

One-Code-Pass User Authentication Based on QR Code and Secret Sharing

Yanjun Liu¹, Chin-Chen Chang¹, and Peng-Cheng Huang^{1,2}

(Corresponding author: Peng-Cheng Huang)

Department of Information Engineering and Computer Science, Feng Chia University¹
Taichung 40724, Taiwan

College of Computer and Information Engineering, Xiamen University of Technology²
Xiamen, Fujian, China

(Email: pc4hpc@gmail.com)

(Received July 10, 2018; Revised and Accepted Feb. 7, 2019; First Online Oct. 6, 2019)

Abstract

The quick response (QR) code has gained extensive popularity in information storage and identification in our daily lives due to its small printout size, high storage capacity and error correction ability. Taking into account these fascinating features of the QR code, we propose a user authentication protocol based on QR code and secret sharing. It is the first user authentication protocol that implements the “one-code-pass” functionality in which an authorized user can use only one QR code to access various services from all departments within an organization. In the proposed protocol, a secret is divided into many shares in the form of QR codes held among different departments and users. The original secret must be restored by the cooperation of both the department’s share and the user’s share for the authentication. Experimental results demonstrate that the proposed protocol has high robustness and is secure against various typical attacks.

Keywords: One-Code-Pass; QR Code; Security; Secret Sharing; User Authentication

1 Introduction

The user authentication mechanism has been regarded as a very important technique to efficiently verify the identity of the user through various kinds of secure communications. In 1981, for the first time Lamport [8] introduced a password-based remote user authentication protocol. Since then, numerous variants [6, 7, 9, 18] of Lamport’s protocol have been developed in the literature, noticeably extending the scope of applications for user authentication in the field of secure communications, such as the agreement and distribution of session keys, e-business systems and wireless network communications, *etc.*

At present, user authentication protocols generally fall into four categories, *i.e.*, password-based, smart card-

based, biometrics-based and image morphing-based protocols. In a password-based user authentication protocol [8, 18], the user first registers at the remote server by transmitting a selected password to the server privately. Then, the server can provide the user with required services after the authentication process, in which the password presented by the user is checked to confirm that the user is legal. However, a cost-inefficient problem arises due to the fact that a verifier table maintaining users’ private information for authentication must be stored on the server and the volume of the verifier table is in proportion to the increased number of users. Therefore, the verifier table needs to occupy much storage space when a lot of users need to be authenticated. Besides, private information of the users may be leaked out since the verifier table is prone to be stolen with malicious intention.

To overcome the aforementioned shortcomings, the smart card is employed extensively in the design of a user authentication protocol. There are two main advantages for the use of smart card [6]. Firstly, the level of security can be enhanced significantly. Each user individually owns a smart card which stores important and confidential information for mutual authentication that can authenticate not only the user but also the remote server. Furthermore, the private information of all users is fully dispersed by smart cards rather than being centralized in a verifier table, substantially attenuating the risk of information disclosure. Secondly, the authentication protocol becomes more cost-efficient because there is no need to maintain a great deal of users’ information on the server. A typical smart card based authentication protocol is conducted as follows [9]. First of all, the user submits a registration request to the server, and then, the server delivers a smart card storing private information of both the user and the server to the user over a secure channel. When the user inserts the smart card into a card reader for specific services provided by the server, the identity of the user should be verified to confirm that the user is the

true card owner. The private information maintained in the smart card is extracted by the card reader and then transmitted to the server for mutual authentication. If the authentication is passed, a shared session key is usually established by the authorized user and the server to ensure subsequent secure communication.

Unfortunately, the smart card is liable to be forged since an illegal user may easily invade the secret information preserved in the smart card due to weak computing power [7]. Consequently, biometrics information [16] referring to unique biometric feature of a person that is unable to be stolen or forged, has been employed as a popular tool to further increase the authentication security. Fingerprint, face, iris, voice and gait are the most common biometric information used to verify the identity of the user since it is impossible for two people to present identical data of these biometric features [20, 21]. The biometric information of the true user is usually stored in advance. For authentication, the current biometrics feature is retrieved by the biometric reader and then compared with the stored information. If they can match, the identity of the user is authenticated; otherwise, the authentication process fails.

