IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received September 9, 2018, accepted October 2, 2018, date of publication October 8, 2018, date of current version November 8, 2018.

Digital Object Identifier 10.1109/ACCESS.2018.2874527

Visual Cryptography Scheme With Meaningful Shares Based on QR Codes

ZHENGXIN FU, YUQIAO CHENG, AND BIN YU
Zhengzhou Information Science and Technology Institute, Zhengzhou 450001, China

Corresponding author: Yuqiao Cheng (xdqiao2015@163.com)

This work was supported in part by the National Natural Science Foundation of China under Grant 61602513 and in part by the Outstanding Youth Foundation of the Zhengzhou Information Science and Technology Institute under Grant 2016611303.

ABSTRACT In the past few years, visual cryptography scheme (VCS) has aroused much research attention and developed rapidly because of its simple decryption. However, meaningless shares remain a continuing challenge of VCS to its practical applications. In this paper, we propose a (k, n)-VCS combining with QR codes. To enlarge the allowable maximum size of secret image, a probabilistic sharing model is utilized. Based on it, a secret sharing method is presented with high relative difference. Furthermore, we embed the initial shares into cover QR codes by using encoding redundancy. After that, each share is meaningful and can be read by any standard QR code reader. Different from previous work, error correction capacities of the covers are perfectly preserved. We also highlight that our scheme can be used to authenticate the security of QR codes from some uncertain sources. Finally, experimental results and comparisons are provided to show the feasibility and advantages of the proposed scheme.

INDEX TERMS Encoding redundancy, high relative difference, (k, n)-VCS, meaningful shares, probabilistic sharing method, QR codes.

I. INTRODUCTION

Visual cryptography scheme [1] (VCS) is a kind of image sharing technology that was first proposed by Naor and Shamir. The basic model of VCS is to distribute a secret image into a number of shares. The secret can be visually decrypted by stacking any qualified subset of shares while forbidden subsets cannot. Because of low-computation decryption, VCS has attracted much research attention, and related studies have been continuously investigated, including recovery effect promotion [2]–[4], access structure flexibility [5], [6], image color extension [7], [8] and sharing strategy enrichment [9]–[11]. However, shares in most schemes are meaningless, which will easily arouse attackers' suspicion when transmitting via public channels, and in addition, inconvenience of managing these shares is increased. To generate meaningful shares, [1] and [12]–[14] added some columns to the basis matrices. These extra columns were used to carry the cover information of each share. For better visual effect, [15]–[17] introduced halftone technology into the design of schemes. However, there was still much noise visible in the shares with poor visual effect.

QR code is a kind of machine recognition code developed by the Japanese Denso Wave Company, and now has been adopted as a universal specification performed by ISO [18]. With the development of intelligent handset technology, QR code has been widely used in applications such as product propaganda, electric identity and mobile payment. Because of the low visual recognition feature, acquiring the message of a QR code by human vision is almost impossible. In turn, the QR code can be an excellent mask for VCS since its dark and light modules are evenly distributed with random look. Therefore, combinations of the VCS and QR codes have been considerably investigated [19]–[22], [27]. Based on machine recognition characteristic, a scheme with two-level information storage was presented [21]. In that scheme, decoding shares were inconvenient unless a quite appropriate scanning distance and angle is found. And then, a (n, n) sharing method was designed by exploiting error correction mechanism of QR codes [22]. Later, under random grids theory [23]–[26], a (k, n)-VCS were implemented in [27], where relative difference of the recovered secret requires further improving. Moreover, error correction capacities of the shares were decreased in [22] and [27] since some codewords were modified during the sharing process. That may influence the robustness of QR codes to symbol damage or loss.

In this paper, we propose a (k, n)-VCS combining with QR codes. By classifying all minimal qualified subsets, we present a method of constructing sharing matrix sets.

This design is based on probabilistic sharing model, of which the unexpanded property allows larger secret size. Additionally, higher, or even perfect, recovered performance can be achieved. Further, we utilize the encoding redundancy of QR codes to embed original shares into their corresponding covers. Finally, a number of meaningful shares are obtained. Compared with previous work, error correction capacities are fully preserved in this paper. Experimental results and comparisons show the effectiveness of the proposed scheme.

The remainder of this paper is organized as follows. Section II introduces some preliminaries concerning our study. The proposed scheme is described in Section III while its validity is theoretically proved in Section IV. Section V provides the experiments and analysis to illustrate the feasibility of this work and how it improves on previous work. Finally, conclusions are given in Section VI.

II. PRELIMINARIES

The maximum size of QR codes limits the largest secret payload allowable in QR codes. The larger pixel expansion means the smaller size of secret image. Therefore, probabilistic method [28]–[30] is adopted because it has no pixel expansion.

A. PROBABILISTIC METHOD

By probabilistic method, secret pixels are correctly restored with a certain probability. To promote an understanding of the subsequent results, Table I gives the denotation of symbols used in our study.

TABLE 1. Denotation of symbols.

Symbol	Denotation
$P_i \circ P_j$	all possible results obtained by any two elements from P_i and P_j, respectively
$M_{k,even}$	a matrix consisting of all k-dimensional columns with even weight
$M_{k,odd}$	a matrix consisting of all k-dimensional columns with odd weight
$B(i)$	row i of matrix B
$B(i, j)$	element j of row $B(i)$
B_Q	a sub-matrix constituted by rows $i_1, i_2, \cdots, i_t$ of matrix B if $Q = \{i_1, i_2, \cdots, i_t\}$
$\mathrm{Tr}(A)$	a vector set of all columns of A
$\mathrm{con}(A, B)$	horizontally connect matrix A with matrix B
$\mathrm{del}(A, B)$	delete common columns of matrices A and B
$\oplus(A)$	the result of XOR-ing all rows of matrix A
$n(v)$	the number of 0 in vector v
$p(R)$	the possibility of [0] in set R

Definition 1: Suppose there are two sets of n-dimensional columns $C_0 = \{\alpha_1, \alpha_2, \cdots, \alpha_h\}$ and $C_1 = \{\beta_1, \beta_2, \cdots, \beta_t\}$. To share a white (or black) pixel, we randomly select a column from C_1 (or C_0) and distribute its row i to share i. Then, a (k, n)-VCS based on probabilistic method is formed if C_0 and C_1 satisfy the following conditions.

