^{M}\sum_{j=1}^{N}T(P[i,j]).$$

Definition 2 (Contrast [19]). Let $S(0)$ (resp. $S(1)$) denote the area of all the white (resp. black) pixels in the secret image and $R_{i_1\otimes\cdots\otimes i_t}[S(0)]$ (resp. $R_{i_1\otimes\cdots\otimes i_t}[S(1)]$) denote the corresponding area of all the white (resp. black) pixels in the recovered secret image. The contrast of the recovered secret image $R_{i_1\otimes\cdots\otimes i_t}=R_{i_1}\otimes\cdots\otimes R_{i_t}$ with respect to the original secret image S is

$$\alpha=\frac{T(R_{i_1\otimes\cdots\otimes i_t}[S(0)])-T(R_{i_1\otimes\cdots\otimes i_t}[S(1)])}{1+T(R_{i_1\otimes\cdots\otimes i_t}[S(1)])}.$$

Contrast determines how well human visual system can recognize the recovered secret image. It is considered to be as large as possible.

Definition 3 (Visual recognition [21]). The recovered secret image $R_{i_1\otimes\cdots\otimes i_t}=R_{i_1}\otimes\cdots\otimes R_{i_t}$ is visual recognizable with respect to the original secret image S by contrast $\alpha>0$, which means that $T(R_{i_1\otimes\cdots\otimes i_t}[S(0)])>T(R_{i_1\otimes\cdots\otimes i_t}[S(1)])$. Whereas, the recovered secret image gives no clue about the original secret image when $\alpha=0$.

At present, several algorithms [22, 33-34, 35-36] for (k, n) RG-based VCS were proposed. Herein, we review and analyze some classical related schemes especially Chen et al. [22], Guo et al. [33], Wu and Sun [34], which are presented as Algorithm 1, Algorithm 2, and Algorithm 3, respectively.

Algorithm 1 [22]

Input: A binary secret image S, whose size is $M\times N$.

Output: n random grids $R_1,\cdots,R_n$.

Step 1: For each secret pixel $S(i,j)$, where $1\le i\le M, 1\le j\le N$, repeat Step 2-4.

Step 2: Generate k-1 pixels $r_1,\cdots,r_{k-1}$ by assigning 0 or 1 randomly and the k-th pixel r_k by $r_k=S(i,j)\oplus r_{k-1}\oplus\cdots\oplus r_1$.

Step 3: Generate $n-k$ pixels $r_{k+1},\cdots,r_n$ by assigning 0 or 1 randomly.

Step 4: Randomly assign the above pixels $r_1,\cdots,r_n$ to $R_1(i,j),\cdots,R_n(i,j)$.

Step 5: Output the n random grids $R_1,\cdots,R_n$.

Algorithm 2 [33]

Input: A binary secret image S, whose size is $M\times N$.

Output: n random grids $R_1,\cdots,R_n$.

Step 1: For each secret pixel $S(i,j)$, where $1\le i\le M, 1\le j\le N$, repeat Step 2-4.

Step 2: Generate k-1 pixels $r_1,\cdots,r_{k-1}$ by assigning 0 or 1 randomly and the k-th pixel r_k by $r_k=S(i,j)\oplus r_{k-1}\oplus\cdots\oplus r_1$.

Step 3: Repeat Step 2 $\left\lfloor \frac{n}{k} \right\rfloor$ times to generate $k \times \left\lfloor \frac{n}{k} \right\rfloor$ pixels in total. Then generate $n - k \times \left\lfloor \frac{n}{k} \right\rfloor$ pixels by assigning 0 or 1 randomly.

Step 4: Randomly assign the above pixels $r_1, \cdots, r_n$ to $R_1(i, j), \cdots, R_n(i, j)$.

Step 5: Output the n random grids $R_1, \cdots, R_n$.

Algorithm 3 [34]

Input: A binary secret image S, whose size is $M \times N$.

Output: n random grids $R_1, \cdots, R_n$.

Step 1: For each secret pixel $S(i, j)$, where $1 \le i \le M, 1 \le j \le N$, repeat Step 2-4.

Step 2: Generate k-1 pixels $r_1, \cdots, r_{k-1}$ by assigning 0 or 1 randomly and the k-th pixel r_k by $r_k = S(i, j) \oplus r_{k-1} \oplus \cdots \oplus r_1$.

Step 3: Generate $n-k$ pixels $r_{k+1}, \cdots, r_n$ by $r_{k+1} = \cdots = r_n = r_k$.

Step 4: Randomly assign the above pixels $r_1, \cdots, r_n$ to $R_1(i, j), \cdots, R_n(i, j)$.

Step 5: Output the n random grids $R_1, \cdots, R_n$.

Remark: Comparing the above three algorithms, we find out the following results:

(1) They are the same in Step 2, which realizes a (k, k) RG-based VCS [20-21]. As a result, for $k = n$, the three algorithms are reduced to a (k, k) RG-based VCS.

(2) They are the same in Step 4, which guarantees that stacking any k or more random grids of $R_1, \cdots, R_n$ can recover the secret image.

(3) They are only different in Step 3, which generates the $n-k$ pixels $r_{k+1}, \cdots, r_n$. As a result, the key step to improve the contrast is how to generate the $n-k$ pixels $r_{k+1}, \cdots, r_n$.

3. The Proposed Algorithm

In this section, we develop a contrast-improved algorithm, presented as Algorithm 4, for (k, n) RG-based VCS. Diagram of the proposed algorithm is illustrated in **Fig. 1**.

Algorithm 4

Input: A binary secret image S, whose size is $M \times N$.

Output: n random grids $R_1, \cdots, R_n$.

Step 1: For each secret pixel $S(i, j)$, where $1 \le i \le M, 1 \le j \le N$, repeat Step 2-4.

Step 2: Generate k-1 bits $r_1, \cdots, r_{k-1}$ by assigning 0 or 1 randomly and the k-th pixel r_k by $r_k = S(i, j) \oplus r_{k-1} \oplus \cdots \oplus r_1$.

Step 3: Generate $n-k$ pixels $r_{k+1}, \cdots, r_n$ by

$$\begin{cases} r_{k+1} = S[i, j] \oplus r_k \oplus r_{k-1} \oplus \cdots \oplus r_2 \\ r_{k+2} = S[i, j] \oplus r_{k+1} \oplus r_k \oplus \cdots \oplus r_3 \\ \vdots \\ r_n = S[i, j] \oplus r_{n-1} \oplus r_{n-2} \oplus \cdots \oplus r_{n-k+1} \end{cases}.$$

Step 4: Randomly assign the above pixels $r_1,\cdots,r_n$ to $R_1(i,j),\cdots,R_n(i,j)$.

Step 5: Output the n random grids $R_1,\cdots,R_n$.

