International Journal of Digital Crime and Forensics
Volume 11 • Issue 1 • January-March 2019

General Construction for Extended Visual Cryptography Scheme Using QR Codes

Yuqiao Cheng, Science and Technology on Information Assurance Laboratory, Beijing, China
Zhengxin Fu, Zhengzhou Information Science and Technology Institute, Zhengzhou, China
Bin Yu, Zhengzhou Information Science and Technology Institute, Zhengzhou, China
Gang Shen, Zhengzhou Information Science and Technology Institute, Zhengzhou, China

ABSTRACT

This article describes how a visual cryptography scheme, with one prominent feature—decrypting simply, has attracted much research attention since it was first proposed. However, meaningless shares remain a continuing challenge in the development of VCS. In this article, an extended visual cryptography scheme (EVCS) based on XOR operation is proposed, in which QR codes are utilized as the cover images of shares. By designation, all the shares generated in the scheme can be decoded by standard QR code readers with specific meaning. In addition, to achieve high sharing efficiency, a method of simultaneously sharing a secret QR code among multiple subsets is presented. Also, sufficient and necessary conditions of the method are analyzed with an integer programming model, providing a general construction approach for EVCS under arbitrary access structures.

KEYWORDS

Error Correction Capacity, Extended Visual Cryptography Scheme (EVCS), General Access Structure, Multiple Subset Sharing (MSS), QR Codes

1. INTRODUCTION

As an important branch of secret sharing, the concept of visual cryptography scheme (VCS) was first proposed by Naor and Shamir (1995). According to the original definition of a (k, n)-VCS, a secret image is distributed into n shares. No secret information will be revealed with possession of fewer than k shares. But when k or more shares are superimposed, the secret can be easily decrypted by human vision. In the past few decades, VCS developed rapidly and has made great progress in many aspects (Liu & Yan, 2014). A scheme for general access structures was given therewith (Ateniese, Blundo, Santis, & Stinson, 1996), getting rid of threshold constraints on the qualified subsets. Optimal pixel expansion (Shyu & Chen, 2015) and contrast (Lin, Chen, & Lin, 2010) were explored later. To further improve the performance of recovery, XOR operation was introduced into the study of VCS (Shen, Liu, Fu, & Yu, 2017; Yang & Wang, 2014; Wu & Sun, 2014). For the sake of flexible sharing strategies, efforts have been made for multiple secrets (Jia, Wang, Nie, & Zhang, 2016), cheat

DOI: 10.4018/IJDCF.2019010101

prevention (Chen, Tsai, & Horng, 2013), region or fully incrementing (Hu, Shen, Fu, Yu, & Wang, 2016; Chen, 2017) and progressive schemes (Hou & Quan, 2012).

All studies mentioned above contribute a lot to the practical applications of VCS. The only downside is that the shares in these schemes are meaningless and easily arouse suspicion of some potential attackers when distributed via a public channel. Therefore, the extended VCS (EVCS) seems more attractive because it generates meaningful shares instead of random images (Naor & Shamir, 1995). By adding some extra columns into the basis matrices, Wang et al. (Wang, Yi, & Li, 2009) designed a (k, n)-EVCS with poor contrast of shares. To improve visual performance, a scheme was proposed on the basis of halftone image technology (Kang, Arce, & Lee, 2011). And other studies have also been attempted with better results (Liu & Wu, 2011; Yang, Sun, & Cai, 2016; Yan, Wang, Niu, & Yang, 2015; Ou, Sun, & Wu, 2015). Nevertheless, the camouflage effect of shares in these schemes was still unsatisfactory since there were many noisy points visible. Later, secret hiding techniques were utilized to generate meaningful shares (Yan, Wang, El-Latif, & Niu, 2015; Amiri & Moghaddam, 2016; Yuan, 2014), but with large computational load.

Quick Response (QR) code is a two-dimensional code developed by the Japanese Denso Wave Company, and now has been adopted as a universal specification performed by ISO (2006). With the popularization of intelligent terminals, QR codes have been widely used in fields such as information storage, mobile payment and electronic tickets. For a given QR code, we can hardly acquire its message by human vision since the dark and light modules are randomly distributed. This meaningless appearance is similar to the image characteristic of VCS shares. As such, QR code can be a good choice for the mask of VCS share. Therefore, investigations of the VCS and QR codes combinations have attracted considerable attention. At first, QR codes were embedded as some parts of shares to authenticate a VCS (Wang, Liu, & Yan, 2014). This method sought the best embedding region of a given share, thus reducing the influence of secret revealing. Later, a continuous-tone VCS (Yang, Liao, Wu, & Yamaguchi, 2016) was developed where the color of a secret module was determined by the grayness of black dots. Subsequently, a class of EVCSs based on QR codes was proposed. In view of machine recognition characteristic, an EVCS was presented for two-level information storage by Liu et al. (Liu, Fu, & Wang, 2016). In this scheme, a proper scanning distance and angle are strictly required to decoding the shares, which significantly increases the inconvenience of practical applications. By exploiting error correction mechanism of QR codes, a (n, n) sharing method was designed (Chow, Susilo, Yang, Phillips, Pranata, & Barmawi, 2016), and then, a (k, n) scheme under the theory of random grids were further implemented (Wan, Lu, Yan, Wang, & Chang, 2017). Sometimes, the secret image may be a QR code, and then Wan et al.'s scheme becomes invalid because the errors contained in the recovered secret are beyond error correction capability. One solution to this problem is that repeatedly performing Chow et al.'s method on each minimal qualified subset. Then, a large number of sharing instances are required.

In this paper, a novel EVCS is presented combining with QR codes. First, to reduce the number of sharing instances, we introduce an idea of MSS and provide its sufficient and necessary conditions with an integer programming model. And based on this model, we divide the initial access structure into several collections, each of which can achieve a MSS instance. Further, detailed sharing algorithm of MSS is presented. Experimental results and comparisons show the validity and advantages of the proposed scheme.

The remainder of this paper is organized as follows. Section 2 introduces some preliminaries concerning our study. The proposed scheme is described in Section 3 while some conditions are theoretically proved in Section 4. Experiments and analysis are presented in Section 5 to illustrate the feasibility of this work and how it improves on previous work.

2. PRELIMINARIES

In this section, we will give some basic definitions concerning the VCS and the QR code. First, the denotation of symbols in our paper is given in Table 1.

2.1. EVCS

Extended XOR-based VCS (EXVCS) is a type of EVCS, in which the recovery process is based on XOR operation. Because XOR operation can reverse 1 to 0, recovered contrast is significantly improved in EXVCS, especially in (n, n)-EXVCS the secret is completely reconstructed.

Definition 1 [3]. Suppose all participants constitute a set $P = \{1, 2, \cdots, n\}$. Let $\Gamma_Q, \Gamma_F \subseteq 2^P$ and $\Gamma_Q \cap \Gamma_F = \varnothing$. Members of Γ_Q and Γ_F are defined as qualified subsets and forbidden subsets, respectively. The pair (Γ_Q, Γ_F) is called an access structure. If Γ_Q is monotone increasing while Γ_F is monotone decreasing, and $\Gamma_Q \cup \Gamma_F = 2^P$, then (Γ_Q, Γ_F) is said to be strong. Moreover, define the basis $\Gamma_0 = \{Q \in \Gamma_Q \mid Q' \notin \Gamma_Q \text{ if } Q' \subset Q\}$. All of the members in Γ_0 are minimal qualified subsets.

