Signal Processing 108 (2015) 604–621

Contents lists available at ScienceDirect

Signal Processing

journal homepage: www.elsevier.com/locate/sigpro

Non-expansible XOR-based visual cryptography scheme with meaningful shares

Duanhao Ou [a], Wei Sun [b,c,*], Xiaotian Wu [a]

[a] School of Information Science and Technology, Sun Yat-sen University, Guangzhou 510006, China
[b] School of Software, Sun Yat-sen University, Guangzhou 510006, China
[c] State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, Beijing 100093, China

ARTICLE INFO

Article history:
Received 22 April 2014
Received in revised form
29 September 2014
Accepted 8 October 2014
Available online 16 October 2014

Keywords:
XOR-based visual cryptography
Secret sharing
Meaningful shares
No pixel expansion
Visual quality

ABSTRACT

XOR-based visual cryptography (VC), a brand-new type of VC, is suitable for solving the low image quality and alignment problems in VC system. However, meaningless share and pixel expansion remain to be continuing challenges in existing XOR-based VC. To fix those mentioned defects, XOR-based VC with meaningful shares is introduced in this paper. A basic algorithm implemented by a simple $2^n \times n$ matrix for constructing a (n,n) XOR-based VC is first proposed. In the following stage, a (n,n) XOR-based VC with meaningful shares is investigated by adopting the basic algorithm, where the meaningful share can be directly generated without extra process. Extensive experimental results are demonstrated, exhibiting the effectiveness and advantages of the proposed method. Further, sufficient theoretical proofs are provided for illustrating the correctness of the proposed XOR-based VC.

1. Introduction

Visual cryptography (VC) is a paradigm of cryptography which involves the notions of perfect cipher and human visual system. A conventional (k,n) threshold VC encodes a secret image into n random-liked images (called shares or shadows) in such a way that any k or more shares can visually decrypt the secret by stacking operation, whereas, any $k-1$ or less shares give no clue about the secret. VC scheme is unconditional secure and provides unbreakable encryption if a random-liked share includes truly random pixels such that it can be regarded as a one-time pad system. Unlike traditional cryptographic methods such as data encryption standard (DES) scheme and advanced encryption standard (AES) scheme, VC provides fast decryption without any complex computation.

A basic model of VC was proposed by Naor and Shamir [1], where a secret image is encrypted into several shares by using two basic matrices. To decrypt the secret, sufficient shares are printed on the transparencies and stacked together. The stacking operation can be simulated by the OR operation, as a result, the conventional VC is referred as OR-based VC. Based on the pioneer work of Naor and Shamir, many issues on OR-based VC scheme have been extensively studied, such as the meaningless share [2,3], the contrast of revealed secret image [4,5], perfect reconstruction of the black pixels [6,7], and the cheating prevention issue [8–10]. However, drawbacks such as pixel expansion and tailor-made codebook requirement still remain. To overcome the two above-mentioned problems, random grid-based VC scheme (RGVCS) is introduced. The initial model of RGVCS was introduced by Kafri and Keren [11] to encode a secret image into two random-liked shares. The size of each share is the same as that of the

* Corresponding author at: School of Software, Sun Yat-sen University, Guangzhou 510006, China.
E-mail addresses: ouduanh@mail2.sysu.edu.cn, ouduanhao@163.com (D. Ou), sunwei@mail.sysu.edu.cn (W. Sun), wxt.sysu@gmail.com (X. Wu).

http://dx.doi.org/10.1016/j.sigpro.2014.10.011
0165-1684/

Table 1
Some notations used in this work.

Notation	Description
0	A black pixel
1	A white pixel
rv	A row vector with 0 and 1 bits
$hw(rv)$	A Hamming weight of a row vector rv
$R_1, \ldots, R_n$	Shares generated by VC schemes
$R_{\{\oplus, x_1, \ldots, x_n\}}$	XOR-ed result by shares $R_{x_1}, \ldots, R_{x_n}$
α_{xor}	Contrast of the revealed secret image by XOR operation
α_{share}	Contrast of the meaningful share

original secret image, which implies pixel expansion is solved. Inspired by Kafri and Keren, extended capabilities for RGVCS including (n,n) scheme for grayscale/color image [12], $(2, n)$ scheme [13], (k,n) scheme [14] and access structure scheme [15] are further investigated. Other studies such as improving the visual quality of RGVCS [16–18] and constructing RGVCS with abilities of OR and XOR decryption [19] are presented as well. Unfortunately, shares generated by the above-mentioned VC schemes are meaningless. To manage the shares efficiently, offering meaningful shares for OR-based VC schemes [20–23] becomes inevitable.

Contrast is used to evaluate the visual quality of revealed secret image. It is expected to be as large as possible. Due to the stacking decryption, the contrast of the revealed secret image achieves at most 1/2 in OR-based VC. Such low image quality further limits the applications. In order to achieve better visual quality of revealed secret image, some XOR-based VC schemes were presented, where the secret image is decrypted by XOR operation instead of OR operation. XOR-based VC scheme is a new branch of VC system, where only some small, cheap and lightweight computational devices are needed. Due to the decryption of XOR operation, better visual quality can be achieved and the alignment problem is solved as well. Recently, many works on XOR-based VC scheme [24,25,19,26–28] have been investigated. In [28], Tuyls et al. gave some valid constructions for the XOR-based VC scheme, but codebooks are still required. Moreover, the generated shares are meaningless which may impose difficulty in managing the shares. Liu et al. [27] presented an optimal XOR-based VC scheme for improving the contrast, but the drawbacks such as meaningless share, codebook required and pixel expansion remain in their scheme. To address the above-mentioned problems, Wu and Sun [26] introduced a (n,n) XOR-based meaningful VC scheme by utilizing generalized random grid. To generate meaningful shares, the light transmission of a share should be adjusted according to the corresponding cover image. The appropriate values for the parameters related to the light transmission are difficult to be achieved, and the inappropriate parameters may lead to unexpected inhomogeneous appearance in the revealed secret image. Moreover, the visual quality of both the share and revealed secret image by Wu and Sun's scheme is still poor.

In this paper, a non-expansible XOR-based VC scheme with meaningful shares is developed. First, a basic algorithm for constructing a (n,n) XOR-based VC scheme based on a simple $2^n \times n$ matrix is given. The simple matrix can be generated by a trivial method. However, the shares generated by the basic algorithm are meaningless. Later, in order to obtain meaningful shares, a (n,n) XOR-based meaningful VC scheme is constituted by adopting the basic algorithm. The main contributions of the proposed XOR-based VC scheme are summarized as follows.

1. The proposed method solves the problems of low image quality and pixel alignment in OR-based VC scheme. The contrast of the revealed secret image by our scheme varies on the open interval $(0, 1)$, while the contrast by the OR-based VC scheme varies on the open interval $(0, 1/2)$. As a result, superior visual quality is achieved.
2. For some reported meaningful VC schemes [2,3,29,30], they generally require an extra data hiding process [31,32] to conceal random-liked shares into innocent-looking images, which increases the computation cost. Unlike the above-mentioned VC schemes, the proposed XOR-based VC scheme can directly generate meaningful shares during the sharing procedure.
3. The proposed method provides perfect reconstruction of black pixels, that is, all the revealed pixels associated to the black secret pixels are definitely black. Thus, the revealed secret image would be well identified by human visual system.
4. The application of the proposed scheme becomes flexible. By setting different parameters for different applications, the tradeoff between the visual quality of revealed image and shares varies from the application to application.
5. Sufficient theoretical proofs are provided to validate the correctness of the proposed method.

The remaining part of this paper is organized as follows. Section 2 gives some definitions on VC scheme. In Section 3, a (n,n) XOR-based VC scheme with meaningful shares is proposed. Experimental results and theoretical analysis are provided to demonstrate the feasibility of the proposed scheme in Section 4, and finally some conclusions are stated in Section 5.

2. Preliminaries

Some definitions on VC scheme are given in this section. In a (k,n) VC scheme, a secret is encoded into n

shares which are then distributed to the n related participants. Any k or more shares can visually reveal the secret image. But the knowledge of any $k-1$ or less shares gives no clue about the secret image. To facilitate expression, some notations used in this work are demonstrated in Table 1. In the following, some definitions are introduced for substantiating the analysis of the proposed XOR-based VC schemes.

Definition 1 (*Average light transmission [33,26]*). For a certain pixel p in a binary image I which is $H \times W$ in size, the probability of pixel p is white, called $Prob(p=1)$, represents the light transmission of pixel p, which is denoted as $T(p)$. The light transmission of a white pixel p is $T(p)=1$, while the light transmission of a black pixel p is $T(p)=0$. Totally, the average light transmission of I is defined as

$$T(I)=\frac{\sum_{i=1}^{H}\sum_{j=1}^{W}T(I_{i,j})}{H\times W}. \tag{1}$$

Definition 2 (*Area representation [33,26]*). Let $A(1)$ (resp. $A(0)$) be the area of all the white (resp. black) pixels in image A where $A=A(1)\cup A(0)$ and $A(1)\cap A(0)=\varnothing$. Therefore, $B[A(1)]$ (resp. $B[A(0)]$) is the corresponding area of all the white (resp. black) pixels in image B.

Definition 3 (*Contrast of the revealed secret image [33,26]*). The contrast of the revealed secret image $R_{\{\oplus,1,\ldots,n\}}=R_1\oplus\cdots\oplus R_n$ with respect to the original secret image S is

$$\alpha_{xor}=\frac{T(R_{\{\oplus,1,\ldots,n\}}[S(1)])-T(R_{\{\oplus,1,\ldots,n\}}[S(0)])}{1+T(R_{\{\oplus,1,\ldots,n\}}[S(0)])}. \tag{2}$$

The revealed secret image by XOR operation can disclose the content of the original secret image S if the contrast of the revealed secret image satisfies $\alpha_{xor}>0$ [14]. Generally, the contrast is used to evaluate the visual quality of the revealed secret image. It is expected to be as large as possible, because secret image in the revealed result can be well identified by human visual system with large α. Note that, when $T(R_{\{\oplus,1,\ldots,n\}}[S(0)])=0$, all the revealed pixels associated to the black secret pixels are definitely black. Similar to the revealed secret image, the contrast of the share is as given as Definition 4.

Definition 4 (*Contrast of the share*). The contrast of the share R with respect to the original cover image C is

$$\alpha_{share}=\frac{T(R[C(1)])-T(R[C(0)])}{1+T(R[C(0)])}. \tag{3}$$

Similarly, the share R resembles the cover image C if the contrast of the share meets $\alpha_{share}>0$; otherwise, if $\alpha_{share}=0$, the generated shares are meaningless and hard to be identified. Based on the above conclusions, security condition for a (n,n) XOR-based VC scheme is formally given as Definition 5.

Definition 5 (*Security condition*). Given n shares $R_1,\ldots,R_n$, a (n,n) XOR-based VC scheme is secure if the XOR-result of any k $(1\le k<n)$ shares does not depend on the secret image S: $T(R_{\{\oplus,x_1,\ldots,x_k\}}[S(1)])=T(R_{\{\oplus,x_1,\ldots,x_k\}}[S(0)])$, where $\{x_1,\ldots,x_k\}\subseteq\{1,\ldots,n\}$.

The above-mentioned definitions would be further employed to analyze the proposed algorithms, as described in Appendices A and B.

3. The proposed XOR-based VC schemes

In this paper, a basic algorithm for constructing a (n,n) XOR-based VC scheme is first introduced for increasing the image quality and solving the pixel expansion. Subsequently, the basic algorithm is adopted for constituting a (n,n) XOR-based VC with meaningful shares. Finally, theoretical analysis is provided to proof the correctness of the proposed scheme.

3.1. The basic algorithm for XOR-based VC scheme

A $2^n\times n$ matrix used to construct a (n,n) XOR-based VC scheme can be generated by Algorithm 1.

Algorithm 1. Generate a $2^n\times n$ matrix for (n,n) XOR-based VC scheme.

Input: A parameter n
Output: A $2^n\times n$ matrix M_n.
1: **for** $i=1$; $i<=2^n$; $i=i+1$ **do**
2: $M_n(i,1:n)=de2bi(i-1,n)$.
3: **end for**
4: Output the matrix M_n.

In Algorithm 1, function $de2bi(i-1,n)$ is to convert a decimal $i-1$ into a row vector of n bits, e.g., $de2bi(2,3)=[0,1,0]$ and $de2bi(5,4)=[0,1,0,1]$. After performing Algorithm 1, the output matrix M_n includes binary codes of the decimals from 0 to 2^n-1. Before constructing (n,n) XOR-based VC scheme, the matrix M_n would be divided into two $2^{n-1}\times n$ sub-matrices M_n^{odd} and M_n^{even}, where M_n^{odd} includes the row vectors whose hamming weigh is an odd numbers while M_n^{even} includes the row vectors whose hamming weigh is an even numbers. It is observed that two sub-matrices, M_n^{odd} and M_n^{even}, have some important properties, as described as follows:

- Given any k $(1\le k<n)$ column vectors from M_n^{odd} (M_n^{even}), and form a new $2^{n-1}\times k$ matrix by these k column vectors such that $M_k^{odd}=M_n^{odd}(1:2^{n-1},[x_1,\ldots,x_k])$ ($M_k^{even}=M_n^{even}(1:2^{n-1},[x_1,\ldots,x_k])$), where $\{x_1,\ldots,x_k\}\subseteq\{1,\ldots,n\}$. When we randomly select a row vector $M_k^{odd}(r,1:k)$ ($M_k^{even}(r,1:k)$) from the new matrix M_k^{odd} (M_k^{even}) with identical probability, the average light transmission of the XOR-ed result by $M_k^{odd}(r,1:k)$ ($M_k^{even}(r,1:k)$) is 1/2 (1/2).
- When we randomly select a row vector $M_n^{odd}(r,1:n)$ ($M_n^{even}(r,1:n)$) from M_n^{odd} (M_n^{even}) with identical probability, the average light transmission of the XOR-ed result by $M_n^{odd}(r,1:n)$ ($M_n^{even}(r,1:n)$) is 1 (0).