Recognition rate that indicates the identification accuracy is one of the most important measurements for performance evaluation of a biometrics-based authentication protocol [21]. Therefore, the research subject on recognition rate has attracted scholars' attention in recent years and great recognition rate has been obtained by unceasing improvements on feature matching algorithms. However, this type of authentication protocol has the following weaknesses [16, 20, 21]. Firstly, it just provides weak privacy protection since personal biometric information may be disclosed and then abused by malicious adversaries. Secondly, if the true user's biometric information is destroyed because of diseases or accidents, it will induce incorrect authentication. At last, development of a robust biometric reader is both time-consuming and money-consuming.

To make further efforts on the uplift in security and performance, a new type of authentication protocols based on image morphing has flourished. The image morphing technology suspends from the production of special image effects in the film industry in such a way that given a source image and a target image, a morphed image is created. The morphed image looks like both the source image and the target image. This attractive characteristic can be well applied to identity authentication. Up to date lots of user authentication protocols combining image morphing with smart card are introduced [13, 15, 22]. Zhao and Hsieh [22] presented a card user authentication protocol in which a morphed image MI is first created via the card owner's face image OI and a pre-selected face image SI and then printed on the smart card. When a card user needs to be authenticated, the image OI is recovered by a de-morphing process operating on the images MI and SI . Then, the image OI is compared with the face image of the user. If they are the same, it implies

that the user is legal; otherwise, an unauthorized user is successfully detected. Since the original face image of the card owner is no longer stored anywhere, this protocol can furnish efficient privacy protection and higher security level. In 2015, Mao *et al.* [15] introduced a proxy user authentication protocol. In their protocol, the proxy user has authority to act on behalf of the primary user and all users are able to be authenticated by image exchange based on morphing technology.

In 2017, Liu and Chang [13] innovatively extended the image morphing-based authentication protocol to a "one-card-pass" scenario with high practical use. Under this scenario, an organization contains various kinds of departments providing diverse services. An authorized user can register at any department to acquire a smart card storing a generated morphed image. After that, the user can utilize this smart card to obtain services from different departments without registering again if the user passes the authentication such that the face image of the user is identical to that restored by de-morphing the morphed image and another face image maintained on the cloud storage servers. Nevertheless, most of the morphed images generated in authentication protocols look unnatural, which is prone to arouse suspicion among malicious attackers. Therefore, the research of optimization algorithms [14] on the selection of control points to achieve better visual effect of morphed images becomes a very challenging task.

Nowadays, the quick response (QR) code [11, 12] plays a very important role in information storage and identification in our daily lives. The QR code has many fascinating features [11, 12, 19], such as small printout size, high storage capacity and error correction ability. Since the QR code is very easy to be decoded by any standard QR code reader, it also has gained extensive popularity in real-time applications. Due to these advantages, the QR code is very suitable for storing the user's personal information to verify the identity of the user. In 2018, Huang *et al.* [5] applied the aesthetic QR code and the single-key-lock mechanism to a smart-building access control system. The single-key-lock mechanism produces keys for users and locks for doors. After encryption and fusion procedures, the keys are used to generate aesthetic QR codes as the user's credential. This access control system has the attributes of high security and robustness. Different from Huang *et al.*'s access control system, we consider the application of QR code from another aspect. The application scenario of our user authentication protocol is similar to that of Liu and Chang's morphing-based "one-card-pass" method, but ours offers "one-code-pass" functionality via the combination of QR code and secret sharing. That is to say, an authorized user can successfully use only one QR code to access various services from all departments within an organization. Suppose that there is a secret provided by the server of the organization in the proposed protocol. The secret is divided into many shares in the form of beautified QR codes and each department holds its own share beforehand. During the

registration, a user can register at any department and acquire his/her share from the department. When the user wants to access services of any of the departments, the original secret must be restored by the cooperation of both the department's share and the user's share; knowing only one share is unable to derive any valuable information about the secret. If the restored secret is not correct, the user is illegal. Experimental results demonstrate that the proposed protocol is secure against various attacks and the generated beautified QR code has high robustness.