Definition 2. Let $\Gamma = (\Gamma_Q, \Gamma_F)$ be an access structure on P and its basis $\Gamma_0 = \{Q_1, Q_2, \cdots, Q_t\}$. An EXVCS based on QR codes is constituted under Γ if three conditions are satisfied.

(1) Each share can be decoded by a standard QR code reader and its message is meaningful.
(2) Any forbidden subset $Q_f = \{i_1, i_2, \cdots, i_f\} \in \Gamma_F$ is inaccessible to the secret information.
(3) For any qualified subset $Q_q \in \Gamma_Q$, $\exists Q' \subseteq Q_q$ and $Q' \in \Gamma_0$, the secret can be reconstructed by XOR-ing the shares of Q'.

2.2. QR Code

QR codes convey information based on the arrangement of dark and light modules. There are 40 versions with different data capacities. Version 1 is composed of 21×21 modules. Each subsequent version increases by four additional modules per side, up to version 40, which is composed of 177×177 modules.

Table 1. Denotation of symbols

Symbol	Denotation
c	the number of all codewords in a block
b	the number of data codewords in a block
r	the number of errors allowable in a block
S	the secret QR code
T_j	the share of the j-th participant
C_j	the cover QR code of T_j
Q_i	the i-th minimal qualified subset
$R[Q_i]$	the result of $T_1 \oplus T_2 \oplus \cdots \oplus T_m$ if $Q_i = \{1, 2, \cdots, m\}$
$D[Q_i]$	the result of $R[Q_i] \oplus S$
$T_j(u, v)$	module of T_j at the u-th row and v-th column
$Q_1 \Delta Q_2$	the symmetric difference of Q_1 and Q_2

Figure 1 is the structure of version 7. As shown, a QR code includes two parts: function patterns and encoding region. The former are specific structures designed for geometric correction and effective decoding, and the latter contains several QR blocks and some auxiliary format or version information, such as error correction levels, mask patterns, and symbol versions. The format information is a binary sequence with five data bits and ten error correction bits.

Another significant feature of a QR code is error correction, which allows QR code readers to correctly decode data, even if parts of the symbol are dirty or damaged. There are four error correction levels to provide different capabilities (L: 7%, M: 15%, Q: 25%, and H: 30%). A higher level corresponds to a larger data payload. Table 2 lists the characteristic of version 4∼7.

3. THE PROPOSED SCHEME

This section proposes a scheme with meaningful shares for general access structures. By taking full advantage of the error correction capacities of QR codes, less storage space of shares is required in the proposed scheme. As shown in Figure 2, the whole sharing process includes two parts: collection division and MSS, with their detailed algorithms illustrated in Section 2.1 and 2.2, respectively.

3.1. Collection Division

By the (n, n) sharing method (Chow, Susilo, Yang, Phillips, Pranata, & Barmawi, 2016), for any $\Gamma_0 = \{Q_1, Q_2, \cdots, Q_h\}$, the EXVCS under Γ_0 is constructed as follows.

In Figure 3, a participant needs t shares if it belongs to t subsets of Γ_0, which would cost much space to store shares as t grows. To improve sharing efficiency, we attempt to deal with multiple subsets by only one (n, n)-MSS instance.

Different from previous work, the proposed method illustrated in Figure 4 performs only one MSS instance as $n = |Q_1 \cup Q_2 \cup \cdots \cup Q_h|$. Then a participant needs only one share even if it is contained in more than one subsets. However, there are some constraints to the existence of such an instance. Initially, we let $T_j = C_j$ $(j = 1, 2, \cdots, n)$. To obtain the secret message of S, differences between $R[Q_i]$ $(i = 1, 2, \cdots, h)$ and S should be within the error correction capacity of S. Therefore, some codewords of T_j $(j = 1, 2, \cdots, n)$ need modifying to adjust the value of $R[Q_i]$. We take each QR code block as the research object for subsequent analysis. Let X be a three-dimensional matrix with the size of $h \times (n + 1) \times c$. A mathematical model is set up to determine whether a (n, n)-MSS instance of Q_1, Q_2, $\cdots$, Q_h can be satisfied.

Figure 1. The symbol structure of version 7

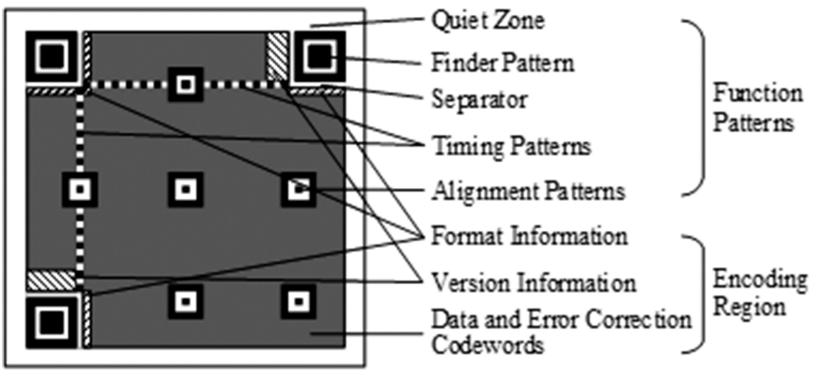


Table 2. Error correction characteristics of several versions

Version	Error correction level	Number of blocks	(c, b, r)
4	L	1	(100,80,10)
	M	2	(50,32,9)
	Q	2	(50,24,13)
	H	4	(25,9,8)
5	L	1	(134,108,13)
	M	2	(67,43,12)
	Q	2	(33,15,9)
		2	(34,16,9)
	H	2	(33,11,11)
		2	(34,12,11)
6	L	2	(86,68,9)
	M	4	(43,27,8)
	Q	4	(43,19,12)
	H	4	(43,15,14)
7	L	2	(98,78,10)
	M	4	(49,31,9)
	Q	2	(32,14,9)
		4	(33,15,9)
	H	4	(39,13,13)
		1	(40,14,13)

