Improving Contrast in Random Grids Based Visual Secret Sharing

Sachin Kumar and R. K. Sharma

Department of Mathematics, Indian Institute of Technology Delhi
Hauz Khas, New Delhi - 110016, India.
skiitd09@gmail.com, rksharma@maths.iitd.ac.in

Abstract

In the existing random grids based (n, n) visual secret sharing (VSS) schemes, decryption is done with the help of human visual system by stacking the cipher grids. The stacking operation is computationally modeled as Boolean OR operation, which suffers from two drawbacks. Firstly, the contrast of the reconstructed image decreases exponentially by increasing n (≥2) and secondly, it requires perfect alignment of stacking the cipher grids. In this paper, we propose Boolean XOR operation as decryption operation for the existing random grids based (n, n) VSS schemes. The proposed operation removes both the drawbacks and does lossless secret reconstruction. We have demonstrated the improvement in the contrast of the reconstructed image by formal proofs and experimental results.

Keywords: *Visual secret sharing, Visual cryptography, Random grids, Image encryption, Contrast improvement*

1. Introduction

Shamir [10] and Blakley [1] proposed independently (*k*, *n*) threshold secret sharing (SS) scheme, which encrypts a secret into *n* shares such that any *k*-1 or fewer shares provide no information about the secret and the secret information can be obtained by combining at least *k* (≤*n*) shares together. The traditional SS schemes [10, 1, 3] share non-visual secret information and reconstruct the secret accurately by using complex numerical computations. Visual secret sharing (VSS) schemes [2, 4-9, 11-15] are developed for visual secret information, can involve complex, little or no computation in the decryption phase. The schemes [2, 11-14] are based on Shamir's idea [10] and employ the complex computations. The advantage of these schemes is that size of the shares reduces to 1/*k* size of the secret, and the secret is reconstructed exactly same as original without any loss of information. Wang et al. [15] proposed two different Boolean based VSS schemes, called deterministic (*n*, *n*) and probabilistic (2, *n*) scheme, to encode binary, gray-level and color images. Both the schemes have advantage in terms of reconstruction accuracy and no pixel expansion, but have used the little computational cost in the decryption phase.

To solve the problem of computation involved in the decryption phase of VSS schemes, Naor and Shamir [7] proposed a new technique for secret image sharing, known as Visual Cryptography (VC). In VC scheme, a secret image is encrypted into *n* meaningless shares and reconstructed by stacking at least *k* (≤*n*) shares together. However, knowledge of less than *k* shares reveals nothing about the secret image. The reconstruction is performed by human visual system without any computation. In this model, each original pixel of a black and white secret image appears in *n* shares and each share is again a collection of *m* black and white sub pixels, referred as pixel expansion. Pixel expansion represents the loss in resolution

of the original image from the recovered one, and is preferred as small as possible. Naor and Shamir [7] proved that 2^{n-1} is the optimal pixel expansion for (n, n) VC scheme, where n is number of participants sharing the secret image. We can note that pixel expansion increases exponentially as n increases, makes impractical to use VC for large value of n. In addition, VC schemes also require the generation of a code book prior to share a secret image.

VSS technique without the above mentioned drawbacks is proposed by Kafri and Keren [6], in which a binary secret image is encrypted into two random cipher grids of same size as the secret image without any pixel expansion and code book requirement. The decryption is same as in traditional VC. Shyu [8] extended Kafri and Keren's method to encrypt the gray level and color images. Shyu [9] defined the visual cryptogram of n random grids and proposed encryption scheme for binary, gray level and color images such that only group of n participants can decode the secret image, while any group of less than n participants cannot obtain any information about the secret image. Chen [4] also proposed (2, n) and (n, n) VSS schemes based on random grids and proved that these schemes are as secure as original Kafri and Keren's VSS scheme. In all the above mentioned VSS schemes by random grids, secret image is reconstructed by stacking the cipher grids. The stacking operation is computationally modeled as Boolean OR operation, which suffers from the following drawbacks.

1. Contrast of the reconstructed image is measured in terms of the average light transmission, which decreases exponentially by increasing n (number of random cipher grids). Therefore, for large value of n, the reconstructed image looks like a meaningless image and it becomes very difficult to identify the reconstructed image. This limits the applicability of random grids based VSS for sharing into a small group of participants only.
2. Decryption process requires perfect alignment of stacking cipher grids, which is not easy to do in practical even for experienced participants. If stacking of cipher grids is deviated from few pixels or angles, then it becomes very difficult to recognize the information appeared on the reconstructed image.

To remove the above mentioned drawbacks, we have proposed Boolean XOR operation for decryption in the random grids based (n, n) VSS schemes. We have examined Kafri and Keren's (2, 2), Chen and Tsao's (n, n) and Shyu's (n, n) VSS schemes under the proposed decryption operation. We have proven theoretically and experimentally that the proposed decryption operation improves the contrast value significantly for all three VSS schemes. The proposed decryption operation XOR has the following advantages compare to the existing operation OR.

1. Lossless secret reconstruction - The reconstructed image is same as the original secret image.
2. No need to align - The difficulty of aligning all the cipher grids precisely in the decryption phase is removed.

The rest of this paper is organized as follows. In Section 2, first we have examined the properties of random grids under the proposed decryption operation XOR, and then we have proposed Kafri and Keren's (2, 2) VSS scheme under it. In Section 3 and 4, we have examined multiple random grids VSS schemes, i.e., Chen and Tsao's (n, n) VSS scheme and Shyu's (n, n) VSS scheme under the decryption operation XOR respectively. Section 5 demonstrates the experimental results and discussions. Finally, we conclude in Section 6.

2. Kafri and Keren's VSS Scheme under the Proposed Decryption Operation XOR

In Kafri and Keren's (2, 2) VSS scheme [6], a binary image is encrypted in two cipher grids and recovered by superimposing both cipher grids. Kafri and Keren proposed the three different algorithms to encrypt a binary image into two cipher grids, which are regarded as Algorithms 1-3.

Input: Binary secret image A of size $h \times w$ such that $A[i, j] \in \{0, 1\}$, where $1 \le i \le h$ and $1 \le j \le w$.

Output: Two random cipher grids R_1 and R_2 of size $h \times w$ such that $R_1[i, j] \in \{0, 1\}$ and $R_2[i, j] \in \{0, 1\}$, where $1 \le i \le h$ and $1 \le j \le w$.

Algorithm 1.

Step I: Generate R_1 randomly, i.e., $R_1[i, j] = randomValue(0, 1)$ for $1 \le i \le h$ and $1 \le j \le w$

Step II: Generate R_2 by R_1 and A as follows

```
for (each pixel A[i, j], 1 ≤ i ≤ h and 1 ≤ j ≤ w)
{
    if (A[i, j] = 0) R2[i, j] = R1[i, j]
    else R2[i, j] = R̄1[i, j]
}
```

Algorithm 2.

Step I: Generate R_1 randomly, i.e., $R_1[i, j] = randomValue(0, 1)$ for $1 \le i \le h$ and $1 \le j \le w$

Step II: Generate R_2 by R_1 and A as follows

```
for (each pixel A[i, j], 1 ≤ i ≤ h and 1 ≤ j ≤ w)
{
    if (A[i, j] = 0) R2[i, j] = R1[i, j]
    else R2[i, j] = randomValue(0, 1)
}
```

Algorithm 3.

Step I: Generate R_1 randomly, i.e., $R_1[i, j] = randomValue(0, 1)$ for $1 \le i \le h$ and $1 \le j \le w$

Step II: Generate R_2 by R_1 and A as follows

```
for (each pixel A[i, j], 1 ≤ i ≤ h and 1 ≤ j ≤ w)
{
    if (A[i, j] = 0) R2[i, j] = randomValue(0, 1)
    else R2[i, j] = R̄1[i, j]
}
```

randomValue(0, 1) is a function that returns a random value either 0 or 1 by using a coin flip procedure. $\overline{R}$ is 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 $1 \le i \le h$ and $1 \le j \le w$.

The effectiveness of VSS schemes based on random grids is measured by the contrast of the reconstructed image, which is defined in terms of the average light transmission.

Definition 1. *Let R be a binary grid. For a pixel $r \in R$, the light transmission $T(r)$ is defined as $T(r) = 1$ if r is white (0) and $T(r) = 0$ if r is black (1). The average light transmission of R is defined as* $T(R) = \frac{1}{h \times w} \sum_{i=1}^{h} \sum_{j=1}^{w} T(R[i, j])$.

