J. Vis. Commun. Image R. 87 (2022) 103567

Contents lists available at ScienceDirect

Journal of Visual Communication and Image Representation

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

Full Length Article

Distributed three-level QR codes based on visual cryptography scheme

Zhengxin Fu *, Liguo Fang, Hangying Huang, Bin Yu

Zhengzhou Information Science and Technology Institute, Zhengzhou, China

ARTICLE INFO

Keywords:
Three-level QR code
Visual cryptography scheme
Multiple formats

ABSTRACT

Owing to the large storage and fast machine recognition, QR codes have been widely utilized in many fields such as mobile payment, website navigation and user identity authentication. However, any QR code reader can access to the message contained in the QR code, the security becomes a major challenge to QR codes for privacy usage scenarios. Moreover, the management of QR codes for users are also inconvenient, since the human vision is hard to distinguish a QR code from the others. To solve the security and management problems, we propose the three-level QR codes for a group of participants. The first-level management information and the second-level public information are recognizable for the human vision and QR code reader device, respectively. The third-level privacy information is protected using visual cryptography scheme, and can be decoded using simple and non-cryptography computations. Furthermore, the shares can be stored or transferred in not only e-format but also print-format and photo-format, leading to the broad applicability. Experimental results and analysis demonstrate that the proposed scheme can encode three-level information into several distributed QR codes, and has more advantages compared with the previous schemes.

1. Introduction

Quick response code, a kind of two-dimensional barcode, was designed by Japan Denso Company in September 1994, which had the advantages of fast identification, large amount of information and high reliability [1]. Since the QR code can be read easily by the decoder device or smartphone with reader software, it is widely used in many practical applications, such as information storage, website redirection, product tracking and passenger identification, etc [2]. However, the QR code brings us not only convenience but also privacy security issues.

As we all know, everyone can obtain the information of the QR code without password. However, in some fields, only parts of the information are wanted to be disclosed, while the other parts are hoped to be protected. For example, the clients only want their addresses known to the courier, while their personal information such as the detailed house number or the phone number is not allowed to be obtained. In order to solve this problem, Tkachenko et al. [3] denoted a novel QR code named two-level QR code (public and privacy) by using the error correction mechanism of the QR code. The public-level information was encoded to the QR code directly and could be obtained by any common QR code reader, while the privacy-level information can only be decoded by the person with a legal key. When QR code was taken as the cover image to transfer privacy information, as the scale of the privacy information increases, the size of the two-level QR code would be too large [4,5], which may cause great inconvenience. What's more, the aforementioned schemes based on the stenography or encryption techniques brought some disadvantages such as the high computational cost.

Visual cryptography scheme (VCS) was proposed by Naor and Shamir [6] with the advantage of low computational complexity. Taking the (k, n)-VCS as example, it encodes the secret image into n shares, which are printed on the transparency films and then distributed to n participants. When stacking any k or more transparency films, the secret can be observed by the human visual system (HVS) directly. Meanwhile, any t $(t < k)$ shares cannot get any information about the secret image. Due to the simplicity of decryption, many scholars focused on VCS. They have improved VCS from the perspectives of access structure, image color, recovery effect and applications [7–15]. With the mature development of QR code, the secure QR code [16–20] based on VCS gradually becomes a hot topic.

Weir and Yan [16] proposed a scheme to verify the shares generated by VCS using QR codes, where the recovered secret was encoded into a QR code and embedded into the verification information. Wang et al. [17] designed an anti-fraud scheme by embedding QR codes into different shares. In order to maintain the visual effect of the recovery result, the best area of a given share was selected to embed the QR code. However, since these shares were generated randomly in Ref. [16,17],

* Corresponding author.
E-mail address: fzx2515@163.com (Z. Fu).

https://doi.org/10.1016/j.jvcir.2022.103567
Received 1 July 2021; Received in revised form 13 October 2021; Accepted 12 June 2022
Available online 15 June 2022

the shares were meaningless which may cause the suspicions from the potential attackers. Chow et al. [18] proposed a $(n, n)(n \geq 3)$ threshold secret sharing scheme by encoding a secret QR code into several QR code shares. Each QR code share could be recognized by a common QR code reader device. The secret QR code was decoded by performing the XOR operation on all n shares. Wan et al. [19] present a (k, n) visual secret sharing scheme based on the QR code, where two methods were designed to recovery the secret image. On the one hand, when the computation device was unavailable, the secret image can be reconstructed by stacking any t $(t \geq n)$ shares. On the other hand, when the lightweight computation device was available, the secret image can be recovered by XOR-ing the shares with better visual effects. Based on the machine-recognition characteristics of the QR code, Fu et al. [20] proposed a two-level QR code with multiple decryptions, where several cells with different contrast were designed to replace the black and white modules. However, the relative difference of the recovered secret image was 1/4 or 1/2 for different recovery algorithms, which reduced the decoding efficiency of the QR code. Tan et al. [21] replaced the padding codewords by shares encoding the secret image using XOR VCS. The scheme could decode the secret image perfectly, and was robust against with some conventional image attacks. However, the size of the secret image is limited by the number of padding codewords of the cover QR code.

Combing the QR code with VCS, this paper proposes a novel three-level QR code to encode visual, public and privacy information into several shares distributed to different participants. The visual-level information is placed in the middle of the QR code, which can be directly observed by the users' eyes. If the participants want to classify the shares into several groups, one group is distributed with the assigned visual-level information to distinguish from the others. The public-level information can be recognized directly from the shares using the ordinary QR code reader device or software, which is used to decrease the attackers' attentions to the shares. The privacy-level information is encoded into the shares, and could be recovered by using the several shares of the qualified participant set. According to the recognition characteristics (key-point and average-gray) of QR code, the basis unit consisting of 3×3 modules is designed with 1 public module and 8 privacy modules. In order to recover the privacy information perfectly, the general access structure is divided into several ideal access structures by using the special division algorithm. Then, the share-generation algorithm is proposed to construct 3-level QR code shares, while the privacy recovering algorithm is designed to reconstructed the privacy-level information. Furthermore, our 3-level QR code shares can be stored and used with not only e-format but also print-format and photo-format, which makes the use of the scheme more convenient. The experimental results demonstrate the effectiveness of the scheme, and the comparison between the scheme with the previous ones will be discussed in detail.

The contributions of this paper are provided as follows. 1) The QR code-like shares carry three different levels of information: visual-level, public-level and privacy-level. The visual-level information makes the distributed shares are easy to be managed, and the recognizable public-level information can reduce the attackers' attentions to the shares. Furthermore, the privacy-level information can only be recovered by the qualified set of participants without complicated computations. 2) Suitable to the general access structure. The proposed scheme is not limited to (n, n) or (k, n) threshold access structure, but suitable to the general access structure. In order to improve the recovery effect of privacy information, the general access structure is divided into some ideal access structures, which can reconstruct the privacy QR code perfectly using XOR operations. 3) Multiple formats of shares. The proposed scheme supports not only the e-format shares to recovery the privacy QR code, but also the print-format and photo-format shares which are the common formats in the real-world. Although the print-format and photo-format shares have distortions, they can be used to recovering the privacy-level information after the special rectifications.

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. Experiments and Comparisons are presented in Section 4 to illustrate the feasibility of this work and demonstrate how it improves on previous work. Finally, Section 5 provides conclusions.

2. Preliminaries

To promote an understanding of the subsequent results, we will provide some basic terms and the notations concerning in the study. First, the denotation of some symbols used in the paper is illustrated in Table 1.