Figure 2. The sharing process of the proposed scheme

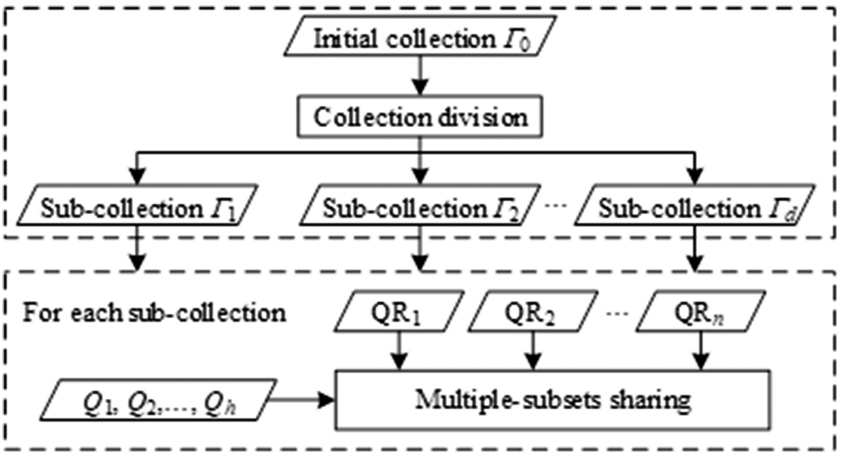


Figure 3. The previous method

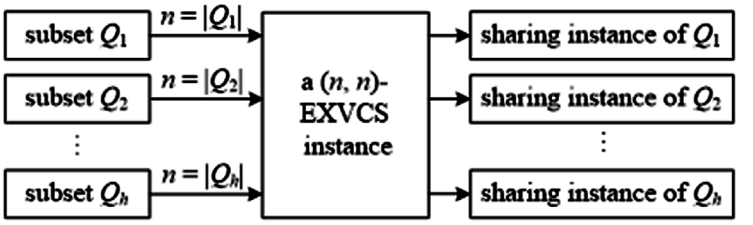
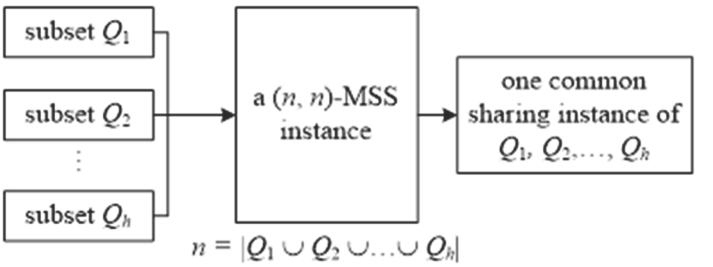


Figure 4. The proposed method



$$\begin{cases} \sum_{j=1}^{n+1} X_{ijk} = 1 (1 \le i \le h, 1 \le k \le c) \\ \sum_{i=1}^{h} \sum_{k=1}^{c} X_{ijk} \le r (1 \le j \le n) \\ \sum_{k=1}^{c} X_{i(n+1)k} \le r (1 \le i \le h) \\ X_{ijk} = 0 (1 \le i \le h, j \notin Q_i, 1 \le k \le c) \\ X_{ijk} \in \{0,1\} (1 \le i \le h, 1 \le j \le n+1, 1 \le k \le c) \end{cases} \tag{1}$$

Choose any t ($2 \le t \le h$) subsets from $Q_1, Q_2, \cdots, Q_h$ and assume they are $Q_{p_1}, Q_{p_2}, \cdots, Q_{p_t}$. Let $Q_a = Q_{p_1} \cup Q_{p_2} \cup \cdots \cup Q_{p_t} - Q_{p_1} \Delta Q_{p_2} \Delta \cdots \Delta Q_{p_t}$, then

$$X_{p_1 v_1 k} + X_{p_2 v_2 k} + \cdots + X_{p_t v_t k} < t (v_1, v_2, \cdots, v_t \in Q_a, 1 \le k \le c) \tag{2}$$

If (1) and (2) have a common solution, $Q_1, Q_2, \cdots, Q_h$ can constitute a collection, of which all subsets can be shared by one (n, n)-MSS instance. $X_{ijk} = 1$ indicates that the k-th codeword ($1 \le k \le c$) of T_j would be modified to let $R[Q_i] = S$. And $X_{i(n+1)k} = 1$ denotes that the k-th codeword of $R[Q_i]$ is different with that of S. In some cases, more than one common solution to (1) and (2) are possible, so we are supposed to choose a proper one from them. Generally, a solution is good or not depends on the difference between the number of errors in T_j ($j = 1, 2, \cdots, n$) and that in $R[Q_i]$ ($i = 1, 2, \cdots, h$), namely

$$\min\left\{\left|\sum_{i=1}^{h}\sum_{k=1}^{c}X_{ijk}-\sum_{k=1}^{c}X_{i(n+1)k}\right|\right\} \tag{3}$$

With above model, basis Γ_0 of any access structure can be divided into a number of collections $\Gamma_1, \Gamma_2, \cdots, \Gamma_d$.

3.2. MMS

In the sharing procedure, the modules of function patterns and version information, as well as ten error correction bits of format information, are fixed. Detailed algorithm is given in Algorithm 1.

In order to restore the secret, we first obtain $R[Q_k]$ $(1 \le k \le h)$ by XOR-ing shares in Q_k. And then we can deduce secret format information according to the format data bits of $R[Q_k]$. Finally, the secret message is reconstructed. Note that the fixed modules will not be handled with during the recovery process.

4. THEORETICAL PROOFS

The validity of the proposed scheme is analyzed in this section from two aspects. One proves the security that forbidden subsets are hardly to obtain secret messages; the other illustrates that a common solution to (1) and (2) is the sufficient and necessary conditions of a MSS instance.

4.1. Security

Theorem 1. Any individual share cannot obtain any information about the secret.

Proof: Because QR codes adopt a universal encoding standard, an adversary can easily decode the message of a share, further inferring the knowledge of its corresponding cover QR code. According to the proposed scheme, no more than r codewords are different between a share and its cover. And this difference makes no sense because the adversary knows nothing about other shares. Therefore, reconstructing the secret with only one share is impossible.

Algorithm 1. Sharing algorithm

Input: The set $P = \{1, 2, \cdots, n\}$ that consists of all participants from $Q_1, Q_2, \cdots, Q_h$; n cover QR codes $C_1, C_2, \cdots, C_n$; a secret QR code S. (Each QR code has d blocks and the symbol size is $a \times a$.)
Output: n shares $T_1, T_2, \cdots, T_n$.
Algorithm starts.
Step 1: Let $i = j = 0$ and $T_k = C_k$ $(1 \le k \le n)$. Go to Step 2.
Step 2: Calculate a common solution to (1) and (2) for the u-th block $(1 \le u \le d)$ and denote it by X^u. Moreover, a common solution X where $X_{k(n+1)v} = 0$ $(1 \le k \le h, 1 \le v \le 5)$ is calculated for sharing five format information data bits. Go to Step 3.
Step 3: Let $i = i + 1$. If $i \le a$, go to Step 4; else, go to Step 9.
Step 4: Let $j = j + 1$. If $j \le a$, go to Step 5; else, let $j = 0$ and go to Step 3.
Step 5: If $S(i, j)$ is a fixed module, skip and go to Step 4; else if $S(i, j)$ is a module from data and error correction block, go to Step 6; else, go to Step 7.
Step 6: Suppose $S(i, j)$ is a module of the v-th codeword of the u-th block. For Q_k $(1 \le k \le h)$, find the q-th element that satisfies $X^u_{kqv} = 1$. If $q = n + 1$, skip and go to Step 4; else, go to Step 8.
Step 7: Suppose $S(i, j)$ is the v-th bit of format information. For Q_k $(1 \le k \le h)$, find the q-th element that satisfies $X_{kqv} = 1$. Go to Step 8.
Step 8: Adjust $T_q(i, j)$ to let $S(i, j) = R[Q_k](i, j)$, and go to Step 4.
Step 9: Output n shares $T_1, T_2, \cdots, T_n$.
Algorithm ends.