Definition 2. *Let A be a secret image and S denotes the reconstructed image. The contrast of S is defined as* $\alpha = \frac{T(S[A(0)]) - T(S[A(1)])}{1 + T(S[A(1)])}$. *$A(0)$ and $A(1)$ denote the corresponding area of all white and black pixels respectively in A, with $A = A(0) \cup A(1)$ and $A(0) \cap A(1) = \phi$. $S[A(0)]$ and $S[A(1)]$ denote the corresponding area of all white and black pixels respectively in S.*

Recognition of the reconstructed image depends on the value of α, which is preferred as large as possible. Therefore, the contrast value of the reconstructed image is an important parameter, which needs to be optimize for better visual recognition of it. In Theorem 1, we have stated the security and contrast conditions of Kafri and Keren's (2, 2) VSS scheme under decryption operation OR. The proof of Theorem 1 can be referred from [6].

Theorem 1. *Cipher grids R_1 and R_2 generated by Algorithms* 1-3 *do not reveal any information about the secret image A individually, while the reconstructed image S obtained by superimposing R_1 and R_2 is enough to reveal A.*

Before analyzing Kafri and Keren's (2, 2) VSS scheme under XOR operation, we have stated and proved the properties of random grids under it.

Let $\oplus$ denotes Boolean XOR operation and $R_1 \oplus R_2$ denotes a grid obtained by applying XOR operation on the corresponding pixels of two same size cipher grids R_1 and R_2. The results of XOR operation of two random pixels $r_1 \in R_1$ and $r_2 \in R_2$ is given in Table 1.

Table 1. Results of Boolean XOR of Two Random Pixels

r_1	r_2	$r_1 \oplus r_2$
0	0	0
0	1	1
1	0	1
1	1	0

Lemma 1. *If R is a random grid, then* $T(R) = \frac{1}{2}$.

Proof. For any $r \in R$, $Prob(r = 0) = Prob(r = 1) = \frac{1}{2}$, i.e., $T(r) = \frac{1}{2}$. Therefore, $T(R) = \frac{1}{h \times w} \sum_{i=1}^{h} \sum_{j=1}^{w} T(R[i, j]) = \frac{1}{h \times w} \sum_{i=1}^{h} \sum_{j=1}^{w} \frac{1}{2} = \frac{1}{2}$. □

Lemma 2. *If R_1 and R_2 are two random grids, then* $T(R_1 \oplus R_2) = \frac{1}{2}$.

Proof. For any $r_1 \in R_1$ and $r_2 \in R_2$, from Table 1 we know that $r_1 \oplus r_2$ is 0 twice among the four possibilities, i.e., $Prob(r_1 \oplus r_2 = 0) = \frac{1}{2}$. Therefore, $T(r_1 \oplus r_2) = \frac{1}{2}$, i.e., $T(R_1 \oplus R_2) = \frac{1}{2}$. □

Lemma 3. *If R is a binary grid, then* $T(R \oplus R) = 1$.

Proof. For any $r \in R$, we know that $r \oplus r$ is 0. Therefore, $T(r \oplus r) = 1$, i.e., $T(R \oplus R) = 1$. □

Lemma 4. *If $\overline{R}$ is the inverse grid of a binary grid R, then* $T(R \oplus \overline{R}) = 0$.

Proof. For any $r \in R$ and its corresponding pixel $\bar{r} \in \overline{R}$, we have $r \oplus \bar{r} = 1$. Therefore, $T(r \oplus \bar{r}) = 0$, i.e., $T(R \oplus \overline{R}) = 0$. □

Lemma 5. *If R_1, R_2, …, and R_n are n random grids, then* $T(R_1 \oplus R_2 \oplus \ldots \oplus R_n) = \frac{1}{2}$.

Proof. We will prove the result by induction on n. By Lemma 2, $T(R_1 \oplus R_2) = \frac{1}{2}$, i.e., result is true for $n = 2$.

Let us assume that result holds for n-1, i.e., $T(R_1 \oplus R_2 \oplus \ldots \oplus R_{n-1}) = \frac{1}{2}$. We have to prove that it holds for n also. For $r_i \in R_i$ ($1 \le i \le n$), we know that $Prob(r_1 \oplus r_2 \oplus \ldots \oplus r_{n-1} \oplus r_n = 0) = (Prob(r_1 \oplus r_2 \oplus ... \oplus r_{n-1} = 0) \times Prob(r_n = 0)) + (Prob(r_1 \oplus r_2 \oplus ... \oplus r_{n-1} = 1) \times Prob(r_n = 1)) = (\frac{1}{2} \times \frac{1}{2}) + (\frac{1}{2} \times \frac{1}{2}) = \frac{1}{2}$. Therefore, $T(R_1 \oplus R_2 \oplus ... \oplus R_n) = \frac{1}{2}$. □

In Kafri and Keren's (2, 2) VSS scheme, the security condition is independent of the decryption operation and will not be violated by changing the decryption operation. Thus, we need to analyze only the contrast condition under the proposed operation, which we have stated and analyzed in the next theorem.

Theorem 2. *Let R_1 and R_2 be cipher grids generated by Algorithms* 1-3 *for the secret image A. The reconstructed image S obtained by XOR of R_1 and R_2, i.e., $S = R_1 \oplus R_2$ is high enough to reveal A.*

Proof: In Algorithms 1-3, R_1 is generated as a random grid. By Lemma 1, $T(R_1) = \frac{1}{2}$. Generation of R_2 differs in Algorithms 1-3.

In Algorithm 1, $R_2[A(0)] = R_1[A(0)]$ and $R_2[A(1)] = \overline{R_1[A(1)]}$. We have $S[A(0)] = R_1[A(0)] \oplus R_2[A(0)] = R_1[A(0)] \oplus R_1[A(0)]$ = fully white. Therefore, $T(S[A(0)]) = 1$. We have $S[A(1)] = R_1[A(1)] \oplus R_2[A(1)] = R_1[A(1)] \oplus \overline{R_1[A(1)]}$ = fully black. Therefore, $T(S[A(1)]) = 0$. Thus, the contrast of S is $\alpha_{XOR} = \frac{T(S[A(0)]) - T(S[A(1)])}{1 + T(S[A(1)])} = \frac{1 - 0}{1 + 0} = 1$.

In Algorithm 2, $R_2[A(0)] = R_1[A(0)]$ and $R_2[A(1)] = randomValue(0, 1)$. We have $S[A(0)]$ = fully white, i.e., $T(S[A(0)]) = 1$. We have $S[A(1)] = R_1[A(1)] \oplus R_2[A(1)]$. By Lemma 2, $T(S[A(1)]) = \frac{1}{2}$. Thus, the contrast of S is $\alpha_{XOR} = \frac{T(S[A(0)]) - T(S[A(1)])}{1 + T(S[A(1)])} = \frac{1 - \frac{1}{2}}{1 + \frac{1}{2}} = \frac{1}{3}$.

In Algorithm 3, $R_2[A(0)] = randomValue(0, 1)$ and $R_2[A(1)] = \overline{R_1[A(1)]}$. We have, $S[A(0)] = R_1[A(0)] \oplus R_2[A(0)]$. By Lemma 2, $T(S[A(0)]) = \frac{1}{2}$. We have, $S[A(1)]$ = fully black, i.e., $T(S[A(1)]) = 0$. Thus, the contrast of S is $\alpha_{XOR} = \frac{T(S[A(0)]) - T(S[A(1)])}{1 + T(S[A(1)])} = \frac{\frac{1}{2} - 0}{1 + 0} = \frac{1}{2}$.

We obtain, $\alpha_{XOR} \ge \frac{1}{3}$, the reconstructed image S obtained by XOR of R_1 and R_2 is high

enough to reveal the secret image A. □

Table 2. Contrast of the Reconstructed Image Obtained under OR and XOR Operation

Algorithm	α_{OR}	α_{XOR}	Remarks
1	$\frac{1}{2}$	1	$\alpha_{XOR} > \alpha_{OR}$
2	$\frac{1}{5}$	$\frac{1}{3}$	$\alpha_{XOR} > \alpha_{OR}$
3	$\frac{1}{4}$	$\frac{1}{2}$	$\alpha_{XOR} > \alpha_{OR}$

Table 2 shows the comparison of the contrast values of the reconstructed image obtained under OR (α_{OR}) [6] and XOR (α_{XOR}) operation. The proposed operation improves the contrast of the reconstructed image for all three Algorithms. In case of Algorithm 1, the contrast value of the reconstructed image under the proposed operation is 1, i.e., the reconstructed image is exactly same as the original secret image and recognizable perfectly. While for Algorithm 2 and 3, the reconstructed image will be more visually recognizable under the proposed operation compare to the existing operation.