(a) For any subset $Q = \{i_1, i_2, \cdots, i_k\} \subseteq \{1, 2, \cdots, n\}$, there is

$$p(\{\oplus(\alpha_{1Q}), \oplus(\alpha_{2Q}), \cdots, \oplus(\alpha_{mQ})\}) > p(\{\oplus(\beta_{1Q}), \oplus(\beta_{2Q}), \cdots, \oplus(\beta_{mQ})\}).$$

(b) For any subset $Q' = \{i_1, i_2, \cdots, i_t\} \subseteq \{1, 2, \cdots, n\}$ $(t < k)$, there is

$$p(\{\oplus(\alpha_{1Q'}), \oplus(\alpha_{2Q'}), \cdots, \oplus(\alpha_{mQ'})\}) = p(\{\oplus(\beta_{1Q'}), \oplus(\beta_{2Q'}), \cdots, \oplus(\beta_{mQ'})\}).$$

(a) is contrast condition, which indicates that any k participants can obtain the secret information by probabilistic difference. And if there are more than k participants, only k from them are required. (b) is security condition, ensuring that less than k participants are inaccessible to the secret.

B. QR CODES

QR codes have a number of data capacities under different V-E. V (1∼40) is the version number, which determines the size of a QR code. E (L, M, Q, H) denotes four error correction levels, corresponding to four error correction capacities (7%, 15%, 25%, 30%), respectively. Fig. 1 is the structure of version 7.

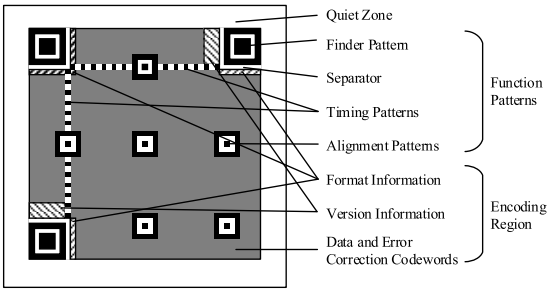

FIGURE 1. Symbol structure of version 7.

As shown, each QR code includes two parts: encoding region and functional patterns. The former contains version or format information, data and error correction codewords. The latter includes some patterns designed for geometric correction and efficient recognition. Fig. 2 illustrates the main encoding and decoding procedures of a QR code.

During the encoding procedure, XOR-ing with mask patterns are required to guarantee that 1011101 will not occur in regions out of finder patterns, avoiding influence on symbol orientation. Because the white and black pixels of original shares are randomly distributed, symbol orientation of QR codes will not be affected even if the shares are embedded. So the version and format information of cover QR codes are unchanged in our design.

In addition, a QR code may have multiple blocks. Each block is composed of some data codewords and corresponding error correction codewords calculated by Reed-Solomon code. In Section III-B, all operations on codewords are performed block by block.

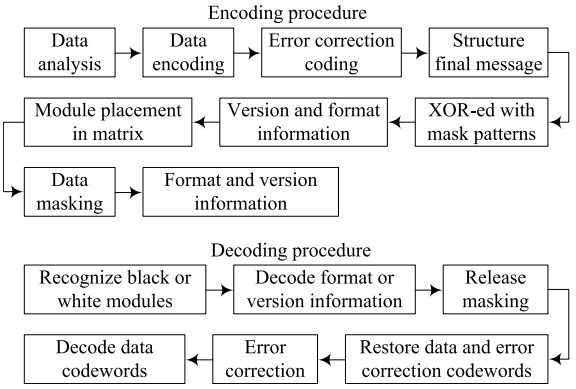

FIGURE 2. Encoding and decoding procedures of QR codes.

III. THE PROPOSED SCHEME

An overview of the proposed scheme is shown in Fig. 3.

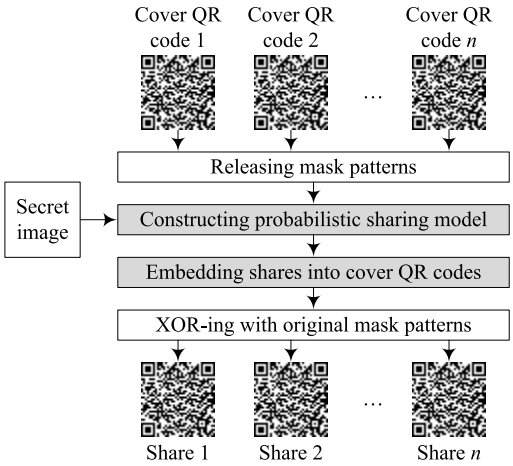

FIGURE 3. Illustration of the proposed scheme.

In Fig. 3, designing matrix sets of (k, n) probabilistic sharing and method of embedding are two key points of our study.

A. DESIGN OF MATRIX SETS

Fig. 4 exhibits the processes to construct matrix sets. By specifying equivalent relationship among participants, the initial collection is divided into several sub-collections. Then, basic matrices for each sub-collection can be obtained with two matrix units $M_{k,even}$ and $M_{k,odd}$. After that, we connect these basic matrices and transform the result into the final matrix sets.

The detailed algorithm is provided.

Example 1: To understand this algorithm better, an example of (2, 4)-VCS is given below.

Initially, $\Gamma_0 = \{\{1, 2\}, \{1, 3\}, \{1, 4\}, \{2, 3\}, \{2, 4\}, \{3, 4\}\}$. First, we choose $Q = \{1, 3\} \in \Gamma_0$. Let $P_1 = \{1, 2\}$, $P_2 = \{3, 4\}$, then we can get $\Gamma_1 = \{\{1, 3\}, \{1, 4\}, \{2, 3\}, \{2, 4\}\}$ and two basic matrices:

$$B_0^1 = \begin{bmatrix} 1 & 0 \\ 1 & 0 \\ 1 & 0 \\ 1 & 0 \end{bmatrix}, \quad B_1^1 = \begin{bmatrix} 1 & 0 \\ 1 & 0 \\ 0 & 1 \\ 0 & 1 \end{bmatrix}.$$

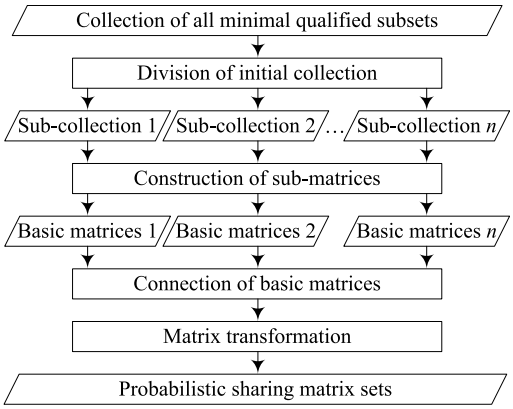

FIGURE 4. Processes of constructing probabilistic sharing sets.