2.1. QR code

The QR code [1] is a kind of two-dimensional code which encodes information through the arrangement of dark and light modules. The QR symbol version is indicated by version V-E, where V indicates the version number (1 to 40) and E indicates the error correction level (L, M, Q, H). Symbol specifications are from 21×21 modules (versions 1) to 177×177 177×177 modules (versions 40) with 4 additional modules per side of the previous version. Four kinds of error correction level ratio are: L 7%, M 15%, Q 25%, H 30%. For instance, level H can tolerate approximately 30% of error codes in the data and error correction code words. The black module and white module represent digits 1 and 0, respectively. A QR symbol includes two parts, the encoding region and the function patterns. Fig. 1 shows the structure of QR code with version 7.

As depicted in Fig. 1, the QR code consists of two parts: the functional patterns and the coding area. Functional pattern refers to position detection patterns, and alignment patterns. The coding region contains format information, version information, data and error correction codewords. And the functional patterns are used to locate and correct the images, which are used to preventing from the geometry deformation.

2.2. XOR-VCS

Definition 1. *([2])* Let P={1,2,…,n} $P = \{1, 2, \cdots, n\}$ $P = \{1, 2, \cdots, n\}$ be a set of participants and let 2^P denote all subsets of P. Let$\Gamma_Q \subseteq 2^P\Gamma_Q \subseteq 2^P$, where$\Gamma_Q \forall \Gamma_F = \varnothing\Gamma_Q \cap \Gamma_F = \varnothing$. We refer to members of $\Gamma_Q\Gamma_Q$ as qualified sets and call members of $\Gamma_F\Gamma_F$ forbidden subsets. The pair $\Gamma = (\Gamma_Q, \Gamma_F)\Gamma = (\Gamma_Q, \Gamma_F)$ is called the access structure of the

Table 1
Denotation Of Symbols.

Notions	Descriptions
P={1, 2, …, n}	The set of n participants
ΓQ	The set of qualified subsets
ΓF	The set of forbidden subsets
$\Gamma 0$	The set of minimal qualified subsets
GAS	General access structure
IAS_1, IAS_2, …, IAS_d	Ideal access structures 1, 2, …, d
V_1, V_2, …, V_n	Visual images 1, 2, …, n
P_1, P_2, …, P_n	Public QR codes 1,2, …, n
$M[X]$	The sub-matrix consisting of $i_1, i_2, \cdots, i_p$-th rows of matrix M, and $X=\{i_1, i_2, \cdots, i_p\}$
XOR(M)	The row vector after XOR-ing all rows of M
$H(V)$	The Hamming weight of vector V
S	Secret QR code
$T_i{}^j$	The j-th sub-share of the user i, $1 \leq i \leq n$, $1 \leq j \leq d$
a	The side length of public and secret QR codes
la	The side length of 3-L QR code share, $la = 3a$
lb	The side length of printed or photo format 3-L QR code
lc	The side length of rectified 3-L QR codes, and lc/la is an integer

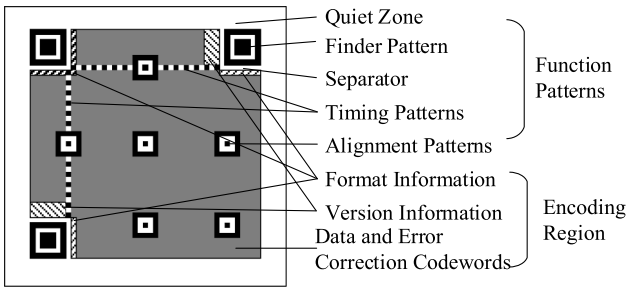

Fig. 1. Symbol structure of QR code with Version 7.

scheme.

Definition 2. *([2])* Define $\Gamma_0 = \{A \in \Gamma_Q : \forall B \subset A \Rightarrow B \notin \Gamma_Q\}$ as the minimal qualified sets. A is a minimal qualified subset when $A \in \Gamma_0$.

In this paper, we only consider strong access structure $\Gamma = (\Gamma_Q, \Gamma_F)$, where Γ_Q is monotone increasing and Γ_F is monotone decreasing. Meanwhile, $\Gamma_Q = cl(\Gamma_0)$ and $\Gamma_F = 2^P - cl(\Gamma_0)$, where $cl(\Gamma_0) = \{B : \exists A \in \Gamma_0, B \supseteq A\}$. Therefore, Γ_Q and Γ_F can be denoted by Γ_0. Suppose that $X = \{i_1, i_2, \cdots, i_p\} \subseteq \{1, 2, \cdots, n\} (1 \le i_1 \le i_2 \le \cdots \le i_p \le n)$ is a set of participants. $M[X]$ denotes the sub-matrix consisting of $i_1, i_2, \cdots, i_p$-th rows of matrix M. Taking each row of M as a vector, XOR(M) means the vector after XOR-ing all rows of M. The Hamming weight of vector V is denoted by $H(V)$. The classical definition of XOR visual cryptography scheme (XVCS) under general access structure is followed.

Definition 3. *([12])* XVCS under (Γ_Q, Γ_F) consists of two collections of $n \times m$ Boolean matrices C_0 and C_1. C_0 (C_1) is used to sharing a white (black) into n shares with m subpixels. C_0 and C_1 satisfy the following two conditions.

(1) $\forall X \in \Gamma_Q, M_0 \in C_0, M_1 \in C_1$, then $H(XOR(M_0[X])) \le t_X - \alpha \bullet m$ and $H(XOR(M_1[X])) \ge t_X$.
(2) $\forall X \in \Gamma_F, D_0 = \{M[X] | M \in C_0\}, D_1 = \{M[X] | M \in C_1\}$, then $D_0 = D_1$.

The condition (1) is a contrast property indicating that the pixel of the secret image can be inferred from the Hamming weight of the result of XOR-ing the shares of a minimal qualified subsets. The condition (2) is a security property means that the information of the secret image cannot be obtained by any forbidden subsets. The parameter t_X is the minimum Hamming weight of subpixels corresponding to the original black pixel. m represents the pixel expansion, that is, the number of subpixels corresponding to an original secret pixel. α indicates the relative difference, reflecting the color difference of black and white secret pixels in the recovery image. When $m = 1$ and $\alpha = 1$, the scheme is named as the **ideal XVCS** and the access structure is named as the ideal access structure (**IAS**), which means the secret image can be completely recovered. As we know, (n, n)-XVCS is a special case of ideal XVCS, where C_0 (C_1) is consists of all $n \times 1$ vectors with even (odd) Hamming wight.

Example 1. *((2, 2)-VCS)*

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

For this scheme, $m = 1$ and $\alpha = 1$. Taking a binary Lena image as an example, the two shares and recovery image are shown in Fig. 2.

Actually, only some special access structures are the ideal. Shen [15] and Fu [21] had analyzed the basic characteristics of IAS, and proposed the secret sharing and recovery algorithms of IAS.

Definition 4. *([21])* Assume that A and B are two participant sets. Let $\times$ denote an operation of two sets, where $A \times B = (A \bigcup B) - (A \bigcap B)$.