3. Chen and Tsao's (*n*, *n*) VSS Scheme Under the Proposed Decryption Operation XOR

Chen and Tsao [4] proposed a method to encrypt a secret image into n (≥ 2) cipher grids such that the secret image is reconstructed by superimposing all n cipher grids, and any subset of n cipher grids reveals nothing about the secret image. The procedure for generating n cipher grids is given in Algorithm 4.

Input: Binary secret image A of size $h \times w$ such that $A[i, j] \in \{0, 1\}$, where $1 \leq i \leq h$ and $1 \leq j \leq w$.

Output: Cipher grids $R_1, R_2, \ldots$, and R_n of size $h \times w$ such that $R_k[i, j] \in \{0, 1\}$, where $1 \leq i \leq h$, $1 \leq j \leq w$ and $1 \leq k \leq n$.

Algorithm 4.

Step I: Select one algorithm from Algorithms 1-3 as a function $RG(\ )$

Step II: Generate two cipher grids R_1 and RB_1 by $RG(\ )$, i.e., $R_1 \parallel RB_1 = RG(A)$

Step III: Generate cipher grids R_2 to R_n recursively as follows

```
for (k = 2 to n - 1)
{
    R_k || RB_k = RG(RB_{k-1})
}
```

Step IV: $R_n = RB_{n-1}$

Step V: output(R_1, R_2, ..., R_n)

Here, $R_k \parallel RB_k = RG(RB_{k-1})$ denotes that function $RG(\ )$ takes cipher grid RB_{k-1} as input and produces cipher grids R_k and RB_k as output.

Theorem 3. *In Chen and Tsao's* (*n*, *n*) *VSS scheme, each cipher grid is random and superimposition of less than n cipher grids cannot reconstruct the secret image.*

The above theorem states the security condition and its proof can be referred from [4]. To analyze the contrast of the reconstructed image, we have stated and proved two new results as follows.

Lemma 6. *Sharing of a white pixel of the secret image A is possible into* 2^n - 2 *different ways by Algorithm* 4 *based on Algorithm* 2.

Proof. Let R_1, R_2, ..., R_n, RB_1, ..., and RB_{n-2} be generated as in Algorithm 4. Let $r_1(0)$, $r_2(0)$, ..., $r_{n-2}(0)$, $r_{n-1}(0)$ and $r_n(0)$ be any pixel values of R_1, R_2, ..., R_{n-2}, R_{n-1} and R_n corresponding to a white pixel (0) of *A* respectively. We claim that a white pixel of *A* will never be shared in two ways 0, 0, ..., 0, 1, 0 and 0, 0, ..., 0, 0, 1 by Algorithm 4 based on Algorithm 2.

Considering the value of cipher grids R_1, R_2, ..., and R_{n-2} as 0, 0, ..., and 0 respectively, we have by Algorithm 4 based on Algorithm 2, $rb_i = 0$ for $rb_i \in RB_i$ and $1 \le i \le n - 2$. For $rb_{n-2} = 0$, we have by Algorithm 4 based on Algorithm 2, $r_n(0) = 0$ if $r_{n-1}(0) = 0$, and $r_n(0) = 1$ if $r_{n-1}(0) = 1$. Therefore, sharing of a white pixel is not possible in two ways 0, 0, ..., 0, 1, 0 and 0, 0, ..., 0, 0, 1. Out of total 2^n possible ways of sharing a white pixel into *n* cipher grids, two are not possible. Hence, sharing of a white pixel of *A* is possible into 2^n- 2 different ways by Algorithm 4 based Algorithm 2. □

Lemma 7. *Sharing of a black pixel of the secret image A is possible into* 2^n - 2 *different ways by Algorithm* 4 *based on Algorithm* 3.

Proof. Let R_1, R_2, ..., R_n, RB_1, ..., and RB_{n-2} be generated as in Algorithm 4. Let $r_1(1)$, $r_2(1)$, ..., $r_{n-2}(1)$, $r_{n-1}(1)$ and $r_n(1)$ be any pixel values of R_1, R_2, ..., R_{n-2}, R_{n-1} and R_n corresponding to a black pixel (1) of *A* respectively. We claim that a black pixel of *A* will never be shared in two ways 0, 0, ..., 0, 0, 0 and 0, 0, ..., 0, 1, 1 by Algorithm 4 based Algorithm 3.

Considering the value of cipher grids R_1, R_2, ..., and R_{n-2} as 0, 0, ..., and 0 respectively, we have by Algorithm 4 based on Algorithm 3, $rb_i = 1$ for $rb_i \in RB_i$ and $1 \le i \le n - 2$. For $rb_{n-2} = 1$, we have by Algorithm 4 based on Algorithm 3, $r_n(1) = 1$ if $r_{n-1}(1) = 0$, and $r_n(1) = 0$ if $r_{n-1}(1) = 1$. Therefore, sharing of a black pixel is not possible in two ways 0, 0, ..., 0, 0, 0 and 0, 0, ..., 0, 1, 1. Out of total 2^n possible ways of sharing a black pixel into *n* cipher grids, two are not possible. Hence, sharing of a black pixel of *A* is possible into 2^n- 2 different ways by Algorithm 4 based Algorithm 3. □

Theorem 4. *In Chen and Tsao's* (*n*, *n*) *VSS scheme, the reconstructed image S obtained by superimposition of all n cipher grids reveals the secret image A.*

Proof. Let R_1, R_2, ..., and R_n be *n* cipher grids generated by Algorithm 4 for the secret image *A*. We have, $S = R_1 \otimes R_2 \otimes ... \otimes R_n$, where $\otimes$ denotes superimposition operation OR. The cipher grids R_1, R_2, ..., R_{n-1} are generated as random grids independently and the cipher grid

R_n is generated based on the selection from either of Algorithm 1, 2 or 3.

In Algorithm 1, $R_n[i, j] = R_{n-1}[i, j]$ if $RB_{n-2}[i, j] = 0$, and $R_n[i, j] = \overline{R_{n-1}[i, j]}$ if $RB_{n-2}[i, j] = 1$, where $1 \le i \le h$ and $1 \le j \le w$. We have, $S[A(0)] = R_1[A(0)] \otimes \ldots \otimes R_{n-1}[A(0)] \otimes R_n[A(0)] = R_1[A(0)] \otimes \ldots \otimes R_{n-2}[A(0)] \otimes R_{n-1}[A(0)]$. As R_1, ..., R_{n-2} and R_{n-1} are random, we obtain $T(S[A(0)]) = \frac{1}{2^{n-1}}$. In addition, $S[A(1)] = R_1[A(1)] \otimes \ldots \otimes R_{n-2}[A(1)] \otimes R_{n-1}[A(1)] \otimes R_n[A(1)] = R_1[A(1)] \otimes \ldots \otimes R_{n-2}[A(1)] \otimes RB'_{n-2}[A(1)] = R_1[A(1)] \otimes \ldots \otimes R_{n-3}[A(1)] \otimes RB'_{n-3}[A(1)] = \ldots\ldots\ldots = R_1[A(1)] \otimes RB'_1[A(1)]$ = fully black. Therefore, $T(S[A(1)]) = 0$. Thus, the contrast of S is $\alpha_{OR} = \frac{T(S[A(0)]) - T(S[A(1)])}{1 + T(S[A(1)])} = \frac{\frac{1}{2^{n-1}} - 0}{1 + 0} = \frac{1}{2^{n-1}}$.