Algorithm 1

Input: A participant set $P = \{1, 2, \cdots, n\}$ and initial collection of all minimal qualified subsets $\Gamma_0 = \{A||A| = k, A \subseteq P\}$.

Output: Matrix sets C_0 and C_1.

Step 1: Let $i = d = 0$, $P_1 = P_2 = \cdots = P_k = \emptyset$, then go to Step 2.

Step 2: If $\Gamma_0 \neq \emptyset$, let $i = i + 1$ and choose a subset $Q \in \Gamma_0$ (Suppose $Q = \{i_1, i_2, \cdots, i_k\}$, $P - Q = \{i_{k+1}, i_{k+2}, \cdots, i_n\}$, $p = \lfloor n/k \rfloor$ and $q = n - p \cdot k$.), then go to Step 3; else, let $d = i$ and go to Step 6.

Step 3: Let $P_1 = \{i_1, i_{k+1}, \cdots, i_{pk+1}\}$, $P_2 = \{i_2, i_{k+2}, \cdots, i_{pk+2}\}, \cdots, P_q = \{i_q, i_{k+q}, \cdots, i_{pk+q}\}$, $P_{q+1} = \{i_{q+1}, i_{k+q+1}, \cdots, i_{(p-1)k+q+1}\}, \cdots, P_k = \{i_k, i_{2k}, \cdots, i_{pk}\}$ and let $\Gamma_i = P_1 \check{r} P_2 \check{r} \cdots \check{r} P_k$. Delete $\Gamma_0 \cap \Gamma_i$ from Γ_0, and redefine P as all participants in current Γ_0. Then, go to Step 4.

Step 4: Construct two $n \times 2^k$ null matrices B_0^i and B_1^i. Let $B_{0Q}^i = M_{k,even}$, $B_{1Q}^i = M_{k,odd}$, and go to Step 5.

Step 5: Assign values to remaining rows. According to P_1, let $B_0^i(i_{uk+1}) = B_0^i(i_1)$ and $B_1^i(i_{uk+1}) = B_1^i(i_1)$ $(1 \leq u \leq p)$. Similarly, results for $P_2, P_3, \cdots, P_k$ can be obtained. Go to Step 2.

Step 6: Horizontally connect all basic matrices $B_0 = \text{con}(B_0^1, B_0^2, \cdots, B_0^d)$, $B_1 = \text{con}(B_1^1, B_1^2, \cdots, B_1^d)$. Then delete common columns of B_0 and B_1, that is, $(B_0', B_1') = \text{del}(B_0, B_1)$. Go to Step 7.

Step 7: Get the final matrix sets $C_0 = \text{Tr}(B_0')$ and $C_1 = \text{Tr}(B_1')$, then algorithm ends.

Similarly, we obtain the other sub-collection $\Gamma_2 = \{\{1, 2\}, \{3, 4\}, \{1, 4\}, \{2, 3\}\}$ and its corresponding basic matrices:

$$B_0^2 = \begin{bmatrix} 1 & 0 \\ 1 & 0 \\ 1 & 0 \\ 1 & 0 \end{bmatrix}, \quad B_1^2 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \\ 1 & 0 \\ 0 & 1 \end{bmatrix}.$$

By "ř ", "del(·)" and "Tr(·)" operations, final sets are formed:

$$C_0 = \left\{ \begin{bmatrix} 1 \\ 1 \\ 1 \\ 1 \end{bmatrix}, \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \end{bmatrix} \right\},$$

$$C_1 = \left\{ \begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 0 \\ 1 \\ 1 \end{bmatrix}, \begin{bmatrix} 1 \\ 0 \\ 1 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 1 \\ 0 \\ 1 \end{bmatrix} \right\}.$$

If the secret pixel is black, we arbitrarily get an $n \times 1$ matrix from C_0; else, randomly select a matrix from C_1. For the chosen matrix, assign the element of each row to its corresponding share. Then, the original shares are generated.

B. DESIGN OF EMBEDDING METHOD

After initial sharing, meaningful shares are supposed in this section. According to [18], any QR code has a determined data and error correction capacity if its version and error correction level are given. In most cases, all codewords of a block includes three parts, as shown in Fig. 5.

FIGURE 5. Three parts of data and error correction codewords.

To obtain the message of a QR code, valid data cannot be modified since it concerns all useful information of decoding. Padding data are added to fill encoding redundancy and error correction codewords are designed to restore original data even if some errors exist. By analysis, we will use padding data to design meaningful shares.

First, the size of cover QR codes is determined. Suppose the original shares are $Tr_1, Tr_2, \cdots, Tr_n$ with the size of $a \times b$. We calculate the least number of data codewords

$$s = (l_0 + a \times b)/8.$$

With a given error correction level, we can infer the required version h of QR codes. Further, check whether the region size of padding data is adequate for embedding an original share. If not, $h = h + 1$ until the size is large enough.

Next, embed original shares into their covers $C_1, C_2, \cdots, C_n$. Suppose the top left corner of embedding region is (p, q). For any module $C_k(p+i-1, q+j-1)$ $(1 \le i \le a, 1 \le j \le b, 1 \le k \le n)$, if it is a padding data, let

$$C_k(p + i - 1, q + j - 1) = Tr_k\,(i, j)\,.$$

Finally, recalculate error correction codewords for current data codewords. Then, final messages before XOR-ing mask patterns are prepared.

IV. VALIDITY PROOF

Security and relative difference are two crucial properties to determine the validity of a VCS. Since embedding process will not change the security and relative difference of original shares, we only need to discuss the validity of probabilistic method in this section.