Theorem 2. No knowledge of the secret can be obtained with shares of any forbidden subset.

Proof: In terms of QR code specification, dark and light modules of a QR code are randomly distributed. Therefore, the possibility of each module's color is approximately 0.5. For $\forall Q \in \Gamma_0$ and $Q_F \subset Q$, suppose $Q = \{a_1, a_2, \cdots, a_x, b_1, b_2, \cdots, b_y\}$ and $Q_F = \{b_1, b_2, \cdots, b_y\}$. Then,

$$T_{b_1} \oplus T_{b_2} \oplus \cdots \oplus T_{b_y} = S \oplus T_{a_1} \oplus T_{a_2} \oplus \cdots \oplus T_{a_x} \tag{4}$$

Since $T_{a_1} \oplus T_{a_2} \oplus \cdots \oplus T_{a_x}$ are random, the information about S is inaccessible.

4.2. Sufficient and Necessary Conditions

Theorem 3. There is at least one common solution to (1) and (2) if a MSS instance can be satisfied.

Proof: If a multi-subset sharing instance can be applied on $Q_1, Q_2, \cdots, Q_h$, there is $R[Q_i] \oplus D[Q_i] = S$ $(1 \le i \le h)$. Considering the sharing of Q_1 and suppose $Q_1 = \{j_1, j_2, \cdots, j_m\}$. In order to satisfy the result $R[Q_1](u, v) \oplus D[Q_1](u, v) = S(u, v)$ $(1 \le u \le a, 1 \le v \le a)$, a module from $T_1(u, v)$, $T_2(u, v), \cdots, T_m(u, v)$ should be reversed or let $D[Q_1](u, v) = 1$. This step is not required unless $T_1(u, v) \oplus T_2(u, v) \oplus \cdots \oplus T_m(u, v) = S(u, v)$ under the possibility of 1/2. For the k-th codeword $(1 \le k \le c)$, there is

$$\begin{cases} \sum_{j=1}^{n+1} X_{1jk} = 1 \left(\text{the probability of this event is} \frac{255}{256} \right) \\ \sum_{j=1}^{n+1} X_{1jk} = 0 \left(\text{the probability of this event is} \frac{1}{256} \right) \end{cases} \tag{5}$$

Similarly, the conclusion is applied to analysis of $Q_2, Q_3, \cdots, Q_h$. Thus, for any subset Q_i $(1 \le i \le h)$ and any codeword k $(1 \le k \le c)$, there is

$$\begin{cases} \sum_{j=1}^{n+1} X_{ijk} = 1 \left(\text{the probability of this event is} \frac{255}{256} \right) \\ \sum_{j=1}^{n+1} X_{ijk} = 0 \left(\text{the probability of this event is} \frac{1}{256} \right) \end{cases} \tag{6}$$

Since the probability of 255/256 is far larger than 1/256, thus we can approximately consider (6) as $\sum_{j=1}^{n+1} X_{ijk} = 1$. Moreover, to keep both readability of the reconstructed secret and shares, there are $\sum_{k=1}^{c} X_{i(n+1)k} \le r$ and $\sum_{i=1}^{h} \sum_{k=1}^{c} X_{ijk} \le r$. Therefore, (1) can be inferred.

Considering the intersection among $Q_1, Q_2, \cdots, Q_t$, the relationship $X_{ajk} = X_{bjk} = 1$ may not always be satisfied for any a and b. For example, suppose two subsets $Q_p = \{j_{a1}, j_{a2}, \cdots, j_{at}, j_{b1}, j_{b2}, \cdots, j_{bx}\}$ and $Q_q = \{j_{a1}, j_{a2}, \cdots, j_{at}, j_{c1}, j_{c2}, \cdots, j_{cy}\}$. Because $R[Q_p] \oplus D[Q_p] = R[Q_q] \oplus D[Q_q] = S$, there is

$$T_{j_{b1}} \oplus T_{j_{b2}} \oplus \cdots \oplus T_{j_{bx}} \oplus T_{j_{c1}} \oplus T_{j_{c2}} \oplus \cdots \oplus T_{j_{cy}} = D[Q_p] \oplus D[Q_q] \tag{7}$$

To satisfy (7), two approaches are provided in the following.

1. Change a codeword from $T_{j_{b1}}$, $T_{j_{b2}}$, $\cdots$, $T_{j_{bx}}$, $T_{j_{c1}}$, $T_{j_{c2}}$, $\cdots$, $T_{j_{cy}}$;
2. Let $D[Q_p] = 1$ or $D[Q_q] = 1$.

At this moment, if $a \in Q_p \cap Q_q$ and $b \in Q_p \cap Q_q$, $X_{ajk} = X_{bjk} = 1$ is almost impossible. So (2) can be obtained.

Theorem 4. A MSS instance can be constructed if (1) and (2) have a common solution.

Proof: If (1) and (2) have a common solution, it means there is an X that satisfies (1) and (2) at the same time. Apparently, X ensures that errors contained in the recovered secret and the shares are both within their error correction capacities. Suppose any t ($2 \le t \le h$) subsets from $Q_1, Q_2, \cdots, Q_h$ are Q_{p_1}, Q_{p_2}, $\cdots$, Q_{p_t}, there is

$$R[Q_{p_1}] \oplus D[Q_{p_1}] = R[Q_{p_2}] \oplus D[Q_{p_2}] = \cdots = R[Q_{p_t}] \oplus D[Q_{p_t}] = S \tag{8}$$

Assume $Q_b = Q_{p_1} \Delta Q_{p_2} \Delta \cdots \Delta Q_{p_t} = \{i_1, i_2, \cdots, i_x\}$. Then (8) can be simplified as

$$\begin{cases} T_{i_1} \oplus T_{i_2} \oplus \cdots \oplus T_{i_x} \oplus D[Q_{p_1}] \oplus D[Q_{p_2}] \oplus \cdots \oplus D[Q_{p_t}] = 0 (t = 2,4,6,\cdots) \\ T_{i_1} \oplus T_{i_2} \oplus \cdots \oplus T_{i_x} \oplus D[Q_{p_1}] \oplus D[Q_{p_2}] \oplus \cdots \oplus D[Q_{p_t}] = S (t = 1,3,5,\cdots) \end{cases} \tag{9}$$

Under the requirements given by (2), we can always find a codeword from T_{i_1}, T_{i_2}, $\cdots$, T_{i_x}, or let one of $D[Q_{p_1}]$, $D[Q_{p_2}]$, $\cdots$, $D[Q_{p_t}]$ be 1. Then, (9) can be satisfied.

