Multimedia Tools and Applications (2019) 78:10157–10180
https://doi.org/10.1007/s11042-018-6478-3

On the security of threshold random grid-based visual secret sharing

Bing-Jian Wang[1] · Tzer-Shyong Chen[2] · Fuh-Gwo Jeng[3] · Tzung-Her Chen[1]

Received: 5 January 2018 / Revised: 17 May 2018 / Accepted: 26 July 2018 /
Published online: 3 September 2018

Abstract
Visual secret sharing (VSS) technology encodes a secret image into some share images for sharing some classified information. Only when the participants gather and stack their share pictures the secret image would be reconstructed and recognizable by the human visual system. Two well-known encoding ways of VSS, visual cryptography (VC) and random grid (RG), have been developed in recent years. As both VC and RG have been considered as a secure way for communicating with high security, they have been pointed out with cheating problems. In this paper, we propose two RG-based VSS schemes with fraud prevention for the cases of (2,*n*) and (*k*,*n*). The experimental results and the analysis of security and contrast show that the proposed method is efficient and practical.

Keywords Visual secret sharing · Visual cryptography · Random grid · Cheating prevention

1 Introduction

For secure communication, visual secret sharing (VSS) turns a secret image into some meaningless share images in visual, only if stacking enough number of share images the secret image would be revealed in visual. Except for secure communication, VSS can also be applied in visual authentication [17, 18], image hiding [2, 8] or digital watermarking [11, 24, 25] and so on.

In VSS scheme, the encoding way is mainly classified into visual-cryptography-based (VC-based) and random-grid-based (RG-based). The features of VC-based VSS scheme can be summarized in two. 1) For each case of *k*-out-of-*n* (noted by (*k*,*n*)), it needs a tailor-made

✉ Tzung-Her Chen
thchen@mail.ncyu.edu.tw

1 Department of Computer Science and Information Engineering, National Chiayi University, Chiayi City, Taiwan 60004, Republic Of China

2 Department of Information Management, Tunghai University, Taichung City, Taiwan 40704, Republic Of China

3 Department of Applied Mathematics, National Chiayi University, Chiayi City, Taiwan 60004, Republic Of China

codebook for encoding. 2) The size of generated share images and the reconstructed secret image is larger than the original secret image, that is, pixel expansion. The first threshold VC-based VSS was defined and proposed by Naor and Shamir [19] in 1995. After that, more improved threshold VC-based VSS schemes with different thresholds and codebook designs have been proposed [1, 6, 12].

Comparing with VC-based VSS, the feature of RG-based VSS is also considered in two. 1) It only needs to design an encoding algorithm, and the algorithm can be applied in each (k,n). 2) The size of share images and the reconstructed secret image keeps the same as the original secret image, that is, no pixel expansion. The first threshold RG-based VSS was proposed by Kafri and Keren [13]. Although RG-based VSS is still in its infancy, many schemes have also been proposed [3–5, 7, 15, 16, 21] in the past decade.

Taking the security of VC-based VSS into account, Horng et al. [9] pioneered in claiming the (k,n) VC-based VSS suffering from the cheating of malicious participants intending to mislead honest participants by generating a share to cheat honest members to accept the wrongly revealed secret information. Furthermore, the first scheme [9] is presented to prevent VSS from cheating by the designed that every participant has one extra share image to authenticate the validity of the generic share of the other participants. The second scheme adopted a $(2,n + l)$ VC-based VSS scheme in which $n + l$ shares are generated but only deliver n share images to n participants while l shares are discarded. Since the fraud problem was found, a series of cheating prevention schemes [10, 20, 22, 23] have been designed. Tsai et al. [22] proposed another cheating-prevention scheme using the computation-expensive. Hu and Tzeng [10] proposed three kinds of cheating and a preventive scheme.

Nevertheless, unfortunately, threshold RG-based VSS has also pointed out that it suffers from cheating problem [14, 26]. In the case of $(2,n)$ (or (k,n)) RG-based VSS [4], at least 2 (or k) malicious participants can reconstruct secret information before the rest associates know the secret information. The malicious participants then can generate artificial share images with a cheating message and send to the rest participants. After stacking with the artificial share images, the rest participants will reconstruct the cheating message without awareness.

Lee and Chen [14] pointed out that the collusion attack did work in $(2,n)$ and (k,n) RG-based VSS [4]. In $(2,n)$ RG-based VSS, the area in the reconstructed secret image corresponding to the white secret pixels can be maliciously operated by cheaters turning white to black; furthermore, in (k,n) RG-based VSS, cheaters can choose a cheating image freely.

Hence, in this paper, we propose two threshold RG-based VSS schemes with cheating prevention for cases $(2,n)$ and (k,n). We add an authentication image into the algorithm and let each two share images be able to perform the authentication process. The fake share images will be detected by the authentication process.

The rest of this paper is organized as follows. The next section briefly reviews the cheating problem in threshold RG-based VSS [14]. The proposed $(2,n)$ scheme, its experimental results, and performance analysis are illustrated in Section 3, and the proposed (k,n) scheme is described in Section 4. Finally, the further discussion and the conclusion are shown in Section 5 and 6.

2 The cheating problem

Lee and Chen [14] pointed out that the cheating attacks in threshold RG-based VSS were possible and demonstrated how to work in $(2,n)$ and (k,n) cases. The reviewing is as follows.

2.1 The cheating problem in (2,n) RG-based VSS

In the cheating process, supposing that two malicious participants (cheaters) intend to cheat the other participants, they stack the random-grids which they have to confirm the secret information previously. With the known secret information, the cheaters can modify the secret information and make a cheating image. Forwardly, the cheaters generate a fake random-grid with their grids and the cheating image by the cheating process.

In the encoding algorithm of (2,n) scheme, when secret pixel is white, the same positions in each random grid have the same pixel values no matter white or black. When the secret pixel is black, the same positions of each random grid are randomly determined separately. Therefore, based on their own random grid, the cheater let a part of the pixel values which are known as a white area of the secret image be random, that is, the cheater is able to modify the secret information. The modified random grid is regarded as the fake grid. When stacking with the fake grid, the rest participants will see the modified information. The concept of cheating attacks in (2,n) scheme is shown in Fig. 1.

2.2 The cheating problem in (k,n) RG-based VSS

At least k malicious participants reconstruct the secret image previously and try to generate an evaluated grid. The pixels in the evaluated grid have a high probability that similar with the rest members. Then, the malicious participants perform (k,n) VSS scheme with a picked

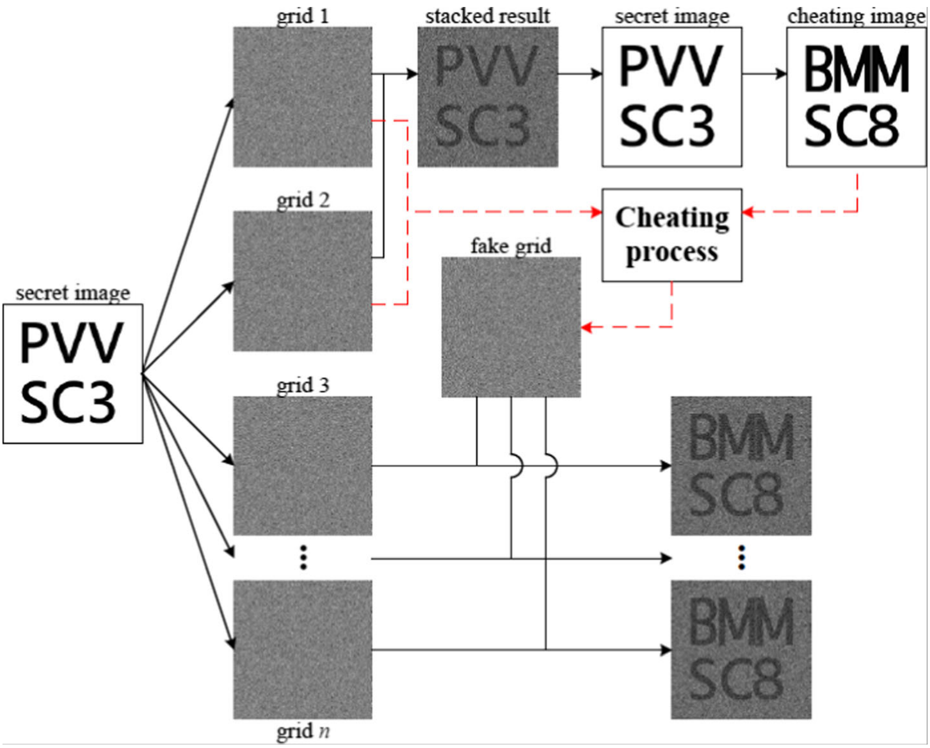


Fig. 1 The concept of cheating attacks in (2,n) scheme

cheating image and the evaluated grid to generated k-1 fake grids. When the rest participants stack with the k-1 fake grids, they will reconstruct the cheating image in visual. The concept of cheating attacks in (k,n) scheme is shown in Fig. 2.

3 The proposed (2,n) VSS scheme with cheating prevention

In this section, the proposed (2,n) RG-based VSS scheme with cheating prevention is described as follows, and the experimental results and performance analysis are shown after it.

3.1 The proposed scheme

The main design aims at that two generated share images can be superimposed to disclose the secret image and simultaneously one share and the other rotated share can be superimposed to appear the authentication message. In such a way, the cheating-prevention VSS scheme does work. The proposed scheme is mainly disported to two phases: (2,2) generation and (2,n) generation.

