Fundamenta Informaticae 137 (2015) 1–18
DOI 10.3233/FI-2015-1180
IOS Press

Random-Grid Based Region Incrementing Visual Secret Sharing

Sachin Kumar[*], **Rajendra Kumar Sharma**
Department of Mathematics
Indian Institute of Technology Delhi
Hauz Khas, New Delhi - 110016, India
skiitd09@gmail.com; rksharma@maths.iitd.ac.in

Abstract. The concept of region incrementing in visual cryptography was introduced to encrypt an image into multiple secrecy levels. But, it suffers from the pixel expansion increasing exponentially as the number of participants grows. In this paper, we propose a region incrementing visual secret sharing (RIVSS) scheme based on random grids. The proposed scheme is a general (k, n)-RIVSS scheme, in which any t $(k \leq t \leq n)$ shares can be used to reconstruct the secret regions up to $t - k + 1$ levels. However, no information about the input image can be revealed by any $k - 1$ or fewer shares. With a nice property of region incrementing, the proposed scheme benefits by sharing an image without any pixel expansion and codebook requirement. We give formal proofs and experimental results to confirm both correctness and feasibility of our scheme.

Keywords: visual secret sharing, visual cryptography, region incrementing, random grids.

1. Introduction

A secret sharing scheme permits a secret to be shared among participants in such a way that only qualified sets of participants can reconstruct the secret, but any unqualified set of participants has absolutely no information about the secret. In 1979, Shamir [13] and Blakley [1] independently introduced the concept of secret sharing, which guarantees the security of the data against destruction and stealing.

In 1994, Naor and Shamir [12] extended the concept of secret sharing for a secret information of visual type, known as Visual Cryptography (VC). A (k, n)-threshold VC scheme encodes a black and

[*] Address for correspondence: Department of Mathematics, Indian Institute of Technology Delhi, Hauz Khas, New Delhi - 110016, India.

Received October 2013; revised November 2014.

white secret image into n meaningless shares (images) such that any $k-1$ or fewer shares cannot reveal any information about the secret image. However, the secret image reconstruction can be performed by printing at least k $(\leq n)$ shares on transparencies and stacking these transparencies together. The decryption process in a VC scheme is computation free as it is performed with the help of human visual system. The basic model of a VC scheme [12] considers the secret image as a collection of black and white pixels, where each pixel of the original image appears into n shares in such a way that each pixel of any share is again a collection of m black and white sub-pixels, referred to as pixel expansion. In a VC scheme, encoding of each pixel depends upon the collections of basis matrices, referred to as codebook, constructed prior to encoding process. Thus, the performance of the VC schemes is degraded as they require to construct codebook prior to encoding process (which is not always trivial), and have large pixel expansion. For example, in a (n, n) VC scheme [12], the optimal pixel expansion is 2^{n-1}, which increases exponentially as n increases. The approach of Boolean operations-based [20, 10, 2, 5] VSS overcome the problem of large pixel expansion, but violate the property of no computation in the decoding process as they require a computational device to perform the decoding process.

In 1987, Kafri and Keren [6] proposed another VSS technique by using random grids with no pixel expansion and codebook requirement. They proposed three different algorithms to share a binary secret image into two same size cipher grids. The decryption is done in the same way as in traditional VC with the help of human visual system. Shyu [14] extended Kafri and Keren's binary construction to gray-level and color images. Later, Shyu [15] and Chen and Tsao [3] independently generalized Kafri and Keren's $(2, 2)$ scheme to a (n, n) scheme for any n (≥ 2). Kumar and Sharma [7] proposed a method to enhance the contrast in random-grid based (n, n) VSS schemes. Further, Chen and Tsao [4] proposed a (k, n)-threshold VSS scheme based on random grids. The schemes [23, 9, 16] generalized the threshold VSS to general access structures by using the random grids so that they can be used to realize complex sharing strategies. Kumar and Sharma [8] proposed a random-grid based method for recursive hiding of secrets by embedding smaller secrets into the shares of larger secrets in a recursive manner.

Wang [21] introduced the concept of region incrementing in visual cryptography (RIVC) widening the possible applications of VC. They proposed a $(2, n)$-RIVC scheme, in which the secret image is encoded by using multiple encoding rules. The secret image is decomposed into multiple regions of different secrecy levels in such a way that any t (≥ 2) shares can be used to reconstruct regions up to secrecy levels $t-1$. In [21], the basis matrices for constructing $(2, n)$-RIVC scheme were reported only for small values of $n = 2, 3, 4$. Shyu [17] designed a construction using linear programming approach to obtain basis matrices for given n. Later, Yang et al. [24] proposed a general construction for a (k, n)-RIVC scheme. The existing methods for RIVC [21, 17, 24] result in large pixel expansion and require codebook prior to encoding process. The large pixel expansion indicates the shares of the larger size, which are difficult for processing such as distribution and storage. Wang et al. [22] introduced the random-grid based construction methods for $(2, 3)$-RIVSS, which is recently extended to a $(2, n)$-threshold case for binary images [25].

In this paper, we design a general (k, n)-RIVSS scheme by using random grids. The main contributions of this paper are as follows.

1. Generalized - The proposed scheme is a general (k, n)-RIVSS scheme, in which any t $(k \leq t \leq n)$ shares can be used to reconstruct the secret regions up to $t-k+1$ levels. However, any information about the original image cannot be revealed by any $k-1$ or fewer shares.

2. No pixel expansion - The proposed scheme generates shares of the size same as that of the original image, which can be stored and distributed more efficiently.

3. No codebook requirement - The proposed scheme does not have any overhead to construct the codebook prior to encryption process.

4. No computation in decoding - The decoding process is performed by identifying the stacked shares using our visual system without any computational device.

5. Wide image format - The proposed scheme can be used to encrypt not only binary images but also gray-level or color images.

The rest of this paper is organized as follows. In Section 2, we review the traditional method of VSS by using random grids. Section 3 presents the proposed scheme with its security and reconstruction analysis. In Section 4, we demonstrate the feasibility of our scheme by experimental results and comparison with the related works. Finally, we conclude in Section 5.

2. Review of Traditional VSS by Random Grids

We discuss the basic characteristics of random grids and three basic algorithms based on random grids for $(2, 2)$-VSS [6], which are used as a function in constructing of our scheme.

A random grid is defined as a transparency comprising a two-dimensional array of pixels, where each pixel is either transparent (0) or opaque (1) chosen by a random process similar to a coin-flip procedure. For any pixel r belonging to a random grid, we have $Prob(r = 0) = Prob(r = 1) = \frac{1}{2}$. The transparent (white) pixels allow light to transmit through it, whereas the opaque (black) pixels stop the transmission of light. For a binary image A, we can find its average light transmission as follows.

Definition 2.1. (*Average light transmission [14]*) Let A be a binary image of size $h \times w$. For a pixel $a \in A$, the light transmission $t(a)$ of a is defined as the probability a to be transparent (i.e., $t(a) = Prob(a = 0)$). Therefore, $t(a) = 1$ if a is transparent, while $t(a) = 0$ if a is opaque. The average light transmission of A is defined as $T(A) = \frac{1}{h \times w} \sum_{i=1}^{h} \sum_{j=1}^{w} t(A[i, j])$.

If R is a random grid, then for any pixel $r \in R$, we have $Prob(r = 0) = \frac{1}{2}$, i.e., $t(r) = \frac{1}{2}$. Therefore, we obtain $T(R) = \frac{1}{2}$. The binary grid $\overline{R}$ can be defined as an inverse grid of a binary grid R of size $h \times w$, which is obtained by bitwise complementing of R, i.e., $\overline{R[i, j]} = 1 - R[i, j]$ for $1 \leq i \leq h$ and $1 \leq j \leq w$. If R is a random grid, then we obtain $T(\overline{R}) = \frac{1}{2}$.

Definition 2.2. (*Contrast [14]*) Let S denote a binary image, which is reconstructed for the original binary image A. The contrast of S is defined as $\alpha = \frac{T(S[A(0)]) - T(S[A(1)])}{1 + T(S[A(1)])}$, where $A(0)$ (resp. $A(1)$) denotes the area of all transparent (resp. opaque) pixels in A with $A = A(0) \cup A(1)$ and $A(0) \cap A(1) = \emptyset$. Further, $S[A(0)]$ (resp. $S[A(1)]$) denotes the area of pixels in S corresponding to $A(0)$ (resp. $A(1)$), i.e., the pixel s is in $S[A(0)]$ (resp. $S[A(1)]$) if and only if its corresponding pixel a is in $A(0)$ (resp. $(A(1))$.