The rest of the paper is organized as follows. In Section 2, we first introduce elementary knowledge of QR code and secret sharing, and then, review related works [13] and [5]. In Section 3, a novel "one-code-pass" user authentication protocol based on QR code and secret sharing is proposed. Section 4 demonstrates the experimental results of the proposed protocol and Section 5 gives the security and performance analyses. Finally, our conclusions are presented in Section 6.

2 Preliminaries

In this section, we first introduce main building blocks of a new user authentication protocol that will be proposed in the next section. After that, we provide a brief review of the morphing-based "one-card-pass" authentication protocol [13] and the QR code-based access control system [5].

2.1 QR Code

The QR code, invented by the Japanese Denso-Wave Company in 1994 [4], is a two-dimensional graphical code that consists of black and white square modules representing bit information. As illustrated in Figure 1, the structure of a standard QR contains message region, padding region and error correction region, together with version information, format information, position detecting patterns, alignment patterns and timing patterns.

The QR code is extensively used in information storage and identification applications due to its advantages on small printout size, high storage capacity and error correction ability [11, 12, 19]. As many as 40 QR code versions are used to determine different storage capacities such that the QR code with a higher version number can provide larger data payload. As another extraordinary feature of the QR code, the error correction capability with four error correction levels (*i.e.* L, M, Q and H) ensures successful decodability when portions of the QR code are dirty or damaged.

One of the most important processes for generating a QR code is to encode information using Reed-Solomon (RS) code. A t -bit RS code, shown in Figure 2, is composed of three segments, *i.e.*, l message bits, m padding bits and n parity bits. The to-be-embedded message is first decoded into a l -bit binary stream, followed by m

padding bits. Then, n parity bits are created for detecting and correcting errors when scanning the QR code. Figure 1 demonstrates how to place an RS code into a 2D QR code. Especially, each message/padding/parity bit is located onto one module of the message/padding/error correction region.

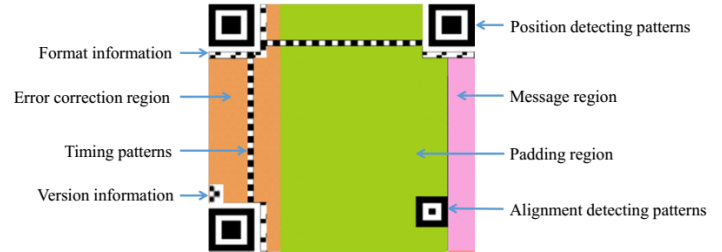


Figure 1: The structure of a QR code

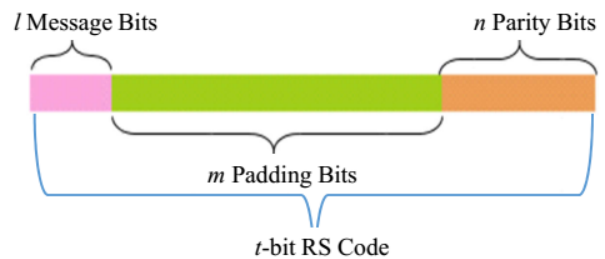


Figure 2: RS code

2.2 Shamir's Threshold Secret Sharing

The concept of secret sharing, independently introduced by Shamir [17] and Blakley [3] in 1979, is an efficient mechanism for data protection. The popularity of Shamir's threshold secret sharing (TSS) has noticeably increased due to its high efficiency and security. In a (t, r) TSS scheme ($t \leq r$), a secret is divided into r shares to be held by r participants. The secret can be simply recovered by the collaboration of at least t shares; otherwise, if fewer than t shares are collected, the original secret cannot be retrieved correctly.

Assume that there is a dealer and r participants, and the secret is denoted as s . The (t, r) TSS scheme contains the share establishment phase and the secret recovery phase, which are described as follows.