In Algorithm 2, $R_n[i, j] = R_{n-1}[i, j]$ if $RB_{n-2}[i, j] = 0$, and $R_n[i, j] = randomValue(0, 1)$ if $RB_{n-2}[i, j] = 1$, where $1 \le i \le h$ and $1 \le j \le w$. By Lemma 6, encryption of a white pixel is possible into total 2^n-2 different ways but only one way decrypts white pixel correctly, i.e., $Prob(R_1[A(0)] \otimes \ldots \otimes R_n[A(0)] = 0) = \frac{1}{2^n - 2}$. Therefore, $T(S[A(0)]) = \frac{1}{2^n - 2}$. The cipher grid R_n is generated randomly corresponding to black area of the secret image A. Therefore, $T(S[A(1)]) = T(R_1[A(1)] \otimes R_2[A(1)] \otimes \ldots \otimes R_n[A(1)]) = \frac{1}{2^n}$. Thus, the contrast of S is $\alpha_{OR} = \frac{T(S[A(0)]) - T(S[A(1)])}{1 + T(S[A(1)])} = \frac{\frac{1}{2^n - 2} - \frac{1}{2^n}}{1 + \frac{1}{2^n}} = \frac{2}{(2^n - 2)(2^n + 1)}$.

In Algorithm 3, $R_n[i, j] = randomValue(0, 1)$ if $RB_{n-2}[i, j] = 0$, and $R_n[i, j] = \overline{R_{n-1}[i, j]}$ if $RB_{n-2}[i, j] = 1$, where $1 \le i \le h$ and $1 \le j \le w$. The cipher grid R_n is generated randomly corresponding to white area of the secret image A. Therefore, $T(S[A(0)]) = T(R_1[A(0)] \otimes R_2[A(0)] \otimes \ldots \otimes R_n[A(0)]) = \frac{1}{2^n}$. By Lemma 7, we know that a black pixel will never be shared as 0, 0, ..., 0, 0, 0 by Algorithm 4 based on Algorithm 3, i.e., $Prob(R_1[A(1)] \otimes \ldots \otimes R_n[A(1)] = 0) = 0$. Therefore, $T(S[A(1)]) = 0$. Thus, the contrast of S is $\alpha_{OR} = \frac{T(S[A(0)]) - T(S[A(1)])}{1 + T(S[A(1)])} = \frac{\frac{1}{2^n} - 0}{1 + 0} = \frac{1}{2^n}$.

$\alpha_{OR} > 0$ for $n \ge 2$, the secret image A can be recognized from the reconstructed image S. □

While analyzing Chen and Tsao's (n, n) VSS scheme under OR operation, we have obtained the correct contrast value in case of Algorithm 4 based on Algorithm 2. For Algorithm 4 based on Algorithm 2, Chen and Tsao [4] proved that contrast value is $\frac{1}{2^n + 1}$ by taking same value of $T(S[A(0)]) = \frac{1}{2^{n-1}}$ for Algorithm 1 and 2, which is not possible because encryption function differs for Algorithm 1 and 2. By the help of Lemma 6, we have proved that $T(S[A(0)]) = \frac{1}{2^n - 2}$ and obtained the correct contrast value equals to $\frac{2}{(2^n - 2)(2^n + 1)}$.

We have analyzed both the security and contrast conditions for Chen and Tsao's (n, n) VSS scheme under the proposed operation as follows.

Theorem 5. *In Chen and Tsao's* (n, n) *VSS scheme, image obtained by XOR of less than n cipher grids reveals nothing about the secret image A.*

Proof. Let R_{i_1}, R_{i_2}, …, and R_{i_k} be any k cipher grids selected from n cipher grids R_1, R_2, ..., and R_n, where $\{i_1, i_2, ..., i_k\} \subset \{1, 2, ..., n\}$. We have to prove that $R_{i_1} \oplus R_{i_2} \oplus \ldots \oplus R_{i_k} \neq A$ for any $\{i_1, i_2, \ldots, i_k\} \subset \{1, 2, ..., n\}$. There are two cases. Case 1 is $n \notin \{i_1, i_2, ..., i_k\}$ and Case 2 is $n \in \{i_1, i_2, ..., i_k\}$.

Case 1. If $n \notin \{i_1, i_2, ..., i_k\}$, then R_{i_1}, R_{i_2}, …, and R_{i_k} are generated independently as random grids. By Lemma 5, $T(R_{i_1}[A(0)] \oplus \ldots \oplus R_{i_k}[A(0)]) = T(R_{i_1}[A(1)] \oplus \ldots \oplus R_{i_k}[A(1)]) = \frac{1}{2}$. Thus, $R_{i_1} \oplus R_{i_2} \oplus \ldots \oplus R_{i_k} = random\ grid \neq A$.

Case 2. We assume the set of indices as $\{i_1, i_2, ..., i_{k-1}, n\}$. For any $k \leq n$, R_{i_1}, R_{i_2}, …, and $R_{i_{k-1}}$ are generated randomly. By Lemma 5, $T(R_{i_1}[A(0)] \oplus \ldots.. \oplus R_{i_{k-1}}[A(0)]) = T(R_{i_1}[A(1)] \oplus \ldots \oplus R_{i_{k-1}}[A(1)]) = \frac{1}{2}$. As generation of R_n depends upon random grids RB_{n-2} and R_{n-1}, R_n is also a random grid, i.e., $T(R_n[A(0)]) = T(R_n[A(1)]) = \frac{1}{2}$. Therefore, $T(R_{i_1}[A(0)] \oplus ... \oplus R_{i_{k-1}}[A(0)] \oplus R_n[A(0)]) = T(R_{i_1}[A(1)] \oplus \ldots \oplus R_{i_{k-1}}[A(1)] \oplus R_n[A(1)]) = \frac{1}{2}$. Thus, $R_{i_1} \oplus R_{i_2} \oplus \ldots \oplus R_{i_k} \oplus R_n = random\ grid \neq A$.

Hence, image obtained by XOR of less than n cipher grids is random and reveals nothing about the secret image A. □

Theorem 6. *In Chen and Tsao's* (n, n) *VSS scheme, the reconstructed image S obtained by XOR of all n cipher grids reveals the secret image A.*

Proof. Let R_1, R_2, ..., and R_n be n cipher grids generated by Algorithm 4 for the secret image A. We have, $S = R_1 \oplus R_2 \oplus ... \oplus R_n$. The cipher grids R_1, R_2, ..., and R_{n-1} are generated randomly and cipher grid R_n is generated based on the algorithm selected from Algorithms 1-3.

In Algorithm 1, $R_n[i, j] = R_{n-1}[i, j]$ if $RB_{n-2}[i, j] = 0$, and $R_n[i, j] = \overline{R_{n-1}[i, j]}$ if $RB_{n-2}[i, j] = 1$, where $1 \leq i \leq h$ and $1 \leq j \leq w$. We have, $S[A(0)] = R_1[A(0)] \oplus ... \oplus R_{n-1}[A(0)] \oplus R_n[A(0)] = R_1[A(0)] \oplus ... \oplus R_{n-2}[A(0)] \oplus RB_{n-2}[A(0)] = R_1[A(0)] \oplus ... \oplus R_{n-3}[A(0)] \oplus RB_{n-3}[A(0)] = \ldots.. = R_1[A(0)] \oplus RB_1[A(0)] = R_1[A(0)] \oplus R_1[A(0)]$ = fully white. Therefore, $T(S[A(0)]) = 1$. In addition, $S[A(1)] = R_1[A(1)] \oplus ... \oplus R_{n-1}[A(1)] \oplus R_n[A(1)] = R_1[A(1)] \oplus ... \oplus R_{n-2}[A(1)] \oplus RB_{n-2}[A(1)] = R_1[A(1)] \oplus ... \oplus R_{n-3}[A(1)] \oplus RB_{n-3}[A(1)] = \ldots\ldots = R_1[A(1)] \oplus RB_1[A(1)] = R_1[A(1)] \oplus \overline{R_1[A(1)]}$ = fully black. Therefore, $T(S[A(1)]) = 0$. Thus, the contrast of S is $\alpha_{XOR} = \frac{T(S[A(0)]) - T(S[A(1)])}{1 + T(S[A(1)])} = \frac{1 - 0}{1 + 0} = 1$.