Definition 2.3. (*Visual recoverability [3]*) For the contrast $\alpha > 0$, the reconstructed image S visually reveals the original image A. Precisely, $\alpha > 0$ implies $T(S[A(0)]) > T(S[A(1)])$, S is visually recognizable as A due to difference in the average light transmission. For $\alpha = 0$ (i.e. $T(S[A(0)]) = T(S[A(1)])$), S is meaningless and does not reveal any information about A.

Kafri and Keren [6] proposed a $(2,2)$-VSS scheme, in which a binary secret image is encrypted into two cipher grids such that individual cipher grid is random. However, the secret image can be reconstructed by stacking both the cipher grids together. They presented three different algorithms to encrypt a binary secret image into two cipher grids, which are regarded as Algorithms 1-3. Algorithm 1, 2 or 3 inputs a binary secret image A of size $h \times w$ and outputs the cipher grids R_1 and R_2 of size same as that of A. In each Algorithm 1, 2 or 3, cipher grid R_1 is generated randomly, i.e., $R_1[i,j] = random(0,1)$ for $1 \leq i \leq h$ and $1 \leq j \leq w$, where $random(0,1)$ is a function that returns a random value either 0 or 1 with an equal probability $\frac{1}{2}$. In Algorithms 1-3, the pixel at location $[i,j]$ $(1 \leq i \leq h, 1 \leq j \leq w)$ of the cipher grid R_2, i.e., $R_2[i,j]$ is computed based on the original image pixel $A[i,j]$ and cipher grid pixel $R_1[i,j]$ as follows.

In Algorithm 1

$$R_2[i,j] = \begin{cases} R_1[i,j] & \text{if } A[i,j] = 0, \\ \overline{R_1[i,j]} & \text{otherwise.} \end{cases} \tag{1}$$

In Algorithm 2

$$R_2[i,j] = \begin{cases} R_1[i,j] & \text{if } A[i,j] = 0, \\ random(0,1) & \text{otherwise.} \end{cases} \tag{2}$$

In Algorithm 3

$$R_2[i,j] = \begin{cases} random(0,1) & \text{if } A[i,j] = 0, \\ \overline{R_1[i,j]} & \text{otherwise.} \end{cases} \tag{3}$$

In Algorithms 1-3, both cipher grids R_1 and R_2 are random, i.e., $T(R_1) = T(R_2) = \frac{1}{2}$. As the human visual system can be simulated by Boolean OR operation ($\otimes$), an image reconstructed by stacking R_1 and R_2 can be represented by $R_1 \otimes R_2$. The visual quality of the reconstructed image varies in Algorithms 1-3 as the reconstructed image has the contrast equals to $\frac{1}{2}$, $\frac{1}{5}$ and $\frac{1}{4}$ in Algorithms 1, 2 and 3 respectively. Thus, the reconstructed image achieves the better visual quality in Algorithm 1.

3. The Proposed Scheme

We first propose the random-grid based (k,n)-RIVSS scheme for binary as well as color images. Then, we analyze our scheme for security and reconstruction properties.

To construct a general (k,n)-RIVSS scheme for any $2 \leq k \leq n$, we utilize the concept of the random-grid based image sharing. In our scheme, first the content of the input binary image A is partitioned into multiple regions and assigned a secrecy level to each region. As our scheme is a general (k,n)-RIVSS scheme, the image A is partitioned into $n-k+1$ regions of different secrecy levels. Let L_r denote r^{th} secrecy level for $1 \leq r \leq n-k+1$, where $L_1 < L_2 < ... < L_{n-k+1}$ (i.e., L_1 is the least significant and L_{n-k+1} is the most significant). Thus, each region can be assigned a secrecy level from levels $L_1, L_2, ..., L_{n-k+1}$ according to the dealer's specification for the particular degree of the secrecy of that region. Let L_0 denote the level of background of the image A, and A_r denote the region of the image A with level L_r, where $0 \leq r \leq n - k + 1$. If a pixel $A[i,j]$ belongs to the region A_1, then it can be reconstructed by any k or more shares. Similarly, a pixel $A[i,j]$ belonging to the region A_2 can be reconstructed by any $k+1$ or more shares. Thus, in general, at least $k + r - 1$ shares are required to reconstruct a pixel belonging to the region A_r, where $1 \leq r \leq n - k + 1$.

Before presenting our scheme, we define a function $RG : RG(x,y) \rightarrow z$ such that it inputs pixels x and y, and outputs pixel z. The function RG is selected based on Algorithm 1, 2 or 3 such that output pixel z is determined by Eq. (1), (2) or (3) respectively, where x acts the secret image pixel and y acts as the other random pixel. The procedure to encrypt a binary image A with multiple secrecy levels for (k,n)-threshold access structure is given in Algorithm 4, where $\oplus$ denotes the Boolean XOR operation.

Algorithm 4.

```
Step 1 For each pixel $A[i,j] \in A$ $(1 \leq i \leq h, 1 \leq j \leq w)$, do as follows:
Step 2 If $A[i,j] \in A_0$ then follow Step 3; else follow Steps 4 to 5.
Step 3 Generate the pixel value at location $[i,j]$ of each share randomly, i.e., $R_l[i,j] = random(0,1)$
    for $1 \leq l \leq n$.
Step 4 Randomly select $k+r-1$ shares $R_{i_1}, R_{i_2}, \ldots, R_{i_{k+r-1}}$ from $n$ shares and generate the pixel
    values at location $[i,j]$ of these shares.
    Step 4.1 Generate $k+r-2$ binary values $a_1, a_2, \ldots, a_{k+r-2}$ randomly, i.e., $a_l = random(0,1)$
        for $1 \leq l \leq k+r-2$.
    Step 4.2 Generate $k+r-1$ pixel values as follows:
        for $(1 \leq l \leq k+r-2)$
        {
            $R_{i_l}[i,j] = a_l$
        }
        $R_{i_{k+r-1}}[i,j] = RG(A_r[i,j], a_1 \oplus ... \oplus a_{k+r-2})$.
Step 5 Generate the pixel values at location $[i,j]$ of the remaining $(n-k-r+1)$ shares as $R_l[i,j] =$
    $random(0,1)$, where $R_l \in \{R_1, ..., R_n\} \setminus \{R_{i_1}, ..., R_{i_{k+r-1}}\}$.
Step 6 output $(R_1, R_2, \ldots, R_n)$.
```

Figure 1 shows the diagram of encoding process of our scheme. The proposed scheme for binary images can be easily extended to color images. Similar to method for binary images, first the content of the color image is partitioned into multiple regions of different secrecy levels. Then, the color image is decomposed into three components by using either additive (RGB) or subtractive (CMY) color model. The secrecy level of a particular region after color decomposition will remain same in each of three color components. The procedure given in Algorithm 5 can be adopted to encrypt a color image B with multiple secrecy levels.