A. SECURITY

Lemma 1: If $A = \mathrm{con}(C, D)$, $B = \mathrm{con}(C, E)$ and $|A| = |B|$, for $\forall Q \in 2^P$, there is

$$n(\oplus(A_Q)) - n(\oplus(B_Q)) = n(\oplus(D_Q)) - n(\oplus(E_Q)). \quad (1)$$

Proof: Because $A = \mathrm{con}(C, D)$ and $B = \mathrm{con}(C, E)$, there are

$$\begin{cases} n(\oplus(A_Q)) = n(\oplus(C_Q)) + n(\oplus(D_Q)) \\ n(\oplus(B_Q)) = n(\oplus(C_Q)) + n(\oplus(E_Q)). \end{cases} \quad (2)$$

Apparently, (1) is satisfied.

Lemma 2: Suppose $B = \mathrm{Tr}(A) = \{\beta_1, \beta_2, \cdots, \beta_s\}$ and $Q \subseteq 2^P$. The possibility of [0] in $\{\oplus(\beta_{1Q}), \oplus(\beta_{2Q}), \cdots, \oplus(\beta_{sQ})\}$ is

$$p\{\oplus(\beta_{1Q}), \oplus(\beta_{2Q}), \cdots, \oplus(\beta_{sQ})\} = n(\oplus(A_Q))/s. \quad (3)$$

Proof: Because $A_Q = \mathrm{con}(\beta_{1Q}, \beta_{2Q}, \cdots, \beta_{sQ})$, the frequency of [0] in $\{\oplus(\beta_{1Q}), \oplus(\beta_{2Q}), \cdots, \oplus(\beta_{sQ})\}$ is equal to the number of 0 in $\oplus(A_Q)$. Thus, (3) is proved.

Theorem 1. Suppose $A = \mathrm{con}(C, D)$, $B = \mathrm{con}(C, E)$, $\mathrm{Tr}(D) = \{\alpha_1, \alpha_2, \cdots, \alpha_s\}$ and $\mathrm{Tr}(E) = \{\beta_1, \beta_2, \cdots, \beta_s\}$. For $\forall Q \subseteq 2^P$, there is

$$\begin{aligned} &p\{\oplus(\alpha_{1Q}), \oplus(\alpha_{2Q}), \cdots, \oplus(\alpha_{sQ})\} \\ &\quad - p\{\oplus(\beta_{1Q}), \oplus(\beta_{2Q}), \cdots, \oplus(\beta_{sQ})\} \\ &= [n(\oplus(D_Q)) - n(\oplus(E_Q))]/s = [n(\oplus(A_Q)) - n(\oplus(B_Q))]/s. \end{aligned} \quad (4)$$

Proof: According to (1) of Lemma 1 and (3) of Lemma 2, (4) is concluded.

Lemma 3: Suppose B_0^i and B_1^i are two basic matrices of Γ_i. For $\forall Q' \subset Q \in \Gamma_i$, there is

$$n(\oplus(B_{0Q'}^i)) = n(\oplus(B_{1Q'}^i)). \quad (5)$$

Proof: For $\forall k$, $M_{k,even}$ is formed by adding a 0 row to $M_{k-1,even}$ and a 1 row to $M_{k-1,odd}$. Likewise, $M_{k,odd}$ is constituted by adding a 1 row to $M_{k-1,even}$ and a 0 row to$M_{k-1,odd}$. For $\forall Q \subseteq \Gamma_i$, the respective matrices consisting of any t $(t < k)$ rows from B_0^i and B_1^i are identical. Then, (5) can be deduced.

Theorem 2: Suppose B_0^i and B_1^i are two basic matrices of Γ_i. For $\forall Q$ $(|Q| < k)$, there is

$$n(\oplus(B_{0Q}^i)) = n(\oplus(B_{1Q}^i)). \quad (6)$$

Proof: According to Lemma 3, if $Q \subseteq Q_{qual} \in \Gamma_i$, we can get the result of (6).

If no $Q_{qual} \in \Gamma_i$ satisfies $Q \subseteq Q_{qual}$, and $|Q| < k$, there must be two rows at least of B_0^i and B_1^i are identical. Assume that $\exists X = \{p, q\} \in Q$, $B_0^i(p) = B_0^i(q)$ and $B_1^i(p) = B_1^i(q)$. Then, both $\oplus(B_{0X}^i)$ and $\oplus(B_{1X}^i)$ are 0 vectors. So

$$\begin{cases} n(\oplus(B_{0Q}^i)) = n(\oplus(B_{0Q-X}^i)) \\ n(\oplus(B_{1Q}^i)) = n(\oplus(B_{1Q-X}^i)). \end{cases} \tag{7}$$

By analogy, there must be a Y that satisfies $\oplus(B_{0Y}^i)$ and $\oplus(B_{1Y}^i)$ are 0 vectors and $Q - Y \subseteq Q_{qual} \in \Gamma_i$. According to Theorem 2, there is

$$n(\oplus(B_{0Q-Y}^i)) = n(\oplus(B_{1Q-Y}^i)). \tag{8}$$

With (7) and (8), we can infer that

$$n(\oplus(B_{0Q}^i)) = n(\oplus(B_{0Q-Y}^i)) = n(\oplus(B_{1Q-Y}^i)) = n(\oplus(B_{1Q}^i)). \tag{9}$$

In conclusion, Theorem 2 is proved.

Corollary 1: Suppose B_0^i and B_1^i are two basic matrices of Γ_i. And let $B_0 = \text{con}(B_0^1, B_0^2, \cdots, B_0^d)$ and $B_1 = \text{con}(B_1^1, B_1^2, \cdots, B_1^d)$, $(B_0', B_1') = \text{del}(B_0, B_1)$, $C_0 = \text{Tr}(B_0')$ and $C_1 = \text{Tr}(B_1')$. For $C_0 = \{\alpha_1, \alpha_2, \cdots, \alpha_m\}$ and $C_1 = \{\beta_1, \beta_2, \cdots, \beta_m\}$, there is

$$p\{\oplus(\alpha_{1Q}), \oplus(\alpha_{2Q}), \cdots, \oplus(\alpha_{mQ})\} = p\{\oplus(\beta_{1Q}), \oplus(\beta_{2Q}), \cdots, \oplus(\beta_{mQ})\}. \tag{10}$$

According to Theorem 1 and Theorem 2, (10) is true, which demonstrates the security of the proposed scheme.