In the first phase, input a secret image $S = \{S[i,j] | S[i,j] \in \{0, 1\}, 0 \leq i \leq (w-1), 0 \leq j \leq (h-1)\}$ ("0" presents the white pixel, and "1" the black one.) and an authentication image

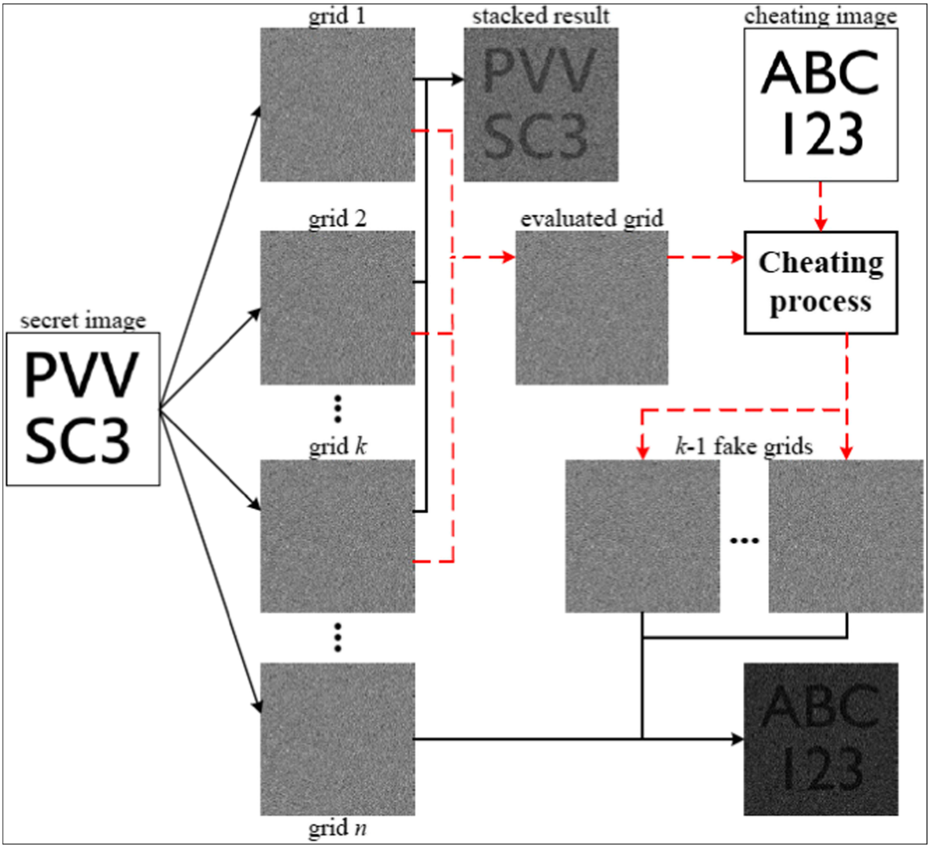


Fig. 2 The concept of cheating attacks in (k,n) scheme

$A = \{A[i,j] | A[i,j] \in \{0, 1\}, 0 \le i \le (w-1), 0 \le j \le (h-1)\}$ with RG-based VSS scheme to generate two random-grids P_1 and P_2 ($P_{1(\mathrm{or}\,2)} = \{P_{1(\mathrm{or}\,2)}[i,j] | P_{1(\mathrm{or}\,2)}[i,j] \in \{0, 1\}, 0 \le i \le (w-1), 0 \le j \le (h-1)\}$).When stacking P_1 and P_2, the secret image S will be reconstructed. When stacking P_1 and RP_2 (90 degrees rotated P_2), the authentication image A will be reconstructed.

In the second phase, distribute the pixels of P_1 and P_2 into n random-grids, $G_m = \{G_m[i,j] | G_m[i,j] \in \{0, 1\}, 0 \le i \le (w-1), 0 \le j \le (h-1)\}$, where $m = 1, 2, \ldots, n$. Then, the n random-grids are the final output. Stacking each two of these random-grids can reconstruct the secret image S. Furthermore, rotating one of them by 90 degrees and stacking can reconstruct the authentication image A.

3.1.1 Phase 1: Generate (2,2) random-grids P_1 and P_2

(From **Step 1.1** to **1.8**, see Fig. 3.)

Step 1.1: Randomly choose $P_1[i,j] \in \{0, 1\}$. ("0" presents the white pixel, and "1" the black one.)
Step 1.2: Determine $P_2[h-j, i]$ by referring $P_1[i,j]$ and $A[i,j]$ as $P_2[h-j,i] = \{ P_1[i,j]$ if $A[i,j] = 0$ $(P_1[i,j] + 1)$ mod2 if $A[i,j] = 1$.
Step 1.3: Determine $P_1[h-j, i]$ by referring $P_2[h-j, i]$ and $S[h-j, i]$ as $P_1[h-j,i] = \{ P_2[h-j,i]$ if $S[h-j,i] = 0$ $(P_2[h-j,i] + 1)$ mod2 if $S[h-j,i] = 1$.
Step 1.4: Determine $P_2[w-i, h-j]$ by referring $P_1[h-j, i]$ and $A[h-j, i]$ as $P_2[w-i,h-j] = \{ P_1[h-j,i]$ if $A[h-j,i] = 0$ $(P_1[h-j,i] + 1)$ mod2 if $A[h-j,i] = 1$.
Step 1.5: Randomly choose $P_1[w-i, h-j] \in \{0, 1\}$.
Step 1.6: Determine $P_2[j, h-i]$ by referring $P_1[w-i, h-j]$ and $A[w-i, h-j]$ as $P_2[j,h-i] = \{ P_1[w-i,h-j]$ if $A[w-i,h-j] = 0$ $(P_1[w-i,h-j] + 1)$ mod2 if $A[w-i,h-j] = 1$.
Step 1.7: Determine $P_1[j, h-i]$ by referring $P_2[j, h-i]$ and $S[j, h-i]$ as $P_1[j,h-i] = \{ P_2[j,h-i]$ if $S[j,h-i] = 0$ $(P_2[j,h-i] + 1)$ mod2 if $S[j,h-i] = 1$.
Step 1.8: Determine $P_2[i,j]$ by referring $P_1[j, h-i]$ and $A[j, h-i]$ as $P_2[i,j] = \{ P_1[j,h-i]$ if $A[j,h-i] = 0$ $(P_1[j,h-i] + 1)$ mod2 if $A[j,h-i] = 1$.

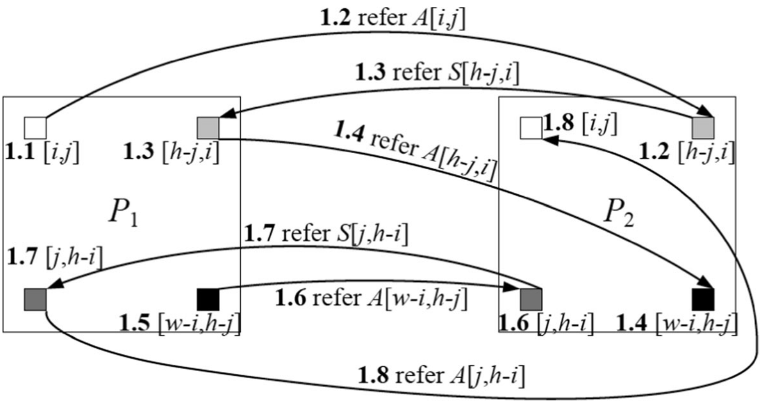


Fig. 3 Concept of **Step 1.1** to **1.8**

Step 1.9: Repeat **Step 1.1** to **1.8** until all pixels of P_1 and P_2 are determined, but notice that each circle from **Step 1.1**to **1.8** determines 4 pixel values in P_1 (and in P_2). Hence, P_1 can be derived into 4 blocks with same size.

When each circle starts from **Step 1.1**, the beginning position $P_1[i,j]$ can be randomly located in one of blocks I~VI, except the pixels which have been determined already.

3.1.2 Phase 2: Gererate (2,n) random-grids by distributing P_1 and P_2 into G_m, where m = 1,2,…,n

Step 2.1: For $G_m[i,j]$, randomly choose P_1 or P_2 and distribute its four pixel values at one time with positions (i,j), $(h-j, i)$, $(w-i, h-j)$ and $(j, h-i)$ into corresponding $G_m[i,j]$, $G_m[h-j, i]$, $G_m[w-i, h-j]$ and $G_m[j, h-i]$.

Step 2.2: For a grid G_m, where $0 \le i \le (w/2-1)$, $0 \le j \le (h/2-1)$, repeat **Step 2.1** until all pixel values of G_m are determined.

Step 2.3: Repeat **Step 2.1** and **2.2** until all random-grids G_m are generated, where $m = 1, 2, \ldots, n$.

The concept of **Phase 2** is shown in Fig. 4.

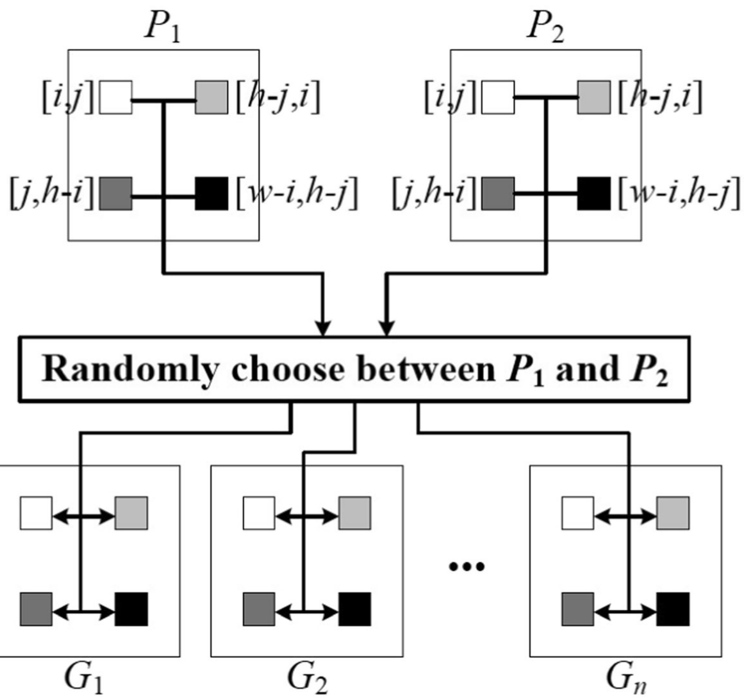


Fig. 4 Concept of **Phase 2**

The algorithm of the proposed encoding process is briefly illustrated as follows.