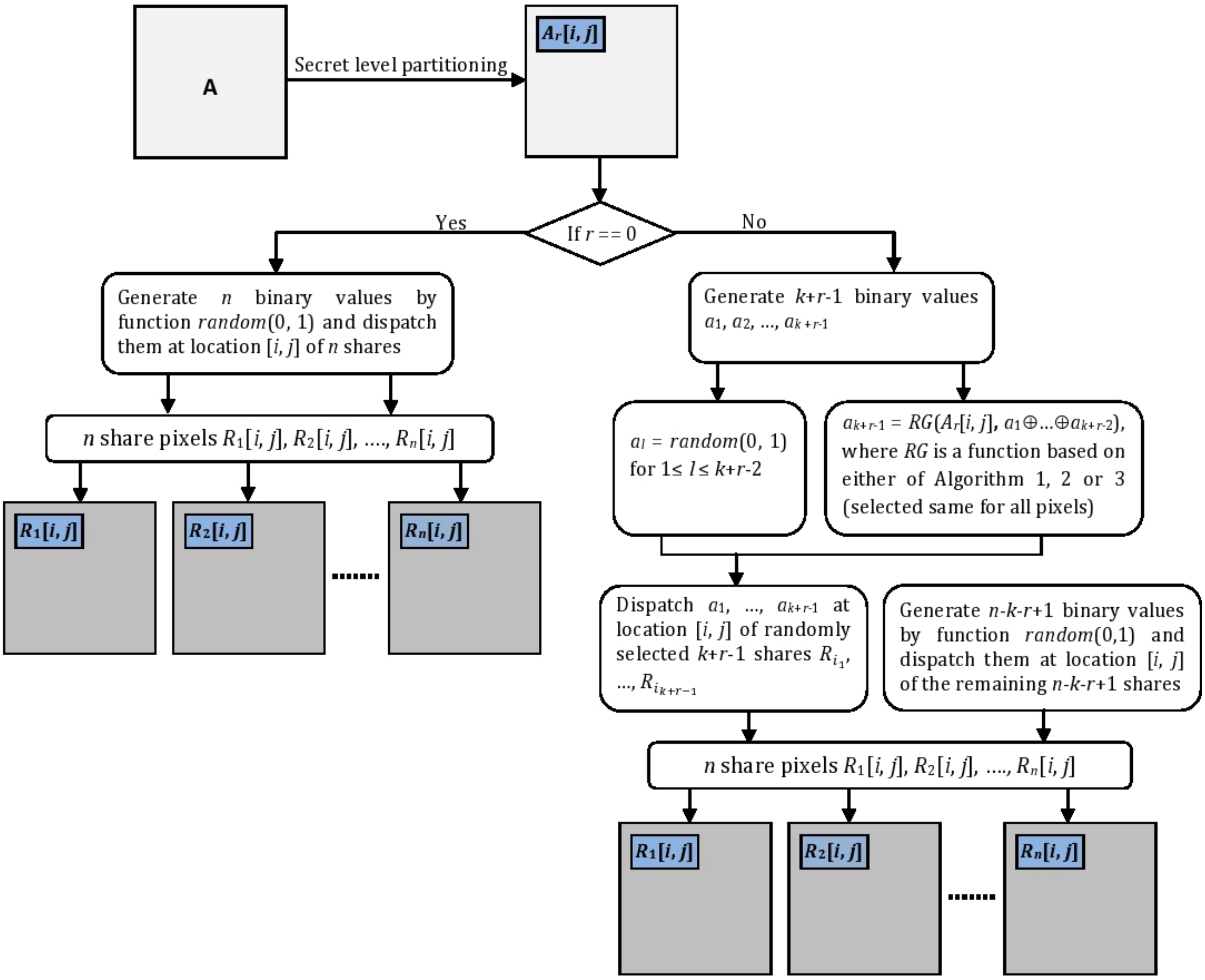

A
Secret level partitioning
Ar[i, j]
If r == 0
Yes
No
Generate n binary values by function random(0, 1) and dispatch them at location [i, j] of n shares
n share pixels R1[i, j], R2[i, j], ..., Rn[i, j]
R1[i, j]
R2[i, j]
....
Rn[i, j]
Generate k+r-1 binary values a1, a2, ..., ak+r-1
al = random(0, 1) for 1≤ l ≤ k+r-2
ak+r-1 = RG(Ar[i, j], a1⊕...⊕ak+r-2), where RG is a function based on either of Algorithm 1, 2 or 3 (selected same for all pixels)
Dispatch a1, ..., ak+r-1 at location [i, j] of randomly selected k+r-1 shares Ri1, ..., Rik+r−1
Generate n-k-r+1 binary values by function random(0,1) and dispatch them at location [i, j] of the remaining n-k-r+1 shares
n share pixels R1[i, j], R2[i, j], ..., Rn[i, j]
R1[i, j]
R2[i, j]
....
Rn[i, j]

Figure 1. The diagram of encoding process of the proposed (k, n)-RIVSS scheme.

Algorithm 5.

Step 1 Decompose the color secret image B into three color components Cyan, Magenta and Yellow (CMY), i.e., B^C, B^M and B^Y.

Step 2 Transform color components B^C, B^M and B^Y into halftone images, i.e., HB^C, HB^M and HB^Y by halftone techniques [19, 11, 18].

Step 3 For each of halftone (binary) images HB^C, HB^M and HB^Y, generate n shares by Algorithm 4, i.e., R_l^C, R_l^M and R_l^Y for $1 \leq l \leq n$.

Step 4 Combine color components of R_l^C, R_l^M and R_l^Y to form eight color share R_l, i.e., $R_l = (R_l^C, R_l^M, R_l^Y)$ for $1 \leq l \leq n$.

Step 5 output $(R_1, R_2, ..., R_n)$.

3.1. Security and Reconstruction Analysis

We analyze our scheme for security of secret regions against any unqualified set, and ability to reconstruct the secret regions for any qualified set. We prove that our scheme is secure, i.e., any $k + r - 2$ or fewer shares cannot obtain any information about the region of the secrecy level L_r, where $r \in \{1, 2, ..., n - k + 1\}$. We also prove that our scheme has reconstruction ability, i.e., any $k + r - 1$ or more shares can reconstruct the secret pixels up to secrecy levels L_r. In our scheme, the generated shares depend upon Algorithm (function RG) selected based on either of Algorithm 1, 2 or 3. Since Algorithm 1 achieves the best visual quality among all there algorithms, we choose Algorithm 1 as the core to analyze the performance of our scheme. Therefore, we have

$$z = RG(x, y) = \begin{cases} y & \text{if } x = 0, \\ \overline{y} & \text{otherwise}. \end{cases} \tag{4}$$

The subsequent reasoning and inferences, which we will obtain from analyzing Algorithm 4 based on Algorithm 1 can also be easily applied to obtain the results based on Algorithms 2 and 3.

Lemma 3.1. If $r_1, r_2, ..., r_n$ are n pixels generated by function $random(0, 1)$, then $Prob(r_1 \otimes r_2 \otimes ... \otimes r_n = 0) = \frac{1}{2^n}$.

Lemma 3.2. If $r_1, r_2, ..., r_n$ are n pixels generated each by function $random(0, 1)$, then $Prob(r_1 \oplus r_2 \oplus ... \oplus r_n = 0) = \frac{1}{2}$.

The proofs of Lemmas 3.1 and 3.2 are easy to understand as a straight consequence of independence, and can be referred from [15] and [10] respectively.

Theorem 3.3. In the proposed (k, n)-RIVSS scheme, each share is meaningless and does not reveal any information about the image A.

Proof:
In the proposed scheme, each pixel $A_r[i, j] \in A$ is encrypted corresponding to its level L_r, where $r \in \{0, 1, ..., n - k + 1\}$. We consider two cases. Case 1 is $r = 0$, and Case 2 is $r \neq 0$.

Case 1: In this case, the pixel $A_0[i, j]$ belongs to the background region and its corresponding share pixel $R_l[i, j]$ $(1 \leq l \leq n)$ is generated by function $random(0, 1)$. Therefore, for $A_0[i, j] = 0$ or 1, we obtain

$$Prob(R_l[i, j] = 0) = \tfrac{1}{2},$$

where $1 \leq l \leq n$.

Case 2: In this case, the pixel values at location $[i, j]$ of $k + r - 2$ shares $R_{i_1}, R_{i_2}, \ldots, R_{i_{k+r-2}}$ are generated by assigning randomly generated $a_1, a_2, ..., a_{k+r-2}$ respectively. For $A_r[i, j] = 0$ or 1, we obtain

$$Prob(R_l[i, j] = 0) = \tfrac{1}{2},$$

where $1 \leq l \leq k + r - 2$.

We know that $R_{i_{k+r-1}}[i,j] = RG(A_r[i,j], a_1 \oplus ... \oplus a_{k+r-2})$. From Eq. (4), if $A_r[i,j] = 0$ then $R_{i_{k+r-1}}[i,j] = a_1 \oplus ... \oplus a_{k+r-2}$, else $R_{i_{k+r-1}}[i,j] = \overline{a_1 \oplus ... \oplus a_{k+r-2}}$. As $a_1, ..., a_{k+r-2}$ are random values, by Lemma 3.2, $Prob(a_1 \oplus ... \oplus a_{k+r-2} = 0) = \frac{1}{2}$. For $A_r[i,j] = 0$ or 1, we obtain

$$Prob(R_{i_{k+r-1}}[i,j] = 0) = \tfrac{1}{2}.$$

In addition, the pixel value at location $[i,j]$ of any share $R_l \in \{R_1, ..., R_n\} \setminus \{R_{i_1}, ..., R_{i_{k+r-1}}\}$ is generated by function $random(0,1)$. Therefore, for $A_r[i,j] = 0$ or 1, we have $Prob(R_l[i,j] = 0) = \frac{1}{2}$.