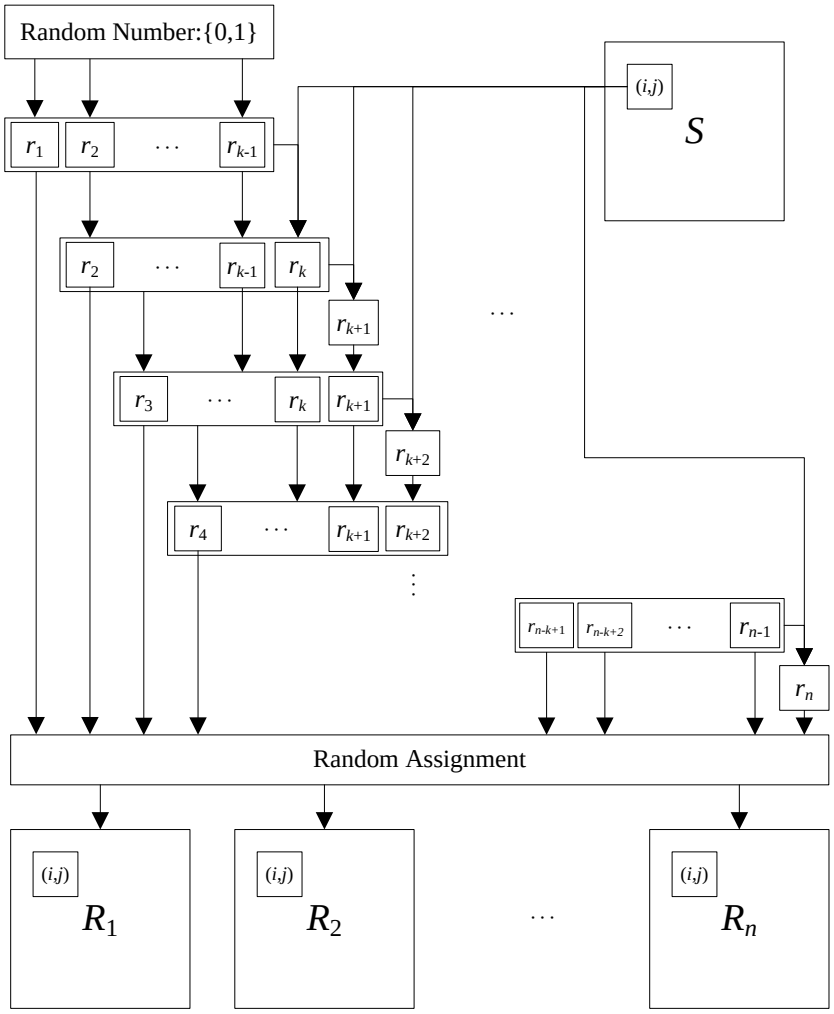

Fig. 1. Diagram of the proposed contrast-improved algorithm.

Remark:

(1) Comparing Algorithm 4 with Algorithm 1-3, the only difference is in Step 3. To improve the contrast, Algorithm 4 generates the $n-k$ pixels by $r_{k+t}=S[i,j]\oplus r_{k+t-1}\oplus r_{k+t-2}\oplus\cdots\oplus r_{t+1}$, where $t=1,2,\cdots,n-k$. When encoding, the n original pixels in the empty shares are divided into k groups $G_1,G_2,\cdots,G_k$, where $G_1=\{r_1,r_{k+1},\cdots,r_{(\lceil n/k\rceil-1)k+1}\}$, $G_2=\{r_2,r_{k+2},\cdots,r_{(\lceil n/k\rceil-1)k+2}\}$, $\cdots$, $G_k=\{r_k,r_{2k},\cdots,r_{(\lceil n/k\rceil-1)k}\}$.

(2) The proposed scheme can be extended to share a grayscale/color secret image combining with the halftone technologies such as error diffusion [10]. To share a grayscale image, the original grayscale image can be converted into a binary image using halftone method, after then our scheme can be implemented to encode the halftone secret image. More details can be referred to [10].

Theoretical analysis on Algorithm 4 is provided as follows.

Lemma 1. Given a secret pixel $S[i, j]$, the pixels $r_1, \cdots, r_n$ satisfy the following two conditions:

(i) $Prob(r_t = 0) = Prob(r_t = 1) = \frac{1}{2}, t = 1, 2, \cdots, n$.

(ii)
$$\begin{cases} r_1 = r_{k+1} = \cdots = r_{\left(\left\lfloor \frac{n}{k} \right\rfloor - 1\right)k+1} \\ r_2 = r_{k+2} = \cdots = r_{\left(\left\lfloor \frac{n}{k} \right\rfloor - 1\right)k+2} \\ \vdots \\ r_{(n-1) \bmod k+1} = r_{k+(n-1) \bmod k+1} = \cdots = r_{\left(\left\lfloor \frac{n}{k} \right\rfloor - 1\right)k+(n-1) \bmod k+1} \\ r_{(n-1) \bmod k+2} = r_{k+(n-1) \bmod k+2} = \cdots = r_{\left(\left\lfloor \frac{n}{k} \right\rfloor - 2\right)k+(n-1) \bmod k+2} \\ \vdots \\ r_k = r_{2k} = \cdots = r_{\left(\left\lfloor \frac{n}{k} \right\rfloor - 1\right)k} \end{cases}.$$

Proof. The first $k-1$ pixels are randomly assigned the value 0 or 1, therefore $Prob(r_t = 0) = Prob(r_t = 1) = \frac{1}{2}$ for $1 \le t \le k-1$. Since $r_k = r_{k-1} \oplus \cdots \oplus r_1 \oplus S[i, j]$, we obtain $Prob(r_k = 0) = Prob(r_k = 1) = \frac{1}{2}$ no matter $S[i, j]$ is 0 or 1.

For the rest $n-k$ pixels, since

$$\begin{aligned} r_{k+1} &= r_k \oplus \cdots \oplus r_2 \oplus S[i, j] \\ r_{k+2} &= r_{k+1} \oplus \cdots \oplus r_3 \oplus S[i, j] \\ &\vdots \\ r_n &= r_{n-1} \oplus \cdots \oplus r_{n-k+1} \oplus S[i, j] \end{aligned},$$

the following cases are considered:

(1) if $\left\lfloor \frac{n}{k} \right\rfloor \le 2$,

$$r_{k+1} = r_1, r_{k+2} = r_2, \cdots, r_{k+(n-1) \bmod k+1} = r_{(n-1) \bmod k+1}.$$

(2) if $2 < \left\lfloor \frac{n}{k} \right\rfloor \le 3$,

$$r_{2k+1} = r_{k+1} = r_1, r_{2k+2} = r_{k+2} = r_2, \cdots, r_{2k+(n-1) \bmod k+1} = r_{k+(n-1) \bmod k+1} = r_{(n-1) \bmod k+1}.$$

And so on.

To sum up the above cases generally, we conclude the second condition immediately. In other words, the rest $n-k$ pixels are equal to the first k pixels correspondingly. Since

$$Prob(r_t = 0) = Prob(r_t = 1) = \frac{1}{2}, t = 1, 2, \cdots, k,$$

we have

$$Prob(r_t = 0) = Prob(r_t = 1) = \frac{1}{2}, t = k+1, k+2, \cdots, n,$$

and the first condition is proved.

Lemma 2. Given a secret pixel $S[i, j]$, any t ($t < k$) pixels of $r_1, \cdots, r_k$ satisfy

$$T(r_{i_1 \otimes \cdots \otimes i_t}[S[i, j] = 0]) = T(r_{i_1 \otimes \cdots \otimes i_t}[S[i, j] = 1]) = \left(\frac{1}{2}\right)^t, t < k,$$

where $r_{i_1 \otimes \cdots \otimes i_t} = r_{i_1} \otimes \cdots \otimes r_{i_t}$ and $\{r_{i_1}, \cdots, r_{i_t}\} \subset \{r_1, \cdots, r_k\}$.