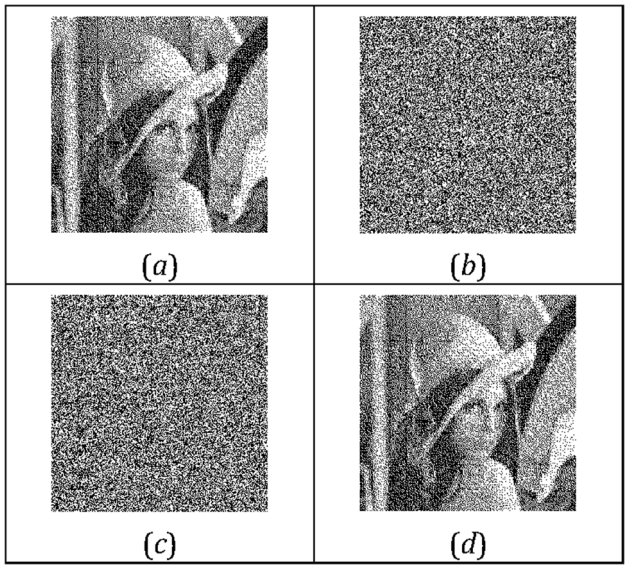

Fig. 2. (2, 2)-VCS: (*a*) Lena; (*b*) Share 1; (*c*) Share 2; (*d*) The recovery image using XOR-ing two shares.

Definition 5. *([21])* Assume that $X = \{p_1, p_2, \cdots, p_x\} \in 2^P$ is a participant set and let T_i denotes the share of the i-th participant. The secret recovery function $f(X) = T_{p1} \oplus T_{p2} \oplus \cdots \oplus T_{px}$ denotes the XOR-ing the shares of X.

Theorem 1. *([21])* *If* $A, B \in 2^P$, *then* $f(A \times B) = f(A) \oplus f(B)$.

Definition 6. *([21])* Assume that S denotes the secret image and $\Gamma_0 = \{Q_1, Q_2, \cdots, Q_t\}$ consists of the minimal qualified sets for access structure (Γ_Q, Γ_F). If $\forall Q \in \Gamma_0$, there always exists f (Q) = S, then (Γ_Q, Γ_F) is an IAS.

Theorem 2. *([21])* Let $\Gamma_0 = \{Q_1, Q_2, \cdots, Q_t\}$ be minimal qualified sets for the access structure (Γ_Q, Γ_F). If the access structure is ideal, the two following conditions are always satisfied.

(1) The result of ' $\times$ ' on odd elements of Γ_0 is a qualified set. That is $Q_{i_1} \times \cdots \times Q_{i_{2k-1}} \in \Gamma_Q$.
(2) The result of ' $\times$ ' on even elements of Γ_0 is the empty set or not included in any minimal qualified set. That is $Q_{i_1} \times \cdots \times Q_{i_{2k}} = \varnothing$ or $Q_{i_1} \times \cdots \times Q_{i_{2k}} \not\subseteq Q_j (\forall Q_j \in \Gamma_0)$.

2.3. Recognition characteristics of QR code

In our scheme, the QR code-like shares contain three-level (visual, public and privacy) information. The visual-level information is a common image, which can be observed by human vision system. The public-level information can be read out directly from the shares by standard QR code readers or software. Different from the visual-level and public-level information, it needs two steps to decode the privacy-level information: 1) XOR-ing the shares of the qualified subset; 2) reading the XOR-ed result by standard QR code readers. The distribution

Fig. 3. Design of the share and a basic sharing unit of 3 $\times$ 3 modules.

of three different information in one share is shown in Fig. 3.

In Fig. 3, the share looks like a QR code with the unmodified function patterns, modified (encrypted) encoding region and a visual image. The visual image is placed in the central part of the share. The public information and encrypted privacy information are arranged in encoding region of the QR code with the sharing unit of 3 × 3 modules, consisting of 1 public module and 8 same privacy modules. The public module is in the central position of the unit, while the privacy modules are surrounding with the public module. Although the visual image covers a part of public and secret information, the readability of public QR code and decrypted privacy QR code will not be influenced based on the error correction capacity of QR code. The size of visual image is decided by the version of the selected QR codes, which will be discussed in Section 4.

It is interesting that there are two different recognition results for one unit of 3 × 3 modules. The first one result, called **key-point** characteristic, is the central (public) module when the QR code reader is close with the unit. The other recognition result, called **average-gray** characteristic, is the surrounding (privacy) modules when the QR code reader is far away from the unit. Fig. 4 shows two different recognition methods for the typical units with 3 × 3 modules, in which the red arrows mean the long-distance recognition and the black arrows mean the short-distance recognition, respectively. In Fig. 4, the '8B1W' unit, consisting of 8 black privacy modules and 1 white public module, can be read as black (white) module at the long (short) distance recognition. Meanwhile, the '8W1B' unit, consisting of 8 white privacy modules and 1 black public module, can be read as white (black) module at the long (short) distance recognition. In Section 3, the key-point characteristic, average-gray characteristic and error correction capacity of QR code are used to design the 3-L QR code.

3. The proposed scheme

3.1. Overview

The motivation of our scheme is to encode the visual, public and privacy information into several QR codes distributed for a group of users. The visual and public information is accessible for anyone in the group, while the privacy information can only be caught by the qualified subset of users. This section presents the generation procedure of 3-L QR codes (Fig. 5) and the recovery procedure of the secret information (Fig. 6).

In Fig. 5, the general access structure is divided into several IASs using IAS division algorithm firstly. Secondly, the shares for one selected IAS are constructed using 3-L QR code generation algorithm, taking one visual image, n public QR codes and the privacy QR code as inputs. Finally, the dealer traverses all IASs and distributes all 3-L QR code shares to users.

In the real-world, the 3-L QR code shares may be stored in different formats, such as the print-format, photo-format and e-format. Therefore, the image distortion rectifying algorithm is designed to transform the print-format and photo-format shares into e-format shares in Fig. 6. Next, the XVCS recovering algorithm is used to decrypting the privacy QR code from all e-format shares, which are selected according to the i-th IAS. Finally, the privacy information can be read out from the recovered image using QR code reader device or software.

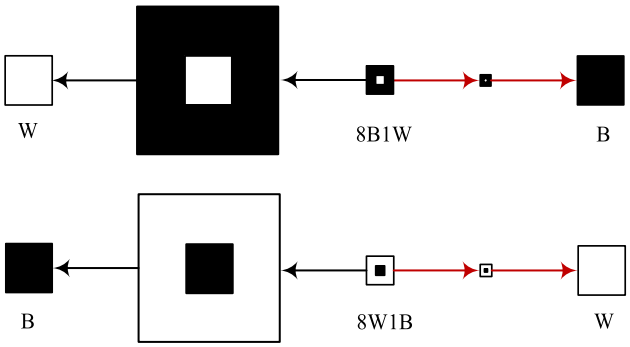

Fig. 4. Two different recognition methods for the unit of 3 × 3 modules.

The main difficulties in the above procedures conclude the IAS division algorithm, 3-L QR code generation algorithm, image distortion rectifying algorithm and privacy recovering algorithm, while the encoding and decoding of common QR code are very mature. According to the previous study of VCS, the shares and recovered secret image have noise-like distortions, which may disturb the recognition of the QR code reader. Therefore, how to decrease the distortions of shares and recovered image is the main work of this paper. The detailed algorithms are designed in Section 3.2.

3.2. Algorithms

3.2.1. IAS division algorithm

No pixel expansion and perfect recovery are the advantages of the XVCS under IAS. However, most of the generic access structures (GAS) are not ideal due to the strict limitations of IAS. So, Algorithm 1 [21] is used to divide the GAS into several IASs.