Input: A secret image $S=\{S[i,j]\,|\,S[i,j]\in\{0,1\},0\le i\le(w-1),0\le j\le(h-1)\}$, an authentication image $A=\{A[i,j]\,|\,A[i,j]\in\{0,1\},0\le i\le(w-1),0\le j\le(h-1)\}$.

Output: n random-grids $G_m=\{G_m[i,j]\,|\,G_m[i,j]\in\{0,1\},0\le i\le(w-1),0\le j\le(h-1)\}$ $(m=1,2,\ldots,n)$

//Phase 1: Generate random-grids P_1 and P_2

for $i=0$ **to** $w/2-1$

for $j=0$ **to** $h/2-1$

Except for the determined pixels, randomly choose a starting position (i,j) in blocks I~VI. //**Step 1.9**

Randomly determine $P_1[i,j]$ in $\{0,1\}$ //**Step 1.1**

$$P_2[h-j,i]=\begin{cases}P_1[i,j] & \text{if } A[i,j]=0\\(P_1[i,j]+1)\bmod 2 & \text{if } A[i,j]=1\end{cases}$$ //**Step 1.2**

$$P_1[h-j,i]=\begin{cases}P_2[h-j,i] & \text{if } S[h-j,i]=0\\(P_2[h-j,i]+1)\bmod 2 & \text{if } S[h-j,i]=1\end{cases}$$ //**Step 1.3**

$$P_2[w-i,h-j]=\begin{cases}P_1[h-j,i] & \text{if } A[h-j,i]=0\\(P_1[h-j,i]+1)\bmod 2 & \text{if } A[h-j,i]=1\end{cases}$$ //**Step 1.4**

Randomly determine $P_1[w-i,h-j]$ in $\{0,1\}$ //**Step 1.5**

$$P_2[j,h-i]=\begin{cases}P_1[w-i,h-j] & \text{if } A[w-i,h-j]=0\\(P_1[w-i,h-j]+1)\bmod 2 & \text{if } A[w-i,h-j]=1\end{cases}$$ //**Step 1.6**

$$P_1[j,h-i]=\begin{cases}P_2[j,h-i] & \text{if } S[j,h-i]=0\\(P_2[j,h-i]+1)\bmod 2 & \text{if } S[j,h-i]=1\end{cases}$$ //**Step 1.7**

$$P_2[i,j]=\begin{cases}P_1[j,h-i] & \text{if } A[j,h-i]=0\\(P_1[j,h-i]+1)\bmod 2 & \text{if } A[j,h-i]=1\end{cases}$$ //**Step 1.8**

//Phase 2: Distribute P_1 and P_2 into G_m, where m=1,2,…,n

for $m=1$ **to** n //**Step 2.3**

for $i=0$ **to** $w/2-1$

for $j=0$ **to** $h/2-1$ //**Step 2.2**

Randomly choose between P_1 and P_2 and set K is the chosen one (i.e. $K=P_1$ or $K=P_2$)

$G_m[i,j]=K[i,j]$

$G_m[h-j,i]=K[h-j,i]$

$G_m[w-i,h-j]=K[w-i,h-j]$

$G_m[j,h-i]=K[j,h-i]$ //**Step 2.1**

The decoding process directly stacks two or more random-grids to reconstruct the secret image detectable by the human visual system. Rotating one of them by 90 degrees and stacking will rebuild the authentication image.

3.2 Experimental results

To demonstrate that the proposed scheme achieves the collusion attack prevention and its feasibility, the experimental results are given in this section.

First, we choose images Fig. 5a as the secret image and Fig. 5b as the authentication image with both size 1024×1024. After performing the proposed encoding process with $n = 3$, we have three random-grids Fig. 5c, d and e.

3.2.1 Stacking results of (2,3) case

Then, the results of stacking each two random-grids are Fig. 5f, g and h. The authentication results are as Fig. 5i, j and k. Notice that RG_1, RG_2 and RG_3 stand for the 90 degrees rotated random-grids. Finally, Fig. 5l is the result of stacking all random-grids.

3.2.2 Stacking results of (2,3) case with cheating attacks

Next, we implement the collusion attacks of $(2,n)$ introduced in Ref. [14] on the proposed scheme. Supposing that the two participants, u_1 and u_2, have random-grids, G_1 and G_2, perform the collusion attacks to cheat the rest participant, u_3. Because, by stacking G_1 and G_2, u_1 and u_2 have already known the secret information, they modify the secret information as Fig. 6a and generate a fake image, FG, Fig. 6b, to cheat u_3. When u_3 receives FG and stacks with G_3, Fig. 6c, u_3 will recover the cheating information. However, if u_3 performs the authentication Fig. 6d, (s)he will see that the authenticating result is different from the authentication image Fig. 5b. Hence, u_3 can tell that FG is a fake grid.

3.3 Security analysis

To show the security and performance of the proposed schemes, the values of average light transmission and contrast are popularly used in VSS scheme. Hence, the definitions are given as follows.

- Definition 1. (Average light transmission)

For a binary image I with size $w \times h$, the light transmission of some pixel $I[i,j]$ is defined as $t[I[i,j]] = \{ 0 \text{ if } I[i,j] = 1 \;\; 1 \text{ if } I[i,j] = 0$ ($I[i,j] = 0$ stands for the white pixels of I, and the other is black). Furthermore, the average light transmission of I is defined as $T[B] = \frac{1}{w \times h} \sum_{i=0}^{w-1} \sum_{j=0}^{h-1} t[B[i,j]]$, that is, the ratio of white pixels in I.

- Definition 2. (Contrast)

The contrast of a binary image I on the secret image S is defined as $\alpha = \frac{T[I[S(0)]] - T[I[S(1)]]}{1 + T[I[S(1)]]}$ from [30]. $T[I[S(0)]]$ means the average light transmission of the area in I which is according to the