Proof. Let $Prob(A|B)$ denote the probability for A if B is satisfied. To prove this lemma, we have the following two cases to be considered:

(1) $r_k \in \{r_{i_1}, \cdots, r_{i_t}\}$

Since $r_1, \cdots, r_{k-1}$ are randomly generated, their positions are equivalent. Without loss of generality, assume $\{r_{i_1}, r_{i_2}, \cdots, r_{i_t}\} = \{r_1, r_2, \cdots, r_{t-1}, r_k\}$. Because the $t-1$ pixels $r_1, r_2, \cdots, r_{t-1}$ are randomly generated and they are independent of $S[i, j]$, we get

$$T(r_{1 \otimes \cdots \otimes (t-1)}[S[i, j] = 0]) = T(r_{1 \otimes \cdots \otimes (t-1)}[S[i, j] = 1]) = \left(\frac{1}{2}\right)^{t-1}.$$

Since

$$r_k = r_{k-1} \oplus \cdots \oplus r_1 \oplus S[i, j],$$

we get

$$\begin{aligned} & Prob(r_k = 0 | r_1 = 0, \cdots, r_{t-1} = 0, S[i, j] = 0) \\ = \; & Prob(r_{k-1} \oplus r_{k-2} \oplus \cdots \oplus r_t = 0) \end{aligned},$$

and

$$\begin{aligned} & Prob(r_k = 0 | r_1 = 0, \cdots, r_{t-1} = 0, S[i, j] = 1) \\ = \; & Prob(r_{k-1} \oplus r_{k-2} \oplus \cdots \oplus r_t \oplus 1 = 0) \\ = \; & Prob(r_{k-1} \oplus r_{k-2} \oplus \cdots \oplus \overline{r_t} = 0) \end{aligned}.$$

Since $r_t, \cdots, r_{k-2}, r_{k-1}$ are randomly generated and $\overline{r_t}$ is random as well as r_t, we have

$$\begin{aligned} & Prob(r_k = 0 | r_1 = 0, \cdots, r_{t-1} = 0, S[i, j] = 0) \\ = \; & Prob(r_k = 0 | r_1 = 0, \cdots, r_{t-1} = 0, S[i, j] = 1). \\ = \; & \frac{1}{2} \end{aligned}$$

Therefore,

$$\begin{aligned} & T(r_{1 \otimes \cdots \otimes (t-1) \otimes k}[S[i, j] = 0]) \\ = \; & Prob(r_1 \otimes \cdots \otimes r_{t-1} \otimes r_k = 0 | [S[i, j] = 0]) \\ = \; & Prob(r_k = 0 | r_1 \otimes \cdots \otimes r_{t-1} = 0, S[i, j] = 0) \times Prob(r_1 \otimes \cdots \otimes r_{t-1} = 0 | S[i, j] = 0), \\ = \; & Prob(r_k = 0 | r_1 = 0, \cdots, r_{t-1} = 0, S[i, j] = 0) \times T(r_{1 \otimes \cdots \otimes (t-1)}[S[i, j] = 0]) \\ = \; & \frac{1}{2} \times \left(\frac{1}{2}\right)^{t-1} = \left(\frac{1}{2}\right)^t \end{aligned}$$

and

$$
\begin{aligned}
& T(r_{1\otimes\cdots\otimes(t-1)\otimes k}[S[i,j]=1]) \\
= \ & Prob(r_1\otimes\cdots\otimes r_{t-1}\otimes r_k=0\big|[S[i,j]=1]) \\
= \ & Prob(r_k=0\big|r_1\otimes\cdots\otimes r_{t-1}=0,S[i,j]=1)\times Prob(r_1\otimes\cdots\otimes r_{t-1}=0\big|S[i,j]=1). \\
= \ & Prob(r_k=0\big|r_1=0,\cdots,r_{t-1}=0,S[i,j]=1)\times T(r_{1\otimes\cdots\otimes(t-1)}[S[i,j]=1]) \\
= \ & \frac{1}{2}\times\left(\frac{1}{2}\right)^{t-1}=\left(\frac{1}{2}\right)^{t}
\end{aligned}
$$

To conclude the above results generally, we have

$$T(r_{i_1\otimes\cdots\otimes i_t}[S[i,j]=0])=T(r_{i_1\otimes\cdots\otimes i_t}[S[i,j]=1])=\left(\frac{1}{2}\right)^{t}.$$

(2) $r_k\notin\left\{r_{i_1},\cdots,r_{i_t}\right\}$

The pixels $r_{i_1},\cdots,r_{i_t}$ are all randomly generated no matter $S[i,j]$ is 0 or 1. Hence, we have

$$T(r_{i_1\otimes\cdots\otimes i_t}[S[i,j]=0])=T(r_{i_1\otimes\cdots\otimes i_t}[S[i,j]=1])=\left(\frac{1}{2}\right)^{t}. \quad \square$$

Lemma 3. Given a secret pixel $S[i,j]$, the pixels $r_1,\cdots,r_k$ satisfy

$$T(r_{i_1\otimes\cdots\otimes i_k}[S[i,j]=0])=\left(\frac{1}{2}\right)^{k-1},T(r_{i_1\otimes\cdots\otimes i_k}[S[i,j]=1])=0.$$

Proof. By Lemma 2, we have

$$T(r_{i_1\otimes\cdots\otimes i_{k-1}}[S[i,j]=0])=T(r_{i_1\otimes\cdots\otimes i_{k-1}}[S[i,j]=1])=\left(\frac{1}{2}\right)^{k-1}.$$

Since the $k-1$ pixels $r_1,r_2,\cdots,r_{k-1}$ are randomly generated and $r_k=r_{k-1}\oplus\cdots\oplus r_1\oplus S[i,j]$, we have

$$
\begin{aligned}
& T(r_{1\otimes\cdots\otimes k}[S[i,j]=0]) \\
= \ & Prob(r_1\otimes\cdots\otimes r_k=0\big|[S[i,j]=0]) \\
= \ & Prob(r_k=0\big|r_1\otimes\cdots\otimes r_{k-1}=0,S[i,j]=0)\times Prob(r_1\otimes\cdots\otimes r_{k-1}=0\big|S[i,j]=0), \\
= \ & Prob(r_k=0\big|r_1=0,\cdots,r_{k-1}=0,S[i,j]=0)\times T(r_{1\otimes\cdots\otimes(k-1)}[S[i,j]=0]) \\
= & 1\times\left(\frac{1}{2}\right)^{k-1}=\left(\frac{1}{2}\right)^{k-1} \\
& T(r_{1\otimes\cdots\otimes k}[S[i,j]=1]) \\
= \ & Prob(r_1\otimes\cdots\otimes r_k=0\big|[S[i,j]=1]) \\
= \ & Prob(r_k=0\big|r_1\otimes\cdots\otimes r_{k-1}=0,S[i,j]=1)\times Prob(r_1\otimes\cdots\otimes r_{k-1}=0\big|S[i,j]=1). \ \square \\
= \ & Prob(r_k=0\big|r_1=0,\cdots,r_{k-1}=0,S[i,j]=1)\times T(r_{1\otimes\cdots\otimes(k-1)}[S[i,j]=1]) \\
= & 0\times\left(\frac{1}{2}\right)^{k-1}=0
\end{aligned}
$$

Lemma 4. Given a secret pixel $S[i,j]$, any t ($t<k$) pixels of $r_1,\cdots,r_n$ satisfy

$$T(r_{i_1\otimes\cdots\otimes i_t}[S[i,j]=0])=T(r_{i_1\otimes\cdots\otimes i_t}[S[i,j]=1]),t<k,$$

where $\{r_{i_1},\cdots,r_{i_t}\}\subset\{r_1,\cdots,r_n\}$.