B. RELATIVE DIFFERENCE

Lemma 4: Suppose B_0^i and B_1^i are two basic matrices of Γ_i with m columns. For $\forall Q \in \Gamma_i$, there is

$$n(\oplus(B_{0Q}^i)) - n(\oplus(B_{1Q}^i)) = m > 0. \tag{11}$$

Proof: For $Q \in \Gamma_i$, $B_{0Q}^i = M_{k,even}$ and $B_{1Q}^i = M_{k,odd}$. Therefore, $\oplus(B_{0Q}^i)$ is a 0 vector while $\oplus(B_{1Q}^i)$ is a 1 vector. Then, (11) is got.

Lemma 5: Suppose B_0^i and B_1^i are two basic matrices of Γ_i. For $\forall Q \in \Gamma_j$ $(|Q| = k)$, there is $n(\oplus(B_{0Q}^i)) = n(\oplus(B_{1Q}^i))$.

$$n(\oplus(B_{0Q}^i)) = n(\oplus(B_{1Q}^i)). \tag{12}$$

Proof: If $Q \in \Gamma_j$ $(|Q| = k)$, there must be at least two elements in Q, of which the corresponding rows in B_0^i and B_1^i are identical. Assume that $\exists X = \{p, q\} \in Q$, $B_0^i(p) = B_0^i(q)$ and $B_1^i(p) = B_1^i(q)$. Then, (7) is satisfied since both $\oplus(B_{0X}^i)$ and $\oplus(B_{1X}^i)$ are 0 vectors. According to Theorem 2, (12) is tenable because $|Q - X| < k$.

Theorem 3: Suppose B_0^i and B_1^i are two basic matrices of Γ_i. And let $B_0 = \text{con}(B_0^1, B_0^2, \cdots, B_0^d)$ and $B_1 = \text{con}(B_1^1, B_1^2, \cdots, B_1^d)$, $(B_0', B_1') = \text{del}(B_0, B_1)$, $C_0 = \text{Tr}(B_0')$ and $C_1 = \text{Tr}(B_1')$. For $C_0 = \{\alpha_1, \alpha_2, \cdots, \alpha_m\}$, $C_1 = \{\beta_1, \beta_2, \cdots, \beta_m\}$ and $\forall Q \in \Gamma_0$ $(|Q| = k)$, there is

$$p\{\oplus(\alpha_{1Q}), \oplus(\alpha_{2Q}), \cdots, \oplus(\alpha_{mQ})\} - p\{\oplus(\beta_{1Q}), \oplus(\beta_{2Q}), \cdots, \oplus(\beta_{mQ})\} > 0. \tag{13}$$

Proof: Assume that $Q \in \Gamma_s$ $(s = i_1, i_2, \cdots, i_h)$, (14) can be inferred by Lemma 4.

$$n(\oplus(B_{0Q}^s)) > n(\oplus(B_{1Q}^s)) \tag{14}$$

Meanwhile, since $Q \notin \Gamma_t$ $(t \neq i_1, i_2, \cdots, i_h)$, according to Lemma 5, we can deduce that

$$n(\oplus(B_{0Q}^t)) = n(\oplus(B_{1Q}^t)). \tag{15}$$

Because $B_0 = \text{con}(B_0^1, B_0^2, \cdots, B_0^d)$ and $B_1 = \text{con}(B_1^1, B_1^2, \cdots, B_1^d)$, there is

$$\begin{cases} n(\oplus(B_{0Q})) = n(\oplus(B_{0Q}^1)) + n(\oplus(B_{0Q}^2)) + \cdots + n(\oplus(B_{0Q}^d)) \\ n(\oplus(B_{1Q})) = n(\oplus(B_{1Q}^1)) + n(\oplus(B_{1Q}^2)) + \cdots + n(\oplus(B_{1Q}^d)). \end{cases} \tag{16}$$

Since $C_0 = \text{Tr}(B_0')$ and $C_1 = \text{Tr}(B_1')$ while $B_0' = \text{con}(B_0, X)$ and $B_1' = \text{con}(B_1, X)$, we can obtain the final conclusion of (13). Therefore, the relative difference is proved.

V. EXPERIMENTS AND ANALYSIS

In this section, feasibility of the proposed scheme, including security, secret recovery and meaningful shares, is illustrated by experiments. In addition, some comparisons and analysis on related work are provided.

A. EXPERIMENTS

For (3, 4)-VCS, we get two divided sub-collections $\Gamma_1 = \{\{1, 2, 3\}, \{1, 2, 4\}\}$ and $\Gamma_2 = \{\{1, 3, 4\}, \{2, 3, 4\}\}$. Further, matrix sets of probabilistic sharing are formed.

$$C_0 = \left\{ \begin{bmatrix} 1 \\ 0 \\ 1 \\ 1 \end{bmatrix}, \begin{bmatrix} 0 \\ 1 \\ 1 \\ 1 \end{bmatrix}, \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \end{bmatrix}, \begin{bmatrix} 1 \\ 1 \\ 1 \\ 0 \end{bmatrix}, \begin{bmatrix} 1 \\ 1 \\ 0 \\ 1 \end{bmatrix}, \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \end{bmatrix} \right\},$$

$$C_1 = \left\{ \begin{bmatrix} 1 \\ 1 \\ 1 \\ 1 \end{bmatrix}, \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \end{bmatrix}, \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix}, \begin{bmatrix} 1 \\ 1 \\ 1 \\ 1 \end{bmatrix}, \begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \end{bmatrix}, \begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \end{bmatrix} \right\}$$

Fig. 6 is the experimental result of (3, 4)-VCS. Fig. 6 (a)-(d) are shares T_1, T_2, T_3, and T_4, respectively. As shown, a single share reveals no information about the secret while its cover message is readable. Fig. 6 (e) gives the decoding result of T_1. We use the demonstration software provided by ZXing.Net to decode the QR codes in our paper.

Fig. 6 (f) is the secret image S with the size of 80 × 80. Fig. 6 (g) shows the XOR-ed result of {1, 2}, indicating that any two participants cannot restore the secret information. By XOR-ing the shares of any qualified subset, the secret is revealed and can be visually recognized, as shown in Fig. 6 (h).