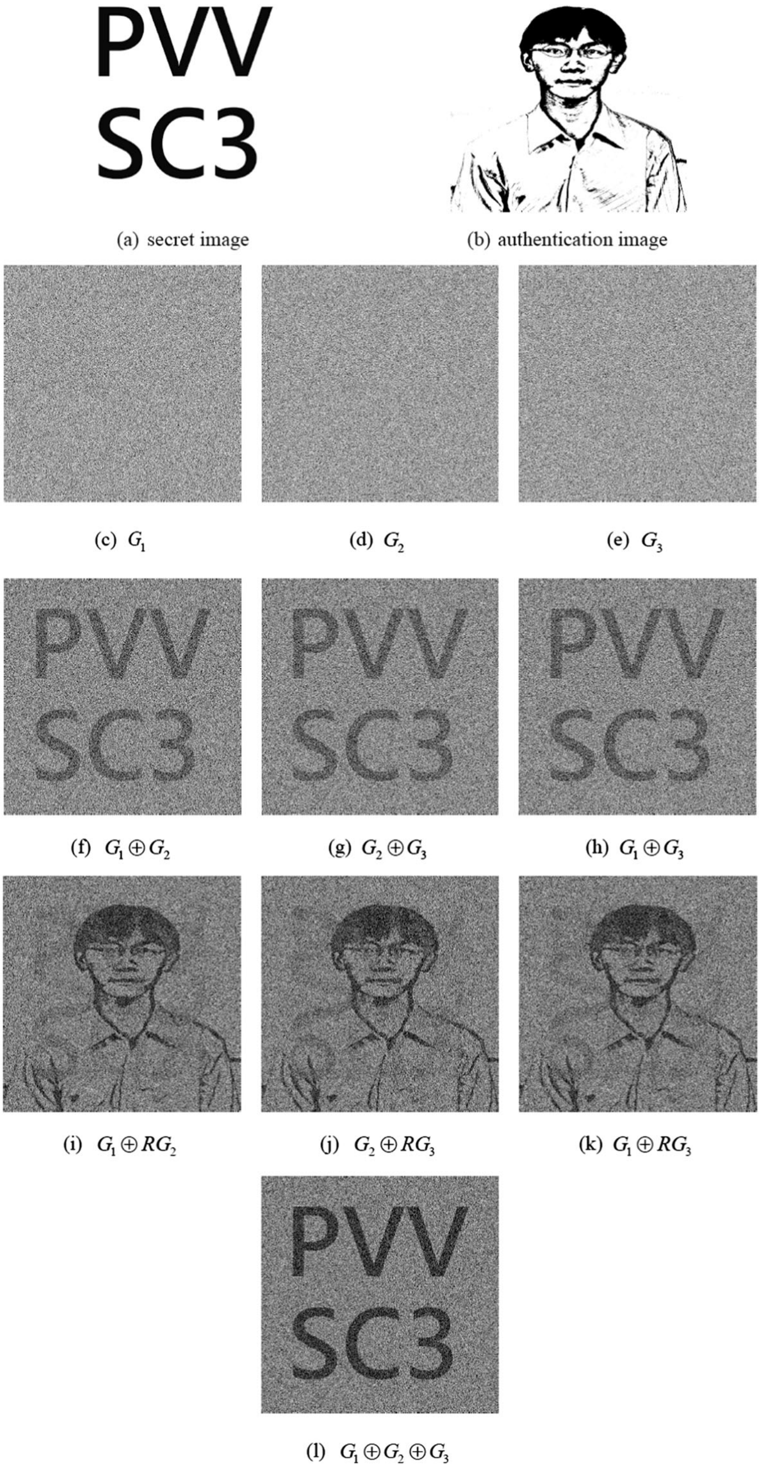


Fig. 5 The experimental results of the proposed scheme with $n = 3$

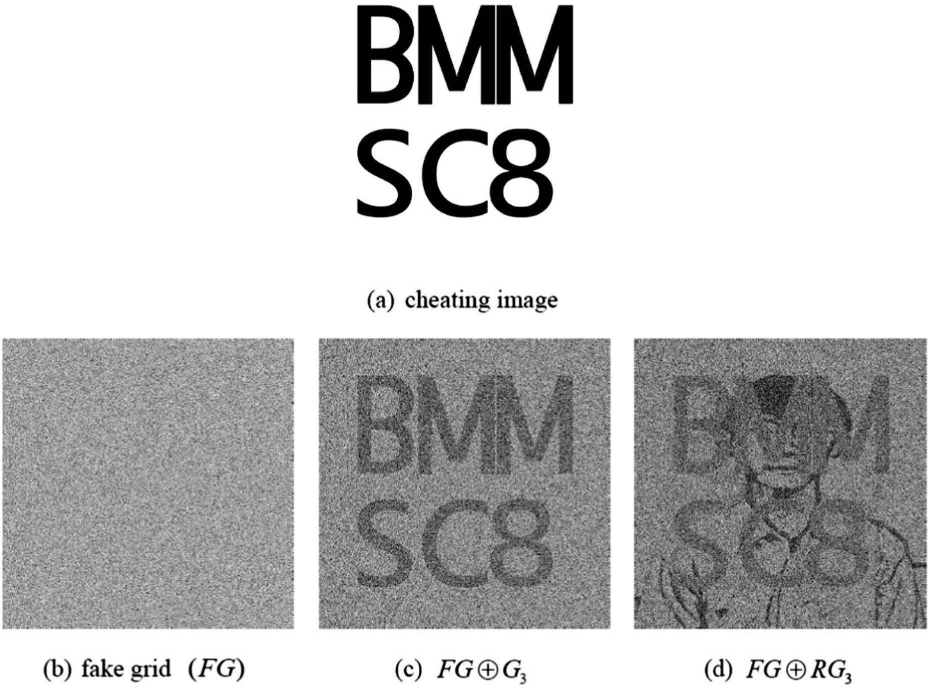


Fig. 6 The collusion attacks [14] in the proposed scheme

white area of S, and $T[I[S(1)]]$ is according to the black area. The range of α is $-1 \leq \alpha \leq 1$, but the secret information in I is visually recognizable when $\alpha \neq 0$, and the visual quality is better when α is larger in positive or smaller in negative.

3.3.1 Proposition 1 (Security of each random-grid)

Without stacking, each random-grid reveals neither secret information nor authentication information.

Proof In the proposed scheme, the first step randomly determines $P_1[i,j] \in \{0, 1\}$, so its probability of white pixel is $\frac{1}{2}$. Then, determine pixel values by referencing the authentication image A or the secret image S. According to the rule of reference, the probability of white pixel keeps $\frac{1}{2}$ no matter referencing A or S. Therefore, the white pixel's probability of each pixel in P_1 or P_2 is always $\frac{1}{2}$, even distributing the pixel into $G_1, G_2, \ldots, G_n$. Hence, for some G_m, where $m = 1, 2, \ldots, n$, the average light transmission according to white area in S is $T[G_m[S(0)]] = \frac{1}{|S(0)|}\sum_{1}^{|S(0)|}\frac{1}{2} = \frac{1}{2}$, and $T[G_m[S(1)]] = \frac{1}{|S(1)|}\sum_{1}^{|S(1)|}\frac{1}{2} = \frac{1}{2}$ is for black area ($|\cdot|$ is the number of pixels). Then, the contrast is $\alpha = \frac{T[G_m[S(0)]]-T[G_m[S(1)]]}{1+T[G_m[S(1)]]} = \frac{1/2-1/2}{1+1/2} = 0$, that is, the random-grid G_m reveals no secret information in visual. On the other hand, the average light transmission according to white area in A is $T[G_m[A(0)]] = \frac{1}{|A(0)|}\sum_{1}^{|A(0)|}\frac{1}{2} = \frac{1}{2}$ is for black area. Then, the contrast is

$\alpha = \frac{T[G_m[A(0)]]-T[G_m[A(1)]]}{1+T[G_m[A(1)]]} = \frac{1/2-1/2}{1+1/2} = 0$, that is, the random-grid G_m also reveals no authentication information in visual.

3.3.2 Proposition 2 (Cheating prevention)

Analyzing with two or more random-grids cannot infer another random-grid.

Proof When two or more malicious participants intend to cheat another participant, for generating fake grids, they must analyze the grids they have and guess the pixel values of another random-grid. A success cheating attacks based on the high similarity between estimating random-grid and aim random-grid. In other words, if the attackers fail in inferring pixel values, the cheating attacks cannot be performed. In **Phase 2** of the proposed scheme, the pixel values of P_1 and P_2 are randomly distributed into $G_1, G_2, \ldots, G_n$, that is, each random-grid can be viewed as a random combination of P_1 and P_2 alone. Therefore, even gathering two or more random-grids, the probability of guessing each pixel in another random-grid is always $\frac{1}{2}$. Forwardly, generate the estimating random-grid based on the $\frac{1}{2}$ fail guessing and make a fake random-grid. Then, in the authentication process, the fake information or doctoring trail will appear on the authenticating result. Hence, the proposed (2,n) scheme can prevent cheating attacks.

3.4 Contrast analysis

In the proposed (2,n) scheme, $G_1, G_2, \ldots, G_n$ are generated by randomly distributing the pixels of P_1 and P_2. Hence, before giving the analysis of stacking results of $G_1, G_2, \ldots, G_n$, we should analyze the stacking result of P_1 and P_2 first.

3.4.1 Proposition 1 (Contrast of stacking result with P_1 and P_2)

When stacking P_1 and P_2, the contrast of the reconstructed secret image is $\alpha = \frac{2}{9}$ (The average light transmission appears $T[P_1 \oplus P_2[S(0)]] = \frac{3}{8}$ and $T[P_1 \oplus P_2[S(1)]] = \frac{1}{8}$.). When authenticating with P_1 and P_2, the contrast of the revealed authentication image is $\alpha = \frac{1}{2}$ (The average light transmission appears $T[P_1 \oplus RP_2[A(0)]] = \frac{1}{2}$ and $T[P_1 \oplus RP_2[A(1)]] = 0$, where RP_2 means rotating P_2 with 90 degrees.).

Proof In the process of generating P_1 and P_2, for each four relating positions, the secret image, S, is referenced only two times, while the authentication image, A, is four times. This implies that half pixels of the secret image won't be correctly reconstructed, and the authentication image can be fully reconstructed. The definition of successfully reconstructing is that the stacking result is same with (2,2) scheme; that is, considering the normally reconstructed secret image in (2,2) scheme, the average light transmission of stacking result corresponding to white (or black) area of the secret image is $\frac{1}{2}$ (or 0). Therefore, when reconstructing the secret image with P_1 and P_2, for the pixels which are corresponding to the white (or black) area in S, there are half pixels that the probability of white pixels is $\frac{1}{2} \times \frac{1}{2}$ (failing reconstruction), and the other's probability is $\frac{1}{2}$ (or 0) (successful reconstruction). Hence, the average light transmission appears $T[P_1 \oplus P_2[S(0)]] = \frac{1}{|S(0)|}\left[\left(\sum_{1}^{|S(0)|/2} \frac{1}{2} \times \frac{1}{2}\right) + \left(\sum_{1}^{|S(0)|/2} \frac{1}{2}\right)\right] = \frac{1}{8} + \frac{1}{4} = \frac{3}{8}$ and $T[P_1 \oplus P_2[S(1)]] = \frac{1}{|S(1)|}\left[\left(\sum_{1}^{|S(1)|/2} \frac{1}{2} \times \frac{1}{2}\right) + \left(\sum_{1}^{|S(1)|/2} 0\right)\right] = \frac{1}{8}$.

Forwardly, the contrast of the revealed secret image with P_1 and P_2 is $\alpha = \frac{T[P_1 \oplus P_2[S(0)]] - T[P_1 \oplus P_2[S(1)]]}{1 + T[P_1 \oplus P_2[S(1)]]} = \frac{3/8 - 1/8}{1 + 1/8} = \frac{2}{9}$. On the other hand, when authenticating with P_1 and P_2, all pixels are reconstructed successfully, so the result is same with (2,2) scheme. Hence, the average light transmission appears $T[P_1 \oplus RP_2[A(0)]] = \frac{1}{|A(0)|} \sum_1^{|A(0)|} \frac{1}{2} = \frac{1}{2}$ and $T[P_1 \oplus RP_2[A(1)]] = \frac{1}{|A(1)|} \sum_1^{|A(1)|} 0 = 0$. Forwardly, the contrast of the revealed authentication image with P_1 and P_2 is $\alpha = \frac{T[P_1 \oplus RP_2[A(0)]] - T[P_1 \oplus RP_2[A(1)]]}{1 + T[P_1 \oplus RP_2[A(1)]]} = \frac{1/2 - 0}{1 + 0} = \frac{1}{2}$.

3.4.2 Proposition 2 (Contrast of reconstructed secret image)

The contrast of the reconstructed secret image in the proposed (2,*n*) scheme is $\alpha = \frac{2^n - 2^{n-r+1}}{9 \times 2^{n-1} + 3 \times 2^{n-r} - 12}$, where $r = 2, 3, \ldots, n$ is the number of stacked grids.