Proof. According to the second condition of Lemma 1, the n pixels $r_1,\cdots,r_n$ are divided into k groups $G_1,G_2,\cdots,G_k$ and all pixels of the group G_j ($j=1,2,\cdots,k$) are equal to r_j. That means, the stacking result of any t ($t<k$) pixels is equal to the stacking result of w ($w\le t<k$) pixels of $r_1,\cdots,r_k$. For $\{r_{i_1},\cdots,r_{i_t}\}\subset\{r_1,\cdots,r_n\}$, there exists $\{r_{i_1},\cdots,r_{i_w}\}\subset\{r_1,\cdots,r_k\}$ satisfying

$$\begin{aligned}T(r_{i_1\otimes\cdots\otimes i_t}[S[i,j]=0])&=T(r_{i_1\otimes\cdots\otimes i_w}[S[i,j]=0])\\ T(r_{i_1\otimes\cdots\otimes i_t}[S[i,j]=1])&=T(r_{i_1\otimes\cdots\otimes i_w}[S[i,j]=1])\end{aligned}.$$

By Lemma 2, we have

$$T(r_{i_1\otimes\cdots\otimes i_w}[S[i,j]=0])=T(r_{i_1\otimes\cdots\otimes i_w}[S[i,j]=1])=\left(\frac{1}{2}\right)^w.$$

Hence,

$$T(r_{i_1\otimes\cdots\otimes i_t}[S[i,j]=0])=T(r_{i_1\otimes\cdots\otimes i_t}[S[i,j]=1]).\quad\square$$

Lemma 5. Given a secret pixel $S[i,j]$, any t ($t\ge k$) pixels of $r_1,\cdots,r_n$ satisfy

$$T(r_{i_1\otimes\cdots\otimes i_t}[S[i,j]=0])=Prob_k\times\left(\frac{1}{2}\right)^{k-1}+\sum_{w=1}^{k-1}Prob_w\times\left(\frac{1}{2}\right)^w,$$

$$T(r_{i_1\otimes\cdots\otimes i_t}[S[i,j]=1])=\sum_{w=1}^{k-1}Prob_w\times\left(\frac{1}{2}\right)^w,$$

where $Prob_w$ denotes the probability for selecting t pixels from any w ($1\le w\le k$) groups of $G_1,G_2,\cdots,G_k$ and $\sum_{w=1}^{k}Prob_w=1$.

Proof. Similar to the proof of Lemma 4, the stacking result of any t ($t\ge k$) pixels is equal to the stacking result of w ($w\le k$) pixels of $r_1,\cdots,r_k$. Two cases are taken into consideration: (1) $w=k$, (2) $w<k$.

(1) $w=k$. By Lemma 3, we have

$$T(r_{i_1\otimes\cdots\otimes i_t}[S[i,j]=0])=\left(\frac{1}{2}\right)^{k-1},T(r_{i_1\otimes\cdots\otimes i_t}[S[i,j]=1])=0,$$

where $\{r_{i_1},\cdots,r_{i_t}\}\subset\{r_1,\cdots,r_n\}$. The probability for this case is $Prob_k$.

(2) $w<k$. By Lemma 2, we have

$$T(r_{i_1\otimes\cdots\otimes i_t}[S[i,j]=0])=T(r_{i_1\otimes\cdots\otimes i_t}[S[i,j]=1])=\left(\frac{1}{2}\right)^w.$$

The total probability for this case is $\sum_{w=1}^{k-1}Prob_w$.

Therefore, the light transmission of the stacking result of any t pixels of $r_1,\cdots,r_n$ is

$$T(r_{i_1\otimes\cdots\otimes i_t}[S[i,j]=0])=Prob_k\times\left(\frac{1}{2}\right)^{k-1}+\sum_{w=1}^{k-1}Prob_w\times\left(\frac{1}{2}\right)^w,$$

$$T(r_{i_1\otimes\cdots\otimes i_t}[S[i,j]=1])=\sum_{w=1}^{k-1}Prob_w\times\left(\frac{1}{2}\right)^w. \quad \square$$

Theorem 1. Given a secret image S, Algorithm 4 is a valid construction for (k, n) RG-based VCS, which meets the following three conditions and its theoretical contrast $\alpha=\dfrac{Prob_k\times\left(\frac{1}{2}\right)^{k-1}}{1+\sum_{w=1}^{k-1}Prob_w\times\left(\frac{1}{2}\right)^w}$, where $1\le w\le k\le t\le n$.

(i) Each of n shares $R_1,\cdots,R_n$ is determined in a totally random way.

(ii) If $t<k$, $T(R_{i_1\otimes\cdots\otimes i_t}[S(0)])=T(R_{i_1\otimes\cdots\otimes i_t}[S(1)])$.

(iii) If $t\ge k$, $T(R_{i_1\otimes\cdots\otimes i_t}[S(0)])>T(R_{i_1\otimes\cdots\otimes i_t}[S(1)])$.

Proof. By Lemma 1, we derive the first condition of this theorem immediately.

If $t<k$, by Lemma 4, we have $T(r_{i_1\otimes\cdots\otimes i_t}[S[i,j]=0])=T(r_{i_1\otimes\cdots\otimes i_t}[S[i,j]=1])$. According to Definition 1, we get $T(R_{i_1\otimes\cdots\otimes i_t}[S(0)])=T(R_{i_1\otimes\cdots\otimes i_t}[S(1)])$.

If $t\ge k$, by Lemma 5, we have

$$\begin{aligned}&T(r_{i_1\otimes\cdots\otimes i_t}[S[i,j]=0])-T(r_{i_1\otimes\cdots\otimes i_t}[S[i,j]=1])\\ =\;& Prob_k\times\left(\frac{1}{2}\right)^{k-1}+\sum_{w=1}^{k-1}Prob_w\times\left(\frac{1}{2}\right)^w-\sum_{w=1}^{k-1}Prob_w\times\left(\frac{1}{2}\right)^w.\\ =\;& Prob_k\times\left(\frac{1}{2}\right)^{k-1}\end{aligned}$$

Noticing that $Prob_k>0$, we get $T(R_{i_1\otimes\cdots\otimes i_t}[S(0)])>T(R_{i_1\otimes\cdots\otimes i_t}[S(1)])$. $\square$

By Definition 2 and Lemma 5, the contrast of the proposed algorithm is

$$\alpha=\frac{Prob_k\times\left(\frac{1}{2}\right)^{k-1}}{1+\sum_{w=1}^{k-1}Prob_w\times\left(\frac{1}{2}\right)^w}.$$

Note that, the probability $Prob_w$ ($w=1,2,\cdots,k$) denotes the probability for selecting t pixels from any w ($1\le w\le k$) groups of $G_1,G_2,\cdots,G_k$ and $\sum_{w=1}^{k}Prob_w=1$. It is determined by the values of k, n and t.

4. Experimental Results and Discussions

This section first conducts some experiments to demonstrate the feasibility of the proposed scheme. Then some comparisons and discussions are given at last.

4.1 Feasibility analysis

Firstly, to verify the effectiveness of the proposed algorithm for (k, n) RG-based VCS, we conduct two experiments for (3, 4) and (3, 6) threshold, which are illustrated in **Fig. 2** and **Fig. 3** respectively. The size of the first binary secret image **Fig. 2(a)** is 700×700 and the

second secret image as shown in **Fig. 3(a)** with the size of 1024×1024. The feasibility of a VCS contains two aspects: the security and contrast properties.

For the first experiment of (3, 4) case, we can see that the 4 share images as shown in **Fig. 2(b-e)** are noise like, give no clue about the secret information. **Fig. 2(f-k)** indicate that stacking any less than 3 share images cannot give any information about the secret image. The above results indicate that the proposed scheme is secure. From **Fig. 2(l-p)**, the stacked results with any 3 or 4 share images can visually decode the secret image, which indicates that our scheme satisfies the visual recognition condition (contrast property) of Definition 3.