In Algorithm 2, $R_n[i, j] = R_{n-1}[i, j]$ if $RB_{n-2}[i, j] = 0$, and $R_n[i, j] = randomValue(0, 1)$ if $RB_{n-2}[i, j] = 1$, where $1 \leq i \leq h$ and $1 \leq j \leq w$. By Lemma 6, encryption of a white pixel is possible into total $2^n - 2$ different ways. The two not possible ways 0, 0, …, 0, 1, 0 and 0, 0, …, 0, 0, 1 decrypt a black pixel (1) under XOR operation. Out of total $2^n - 2$ possible ways, a white pixel can be correctly decrypted by XOR operation in 2^{n-1} ways, i.e., $Prob(R_1[A(0)] \oplus \ldots \oplus R_n[A(0)] = 0) = \frac{2^{n-1}}{2^n - 2}$. Therefore, $T(S[A(0)]) = \frac{2^{n-1}}{2^n - 2}$. The cipher grid R_n is generated randomly corresponding to black area of the secret image A. By Lemma 5,

$T(S[A(1)]) = T(R_1[A(1)] \oplus R_2[A(1)] \oplus ... \oplus R_n[A(1)]) = \frac{1}{2}$. Thus, the contrast of S is $\alpha_{XOR} = \frac{T(S[A(0)]) - T(S[A(1)])}{1 + T(S[A(1)])} = \frac{\frac{2^{n-1}}{2^n - 2} - \frac{1}{2}}{1 + \frac{1}{2}} = \frac{2}{3(2^n - 2)}$.

In Algorithm 3, $R_n[i, j] = randomValue(0, 1)$ if $RB_{n-2}[i, j] = 0$, and $R_n[i, j] = \overline{R_{n-1}[i, j]}$ if $RB_{n-2}[i, j] = 1$, where $1 \le i \le h$ and $1 \le j \le w$. The cipher grid R_n is generated randomly corresponding to white area of A. By Lemma 5, $T(S[A(0)]) = \frac{1}{2}$. By Lemma 7, encryption of a black pixel is possible into total $2^n - 2$ different ways. The two not possible ways 0, 0, …, 0, 0, 0 and 0, 0, …, 0, 1, 1 decrypt a white pixel under XOR operation. Therefore, $Prob(R_1[A(1)] \oplus \ldots \oplus R_n[A(1)] = 0) = \frac{2^{n-1} - 2}{2^n - 2}$, i.e., $T(S[A(1)]) = \frac{2^{n-1} - 2}{2^n - 2}$. Thus, the contrast of S is $\alpha_{XOR} = \frac{T(S[A(0)]) - T(S[A(1)])}{1 + T(S[A(1)])} = \frac{\frac{1}{2} - \frac{2^{n-1} - 2}{2^n - 2}}{1 + \frac{2^{n-1} - 2}{2^n - 2}} = \frac{1}{2^n + 2^{n-1} - 4}$.

$\alpha_{XOR} > 0$ for $n \ge 2$, secret image A can be recognized form the reconstructed image S. □

Table 3. Contrast of the Reconstructed Image Obtained under OR and XOR Operation in Chen and Tsao's (*n*, *n*) VSS Scheme

Algorithm 4 based on Algorithm	α_{OR}	α_{XOR}	Remarks
1	$\frac{1}{2^{n-1}}$	1	$\alpha_{XOR} > \alpha_{OR}$ for all $n \ge 2$
2	$\frac{2}{(2^n - 2)(2^n + 1)}$	$\frac{2}{3(2^n - 2)}$	$\alpha_{XOR} > \alpha_{OR}$ for all $n \ge 2$
3	$\frac{1}{2^n}$	$\frac{1}{2^n + 2^{n-1} - 4}$	$\alpha_{XOR} \ge \alpha_{OR}$ for all $2 \le n \le 3$ and $\alpha_{XOR} < \alpha_{OR}$ for all $n \ge 4$

In Table 3, we have shown the comparison of the contrast values obtained under XOR and OR operation in Chen and Tsao's (*n*, *n*) VSS scheme. In case of Algorithm 4 based on Algorithm 1, we can share a secret image into any number of cipher grids under the proposed decryption operation such that reconstructed image will be exactly as same as the original secret image. The proposed decryption operation also improves the contrast in case of Algorithm 4 based on Algorithm 2 and 3.

4. Shyu's (*n*, *n*) VSS Scheme under the Proposed Decryption Operation XOR

Shyu [9] designed an algorithm, which encrypts a secret image into a set of visual cryptograms of *n* random grids. The visual cryptograms of *n* random grids based on OR operation, referred as $VCRG_{OR}$-*n* is defined as follows.

Definition 3. *A set* $\{R_1, R_2, ..., R_{n-1}, R_n\}$ *of n random grids with respect to the secret image A is* $VCRG_{OR}$*-n of A, if following conditions are true:*

(i) R_i *is a random grid, i.e.,* $T(R_i) = \frac{1}{2}$ *for* $1 \le i \le n$;

(ii) $T(R_{i_1}[A(0)] \otimes R_{i_2}[A(0)] \otimes ... \otimes R_{i_d}[A(0)]) = T(R_{i_1}[A(1)] \otimes R_{i_2}[A(1)] \otimes ... \otimes R_{i_d}[A(1)])$ *for any d distinct random grids with* $2 \le d \le n$-1 *and* $1 \le i_1 < i_2 < ... < i_d \le n$;

(iii) $T(R_1[A(0)] \otimes R_2[A(0)] \otimes ... \otimes R_n[A(0)]) > T(R_1[A(1)] \otimes R_2[A(1)] \otimes .... \otimes R_n[A(1)])$.

Condition (i) and (ii) are security conditions and ensure that secret image cannot be reconstructed by any subset of n cipher grids. Condition (iii) is contrast condition, which claims that superimposed result of all n cipher grids reconstructs the secret image. Algorithm 5 generates a set $\{R_1, R_2, ..., R_{n-1}, R_n\}$, which constitutes $VCRG_{OR}$-n.

Input: Binary secret image A of size $h \times w$ such that $A[i, j] \in \{0, 1\}$, where $1 \le i \le h$ and $1 \le j \le w$.
Output: Cipher grids $R_1, R_2, \ldots$, and R_n of size $h \times w$ such that $R_k[i, j] \in \{0, 1\}$, where $1 \le i \le h$, $1 \le j \le w$ and $1 \le k \le n$.

Algorithm 5.

Step I: Generate R_i as a random grid, i.e., $T(R_i) = \frac{1}{2}$ where $1 \le i \le n$ -1

Step II: Generate RB from R_1, R_2, ..., and R_{n-1} as follows

```
for (1 ≤ i ≤ h and 1 ≤ j ≤ w)
{
    b_1 = R_1[i, j]
    for (2 ≤ k ≤ n - 1)
    {
        if (R_k[i, j] = 0)  then b_k = b_{k-1}
        else b_k = complement(b_{k-1})
    }
    RB[i, j] = b_{n-1}
}
```

Step III: Select one algorithm from Algorithms 1-3

Step IV: Create R_n by RB and secret image A by using selected algorithm

```
Case 1: Algorithm 1 is selected
    for (1 ≤ i ≤ h and 1 ≤ j ≤ w)
    {
        if (A[i, j] = 0) R_n[i, j] = RB[i, j]
        else R_n[i, j] = complement(RB[i, j])
    }
Case 2: Algorithm 2 is selected
    for (1 ≤ i ≤ h and 1 ≤ j ≤ w)
    {
        if (A[i, j] = 0) R_n[i, j] = RB[i, j]
        else R_n[i, j] = randomValue(0, 1)
    }
Case 3: Algorithm 3 is selected
    for (1 ≤ i ≤ h and 1 ≤ j ≤ w)
```

{
if ($A[i, j] = 0$) $R_n[i, j]$ = *randomValue*(0, 1)
else $R_n[i, j] = \overline{RB[i, j]}$
}

Step V: output (R_1, R_2, ..., R_n)

Lemma 8. *If RB is generated from random grids R_1, R_2, ..., and R_{n-1} as in Step II of Algorithm 5, then RB is also a random grid.*

Theorem 7. *A set $\{R_1, R_2, ..., R_{n-1}, R_n\}$ generated by Algorithm 5 with respect to the secret image A is $VCRG_{OR}$-n of A.*

The proof of Lemma 8 and Theorem 7 can be referred from [9]. To analyze Shyu's (n, n) VSS scheme under the proposed decryption operation, first we have defined the visual cryptograms of n random grids based on decryption operation XOR, referred as $VCRG_{XOR}$-n.