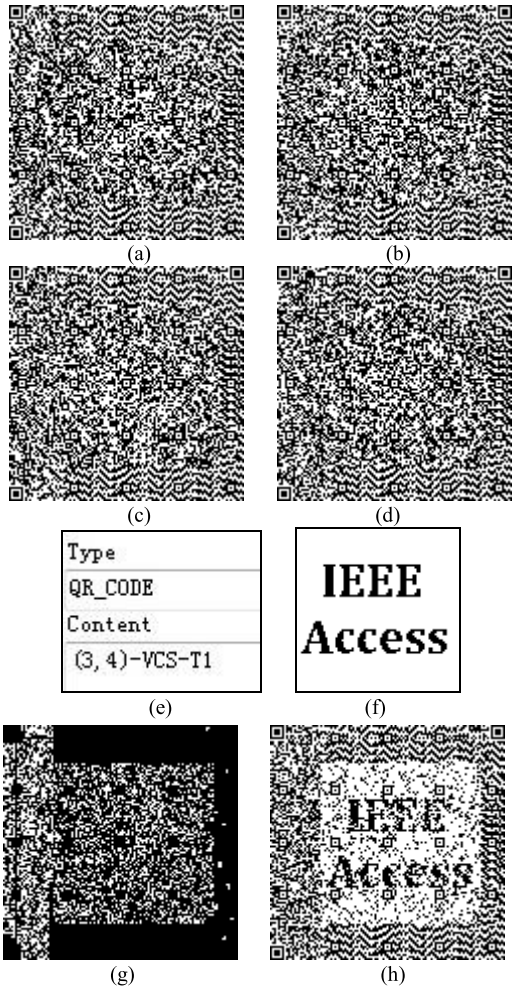

FIGURE 6. Sharing and recovery result of (3, 4)-VCS. (a)-(d) shares T_1, T_2, T_3, T_4; (e) decoding of T_1; (f) secret image S; (g) XOR-ed result of {1, 2} $r_1 = T_1 \oplus T_2$; (h) XOR-ed result of {1, 2, 3} $r_2 = T_1 \oplus T_2 \oplus T_3$.

According to probabilistic sharing sets, for a qualified subset, the possibility of recovering a black pixel is 1 if the secret pixel is black. In addition, the possibility of obtaining a black pixel is 0.5 when the secret pixel is white. Thus, the relative difference in this experiment is 0.5.

By the algorithm in Section III-A, one subset may belong to multiple sub-collections simultaneously. In such case, this subset can reconstruct the secret with higher relative difference than others. For instance, in (2, 4)-VCS the initial collection is divided into two sub-collections $\Gamma_1 = \{\{1, 3\}, \{1, 4\}, \{2, 3\}, \{2, 4\}\}$ and $\Gamma_2 = \{\{1, 2\}, \{3, 4\}, \{1, 4\}, \{2, 3\}\}$. Apparently, subsets $\{1, 4\}$ and $\{2, 3\}$ are both contained by Γ_1 and Γ_2. Then, the sharing sets are constructed.

$$C_0 = \left\{ \begin{bmatrix} 1 \\ 1 \\ 1 \\ 1 \end{bmatrix}, \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \end{bmatrix} \right\}, \quad C_1 = \left\{ \begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 0 \\ 1 \\ 1 \end{bmatrix}, \begin{bmatrix} 1 \\ 0 \\ 1 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 1 \\ 0 \\ 1 \end{bmatrix} \right\}$$

Fig. 7 is the experimental result of (2, 4)-VCS. Fig. 7 (a)-(d) are shares T_1, T_2, T_3, and T_4, all of which can be correctly decoded by QR code readers. Fig. 7 (e) shows the decoding result of T_1.

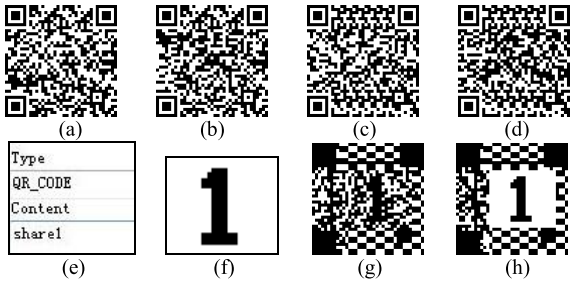

FIGURE 7. Sharing and recovery result of (2, 4)-VCS. (a)-(d) shares T_1, T_2, T_3, T_4; (e) decoding of T_1; (f) secret image S; (g) XOR-ed result of {1, 2} $r_1 = T_1 \oplus T_2$; (h) XOR-ed result of {1, 4} $r_2 = T_1 \oplus T_4$.

Fig. 7 (f) is the original secret S with the size of 22×19. Fig. 7 (g) and (h) are recovered images $r_1 = T_1 \oplus T_2$ and $r_2 = T_1 \oplus T_4$. In line with C_0 and C_1, the possibility that $\{1, 2\}$ restores a black pixel when the secret pixel is black (or white) is 1 (or 0.5). So the relative difference of $\{1, 2\}$ is 0.5. Different from $\{1, 2\}$, $\{1, 4\}$ is contained in both Γ_1 and Γ_2, so the possibility that $\{1, 4\}$ obtains a black pixel when the secret pixel is black (or white) is 1 (or 0). Apparently, the relative difference of $\{1, 4\}$ is 1, which means that the secret image is completely recovered. And the similar result can be also got by $\{2, 3\}$.

B. ANALYSIS

1) ERROR CORRECTION CAPACITY

Error correction is a significant property of QR codes. It allows some errors or damage in the symbol, which makes QR codes more suitable for practical usage. Compared with other related work, error correction capacities of all cover QR codes are completely remained in our proposed scheme. Fig. 8 shows the comparison result of this paper and [22] and [27].

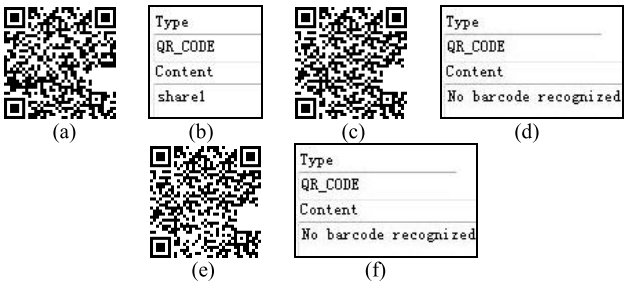

FIGURE 8. Error correction capacities comparison. (a) damaged share T_1 of this paper; (b) decoding of (a); (c) damaged share T_1 of [22]; (d) decoding of (c); (e) damaged share T_1 of [27]; (f) decoding of (e).