Algorithm 1. Divide GAS into Several IASs

Input: the minimal qualified set Γ_0 of GAS, and two sets $Q = F = \varnothing, i = 1$. Output: d minimal qualified subsets $\Gamma_0^1, \Gamma_0^2, \cdots, \Gamma_0^d$, which belong to different IASs respectively.
Step 1: Choose a set X randomly from Γ_0, then $Q = Q \cup X$ and $\Gamma_0 = \Gamma_0 - X$;
Step 2: Traverse Γ_0 to find the existence of a set Y, which $Q \cup Y$ satisfies with condition (1) and (2) of Theorem 2. If Y exists, then $Q = Q \cup Y$, $\Gamma_0 = \Gamma_0 - Y$ and turn to Step3. Otherwise, let $\Gamma_0^i = Q$, $\Gamma_0 = \Gamma_0 \cup F$, $Q = F = \varnothing$ and $i = i + 1$, then turn to Step 1;
Step 3: For set Q, let Z_e represent all results of 'x' on even elements of Q. $\forall A \in \Gamma_0$, if $Z_e \subseteq A$, then move Z_e from Γ_0 into F;
Step 4: For set Q, let Z_o represent all results of 'x' on odd elements of Q. If $Z_o \in \Gamma_0$, then move Z_o from Γ_0 into Q ;
Step 5: If $\Gamma_0 \neq \varnothing$ then turn to step 2; If $\Gamma_0 = \varnothing$ and $F \neq \varnothing$, then let $\Gamma_0^i = Q, \Gamma_0 = F, Q = F = \varnothing, i = i+1$ and turn to Step 1. If $\Gamma_0 = \varnothing$ and $F = \varnothing$, then let $d = i$, output IASs $\Gamma_0^1, \Gamma_0^2, \cdots, \Gamma_0^d$, and algorithm ends.

3.2.2. 3-L QR code generation algorithm

Since the readability of QR code is very sensitive to the correctness of modules in the function patterns, our algorithm leaves these modules untouched and only manipulates the data modules. We recommend readers to refer to the QR code ISO standard [1] for technical details regarding QR code generation.

Algorithm 2. 3-L QR Code Generation Algorithm

Inputs: IAS$_j$ $(\Gamma_Q, \Gamma_F, \Gamma_0)$, visual image V_j, n public QR codes $P_1, P_2, \cdots, P_n$ with size of $a \times a$, secret QR code S with size of $a \times a$
Outputs: j-th sub-shares $T_1^j, T_2^j, \cdots, T_n^j$ with size of $3a \times 3a$
Step 1. Encrypting S into n shares satisfying IAS$_j$.
Step 1.1 Choose the maximal subsets Q_{max} of Γ_0. For $Q_{max} = \{i_1, i_2, \cdots, i_{|Q_{max}|}\}$, generate $|Q_{max}| - 1$ shares $T_{i_1}, T_{i_2}, \cdots, T_{i_{|Q_{max}|-1}}$ randomly. Then, compute $T_{i_{|Q_{max}|-1}} = S \oplus T_{i_1} \oplus T_{i_2} \oplus \cdots \oplus T_{i_{|Q_{max}|-1}}$.
Step 1.2 Let $\Gamma_0 = \Gamma_0 - Q_{max}$. If $\Gamma_0 = \varnothing$, algorithm ends. Otherwise, turn to Step1.3.
Step 1.3 If there exists $Q_i \in \Gamma_0$ in which one participant has already be evaluated at least, then turn to Step1.4; otherwise, turn to Step1.1.
Step 1.4 If all the shares of Q_i have been valuated, turn to Step 1.5. Otherwise, Q_i is denoted as $Q_i = \{A_1, \cdots, A_x, B_1, \cdots, B_y\}, (1 \le x \le n-1, 1 \le y \le n-1, 2 \le x+y \le n)$. Suppose that shares $T_{A_1}, T_{A_2}, \cdots, T_{A_x}$ of participants $A_1, A_2, \cdots, A_x$ have already been evaluated, while the shares $T_{B_1}, T_{B_2}, \cdots, T_{B_y}$ of participants $B_1, B_2, \cdots, B_y$ are needed to be evaluated. Firstly, generate random shares $T_{B_1}, T_{B_2}, \cdots, T_{B_{y-1}}$ with same size to secret image, then compute $T_{B_y} = S \oplus T_{A_1} \oplus T_{A_2} \oplus \cdots \oplus T_{A_x} \oplus T_{B_1} \oplus T_{B_2} \oplus \cdots \oplus T_{B_{y-1}}$.
Step1.5 Let $\Gamma_0 = \Gamma_0 - Q_i$. If $\Gamma_0 = \varnothing$, turn to Step 2. Otherwise, turn to Step 1.3.
Step 2. Expanding the sizes of shares and embedding the public modules.
Step 2.1 Let $i, k, l = 0$
Step 2.2 Let $i \leftarrow i + 1$. If $i \le n$, go to Step 2.3; else, go to Step 3.
Step 2.3 Let $k \leftarrow k + 1$. If $k \le a$, go to Step 2.4; else, go to Step 2.2.
Step 2.4 Let $l \leftarrow l + 1$. If $l \le a$, let $T_i^j(3k-2 : 3k, 3l-2 : 3k) = T_i(k, l) \times ones(3, 3)$, $T_i^j(3k-1, 3l-1) = P_i(k, l)$, go to Step 2.4; otherwise, go to Step2.3.

(continued on next page)

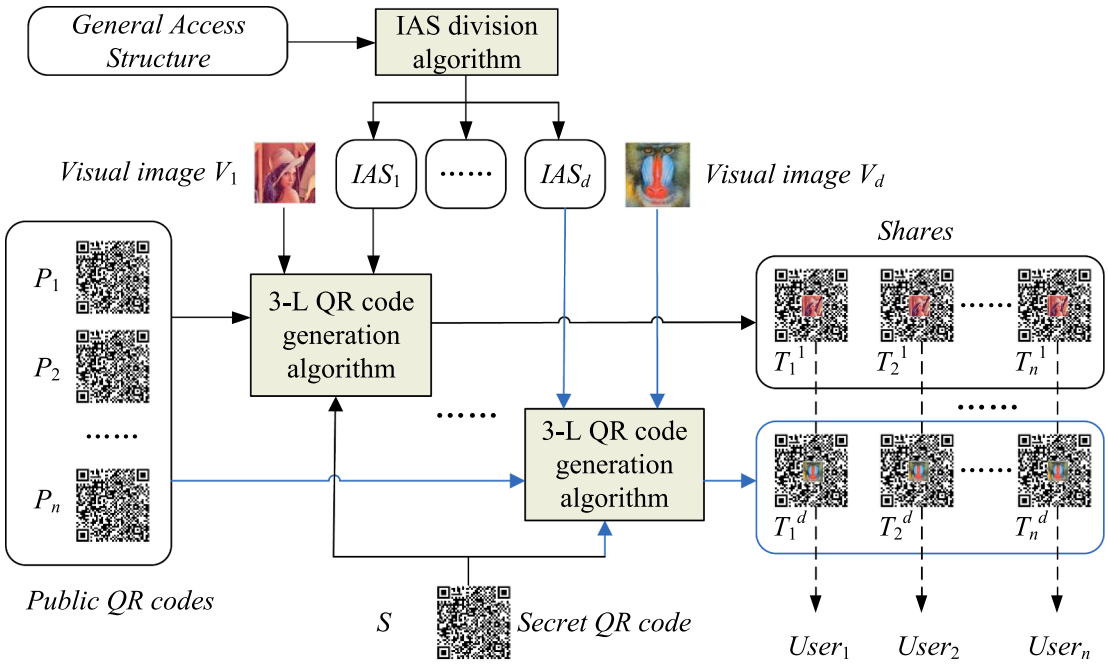

Fig. 5. The generation procedure of 3-L QR code shares.