Definition 4. *A set $\{R_1, R_2, ..., R_{n-1}, R_n\}$ of n random grids with respect to the secret image A is $VCRG_{XOR}$-n of A, if following conditions are true:*

(i) R_i *is a random grid, i.e.,* $T(R_i) = \frac{1}{2}$ *for* $1 \le i \le n$;

(ii) $T(R_{i_1}[A(0)] \oplus R_{i_2}[A(0)] \oplus ... \oplus R_{i_d}[A(0)]) = T(R_{i_1}[A(1)] \oplus R_{i_2}[A(1)] \oplus ... \oplus R_{i_d}[A(1)])$ *for any d distinct random grids with* $2 \le d \le n$-1 and $1 \le i_1 < i_2 < ... < i_d \le n$;

(iii) $T(R_1[A(0)] \oplus R_2[A(0)] \oplus ... \oplus R_n[A(0)]) > T(R_1[A(1)] \oplus R_2[A(1)] \oplus ... \oplus R_n[A(1)])$.

We have stated and proved a new Lemma 9, which we will use to prove that $\{R_1, R_2, ..., R_{n-1}, R_n\}$ generated by Algorithm 5 with respect to the secret image A is $VCRG_{XOR}$-n of A.

Lemma 9. *If R_1, R_2, ..., R_{n-1} and RB are random grids generated as in Algorithm 5, then $RB = R_1 \oplus R_2 \oplus ... \oplus R_{n-1}$.*

Proof. Let $r_b \in RB$ and $r_i \in R_i$, where $1 \le i \le n$-1. We have to prove that $r_b = r_1 \oplus r_2 \oplus ... \oplus r_{n-1}$.

From Algorithm 5, we have $b_1 = r_1$. If $r_2 = 0$ then $b_2 = b_1 = r_1$, else $b_2 = \overline{b_1} = \overline{r_1}$. Thus, for $r_2 = 0$, we obtain $b_2 = r_1 = r_1 \oplus 0 = r_1 \oplus r_2$ and for $r_2 = 1$, we obtain $b_2 = \overline{r_1} = r_1 \oplus 1 = r_1 \oplus r_2$. Similarly, if $r_3 = 0$, we obtain $b_3 = b_2 = b_2 \oplus 0 = b_2 \oplus r_3 = r_1 \oplus r_2 \oplus r_3$ and if $r_3 = 1$, we obtain $b_3 = \overline{b_2} = b_2 \oplus 1 = b_2 \oplus r_3 = r_1 \oplus r_2 \oplus r_3$. Thus, $b_3 = r_1 \oplus r_2 \oplus r_3$.

Therefore, following similarly we have, $b_{n-2} = r_1 \oplus r_2 \oplus ... \oplus r_{n-2}$. As value r_b depends upon b_{n-2} and r_{n-1}, we have for $r_{n-1} = 0$, $r_b = b_{n-2} = b_{n-2} \oplus 0 = b_{n-2} \oplus r_{n-1}$ and for $r_{n-1} = 1$, we have $r_b = \overline{b_{n-2}} = b_{n-2} \oplus 1 = b_{n-2} \oplus r_{n-1}$. Thus, $r_b = b_{n-2} \oplus r_{n-1} = r_1 \oplus r_2 \oplus ... \oplus r_{n-2} \oplus r_{n-1}$, i.e., $RB = R_1 \oplus R_2 \oplus ... \oplus R_{n-2} \oplus R_{n-1}$. □

Theorem 8. *A set $\{R_1, R_2, ..., R_{n-1}, R_n\}$ generated by Algorithm 5 with respect to the secret image A is $VCRG_{XOR}$-n of A.*

Proof. To prove that $\{R_1, R_2, ..., R_{n-1}, R_n\}$ is $VCRG_{XOR}$-n of A, we have to prove that all three conditions in Definition 4 holds.

(i) This first condition of Definition 4 states that each cipher grid is random, and does not depend upon changing the decryption operation. The proof of this condition is same as the proof of the condition (i) in Theorem 7 and can be referred from [9].

(ii) Let $\{R_{i_1}, R_{i_2}, ..., R_{i_d}\} \subset \{R_1, R_2, ..., R_n\}$ with $2 \le d \le n$-1 and $1 \le i_1 < i_2 < ... < i_d \le n$. We consider two cases: Case 1 is $R_n \notin \{R_{i_1}, R_{i_2}, ..., R_{i_d}\}$ and Case 2 is $R_n \in \{R_{i_1}, R_{i_2}, ..., R_{i_d}\}$.

Case 1. $R_{i_1}, R_{i_2}, ...,$ and R_{i_d} are independently generated as random grids. By Lemma 5, $T(R_{i_1}[A(0)] \oplus R_{i_2}[A(0)] \oplus ... \oplus R_{i_d}[A(0)]) = T(R_{i_1}[A(1)] \oplus R_{i_2}[A(1)] \oplus ... \oplus R_{i_d}[A(1)]) = \frac{1}{2}$.

Case 2. Assume that $D = \{R_{i_1}, R_{i_2}, ..., R_{i_{d-1}}, R_n\}$. Here, $R_{i_1}, R_{i_2}, ...,$ and $R_{i_{d-1}}$ are independently generated as random grids. As R_n is generated based on the selection from either of Algorithm 1, 2 or 3, we have three cases for $a \in A$, $r_b \in RB$ and $r_n \in R_n$.

In Algorithm 1, if $a = 0$ then $r_n = r_b$. By Lemma 9, $r_n = r_1 \oplus r_2 \oplus \ldots \oplus r_{n-1}$, where $r_i \in R_i$ and $1 \le i \le n$-1. We can assume that $r_n = r_{i_1} \oplus ... \oplus r_{i_{d-1}} \oplus r_{i_d} \oplus ... \oplus r_{i_{n-1}}$. We have, $r_{i_1} \oplus \ldots \oplus r_{i_{d-1}} \oplus r_n = r_{i_1} \oplus \ldots \oplus r_{i_{d-1}} \oplus r_{i_1} \oplus \ldots \oplus r_{i_{d-1}} \oplus r_{i_d} \oplus \ldots \oplus r_{i_{n-1}} = r_{i_d} \oplus \ldots \oplus r_{i_{n-1}}$. For $a = 0$, $T(r_{i_1} \oplus \ldots \oplus r_{i_{d-1}} \oplus r_n) = T(r_{i_d} \oplus \ldots \oplus r_{i_{n-1}}) = \frac{1}{2}$, i.e., $T(R_{i_1}[A(0)] \oplus \ldots \oplus R_{i_{d-1}}[A(0)] \oplus R_n[A(0)]) = \frac{1}{2}$. If $a = 1$ then $r_n = \overline{r_b}$. We have, $r_{i_1} \oplus ... \oplus r_{i_{d-1}} \oplus r_n = r_{i_1} \oplus ... \oplus r_{i_{d-1}} \oplus \overline{r_{i_1} \oplus \ldots \oplus r_{i_{d-1}} \oplus r_{i_d} \oplus \ldots \oplus r_{i_{n-1}}} = \overline{r_{i_d} \oplus ... \oplus r_{i_{n-1}}}$. For $a = 1$, $T(r_{i_1} \oplus \ldots \oplus r_{i_{d-1}} \oplus r_n) = T(\overline{r_{i_d} \oplus \ldots \oplus r_{i_{n-1}}}) = \frac{1}{2}$, i.e., $T(R_{i_1}[A(1)] \oplus \ldots \oplus R_{i_{d-1}}[A(1)] \oplus R_n[A(1)]) = \frac{1}{2}$.

In Algorithm 2, if $a = 0$ then $r_n = r_b$. We obtain by following the same as above $T(R_{i_1}[A(0)] \oplus ... \oplus R_{i_{d-1}}[A(0)] \oplus R_n[A(0)]) = \frac{1}{2}$. If $a = 1$ then $r_n =$ *randomValue*(0, 1). By Lemma 5, $T(R_{i_1}[A(1)] \oplus ... \oplus R_{i_{d-1}}[A(1)] \oplus R_{i_n}[A(1)]) = \frac{1}{2}$.

In Algorithm 3, if $a = 0$ then $r_n =$ *randomValue*(0, 1). By Lemma 5, $T(R_{i_1}[A(0)] \oplus \ldots \oplus R_{i_{d-1}}[A(0)] \oplus R_n[A(0)]) = \frac{1}{2}$. If $a = 1$ then $r_n = \overline{r_b}$. We obtain, $T(R_{i_1}[A(1)] \oplus \ldots \oplus R_{i_{d-1}}[A(1)] \oplus R_n[A(1)]) = \frac{1}{2}$.