5. EXPERIMENTS AND ANALYSIS

In this section, the feasibility of the proposed scheme is evaluated by experiments. Suppose the participant set $P = \{1, 2, \cdots, 9\}$ and its basis $\Gamma_0 = \{\{1, 2, 3, 4\}, \{3, 4, 5, 6\}, \{1, 2, 7, 8\}, \{5, 6, 8, 9\}\}$. The secret message is "IJDCF-2017" and the first cover is "20170801|Beijing|123456789". Message formats of other covers are similar to the first cover, so we omit the description of them for brevity. The experimental dataset is given in Table 3.

Table 3. The experimental dataset

Data groups	Secret QR code	Cover QR code
1	version 6-level H	version 6-level H
2	version 6-level M	version 6-level H
3	version 6-level L	version 6-level H

First, we obtain a solution to (1) and (2) under data group 1. The result is got by the optimizer "Lingo11", as shown in Figure 5.

Figure 5 declares that a common solution to (1) and (2) exists, which indicates that a MSS instance can be implemented with the solved X, and its experimental result is given below. The decoding tool is the source demo provided by ZXing.Net.

In Figure 6, (a) and (e) are the original cover and secret QR codes, respectively. According to the proposed method, (b) is generated from (a) by changing some codewords shown by the white regions in (c). Moreover, (d) demonstrates that the share (b) is readable. (f) is the reconstructed secret obtained by XOR-ing T_1, T_2, T_3 and T_4, and (g) represents the errors contained in (f) that should be corrected by itself. Because the fault codewords in (f) are within the error correction capacity, the message of (f) is correctly decoded. Here we only exhibit the results of T_1 and $R[Q_1]$ for brevity, which are same to those of other shares and reconstructed secrets, except that the messages of cover QR codes are different. Moreover, (i)-(l) demonstrate that no secret information can be obtained by any forbidden subsets.

Next (1) and (2) are solved with the dataset of group 2, and the result is shown by Figure 7 (a).

Figure 7 clarifies that the model of MSS under Γ_0 is unsolvable. Therefore, we divide Γ_0 into two collections Γ_1 and Γ_2, each of which can support a MSS instance. Here we set $\Gamma_1 = \{\{1, 2, 3, 4\}, \{1, 2, 7, 8\}\}$ and $\Gamma_2 = \{\{3, 4, 5, 6\}, \{5, 6, 8, 9\}\}$, and the solution of the model built on Γ_1 is displayed as Figure 8.

Figure 9 is the sharing result of data group 2. Since Γ_0 is divided into two collections, Γ_1 and Γ_2 correspond to two respective MSS instances. Because participant 3 belongs to both of the two collections, it needs two shares, which is shown in Figure 9 (b) and (c). However, participant 2 is only contained by the subsets in collection Γ_1, therefore, participant 2 only needs one share, as shown in Figure 9 (a). Apparently, the MSS method is also useful in this experiment even if the number of shares is not reduced for some participants.

Figure 5. The solution of data group 1

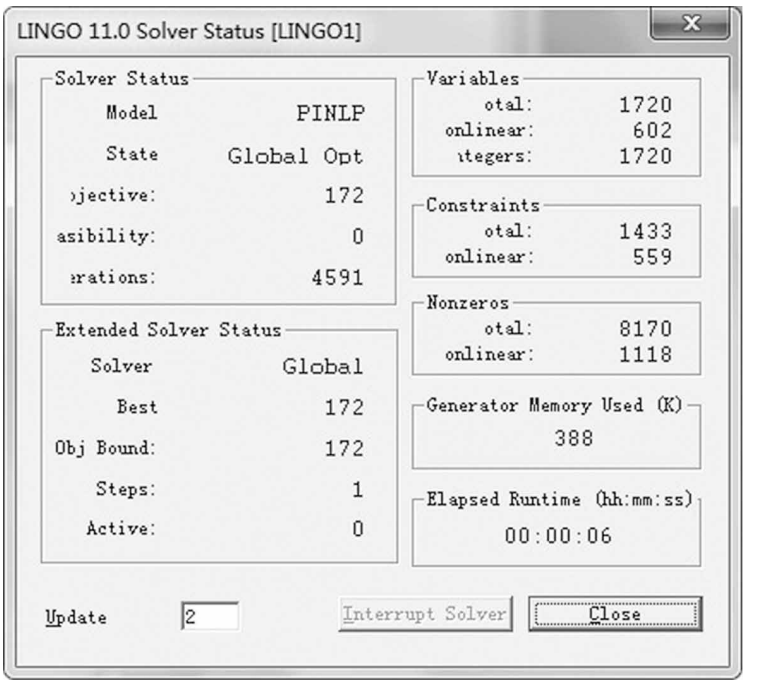


Figure 6. *The MSS result of data group 1.* **(a) cover QR code C_1; (b) share T_1; (c) $C_1 \oplus T_1$; (d) decoding of (b); (e) secret QR code S; (f) recovered secret $R[Q_1]$; (g) $S \oplus R[Q_1]$; (h) decoding of (f); (i) $T_2 \oplus T_3$; (j) $T_2 \oplus T_3 \oplus T_4$; (k) $T_2 \oplus T_3 \oplus T_4 \oplus T_5$; (l) decoding of (i) (or (j),(k))**

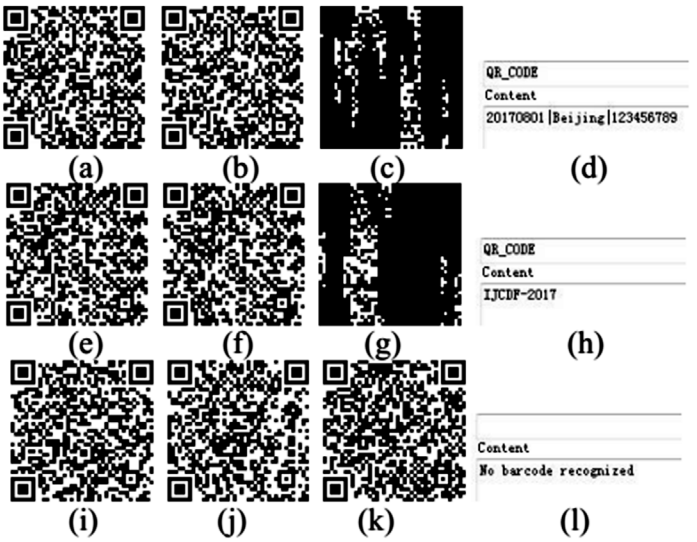
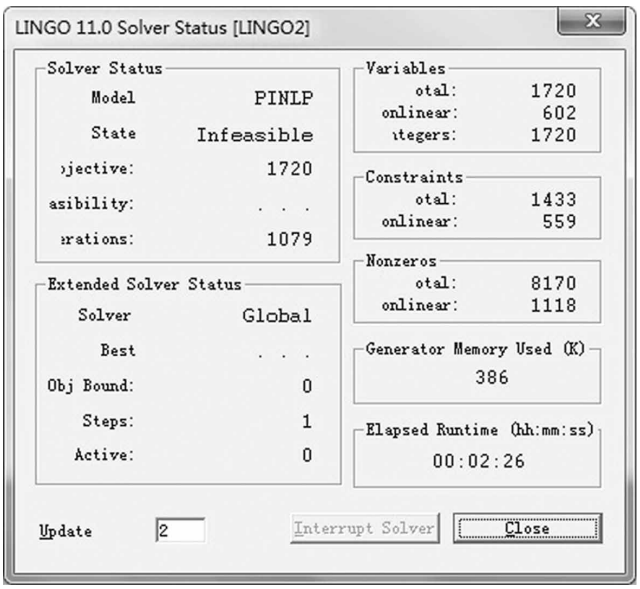