By considering both cases ($r = 0$ and $r \neq 0$), no matter if $A[i,j] = 0$ or 1, for each share R_l ($1 \leq l \leq n$), we obtain $Prob(R_l[i,j] = 0) = \frac{1}{2}$, i.e, $t(R_l[i,j]) = \frac{1}{2}$. Therefore,

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

where $1 \leq l \leq n$. Hence, by Definition 2.3, each share is meaningless and reveals no information about A. □

Theorem 3.4. In the proposed (k,n)-RIVSS scheme, image obtained by stacking any $k+r-2$ or fewer shares reveals no information about the region of the secrecy level L_r, where $r \in \{1, 2, ..., n-k+1\}$.

Proof:
Let S denote the image obtained by stacking of any t shares $R_{q_1}, R_{q_2}, ..., R_{q_t}$, where $t \leq k+r-2$. Therefore,

$$S[i,j] = R_{q_1}[i,j] \otimes ... \otimes R_{q_t}[i,j],$$

where $1 \leq i \leq h$ and $1 \leq j \leq w$. Let $D_1 = \{R_{i_1}, ..., R_{i_{k+r-1}}\}$ and $D_2 = \{R_{q_1}, ..., R_{q_t}\}$, where D_1 is generated as in Step 4 of Algorithm 4. We consider two cases. Case 1 is $D_1 \cap D_2 \neq \emptyset$, and Case 2 is $D_1 \cap D_2 = \emptyset$.

Case 1: Let $F = D_1 \cap D_2 = \{R_{x_1}, ..., R_{x_u}\}$ and $\{R_{y_1}, ..., R_{y_{t-u}}\} = D_2 \setminus F$. Since $R_{i_{k+r-1}} \in D_1$ and $F \subset D_1$, we have either $R_{i_{k+r-1}} \notin F$ or $R_{i_{k+r-1}} \in F$.

If $R_{i_{k+r-1}} \notin F$ then $\{R_{x_1}[i,j], ..., R_{x_u}[i,j]\} \subseteq \{a_1, ..., a_{k+r-2}\}$. Each of $a_1, ..., a_{k+r-2}$ is generated by $random(0,1)$. By Lemma 3.1,

$$Prob(R_{x_1}[i,j] \otimes ... \otimes R_{x_u}[i,j] = 0) = \tfrac{1}{2^u}.$$

If $R_{i_{k+r-1}} \in F$, then consider $R_{i_{k+r-1}} = R_{x_v}$ for some $v \in \{1, ..., u\}$. Therefore, the pixel at location $[i,j]$ of each of the shares other than R_{x_v}, belonging to F, is generated by function $random(0,1)$. If $F_1 = F \setminus \{R_{x_v}\} = \{R_{z_1}, \ldots, R_{z_{u-1}}\}$, then by Lemma 3.1

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

We know that $R_{z_1}[i,j] \otimes \ldots \otimes R_{z_{v-1}}[i,j]$ will be transparent (0) only if

$$R_{z_1}[i,j] = R_{z_2}[i,j] = \ldots\ldots = R_{z_{v-1}}[i,j] = 0.$$

Thus, the pixel $R_{i_{k+r-1}}[i,j]$ will depend on XOR of the remaining random pixels belong to the set $\{a_1,...,a_{k+r-2}\} \setminus F_1$. By using Lemma 3.2, we obtain

$$Prob(R_{i_{k+r-1}}[i,j]=0)=\frac{1}{2}.$$

Therefore, we obtain

$$Prob(R_{x_1}[i,j]\otimes..\otimes R_{x_u}[i,j]=0)=\frac{1}{2^{u-1}}\times\frac{1}{2}=\frac{1}{2^u}.$$

In addition, the pixel at any location $[i,j]$ of each of the shares R_{y_1}, ..., $R_{y_{t-u}}$ is generated by function $random(0,1)$. By Lemma 3.1,

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

Thus, for $A_r[i,j]=0$ or 1, we obtain

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

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

$$T(S[A_r(0)])=T(S[A_r(1)])=\frac{1}{2^t}. \tag{5}$$

Case 2: In this case, each of the pixels $R_{q_1}[i,j],...,R_{q_t}[i,j]$ is generated by function $random(0,1)$. By Lemma 3.1, for $A_r[i,j]=0$ or 1, $Prob(S[i,j]=0)=Prob(R_{q_1}[i,j]\otimes...\otimes R_{q_t}[i,j]=0)=\frac{1}{2^t}$, i.e, $t(S[i,j])=\frac{1}{2^t}$. Therefore,

$$T(S[A_r(0)])=T(S[A_r(1)])=\frac{1}{2^t}. \tag{6}$$

By considering both cases (5) and (6), for any pixel belonging to the region A_r, we obtain $T(S[A_r(0)])=T(S[A_r(1)])$, i.e., $\alpha=0$. In addition, for each pixel $A_0[i,j]$, belonging to the background, the pixels of each share are generated by function $random(0,1)$. For $A_0[i,j]=0$ or 1, we have $Prob(S[i,j]=0)=\frac{1}{2^t}$, i.e, $t(S[i,j])=\frac{1}{2^t}$. For each pixel of background, we obtain $T(S[A_0(0)])=T(S[A_0(1)])$, i.e., $\alpha=0$.

Thus, there is no difference in the average light transmission of the region A_r and the background A_0 in S. Consequently, the image S obtained by stacking of any t $(\leq k+r-2)$ shares is meaningless and gives no clue about the region of the secrecy level L_r. □

Theorem 3.5. In the proposed (k,n)-RIVSS scheme, a region of the secrecy level L_r can be reconstructed by stacking any $k+r-1$ or more shares, where $r\in\{1,2,...,n-k+1\}$.

Proof:
Let S denote the image obtained by stacking any t shares $R_{q_1},R_{q_2},...,R_{q_t}$, where $t\geq k+r-1$. Therefore,

$$S[i,j]=R_{q_1}[i,j]\otimes...\otimes R_{q_t}[i,j],$$

where $1\leq i\leq h$ and $1\leq j\leq w$. For t shares $(R_{q_1},R_{q_2},...,R_{q_t})$, β shares are selected from $k+r-1$ shares generated as in Step 4 and γ shares are selected from $n-k-r+1$ shares generated as in Step 5, where $\beta+\gamma=t$. We consider two cases. Case 1 is $\beta<k+r-1$ and $\gamma=t-\beta$. Case 2 is $\beta=k+r-1$

and $\gamma = t - \beta$. In Case 2, we have

$$Prob(\beta = k + r - 1) = \frac{\binom{t}{k+r-1}}{\binom{n}{k+r-1}}.$$

In Case 1, we have

$$Prob(\beta < k + r - 1) = 1 - \frac{\binom{t}{k+r-1}}{\binom{n}{k+r-1}}.$$

Case 1: In this case, the pixel at any location $[i, j]$ of each of the shares $R_{q_1}, ..., R_{q_t}$ is generated by function $random(0, 1)$. By Lemma 3.1, for $A_r[i, j] = 0$ or 1, we obtain

$$Prob(S[i, j] = 0) = \tfrac{1}{2^t}. \tag{7}$$

Case 2: Let $\{q_1, ..., q_t\} = \{i_1, ..., i_\beta\} \cup \{z_1, ..., z_\gamma\}$. The pixel at any location $[i, j]$ of shares $R_{z_1}, \ldots, R_{z_\gamma}$ is generated by function $random(0, 1)$. Therefore,

$$Prob(R_{z_1}[i, j] \otimes ... \otimes R_{z_\gamma}[i, j] = 0) = \tfrac{1}{2^\gamma}. \tag{8}$$