Proof According to the proposed (2,*n*) scheme, the pixels of P_1 and P_2 are randomly distributed into *n* random-grids. Therefore, when stacking *r* random-grids for reconstructing the secret image, for each pixel, there exists a probability, $\frac{2^{n-r}-1}{2^{n-1}-1}$, of fail reconstructing. Here, the definition of fail reconstructing is that the stacked *r* pixels are all from P_1 (or P_2), and the probability of white pixel of stacked result is $\frac{1}{2}$. On the other hand, if the stacked *r* pixels including pixels of both P_1 and P_2, this is considered as successful reconstructing, and the probabilities of white pixel are same with the average light transmission of stacking results of P_1 and P_2, that is, $T[P_1 \oplus P_2[S(0)]] = \frac{3}{8}$ and $T[P_1 \oplus P_2[S(1)]] = \frac{1}{8}$ (Proposition 1). Hence, the average light transmission appears $T[G_{u_1} \oplus G_{u_2} \oplus \cdots \oplus G_{u_r}\ [S(0)]] = \frac{2^{n-r}-1}{2^{n-1}-1} \times \frac{1}{2} + \left(1 - \frac{2^{n-r}-1}{2^{n-1}-1}\right) \times T[P_1 \oplus P_2[S(0)]] = \frac{1}{8} \times \frac{2^{n-r}-1}{2^{n-1}-1} + \frac{3}{8} = \frac{2^{n-r} + 2^n + 2^{n-1} - 4}{2^{n+2} - 8}$ and $T[G_{u_1} \oplus G_{u_2} \oplus \cdots \oplus G_{u_r}[S(1)]] = \frac{2^{n-r}-1}{2^{n-1}-1} \times \frac{1}{2} + \left(1 - \frac{2^{n-r}-1}{2^{n-1}-1}\right) \times T[P_1 \oplus P_2[S(1)]] = \frac{3}{8} \times \frac{2^{n-r}-1}{2^{n-1}-1} + \frac{1}{8} = \frac{3 \times 2^{n-r} + 2^{n-1} - 4}{2^{n+2} - 8}$ where $G_{u_1}, G_{u_2}, \ldots G_{u_r}$ mean any different *r* random-grids chosen from $G_1, G_2, \ldots G_n$. Forwardly, the contrast is $\alpha = \frac{T\left[G_{u_1} \oplus G_{u_2} \oplus \cdots \oplus G_{u_r}[S(0)]\right] - T\left[G_{u_1} \oplus G_{u_2} \oplus \cdots \oplus G_{u_r}[S(1)]\right]}{1 + T\left[G_{u_1} \oplus G_{u_2} \oplus \cdots \oplus G_{u_r}[S(1)]\right]} = \frac{2^n - 2^{n-r+1}}{9 \times 2^{n-1} + 3 \times 2^{n-r} - 12}$.

To show that the theoretical contrast is close to the experimental result, we give the comparison table, see Table 1.

Table 1 Contrast values of reconstructed secret image and theoretical values

	Contrast of experimental result			Contrast of theoretical function		
r	(2,3)	(2,4)	(2,5)	(2,3)	(2,4)	(2,5)
2	0.132303	0.113305	0.106759	0.133333	0.111111	0.102564
3	0.221636	0.187565	0.173451	0.222222	0.181818	0.166667
4		0.221642	0.208604		0.222222	0.202899
5			0.222990			0.222222

3.4.3 Proposition 3 (Contrast of authentication result)

The contrast of authentication result in the proposed (2,n) scheme is $\alpha = \frac{(n-1)\times 2^{n-1}}{(9\times n+1)\times 2^{n-2}-5\times n}$.

Proof When performing authentication, it is similar to **Proposition 2** that there exists $\frac{2^{n-2}-1}{2^{n-1}-1}$ ($r=2$, the authentication process only uses two random-grids each time.) pixels fail in reconstructing, but because of rotating in authentication, the probability of white pixel is $\frac{1}{2}\times\frac{1}{2}$. However, in the rest $1-\frac{2^{n-2}-1}{2^{n-1}-1}$ pixels, there also exists a probability, $\frac{1}{n}$, of fail reconstructing because of the wrong way of rotating. (From **Proposition 1**, $T[P_1\oplus RP_2[A(0)]] = \frac{1}{2}$ and $T[P_1 \oplus RP_2[A(1)]] = 0$) Hence, the average light transmission appears

$$\begin{aligned} &T[G_{u_1}\oplus RG_{u_2}[A(0)]]\\ &=\frac{2^{n-2}-1}{2^{n-1}-1}\times\frac{1}{4}+\frac{1}{n}\times\left(1-\frac{2^{n-2}-1}{2^{n-1}-1}\right)\times\frac{1}{4}+\frac{n-1}{n}\times\left(1-\frac{2^{n-2}-1}{2^{n-1}-1}\right)\times T[P_1\oplus RP_2[A(0)]]\\ &=\frac{2^{n-2}-1}{2^{n-1}-1}\times\frac{1}{4}+\frac{1}{n}\times\left(1-\frac{2^{n-2}-1}{2^{n-1}-1}\right)\times\frac{1}{4}+\frac{n-1}{n}\times\left(1-\frac{2^{n-2}-1}{2^{n-1}-1}\right)\times\frac{1}{2}\\ &=\frac{2\times n-1}{4\times n}-\frac{n-1}{4\times n}\times\frac{2^{n-2}-1}{2^{n-1}-1}\\ &=\frac{(3\times n-1)\times 2^{n-2}-n}{n\times 2^{n+1}-4\times n} \end{aligned}$$

and

$$\begin{aligned} &T[G_{u_1}\oplus RG_{u_2}[A(1)]]\\ &=\frac{2^{n-2}-1}{2^{n-1}-1}\times\frac{1}{4}+\frac{1}{n}\times\left(1-\frac{2^{n-2}-1}{2^{n-1}-1}\right)\times\frac{1}{4}+\frac{n-1}{n}\times\left(1-\frac{2^{n-2}-1}{2^{n-1}-1}\right)\times T[P_1\oplus RP_2[A(1)]]\\ &=\frac{2^{n-2}-1}{2^{n-1}-1}\times\frac{1}{4}+\frac{1}{n}\times\left(1-\frac{2^{n-2}-1}{2^{n-1}-1}\right)\times\frac{1}{4}\\ &=\frac{1}{4\times n}+\frac{n-1}{4\times n}\times\frac{2^{n-2}-1}{2^{n-1}-1}\\ &=\frac{(n+1)\times 2^{n-2}-n}{n\times 2^{n+1}-4\times n} \end{aligned}.$$

Forwardly, the contrast is $\alpha = \frac{T\left[G_{u_1}\oplus RG_{u_2}[A(0)]\right]-T\left[G_{u_1}\oplus RG_{u_2}[A(1)]\right]}{1+T\left[G_{u_1}\oplus RG_{u_2}[A(1)]\right]} = \frac{(n-1)\times 2^{n-1}}{(9\times n+1)\times 2^{n-2}-5\times n}$.

To show that the theoretical contrast is close to the experimental result, we give the comparison table, see Table 2, with different cases.

4 The proposed (k,n) VSS scheme with cheating prevention

In this section, the proposed (k,n) RG-based VSS scheme with cheating prevention is described as follows. The experimental results and performance analysis are shown after it.

Table 2 Contrast values of reconstructed authentication image and theoretical values

Contrast of experimental result			Contrast of theoretical function		
(2,3)	(2,4)	(2,5)	(2,3)	(2,4)	(2,5)
0.194431	0.184634	0.180406	0.195122	0.1875	0.186589

4.1 The proposed scheme

Because, in the proposed (2,n) scheme in Section 3, the generated random-grids have a property that authentication can be performed between each two random-grids, we expect that the property will also work on our (k,n) scheme. The proposed scheme is mainly disported to three phases: (2,n) generation for the authentication image and a random image, encoding the secret image by a (k,n) scheme, and cheating-prevention (k,n) generation.

- Phase 1: Gererate (2,n) random-grids

Input a random image and an authentication image, A, to perform the proposed (2,n) prevention scheme in Section 3, and denote the n grids by P_1, P_2, …, P_n.

- Phase 2: Gererate (k,n) random-grids

Input the secret image, S, to perform the (k,n) scheme in Ref. [5], and denote the n grids by Q_1, Q_2, …, Q_n.

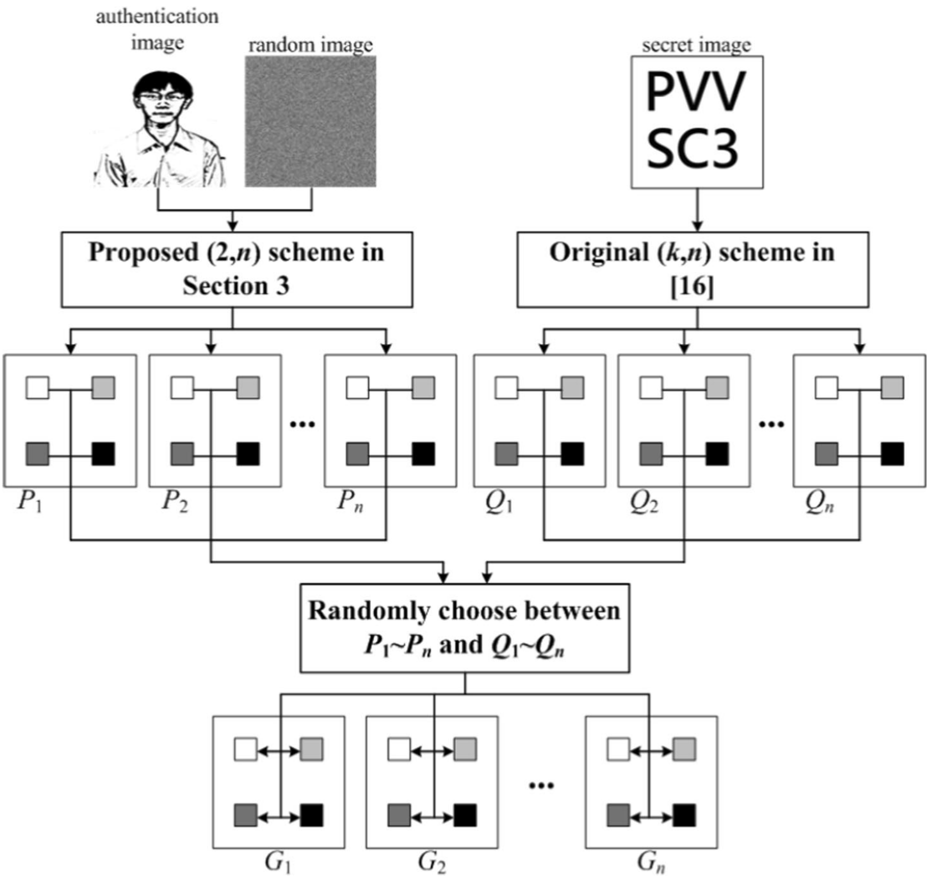


Fig. 7 The concept of the proposed (k,n) scheme

- Phase 3: Gererate (k,n) final random-grids by distributing P_1 and P_2 into G_m, where $m = 1,2,\ldots,n$

Randomly insert some pixels of P_1, P_2, …, P_n into Q_1, Q_2, …, Q_n, and the renewed n grids of Q_1, Q_2, …, Q_n are regarded as final output random-grids, denoted by G_1, G_2, …, G_n.