Figure 7. *Solution of data group 2* **on Γ_0**



Providing that $\Gamma_1 = \{\{1, 2, 3, 4\}, \{1, 2, 7, 8\}\}$ and $\Gamma_2 = \{\{3, 4, 5, 6\}, \{5, 6, 8, 9\}\}$, there is no solution to data group 3. So we re-divide Γ_0 into $\Gamma_1 = \{\{1, 2, 3, 4\}\}$, $\Gamma_2 = \{\{3, 4, 5, 6\}\}$ and $\Gamma_3 = \{\{1, 2, 7, 8\}, \{5, 6, 8, 9\}\}$. And at this time only the number of shares for participant 8 decreases.

To show the efficiency of the proposed scheme, the decrease of sharing instances is calculated under several specific (k, n) access structures, as listed in Table 4. (All of the secret and cover QR codes are of version 6 and level 'H'.) Parts of the collection division result are given in Appendix.

Figure 8. *Solution of data group 2* **on** Γ_1

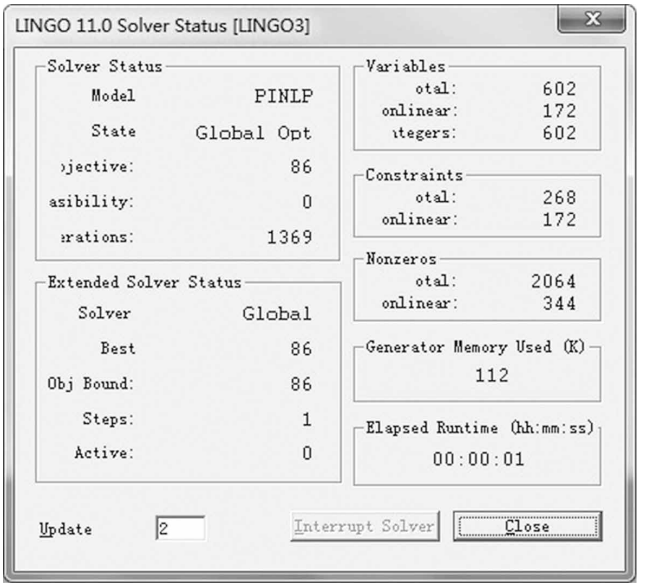


Figure 9. *The sharing result of data group 2.* **(a) share of participant 2; (b) the first share of participant 3; (c) the second share of participant 3**

Table 4. The decreasing number of sharing instances

k	*n*					
	3	**4**	**5**	**6**	**7**	**8**
3	1(1)	4(4)	5(10)	10(20)	12(35)	19(56)
4	—	1(1)	3(5)	8(15)	12(35)	24(70)
5	—	—	1(1)	3(6)	7(21)	19(56)
6	—	—	—	1(1)	3(7)	10(28)
7	—	—	—	—	1(1)	3(8)
8	—	—	—	—	—	1(1)

According to Table 4, the number of instances decreases at least 50% in our scheme, except for (3, 4) and (n, n) access structures since (1) cannot be satisfied in the two cases. In addition, the difficulty of decoding shares in Liu et al.'s (Liu, Fu, & Wang, 2016) scheme is illustrated in Figure 10.

Liu et al.'s scheme is designed on the basis of machine recognition characteristics where each module of its share is distinguished by taking each block consisting of 2×2 sub-modules as a whole. In this case, ZXing.Net demo cannot correctly decode the share as shown in Figure 10 (b), which means that the share is unable to be used electronically. Figure 10 (c) and (d) are decoding results in different scanning distance by a mobile reader "Barcode Scanner". Apparently, a proper scanning way is a key factor to correctly decode the share. Then, decoding is inconvenient. Finally, functional comparisons of this paper with other related work are given in Table 5.

As is exhibited in Table 5, the proposed scheme has a more flexible sharing strategy than some other work(Wang, Yi, & Li, 2009; Yang, Sun, & Cai, 2016; Yan, Wang, Niu, & Yang, 2015; Ou, Sun, & Wu, 2015; Yan, Wang, El-Latif, & Niu, 2015; Amiri & Moghaddam, 2016; Yuan, 2014; Liu, Fu, & Wang, 2016; Chow, Susilo, Yang, Phillips, Pranata, & Barmawi, 2016; Wan, Lu, Yan, Wang, & Chang, 2017), because the proposed scheme is designed for general access structures. For the sake of visual characteristic, the QR code is an excellent choice to cover the shares. Therefore, the camouflage effect is high in this paper and some other work related to QR codes (Liu, Fu, & Wang, 2016; Chow, Susilo, Yang, Phillips, Pranata, & Barmawi, 2016; Wan, Lu, Yan, Wang, & Chang, 2017) or stenography (Ou, Sun, & Wu, 2015; Yan, Wang, El-Latif, & Niu, 2015; Amiri & Moghaddam, 2016; Yuan, 2014). In addition, the computational complexity of VCS is lower than that of other studies (Yan, Wang, El-Latif, & Niu, 2015; Amiri & Moghaddam, 2016).

Figure 10. *The decoding results with different scanning ways.* **(a) share T_1; (b) decoding of (a) by computer demo; (c) decoding of (a) by the mobile reader with the scanning distance of 6cm; (d) decoding of (a) by the mobile reader with the scanning distance of 12cm**

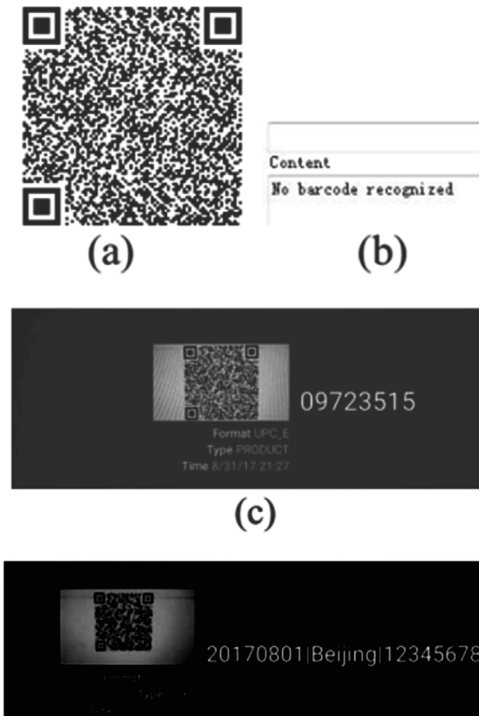


Table 5. Functional comparisons of this paper with other studies

Paper	Access Structure	Camouflage effect	Computational complexity
Wang, Yi, & Li, 2009	(k, n)	low	O(1)
Kang, Arce, & Lee, 2011	general	low	O(1)
Liu & Wu, 2011	general	low	O(1)
Yang, Sun, & Cai, 2016	(k, n)	low	O(1)
Yan, Wang, Niu, & Yang, 2015	(k, n)	low	O(1)
Ou, Sun, & Wu, 2015	(n, n)	high	O(1)
Yan, Wang, El-Latif, & Niu, 2015	(k, n)	high	O(n)
Amiri & Moghaddam, 2016	(n, n)	high	O(n^2)
Yuan, 2014	(k, n)	high	O(1)
Liu, Fu, & Wang, 2016	(2, n)*	high	O(1)
Chow, Susilo, Yang, Phillips, Pranata, & Barmawi, 2016	(n, n)	high	O(1)
Wan, Lu, Yan, Wang, & Chang, 2017	(k, n)	high	O(1)
this paper	general	high	O(1)