The pixels $R_{i_1}[i, j], \ldots, R_{i_\beta}[i, j]$ are generated as in Step 4 of the proposed scheme, i.e, $R_{i_1}[i, j] = a_1, \ldots, R_{i_\beta}[i, j] = a_\beta$, where $\beta = k + r - 1$. From Step 4, we can observe that the pixel values $R_{i_1}[i, j], \ldots, R_{i_{\beta-1}}[i, j]$ are generated by function $random(0, 1)$. By Lemma 3.1, for $A_r[i, j] = 0$ or 1, we have

$$Prob(R_{i_1}[i, j] \otimes ... \otimes R_{i_{\beta-1}}[i, j] = 0) = \tfrac{1}{2^{\beta-1}}.$$

We know that $R_{i_1}[i, j] \otimes ... \otimes R_{i_{\beta-1}}[i, j]$ will be transparent only if

$$R_{i_1}[i, j] = ... = R_{i_{\beta-1}}[i, j] = 0.$$

From Eq. (4), if $A_r[i, j] = 0$ then $R_{i_\beta}[i, j] = R_{i_1}[i, j] \oplus ... \oplus R_{i_{\beta-1}}[i, j] = 0$, i.e., $Prob(R_{i_\beta}[i, j] = 0) = 1$. We obtain,

$$\begin{aligned} Prob(R_{i_1}[i, j] \otimes ... \otimes R_{i_\beta}[i, j] = 0) &= \tfrac{1}{2^{\beta-1}} \times 1 \\ &= \tfrac{1}{2^{\beta-1}}. \end{aligned} \tag{9}$$

For $A_r[i, j] = 0$, from Eqs. (8) and (9), we obtain

$$Prob(S[i, j] = 0) = \tfrac{1}{2^{\beta-1}} \times \tfrac{1}{2^\gamma} = \tfrac{1}{2^{t-1}}. \tag{10}$$

From Eq. (4), if $A_r[i, j] = 1$ then $R_{i_\beta}[i, j] = \overline{R_{i_1}[i, j] \oplus ... \oplus R_{i_{\beta-1}}[i, j]} = 1$, i.e., $Prob(R_{i_\beta}[i, j] = 0) = 0$. We obtain,

$$\begin{aligned} Prob(R_{i_1}[i, j] \otimes ... \otimes R_{i_\beta}[i, j] = 0) &= \tfrac{1}{2^{\beta-1}} \times 0 \\ &= 0. \end{aligned} \tag{11}$$

For $A_r[i, j] = 1$, from Eqs. (8) and (11), we obtain

$$Prob(S[i, j] = 0) = \tfrac{1}{2^\gamma} \times 0 = 0. \tag{12}$$

By considering both cases (7) and (10), for $A_r[i, j] = 0$, we have $Prob(S[i, j] = 0) = \left(1 - \frac{\binom{t}{k+r-1}}{\binom{n}{k+r-1}}\right) \times \frac{1}{2^t} + \frac{\binom{t}{k+r-1}}{\binom{n}{k+r-1}} \times \frac{1}{2^{t-1}} = \left(1 + \frac{\binom{t}{k+r-1}}{\binom{n}{k+r-1}}\right) \times \frac{1}{2^t}$, i.e, $t(S[i, j]) = \left(1 + \frac{\binom{t}{k+r-1}}{\binom{n}{k+r-1}}\right) \times \frac{1}{2^t}$.

Therefore,

$$T(S[A_r(0)]) = \left(1 + \frac{\binom{t}{k+r-1}}{\binom{n}{k+r-1}}\right) \times \frac{1}{2^t}.$$

By considering both cases (7) and (12), for $A_r[i,j] = 1$, we have $Prob(S[i,j] = 0) = \left(1 - \frac{\binom{t}{k+r-1}}{\binom{n}{k+r-1}}\right) \times \frac{1}{2^t} + \frac{\binom{t}{k+r-1}}{\binom{n}{k+r-1}} \times 0 = \left(1 - \frac{\binom{t}{k+r-1}}{\binom{n}{k+r-1}}\right) \times \frac{1}{2^t}$, i.e., $t(S[i,j]) = \left(1 - \frac{\binom{t}{k+r-1}}{\binom{n}{k+r-1}}\right) \times \frac{1}{2^t}$. Therefore,

$$T(S[A_r(1)]) = \left(1 - \frac{\binom{t}{k+r-1}}{\binom{n}{k+r-1}}\right) \times \frac{1}{2^t}.$$

For each pixel $A_0[i,j]$ belonging to the background, the pixels of each share are generated by function $random(0,1)$. For $A_0[i,j] = 0$ or 1, we obtain $Prob(S[i,j] = 0) = \frac{1}{2^t}$, i.e, $t(S[i,j]) = \frac{1}{2^t}$. For each pixel of background, we obtain $T(S[A_0(0)]) = T(S[A_0(1)]) = \frac{1}{2^t}, i.e., \alpha = 0$.

Thus, the contrast of the region A_r relative to background A_0 is $\alpha = \frac{T(S[A_r(0)])-T(S[A_r(1)])}{1+T(S[A_r(1)])} = \frac{\left(1+\frac{\binom{t}{k+r-1}}{\binom{n}{k+r-1}}\right)\times\frac{1}{2^t}-\left(1-\frac{\binom{t}{k+r-1}}{\binom{n}{k+r-1}}\right)\times\frac{1}{2^t}}{1+\left(1-\frac{\binom{t}{k+r-1}}{\binom{n}{k+r-1}}\right)\times\frac{1}{2^t}} = \frac{2\times\binom{t}{k+r-1}}{(2^t+1)\times\binom{n}{k+r-1}-\binom{t}{k+r-1}}$.

Consequently, we obtain $\alpha > 0$, i.e., the image obtained by stacking any t $(\geq k+r-1)$ shares reconstructs the region of the secrecy level L_r. □

In our (k,n)-RIVSS scheme, we have proved that a particular region of the secrecy level L_r can only be reconstructed by stacking any $k+r-1$ or more shares. While we stack any t $(\geq k)$ shares, the resultant image reconstructs the regions of secrecy levels from L_1 to L_{t-k+1}. For example, in a $(3,5)$-RIVSS scheme, where $k=3$ and $n=5$, we have 3 $(= n-k+1)$ regions of secrecy levels L_1, L_2 and L_3. Whenever any 3 $(= t)$ shares are stacked, it reconstructs the region of the secrecy level L_1. By stacking any 4 shares, the regions of secrecy levels L_1 and L_2 are reconstructed. All three secret regions (levels L_1, L_2 and L_3) can be reconstructed by stacking all 5 shares.

4. Experimental and Comparison Results

We first conduct three experiments to verify the feasibility of our scheme. Then, we show the superiority of our scheme by comparing it with the related works.

4.1. Experiment 1

This experiment is conducted for a $(2,3)$-RIVSS scheme with a binary image shown in Figure 2(a). The binary image is partitioned into two secret regions of levels 1 and 2, where the level 1 region consists the text “VISUAL” and the level 2 region consists the text “SECRET”. Figures 2(b)-(d) show the three shares generated by our scheme, where each share has the size same as that of the original image and gives no clue about the original image. The stacked images obtained by any two shares reveals the level 1 secret “VISUAL” as shown in Figures 2(e)-(g). The level 1 secret “VISUAL” and level 2 secret “SECRET” can be visually recognized by stacking all three shares (see Figure 2(h)).