For example, matrix M_3 generated by Algorithm 1 and its two sub-matrices M_3^{odd} and M_3^{even} are illustrated in

Fig. 1, where matrix M_3 is 8×3 in size, and two sub-matrices are both 4×3 in size. Meanwhile, Table 2 shows the properties of matrix M_3, where $[\cdot]^T$ denotes the transpose of a matrix $[\cdot]$. It is clearly observed that the two sub-matrices M_3^{odd} and M_3^{even} have the important properties mentioned above.

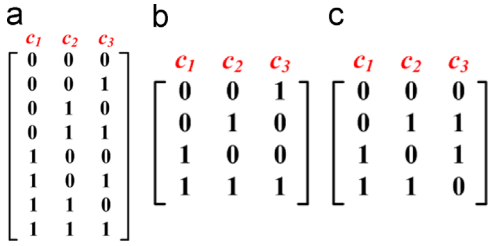

Fig. 1. The matrix M_3 and its two sub-matrices. (a) M_3, (b) M_3^{odd}, (c) M_3^{even}.

Table 2
The XOR-ed results by different combination of columns in M_3^{odd} and M_3^{even}.

Sub-matrices	M_3^{odd}	M_3^{even}
c_1	$[0\ 0\ 1\ 1]^T$	$[0\ 0\ 1\ 1]^T$
c_2	$[0\ 1\ 0\ 1]^T$	$[0\ 1\ 0\ 1]^T$
c_3	$[1\ 0\ 0\ 1]^T$	$[0\ 1\ 1\ 0]^T$
$c_1\oplus c_2$	$[0\ 1\ 1\ 0]^T$	$[0\ 1\ 1\ 0]^T$
$c_1\oplus c_3$	$[1\ 0\ 1\ 0]^T$	$[0\ 1\ 0\ 1]^T$
$c_2\oplus c_3$	$[1\ 1\ 0\ 0]^T$	$[0\ 0\ 1\ 1]^T$
$c_1\oplus c_2\oplus c_3$	$[1\ 1\ 1\ 1]^T$	$[0\ 0\ 0\ 0]^T$

With the matrix M_n generated by Algorithm 1, a basic algorithm for a (n,n) XOR-based VC scheme can be constructed, as given in Algorithm 2.

Algorithm 2. The basic algorithm for a (n,n) XOR-based VC scheme.

Input: A binary secret image S with $H\times W$ pixels, and a $2^n\times n$ matrix M_n

Output: n shares $R_1,\ldots,R_n$, each of which is $H\times W$ in size.

1. Divide the input matrix M_n into two sub-matrices, M_n^{odd} and M_n^{even}, where $M_n=M_n^{odd}\cup M_n^{even}$ and $M_n^{odd}\cap M_n^{even}=\varnothing$. First, let $M_n^{odd}=\varnothing$ and $M_n^{even}=\varnothing$. For each row vector $M_n(i,1{:}n)$ in M_n, if the hamming weight $hw(M_n(i,1{:}n))$ is an odd numbers, then add the row vector $M_n(i,1{:}n)$ into the matrix M_n^{odd}; otherwise, add the row vector $M_n(i,1{:}n)$ into the matrix M_n^{even}. When all the row vectors in M_n are processed completely, two sub-matrices M_n^{even} and M_n^{odd} are generated, each of which is $2^{n-1}\times n$ in size.
2. For each position (i,j) in the secret image S, M_n^{odd} or M_n^{even} is adopted to construct n share pixels $R_1(i,j),\ldots,R_n(i,j)$ according to the color of secret pixel $S(i,j)$.

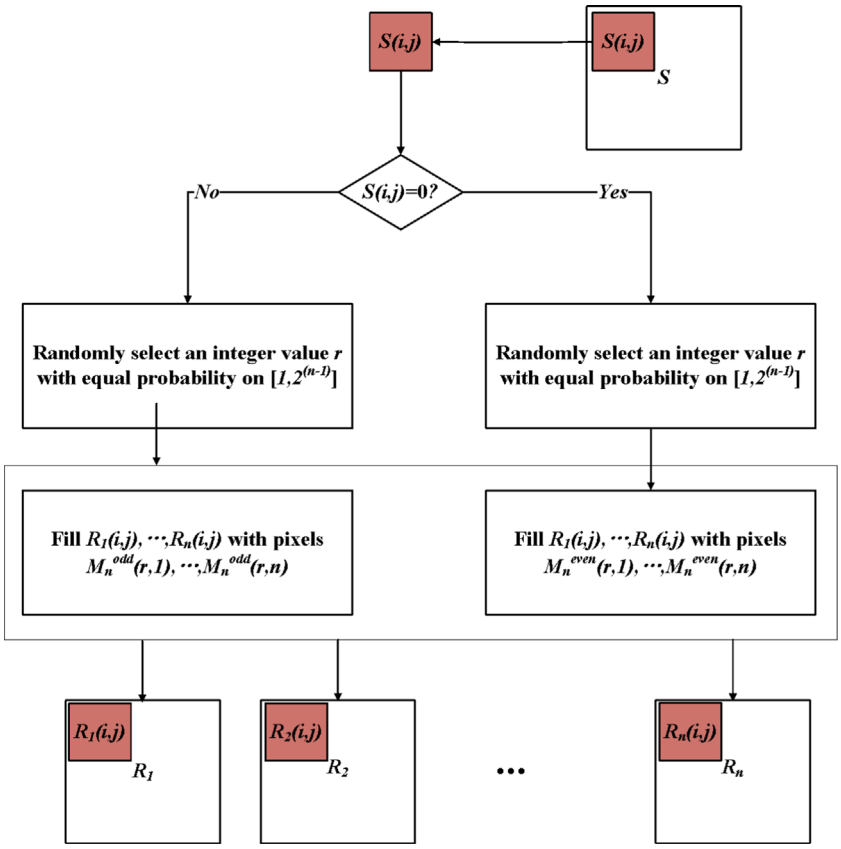

Fig. 2. Sharing procedure of the proposed (n,n) XOR-based VC scheme.

3. If $S(i,j)=0$, construct n share pixels $R_1(i,j),\ldots,R_n(i,j)$ by adopting the matrix M_n^{even}. Randomly choose a row vector $M_n^{even}(r,1:n)$ from M_n^{even} with identical probability $1/(2^{n-1})$. Subsequently, the corresponding n share pixels $R_1(i,j),\ldots,R_n(i,j)$ can be constructed by
$$R_1(i,j)=M_n^{even}(r,1),$$
$$\cdots$$
$$R_n(i,j)=M_n^{even}(r,n).$$

4. If $S(i,j)=1$, construct n share pixels $R_1(i,j),\ldots,R_n(i,j)$ by adopting the matrix M_n^{odd}. Similarly, randomly choose a row vector $M_n^{odd}(r,1:n)$ from M_n^{odd} with identical probability $1/(2^{n-1})$. Subsequently, the corresponding n share pixels $R_1(i,j),\ldots,R_n(i,j)$ can be constructed by
$$R_1(i,j)=M_n^{odd}(r,1),$$
$$\cdots$$
$$R_n(i,j)=M_n^{odd}(r,n).$$

5. Repeat Steps 2–4 until all the secret pixels are processed, and output n shares $R_1,\ldots,R_n$, each of which has the same image size as the secret image.

To show an intuitive idea of Algorithm 2, the sharing procedure for secret pixel $S(i,j)$ is illustrated in Fig. 2.

In Algorithm 2, to achieve a row vector from a $2^{n-1}\times n$ matrix M_n^{even} (M_n^{odd}) with identical probability, the following two steps should be carried out. First, generate a random value r from function $r=RANDI(2^{n-1},1)$ provided by MATLAB, where function $RANDI(2^{n-1},1)$ can generate a random integer value with equal probability $1/2^{n-1}$ on $[1,2^{n-1}]$. Second, select the $r-th$ row vector $M_n^{even}(r,1:n)$ ($M_n^{odd}(r,1:n)$) from matrix M_n^{even} (M_n^{odd}). After performing Algorithm 2, n shares are generated for (n,n) XOR-based VC scheme. With $n-1$ or less generated shares, no clue about the secret image is gained. But all n generated shares can visually reveal the secret image by XOR decryption. Theoretical analysis on Algorithm 2 is provided in Appendix A. In Appendix A, Theorem 1 formulates that Algorithm 2 is a valid construction for a (n,n) XOR-based VC scheme. Meanwhile, contrast of the revealed secret image by XOR decryption is also analyzed in Theorem 2. By Theorem 2, the contrast of the revealed secret image by Algorithm 2 is equal to 1, such that $\alpha_{xor}=1$. Thus, the revealed secret image is exactly the same as the original secret image. An example of constructing a (2,2) XOR-based VC scheme is shown in the following. A $2^2\times 2$ matrix used in a (2,2) XOR-based VC scheme is

$$M_2=\begin{bmatrix}0&0\\0&1\\1&0\\1&1\end{bmatrix},$$

which can be generated by Algorithm 1 with taking 2 as an input number. By applying Algorithm 2, matrix M_2 is first divided into two sub-matrices, as represented by

$$M_2^{odd}=\begin{bmatrix}0&1\\1&0\end{bmatrix}$$

and

$$M_2^{even}=\begin{bmatrix}0&0\\1&1\end{bmatrix}.$$

Subsequently, two shares R_1 and R_2 generated by Algorithm 2 are respectively illustrated in Fig. 4(b) and (c), where Fig. 4(a) shows an original secret image with 512×512 pixels. Observed from Fig. 4(b) and (c), the two shares are random-looking and give no clue about the secret. But the XOR-ed result $R_1\oplus R_2$ can perfectly reveal the secret, where the contrast is 1, as calculated by Definition 3. Generally, random-liked shares may impose difficulty in share management. Therefore, the basic algorithm is further utilized for constructing a XOR-based VC scheme with meaningful shares.

3.2. XOR-based VC scheme with meaningful shares

The proposed VC scheme with meaningful shares inherits the advantages of no pixel expansion, perfect reconstruction of black pixels and superior visual quality. Further, it can provide meaningful shares and make share management efficiently. Detailed description of the proposed VC scheme are given in Algorithm 3.

Algorithm 3. (n,n) XOR-based VC scheme with meaningful shares.

Input: A binary secret image S and a cover image C, both with $H\times W$ pixels, and a parameter β

Output: n meaningful shares $R_1,\ldots,R_n$, each of which is $H\times W$ in size.

1. For each position (i,j) in the secret image S, Steps 2–4 are performed to construct n share pixels $R_1(i,j),\ldots,R_n(i,j)$.
2. Generate a random bit d, which is 1 with probability β and 0 with probability $1-\beta$.
3. If $d=1$, the n corresponding share pixels are constructed by
$$R_1(i,j),\ldots,R_n(i,j)=Alg\_2((n,n),S(i,j),M_n),$$
where procedure Alg_2 is implemented by Algorithm 2, matrix M_n is generated by Algorithm 1, and $S(i,j)$ is the secret pixel.
4. If $d=0$, the following steps are carried out to construct the corresponding n share pixels. First, let $t=n\times C(i,j)$. If t is an even numbers, the n share pixels are constructed by
$$R_1(i,j)=C(i,j),\ldots,R_n(i,j)=C(i,j);$$
otherwise if t is an odd numbers, we randomly choose a number f from $\{1,\ldots,n\}$ with identical probability $1/n$, and set the $f-th$ share pixel to $1-C(i,j)$, and other $n-1$ share pixels are set to $C(i,j)$, such that
$$R_1(i,j)=C(i,j),\ldots,R_f(i,j)=1-C(i,j),\ldots,R_n(i,j)=C(i,j).$$
5. Repeat Steps 1–4 until all the secret pixels are processed, and output n shares $R_1,\ldots,R_n$, each of which has the same image size as the secret image.

Similarly, the sharing procedure for secret pixel $S(i,j)$ by Algorithm 3 is shown in Fig. 3.