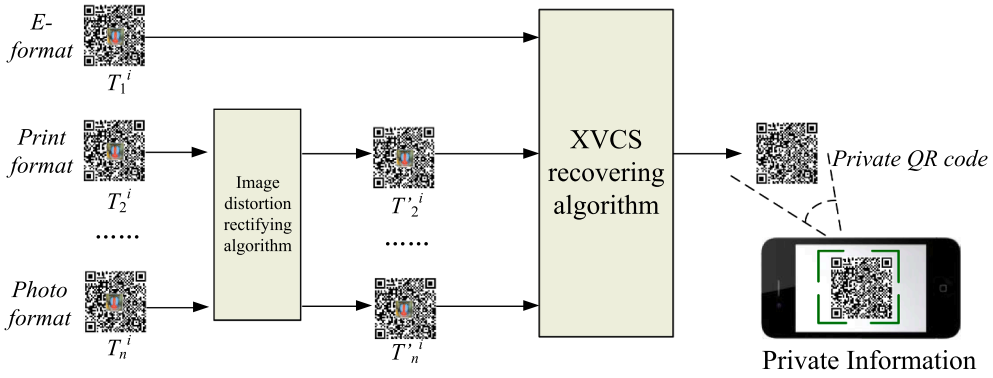

Fig. 6. The recovery procedure of secret information.

(*continued*)

Algorithm 2. 3-L QR Code Generation Algorithm

Step 3. According to error correction level and the size of QR code, the size of visual image v should be limited as $\frac{v^2}{a^2} \leq$ QR E-version. Then, embedding the visual image in the central of shares $T_1^i, T_2^i, \cdots, T_n^i$. The size of visual image should be smaller than the upper limit, in order to increase the robustness of the QR code recognition.

Step 4. Algorithm ends.

3.2.3. *Image distortion rectifying algorithm*

In practical application scenarios, QR code shares are usually stored or transferred in print-format or photo-format. There always exist distortions or noises in the print-format or photo-format shares, compared with the original e-format ones. It is difficult that recovering the privacy QR code from print-format or photo-format shares directly. Therefore, the print-format or photo-format shares are needed to be adjusted into the e-format shares using the image distortion rectifying algorithm. The detailed algorithm is as follows. The experimental result of the image distortion rectifying algorithm will be shown in Section 4. Meanwhile, the relationship between the side length of original share, printed or photo shares and rectified shares will be analyzed.

Algorithm 3. Image Distortion Rectifying Algorithm

Input: the print-format or photo-format QR code-like share T with size of $3b \times 3b$

Output: adjusted binary QR code-like share T' with size of $3c \times 3c$

Step 1. Transform the color image T into grey image g_T.

Step 2. using bot-hat transformation on g_T.

Step 3. binary processing the grey image g_T using Otsu algorithm, and then implementing the binary image b_T.

Step 4. finding four location points from directions of upper left, upper right, bottom left and bottom right. Denote the points as $ul(X_1, Y_1)$, $ur(X_2, Y_2)$, $bl(X_3, Y_3)$ and $br(X_4, Y_4)$, where X and Y mean the coordinates of distorted QR code.

Step 5. Denote the four vertices of the original e-format share as $ul(x_1, y_1)$, $ur(x_2, y_2)$, $bl(x_3, y_3)$ and $br(x_4, y_4)$. Using inverse projection transformation, we have

$$X = \frac{k_0 x + k_1 x + k_2}{k_6 x + k_7 y + 1}, Y = \frac{k_3 x + k_4 x + k_5}{k_6 x + k_7 y + 1} \quad (1)$$

The eight parameters $k_0 \sim k_7$ can be computed from equation (2).

$$\begin{bmatrix} x_1 & x_1 & 1 & 0 & 0 & 0 & -x_1 \cdot X_1 & -y_1 \cdot X_1 \\ 0 & 0 & 0 & x_1 & x_1 & 1 & -x_1 \cdot Y_1 & -y_1 \cdot Y_1 \\ x_2 & x_2 & 1 & 0 & 0 & 0 & -x_2 \cdot X_2 & -y_2 \cdot X_2 \\ 0 & 0 & 0 & x_2 & x_2 & 1 & -x_2 \cdot Y_2 & -y_2 \cdot Y_2 \\ x_3 & x_3 & 1 & 0 & 0 & 0 & -x_3 \cdot X_3 & -y_3 \cdot X_3 \\ 0 & 0 & 0 & x_3 & x_3 & 1 & -x_3 \cdot Y_3 & -y_3 \cdot Y_3 \\ x_4 & x_4 & 1 & 0 & 0 & 0 & -x_4 \cdot X_4 & -y_4 \cdot X_4 \\ 0 & 0 & 0 & x_4 & x_4 & 1 & -x_4 \cdot Y_4 & -y_4 \cdot Y_4 \end{bmatrix} \times \begin{bmatrix} k_0 \\ k_1 \\ k_2 \\ k_3 \\ k_4 \\ k_5 \\ k_6 \\ k_7 \end{bmatrix} = \begin{bmatrix} X_1 \\ Y_1 \\ X_2 \\ Y_2 \\ X_3 \\ Y_3 \\ X_4 \\ Y_4 \end{bmatrix} \quad (2)$$

Step 6. The bilinear interpolation algorithm is used to correct the distorted QR code and then repair the image with morphology. For each pixel $o(x, y)$ in original QR

(*continued on next page*)

(*continued*)

Algorithm 3. Image Distortion Rectifying Algorithm

code, the corresponding projection position $p(X, Y)$ in b_T can be deduced using equation (1). If X and Y are both integers, $o(x, y) = p(X, Y)$. Otherwise, $o(x, y)$ is computed using the bilinear interpolation algorithm with the surrounding four pixels of $p(X, Y)$.

Step 7. Algorithm ends.

3.2.4. Privacy recovering algorithm

For visual-level image, it can be seen from 3-L QR code by human vision system directly. For public-level information, it can be read out from 3-L QR code shares using standard QR code reader device or smart phone with QR code reader software. For privacy-level information, its recovery needs some computations on the shares of qualified subset.

In this section, the privacy recovering algorithm is designed for the privacy-level information using the rectified shares as inputs, which are also the outputs of the image distortion rectifying algorithm. To reconstruct the privacy-level information, only XOR, Add and comparison operations are required, which have low computational costs.

Algorithm 4. Privacy Recovering Algorithm

Input: the rectified shares of $IAS_j, T_1^j, T_2^j, \cdots, T_n^j$ with size of $3c \times 3c$

Output: the recovered privacy QR code S' with size of $a \times a$, and c is the integer times of a.

Step 1. For each pixel $s(x, y)$ in the encoding data region of recovered secret QR, $s(x, y) = T_1^j(x,y) \oplus \cdots \oplus T_n^j(x,y)$.

Step 2. For each pixel $s(x, y)$ in the function pattern region of recovered secret QR, $s(x, y) = T_1^j(x,y)$.

Step 3. Let $i, k, th = 0$

Step 3.1 Let $i \leftarrow i + 1$. If $i \le a$, go to Step 3.2; else, go to Step 4.

Step 3.2 Let $k \leftarrow k + 1$. If $k \le a$, go to Step 3.3; else, go to Step 3.1.

Step 3.3 $th(i, k) = \sum_{u=0}^{u=3c/a-1} \sum_{v=0}^{v=3c/a-1} s(\frac{3c}{a} i - u, \frac{3c}{a} k - v)$.

Step 3.4 If $th(i, k) \ge \frac{9c^2}{2a^2}$, $s'(i,k) = 1$; else, $s'(i,k) = 0$.