Consequently for all three cases, $T(R_{i_1}[A(0)] \oplus \ldots\ldots\ldots ... \oplus R_{i_{d-1}}[A(0)] \oplus R_n[A(0)]) = T(R_{i_1}[A(1)] \oplus \ldots\ldots \oplus R_{i_{d-1}}[A(1)] \oplus R_n[A(1)]) = \frac{1}{2}$, i.e., condition (ii) is satisfied.

(iii) Let S be the reconstructed image obtained by XOR of the cipher grids $R_1, R_2, ...,$ and R_n. The cipher grids $R_1, R_2, \ldots,$ and R_{n-1} are generated randomly. By Lemma 5, $T(R_1[A(0)] \oplus R_2[A(0)] \oplus ... \oplus R_{n-1}[A(0)]) = T(R_1[A(1)] \oplus R_2[A(1)] \oplus ... \oplus R_{n-1}[A(1)]) = \frac{1}{2}$. Since R_n is generated by either of Algorithm 1, 2 or 3, we have three cases for $a \in A$, $r_b \in RB$ and $r_n \in R_n$.

In Algorithm 1, if $a = 0$ then $r_n = r_b$. By Lemma 9, $r_n = r_1 \oplus r_2 \oplus ... \oplus r_{n-1}$, where $r_i \in R_i$ and $1 \le i \le n$-1. We have, $r_1 \oplus \ldots \oplus r_{n-1} \oplus r_n = r_1 \oplus \ldots \oplus r_{n-1} \oplus r_1 \oplus \ldots \oplus r_{n-1} = 0$. For $a = 0$, $T(r_1 \oplus \ldots \oplus r_{n-1} \oplus r_n) = T(0) = 1$, i.e., $T(S[A(0)]) = T(R_1[A(0)] \oplus \ldots \oplus$

$R_{n-1}[A(0)] \oplus R_n[A(0)]) = 1$. If $a = 1$ then $r_n = \overline{r_b}$. We have, $r_1 \oplus ... \oplus r_{n-1} \oplus r_n = r_1 \oplus ... \oplus r_{n-1} \oplus \overline{r_1 \oplus ... \oplus r_{n-1}} = 1$. For $a = 1$, $T(r_1 \oplus \ldots \oplus r_{n-1} \oplus r_n) = T(1) = 0$, i.e., $T(S[A(1)]) = T(R_1[A(1)] \oplus \ldots \oplus R_{n-1}[A(1)] \oplus R_n[A(1)]) = 0$. Hence, $(T(S[A(0)]), T(S[A(1)])) = (1, 0)$.

In Algorithm 2, if $a = 0$ then $r_n = r_b$. By following the same as above we obtain, $T(S[A(0)]) = T(R_1[A(0)] \oplus \ldots \oplus R_{n-1}[A(0)] \oplus R_n[A(0)]) = 1$. If $a = 1$ then $r_n =$ *randomValue*(0, 1). By Lemma 5, $T(S[A(1)]) = T(R_1[A(1)] \oplus \ldots \oplus R_n[A(1)]) = \frac{1}{2}$. Hence, $(T(S[A(0)]), T(S[A(1)])) = (1, \frac{1}{2})$.

In Algorithm 3, if $a = 0$ then $r_n =$ *randomValue*(0, 1). By Lemma 5, $T(S[A(0)]) = T(R_1[A(0)] \oplus R_2[A(0)] \oplus ... \oplus R_n[A(0)]) = \frac{1}{2}$. If $a = 1$ then $r_n = \overline{r_b}$. We obtain, $T(S[A(1)]) = T(R_1[A(1)] \oplus R_2[A(1)] \oplus ... \oplus R_n[A(1)]) = 0$. Hence, $(T(S[A(0)]), T(S[A(1)])) = (\frac{1}{2}, 0)$.

Consequently, $T(R_1[A(0)] \oplus \ldots \oplus R_{n-1}[A(0)] \oplus R_n[A(0)]) > T(R_1[A(1)] \oplus \ldots \oplus R_{n-1}[A(1)] \oplus R_n[A(1)])$, i.e., condition (iii) is satisfied. □

Theorem 9. *In Shyu's* (*n*, *n*) *VSS scheme, the reconstructed image S obtained by XOR of all n cipher grids is high enough to reveal the secret image A.*

Proof. To prove this theorem, we have used the results proved in the proof of Theorem 8.

In case of Algorithm 5 based on Algorithm 1, $(T(S[A(0)]), T(S[A(1)])) = (1, 0)$. Thus, the contrast of S is $\alpha_{XOR} = \frac{T(S[A(0)]) - T(S[A(1)])}{1 + T(S[A(1)])} = \frac{1 - 0}{1 + 0} = 1$.

In case of Algorithm 5 based on Algorithm 2, $(T(S[A(0)]), T(S[A(1)])) = (1, \frac{1}{2})$. Thus, the contrast of S is $\alpha_{XOR} = \frac{T(S[A(0)]) - T(S[A(1)])}{1 + T(S[A(1)])} = \frac{1 - \frac{1}{2}}{1 + \frac{1}{2}} = \frac{1}{3}$.

In case of Algorithm 5 based on Algorithm 3, $(T(S[A(0)]), T(S[A(1)])) = (\frac{1}{2}, 0)$. Thus, the contrast of S is $\alpha_{XOR} = \frac{T(S[A(0)]) - T(S[A(1)])}{1 + T(S[A(1)])} = \frac{\frac{1}{2} - 0}{1 + 0} = \frac{1}{2}$.

$\alpha_{XOR} \geq \frac{1}{3}$, the reconstructed image S is high enough to reveal the secret image A. □

Table 4. Contrast of the Reconstructed Image Obtained under OR and XOR Operation in Shyu's (*n*, *n*) VSS Scheme

Algorithm 5 based on Algorithm	α_{OR}	α_{XOR}	Remarks
1	$\frac{1}{2^{n-1}}$	1	$\alpha_{XOR} > \alpha_{OR}$ for all $n \geq 2$
2	$\frac{1}{2^n + 1}$	$\frac{1}{3}$	$\alpha_{XOR} > \alpha_{OR}$ for all $n \geq 2$
3	$\frac{1}{2^n}$	$\frac{1}{2}$	$\alpha_{XOR} > \alpha_{OR}$ for all $n \geq 2$

Table 4 shows that comparison between α_{XOR} and α_{OR} [9] in Shyu's (n, n) VSS scheme. Under the proposed decryption operation, contrast value of the reconstructed image remains constant of n. In case of Algorithm 5 based on Algorithm 1, secret image can be reconstructed without loss of any information, while in case of Algorithm 5 based on Algorithm 2 and 3 also the proposed operation improves the contrast of the reconstructed image.

5. Experimental Results and Discussions

In order to demonstrate the improvement in the contrast value of the reconstructed secret image under the proposed decryption operation, we have conducted three experiments.

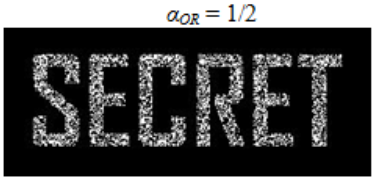
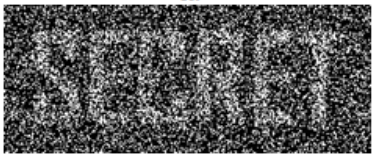
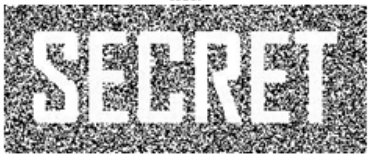
5.1. Experiment 1: Kafri and Keren's (2, 2) VSS Scheme

In this experiment, a secret image as in Figure 1 is encrypted into two cipher grids by Algorithms 1-3.

Figure 1. Secret Image

Table 5 shows the reconstructed results obtained under the decryption operation OR and XOR. From Table 5, it is clear that in case of all three algorithms image reconstructed by XOR operation is visually more recognizable than the image reconstructed by OR operation.