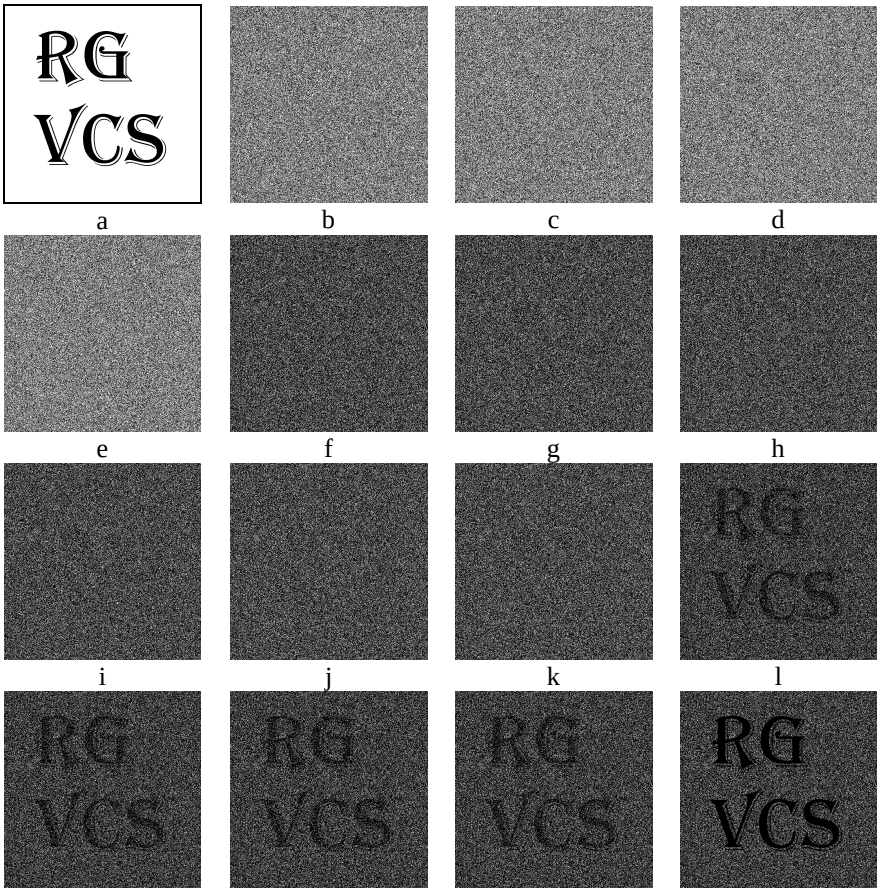

Fig. 2. Experimental results of the proposed scheme for (3, 4) case. (a) The binary secret image, (b)-(e) three random grids: R_1, R_2, R_3, R_4, (f) $R_1 \otimes R_2$, (g) $R_1 \otimes R_3$, (h) $R_1 \otimes R_4$, (i) $R_2 \otimes R_3$, (j) $R_2 \otimes R_4$, (k) $R_3 \otimes R_4$, (l) $R_1 \otimes R_2 \otimes R_3$, (m) $R_1 \otimes R_2 \otimes R_4$, (n) $R_1 \otimes R_3 \otimes R_4$, (o) $R_2 \otimes R_3 \otimes R_4$, (p) $R_1 \otimes R_2 \otimes R_3 \otimes R_4$.

In the second experiment, for saving pages, we simply give one share image and depict the recovered results by stacking different number of share images. **Fig. 3(b)** shows that the single share image is randomness as expected. **Fig. 3(c-f)** show that the stacked results with any 3, 4, 5, 6 share images can reveal the secret image. Moreover, better visual performance can be obtained when more share images are stacked.

Based on the above results, we can get the following conclusions: (1) nobody can recognize the original secret information from any share image alone; (2) one can get none

information about the secret image by stacking any $t < k$ shares. (3) the secret information can be visually decoded by stacking any $t \geq k$ shares. (4) the progressive decoding property of the recovered secret can be gained by the proposed scheme, through which the user can get more details and clear information about the secret image by sharing his share with more other users.

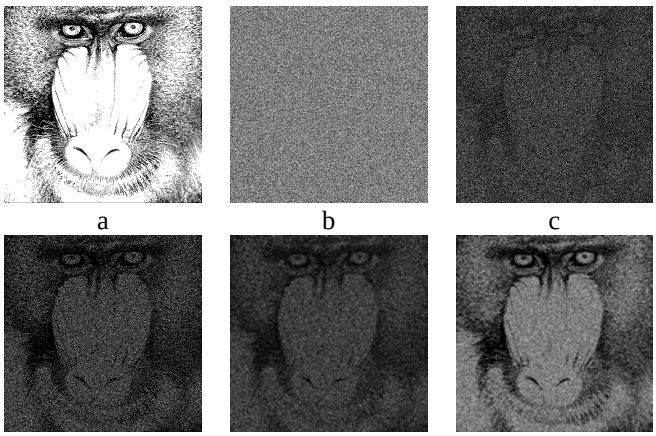

Fig. 3. Experimental results of the proposed scheme for (3, 6) case. (a) The binary secret image, (b) Single random grids R_1 (c) $R_1 \otimes R_2 \otimes R_3$, (d) $R_1 \otimes R_2 \otimes R_3 \otimes R_4$, (e) $R_1 \otimes R_2 \otimes R_3 \otimes R_4 \otimes R_5$, (f) $R_1 \otimes R_2 \otimes R_3 \otimes R_4 \otimes R_5 \otimes R_6$.

4.2 Comparisons and discussions

In this section, we mainly focus on our advantages in contrast improvement, and other common good features such as no codebook design and no pixel expansion are not discussed again here. Firstly, we give the visual quality comparisons of illustrations among ours and related schemes especially Chen and Tsao [22], Guo et al. [33], Wu and Sun [34]. Secondly, considering that the visual quality of the recovered images is evaluated by contrast in Definition 1, we further give the quantitative contrast comparisons. Note that only Chen and Tsao [22], Wu and Sun [34] and ours give the theoretical contrast while Guo et al. [33], Shyu [35] and Yan et al. [36] do not provide. And the contrasts in Guo et al. [33], Shyu [35] and Yan et al. [36] are obtained by experiments. Therefore, we give two types of contrast comparisons: the theoretical contrast and experimental contrast.

4.2.1 Visual quality illustration

The same binary secret image as shown in **Fig. 2(a)** is used to do the experiment for (2, 4) scheme, as depicted in **Fig. 4**, where *t* is the number of stacked shares. The first column (**Fig. 4**(a1, b1, c1)), the second column (**Fig. 4**(a2, b2, c2)), the third column (**Fig. 4**(a3, b3, c3)) and the last column (**Fig. 4**(a4, b4, c4)) are the recovered secret images using Chen and Tsao [22], Guo et al. [33], Wu and Sun [34] and our scheme, respectively.

The visual quality of Chen and Tsao [22] and Guo et al. [33] are so poor for both $t = 2,3,4$ since the backgrounds (corresponding to the white region in the original secret image) in the restored images contain too many black pixels which look so dark. Compared with the former two schemes, Wu and Sun [34] and ours achieve better visual performance since the background is reconstructed with more while pixels so that the secret pattern can be easily recognized. In a further step, the recovered image (**Fig. 4**(a4, b4)) by stacking $t = 2,3$ shares

in our method is clearer than that (**Fig. 4**(a3, b3)) in Wu and Sun's scheme [34]. Overall, our scheme gains the highest visual quality.

Based on the above comparisons, we can get the following discussions: (1) the visual quality of recovered secret images in Chen and Tsao [22] and Guo et al. [33] are low although within an acceptable level, due to the so many black pixels in their reconstructed secret image. (2) Wu and Sun [34] and ours both enhance the visual quality. Besides, our scheme gains the best visual quality.