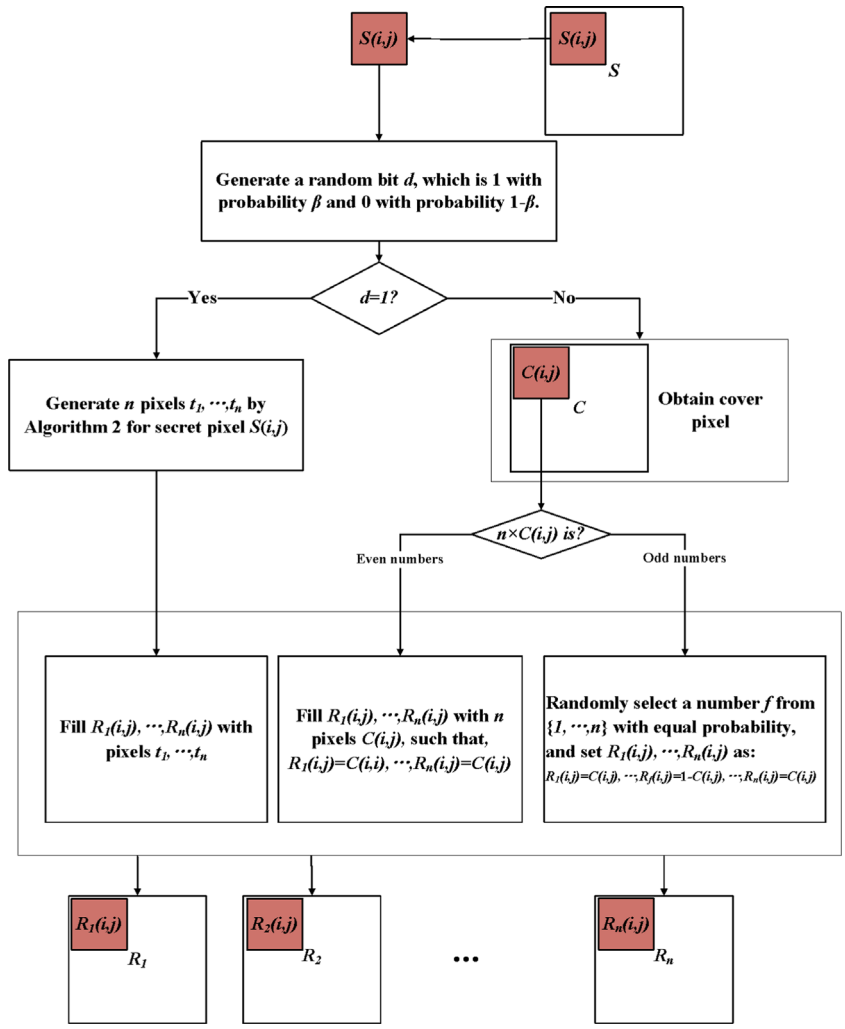

Fig. 3. Sharing procedure of (n,n) XOR-based meaningful VC scheme.

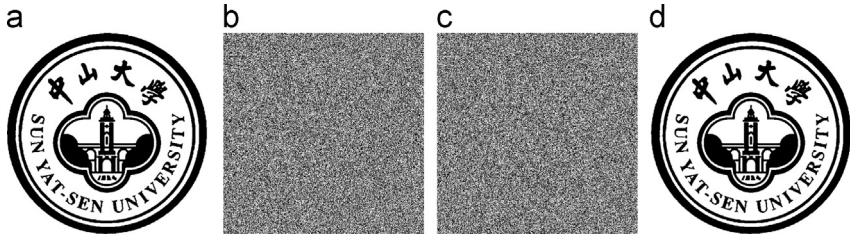

Fig. 4. Experimental results of the (2,2) case by Algorithm 2. (a) The secret image, (b) share R_1, (c) share R_2, (d) $R_1 \oplus R_2$.

As described in Algorithm 3, the proposed XOR-based VC scheme with meaningful shares is achieved by synthesizing Steps 3 and 4, where Step 3 is implemented by Algorithm 2. Step 3 to reveal the secret image on the XOR-ed result executes with probability β, whereas Step 4 to resemble the cover image on shares executes with probability $1-\beta$. It is observed that, when $\beta = 1$, Step 4 would be not performed at all and Algorithm 3 is reduced to Algorithm 2. In this case, the generated shares are meaningless. To guarantee the shares generated by Algorithm 3 are meaningful, the parameter β should meet the condition: $0 < \beta < 1$. By setting a different parameter β in open interval $(0, 1)$, the tradeoff between the visual quality of the revealed image and shares can vary from the application to application. Larger β leads to more visual-pleasing revealed images but lower image quality shares. Since the XOR-ed result of the n pixels constructed in Step 4 is always black, the XOR-ed result of all the n shares would give no clue about the cover image. Further, all the revealed pixels associated to the black secret pixels are definitely black, thus the revealed secret image can be well identified.

Table 3
Comparisons of computational complexity for the decryption among the proposed scheme and other related schemes [26,28,27,21,12,35–37], where n is the number of shares.

Schemes	Computational complexity
Ours	$O(n)$
[26]	$O(n)$
[28]	$O(n)$
[27]	$O(n)$
[21]	$O(1)$
[12]	$O(1)$
[35]	$O(1)$
[36]	$O(n\log^2 n)$
[37]	$O(n\log^2 n)$

The above conclusions are verified theoretically in Appendix B, where Theorem 3 demonstrates that Algorithm 3 is a valid construction for meaningful (n,n) XOR-based VC scheme, and Theorems 4 and 5 formulate the contrasts of a meaningful share and a revealed secret image, respectively.

3.3. Computational complexity

It is desired to calculate the computational complexity of XOR decryption by the proposed scheme. When the XOR decryption is applied, the computation complexity is proportional to the number of XOR-ed shares. Let n be the number of shares, the computation complexity is $O(n)$. Table 3 summarises the comparisons of computational complexity for the decryption among the proposed scheme and other related schemes [26,28,27,21,12,35–37]. As compared to some reported schemes [36,37] based on Shamir's method [38] which involves the polynomial evaluation and interpolation, the computational complexity of the proposed scheme requires less time. For some OR-based VC schemes [21,12,35], no computation is needed when decrypting the secret image. Hence, their computational complexity is $O(1)$. Indeed, the computation complexity of the proposed scheme and other XOR-based VC schemes [26,28,27] is relatively high as that of the OR-based VC schemes. However, the XOR-based VC schemes can achieve superior visual quality and solve the pixel alignment problem of OR-based VC schemes.

3.4. Extension for the gray-scale and color images

In this section, the proposed XOR-based VC scheme with meaningful shares is further extended to handle the gray-scale and color images. Detailed description of the two extended algorithms are illustrated in the following.

3.4.1. Gray-scale XOR-based VC scheme

Halftoning technique such as error diffusion, dot diffusion and order dithering would be employed to transform the gray-scale secret image into binary image. Meanwhile, the gray-scale cover image is required to be transformed into binary image by halftoning method. Subsequently, the transformed binary secret image and binary cover image are considered as the inputs of the proposed XOR-based VC scheme. Finally, n meaningful shares are constructed as the outputs.

3.4.2. Color XOR-based VC scheme

To share the color secret image and generate n color shares, the color decomposition, color composition and halftoning are adopted. Four steps are carried out to share the color secret image. Firstly, both the color secret image and cover image are decomposed into Cyan (C), Magenta (M), Yellow (Y) planes by using subtractive model (CMY model). Secondly, halftoning technique is applied to transform the C,M,Y planes into binary images. Thirdly, the transformed binary images are processed by the proposed XOR-based VC scheme, and the corresponding shares are constructed. Finally, the corresponding binary shares are composed together by CMY model to generate color shares.

4. Experimental results and analysis

4.1. Feasibility

Simulation results by Algorithm 3 for (2,2) case are provided in Fig. 5. Fig. 5(a) and (b) shows a 512×512 secret image and a 512×512 cover image, respectively. In Fig. 5, images $(c)-(e)$, $(f)-(h)$, $(i)-(k)$, $(l)-(n)$, $(o)-(q)$ and $(r)-(t)$ are generated with the parameter $\beta=0, 0.2, 0.4, 0.6, 0.8, 1.0$ respectively. By observing Fig. 5, it can be found that as β increases, the visual quality of shares becomes worse while the visual quality of the revealed secret image becomes better. Extremely, when $\beta=0$, the best visual quality of share is obtained, but the XOR-ed result cannot reconstruct the secret. At the other extreme, when $\beta=1$, the XOR-ed result can reconstruct the secret exactly, but the shares are meaningless. Hence, the parameter β for a XOR-based meaningful VC scheme should be met $0<\beta<1$. According to Fig. 5, Algorithm 3 for (2,2) case with $\beta\in\{0.2, 0.4, 0.6, 0.8\}$ can generate meaningful shares, and the XOR-ed results by the two generated shares can visually reveal the secret. Generally, it is accepted that contrast can reflect visual quality objectively. Thus, the contrast is used to measure the visual quality in this paper. Table 4 illustrates the contrasts of the images in Fig. 5, where the experimental contrasts for the share and revealed secret image are calculated by Definitions 4 and 3, and the theoretical contrasts for the share and revealed secret image can be obtained by equations in Theorems 5 and 4. In Table 4, the increasing of β leads to the increasing of the contrast of the revealed secret image and the decreasing of contrast of the share.

Simulation results by Algorithm 3 for (3,3) case are also provided in Fig. 6 to further demonstrate the feasibility of the proposed scheme, where β is set to 0.5. Table 5 summarizes the experimental contrasts and theoretical contrasts for (3,3) case, where β is increased from 0 to 1 by step of 0.2. It is clearly observed that the experiment contrasts are consistent with the theoretical contrasts, further, when β increases, the contrast of the revealed secret image increases but the contrast of the share decreases.

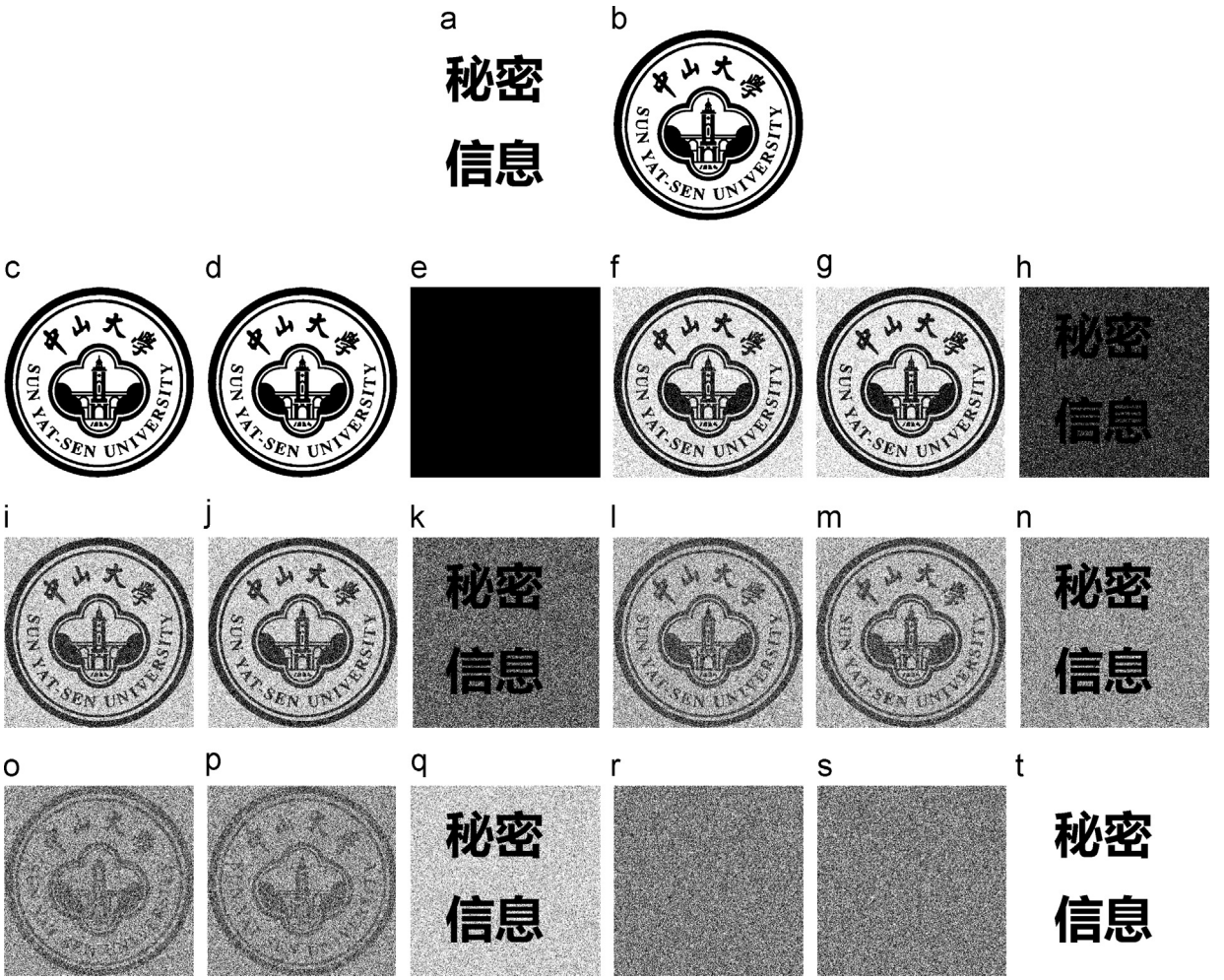

Fig. 5. Simulation results by Algorithm 3 for (2,2) case with β being $0, 0.2, 0.4, 0.6, 0.8, 1$, successively, where all of images are 512×512 in size. (a) S, (b) C, (c) R_1, (d) R_2, (e) $R_1 \oplus R_2$, (f) R_1, (g) R_2, (h) $R_1 \oplus R_2$, (i) R_1, (j) R_2, (k) $R_1 \oplus R_2$, (l) R_1, (m) R_2, (n) $R_1 \oplus R_2$, (o) R_1, (p) R_2, (q) $R_1 \oplus R_2$, (r) R_1, (s) R_2, (t) $R_1 \oplus R_2$.