Step 4. Algorithm ends.

4. Experiments and analysis

To evaluate the feasibility of our approach, we performed several experiments described in this section. In addition, we provide some comparisons with other related schemes.

4.1. Experiment results

4.1.1. 3-L QR code for general access structure

In a bank, there are one general manager (GM) and three assistant managers (AM 1, 2, 3) keeping the password of the vault together. Considering the different weights of GM and AM, GM and any AM can open the door of the vault, while all three AMs can recover the password of the vault. Actually, the password-keeper problem is a general access structure Γ_0= { {1,2}, {1,3}, {1,4}, {2,3,4} }, where '1′ denotes the GM and '234′ denote three AMs, respectively. The experimental dataset for Γ_0 is listed in Table 2.

Table 2
Experimental dataset.

Information level	Information style	Content
Visual Information	image	Lena
Visual Information	image	Baboon
Public Information of GM	QR code	"GM, Alice, ID:1001, Female"
Public Information of AM1	QR code	"AM, Bob, ID:1002, Male"
Public Information of AM2	QR code	"AM, Clark, ID:1003, Male"
Public Information of AM3	QR code	"AM, Doris, ID:1004, Female"
Privacy Information	QR code	"Password of the vault is 123456789″

According to the IAS division algorithm, the GAS Γ_0 is divided into two IASs: IAS_1 Γ_0^1= { {1,2}, {1,3}, {1,4}} and IAS_1 Γ_0^2={ {2,3,4} }. Next, all the shares of GM and AMs are constructed using the 3-L QR code generation algorithm for IAS_1 and IAS_2, respectively. The visual images, public QR codes, secret QR code and all shares are shown in Fig. 7. To evaluate the effectiveness of the proposed scheme, the open-source library ZXing is used to encode and decode the QR code. The version 3-Q (version3, error correction level Q) is selected for the public and secret QR codes with the size 37 × 37 modules. Meanwhile, the size of 3-L QR code shares are 111 × 111 modules, and the size of rectified shares are set as 333 × 333 modules, that is $la = 111$ and $lc = 333$. The size of print-format or photo-format share lb is determined by resolution of the scanner or camera, respectively. Considering the effectiveness of image distortion rectifying algorithm, $lb > lc$ should be guaranteed.

In Fig. 7, (*a*)-(*d*) are four public QR codes $P_1 \sim P_4$, and (*e*) is the secret QR code S. Fig. 7(f)-(g) are two visual images $V_1 \sim V_2$. Fig. 7(h)-(k) are four shares T_1, T_2^1, T_3^1 and T_4^1, which are generated for IAS_1 using Algorithm 2. Fig. 7(l) is the recovery of e-format shares T_1 and T_2^1, or T_1 and T_3^1, or T_1 and T_4^1 using Algorithm 4. Fig. 7 (*m*)-(*o*) are three shares T_2^2, T_3^2 and T_4^2, which are generated for IAS_2 using Algorithm 2. It should be noted that T_1^2 is not generated since {1} is not in Γ_0^2. Fig. 7(p) is the recovery of e-format shares T_2^2, T_3^2 and T_4^2 using Algorithm 4.

For 3-L QR code shares, the visual images can be seen by human visual system directly, which are used for distinguishing the different IASs. Specifically, Lena is for IAS_1 and Baboon is for IAS_2, respectively. Then, the public information can be read out from 3-L QR code share directly by QR code reader device at the short distance. Moreover, Fig. 7 (l) and (p) are similar with the secret QR code except for the central part, which is used for the visual images. Due to the error correction capacity of QR code, the secret information can also be extracted from Fig. 7(l) and (p) using QR code reader device.

4.1.2. Recovery of multi-format shares

In practical applications, the 3-L QR code shares are not only stored in e-format, but also in printed or photo format. In most cases, we must consider the recovery results of the printed or photo format 3-L QR code shares, which are need to be rectified into standard e-format shares at first. To test the effectiveness of the Algorithm 3, we take a picture of the share under the natural light (Fig. 8(c)) as the input of the image distortion rectifying algorithm, and then get the rectified image (Fig. 8 (*d*)) as the output of the algorithm.

In order to evaluate the effectiveness of the image distortion rectifying algorithm, $F = 1 - \frac{\sum XOR(T,T')}{M \cdot N}$ is defined as the fidelity of the rectified photo-format share compared with the original share, where T denotes the binary original share and T' denotes the rectified photo-format share. In this paper, the side length of rectified e-share lc is set as the integer times of la. When we compute the F, the original share is expanded with lc/la times. The relationship between F and lc/la is shown in Fig. 9.

As Fig. 9 shows, when the magnification is 1, the fidelity is relatively high at 84%. As the magnification increases, the recovery fidelity increases significantly. When the magnification is greater than 6, the fidelity is maintained at 97% and the recovery effectiveness is acceptable. Under the premise that each image recovery distortion ratio is 3%, we test the recovery effectiveness of the printed or photo format 3-L QR code shares. The photo format shares, rectified shares and the recovered secret QR code are showed in Fig. 10. In Fig. 10, (*a*)-(*e*) are five photo-format shares, named T_1, T_2^1, T_2^2, T_3^2 and T_4^2. Using Algorithm 3, Fig. 10(f)-(j) are the rectified e-format shares corresponding to T_1, T_2^1, T_2^2, T_3^2 and T_4^2. Fig. 10 (*k*) is the recovery of rectified T_1 and T_2^1 using Algorithm 4, while Fig. 10 (*l*) is the recovery of rectified T_2^2, T_3^2 and T_4^2. The privacy-level information can be extracted from Fig. 10 (*k*) and (*l*), which means the proposed Algorithm 3 and 4 are available to photo-format shares.