Table 5. Kafri and Keren's (2, 2) VSS Scheme

Algorithm	Reconstructed image obtained by decryption operation OR	Reconstructed image obtained by the proposed decryption operation XOR
1	$\alpha_{OR} = 1/2$ 	$\alpha_{XOR} = 1$ 
2	$\alpha_{OR} = 1/5$ 	$\alpha_{XOR} = 1/3$ 
3	$\alpha_{OR} = 1/4$ 	$\alpha_{XOR} = 1/2$ 

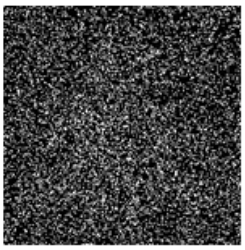
5.2. Experiment 2: Chen and Tsao's (*n*, *n*) VSS Scheme

In this experiment, a secret image as in Figure 2 is encrypted into $n = 3$ cipher grids by Algorithm 4 based on either of Algorithm 1, 2 or 3.

Figure 2. Secret Image

In Table 6, we have shown the reconstructed images obtained by OR and XOR of all three cipher grids. We can note that in case of Algorithm 4 based on Algorithm 2, we cannot recognize image reconstructed by OR operation, while the image reconstructed by XOR operation is easy to recognize.

Table 6. Chen and Tsao's (*n*, *n*) VSS Scheme for *n* = 3

Algorithm 4 based on Algorithm	Reconstructed image obtained by decryption operation OR	Reconstructed image obtained by the proposed decryption operation XOR
1	$\alpha_{OR} = 1/4$ 	$\alpha_{XOR} = 1$ 
2	$\alpha_{OR} = 1/27$ 	$\alpha_{XOR} = 1/9$ 
3	$\alpha_{OR} = 1/8$ 	$\alpha_{XOR} = 1/8$ 

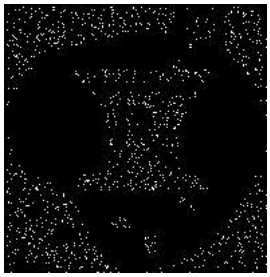
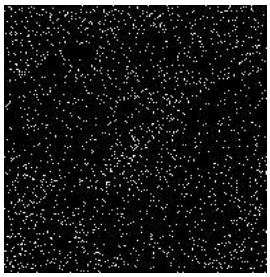
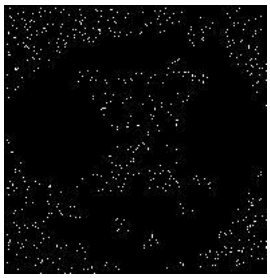
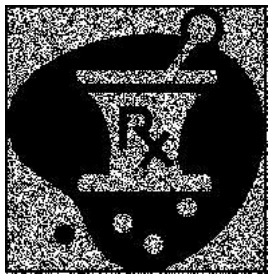
5.3. Experiment 3: Shyu's (*n*, *n*) VSS Scheme

In this experiment, a secret image as in Figure 3 is encrypted into $n = 5$ cipher grids by Algorithm 5 based on either of Algorithm 1, 2 or 3.

Figure 3. Secret Image

Table 7 shows the reconstructed images obtained by OR and XOR of all five cipher grids. We can very easily recognize the image reconstructed by the proposed operation, while it is very difficult to recognize the image reconstructed by OR operation.

Table 7. Shyu's (*n*, *n*) VSS Scheme for *n* = 5

Algorithm 5 based on Algorithm	Reconstructed image obtained by decryption operation OR	Reconstructed image obtained by the proposed decryption operation XOR
1	$\alpha_{OR} = 1/16$ 	$\alpha_{XOR} = 1$ 
2	$\alpha_{OR} = 1/33$ 	$\alpha_{XOR} = 1/3$ 
3	$\alpha_{OR} = 1/32$ 	$\alpha_{XOR} = 1/2$ 

5.4. Computational Efficiency

In Table 8, we have shown the comparison of the computational complexity required in reconstruction phase between the related works and the proposed work. Shamir's scheme [10] requires the polynomial evaluation and interpolation in reconstruction phase, which is $O(nlog^2n)$, where n is the number of shares. VSS schemes [11-14] are based on Shamir's (k, n) scheme. Therefore, the computational complexity of reconstruction phase in these schemes is the same as that of Shamir's scheme, i.e., $O(nlog^2n)$. In addition to Shamir's scheme, Li Bai et al.'s schemes [2-3] used the matrix projection secret sharing scheme for generating the shares of size less than the secret size. The matrix projection scheme involves the matrix operation (i.e., multiplication, transpose and inverse) in the shares generation and secret reconstruction phase. Therefore, the computational complexity requires for reconstruction phase in [2-3] is $O(n^3)$.

In our proposed work, secret image is reconstructed by XOR of all n ($\geq$2) cipher grids. The computational complexity in reconstruction phase depends upon the number and the size of cipher grids. Approximately, we can analyze that the computation complexity required in reconstruction phase of our proposed work is proportional to n, i.e., $O(n)$.

Table 8. Computational Complexity in Decryption Phase of (n, n) SS Schemes

Scheme	Computational complexity in decryption phase
Traditional SS scheme [10]	$O(nlog^2n)$
Traditional VSS schemes [11-14]	$O(nlog^2n)$
SS schemes using matrix projection [2-3]	$O(n^3)$
Our proposed work	$O(n)$

6. Conclusion

In this paper, Boolean XOR operation is proposed to decrypt the secret image, encrypted by (n, n) VSS schemes based on random grids. The proposed operation results in better contrast of the reconstructed image and provides the perfect security. The proposed operation does lossless secret reconstruction for any number of participants and removes the problem of perfect alignment of the shares with little computational cost. The Boolean XOR operation can be easily implemented in common software packages, such as Photoshop and used to reconstruct the secret images. The proposed operation is very good for the applications requiring the quality of the reconstructed images.

References

[1] G. R. Blakley, "Safeguarding Cryptographic Keys", AFIPS Conference Proceedings, Vol. 48, **(1979),** pp. 313-317.

[2] Li Bai, S. Biswas, A. Ortiz, and D. Dalessandro, "An Image Secret Sharing Method", Proceeding of 9th International Conference on Information Fusion, Italy, **(2006),** pp. 1-6.

[3] L. Bai, and X. Zou, "A Proactive Secret Sharing Scheme in Matrix Projection Method", International Journal of Security and Networks, Vol. 4, No. 4, **(2009),** pp. 201 - 209.

[4] T. H. Chen, and K. H. Tsao, "Visual Secret Sharing by Random Grids Revisited", Pattern Recognition, Vol. 42, **(2009),** pp. 2203-2217.

[5] T. H. Chen, and C. S. Wu, "Efficient Multi-secret Image Sharing based on Boolean Operations", Signal Processing, Vol. 91, No. 1, **(2011),** pp. 90-97.

[6] O. Kafri, and E. Keren, "Encryption of Pictures and Shapes by Random Grids", Optics Letters, Vol. 12, **(1987),** pp. 377-379.

[7] M. Naor, and A. Shamir, "Visual Cryptography", In Proceedings of Advances in Cryptology (EUROCRYPT 94), vol. 950, LNCS, Springer-Verlag, **(1995),** pp. 1-12.

[8] S. J. Shyu, "Image Encryption by Random Grids", Pattern Recognition, Vol. 40, **(2007),** pp. 1014-1031.

[9] S. J. Shyu, "Image Encryption by Multiple Random Grids", Pattern Recognition, Vol. 42, **(2009),** pp. 1582-1596.

[10] A. Shamir, "How to Share a Secret", Communication of the ACM, Vol. 22, **(1979),** pp. 612-613.

[11] C. C. Thien, and J. C. Lin, "Secret Image Sharing", Computer & Graphics, Vol. 26, pp. 765-770.

[12] C. C. Thien, and J. C. Lin, "An Image-sharing Method with User-friendly Shadow Images", IEEE Trans. Circuits Syst. Video Technol., Vol. 13, **(2003),** pp. 1161-1169.

[13] R. Z. Wang, and C. H. Su, "Secret Image Sharing with Smaller Shadow Images", Pattern Recognition Lett., Vol. 27, No. 6, **(2006),** pp. 551-555.

[14] Y. S. Wu, C. C. Thien, and J. C. Lin, "Sharing and Hiding Secret Images with Size Constraint", Pattern Recognition, Vol. 37, **(2004),** pp. 1377-1385.

[15] D. Wang, L. Zhang, N. Ma, and X. Li, "Two Secret Sharing Schemes based on Boolean Operations", Pattern Recognition, Vol. 40, No. 10, **(2007),** pp. 2776-2785.