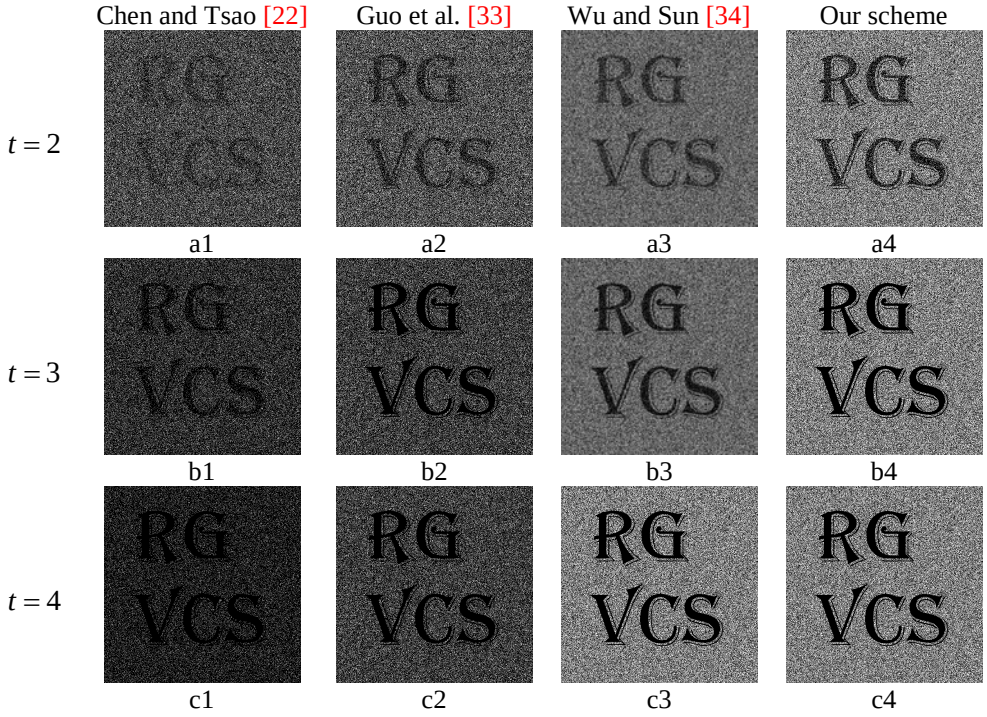

Fig. 4. Experimental result comparisons among ours and other related schemes for (2, 4) case

4.2.2 Theoretical contrast

Theoretical contrast of the recovered secret images for different access structures with (*k*, *n*) ($2 \le n \le 5, 2 \le k \le t \le n$) in our scheme can be calculated by the formula of contrast in Theorem 1. We first show how to calculate our theoretical contrast, taking the (3, 5) ($k=3, n=3$) case as the example, when decoding, the 5 empty share pixels r_1, r_2, r_3, r_4, r_5 are divided into 3 groups $G_1 = \{r_1, r_4\}$, $G_2 = \{r_2, r_5\}$, $G_3 = \{r_3\}$, where $r_1 = r_4$ and $r_2 = r_5$. For calculating $Prob_w$ with $w=2$, $t=3$, the result is equal to the probability of selecting *t* pixels from any *w* groups. Notice that all the possible combinations of selected pixels are $\{r_3, r_1, r_4\}$, $\{r_3, r_2, r_5\}$, $\{r_1, r_2, r_5\}$, $\{r_4, r_2, r_5\}$, $\{r_2, r_1, r_4\}$ and $\{r_5, r_1, r_4\}$, the total number is 6. Besides, the number of all possible combinations containing 3 pixels is $C_5^3 = 10$. Therefore, the value of $Prob_{w=2}$ is $6/10 = 3/5$. Using the same way, we can further calculate $Prob_{w=3} = 2/5$. We list all the results of $Prob_w$ for different (*k*, *n*) cases in **Table 1**. For (3, 5) scheme with stacking 3 shares, using the formula of contrast in Theorem 1, we can obtain its theoretical contrast $a = \left((2/5)\times(1/2)^2\right) \Big/ \left(1+(3/5)\times(1/2)^2\right) = 2/23$.

Table 1. The probability $Prob_w$ in theoretical contrast of the proposed scheme for different (k, n) cases

		$w=1$	$w=2$	$w=3$	$w=4$	$w=5$
(2, 2)	$t=2$		1			
(2, 3)	$t=2$	1/3	2/3			
	$t=3$		1			
(2, 4)	$t=2$	1/3	2/3			
	$t=3$		1			
	$t=4$		1			
(2, 5)	$t=2$	2/5	3/5			
	$t=3$	1/10	9/10			
	$t=4$		1			
	$t=5$		1			
(3, 3)	$t=3$			1		
(3, 4)	$t=3$		1/2	1/2		
	$t=4$			1		
(3, 5)	$t=3$		3/5	2/5		
	$t=4$		1/5	4/5		
	$t=5$			1		
(4, 4)	$t=4$				1	
(4, 5)	$t=4$			3/5	2/5	
	$t=5$				1	
(5, 5)	$t=5$					1

Comparisons of theoretical contrast for different (k, n) cases among the proposed scheme, Chen and Tsao [22] and Wu and Sun [34] are organized in **Table 2**. The results in our scheme with enhancement are marked using bold. Note that the contrast of our scheme is similar as or higher than other related schemes in total. To be noticed, some more conclusions can be obtained as follows.

(1) For the case (n, n) with $t=n$, the contrast of our method is $1/2^{n-1}$, which is the same as that by Chen at Tsao [22] and Wu and Sun [34]. Since the last $n-k$ bits do not exist, the schemes in Chen and Tsao [22] and Wu and Sun [34] are reduced to our method.

(2) For the case (n-1, n) with $t=n-1,\ n$, the contrasts in Wu and Sun [34] are the same as that in ours and greater than the contrasts in Chen and Tsao [22]. Since in Chen and Tsao's scheme [22], the first k bits are generated using (k, k)-VCS and the last bit is randomly generated. If the user wants to collect $r_1, r_2, \cdots, r_k$, he has to obtain the first k bits exactly. However, in Wu and Sun [34] and ours, the last bit $r_n = r_k = r_{n-1}$, so the user can gain through another approach by collecting the first k-1 bits and the last bit. In other words, the probability for the user to collect the full bits is improved. Besides, the scheme of Wu and Sun [34] is reduced to our scheme herein.

(3) For the cases (k, n) ($k < n-1$) with $k \le t < n$, the contrasts of our scheme are higher than both that of Chen and Tsao [22] and Wu and Sun [34]. For example, for the cases (2, 5) with $t=2$, 3, 4, the contrasts by our scheme are 3/4, 3/7, 1/2, which are higher than 2/49, 2/29, 3/41 and 2/13, 6/23, 4/11 by Chen and Tsao [22] and Wu and Sun [34], respectively. The same conclusion also holds for the case (3, 5) with $t=3$, 4, the contrasts achieved by ours are 2/23, 4/21, which are great than 1/44, 4/83 and 1/16, 3/22 gained by Chen and Tsao [22] and Wu and Sun [34], respectively. Since the user in our scheme can obtain full bits by

selecting $r_1, r_2, \cdots, r_k$ from the corresponding groups $G_1, G_2, \cdots, G_k$ respectively. However, the user in Wu and Sun [34] should exactly select the first *k*-1 bits and pick up the last bit from any one of the last *n*-*k* bits, So we achieve the enhanced probability.