Table 4
The experimental and theoretical contrasts of the revealed secret image and shares that are generated by Algorithm 3 for (2,2) case with different βs, where R_1 and R_2 denote the two shares, and $R_1 \oplus R_2$ denotes the revealed secret image.

β	Contrasts	Images		
		R_1	R_2	$R_1 \oplus R_2$
0	Experimental	1	1	0
	Theoretical	1	1	0
0.2	Experimental	0.7278	0.7290	0.2001
	Theoretical	0.7273	0.7273	0.2000
0.4	Experimental	0.4991	0.5041	0.3994
	Theoretical	0.5000	0.5000	0.4000
0.6	Experimental	0.3082	0.3083	0.5984
	Theoretical	0.3077	0.3077	0.6000
0.8	Experimental	0.1445	0.1440	0.7982
	Theoretical	0.1429	0.1429	0.8000
1.0	Experimental	−0.0006	−0.0017	1
	Theoretical	0	0	1

Moreover, a (3,3) experiment by the gray-scale XOR-based VC scheme with $\beta = 0.5$ is organized in Fig. 7. Another experiment of (3,3) color XOR-based VC scheme with $\beta = 0.5$ is depicted in Fig. 8. The two illustrated experiments demonstrate that the extended XOR-based VC scheme for gray-scale and color images does work.

4.2. Comparisons and discussions

Comparisons between our scheme and Guo et al.'s OR-based (n,n) VC scheme [21] are provided. By Theorem 4, the contrast of the revealed secret image by Algorithm 3 is β, which dose not dependent on the number of shares. Thus, no matter how large the number of shares is, the contrast of revealed secret image remains unchanged. On the other hand, the contrast of revealed secret image by Guo et al.'s scheme [21] is calculated by

$$\alpha_{or} = (\tfrac{1}{2})^{n-1} \times (1-P), \tag{4}$$

where n is the number of shares, and P is the parameter whose values is limited in [0,1]. Different from our scheme,

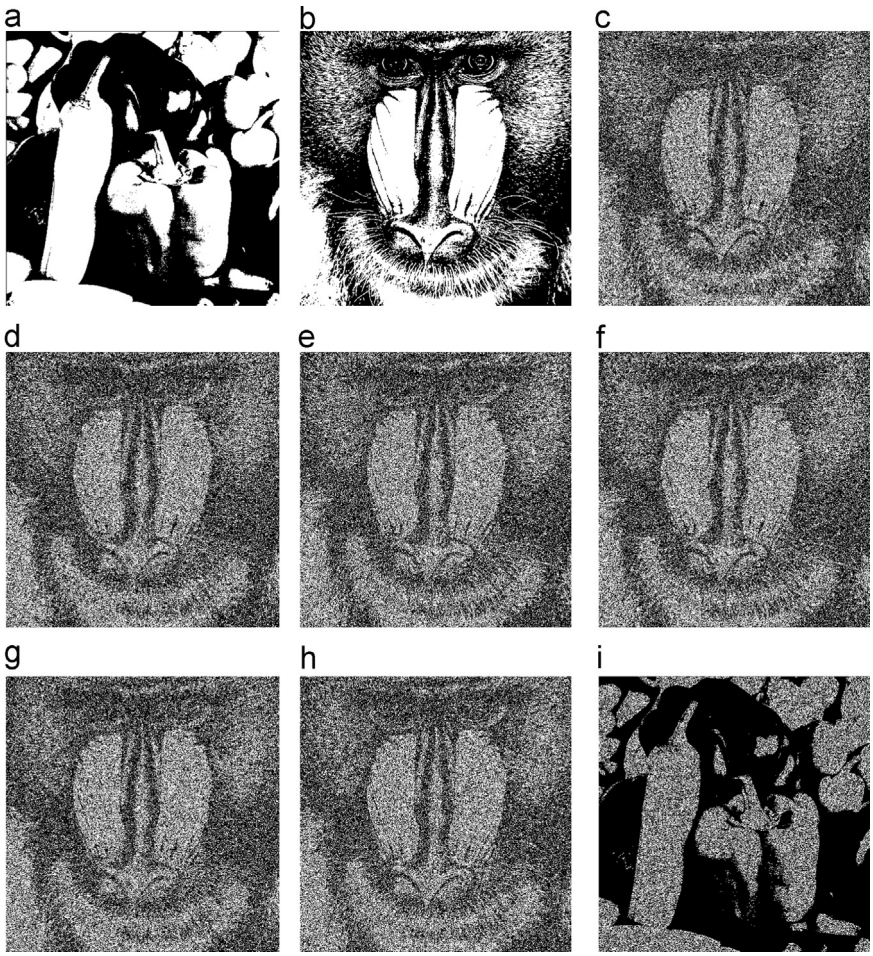

Fig. 6. Simulation results by Algorithm 3 for (3,3) case with β being 0.5, where all of images are 512×512 in size. (a) S (b) C (c) R_1, (d) R_2, (e) R_3, (f) $R_1 \oplus R_2$, (g) $R_1 \oplus R_3$, (h) $R_2 \oplus R_3$, (i) $R_1 \oplus R_2 \oplus R_3$.

Table 5
The experimental and theoretical contrasts of the revealed secret image and shares that are generated by Algorithm 3 for (3,3) case with different βs, where R_1, R_2 and R_3 denote the three shares, and $R_1 \oplus R_2 \oplus R_3$ denotes the revealed secret image.

β	Contrasts	Images			
		R_1	R_2	R_3	$R_1 \oplus R_2 \oplus R_3$
0	Experimental	0.6678	0.6644	0.6678	0
	Theoretical	0.6667	0.6667	0.6667	0
0.2	Experimental	0.4811	0.4839	0.4874	0.2012
	Theoretical	0.4848	0.4848	0.4848	0.2000
0.4	Experimental	0.3308	0.3338	0.3318	0.4011
	Theoretical	0.3333	0.3333	0.3333	0.4000
0.6	Experimental	0.2051	0.2043	0.2051	0.5998
	Theoretical	0.2051	0.2051	0.2051	0.6000
0.8	Experimental	0.0960	0.0955	0.0953	0.7989
	Theoretical	0.0952	0.0952	0.0952	0.8000
1.0	Experimental	0.0006	0.0007	−0.0007	1
	Theoretical	0	0	0	1

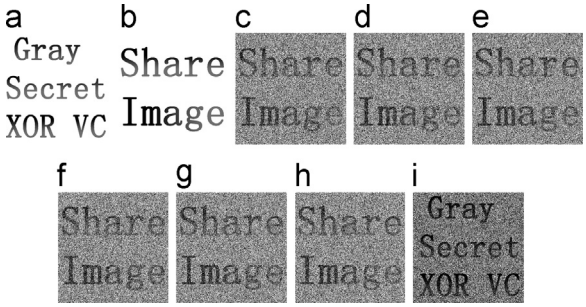

Fig. 7. A (3,3) gray-scale XOR-based VC scheme, where all the images are 512×512 in size. (a) Secret image, (b) cover image, (c) share R_1, (d) share R_2, (e) share R_3, (f) $R_1 \oplus R_2$, (g) $R_1 \oplus R_3$, (h) $R_2 \oplus R_3$, (i) $R_1 \oplus R_2 \oplus R_3$.

in Guo et al.'s OR-based VC scheme [21], as the number of shares increases, the contrast of revealed secret image goes down exponentially. The above discussions are demonstrated in Fig. 9, where the parameter P for Guo et al.'s scheme is set to 0.5 and the parameter β for our scheme is set to 0.5. In addition, as stated in Guo et al.'s

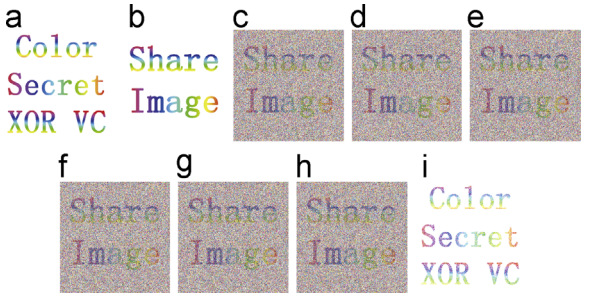

Fig. 8. A (3,3) color XOR-based VC scheme, where all the images are 512×512 in size. (a) Secret image, (b) cover image, (c) share R_1, (d) share R_2, (e) share R_3, (f)-(h) revealed results by any two shares, (i) revealed secret image by three shares.

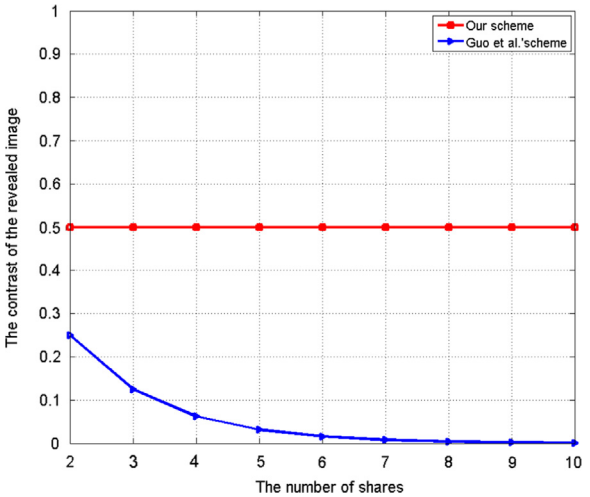

Fig. 9. Contrast curves of Algorithm 3 and Guo et al.'s [21] scheme under the share number from 2 to 10.

scheme, the contrasts of revealed secret image and shares vary in the interval [0,0.5]. However, according to Theorems 4 and 5, the contrasts of the revealed secret image and shares by our scheme can vary in a larger interval [0,1]. In the following, the contrast curves of the revealed secret image under different contrasts of the shares for our scheme and Guo et al.'s scheme are given. For our scheme, we conduct the (2,2), (3,3), (4,4), (5,5), (6,6) and (7,7) experiments with different contrasts of the shares from 0 up to 1 by step of 0.05. Similarly, for Guo et al.'s scheme, we conduct the (2,2), (3,3), (4,4), (5,5), (6,6) and (7,7) experiments with different contrasts of the shares from 0 up to 0.5 by step of 0.05. The corresponding experimental results are illustrated in Fig. 10. According to Fig. 10, while maintaining the same contrast of shares, the proposed scheme always provides larger contrast. Moreover, when the share number is large, bigger contrasts of both the revealed secret image and meaningful shares can be achieved by choosing an appropriate β in our scheme. When more shares are adopted to reconstruct the secret image, the theoretical contrast of the revealed secret image by Guo et al.'s scheme becomes much lower, whereas, the theoretical contrast by our scheme remains a high value. We conduct several experiments for our scheme and Guo et al.'s scheme when the share number n varies from 3 to 8, as shown as in Fig. 12. According to Fig. 12, when the share number $n \geq 5$, the visual quality of revealed secret image by Guo et al.'s scheme becomes much worse, whereas, the visual quality of the revealed secret image by our scheme remains pleasing. It is consistent with the conclusion obtained by theoretical analysis.

Indeed, XOR-based VC scheme offers better visual quality. However, meaningless share, tailor-made codebooks and pixel expansion remain to be continuing challenges in existing XOR-based VC schemes [28,34,27]. In 2013, Wu and Sun proposed a (n,n) XOR-based VC scheme

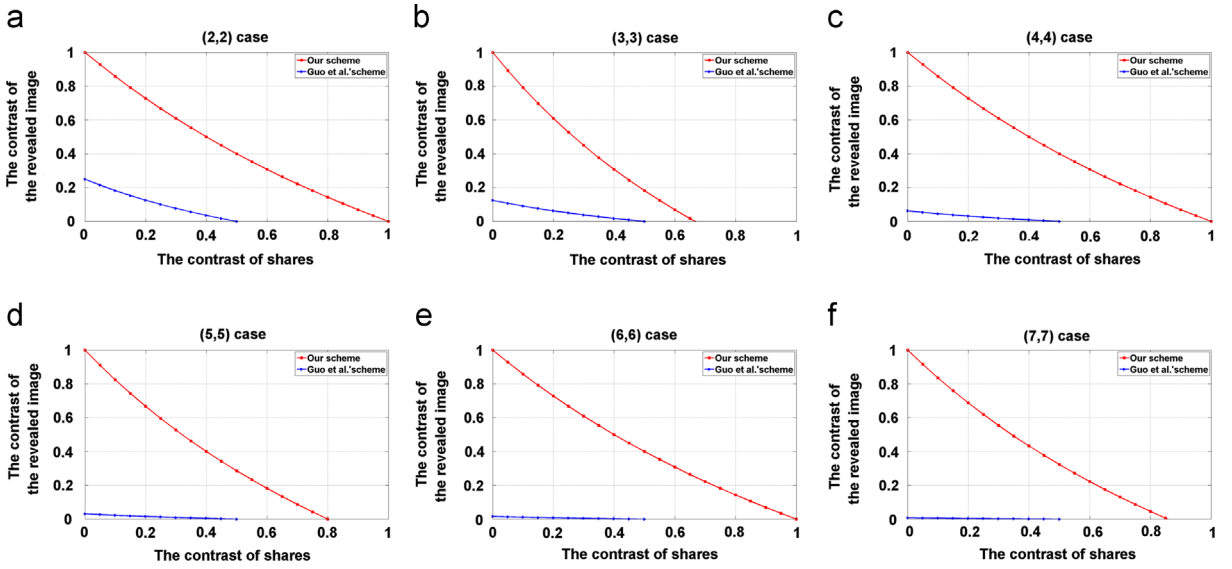

Fig. 10. Contrast curves of the revealed secret images by Algorithm 3 and Guo et al.'s scheme [21] under different contrasts of shares, where the share contrast varies from 0 to 1 by step of 0.05. (a) the (2,2) case, (b) the (3,3) case, (c) the (4,4) case, (d) the (5,5) case, (e) the (6,6) case, (f) the (7,7) case.