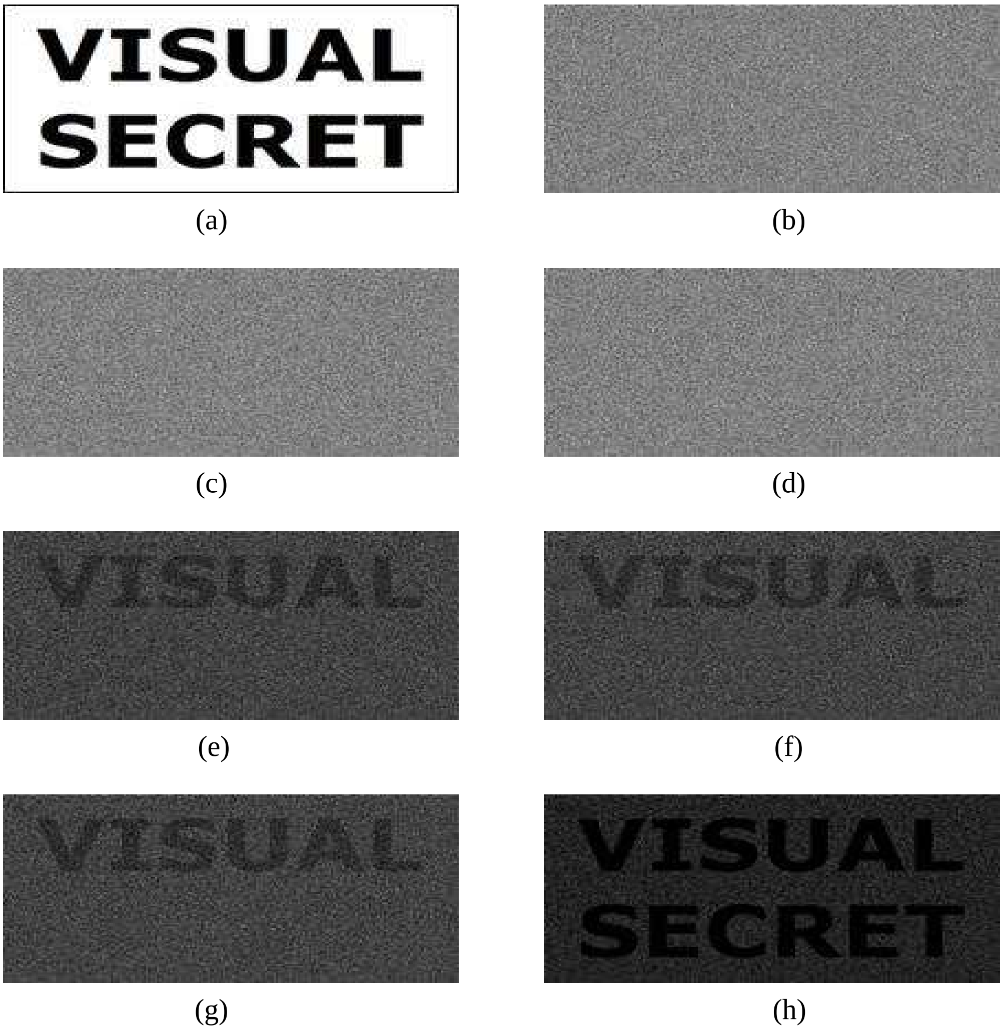
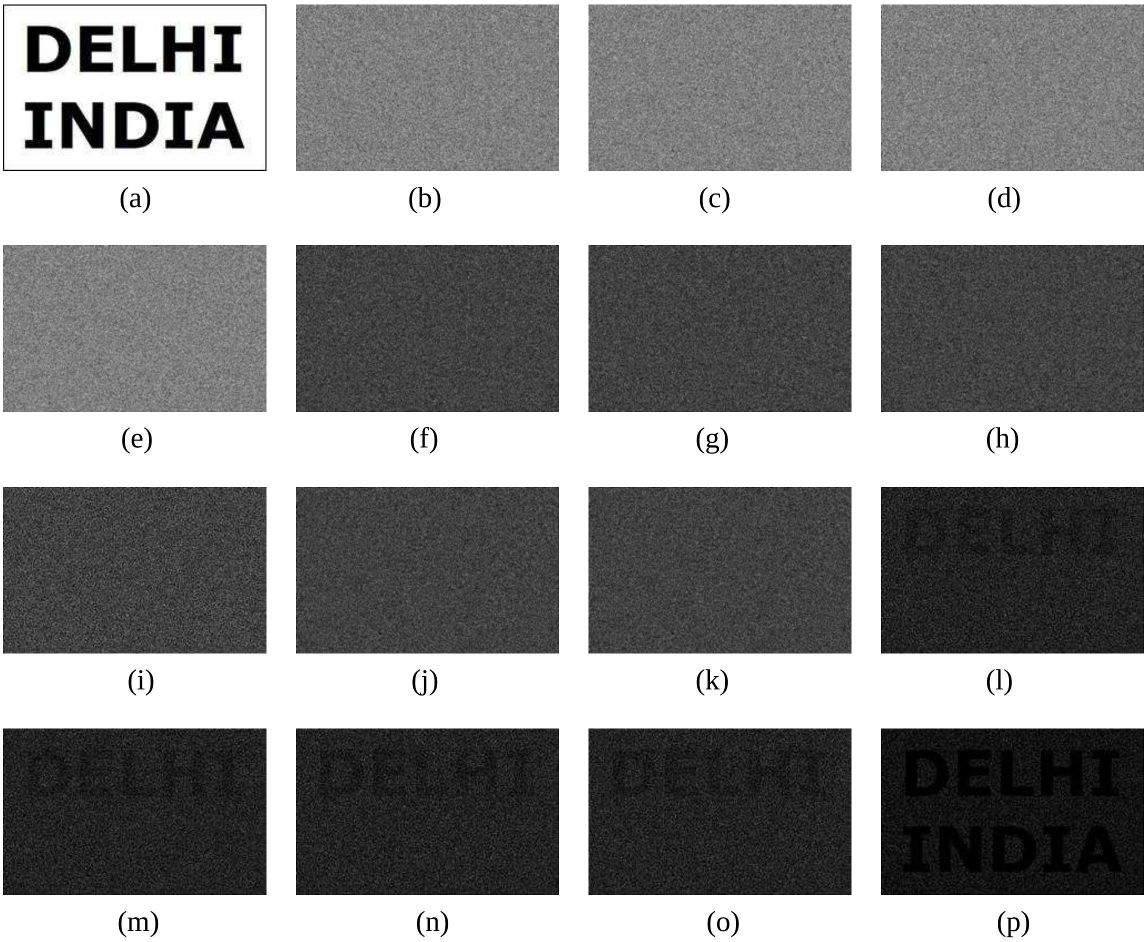


Figure 2. The experimental results of random-grid based $(2, 3)$-RIVSS scheme: (a) Binary image; (b) R_1; (c) R_2; (d) R_3; (e) $R_1 \otimes R_2$; (f) $R_1 \otimes R_3$; (g) $R_2 \otimes R_3$; (h) $R_1 \otimes R_2 \otimes R_3$.

4.2. Experiment 2

We conduct this experiment for a $(3, 4)$-RIVSS scheme with a binary image shown in Figure 3(a). The secret level decomposition partitions the binary image into two secrecy levels, where levels 1 and 2 consist the secrets “DELHI” and “INDIA” respectively. The four shares generated by our scheme are shown in Figures 3(b)-(e), where each share is meaningless image with the size same as that of the original image. The stacking results (see Figures 3(f)-(k)) of any two shares are also meaningless and reveal no secret information. The images obtained by stacking any three shares reconstruct the level 1 secret “DELHI” as shown in Figures 3(l)-(o). By stacking all four shares, we can reconstruct the level 1 secret “DELHI” and the level 2 secret “INDIA” as shown in Figure 3(p).



(a) (b) (c) (d)

(e) (f) (g) (h)