The concept of the proposed scheme is shown in Fig. 7.

The algorithm of the proposed encoding process is briefly illustrated as follows.

Input: A secret image $S = \{S[i,j] \mid S[i,j] \in \{0,1\}, 0 \le i \le (w-1), 0 \le j \le (h-1)\}$, an authentication image $A = \{A[i,j] \mid A[i,j] \in \{0,1\}, 0 \le i \le (w-1), 0 \le j \le (h-1)\}$.

Output: n random-grids $G_m = \{G_m[i,j] \mid G_m[i,j] \in \{0,1\}, 0 \le i \le (w-1), 0 \le j \le (h-1)\}$ $(m = 1,2,\ldots,n)$

// Generate $P_1, P_2, \ldots, P_n$ by (2,*n*) scheme proposed in Section 3

// Generate $Q_1, Q_2, \ldots, Q_n$ by (*k*,*n*) scheme proposed in Ref. [16]

//Randomly insert some pixels of P_i into Q_i, where $i = 1,2,\ldots,n$

for $i = 0$ **to** $w/2-1$

  for $j = 0$ **to** $h/2-1$

    Randomly determine whether performing the next for-loop or not

    for $m = 1$ **to** n

      $Q_m[i,j] = P_m[i,j]$

      $Q_m[h-j,i] = P_m[h-j,i]$

      $Q_m[w-i,h-j] = P_m[w-i,h-j]$

      $Q_m[j,h-i] = P_m[j,h-i]$

for $m = 1$ **to** n

  $G_m = Q_m$

The decoding process directly stacks k or more random-grids to reconstruct the secret image detectable by the human visual system. For each two random-grids, rotating one of them by 90 degrees and stacking will reconstruct the authentication image.

4.2 Experimental results

To demonstrate that the proposed scheme can prevent the collusion attacks and its feasibility, the experimental results are given in this section.

We choose images Fig. 8a as the secret image and Fig. 8b as the authentication image with both size 1024×1024. Then, perform the proposed scheme with (3,4) to generate four random-grids Fig. 8c, d, e and f.

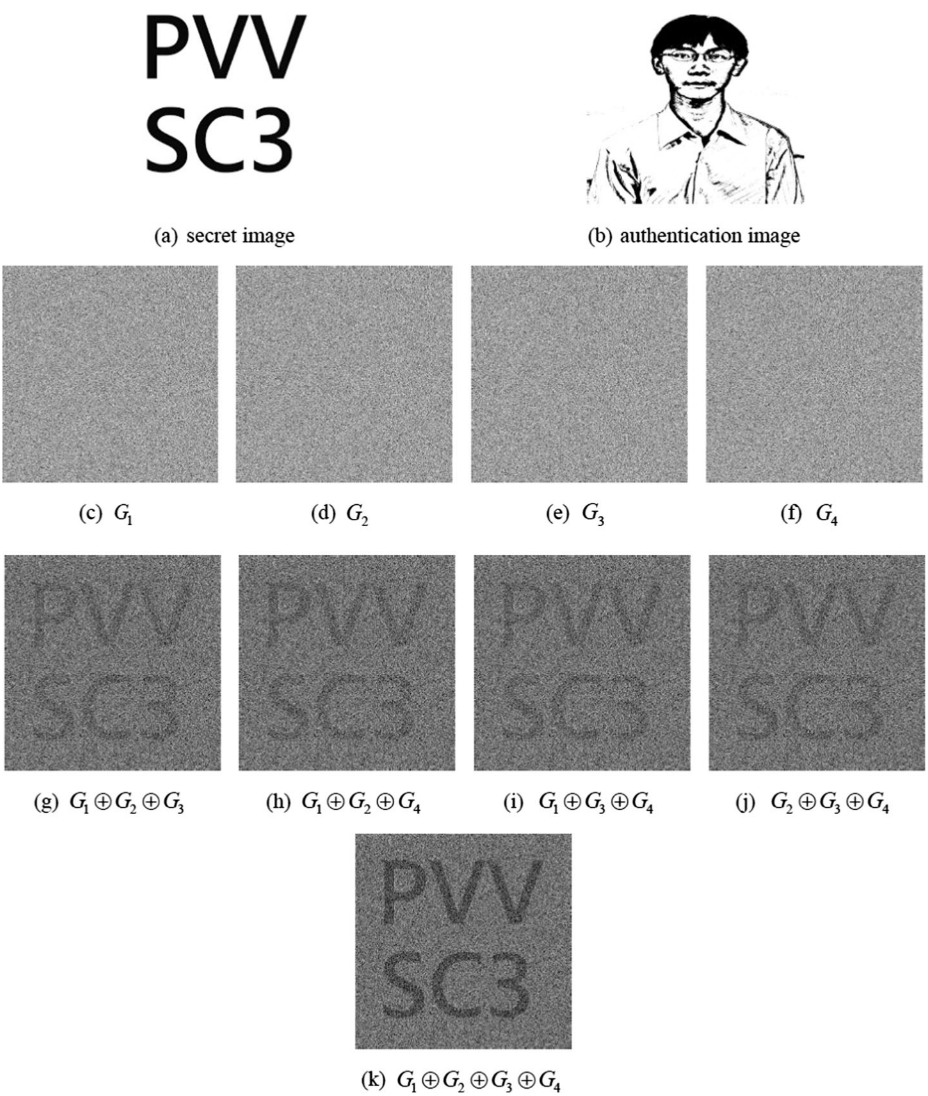


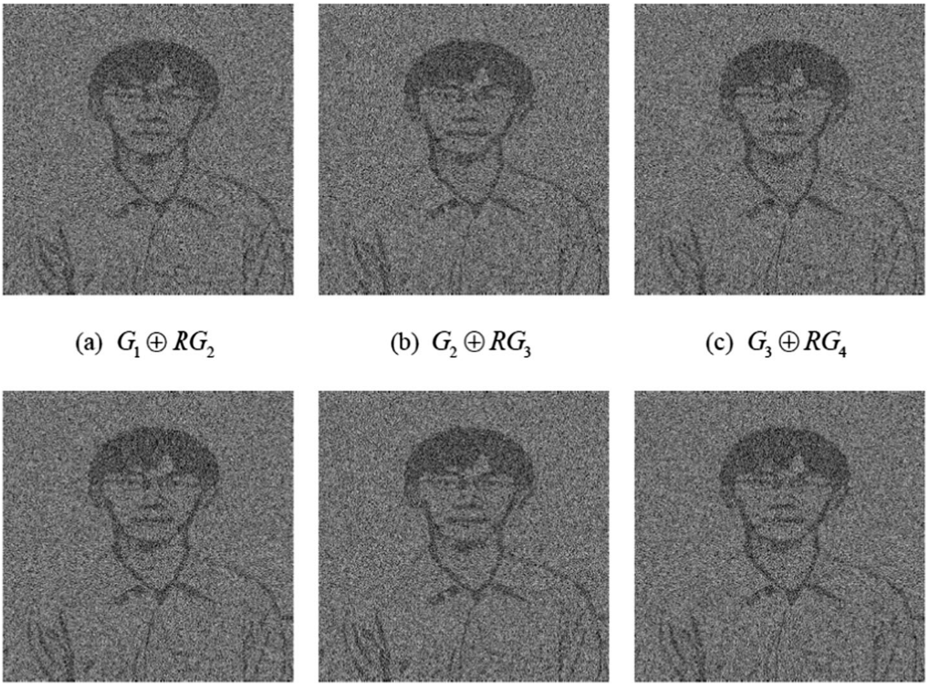
Fig. 8 The experimental results of the proposed scheme with (3,4)

4.2.1 Stacking results of (3,4) case

The results of stacking each three random-grids are Fig. 8g, h, i, j and k for stacking all. The authentication results are as Fig. 9a, b, c, d, e and f. Notice that RG_1, RG_2, RG_3 and RG_4 stand for the 90 degree rotated random-grids.