Table 2. Comparisons of theoretical contrast among Chen and Tsao [22], Wu and Sun [34] and our scheme

(*k*, *n*)	Chen and Tsao [22]				Wu and Sun [34]				Our scheme			
	t=2	*t*=3	*t*=4	*t*=5	*t*=2	*t*=3	*t*=4	*t*=5	*t*=2	*t*=3	*t*=4	*t*=5
(2, 2)	1/2				1/2				1/2			
(2, 3)	1/7	1/4			2/7	1/2			2/7	1/2		
(2, 4)	2/29	2/17	1/8		1/5	1/3	1/2		**2/7**	**1/2**	1/2	
(2, 5)	2/49	2/29	3/41	1/16	2/13	6/23	4/11	1/2	**1/4**	**3/7**	**1/2**	1/2
(3, 3)		1/4				1/4				1/4		
(3, 4)		2/35	1/8			1/9	1/4			1/9	1/4	
(3, 5)		1/44	4/83	1/16		1/16	3/22	1/4		**2/23**	**4/21**	1/4
(4, 4)			1/8				1/8				1/8	
(4, 5)			2/43	1/16			2/43	1/8			2/43	1/8
(5, 5)				1/16				1/16				1/16

4.2.3 Experimental contrast

Since Shyu [35], Yan [36] and Guo et al. [33] fail to give a unified formula of contrast. Their contrasts are calculated based on the experimental statistics with Definition 1. To verify the theoretical contrast by our scheme and present our advantages, we also calculate the experimental average contrast of ours, and compare them with Shyu [35], Yan et al. [36] and Guo et al. [33], as organized in **Table 3**. Some conclusions can be obtained as follows:

(1) For the proposed scheme, note that the experimental results are approximately the same as the theoretical results in our scheme, such as the theoretical value 0.2500 for case (2, 5) with $t = 2$ in **Table 3**, which is approximate equal to the experimental value 0.2506 in **Table 2**. The results also hold for other cases, which verify the accuracy of the proposed general formula of theoretical contrast.

(2) In comparison with Shyu [35], Yan et al. [36] and Guo et al. [33], it is easy to observe that the contrast of ours is similar as or overall greater than others. Compared with Guo et al. [33], we get a higher contrast for each case. The experimental contrasts of Shyu [35] and Yan et al. [36] can be computed by the proposed general formula of contrast. Although the results are approximately the same, we achieve a higher accuracy due to our theoretical values while their results are approximate values. As shown by the example in subsection 4.2.2, the formula of contrast is calculated by exploring the $Prob_w$, which is equal to the probability of selecting t pixels $r_{i_1}, r_{i_2}, \cdots, r_{i_t}$ from any w different groups of $G_1 = \{r_1, r_{k+1}, \cdots, r_{(\lceil n/k \rceil - 1)k+1}\}$, $G_2 = \{r_2, r_{k+1}, \cdots, r_{(\lceil n/k \rceil - 1)k+2}\}$, $\cdots$, $G_k = \{r_k, r_{2k}, r_{(\lceil n/k \rceil - 1)k}\}$. In total, the proposed scheme in this paper achieves the general, precise and improved contrast.

Table 3. Comparisons of experimental contrast among Shyu [35], Yan et al. [36], Guo et al. [33] and ours

(k, n)	Shyu [35]				Yan et al. [36]			
	t=2	t=3	t=4	t=5	t=2	t=3	t=4	t=5
(2, 2)	0.4987				0.4992			
(2, 3)	0.2887	0.4992			0.2840	0.5008		
(2, 4)	0.2864	0.5005	0.4989		0.2848	0.4996	0.4991	
(2, 5)	0.2505	0.4286	0.5004	0.5004	0.2498	0.4290	0.5004	0.5004
(3, 3)		0.2508				0.2496		
(3, 4)		0.1118	0.2483			0.1107	0.2499	
(3, 5)		0.0863	0.1909	0.2490		0.0875	0.1903	0.2505
(4, 4)			0.1241				0.1248	
(4, 5)			0.0469	0.1255			0.0458	0.1249
(5, 5)				0.0623				0.0631
	Guo et al. [33]				Our scheme			
	t=2	t=3	t=4	t=5	t=2	t=3	t=4	t=5
(2, 2)	0.4990				0.5011			
(2, 3)	0.1428	0.2505			0.2852	0.5004		
(2, 4)	0.1417	0.2503	0.2503		0.2846	0.5005	0.5005	
(2, 5)	0.0820	0.1433	0.1499	0.1249	0.2506	0.4290	0.5004	0.5004
(3, 3)		0.2492				0.2496		
(3, 4)		0.0559	0.1248			0.1094	0.2501	
(3, 5)		0.0223	0.0485	0.0627		0.0908	0.1912	0.2504
(4, 4)			0.1253				0.1254	
(4, 5)			0.0461	0.0626			0.0464	0.1248
(5, 5)				0.0624				0.0626

5. Conclusion

In this paper, we develop an algorithm to further improve the contrast of (k, n) RG-based VCS and give the general formula of contrast with higher accuracy. Actually, our algorithm and previous algorithms are all constructed on the basis of (k, k) RG-based VCS and the only difference is how to generate the last $n-k$ pixels, leading to the different amount of (k, k) RG-based VCS in different algorithms: 1 in Chen and Tsao [22], $\left\lfloor \frac{n}{k} \right\rfloor$ in Guo et al. [33], $n-k+1$ in Wu and Sun [34]. $\left(\left\lceil \frac{n}{k} \right\rceil \right)^{(n-1) \bmod k+1} \times \left(\left\lfloor \frac{n}{k} \right\rfloor \right)^{k-((n-1) \bmod k+1)}$ in our algorithm. Then we explore the probability that the user can collect the first k pixels denoted as $Prob_w$ by calculating the amount of (k, k) RG-based VCS the user can gain, which helps to give the final general formula of contrast. The relationship between contrast and the amount of (k, k) RG-based VCS, which is not yet discussed formally, deserves further investigation and it is undoubtedly innovative.

Acknowledgment

We would like to thank the anonymous reviewers for their important and helpful comments. This work was supported by the Natural Science Foundation of China (61602513), the National High Technology Research and Development Program of China (2015AA016006), the National Key Research and Development Program of China (2016YFF0204003), the Equipment Pre-research Foundation during the 13th Five-Year Plan (61400020201), the CCF-Venus "Hongyan" research plan (2017003) and the Key Lab of Information Network Security, Ministry of Public Security (C15604).

References

[1] M. Naor and A. Shamir, "Visual cryptography," in *Proc. of Workshop on the Theory and Application of of Cryptographic Techniques*. vol.950, pp.1-12, 1994. Article (CrossRef Link).
[2] O. Kafri and E. Keren, "Encryption of pictures and shapes by random grids," *Optics Letters*, vol.12, no.6, pp.377-379, 1987. Article (CrossRef Link).
[3] G. Ateniese, C. Blundo, A. De Santis, and D. Stinson, "Visual cryptography for general access structures," *Information and Computation*, vol.129, no.2, pp.86-106, 1996. Article (CrossRef Link).
[4] G. Shen, F. Liu, Z. Fu, and B. Yu, "New insight into linear algebraic technique to construct visual cryptography scheme for general access structure," *Multimedia Tools and Applications*, vol.72, no.16, pp.14511-14533, 2017. Article (CrossRef Link).
[5] Z. Fu and B. Yu, "Optimal pixel expansion of deterministic visual cryptography scheme," *Multimedia Tools and Applications*, vol.73, no.3, pp.1177-1193, 2014. Article (CrossRef Link).
[6] S. Shyu, and M. Chen, "Optimum pixel expansions for threshold visual secret sharing schemes," *IEEE Transactions on Information Forensics and Security*, vol.6, no.3, pp.960-969, 2011. Article (CrossRef Link).
[7] G. Shen, F. Liu, Z. Fu, and B. Yu, "Perfect contrast XOR-based visual cryptography schemes via linear algebra," *Designs Codes and Cryptography*, vol.85, no.1, pp.15-37, 2017. Article (CrossRef Link).
[8] A. De Bonis and A. De Santis, "Randomness in secret sharing and visual cryptography schemes," *Theoretical Computer Science*, vol.314, no.3, pp.351-374, 2004. Article (CrossRef Link).
[9] Y. C. Chen, "Fully incrementing visual cryptography from a succinct non-monotonic structure," *IEEE Transactions on Information Forensics and Security*, vol.12, no.5, pp.1082-1091, 2017. Article (CrossRef Link).
[10] X. Yan, S. Wang, X. Niu, and C. N. Yang, "Halftone visual cryptography with minimum auxiliary black pixels and uniform image quality," *Digital Signal Processing*, vol.38, no.C, pp.53-65, 2015. Article (CrossRef Link).
[11] Y. Ren, F. Liu, T. Guo, R. Feng, and D. Lin, "Cheating prevention visual cryptography scheme using Latin square," *IET Information Security*, vol.11, no.4, pp.211-219, 2017. Article (CrossRef Link).
[12] F. Liu, C. Wu, and X. Lin, "Cheating immune visual cryptography scheme," *IET Information Security*, vol.5, no.1, pp.51-59, 2011. Article (CrossRef Link).
[13] Z. Wang, G. Arce, and G. Di Crescenzo, "Halftone visual cryptography via error diffusion," *IEEE Transactions on Information Forensics and Security*, vol.4, no.3, pp.383-396, 2009. Article (CrossRef Link).
[14] S. Shivendra and A. Suneeta, "Progressive Visual Cryptography with Unexpanded Meaningful Shares," *ACM Transactions on Multimedia Computing, Communications, and Applications*, vol.12, no.4, pp.1-24, 2016. Article (CrossRef Link).
[15] C. Yang, H. Shih, C. Wu, and L. Harn, "*k* out of *n* region incrementing scheme in visual cryptography," *IEEE Transactions on Circuits and Systems for Video Technology*, vol.22, no.5, pp.799-810, 2012. Article (CrossRef Link).