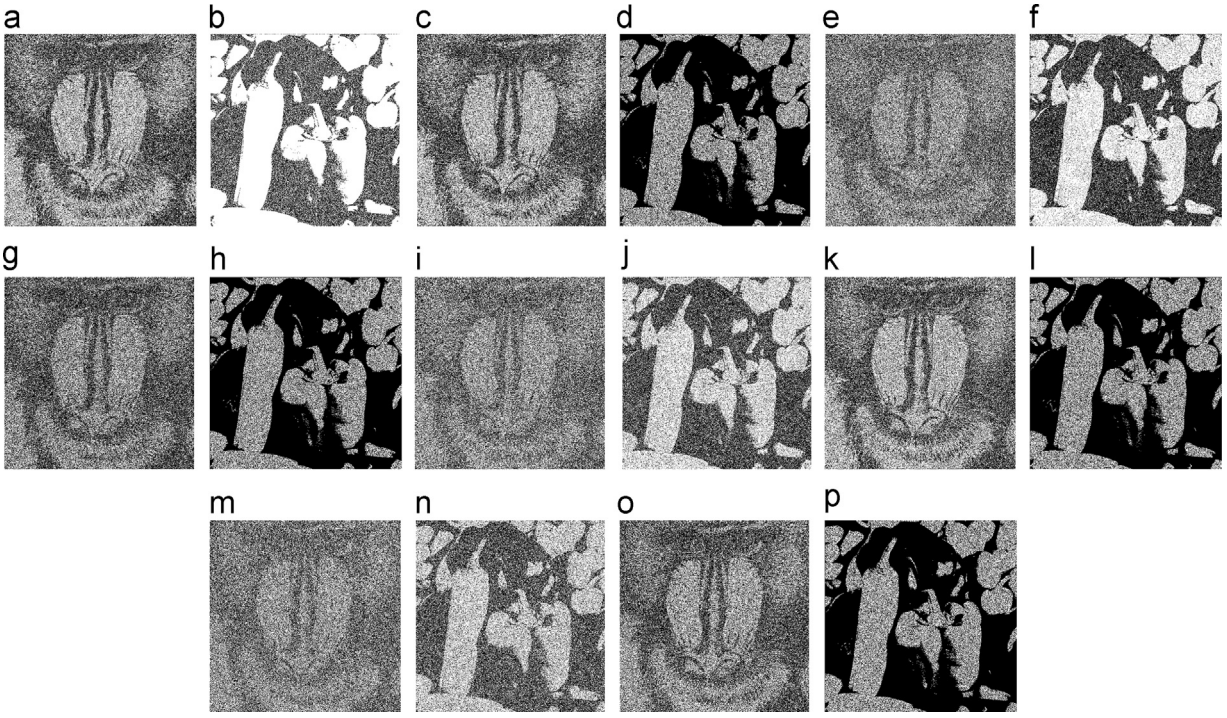

Fig. 11. Comparisons of visual quality between Algorithm 3 and Wu and Sun's scheme [26], where Fig. 6(a) and (b) are taken as the secret image and cover image, respectively. (a)-(b) Wu and Sun's (2,2) case, (c)-(d) our (2,2) case, (e)-(f) Wu and Sun's (3,3) case, (g)-(h) our (3,3) case, (i)-(j) Wu and Sun's (4,4) case, (k)-(l) our (4,4) case, (m)-(n) Wu and Sun's (5,5) case, (o)-(p) our (5,5) case.

Table 6
Comparisons of contrast for the (2,2), (3,3), (4,4) and (5,5) case between Algorithm 3 and Wu and Sun's scheme [26], where Fig. 6(a) and (b) is taken as the secret image and cover image, respectively.

Cases	Schemes	Contrasts						
		R_1	R_2	R_3	R_4	R_5	Revealed image S^R	$T(S^R[S(0)])$
(2,2)	[26]	0.3060	0.3080	-	–	-	0.4276	0.4009
	Ours	0.3078	0.3067	-	-	-	0.5983	0
(3,3)	[26]	0.1424	0.1455	0.1423	-	-	0.5114	0.2578
	Ours	0.2070	0.2056	0.2062	-	-	0.5990	0
(4,4)	[26]	0.1456	0.1423	0.1410	0.1411	-	0.3915	0.3110
	Ours	0.3096	0.3091	0.3079	0.3089	-	0.5982	0
(5,5)	[26]	0.1421	0.1427	0.1393	0.1416	0.1428	0.3073	0.3475
	Ours	0.2481	0.2463	0.2459	0.2452	0.2478	0.6019	0

for addressing the above-mentioned problems, but low visual quality still exists. To demonstrate the superiority of our scheme, another comparisons between our scheme and Wu and Sun's XOR-based (n,n) VC scheme [26] are also made. In the following, both our scheme and Wu and Sun's scheme would be applied on Figs. 6(a) and (b), where Fig. 6(a) is taken as a secret image and Fig. 6(b) is selected as a cover image. In this experiment, we conduct the (2,2), (3,3), (4,4) and (5,5) cases. Fig. 11 shows the comparisons of visual quality between our scheme and Wu and Sun's scheme under different cases. According to Fig. 11, shares generated by our scheme and Wu and Sun's scheme are with meaningful contents. To evaluate visual quality, we calculate the contrasts for the revealed images and shares of Fig. 11, as given as in Table 6. In Table 6, symbol "-" denotes "not available" which means a scheme does not provide the item. Observing from Table 6, our scheme provides larger contrast than Wu and Sun's scheme. Hence, superior visual quality is achieved. Further, $T(S^R[S(0)])$ by our scheme is always equal to 0, whereas, $T(S^R[S(0)])$ by Wu and Sun's scheme is not equal to 0. That means our scheme can provide perfect reconstruction of black pixels, but Wu and Sun's scheme dose not.

More experiments are conducted to further demonstrate the advantages of our scheme. In the experiments, 96 grey-scale images from the CVG-UGR image database (http://decsai.ugr.es/cvg/dbimagenes/) are taken as test images, where all the images are 512×512 in size. Before applying the proposed scheme, 96 512×512 grey-scale images are transformed into 96 binary images by

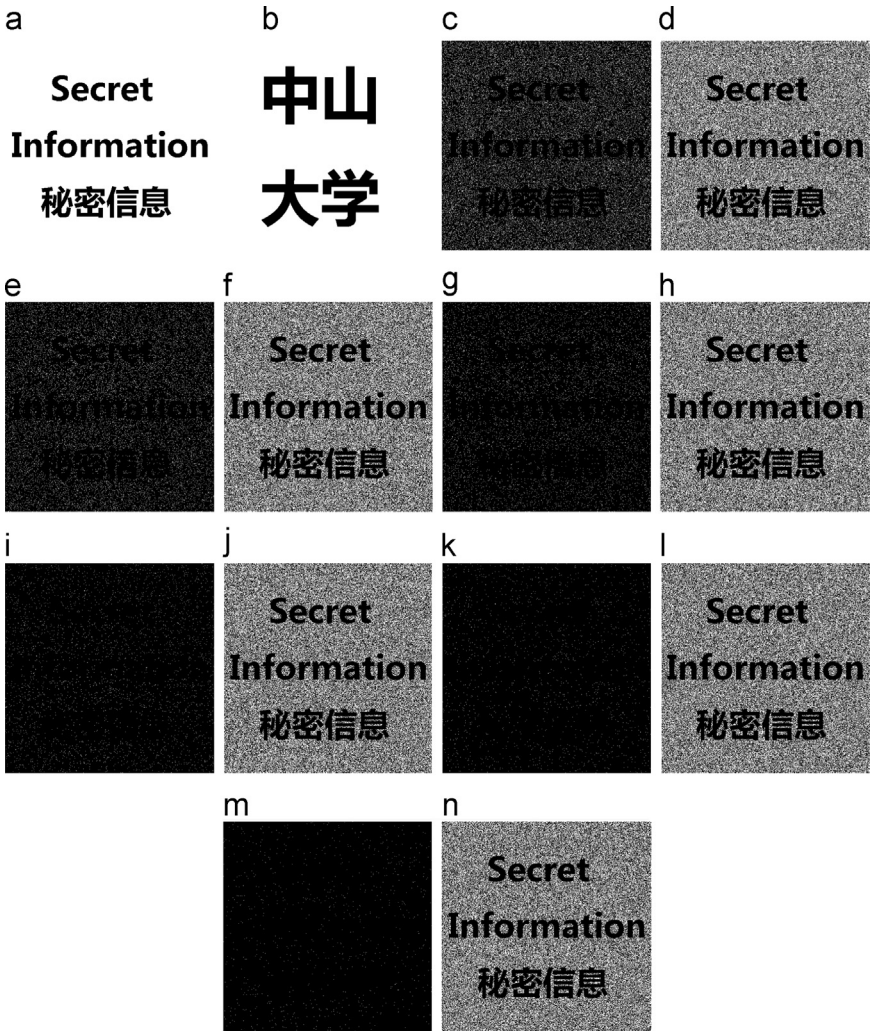

Fig. 12. The revealed secret images by our scheme and Guo et al.'s scheme [21] under different share number, where β and P are set to 0.5. (a) Secret image, (b) cover image, (c) Guo et al.'s (3,3) case, (d) our (3,3) case, (e) Guo et al.'s (4,4) case, (f) our (4,4) case, (g) Guo et al.'s (5,5) case, (h) our (5,5) case, (i) Guo et al.'s (6,6) case, (j) our (6,6) case, (k) Guo et al.'s (7,7) case, (l) our (7,7) case, (m) Guo et al.'s (8,8) case, (n) our (8,8) case.

halftoning method. In the following, we conduct the (2,2), (3,3), (4,4) and (5,5) cases respectively for our scheme, Guo et al.'s scheme [21] and Wu and Sun's scheme [26]. For each (k,k) case, where $k=2$, 3, 4, 5, randomly select 50 pairs of two different images from 96 transformed binary images, where one image in a pair is taken as a secret image and the other one is selected as a cover image. Based on the selected 50 pairs of two images, we conduct 50 experiments for (k,k) case respectively by our scheme with $\beta=0.2$, 0.5, 0.8, Guo et al.'s scheme with $P=0.2$, 0.5, 0.8 and Wu and Sun's scheme. Contrast comparisons of the revealed images among our scheme, Guo et al.'s scheme [21] and Wu and Sun's scheme [26] for different cases are illustrated in Fig. 13, and contrast comparisons of the shares among our scheme, Guo et al.'s scheme [21] and Wu and Sun's scheme [26] are illustrated in Fig. 14. According to Figs. 13 and 14, our scheme with an appropriate β achieves the largest contrast under different cases. Hence, the best visual quality is achieved. The average contrasts of 50 experiments for different cases are also calculated, and the calculated results are demonstrated in Table 7. Our scheme with an appropriate β achieves the largest contrast as compared to other schemes, which is consistent with the conclusion obtained from Figs. 13 and 14. In addition, $T(S^R[S(0)])$ by our scheme and Guo et al.'s scheme is always equal to 0, whereas, $T(S^R[S(0)])$ by Wu and Sun's scheme is not equal to 0. Hence, our scheme and Guo et al.'s scheme achieve perfect reconstruction of black pixels, but Wu and Sun's scheme does not.

Further, feature comparisons among the proposed scheme and other related schemes [26,28,34,27,21,12,14] are also demonstrated in Table 8. Major merits of the proposed scheme are given as follows:

1. Shares with meaningful contents are achieved by our scheme.
2. Meaningful shares can be directly constructed without any extra data hiding process.