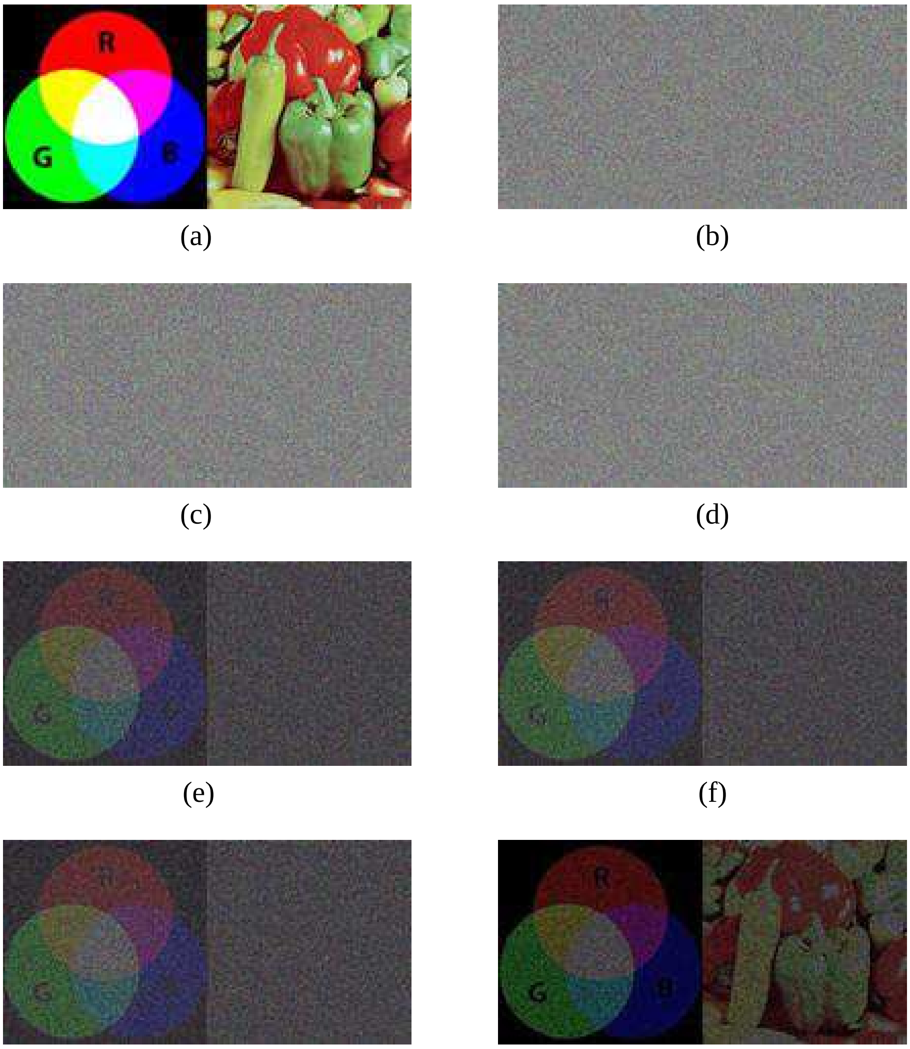
(i) (j) (k) (l)

(m) (n) (o) (p)

Figure 3. The experimental results of random-grid based $(3, 4)$-RIVSS scheme: (a) Binary image; (b) R_1; (c) R_2; (d) R_3; (e) 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) $R_1 \otimes R_2 \otimes R_3 \otimes R_4$.

4.3. Experiment 3

This experiment is conducted for a $(2, 3)$-RIVSS scheme with a color image consisting two secret images "RGB color model" and "Capsicum" as shown in Figure 4(a). The original image is decomposed into two secrecy levels, where "RGB color model" image is the level 1 secret and "Capsicum" image is the level 2 secret. Each share (see Figures 4(b)-(d)) generated by our scheme is meaningless and reveals no information about the original image. While we stack any two shares, the level 1 secret "RGB color model" image is reconstructed as shown in Figures 4(e)-(g). By stacking all three shares, both secret images "RGB color model" (level 1) and "Capsicum" (level 2) can be reconstructed as shown in see Figure 4(h).



(a) (b)

(c) (d)

(e) (f)

(g) (h)

Figure 4. The experimental results of random-grid based $(2,3)$-RIVSS scheme: (a) Color image; (b) R_1; (c) R_2; (d) R_3; (e) $R_1 \otimes R_2$; (f) $R_1 \otimes R_3$; (g) $R_2 \otimes R_3$; (h) $R_1 \otimes R_2 \otimes R_3$.

4.4. Comparison with the Related Works

We compare the efficiency of our scheme with similar schemes having property of either region incrementing or threshold sharing, i.e., Zhong and Wang's scheme [25], Wang's scheme [21], Shyu's scheme [17], Yang et al.'s scheme [24], and Chen and Tsao's scheme [4]. Zhong and Wang [25] have used Chen and Tsao's scheme [4] as a basis to construct their random-grid based RIVSS, where Chen and Tsao's scheme has the property of threshold sharing but lacks region incrementing. In [25], a secret image is shared by constructing the component shares for each of the secrecy level using [4] and then by OR of the component shares belonging to each individual secrecy level to obtain final shares. Compared to [25], the proposed scheme has advantage that it can share a secret image with multiple secrecy levels by using the various (k, n)-threshold access structures. For example, a secret image with 4 different secrecy levels can be shared by using the various threshold access structures such as $(2, 5)$, $(3, 6)$, $(5, 8)$, etc. Whereas, Zhong and Wang's scheme has to be fixed to $(2, n)$-threshold access structure only, i.e., $(2, 5)$-threshold for the given example. Let a secret image with l different secrecy levels is shared by using our scheme and Zhong and Wang's scheme with $(2, l + 1)$-threshold. Let α^r_{ours} and α^r_{ZW} denote the contrast of images reconstructed corresponding to the region of secrecy level r ($1 \leq r \leq l$) using any t ($\geq r + 1$) shares in our scheme and Zhong and Wang's scheme [25] respectively. Then

$$\alpha^r_{ZW} = \frac{\left(\frac{\binom{t}{r+1}}{\binom{l+1}{r+1}}\right) \times \frac{1}{2^{t-1}} \times LT}{1 + \left(1 - \frac{\binom{t}{r+1}}{\binom{l+1}{r+1}}\right) \times \frac{1}{2^t} \times LT},$$

where LT is product of the average light transmission of the stacked result corresponding to the background regions of the secrecy levels other than r, i.e., $LT < 1$. We have

$$\alpha^r_{ours} = \frac{\left(\frac{\binom{t}{r+1}}{\binom{l+1}{r+1}}\right) \times \frac{1}{2^{t-1}}}{1 + \left(1 - \frac{\binom{t}{r+1}}{\binom{l+1}{r+1}}\right) \times \frac{1}{2^t}}.$$

We obtain $\alpha^r_{ours} - \alpha^r_{ZW} > 0$, i.e., $\alpha^r_{ours} > \alpha^r_{ZW}$. Thus, the proposed scheme achieves the higher visual quality of the reconstructed image than Zhong and Wang's scheme. Table 1 shows the comparison of our scheme with other schemes for the contrast of regions of different secrecy levels, where the asterisk (*) denotes the better contrast. It is observed that our scheme can achieve better contrast compared to schemes [21, 17, 24, 4]. It means that the secret regions can be reconstructed with better visual quality so that these can be recognized easily.

Table 1. Comparison of the contrast of different secrecy levels.

Scheme	Number of the stacked shares	Contrast of the secrecy levels														
		Wang's scheme [21]			Shyu's scheme [17]			Yang et al.'s scheme [24]			Chen and Tsao' s scheme [4]			Ours		
		1^{st}	2^{nd}	3^{rd}	1^{st}	2^{nd}	3^{rd}	1^{st}	2^{nd}	3^{rd}	1^{st}	2^{nd}	3^{rd}	1^{st}	2^{nd}	3^{rd}
$(2, 3)$	2	$\frac{1}{4}^*$	–	–	$\frac{1}{4}$	–	–	$\frac{1}{6}$	–	–	$\frac{1}{7}$	–	–	$\frac{1}{7}$	–	–
	3	$\frac{1}{4}$	$\frac{1}{4}$	–	$\frac{1}{2}^*$	$\frac{1}{4}$	–	$\frac{1}{3}$	$\frac{1}{6}$	–	$\frac{1}{4}$	–	–	$\frac{1}{4}$	$\frac{1}{4}^*$	–
$(2, 4)$	2	$\frac{1}{5}^*$	–	–	$\frac{1}{5}$	–	–	$\frac{1}{7}$	–	–	$\frac{2}{29}$	–	–	$\frac{2}{29}$	–	–
	3	$\frac{3}{10}^*$	$\frac{1}{10}$	–	$\frac{3}{10}$	$\frac{1}{10}$		$\frac{3}{14}$	$\frac{1}{14}$	–	$\frac{2}{17}$	–	–	$\frac{2}{17}$	$\frac{1}{8}^*$	–
	4	$\frac{3}{10}$	$\frac{1}{10}$	$\frac{1}{10}$	$\frac{2}{5}^*$	$\frac{1}{5}^*$	$\frac{1}{10}$	$\frac{2}{7}$	$\frac{1}{7}$	$\frac{1}{14}$	$\frac{1}{8}$	–	–	$\frac{1}{8}$	$\frac{1}{8}$	$\frac{1}{8}^*$
$(3, 4)$	3	–	–	–	–	–	–	$\frac{1}{13}^*$	–	–	$\frac{2}{35}$	–	–	$\frac{2}{35}$	–	–
	4	–	–	–	–	–	–	$\frac{2}{13}^*$	$\frac{1}{13}$	–	$\frac{1}{8}$	–	–	$\frac{1}{8}$	$\frac{1}{8}^*$	–
$(4, 5)$	4	–	–	–	–	–	–	$\frac{1}{20}^*$	–	–	$\frac{1}{42}$	–	–	$\frac{1}{42}$	–	–
	5	–	–	–	–	–	–	$\frac{3}{20}^*$	$\frac{1}{20}$	–	$\frac{1}{16}$	–	–	$\frac{1}{16}$	$\frac{1}{16}^*$	–