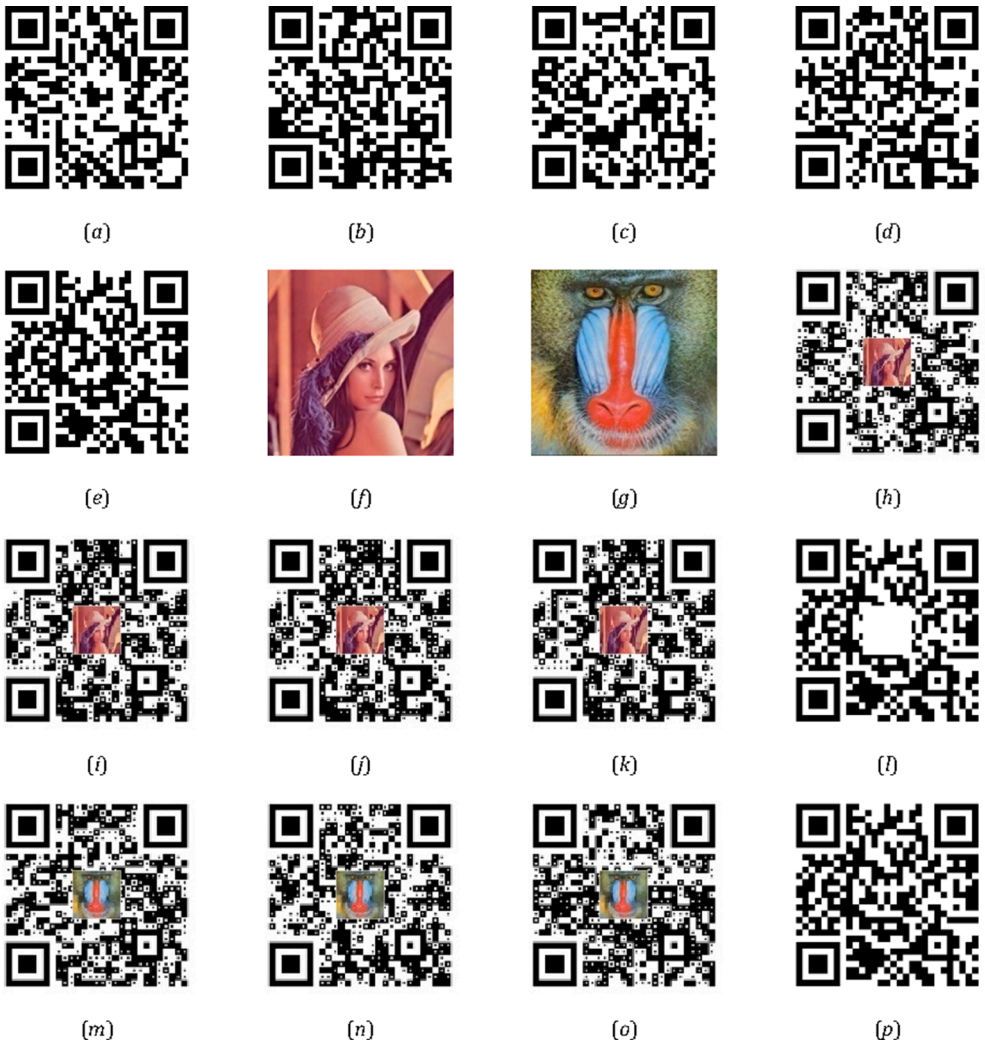

Fig. 7. QR codes, shares and the recovery of e-format shares: (*a*)-(*d*) public QR codes $P_1 \sim P_4$; (*e*) secret QR code *S*; (*f*)-(*g*) visual images $V_1 \sim V_2$; (*h*)-(*k*) shares of IAS_1, T_1, T_2^1, T_3^1 and T_4^1; (*l*) Recovery of T_1 and T_2^1, or T_1 and T_3^1, or T_1 and T_4^1; (*m*)-(*o*) shares of IAS_2, T_2^2, T_3^2 and T_4^2; (*p*) Recovery of T_2^2, T_3^2 and T_4^2.

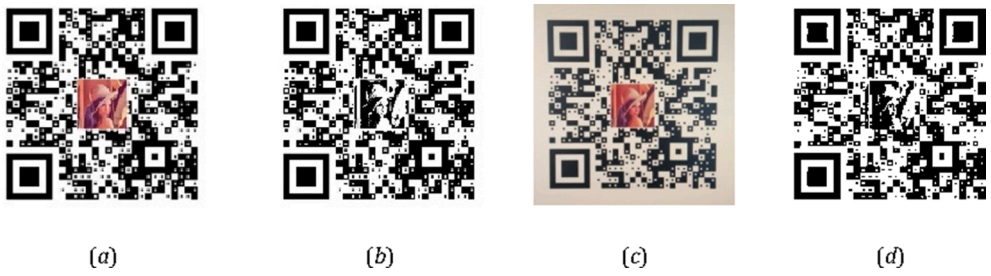

Fig. 8. The result of image distortion rectifying algorithm: (a) original share T_1; (b) binary share T_1; (c) photo-format share T_1; (d) the rectified share T_1.

4.1.3. Size of the visual image

Based on the error correction mechanism of the QR code, when the number of code words covered by the visual image is smaller than the error correction capability of the QR code, the generated QR code can still be correctly read. In the 3-L QR code share, each 3 × 3 module identification unit contains 1-bit information of the carrier QR code, so the size of the visual image should satisfy $\frac{v^2}{(3a)^2} \leq E$, where E indicates the error correction level of the QR code.

4.1.4. Comparison and discussion

The comparison of this paper and other related schemes is described in Table 3.

(1) Meaningful of shares. In Ref [16,17], the shares are noise-like, while the shares in Ref [2,18,19,20,21] are meaningful, and the public information can be decoded by a normal QR code decoder, which reduces the probability of attracting the potential attackers. In this paper, the shares look like ordinary QR codes, and the public-level information can also be read by the QR code decoder. Furthermore, the shares are tagged with visual-level image, which are easy to manage.

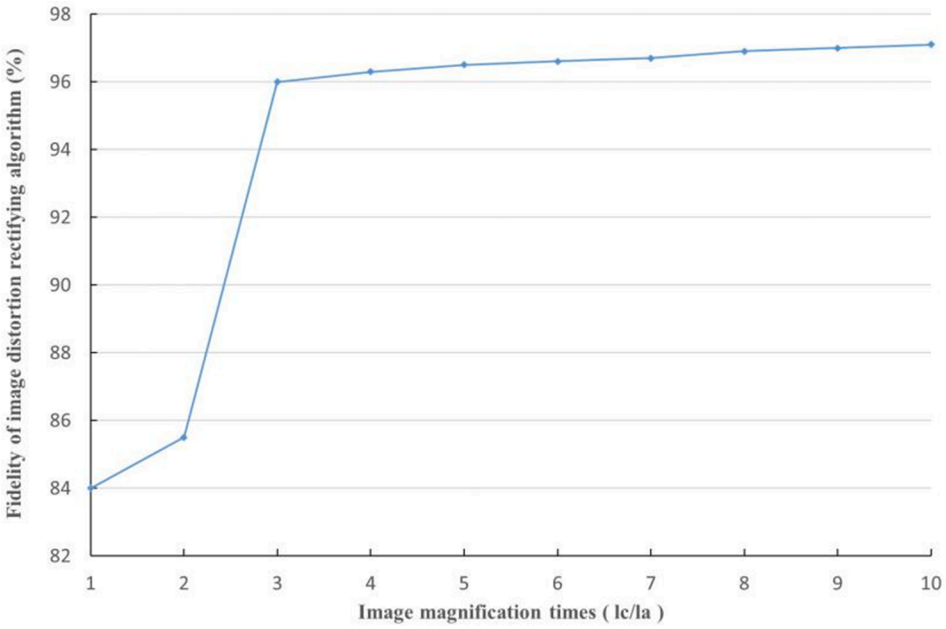

Fig. 9. The relationship between the fidelity and image magnification times.

Fig. 10. Photo-format shares, rectified shares and the recovered privacy QR code: (*a*)-(*e*) photo-format shares T_1, T_2^1, T_2^2, T_3^2 and T_4^2; (*f*)-(*j*) rectified shares of T_1, T_2^1, T_2^2, T_3^2 and T_4^2; (*k*) the recovery of T_1, T_2^1; (*l*) the recovery of T_2^2, T_3^2 and T_4^2.

(2) Levels of information. Most previous schemes have only two levels information: public and privacy. However, the proposed scheme contains three levels information: visual, public and privacy. Therefore, our scheme carries more information than others.

(3) Readability of recovered privacy QR code. The privacy information of Ref [16,17,19,21] are all not QR code but the common images. Ref [20] had a poor decoding efficiency with a small relative difference 1/4. The relative difference of Ref [2,18] was 1/2, which leaded to a quicker decode. In this paper, we divide

Table 3
Functional comparisons of our scheme and the previous ones.