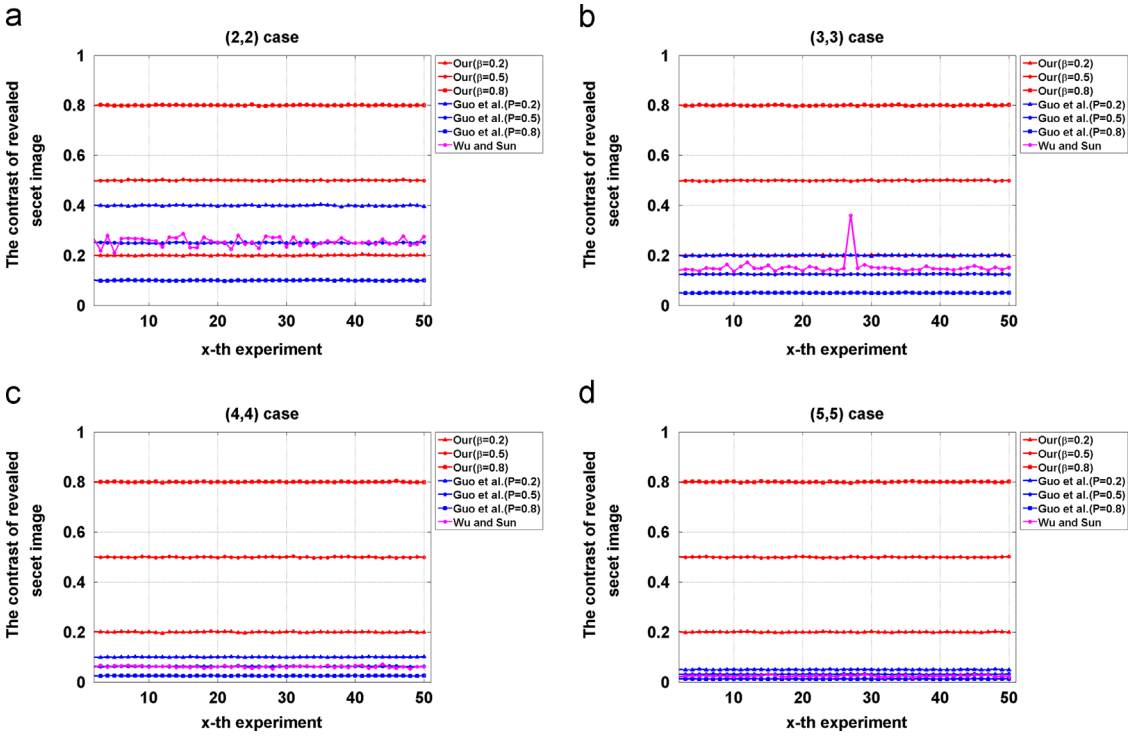

Fig. 13. Contrast comparisons of the revealed images among our scheme, Guo et al.'s scheme [21] and Wu and Sun's scheme [26] for different cases. (a) the (2,2) case, (b) the (3,3) case, (c) the (4,4) case, (d) the (5,5) case.

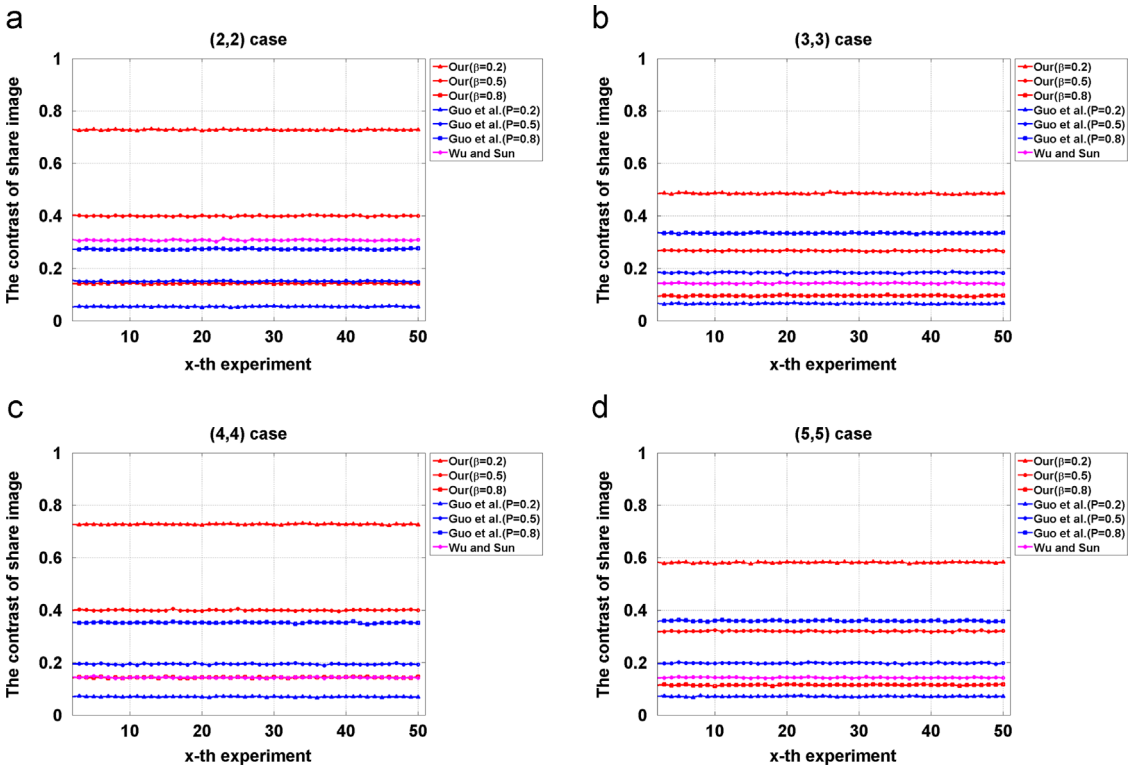

Fig. 14. Contrast comparisons of the shares among our scheme, Guo et al.'s scheme [21] and Wu and Sun's scheme [26] for different cases. (a) the (2,2) case, (b) the (3,3) case, (c) the (4,4) case, (d) the (5,5) case.

Table 7
Average contrasts of both revealed image and share for our scheme, Guo et al.'s scheme [21] and Wu and Sun's scheme [26] under different cases.

Cases	Schemes	Average			
		$T(S^R[S(1)])$	$T(S^R[S(0)])$	α for revealed image	α for share
(2,2)	Ours ($\beta=0.2$)	0.2001	0	0.2001	**0.7277**
	Ours ($\beta=0.5$)	0.5003	0	0.5003	0.3996
	Ours ($\beta=0.8$)	0.8002	0	**0.8002**	0.1424
	Guo et al.'s ($P=0.2$)	0.3994	0	0.3994	0.0537
	Guo et al.'s ($P=0.5$)	0.2502	0	0.2502	0.1502
	Guo et al.'s ($P=0.8$)	0.0999	0	0.0999	0.2725
	Wu and Sun's	0.4831	0.1829	0.2547	0.3073
(3,3)	Ours ($\beta=0.2$)	0.2000	0	0.2000	**0.4849**
	Ours ($\beta=0.5$)	0.4996	0	0.4996	0.2668
	Ours ($\beta=0.8$)	0.7999	0	**0.7999**	0.0951
	Guo et al.'s ($P=0.2$)	0.1998	0	0.1998	0.0651
	Guo et al.'s ($P=0.5$)	0.1251	0	0.1251	0.1832
	Guo et al.'s ($P=0.8$)	0.0499	0	0.0499	0.3335
	Wu and Sun's	0.2645	0.0976	0.1525	0.1428
(4,4)	Ours ($\beta=0.2$)	0.2000	0	0.2000	**0.7274**
	Ours ($\beta=0.5$)	0.4998	0	0.4998	0.3999
	Ours ($\beta=0.8$)	0.8001	0	**0.8001**	0.1430
	Guo et al.'s ($P=0.2$)	0.1000	0	0.1000	0.0694
	Guo et al.'s ($P=0.5$)	0.0626	0	0.0626	0.1941
	Guo et al.'s ($P=0.8$)	0.0251	0	0.0251	0.3523
	Wu and Sun's	0.1431	0.1347	0.0690	0.1431
(5,5)	Ours ($\beta=0.2$)	0.2001	0	0.2001	**0.5815**
	Ours ($\beta=0.5$)	0.4998	0	0.4998	0.3200
	Ours ($\beta=0.8$)	0.8002	0	**0.8002**	0.1144
	Guo et al.'s ($P=0.2$)	0.0498	0	0.0498	0.0707
	Guo et al.'s ($P=0.5$)	0.0313	0	0.0313	0.1976
	Guo et al.'s ($P=0.8$)	0.0125	0	0.0125	0.3591
	Wu and Sun's	0.0735	0.0478	0.0245	0.1426

3. The reconstruction of black pixels is perfect, which means all the revealed pixels associated to the black secret pixels are definitely black.
4. Superior visual quality is achieved as compared to some reported VC schemes.
5. No pixel expansion is achieved.

5. Conclusion

In this paper, a (n,n) XOR-based VC scheme with meaningful shares is proposed. Meanwhile, theoretical analysis is also provided to validate the correctness of the proposed scheme. The proposed scheme solves the problems of poor visual quality and pixel alignment in OR-based VC scheme. Further, other advantages of the proposed scheme are summarized as follows: (1) easy to be implemented due to the simple matrix, (2) no pixel expansion, (3) superior visual quality of both the share and revealed secret image, (4) flexibility with adjustable parameter and (5) the perfect reconstruction of black pixels. In addition, as compared to some reported meaningful VC schemes, the proposed scheme can directly generate meaningful shares without any extra data hiding process. Experimental results and discussions demonstrate the validation and superiority of the proposed scheme. In addition, our results leave the construction of (k,n) XOR-based meaningful VC scheme as an another problem for future study.

Acknowledgments

This work was in part supported by 973 Program (Grant no. 2011CB302400), Natural Science Foundation of Guangdong Province, China (Grant no. S2013010013728) and China Postdoctoral Science Foundation (Grant no. 2014M552269).

Appendix A. Theoretical analysis on Algorithm 2

In this appendix, theoretical analysis on Algorithm 2 is provided. Theorem 1 formulates that Algorithm 2 is a valid construction for a (n,n) XOR-based VC scheme. Meanwhile, contrast of the revealed secret image by XOR decryption is also analyzed in Theorem 2.

Lemma 1. *Given n shares $R_1,\ldots,R_n$ generated from Algorithm 2, each of which is a random-liked image and gives no clue about the secret image S: $T(R_k[S(0)])=T(R_k[S(1)])=1/2$, where $k=1,\ldots,n$.*

Proof. For any $1\times 2^{n-1}$ column vector in M_n^{even} (M_n^{odd}), its hamming weight is always equal to 2^{n-2} (2^{n-2}), that means the number of 1 is half of the vector length. According to Algorithm 2, a row vector would be randomly selected from M_n^{even} (M_n^{odd}) with identical probability $1/2^{n-1}$ to construct n share pixels for secret pixel 0 (1). Thus, a bit 1 or 0 is assigned to share pixel $R_k(i,j)$ $(k=1,\ldots,n)$ with probability 1/2 no matter the secret pixel $S(i,j)$ is 0 or 1. Hence, we can have $Prob(R_k(i,j)=1|S(i,j)=0)=Prob(R_k(i,j)=1|S(i,j)=1)=1/2$ $(k=1,\ldots,n)$, that implies R_k $(k=1,\ldots,n)$ is a random-liked image. By Definitions 1 and 2, we have $T(R_k[S(0)])=T(R_k[S(1)])=1/2$ $(k=1,\ldots,n)$. Therefore, every share gives no clue about the secret image except a random-liked image. □

Table 8
Feature comparisons between the proposed scheme and other related schemes [26,28,34,27,21,12,14].

Schemes	Features					
	Meaningful shares	Pixel expansion	Decryption method	Visual quality	Perfect black	Type of VC scheme
Ours	Yes	No	XOR	Higher	Yes	(n,n)
[26]	Yes	No	XOR	High	No	(n,n)
[28]	No	Yes	XOR	High	No	(k,n)
[34]	No	No	XOR	Higher	Yes	(n,n), $(2,n)$
[27]	No	Yes	XOR	High	No	$(2,n)$
[21]	Yes	No	Stack	Low	Yes	(n,n)
[12]	No	No	Stack	Low	Yes	(n,n)
[14]	No	No	Stack	Low	No	(k,n)

Lemma 2. *Given n shares $R_1,\ldots,R_n$ generated from Algorithm 2, the XOR-ed result by any k $(k<n)$ shares $R_{\{\oplus,x_1,\ldots,x_k\}}=R_{x_1}\oplus\cdots\oplus R_{x_k}$ gives no clue about the secret image S: $T(R_{\{\oplus,x_1,\ldots,x_k\}}[S(1)])=T(R_{\{\oplus,x_1,\ldots,x_k\}}[S(0)])=1/2$.*

Proof. Any k share pixels from $\{R_1(i,j),\ldots,R_n(i,j)\}$ are denoted by $R_{x_1}(i,j),\ldots,R_{x_k}(i,j)$, where $\{x_1,\ldots,x_k\}\subsetneq\{1,\ldots,n\}$. Let a row vector rv be with k elements $R_{x_1}(i,j),\ldots,R_{x_k}(i,j)$, such that $rv=[R_{x_1}(i,j),\ldots,R_{x_k}(i,j)]$.