In Table 2, we highlight the pixel expansion resulted in our scheme and the related schemes [21, 17, 24]. It can be easily noted that the pixel expansion in [21, 17, 24] grows rapidly as n increases or the size of threshold access structure increases. It limits the application of these schemes in sharing small levels of secrets only. While in our scheme, the pixel expansion is no more dependent to n and is always one, i.e., the size of each share is same as that of the original image. Thus, the proposed scheme completely solves the problem of pixel minimization, mentioned in [21, 17, 24], keeping the property of region incrementing.

Table 2. Comparison of the pixel expansion.

Scheme	Pixel expansion			
	Wang's scheme [21]	Shyu's scheme [17]	Yang et al.'s scheme [24]	Ours
$(2,3)$	4	4	6	1
$(2,4)$	10	10	14	1
$(2,5)$	23	20	22	1
$(2,6)$	–	46	–	1
$(2,7)$	–	97	–	1
$(2,8)$	–	223	–	1
$(3,4)$	–	–	13	1
$(3,5)$	–	–	20	1
$(4,5)$	–	–	20	1

Table 3 shows the comparison of our scheme with the related VSS schemes in terms of performance factors such as encoding method, type, region incrementing, pixel expansion, codebook requirement, and secret image format. Compared to the related VSS schemes [12, 6, 15, 4], the proposed scheme

Table 3. Comparison of the proposed scheme with the related VSS schemes.

Scheme	Encoding based on	Type	Region incrementing	Pixel expansion	Codebook requirement	Secret image format
Naor and Shamir [12]	Basis matrices	(k,n)	No	Yes	Yes	Binary
Kafri and Keren [6]	Random-grid	$(2,2)$	No	No	No	Binary
Shyu [15]	Random-grid	(n,n)	No	No	No	Binary and Color
Chen and Tsao [4]	Random-grid	(k,n)	No	No	No	Binary and Color
Wang [21]	Basis matrices	$(2,n)$	Yes	Yes	Yes	Binary
Shyu [17]	Basis matrices	$(2,n)$	Yes	Yes	Yes	Binary
Yang et al. [24]	Basis matrices	(k,n)	Yes	Yes	Yes	Binary
Wang et al. [22]	Random-grid	$(2,3)$	Yes	No	No	Binary
Zhong and Wang [25]	Random-grid	$(2,n)$	Yes	No	No	Binary
Ours	Random-grid	(k,n)	Yes	No	No	Binary and Color

has the nice property of region incrementing. Wang's scheme [21] and Shyu's scheme [17] have the property of region incrementing in visual cryptography but both are suitable only for $(2, n)$ case, where [21] has reported the construction for small values of $n = 2, 3, 4$. Yang et al.'s scheme [24] generalizes the concept of region incrementing for (k, n)-threshold but suffers from the large pixel expansion. In the region incrementing schemes reported above, the generation of shares depends upon the basis matrices constructed prior to encoding process. The construction of basis matrices for a specific application is not always trivial. For example, in [17], the basis matrices are constructed by solving a linear programming problem. As the problem size becomes large, it may be difficult to solve the linear programming efficiently. The schemes proposed in [22, 25] solves the problem of pixel expansion and codebook requirement with the benefit of region incrementing but cannot be used for (k, n)-threshold. The construction methods reported in [22, 25] are for binary images handling the $(2, 3)$ and $(2, n)$-threshold region incrementing respectively. The proposed scheme extends the concept of region incrementing to a general (k, n)-threshold access structure for binary as well as color images. It has the obvious benefits of no pixel expansion and no codebook requirement compared to the other existing regional incrementing VSS schemes.

5. Conclusion

This paper presents a random-grid based (k, n)-RIVSS scheme for any $2 \leq k \leq n$. The proposed scheme satisfies both requirements: security (any $k - 1$ or fewer shares reveals no information about the input image) and recoverability (any t shares can reconstruct the secret regions up to $t - k + 1$ levels, where $k \leq t \leq n$). We have confirmed both the correctness and feasibility of our scheme by formal proofs and experimental results. Compared to other schemes for region incrementing, it has the similar ability of incremental revealing of the secrets of the input image and can reconstruct the secret regions with good contrast. The proposed scheme benefits by encoding the input image into shares of the size same as that of the input image without any priorly constructed set of basis matrices, which is more efficient comparing with the similar schemes [21, 17, 24]. This makes the proposed scheme more flexible and adaptable in practical applications for the sharing multiple weighted secrets.

References

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

[2] K. Y. Chao and J. C. Lin. Secret image sharing: A boolean-operations based approach combining benefits of polynomial-based and fast approaches. *International Journal of Pattern Recognition and Artificial Intelligence*, 23(2):263–285, 2009.

[3] T. H. Chen and K. H. Tsao. Visual secret sharing by random grids revisited. *Pattern Recognition*, 42(9):2203–2217, 2009.

[4] T. H. Chen and K. H. Tsao. Threshold visual secret sharing by random grids. *Journal of Systems and Software*, 84(7):1197–1208, 2011.

[5] T. H. Chen and C. S. Wu. Efficient multi-secret image sharing based on boolean operations. *Signal Processing*, 91(1):90–97, 2011.

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

[7] S. Kumar and R. K. Sharma. Improving contrast in random grids based visual secret sharing. *International Journal of Security and its Applications*, 6(1):9–28, 2012.

[8] S. Kumar and R. K. Sharma. Recursive information hiding of secrets by random grids. *Cryptologia*, 37(2):154–161, 2013.

[9] S. Kumar and R. K. Sharma. Secret image sharing for general access structures using random grids. *International Journal of Computer Applications*, 83(7):1–8, 2013.

[10] S. Kumar and R. K. Sharma. Threshold visual secret sharing based on boolean operations. *Security and Communication Networks*, 7(3):653–664, 2014.

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

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

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

[14] S. J. Shyu. Image encryption by random grids. *Pattern Recognition*, 40(3):1014–1031, 2007.

[15] S. J. Shyu. Image encryption by multiple random grids. *Pattern Recognition*, 42(7):1582–1596, 2009.

[16] S. J. Shyu. Visual cryptograms of random grids for general access structures. *IEEE Transactions On Circuits And Systems For Video Technology*, 23(3):414–424, 2013.

[17] S. J. Shyu and H. W. Jiang. Efficient construction for region incrementing visual cryptography. *IEEE Transactions On Circuits And Systems For Video Technology*, 22(5):769–777, 2012.

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

[19] R. Ulichney. A review of halftoning techniques. *SPIE*, 3963:378–391, 2000.

[20] D. Wang, L. Zhang, N. Ma, and X. Li. Two secret sharing schemes based on boolean operations. *Pattern Recognition*, 40(10):2776–2785, 2007.

[21] R. Z. Wang. Region incrementing visual cryptography. *IEEE Signal Processing Letters*, 16(8):659–662, 2009.

[22] R. Z. Wang, Y. C. Lan, Y. K. Lee, S. Y. Huang, S. J. Shyu, and T. L. Chia. Incrementing visual cryptography using random grids. *Optics Communications*, 283(21):4242–4249, 2010.

[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*, 85(5):1119–1134, 2012.

[24] C. N. Yang, H. W. Shih, C. C. Wu, and L. Harn. k out of n region incrementing scheme in visual cryptography. *IEEE Transactions On Circuits And Systems For Video Technology*, 22(5):799–810, 2012.

[25] G. S. Zhong and J. J. Wang. Region incrementing visual secret sharing scheme based on random grids. In *ISCAS*, pages 2351–2354, 2013.