4.2.2 Stacking results of (3,4) case with cheating attacks

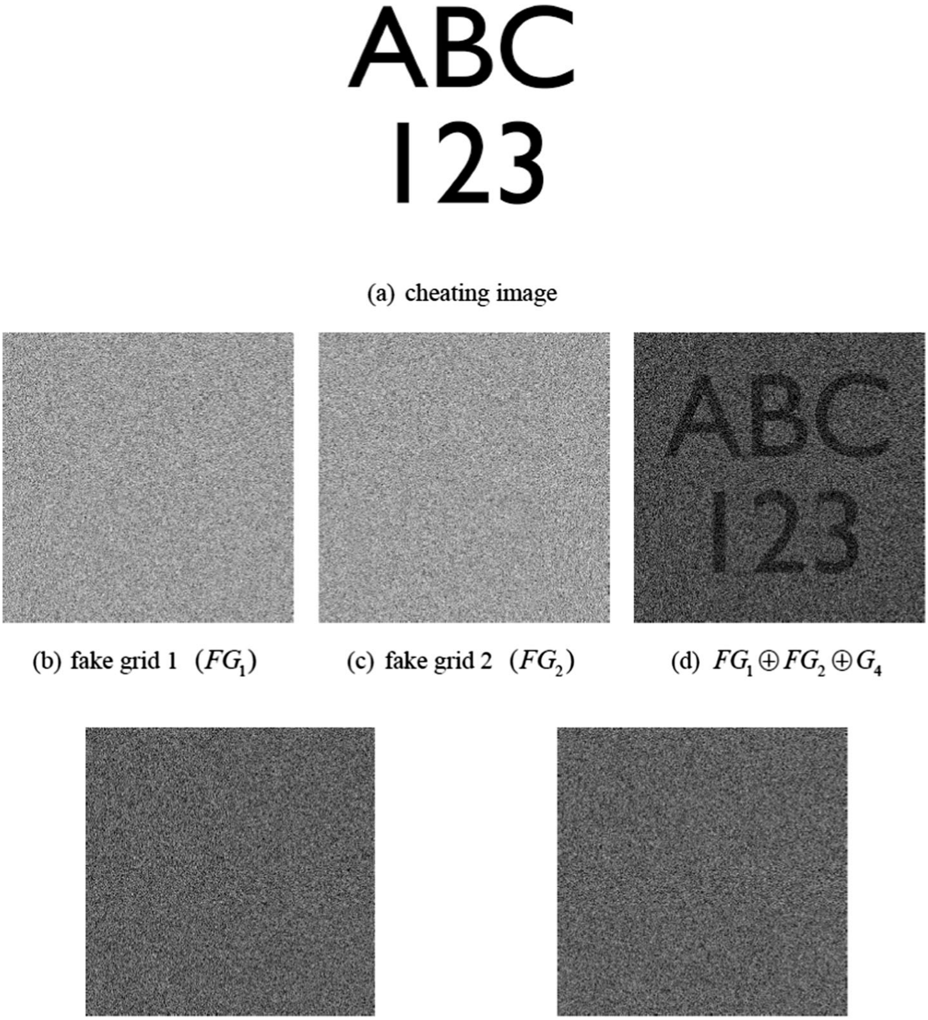
Next, we implement the collusion attacks of (k,n) introduced in Ref. [14] on the proposed scheme. Suppose that three members, u_1, u_2 and u_3, who have random-grids, G_1, G_2 and G_3, perform the collusion attacks to cheat the rest participant, u_4. According to the analysis of the grid pixels in G_1, G_2 and G_3, the three cheaters can generate an evaluated grid which is similar to G_4 with high probability. Then, input the evaluated image and a determined cheating image, Fig. 10a, and perform the (n,n) scheme, where $n = 3$, to generate two fake grids, FG_1 and FG_2, as shown in Fig. 10b and c. When u_4 uses G_4 to stack with FG_1 and FG_2, Fig. 10d, u_4 will recover the cheating information. Nevertheless, if u_4 performs the authentication Fig. 10e and f, (s)he will see the authenticating results being different from the authentication image Fig. 8b. Hence, u_4 can tell that FG_1 and FG_2 are fake grids.



(a) $G_1 \oplus RG_2$ (b) $G_2 \oplus RG_3$ (c) $G_3 \oplus RG_4$

(d) $G_4 \oplus RG_1$ (e) $G_1 \oplus RG_3$ (f) $G_2 \oplus RG_4$

Fig. 9 The authentication of the proposed scheme with (3,4)



(a) cheating image

(b) fake grid 1 (FG_1)

(c) fake grid 2 (FG_2)

(d) $FG_1 \oplus FG_2 \oplus G_4$

(e) $FG_1 \oplus RG_4$

(f) $FG_2 \oplus RG_4$

Fig. 10 The collusion attacks [14] in the proposed scheme

4.3 Security analysis

4.3.1 Proposition 1 (Security of each random-grid)

Without stacking, each random-grid reveals neither secret information nor authentication information.

Proof In the proposed (k,n) scheme, for each generated G_m, where $m = 1, 2, \ldots, n$, it is the random combination of random-grids generated from the proposed $(2,n)$ scheme and Chen and Tsao's (k,n) scheme [5]. The security of the proposed $(2,n)$ scheme has been proven in Section 3.3, and the security of Chen and Tsao's scheme is also proved in their thesis. Hence, the security of the combination with the two scheme's random-grids is also guaranteed.

4.3.2 Proposition 2 (Cheating prevention)

Analyzing with two or more random-grids cannot infer another random-grid.

Proof Although Chen and Tsao's (k,n) scheme [5] has been pointed out the insecurity in cheating attacks [14], the proposed scheme randomly combines the random-grids of the proposed $(2,n)$ scheme and Chen and Tsao's (k,n) scheme. If the attackers do not separate the pixels generated by the proposed $(2,n)$ scheme, the generated fake grid will appear nothing in the authentication process, that is, the cheating attack is not a success. On the other hand, if the attackers intend to guess out the pixels which are generated by Chen and Tsao's scheme and perform the cheating attacks, the probability of correctness is $\frac{1}{2}$. With the $\frac{1}{2}$ fail guessing, after the authentication process, the fake information or doctoring trail will appear on the authenticating result. Hence, the proposed (k,n) scheme can prevent cheating attacks.

4.4 Contrast analysis

4.4.1 Proposition 1(Contrast of reconstructed secret image)

The contrast of authentication result in the proposed (k,n) scheme is $\alpha = \frac{2^{n-k+1}-(n-r+2)\times(n-r-1)}{\left(2^{n-2}+2^{k-2}\right)\times\left(\frac{2^{n+2}+2^{n-1}-2^{n-r}}{2^{n-1}-1}\right)+2^{k-2}\times(n-r+1)\times(n-r)}$, where $r = 2, 3, \ldots, n$ is the number of stacked grids.

Proof. Because G_1, G_2, …, G_n are generated by combining the proposed $(2,n)$ scheme and Chen and Tsao's (k,n) scheme, there is a half stacking result which is same with the proposed $(2,n)$ scheme (or Chen and Tsao's (k,n) scheme). About the stacking result of the proposed $(2,n)$ scheme, a random grid is used as the secret image. Hence, from the proof of **Proposition 2** in Section 3.4, the stacking result's average light transmission of the proposed $(2,n)$ scheme is $\frac{T\left[G_{u_1}\oplus G_{u_2}\oplus\cdots\oplus G_{u_r}[S(0)]\right]+T\left[G_{u_1}\oplus G_{u_2}\oplus\cdots\oplus G_{u_r}[S(1)]\right]}{2} = \frac{2^{n-r}+2^{n-1}-2}{2^{n+1}-4}$. On the other hand, the stacking result's average light transmission of Chen and Tsao's (k,n) scheme is $\frac{1}{2^{k-1}}$ according to white area in the secret image (or 0 to black area). Furthermore, considering the fail stacking in Chen and Tsao's (k,n) scheme, that is, the stacked pixels being same, the average light transmission

Table 3 Contrast values of reconstructed secret image and theoretical values

	Contrast of experimental result			Contrast of theoretical function		
r	(3,4)	(3,5)	(3,6)	(3,4)	(3,5)	(3,6)
3	0.053145	0.036101	0.031709	0.07	0.04	0.032979
4	0.111443	0.077432	0.066352	0.111111	0.085714	0.069663
5		0.111443	0.092943		0.111111	0.096724
6			0.111443			0.111111

Table 4 Contrast values of reconstructed authentication image and theoretical values

Contrast of experimental result			Contrast of theoretical function		
(3,4) 0.057512	(3,5) 0.052594	(3,6) 0.051600	(3,4) 0.058824	(3,5) 0.052545	(3,6) 0.050649

is $\frac{1}{2}$, and its probability is $\frac{\binom{n-r+1}{2}}{2^{n-k}+1}$. Therefore, the average light transmission appear

$$T[G_{u_1}\oplus G_{u_2}\oplus\cdots\oplus G_{u_r}[S(0)]]$$
$$=\frac{1}{2}\times\left(\frac{2^{n-r}+2^{n-1}-2}{2^{n+1}-4}\right)+\frac{1}{2}\times\frac{\binom{n-r+1}{2}}{2^{n-k}+1}\times\frac{1}{2}+\frac{1}{2}\times\left(1-\frac{\binom{n-r+1}{2}}{2^{n-k}+1}\right)\times\frac{1}{2^{k-1}}$$
$$=\frac{1}{2}\times\left(\frac{2^{n-r}+2^{n-1}-2}{2^{n+1}-4}\right)+\frac{1}{4}\times\frac{(n-r+1)\times(n-r)}{2^{n-k+1}+2}+\frac{1}{2^k}\times\left(1-\frac{(n-r+1)\times(n-r)}{2^{n-k+1}+2}\right)$$

and

$$T[G_{u_1}\oplus G_{u_2}\oplus\cdots\oplus G_{u_r}[S(1)]]$$
$$=\frac{1}{2}\times\left(\frac{2^{n-r}+2^{n-1}-2}{2^{n+1}-4}\right)+\frac{1}{2}\times\frac{\binom{n-r+1}{2}}{2^{n-k}+1}\times\frac{1}{2}+\frac{1}{2}\times\left(1-\frac{\binom{n-r+1}{2}}{2^{n-k}+1}\right)\times 0$$
$$=\frac{1}{2}\times\left(\frac{2^{n-r}+2^{n-1}-2}{2^{n+1}-4}\right)+\frac{1}{4}\times\frac{(n-r+1)\times(n-r)}{2^{n-k+1}+2}$$

Forwardly, the contrast is

$$\alpha=\frac{T[G_{u_1}\oplus G_{u_2}\oplus\cdots\oplus G_{u_r}[S(0)]]-T[G_{u_1}\oplus G_{u_2}\oplus\cdots\oplus G_{u_r}[S(1)]]}{1+T[G_{u_1}\oplus G_{u_2}\oplus\cdots\oplus G_{u_r}[S(1)]]}$$
$$=\frac{2^{n-k+1}-(n-r+2)\times(n-r-1)}{\left(2^{n-2}+2^{k-2}\right)\times\left(\frac{2^{n+2}+2^{n-1}-2^{n-r}}{2^{n-1}-1}\right)+2^{k-2}\times(n-r+1)\times(n-r)}$$

To show that the theoretical contrast is close to the experimental result, we give the comparison table, Table 3, with different cases.

4.4.2 Proposition 2 (Contrast of authentication result)

The contrast of authentication result in the proposed (k,n) scheme is $\alpha=\frac{(n-k+1)\times(n-1)\times 2^{n-1}}{(n-k+1)\times(39\times n+1)\times 2^{n-2}-10\times n\times\left(2\times n-2\times k+1+2^{n-1}\right)}$.