According to Algorithm 2, when $S(i,j)=0$, a row vector would be randomly selected from matrix $M_n^{even}(1:2^{n-1},[x_1,\ldots,x_k])$ with identical probability $1/2^{n-1}$, and the selected vector is then assigned to rv. Base on the important properties of simple matrix, we have that the number of the row vectors with odd hamming weight is the same as that of the row vectors with even hamming weight in matrix $M_n^{even}(1:2^{n-1},[x_1,\ldots,x_k])$. As we known, the XOR-ed result by the row vector with even hamming weight is 0, while the XOR-ed result by the row vector with odd hamming weight is 1. Thus, the probability of row vector rv leading to a white pixel is 1/2, such that $Prob(R_{\{\oplus,x_1,\ldots,x_k\}}(i,j)=1|S(i,j)=0)=1/2$.

On the other hand, when $S(i,j)=1$, a row vector would be randomly selected from matrix $M_n^{odd}(1:2^{n-1},[x_1,\ldots,x_k])$ with identical probability $1/2^{n-1}$, and the selected vector is then assigned to rv. Similarly, based on the important properties of simple matrix, we have that the number of the row vectors with odd hamming weight is the same as that of the row vectors with even hamming weight in matrix $M_n^{odd}(1:2^{n-1},[x_1,\ldots,x_k])$. As a result, the probability of row vector rv leading to a white pixel is 1/2, such that $Prob(R_{\{\oplus,x_1,\ldots,x_k\}}(i,j)=1|S(i,j)=1)=1/2$. By Definitions 1 and 2, we have $T(R_{\{\oplus,x_1,\ldots,x_k\}}[S(1)])=T(R_{\{\oplus,x_1,\ldots,x_k\}}[S(0)])=1/2$. As a result, the XOR-ed result by any $k<n$ shares $R_{\{\oplus,x_1,\ldots,x_k\}}=R_{x_1}\oplus\cdots\oplus R_{x_k}$ gives no clue about the secret image. □

Lemma 3. *Given n shares $R_1,\ldots,R_n$ generated from Algorithm 2, the XOR-ed result by n shares $R_{\{\oplus,1,\ldots,n\}}=R_1\oplus\cdots\oplus R_n$ can visually reveal the secret image S: $T(R_{\{\oplus,1,\ldots,n\}}[S(1)])>T(R_{\{\oplus,1,\ldots,n\}}[S(0)])$.*

Proof. Let a row vector rv be with n elements $R_1(i,j),\ldots,R_n(i,j)$, such that $rv=[R_1(i,j),\ldots,R_n(i,j)]$. According to Algorithm 2, when $S(i,j)=0$, a row vector would be randomly selected from matrix M_n^{even} with identical probability $1/2^{n-1}$, and the selected vector is then assigned to rv. Based on the important properties of simple matrix, no matter which row vector of M_n^{even} has been chosen to assign to rv, its hamming weight is always an even numbers. Thus, the XOR-ed result by all bits in rv is always 0. As a result, we obtain $T(R_{\{\oplus,1,\ldots,n\}}[S(0)])=0$.

On the other hand, when $S(i,j)=1$, a row vector would be randomly selected from matrix M_n^{odd} with identical probability $1/2^{n-1}$, and the selected vector is then assigned to rv. Similarly, no matter which row vector of M_n^{odd} has been chosen to assign to rv, its hamming weight is always an odd numbers. Thus, the XOR-ed result by all bits in rv is always 1. Hence, we obtain $T(R_{\{\oplus,1,\ldots,n\}}[S(1)])=1$.

Therefore, we have $T(R_{\{\oplus,1,\ldots,n\}}[S(1)])-T(R_{\{\oplus,1,\ldots,n\}}[S(0)])=1-0=1$. It is clearly found that $T(R_{\{\oplus,1,\ldots,n\}}[S(1)])>T(R_{\{\oplus,1,\ldots,n\}}[S(0)])$. The XOR-ed result by n shares can disclose the secret image. □

Theorem 1. *Let $R_1,\ldots,R_n$ be the n shares generated from Algorithm 2. Algorithm 2 is a valid construction of XOR-based VC scheme for (n,n) case. It should meet the following conditions:*

- *Every share is a random-liked image and gives no clue about the secret image S: $T(R_k[S(0)])=T(R_k[S(1)])=1/2$, where $k=1,\ldots,n$.*
- *The XOR-ed result by any $k<n$ shares $R_{\{\oplus,x_1,\ldots,x_k\}}=R_{x_1}\oplus\cdots\oplus R_{x_k}$ is a random-like image and gives no clue about the secret image S: $T(R_{\{\oplus,x_1,\ldots,x_k\}}[S(1)])=T(R_{\{\oplus,x_1,\ldots,x_k\}}[S(0)])=1/2$.*
- *The XOR-ed result by n shares can visually reveal the secret image S: $T(R_{\{\oplus,1,\ldots,n\}}[S(1)])>T(R_{\{\oplus,1,\ldots,n\}}[S(0)])$.*

Proof. According to Lemmas 1, 2, and 3, the three conditions mentioned above are met. Hence, Algorithm 2 is a valid construction for a (n,n) XOR-based VC scheme. □

Theorem 2. *Given n shares $R_1,\ldots,R_n$ generated from Algorithm 2, the contrast of the XOR-ed result by these n shares is $\alpha_{xor}=1$.*

Proof. From the proof of Lemma 3, we have $T(R_{\{\oplus,1,\ldots,n\}}[S(1)])=1$ and $T(R_{\{\oplus,1,\ldots,n\}}[S(0)])=0$. By Definition 3, the

contrast of the XOR-ed result is calculated by

$$\alpha_{xor}=\frac{T(R_{\{\oplus,1,\ldots,n\}}[S(1)])-T(R_{\{\oplus,1,\ldots,n\}}[S(0)])}{1+T(R_{\{\oplus,1,\ldots,n\}}[S(0)])}=\frac{1-0}{1+0}=1. \quad \square \tag{A.1}$$

Appendix B. Theoretical analysis on Algorithm 3

In this appendix, theoretical analysis on Algorithm 3 is provided. Theorem 3 demonstrates that Algorithm 3 is a valid construction for the proposed XOR-based VC scheme with meaningful shares. Meanwhile, contrasts of both the meaningful share and revealed secret image are also analyzed in Theorems 4 and 5, respectively.

Lemma 4. *Every share R_k $(k=1,\ldots,n)$ generated from Algorithm 3 with $0<\beta<1$ is a meaningful image, which can resemble the cover image C: $T(R_k[C(1)])>T(R_k[C(0)])$, but gives no clue about the secret image S: $T(R_k[S(1)])=T(R_k[S(0)])$.*

Proof. If the share pixel $R_k(i,j)$ $(k=1,\ldots,n)$ is generated by Step 3 of Algorithm 3, we have $Prob(R_k(i,j)=1)=1/2$ no matter what the cover pixel and the secret pixel are. Thus, when the cover image pixel $C(i,j)=0$, we have

$$Prob\big(R_k(i,j)=1\big|C(i,j)=0\big)=\tfrac{1}{2}\beta+\big(1-\beta\big)\times(0)=\tfrac{1}{2}\beta. \tag{B.1}$$

When the cover image pixel $C(i,j)=1$, we have

$$\begin{aligned}Prob(R_k(i,j)=1|C(i,j)=1)&=\tfrac{1}{2}\beta++(1-\beta)(mod(n,2)\\&\quad\times(1-1/n)+(1-mod(n,2)))\\&=\frac{1}{2}\beta+(1-\beta)\left(1-\frac{mod(n,2)}{n}\right),\end{aligned} \tag{B.2}$$

where

$$mod(n,2)=\begin{cases}0 & n \text{ is an even number}\\ 1 & n \text{ is an odd number}\end{cases}.$$

From (Eqs. (B.1) and B.2), it is clearly seen that $Prob(R_k(i,j)=1|C(i,j)=1)>Prob(R_k(i,j)=1|C(i,j)=0)$ when $0<\beta<1$. By Definition 1, we have $T(R_k[C(1)])>T(R_k[C(0)])$, which implies the share R_k $(k=1,\ldots,n)$ is a meaningful image which can resemble the cover image.

On the other hand, when performing Step 3 of Algorithm 3, from Lemma 1, the average light transmission of the share pixel $R_k(i,j)$ $(k=1,\ldots,n)$ is always 1/2 no matter the secret pixel $S(i,j)$ is white or black. When performing Step 4 of Algorithm 3, the generation of the share pixel $R_k(i,j)$ $(k=1,\ldots,n)$ does not depend on the secret pixel $S(i,j)$, either. Based on the two cases mentioned above, the share pixel $R_k(i,j)$ $(k=1,\ldots,n)$ is generated independently on the secret pixel $S(i,j)$. Hence, we have $T(R_k[S(1)])=T(R_k(S(0)))$ $(k=1,\ldots,n)$, which implies the share R_k $(k=1,\ldots,n)$ gives no clue about the secret image. $\square$

Lemma 5. *Given n meaningful shares $R_1,\ldots,R_n$ generated from Algorithm 3, the XOR-ed result by any $k<n$ shares $R_{\{\oplus,x_1,\ldots,x_k\}}=R_{x_1}\oplus\cdots\oplus R_{x_k}$ cannot reveal any information about the secret image S: $T(R_{\{\oplus,x_1,\ldots,x_k\}}[S(1)])=T(R_{\{\oplus,x_1,\ldots,x_k\}}[S(0)])$.*

Proof. When constructing the k share pixels $R_{x_1}(i,j),\ldots,R_{x_k}(i,j)$ in Step 3 of Algorithm 3, based on Lemma 2, the average light transmission of the XOR-ed result by the k share pixels is always 1/2 no matter whether the secret pixel is white or black. On the other hand, when constructing the k share pixels $R_{x_1}(i,j),\ldots,R_{x_k}(i,j)$ in Step 4 of Algorithm 3, since the generation of these k pixels does not depend on the secret pixel $S(i,j)$, the average light transmission of their XOR-ed result is fixed to a constant value v. Since the Step 3 of Algorithm 3 is performed with probability β while Step 4 performed with probability $1-\beta$, we have

$$\begin{aligned}T\big(R_{\{\oplus,x_1,\ldots,x_k\}}[S(1)]\big)&=\frac{1}{2}\beta+(1-\beta)v\\T\big(R_{\{\oplus,x_1,\ldots,x_k\}}[S(0)]\big)&=\frac{1}{2}\beta+(1-\beta)v.\end{aligned} \tag{B.3}$$

Hence, $T(R_{\{\oplus,x_1,\ldots,x_k\}}[S(1)])=T(R_{\{\oplus,x_1,\ldots,x_k\}}[S(0)])$ is achieved. As a result, the XOR-ed result by any k shares gives no clue about the secret image. $\square$

Lemma 6. *Given n meaningful shares $R_1,\ldots,R_n$ generated from Algorithm 3, the XOR-ed result by n shares $R_{\{\oplus,1,\ldots,n\}}=R_1\oplus\cdots\oplus R_n$ can visually reveal the secret image S: $T(R_{\{\oplus,1,\ldots,n\}}[S(1)])>T(R_{\{\oplus,1,\ldots,n\}}[S(0)])$.*

Proof. When the n share pixels are constructed in Step 3 of Algorithm 3, based on the third condition of Theorem 1, for the white area of the secret image, the average light transmission of the XOR-ed result by the n shares can be calculated as $T(R_{\{\oplus,1,\ldots,n\}}[S(1)])=1$; on the other hand, for the black area of the secret image, the average light transmission of the XOR-ed by the n shares can be also calculated as $T(R_{\{\oplus,1,\ldots,n\}}[S(0)])=0$.