6. CONCLUSION

This paper proposes a novel EVCS that all shares are meaningful QR codes. It reduces the likelihood of being suspected by potential attackers if distributed via public channels. Moreover, the proposed scheme can also be used to improve the security when QR codes are applied in some secret application fields. By further utilizing error correction capacities of QR codes, this paper presents a method to share multiple subsets simultaneously, which reduces the number of sharing instances on the basis of previous work. As a result, fewer shares of each participant are required. However, our paper only provides sufficient and necessary conditions for a MSS instance; finding an optimal division method remains an open problem to be solved.

ACKNOWLEDGMENT

The authors thank the anonymous reviewers for their valuable comments. This work was supported in part by the National Natural Science Foundation of China under Grant No.61602513 and the Outstanding Youth Foundation of Zhengzhou Information Science and Technology Institute under Grant No.2016611303.

REFERENCES

Amiri, T., & Moghaddam, M. E. (2016). A new visual cryptography based watermarking scheme using DWT and SIFT for multiple cover images. *Multimedia Tools and Applications*, *75*(14), 8527–8543. doi:10.1007/s11042-015-2770-7

Ateniese, G., Blundo, C., Santis, A. D., & Stinson, D. R. (1996). Visual cryptography for general access structures. *Information and Computation*, *129*(2), 86–106. doi:10.1006/inco.1996.0076

Chen, Y. C. (2017). Fully incrementing visual cryptography from a succinct non-monotonic structure. *IEEE Transactions on Information Forensics and Security*, *12*(5), 1082–1091. doi:10.1109/TIFS.2016.2641378

Chen, Y. C., Tsai, D. S., & Horng, G. (2013). Visual secret sharing with cheating prevention revisited. *Digital Signal Processing*, *23*(5), 1496–1504. doi:10.1016/j.dsp.2013.05.014

Chow, Y. W., Susilo, W., Yang, G., Phillips, J. G., Pranata, I., & Barmawi, A. M. (2016). Exploiting the Error Correction Mechanism in QR Codes for Secret Sharing. In J. Liu, & R Steinfeld (Eds.), *2016 Australasian Conference on Information Security and Privacy, LNCS* (Vol. 9722, pp. 409-425). Berlin, Germany: Springer-Verlag. doi:10.1007/978-3-319-40253-6_25

Hou, Y. C., & Quan, Z. Y. (2012). Progressive visual cryptography with unexpanded shares. *IEEE Transactions on Circuits and Systems for Video Technology*, *21*(11), 1760–1764. doi:10.1109/TCSVT.2011.2106291

Hu, H., Shen, G., Fu, Z., Yu, B., & Wang, J. (2016). General construction for XOR-based visual cryptography and its extended capability. *Multimedia Tools and Applications*, *75*(21). doi:10.1007/s11042-016-3250-4

ISO/IEC. (2015). ISO/IEC 18004:2015 Information - Automatic identification and data capture techniques - QR Code barcode symbology specification.

Jia, X., Wang, D., Nie, D., & Zhang, C. (2016). Collaborative visual cryptographic schemes. *IEEE Transactions on Circuits and Systems for Video Technology*.

Kang, I., Arce, G. R., & Lee, H. K. (2011). Color extended visual cryptography using error diffusion. *IEEE Transactions on Image Processing*, *20*(1), 132–145. doi:10.1109/TIP.2010.2056376 PMID:20615812

Lin, S. J., Chen, S. K., & Lin, J. C. (2010). Flip visual cryptography (FVC) with perfect security, conditionally-optimal contrast, and no expansion. *Journal of Visual Communication and Image Representation*, *21*(8), 900–916. doi:10.1016/j.jvcir.2010.08.006

Liu, F., & Wu, C. (2011). Embedded extended visual cryptography schemes. *IEEE Transactions on Information Forensics and Security*, *6*(2), 307–322. doi:10.1109/TIFS.2011.2116782

Liu, F., & Yan, W. Q. (2014). *Visual cryptography for image processing and security*. Springer International Publishing. doi:10.1007/978-3-319-09644-5

Liu, Y., Fu, Z., & Wang, Y. (2016). Two-level information management scheme based on visual cryptography and QR code. *Jisuanji Yingyong Yanjiu*, *33*(11), 3460–3463.

Naor, M., & Shamir, A. (1995). Visual cryptography. In A. De Santis (Ed.), Lecture Notes in Computer Science: Vol. 950. *Advances in Cryptology — EUROCRYPT'94. EUROCRYPT 1994*. Berlin Heidelberg, Germany: Springer-Verlag. doi:10.1007/BFb0053419

Ou, D., Sun, W., & Wu, X. (2015). Non-expansible xor-based visual cryptography scheme with meaningful shares. *Signal Processing*, *108*, 604–621. doi:10.1016/j.sigpro.2014.10.011

Shen, G., Liu, F., Fu, Z., & Yu, B. (2017). Perfect contrast xor-based visual cryptography schemes via linear algebra. *Designs, Codes and Cryptography*, *85*(1), 15–37. doi:10.1007/s10623-016-0285-5

Shyu, S. J., & Chen, M. C. (2015). Minimizing pixel expansion in visual cryptographic scheme for general access structures. *IEEE Transactions on Circuits and Systems for Video Technology*, *25*(9), 1557–1561. doi:10.1109/TCSVT.2015.2389372

Wan, S., Lu, Y., Yan, X., Wang, Y., & Chang, C. (2017). Visual secret sharing scheme for (k, n) threshold based on qr code with multiple decryptions. *Journal of Real-Time Image Processing*, *9*, 1–16.