[16]G. Wang, W. Yan, and M. Kankanhalli, "Content based authentication of visual cryptography," *Multimedia Tools and Applications*, vol.76, no.7, pp.9427-9441, 2017. Article (CrossRef Link).
[17]C. Yang, "New visual secret sharing schemes using probabilistic method," *Pattern Recognition Letters*, vol.25, no.4, pp. 481-494, 2014. Article (CrossRef Link).
[18]S. Cimato, A. R. Prisco, and D. Santis, "Probabilistic visual cryptography schemes," *The Computer Journal*, vol.49, no.1 pp.97-107, 2006. Article (CrossRef Link).
[19]S. Shyu, "Image encryption by random grids," *Pattern Recognition*, vol.40, no.3, pp.1014-1031, 2007. Article (CrossRef Link).
[20]S. Shyu, "Image encryption by multiple random grids," *Pattern Recognition*, vol.42, no.7, pp.1582-1596, 2009. Article (CrossRef Link).
[21]T. Chen and K. Tsao, "Visual secret sharing by random grids revisited," *Pattern Recognition*, vol.42, no.9, pp.2203-2217, 2009. Article (CrossRef Link).
[22]T. Chen and K. Tsao, "Threshold visual secret sharing by random grids," *Journal of Systems and Software*, vol.84, no.7, pp.1197-1208, 2011. Article (CrossRef Link).
[23]X. Wu and W. Sun, "Random grid-based visual secret sharing for general access structures with cheat-preventing ability," *Journal of Systems and Software*, vol.85, no.5 pp.1119-1134, 2011. Article (CrossRef Link).
[24]X. Wu and W. Sun, "Visual secret sharing for general access structures by random grids," *IET Information Security*, vol.6, no.4, pp.299-309, 2012. Article (CrossRef Link).
[25]S. Shyu, "Visual cryptograms of random grids for general access structures," *IEEE Transactions on Circuits and Systems for Video Technology*, vol.23, no.3, pp.414-424, 2013. Article (CrossRef Link).
[26]X. Wu and W. Sun, "Random grid-based visual secret sharing with abilities of OR and XOR decryptions," *Journal of Visual Communication and Image Representation*, vol.24, no.1, pp.48-62, 2013. Article (CrossRef Link).
[27]T. Chen and K. Tsao, "User-friendly random-grid-based visual secret sharing," *IEEE Transactions on Circuits and Systems for Video Technology*, vol.21, no.11, pp.1693-1703, 2011. Article (CrossRef Link).
[28]X. Yan, Y. Lu, H. Huang, L. Liu, and S. Wan, "Quality-adaptive threshold visual secret sharing by random grids," in *Proc. of IEEE International Conference on Signal and Image Processing*, pp. 323-327, 2017. Article (CrossRef Link).
[29]X. Yan and Y. Lu, "Participants increasing for threshold random grids-based visual secret sharing," *Journal of Real-Time Image Processing*, vol. 14, no.1, pp.13-24, 2018. Article (CrossRef Link).
[30]H. C. Chao and T. Y. Fan, "Random-grid based progressive visual secret sharing scheme with adaptive priority," *Digital Signal Processing*, vol.68, pp.69-80, 2017. Article (CrossRef Link).
[31]Z. Fu and B. Yu, "Visual cryptography and random grids schemes," in *Proc. of 12th International Workshop on Digital-Forensics and Watermarking*, pp.109-122, 2013. Article (CrossRef Link).
[32]C. N. Yang, C. C. Wu, and D. S. Wang, "A discussion on the relationship between probabilistic visual cryptography and random grid," *Information Sciences*, vol.278, no.10, pp.141-173, 2014. Article (CrossRef Link).
[33]T. Guo, F. Liu, and C. Wu, "Threshold visual secret sharing by random grids with improved contrast," *Journal of Systems and Software*, vol.86, no.8, pp.2094-2109, 2013. Article (CrossRef Link).
[34]X. Wu and W. Sun, "Improving the visual quality of random grid-based visual secret sharing," *Signal Processing*, vol.93, no.5, pp.977-995, 2013. Article (CrossRef Link).
[35]S. Shyu, "Visual cryptograms of random grids for threshold access structures," *Theoretical Computer Science*, vol.565, pp.30-49, 2015. Article (CrossRef Link).
[36]X. Yan, X. Liu, and C. N. Yang, "An enhanced threshold visual secret sharing based on random grids," *Journal of Real-Time Image Processing*, pp.1-13, 2015. Article (CrossRef Link).

Hao Hu received his B.S. degree and M.S. degree in the Zhengzhou Information Science and Technology Institute in 2012 and 2015, respectively. He is currently pursuing the Ph.D. degree in information and communication engineering with the China National Digital Switching System Engineering & Technological Research Center. His main research interests include security risk evaluation and secret image sharing.
From 2012 to 2017, he has authored some journal papers indexed by SCI or EI, such as the Security and Communication Networks, Multimedia Tools and Applications, etc.

Gang Shen received his M.S. degree and Ph.D. degree in the Zhengzhou Information Science and Technology Institute in 2013 and 2017, respectively. He was a visiting scholar in the State Key Laboratory of Information Security of Chinese Academy of Science. His main research interests include network security and visual cryptograph.
From 2010 to 2017, he has authored over 10 papers in various conferences indexed by EI and journals indexed by SCI or EI such as Designs, Codes and Cryptography, Multimedia Tools and Applications, etc.

Zhengxin Fu received his M.S. degree and Ph.D. degree in the Zhengzhou Information Science and Technology Institute in 2010 and 2014, respectively. His research interests are visual secret sharing and information security.
Since 2014, he has been a Lecturer with the Department of Computer Science and Information Engineering at Zhengzhou Information Science and Technology Institute, China. He is a Peer Reviewer of the Chinese Journal of Electronics.

Bin Yu received his B.S. degree in Department 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 2002.12 to 2003.12, he worked as vice professor at 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 cryptography and network security.
Mr. Yu published books in Chinese, such as the System Engineering Theory in 2009, and the Visual Cryptograph in 2014. He is the Editor of the Foreign Electronic Measurement Technology.