Fig. 8 (a), (c), and (e) are the damaged shares of this paper and [22] and [27], respectively, of which the corresponding decoding results are given by Fig. 8 (b), (d), and (f). As shown, the damaged share of our paper can be correctly decoded. Actually, the proposed scheme remains full error

TABLE 2. Relative difference comparison of our paper and other work.

n	k	Random grids			Probabilistic sharing			
		[23]	[24]	[25]	[26]	[28]	[29]	Our
2	2	0.4988	0.4999	0.5008	0.4978	0.5000	0.5000	1.0000
3	2	0.2486	0.2526	0.4990	0.4993	0.3333	0.3333	0.5000
	3	0.2493	0.2603	0.2496	0.2497	0.2500	0.2500	1.0000
4	2	0.1252	0.2499	0.4993	0.5018	0.3125	0.3333	0.5000
	3	0.1247	0.1263	0.2508	0.2531	0.1667	0.1667	0.5000
	4	0.1253	0.1247	0.1246	0.1245	0.1250	0.1250	1.0000
5	2	0.0614	0.1249	0.4989	0.5002	0.3000	0.3000	0.3333
	3	0.0620	0.0622	0.2506	0.2485	0.0667	0.0667	0.3333
	4	0.0618	0.0616	0.1267	0.1254	0.0667	0.0667	0.3333
	5	0.0622	0.0626	0.0631	0.0629	0.0625	0.0625	1.0000

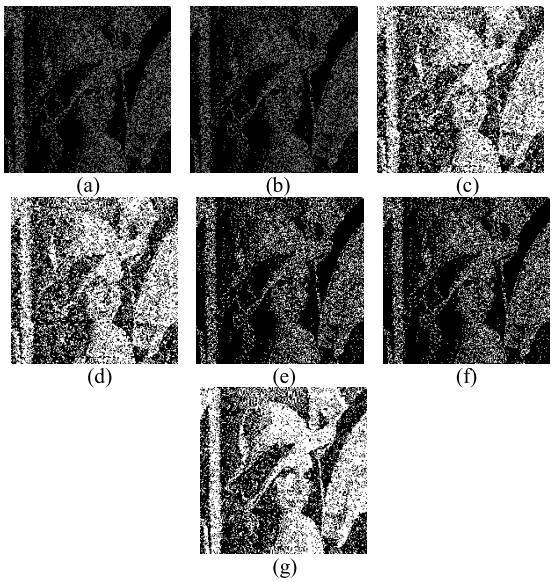

FIGURE 9. Restore secrets of (3, 4)-VCS in this paper and other studies. (a)-(f) recovery of [23]–[29]; (g) recovery of our paper.

correction capacity of the cover QR code because the error correction code is recalculated. Likewise, [22] and [27] are also based on error correction mechanism but they modifies partial codes. Therefore, the error correction capacity is decreased.

2) RELATIVE DIFFERENCE

In previous work, probabilistic sharing and random grids are two methods of constructing VCS without pixel expansion. In Table II, we compare the relative difference of our paper with these unexpanded schemes [23]–[26], [28], [29].

References [23]–[26] designed schemes with random grids while [28], [29], and our study utilized probabilistic method. According to Table II, the recovered secrets in [23], [24], [28], and [29] have poor visual performance because their recovery is based on OR operation, in which the white pixels cannot be reconstructed under semi group structure. References [25], [26], and our scheme has introduced XOR operation. Apparently, the relative difference of our scheme performs better than that of [25] and [26], especially when $k = n$ the secret can be completely recovered. In addition, the values of our paper given in Table II are the low bounds under different (k, n) thresholds. For a specific subset, the value may be higher if the subset is contained by multiple sub-collections.

To show the comparison result more explicitly, Fig. 9 exhibits the restored secrets of (3, 4)-VCS by our method and methods of [23]–[26], [28], and [29].

As shown in Fig. 9 (a), (b), (g), and (f), images of [23], [24], [28], and [29] are dark because white pixels are unable to reconstruct in these schemes. Compared with above results, visual effect of Fig. 9 (c), (d), and (g) are more satisfying. Apparently, our recovered secret preserves more image features and looks best.

VI. CONCLUSION

This paper proposes a novel (k, n)-VCS in which all of the shares are valid QR codes with specific meaning. It reduces the likelihood of being suspected by potential attackers when the shares are distributed via public channels. Additionally, error correction capacities of cover QR codes are preserved even if shares are embedded. Considering practical applications, our scheme can be used to determine the security of some QR codes from unauthorized sources. However, although we have used the probabilistic method to implement no pixel expansion, the size of secret image is still limited. How to improve the secret payload of QR codes remains an open problem to be solved.

ACKNOWLEDGMENT

The authors thank the anonymous reviewers for their valuable comments.

REFERENCES

[1] M. Naor and A. Shamir, "Visual cryptography," in *Advances in Cryptology—EUROCRYPT* (Lecture Notes in Computer Science), vol. 950, A. De Santis Eds. Berlin, Germany: Springer-Verlag, May 1995, pp. 1–12.

[2] C.-N. Yang and D.-S. Wang, "Property analysis of XOR-based visual cryptography," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 24, no. 2, pp. 189–197, Feb. 2014.

[3] G. Shen, F. Liu, Z. Fu, and B. Yu, "Perfect contrast XOR-based visual cryptography schemes via linear algebra," *Des. Codes Cryptogr.*, vol. 85, no. 1, pp. 15–37, Oct. 2017.

[4] S. J. Shyu and M. C. Chen, "Minimizing pixel expansion in visual cryptographic scheme for general access structures," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 25, no. 9, pp. 1557–1561, Sep. 2015.

[5] G. Ateniese, C. Blundo, A. De Santis, and D. R. Stinson, "Visual cryptography for general access structures," *Inf. Comput.*, vol. 129, no. 2, pp. 86–106, Sep. 1996.

[6] S. Arumugam, R. Lakshmanan, and A. K. Nagar, "On $(k, n)^*$-visual cryptography scheme," *Des., Codes Cryptogr.*, vol. 71, no. 1, pp. 153–162, Apr. 2014.

[7] S. Sridhar, R. Sathishkumar, and G. F. Sudha, "Adaptive halftoned visual cryptography with improved quality and security," *Multimedia Tools Appl.*, vol. 76, no. 1, pp. 815–834, Jan. 2017.