2.2.1 Share Establishment Phase

The dealer randomly selects a Lagrange interpolating polynomial g with degree $t-1$ such that $g(x) = s + a_1x + a_2x^2 + \dots + a_{t-1}x^{t-1} \pmod p$, where p is a prime number, and a_1, a_2, \dots, a_{t-1} and s are in the finite field $GF(p)$. Then, the dealer chooses r random numbers x_d for $d = 1, 2, \dots, r$ to establish r shares $s_d = g(x_d)$ for $d = 1, 2, \dots, r$, and provides each participant with a share.

2.2.2 Secret Recovery Phase

The t participants can cooperate to recover the secret s by releasing their shares. Suppose the t out of r shares are denoted as $s_{bh} \in \{s_1, s_2, \dots, s_r\}$ for $h = 1, 2, \dots, t$. According to the principle of the Lagrange interpolating polynomial, $g(x)$ can be recovered by $g(x) = \sum_{h=1}^t s_{bh} \prod_{k=1, k \neq h}^t \frac{x-x_{bk}}{x_{bk}-x_{bh}} \pmod p$. Thus, the secret s can be immediately obtained by $s = g(0)$.

2.3 Related Works

2.3.1 Morphing-Based “One-Card-Pass” Authentication Protocol

Assume that an organization includes many independent departments. For instance, a university may contain a library, a digital information center, a fitness center, a student association, *etc.* We hope that the “one-card-pass” functionality could be provided in such a way that a faculty member or a student could use only one smart card to gain various services from all of the departments. Accordingly, the objective of the “one-card-pass” user authentication protocol is to verify the identity of the card user in each department after the user registers at any of the departments.

Recently, Liu and Chang [13] proposed the first “one-card-pass” user authentication protocol using image morphing technology. This protocol contains three entities, *i.e.*, a card user, a terminal within a department, and cloud storage servers, and it consists of the registration phase and the authentication phase.

In the registration phase, a legal user U can register at any terminal T within any department. The following steps are conducted to fulfill the registration.

Step 1. The user U sends a registration request including his/her identity number to a terminal T .

Step 2. T takes a digital photo of U . This photo, denoted as OI , is used as the original face image of U .

Step 3. T selects a face image SI stored in the cloud storage servers C according to U 's identity number and then C sends SI to T .

Step 4. T generates a morphed image MI using OI as the source image and SI as the target image by a specific morphing algorithm.

Step 5. T stores the information that will be used in the authentication phase in a smart card and prints the morphed image MI on the smart card. Then, T delivers the smart card to U .

Later, in the authentication phase, a terminal T of a department recovers the face image of the true card owner via image de-morphing to verify the validity of the card user U . If the face image of U matches the recovered face image, U passes the authentication and can gain the

service provided by this department. The detailed steps in this phase are listed below.

Step 1. User U presents the smart card to a terminal T .

Step 2. T scans the morphed image MI printed on the smart card and extracts the information for authentication from the smart card.

Step 3. T finds the face image SI stored in the cloud storage servers C according to the extracted information.

Step 4. C sends SI to T .

Step 5. T recovers the face image of the true card owner, OI , by de-morphing images MI and SI .

Step 6. T compares the face image of the user U with OI to see if they are identical. If it holds, U is legal.

This protocol is very practical since it implements the “one-card-pass” functionality. The strategy that the real image of the true card owner is not stored anywhere but hidden in a morphed image increases the security to a certain extent. However, the protocol requires an additional set of cloud storage servers that preserve large numbers of face images for the morphing operation, which may lead to potential security problems. Furthermore, since the procedures of printing and scanning may cause noises, the authentication result may not be correct due to the distortions generated to the recovered face image. To solve these problems, in this paper, we will combine QR code and secret sharing to design a new “one-code-pass” user authentication protocol in Section 3.

2.3.2 QR Code-Based Access Control System

Huang *et al.* [5] presented a novel access control system for smart building based on QR code. The enrollment procedure of this system consists of three steps, *i.e.* the keys and locks generation, key encryption, and the QR code beautification, as listed below:

Step 1. Keys and locks generation. The single-key-lock mechanism is used to generate keys for users and locks for doors on a randomly non-singular matrix.