Proof. Because G_1, G_2, …, G_n are generated by combining the proposed (2,n) scheme and Chen and Tsao's (k,n) scheme, there exist half pixels belonging to Q_1, Q_2, …, Q_n generated by Chen and Tsao's (k,n) scheme. Q_1, Q_2, …, Q_n have no authentication information. Therefore, after rotating and stacking for authenticating with each two random-grids, the half part's

Table 5 Comparison between the related cheating prevention schemes and the proposed schemes

	Horng et al. [9]		Hu and Tzeng [10]	Tsai et al. [22]	The Proposed
Extra share	YES	NO	YES	NO	NO
Pixel expansion for (2,3) VSS scheme	2×2	2×2	$2\times 2+2$	2×2	No
Computation cost in the share generation	Low	Low	Low	High	Low
Cheating prevention	YES	YES	YES	YES	YES

average light transmission is $\frac{1}{2}\times\frac{1}{2}$. And the authentication result of the other half pixels is related to the authentication result of the proposed (2,n) scheme. In this half part, there exist some pixels which fail to reconstruct the authentication image (wrong rotating way) with probability $\frac{n-k}{2\times n-2\times k+1}$, and its average light transmission is $\frac{1}{2}\times\frac{1}{2}$. Then, the authenticating result of the rest part is same with the proposed (2,n) scheme, and the average light transmission is equal to $T[G_{u_1}\oplus RG_{u_2}[A(0)]]$ and $T[G_{u_1}\oplus RG_{u_2}[A(1)]]$ (see the proof of **Proposition 3** in Section 3.4). Hence, the average light transmission appears

$$\begin{aligned}&T[G_{u_1}\oplus RG_{u_2}[A(0)]]\\&=\frac{1}{2}\times\frac{1}{2}\times\frac{1}{2}+\frac{1}{2}\times\frac{n-k}{2\times n-2\times k+1}\times\frac{1}{2}\times\frac{1}{2}+\frac{1}{2}\times\left(1-\frac{n-k}{2\times n-2\times k+1}\right)\times\frac{(3\times n-1)\times 2^{n-2}-n}{n\times 2^{n+1}-4\times n}\\&=\frac{1}{8}+\frac{1}{8}\times\frac{n-k}{2\times n-2\times k+1}+\frac{1}{2}\times\frac{n-k+1}{2\times n-2\times k+1}\times\frac{(3\times n-1)\times 2^{n-2}-n}{n\times 2^{n+1}-4\times n}\end{aligned}$$

and

$$\begin{aligned}&T[G_{u_1}\oplus RG_{u_2}[A(1)]]\\&=\frac{1}{2}\times\frac{1}{2}\times\frac{1}{2}+\frac{1}{2}\times\frac{n-k}{2\times n-2\times k+1}\times\frac{1}{2}\times\frac{1}{2}+\frac{1}{2}\times\left(1-\frac{n-k}{2\times n-2\times k+1}\right)\times\frac{(n+1)\times 2^{n-2}-n}{n\times 2^{n+1}-4\times n}\\&=\frac{1}{8}+\frac{1}{8}\times\frac{n-k}{2\times n-2\times k+1}+\frac{1}{2}\times\frac{n-k+1}{2\times n-2\times k+1}\times\frac{(n+1)\times 2^{n-2}-n}{n\times 2^{n+1}-4\times n}\end{aligned}$$

Forwardly, the contrast is

$$\begin{aligned}\alpha&=\frac{T[G_{u_1}\oplus RG_{u_2}[A(0)]]-T[G_{u_1}\oplus RG_{u_2}[A(1)]]}{1+T[G_{u_1}\oplus RG_{u_2}[A(1)]]}\\&=\frac{(n-k+1)\times(n-1)\times 2^{n-1}}{(n-k+1)\times(39\times n+1)\times 2^{n-2}-10\times n\times\left(2\times n-2\times k+1+2^{n-1}\right)}\end{aligned}$$

To show that the theoretical contrast is close to the experimental result, we give the comparison table, Table 4**,** with different cases.

5 Further discussion

Carry on the demonstration of contract and security analyses in Sections 3 and 4, it's worthwhile to highlight the difference and advantages of the proposed schemes compared with the related work.

Firstly, the proposed scheme does not maintain any extra share like Ref. [9, 10]. Secondly, the pixel expansion is avoided compared to the tradition VSS scheme. Thirdly, the computation cost in the encoding phase is very low compared to Ref. [22] while the decoding phase involves no computation cost. The comparison between the proposed schemes and the related cheating prevention schemes in Ref. [9, 10, 22] is shown in Table 5.

6 Conclusion

In this paper, we propose two threshold RG-based VSS schemes with cheating prevention for cases (2,n) and (k,n). To prevent cheating attacks, each two random grids can perform the authentication process in both proposed schemes, and the fake grids will be detected. The experimental results and the analysis of security and contrast show that the proposed method is efficient and practical.

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

References

1. Blundo C, De Bonis A, De Santis A (2001) Improved schemes for visual cryptography. Des Codes Crypt 24:255–278
2. Chang, CC, Chuang JC, Lin PY (2005) Sharing a secret two-tone image in two gray-level images. Proceedings of the 11th International Conference on Parallel and Distributed Systems, pp. 300-304
3. Chen TH, Tsao KH (2008) Image encryption by (n,n) random grids. Proceedings of 18th Information Security Conference, Hualien
4. Chen TH, Tsao KH (2009) Visual secret sharing by random grids revisited. Pattern Recogn 42(9):2203–2217
5. Chen TH, Tsao KH (2011) Threshold visual secret sharing by random grids. J Syst Softw 84(7):1197–1208
6. Eisen PA, Stinson DR (2002) Threshold visual cryptography schemes with specified whiteness levels of reconstructed pixels. Des Codes Crypt 25(1):15–61
7. Fang WP (2009) Non-expansion visual secret sharing in reversible style. International Journal of Computer Science and Network Security 9(2):204–208
8. Fang WP, Lin JC (2006) Visual cryptography with extra ability of hiding confidential data. Journal of Electronic Imaging 15(2):0230201–0230207
9. Horng GB, Chen TH, Tsai DS (2006) Cheating in Visual Cryptography. Des Codes Crypt 38(2):219–236
10. Hu CM, Tzeng WG (2007) Cheating Prevention in Visual Cryptography. IEEE Trans Image Process 16(1): 36–45
11. Huang JC, Jeng FG, Chen TH (2017) A new buyer-seller watermarking protocol without multiple watermarks insertion. Multimedia Tools and Applications 76(7):9667–9679
12. Ito R, Kuwakado H, Tanaka H (1999) Image size invariant visual cryptography. IEICE Transactions Fundamentals E82-A(10)
13. Kafri O, Keren E (1987) Encryption of pictures and shapes by random grids. Opt Lett 12(6):377–379
14. Lee YS, Chen TH (2012) Insight into collusion attacks in random-grid-based visual secret sharing. Signal Process 92(3):727–736
15. Lin CH, Lee YS, Chen TH (2015) Friendly progressive random-grid-based visual secret sharing with adaptive contrast. J Vis Commun Image Represent 33:31–44
16. Lin KS, Lin CH, Chen TH (2014) Distortionless visual multi-secret sharing based on random grids. Inf Sci 288(1):330–346
17. Lukac R, Plataniotis KN (2005) Bit-level based secret sharing for image encryption. Pattern Recogn 38(5): 767–772
18. Naor M, Pinkas B (1997) Visual authentication and identification. Proceedings of the 17th Annual International Cryptology Conference on Advances in Cryptology, Lecture Notes in Computer Science, Vol. 1294, Santa Barbara, California, USA, pp. 322-336
19. Naor M, Shamir A (1995) Visual cryptography. Proceedings of Advances in Cryptology: Eurocrypt94, Lecture Notes in Computer Science, pp. 1-12
20. Prisco RD, Santis AD (2006) Cheating Immine (2,n)-Threshold Visual Secret Sharing Scheme. Security and Cryptography for Networks, Lecture Notes in Computer Science, 4116
21. Shyu SJ (2007) Image encryption by random grids. Pattern Recogn 40(3):1014–1031
22. Tsai DS, Chen TH, Horng G (2007) A cheating prevention scheme for binary visual cryptography with homogeneous secret images. Pattern Recogn 40(8):2356–2366
23. Tsai DS, Horng G (2007) Cheating in Visual Cryptography Revisited. Proceedings of 17th Information Security Conference, pp. 769-771

24. Tu SF, Hsu CS (2009) "Digital watermarking method based on image size invariant visual cryptographic scheme," Proceedings of Symposia and Workshops on 9th Ubiquitous. Autonomic and Trusted Computing 2009:362–366
25. Vashistha A, Nallusamy R, Das A, Paul S (2010) Watermarking video content using visual cryptography and scene averaged image. Proceedings of IEEE International Conference on Multimedia and Expo 2010: 1641–1646
26. Wu XT, Sun W (2012) Random grid-based visual secret sharing for general access structures with cheat-preventing ability. J Syst Softw 85(5):1119–1134

Bing-Jian Wang received his B.S. and M.S. in Department of Computer Science and Information Engineering from National Chiayi University in 2012 and 2014, respectively. His research interests include information security, and image security.

Tzer-Shyong Chen received the Ph.D. in the Department of Electrical Engineering (Computer Science) at National Taiwan University, Taiwan. He is currently a professor in the Department of Information Management at Tunghai University, Taiwan. Research fields include Information Security, Cryptography, and Network Security.

Fuh-Gwo Jeng received his M.S. in computer and information science from National Chiao Tung University and Ph.D. degree at the Institute of Computer Science, National Chung Hsing University, Taiwan. He is presently an associate professor of Department of Applied Mathematics, Nation Chiayi University. His research interests include information security and computer graphics

Tzung-Her Chen was born in Tainan, Taiwan, Republic of China, in 1967. He received the B.S. degree in Department of Information & Computer Education from National Taiwan Normal University in 1991 and the M.S. degree in Department of Information Engineering from Feng Chia University in 2001. In 2005, he received his Ph.D. degree in Department of Computer Science from National Chung Hsing University. He has been with Department of Computer Science and Information Engineering at National Chiayi University as Professor since August 2011. His research interests include information hiding, multimedia security, digital rights management, blockchain technology. He is an honorary member of the Phi Tau Phi Scholastic Honor Society.