When the n share pixels are constructed in Step 4 of Algorithm 3, the number of 1 in n share pixels is always an even numbers. Thus, the XOR-ed result of these n share pixels is always equal to 0 no matter the secret pixel is white or black. Hence, the average light transmission of the XOR-ed result by the n share pixels generated from Step 4 is always 0. Since the Step 3 of Algorithm 3 is performed with probability β while Step 4 performed with probability $1-\beta$, we have

$$\begin{aligned}T(R_{\{\oplus,1,\ldots,n\}}[S(1)])&=\beta\times1+(1-\beta)\times0=\beta\\T(R_{\{\oplus,1,\ldots,n\}}[S(0)])&=\beta\times0+(1-\beta)\times0=0.\end{aligned} \tag{B.4}$$

Since the parameter β used in Algorithm 3 meets $0<\beta<1$, it can be clearly gained that $T(R_{\{\oplus,1,\ldots,n\}}[S(1)])>T(R_{\{\oplus,1,\ldots,n\}}[S(0)])$. As a result, the XOR-ed result by n shares can visually reveal the secret image. $\square$

Lemma 7. *Given n meaningful shares $R_1,\ldots,R_n$ generated from Algorithm 3, the XOR-ed result by n shares $R_{\{\oplus,1,\ldots,n\}}=R_1\oplus\cdots\oplus R_n$ gives no clue about the cover image C: $T(R_{\{\oplus,1,\ldots,n\}}[C(1)])=T(R_{\{\oplus,1,\ldots,n\}}[C(0)])$.*

Proof. Since the Step 3 of Algorithm 3 is performed independently on the cover image C, we have $T(R_{\{\oplus,1,\ldots,n\}}[C(1)])=T(R_{\{\oplus,1,\ldots,n\}}[C(0)])=1/2$. On the other hand, when the Step 4 of Algorithm 3 is performed, the XOR-ed result of n share pixels is always equal to 0 no matter the cover image pixel is white or black. Since the Step 3 of Algorithm 3 is performed with probability β

while Step 4 performed with probability $1-\beta$, we have

$$T(R_{\{\oplus,1,\ldots,n\}}[C(1)]) = \beta \times 1/2 + (1-\beta) \times 0 = \frac{\beta}{2}$$

$$T(R_{\{\oplus,1,\ldots,n\}}[C(0)]) = \beta \times 1/2 + (1-\beta) \times 0 = \frac{\beta}{2}. \quad \text{(B.5)}$$

Hence, $T(R_{\{\oplus,1,\ldots,n\}}[C(1)]) = T(R_{\{\oplus,1,\ldots,n\}}[C(0)])$. As a result, the XOR-ed result gives no clue about the cover image. □

Theorem 3. *Let $R_1,\ldots,R_n$ be the n shares generated from Algorithm 3 with $0<\beta<1$. Algorithm 3 with $0<\beta<1$ is a valid construction for (n,n) XOR-based VC scheme with meaningful shares. The following conditions are met*:

- *Every share R_k is a meaningful image which can resemble the cover image C: $T(R_k[C(1)]) > T(R_k[C(0)])$, but gives no clue about the secret image S: $T(R_k[S(1)]) = T(R_k[S(0)])$, where $k=1,\ldots,n$.*
- *The XOR-ed result by any $k<n$ shares $R_{\{\oplus,x_1,\ldots,x_k\}} = R_{x_1} \oplus \cdots \oplus R_{x_k}$ cannot reveal any information about the secret image S: $T(R_{\{\oplus,x_1,\ldots,x_k\}}[S(1)]) = T(R_{\{\oplus,x_1,\ldots,x_k\}}[S(0)])$.*
- *The XOR-ed result by the n shares $R_{\{\oplus,1,\ldots,n\}} = R_1 \oplus \cdots \oplus R_n$ can visually disclose the secret image S: $T(R_{\{\oplus,1,\ldots,n\}}[S(1)]) > T(R_{\{\oplus,1,\ldots,n\}}[S(0)])$. Especially, the XOR-ed result by n shares only carries the secret information and gives no clue about the cover image C: $T(R_{\{\oplus,1,\ldots,n\}}[C(1)]) = T(R_{\{\oplus,1,\ldots,n\}}[C(0)])$.*

Proof. According to Lemmas 4–7, the three conditions are satisfied. Hence, Algorithm 3 with $0<\beta<1$ is a valid construction for (n,n) XOR-based VC scheme with meaningful shares. □

Theorem 4. *Given n shares $R_1,\ldots,R_n$ generated from Algorithm 3 with the parameter β, the contrast of the XOR-ed result by these n shares is $\alpha_{xor}=\beta$.*

Proof. From the proof of Lemma 6, we have $T(R_{\{\oplus,1,\ldots,n\}}[S(1)]) = \beta$ and $T(R_{\{\oplus,1,\ldots,n\}}[S(0)]) = 0$. By definition 3, the contrast of the XOR-ed result can be calculated by

$$\alpha_{xor} = \frac{T(R_{\{\oplus,1,\ldots,n\}}[S(1)]) - T(R_{\{\oplus,1,\ldots,n\}}[S(0)])}{1+T(R_{\{\oplus,1,\ldots,n\}}[S(0)])} = \frac{\beta-0}{1+0} = \beta. \quad \square \quad \text{(B.6)}$$

Remark. As stated in Definitions 1 and 2, $T(R_{\{\oplus,1,\ldots,n\}}[S(0)]) = 0$ means all the revealed pixels associated to the black secret pixels are definitely black. It can help to well identify the revealed secret image by human visual system. As β increases, the contrast α_{xor} varies on the open interval $(0,1)$. However, the contrast by OR-based VC scheme achieves at most 1/2. Further, since the contrast of the revealed secret image α_{xor} is dependent of the share number n, α_{xor} remains unchanged as more shares are adopted.

Theorem 5. *Given the share R_k $(k=1,\ldots,n)$ generated from Algorithm 3 with $0<\beta<1$, the contrast of the share R_k is*

$$\alpha_{share} = \begin{cases} \dfrac{1-\beta}{1+\frac{1}{2}\beta} & n \text{ is an even number} \\ \dfrac{(1-\beta)(1-1/n)}{1+\frac{1}{2}\beta} & n \text{ is an odd number} \end{cases}. \quad \text{(B.7)}$$

Proof. From the proof of Lemma 4, we have two following cases.

1. When n is an even numbers, based on Eqs. (B.1) and (B.2), we have

   $$T(R_k[C(0)]) = \frac{1}{2}\beta,$$
   $$T(R_k[C(1)]) = \frac{1}{2}\beta + (1-\beta) = 1-\frac{1}{2}\beta.$$

   By Definition 4, the contrast of the share R_k is calculated by

   $$\alpha_{share} = \frac{T(R_k[C[1]]) - T(R_k[C(0)])}{1+T(R_k[C(0)])} = \frac{1-\frac{1}{2}\beta-1/2\beta}{1+\frac{1}{2}\beta} = \frac{1-\beta}{1+\frac{1}{2}\beta},$$

   where $k=1,\ldots,n$.
2. When n is an odd numbers, based on Eqs. (B.1) and (B.2), we have

   $$T(R_k[C(0)]) = \frac{1}{2}\beta,$$
   $$T(R_k[C(1)]) = \frac{1}{2}\beta + (1-\beta)(1-1/n).$$

   By Definition 4, the contrast of the share R_k is calculated by

   $$\alpha_{share} = \frac{T(R_k[C[1]]) - T(R_k[C(0)])}{1+T(R_k[C(0)])} = \frac{\frac{1}{2}\beta + (1-\beta)(1-1/n) - \frac{1}{2}\beta}{1+\frac{1}{2}\beta} = \frac{(1-\beta)(1-1/n)}{1+\frac{1}{2}\beta},$$

   where $k=1,\ldots,n$.

The two cases mentioned above will easily lead to the conclusion immediately. □

Remark. Based on the proof of Theorem 5, when the share number n is an even numbers, the contrast of the share by Algorithm 3 is fixed to $(1-\beta)/(1+\frac{1}{2}\beta)$, which does not depend on the share number n. As the parameter β varies, the contrast of the share can vary on the open interval $(0,1)$. Once the value of parameter β is set, the contrast of the share remains unchanged even if n is a very large even numbers. On the other hand, when n is an odd numbers, the contrast of the shares can be stated as $(1-\beta)\ (1-1/n)/(1+\frac{1}{2}\beta)$. Similarly, as the parameters β and n varies, the contrast of the shares varies on the open interval $(0,2/3)$.

References

[1] M. Naor, A. Shamir, Visual cryptography, in: Advances in Cryptology EUROCRYPT'94, Springer, 1995, pp. 1–12.
[2] Z. Wang, G.R. Arce, G. Di Crescenzo, Halftone visual cryptography via error diffusion, IEEE Trans. Inf. Forensics Secur. 4 (2009) 383–396.

[3] F. Liu, C. Wu, Embedded extended visual cryptography schemes, IEEE Trans. Inf. Forensics Secur. 6 (2011) 307–322.
[4] T. Hofmeister, M. Krause, H.U. Simon, Contrast-optimal k out of n secret sharing schemes in visual cryptography, Theor. Comput. Sci. 240 (2000) 471–485.
[5] C. Blundo, P. D'Arco, A. De Santis, D.R. Stinson, Contrast optimal threshold visual cryptography schemes, SIAM J. Discret. Math. 16 (2003) 224–261.
[6] C. Blundo, A. De Bonis, A. De Santis, Improved schemes for visual cryptography, Des. Codes Cryptogr. 24 (2001) 255–278.
[7] H. Koga, E. Ueda, Basic properties of the (t, n)-threshold visual secret sharing scheme with perfect reconstruction of black pixels, Des. Codes Cryptogr. 40 (2006) 81–102.
[8] C.M. Hu, W.G. Tzeng, Cheating prevention in visual cryptography, IEEE Trans. Image Process. 16 (2007) 36–45.
[9] Y.C. Chen, G. Horng, D.S. Tsai, Comment on cheating prevention in visual cryptography, IEEE Trans. Image Process. 21 (2012) 3319–3323.
[10] Y.S. Lee, T.H. Chen, Insight into collusion attacks in random-grid-based visual secret sharing, Signal Process. 92 (2012) 727–736.
[11] O. Kafri, E. Keren, Encryption of pictures and shapes by random grids, Opt. Lett. 12 (1987) 377–379.
[12] S.J. Shyu, Image encryption by multiple random grids, Pattern Recognit. 42 (2009) 1582–1596.
[13] T.H. Chen, K.H. Tsao, Visual secret sharing by random grids revisited, Pattern Recognit. 42 (2009) 2203–2217.
[14] T. Chen, K. Tsao, Threshold visual secret sharing by random grids, J. Syst. Softw. 84 (2011) 1197–1208.
[15] X. Wu, W. Sun, Visual secret sharing for general access structures by random grids, Inf. Secur. IET 6 (2012) 299–309.
[16] S.K. Chen, S.J. Lin, Optimal (2, n) and (2, infinity) visual secret sharing by generalized random grids, J. Vis. Commun. Image Represent. 23 (2012) 677–684.
[17] X. Wu, T. Liu, W. Sun, Improving the visual quality of random grid-based visual secret sharing via error diffusion, J. Vis. Commun. Image Represent. 24 (2013) 552–556.
[18] X. Wu, W. Sun, Improving the visual quality of random grid-based visual secret sharing, Signal Process. 93 (2013) 977–995.
[19] X. Wu, W. Sun, Random grid-based visual secret sharing with abilities of or and xor decryptions, J. Vis. Commun. Image Represent. 24 (2013) 48–62.
[20] T.H. Chen, K.H. Tsao, User-friendly random-grid-based visual secret sharing, IEEE Trans. Circuits Syst. Video Technol. 21 (2011) 1693–1703.
[21] T. Guo, F. Liu, C. Wu, k out of k extended visual cryptography scheme by random grids, Signal Process. 94 (2013) 90–101.
[22] X. Wu, W. Sun, Improved tagged visual cryptography by random grids, Signal Process. 97 (2014) 64–82.
[23] D. Ou, W. Sun, Reversible AMBTC-based secret sharing scheme with abilities of two decryptions, J. Vis. Commun. Image Represent. 25 (2014) 1222–1239.
[24] C.N. Yang, D.S. Wang, Property analysis of XOR-based visual cryptography, IEEE Trans. Circuits Syst. Video Technol. 24 (2014) 189–197.
[25] X. Wu, D. Ou, L. Dai, W. Sun, Xor-based meaningful visual secret sharing by generalized random grids, in: Proceedings of the First ACM Workshop on Information Hiding and Multimedia Security, ACM, 2013, pp. 181–190.
[26] X. Wu, w. Sun, Generalized random grid and its applications in visual cryptography, IEEE Trans. Inf. Forensics Secur. 8 (2013) 1541–1553.
[27] F. Liu, C.K. Wu, Optimal xor based (2, n)-visual cryptography schemes, IACR Cryptol., 545, (2010), ePrint Archive.
[28] P. Tuyls, H.D. Hollmann, J.H. Van Lint, L. Tolhuizen, Xor-based visual cryptography schemes, Des. Codes Cryptogr. 37 (2005) 169–186.
[29] G. Ateniese, C. Blundo, A.D. Santis, D.R. Stinson, Extended capabilities for visual cryptography, Theor. Comput. Sci. 250 (2001) 143–161.
[30] Z. Zhou, G.R. Arce, G. Di Crescenzo, Halftone visual cryptography, IEEE Trans. Image Process. 15 (2006) 2441–2453.
[31] D. Ou, W. Sun, High payload image steganography with minimum distortion based on absolute moment block truncation coding, Multim. Tools Appl. (2014) 1–23.
[32] C.K. Chan, L.M. Cheng, Hiding data in images by simple LSB substitution, Pattern recognit. 37 (2004) 469–474.
[33] S.J. Shyu, Image encryption by random grids, Pattern Recognit. 40 (2007) 1014–1031.
[34] D. Wang, L. Zhang, N. Ma, X. Li, Two secret sharing schemes based on boolean operations, Pattern Recognit. 40 (2007) 2776–2785.
[35] C.N. Yang, New visual secret sharing schemes using probabilistic method, Pattern Recognit. Lett. 25 (2004) 481–494.
[36] C. Lin, W. Tsai, Secret image sharing with steganography and authentication, J. Syst. Softw. 73 (2004) 405–414.
[37] C. Yang, T. Chen, K.H. Yu, C. Wang, Improvements of image sharing with steganography and authentication, J. Syst. Softw. 80 (2007) 1070–1076.
[38] A. Shamir, How to share a secret, Commun. ACM 22 (1979) 612–613.