	Meaningful shares	Levels of information	Readability of recovered privacy QR code	Recovery computation	Computational complexity
[2]	Yes	2	Average	secret extracting	O($N\log N$)
[16]	No	2	No	*OR*	O(N)
[17]	No	2	No	*OR*	O(N)
[18]	Yes	2	Average	*XOR* and Adding pattern	O(N)
[19]	Yes	2	No	*OR*, *XOR*	O(N)
[20]	Yes	2	Hard	*OR*, *XOR*, Filtering	O(N)
[21]	Yes	2	No	*XOR*	O(N)
Our scheme	Yes	3	Easy	*XOR*, *Add* and *Comparison*	O(N)

the general access structure into several ideal access structures, which recovery the privacy QR code perfectly. Therefore, the relative difference of our scheme is 1, which means the information of recovered privacy QR code can be easily read out.

(4) Recovery computation. Ref [16,17,19,20] reconstructed the secret image by stacking the shares, which equals to OR-ing the shares. Ref [19,21] utilized the XOR operation as the recovery computation. Ref [2,18] needed extra extraction operations. In our scheme, XOR, Add and comparison operations are used to decode the privacy-level information.

(5) Computational complexity. Assume that there are n participants and N modules of the public and privacy QR codes. According to the privacy recovering algorithm, there needs $(n\text{-}1)N$ "XOR", 8 N "Add" and N "comparison" operations. Therefore, the computational complexity of the proposed scheme is O(N), which is equal to Ref [16–21], and better than [2].

Functional comparisons of the proposed scheme and other related works have been discussed above. And the major advantages of this paper are concluded as follows.

(1) Three-level information protection. The proposed scheme divides the information into three level. The visual-level information is the ordinary image tagged on the surface of the shares, which can be obtained by human's visual system to mark the shares. The public-level information is encoded to generate the carrier QR code, which can be recognized and decoded by any common QR code reader. The privacy-level information can only be obtained by XOR-ing and filtering the shares of qualified participant set, which can prevent the information from leaking.

(2) Perfect recovery of the privacy QR code. In this paper, we divide the general access structure into several IASs, and use several visual images to mark the different IASs. When the participants of one IAS want to recovery the privacy QR code, they firstly choose the corresponding shares of the IAS, and then use the privacy recovering algorithm to reconstructed the privacy QR code perfectly.

(3) Supporting multiple formats of the shares. In the previous schemes, the QR code shares are usually stored in electronic format, and the privacy information is usually recovered by various calculations on the e-format shares. In this paper, the shares can be stored not only in electronic format, but also by printing and photographing formats, which is more practical and easier to be applied in the actual scenes.

5. Conclusions

In the paper, a novel 3-level information protect scheme is proposed based on QR code and VCS. The visual-level image can be observed by human vision system, which is used to classify the shares of different IASs. The public-level QR code can be recognized by any QR code decoder based on the key-point characteristic of QR code. The privacy-level QR code can be recovered perfectly by the distortion rectifying algorithm and privacy recovering algorithm. Compared with other related works, the proposed scheme has the advantages of carrying more information, perfect recovery of privacy QR code and supporting multiple formats of shares. In the future, we plan to investigate some characteristics of machine recognition for the smaller image size and higher privacy payload.

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgments

The authors thank the anonymous reviewers for their valuable comments. This work was supported by the National Natural Science Foundation of China under Grant No.61602513.

References

[1] ISO/IEC 18004, Information Technology Automatic Identification and Data Capture Techniques- Bar Code Symbology-QR Code, 2000.
[2] G.J. Chou, R.Z. Wang, The Nested QR Code, IEEE Signal Process. Lett. 27 (2020) 1230–1234.
[3] I. Tkachenko, W. Puech, C. Destruel, O. Strauss, J.M. Gaudin, C. Guichard, Two-level QR code for privacy message sharing and document authentication, IEEE Trans. Inf. Forensics Secur. 11 (2016) 571–583, https://doi.org/10.1109/TIFS.2015.2506546.
[4] C. Patvardhan, P. Kumar, C. Vasantha Lakshmi, Effective Color image watermarking scheme using YCbCr color space and QR code, Multimedia Tools Appl. 77 (10) (2018) 12655–12677.
[5] P.Y. Lin, Distributed Secret Sharing Approach With Cheater Prevention Based on QR Code, IEEE Trans. Ind. Inf. 12 (2016) 384–392, https://doi.org/10.1109/TII.2015.2514097.
[6] M. Naor, A. Shamir, Visual cryptography. EUROCRYPT 1994: Advances in Cryptology - EUROCRYPT'94, LNCS 950 (1995) 1–12, https://doi.org/10.1007/BFb0053419.
[7] G. Ateniese, C. Blundo, A.D. Santis, D.R. Stinson, Visual cryptography for general access structures, Inf. Comput. 129 (1996) 86–106, https://doi.org/10.1006/inco.1996.0076.
[8] X. Wu, W. Sun, Generalized random grid and its applications in visual cryptography, IEEE Trans. Inf. Forensics Security 8 (9) (2013) 1541–1553.
[9] F. Liu, C. Wu, Embedded extended visual cryptography schemes, IEEE Trans. Inf. Forensics Security 6 (2) (2011) 307–322.
[10] X.H. Yan, Q.H. Gong, L.L. Li, G. Yang, J. Liu, Secret image sharing with separate shadow authentication ability, Signal Process.-Image Commun. 82 (2020).
[11] C.N. Yang, C.H. Wu, Z.X. Yeh, D.S. Wang, C. Kim, A new sharing digital image scheme with clearer shadow images, Comput. Stand. Interfaces 51 (2017) 118–131, https://doi.org/10.1016/j.csi.2016.11.015.
[12] P. Tuyls, H.D. Hollmann, J.H. Lint, L. Tolhuizen, XOR-based visual cryptography schemes, Des. Codes Crypt. 37 (2005) 169–186, https://doi.org/10.1007/s10623-004-3816-4.
[13] Z.X. Fu, B. Yu, Optimal pixel expansion of deterministic visual cryptography scheme, Multimedia Tools Appl. 73 (2014) 1177–1193.
[14] C.N. Yang, C. Wu, D. Wang, A discussion on the relationship between probabilistic visual cryptography and Random Grid, Inf. Sci. 278 (2014) 141–173.
[15] G. Shen, F. Liu, Z. Fu, B. Yu, Perfect Contrast XOR-based Visual Cryptography Schemes via Linear Algebra, Des. Codes Crypt. 85 (1) (2017) 15–37.
[16] J. Weir, W.Q. Yan, Authenticating Visual Cryptography Shares Using 2D Barcodes, in: IWDW 2011: Digital Forensics and Watermarking 7128, 2011, pp. 196–210, https://doi.org/10.1007/978-3-642-32205-1_17.
[17] G. Wang, F. Liu, W.Q. Yan, 2D barcodes for visual cryptography, Multimedia Tools Appl. 75 (2) (2016) 1223–1241.
[18] Y.W. Chow, W. Susilo, G. Yang, J.G. Phillips, I. Pranata, A.M. Barmawi, in: Exploiting the Error Correction Mechanism in QR Codes for Secret Sharing,

Springer International Publishing, 2016, pp. 409–425, https://doi.org/10.1007/978-3-319-40253-6_25.
[19] S. Wan, Y. Lu, X. Yan, Y. Wang, C. Chang, Visual secret sharing scheme for (k, n) threshold based on QR code with multiple decryptions, J. Real-Time Image Proc. 14 (2018) 25–40.
[20] Z. Fu, Y. Cheng, S. Liu, B. Yu, A new two-level information protection scheme based on visual cryptography and QR code with multiple decryptions, Measurement 141 (2019) 267–276.
[21] L. Tan, Y. Lu, X. Yan, L. Liu, X. Zhou, XOR-ed visual secret sharing scheme with robust and meaningful shadows based on QR codes, Multimedia Tools Appl. 79 (2019) 5719–5741.