[8] C.-N. Yang, L.-Z. Sun, and S.-R. Cai, "Extended color visual cryptography for black and white secret image," *Theor. Comput. Sci.*, vol. 609, pp. 143–161, Sep. 2016.

[9] H. Hu, G. Shen, Z. Fu, B. Yu, and J. Wang, "General construction for XOR-based visual cryptography and its extended capability," *Multimedia Tools Appl.*, vol. 75, no. 21, pp. 13883–13911, Jan. 2016.

[10] Y.-C. Chen, "Fully incrementing visual cryptography from a succinct non-monotonic structure," *IEEE Trans. Inf. Forensics Security*, vol. 12, no. 5, pp. 1082–1091, May 2017.
[11] Y.-C. Hou and Z.-Y. Quan, "Progressive visual cryptography with unexpanded shares," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 21, no. 11, pp. 1760–1764, Nov. 2012.
[12] F. Liu and C. Wu, "Embedded extended visual cryptography schemes," *IEEE Trans. Inf. Forensics Security*, vol. 6, no. 2, pp. 307–322, Jul. 2011.
[13] K.-H. Lee and P.-L. Chiu, "An extended visual cryptography algorithm for general access structures," *IEEE Trans. Inf. Forensics Security*, vol. 7, no. 1, pp. 219–229, Feb. 2012.
[14] D. Wang, F. Yi, and X. Li, "On general construction for extended visual cryptography schemes," *Pattern Recognit.*, vol. 42, no. 11, pp. 3071–3082, Nov. 2009.
[15] I. Kang, G. R. Arce, and H.-K. Lee, "Color extended visual cryptography using error diffusion," *IEEE Trans. Image Process.*, vol. 20, no. 1, pp. 132–145, Jan. 2011.
[16] X. Yan, S. Wang, X. Niu, and C.-N. Yang, "Halftone visual cryptography with minimum auxiliary black pixels and uniform image quality," *Digit. Signal Process.*, vol. 38, pp. 53–65, Mar. 2015.
[17] Z. Wang, G. R. Arce, and G. Di Crescenzo, "Halftone visual cryptography via error diffusion," *IEEE Trans. Inf. Forensics Security*, vol. 4, no. 3, pp. 383–396, Sep. 2009.
[18] *Information—Automatic Identification and Data Capture Techniques—QR Code Barcode Symbology Specification*, document ISO/IEC 18004:2015, 2015.
[19] G. Wang, F. Liu, and W. Q. Yan, "2D barcodes for visual cryptography," *Multimedia Tools Appl.*, vol. 75, no. 2, pp. 1223–1241, Jan. 2016.
[20] C.-N. Yang, J.-K. Liao, F.-H. Wu, and Y. Yamaguchi, "Developing visual cryptography for authentication on smartphones," in *Proc. Int. Conf. Ind. IoT Technol. Appl.* (Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering), vol. 173, J. Wan, I. Humar, and D. Zhang, Eds. Berlin, Germany: Springer-Verlag, Aug. 2016, pp. 189–200.
[21] Y. Liu, Z. Fu, and Y. Wang, "Two-level information management scheme based on visual cryptography and QR code," *Appl. Res. Comput.*, vol. 33, no. 11, pp. 3460–3463, Nov. 2016.
[22] Y.-W. Chow, W. Susilo, G. Yang, J. G. Phillips, I. Pranata, and A. M. Barmawi, "Exploiting the error correction mechanism in QR codes for secret sharing," in *Proc. Australas. Conf. Inf. Secur. Privacy*, in Lecture Notes in Computer Science, vol. 9722, J. Liu and R. Steinfeld, Eds. Berlin, Germany: Springer-Verlag, Jul. 2016, pp. 409–425.
[23] T.-H. Chen and K.-H. Tsao, "Threshold visual secret sharing by random grids," *J. Syst. Softw.*, vol. 84, no. 7, pp. 1197–1208, Jul. 2011.
[24] T. Guo, F. Liu, and C. Wu, "Threshold visual secret sharing by random grids with improved contrast," *J. Syst. Softw.*, vol. 86, no. 8, pp. 2094–2109, Aug. 2013.
[25] X. Wu, T. Liu, and W. Sun, "Improving the visual quality of random grid-based visual secret sharing via error diffusion," *J. Vis. Commun. Image Represent.*, vol. 24, no. 5, pp. 552–566, Jul. 2013.
[26] X. Yan, X. Liu, and C.-N. Yang, "An enhanced threshold visual secret sharing based on random grids," *J. Real-Time Image Process.*, vol. 14, no. 1, pp. 61–73, Oct. 2015.
[27] S. Wan, Y. Lu, X. Yan, Y. Wang, and C. Chang, "Visual secret sharing scheme for (k, n) threshold based on QR code with multiple decryptions," *J. Real-Time Image Process.*, vol. 14, no. 1, pp. 25–40, Mar. 2017.
[28] C.-N. Yang, "New visual secret sharing schemes using probabilistic method," *Pattern Recognit. Lett.*, vol. 25, no. 4, pp. 481–494, Mar. 2004.
[29] S. Cimato, R. De Prisco, and A. De Santis, "Probabilistic visual cryptography schemes," *Comput. J.*, vol. 49, no. 1, pp. 97–107, Jan. 2006.
[30] C.-N. Yang, C.-C. Wu, and D.-S. Wang, "A discussion on the relationship between probabilistic visual cryptography and random grid," *Inf. Sci.*, vol. 278, no. 10, pp. 141–173, Sep. 2014.

ZHENGXIN FU received the M.S. and Ph.D. degrees from the Zhengzhou Information Science and Technology Institute in 2010 and 2014, respectively. His research interests include visual cryptography and information security.

YUQIAO CHENG received the M.S. degree from the Zhengzhou Information Science and Technology Institute in 2018. Her research interests include visual cryptography and information security.

BIN YU received the B.S. degree from the Department of Electronic Engineering, University of Shanghai Jiao Tong, in 1986, the M.S. degree from the Department of Automatic Engineering, South China University of Technology, in 1991, and the Ph.D. degree in 1999. From 1997 to 1999, he was a Research Assistant with The Hong Kong University of Science and Technology. From 2003 to 2004, he was a Vice Professor with the University of Waterloo, ON, Canada. He is currently a Professor with the Department of Computer Science and Information Engineering, Zhengzhou Information Science and Technology Institute, China. His research interests include the design and analysis of algorithms, visual secret sharing, and network security.