Wang, D., Yi, F., & Li, X. (2009). On general construction for extended visual cryptography schemes. *Pattern Recognition*, *42*(11), 3071–3082. doi:10.1016/j.patcog.2009.02.015

Wang, G., Liu, F., & Yan, W. Q. (2016). 2D Barcodes for visual cryptography. *Multimedia Tools and Applications*, *75*(2), 1223–1241. doi:10.1007/s11042-014-2365-8

Wu, X., & Sun, W. (2014). Extended capabilities for xor-based visual cryptography. *IEEE Transactions on Information Forensics and Security*, *9*(10), 1592–1605. doi:10.1109/TIFS.2014.2346014

Yan, X., Wang, S., El-Latif, A. A. A., & Niu, X. (2015). New approaches for efficient information hiding-based secret image sharing schemes. *Signal, Image and Video Processing*, *9*(3), 499–510. doi:10.1007/s11760-013-0465-y

Yan, X., Wang, S., Niu, X., & Yang, C. N. (2015). Halftone visual cryptography with minimum auxiliary black pixels and uniform image quality. *Digital Signal Processing*, *38*(C), 53–65. doi:10.1016/j.dsp.2014.12.002

Yang, C. N., Liao, J. K., Wu, F. H., & Yamaguchi, Y. (2016). Developing visual cryptography for authentication on smartphones. In J. Wan, I. Humar, & D Zhang (Eds.), *2016 International Conference on Industrial IoT Technologies and Applications, LNICSSITE* (Vol. 173, pp. 189-200). Berlin Heidelberg, Germany: Springer-Verlag. doi:10.1007/978-3-319-44350-8_19

Yang, C. N., Sun, L. Z., & Cai, S. R. (2016). Extended color visual cryptography for black and white secret image. *Theoretical Computer Science*, *609*(P1), 143–161. doi:10.1016/j.tcs.2015.09.016

Yang, C. N., & Wang, D. S. (2014). Property analysis of xor-based visual cryptography. *IEEE Transactions on Circuits and Systems for Video Technology*, *24*(2), 189–197. doi:10.1109/TCSVT.2013.2276708

Yuan, H. D. (2014). Secret sharing with multi-cover adaptive steganography. *Information Sciences*, *254*, 197–212. doi:10.1016/j.ins.2013.08.012

APPENDIX

1) Collections of (3, 5) access structure:

$\Gamma_1 = \{\{1, 2, 3\}, \{1, 4, 5\}\}$; $\Gamma_2 = \{\{1, 2, 4\}, \{2, 3, 5\}\}$; $\Gamma_3 = \{\{1, 2, 5\}, \{3, 4, 5\}\}$;
$\Gamma_4 = \{\{1, 3, 5\}, \{2, 3, 4\}\}$; $\Gamma_5 = \{\{1, 3, 4\}, \{2, 4, 5\}\}$.

2) Collections of (4, 6) access structure:

$\Gamma_1 = \{\{1, 2, 3, 4\}, \{1, 2, 3, 5\}\}$; $\Gamma_2 = \{\{1, 2, 3, 6\}, \{1, 2, 4, 5\}\}$;
$\Gamma_3 = \{\{1, 2, 4, 6\}, \{1, 2, 5, 6\}\}$; $\Gamma_4 = \{\{1, 3, 4, 5\}, \{1, 3, 4, 6\}\}$;
$\Gamma_5 = \{\{1, 3, 5, 6\}, \{1, 4, 5, 6\}\}$; $\Gamma_6 = \{\{2, 3, 4, 5\}, \{2, 3, 4, 6\}\}$;
$\Gamma_7 = \{\{2, 3, 5, 6\}, \{2, 4, 5, 6\}\}$; $\Gamma_8 = \{\{3, 4, 5, 6\}\}$.

3) Collections of (5, 7) access structure:

$\Gamma_1 = \{\{1, 2, 3, 4, 5\}, \{1, 2, 3, 4, 6\}, \{1, 2, 3, 4, 7\}\}$;
$\Gamma_2 = \{\{1, 2, 3, 5, 7\}, \{1, 2, 3, 6, 7\}, \{1, 2, 4, 6, 7\}\}$;
$\Gamma_3 = \{\{1, 2, 5, 6, 7\}, \{1, 3, 4, 5, 6\}, \{1, 3, 4, 5, 7\}\}$;
$\Gamma_4 = \{\{1, 3, 4, 6, 7\}, \{2, 3, 4, 5, 6\}, \{2, 3, 4, 6, 7\}\}$;
$\Gamma_5 = \{\{1, 3, 5, 6, 7\}, \{1, 4, 5, 6, 7\}, \{2, 3, 4, 5, 6\}\}$;
$\Gamma_6 = \{\{2, 3, 5, 6, 7\}, \{2, 4, 5, 6, 7\}, \{1, 2, 4, 5, 6\}\}$;
$\Gamma_7 = \{\{3, 4, 5, 6, 7\}, \{1, 2, 4, 5, 7\}, \{1, 2, 3, 5, 6\}\}$.

4) Collections of (6, 8) access structure:

$\Gamma_1 = \{\{1, 2, 3, 4, 5, 6\}, \{1, 2, 3, 4, 5, 7\}, \{1, 2, 3, 4, 5, 8\}\}$;
$\Gamma_2 = \{\{1, 2, 3, 5, 6, 7\}, \{1, 2, 3, 5, 6, 8\}, \{1, 2, 3, 4, 6, 7\}\}$;
$\Gamma_3 = \{\{1, 2, 3, 5, 7, 8\}, \{1, 2, 3, 6, 7, 8\}, \{1, 2, 3, 4, 6, 8\}\}$;
$\Gamma_4 = \{\{1, 2, 4, 5, 6, 7\}, \{1, 2, 4, 5, 6, 8\}, \{2, 3, 5, 6, 7, 8\}\}$;
$\Gamma_5 = \{\{1, 2, 4, 5, 7, 8\}, \{1, 2, 4, 6, 7, 8\}, \{1, 3, 4, 6, 7, 8\}\}$;
$\Gamma_6 = \{\{1, 2, 5, 6, 7, 8\}, \{1, 3, 4, 5, 6, 7\}, \{1, 3, 5, 6, 7, 8\}\}$;
$\Gamma_7 = \{\{2, 3, 4, 5, 6, 7\}, \{2, 3, 4, 5, 6, 8\}, \{1, 3, 4, 5, 6, 8\}\}$;
$\Gamma_8 = \{\{2, 3, 4, 5, 7, 8\}, \{3, 4, 5, 6, 7, 8\}, \{1, 3, 4, 5, 7, 8\}\}$;
$\Gamma_9 = \{\{1, 2, 3, 4, 7, 8\}, \{2, 3, 4, 6, 7, 8\}, \{2, 4, 5, 6, 7, 8\}\}$;
$\Gamma_{10} = \{\{1, 4, 5, 6, 7, 8\}\}$.

Yuqiao Cheng received the MS degree in information security at Zhengzhou Information Science and Technology Institute. Her research interests include visual cryptography and information security.

Zhengxin Fu received the PhD degree from Zhengzhou Information Science and Technology Institute in 2014. His research interests include visual cryptography and information security.

Bin Yu is a professor of the Department of Computer Science and Information Engineering at Zhengzhou Information Science and Technology Institute. His research interests include the design and analysis of algorithms, visual secret sharing and network security.

Gang Shen received the PhD degree from Zhengzhou Information Science and Technology Institute in 2017. His research interests include: visual security and cryptography, image security.