Step 2. Key encryption. Each key is encrypted by a symmetrickey cryptography algorithm to prevent the leak of key. Then, a QR code generated by the encrypted keys is sent to the user.

Step 3. QR code beautification. The owner of original QR code produced by Step 2 cannot be distinguished by human eyes for a number of confused black and white modules. This would induce difficulties in the management of QR codes when the number of users (keys) grows sharply. Therefore, these QR code need to be beautified to show the user's photo on its own. The beautification process includes:

- a) Construct the basis vector matrix.
- b) Generate an XORed QR code by perform the XOR operation between the Reed-Solomon message of the QR code and the basis vector matrix. In the XORed QR code, most modules in the padding region are modified and middle modules are kept clear to make the preparation of embedding the user's photo.
- c) Synthesize an aesthetic QR code from the user's photo and the XORed QR code as the user's credential.

When a user presents the aesthetic QR code to request the access to a door, the reader on the door would decrypt and retrieve the user's key from the aesthetic QR code, and then, verifies the access right via conducting an operation on the key and the lock.

3 The Proposed Protocol

In this section, we propose a novel "one-code-pass" user authentication protocol. The proposed protocol contains the initialization phase, the registration phase and the authentication phase. In the following, we first point out the contribution of the proposed protocol, then address its main idea, and finally elaborate on each phase.

3.1 Contribution

The contribution of the proposed protocol is described as follows:

- 1) It is the first user authentication protocol that can fully accomplish the goal of "one-code-pass" in a specified organization. More specifically, a user is able to make registration on any department to gain his/her own beautified QR code. By using the QR code, the user is immediately authenticated and directly accesses diverse services from all departments in this organization.
- 2) The QR code technique is combined with secret sharing mechanism to implement the proposed protocol. A secret is divided into a number of shares that are held among different departments and authorized users. The share actually is a beautified QR code containing some authentication information. Each department gains its share in advance and each user obtains his/her share from the department on which the registration operation for the user is conducted. To verify the identity of the user, the original secret should be recovered by the cooperation of both the department's share and the user's share. If the restored secret is correct, the user is eligible to get services from all departments.
- 3) The proposed protocol is significantly secure. Based on the secret sharing mechanism, both shares on the

user and department sides must be collected to recover the original secret; Just one share is impossible to leak the secret. In addition to this, the proposed protocol is secure against various attacks, such as the impersonation attack, the collusion attack, the replay attack, *etc.* It can also achieve high robustness as it is tolerant of various quality degradation situations.

3.2 Main Idea

To authenticate the identity of a user, a $(2, M + N)$ TSS is exploited in the proposed protocol for an organization containing M users and N departments. At first, some initialization work should be done. The server of the organization selects a secret s and generates N shares such that each share is held by a corresponding department. Then, for each user, he/she can register at any department and acquire his/her own share from the department with the help of the server. It is noted that each share of a department/user is a beautified QR code that not only encodes authentication information, but also embeds a logo/photo of the department/user in its padding region for efficient management of QR codes. When a user wants to access services of any of the departments, the user is authenticated by recovering the original secret s through the cooperation of both the department's share and the user's share. The photo of the authorized user on the beautified QR code also provides an auxiliary way for user authentication. Figure 3 shows the architecture of the proposed protocol, in which a user first registers at the department 1, and then is authenticated by the departments 1 and 2, respectively.

Before addressing the detailed protocol, some notations used in the paper are described in Table 1.

Table 1: Notation description

| Notation | Description |
|-------------------------|---|
| S | The server |
| $U_i (1 \leq i \leq M)$ | The user i |
| ID_{U_i} | The identity number of U_i |
| Q_{U_i} | The beautified QR code for U_i |
| $D_j (1 \leq j \leq N)$ | The department j |
| ID_{D_j} | The identity number of D_j |
| Q_{D_j} | The beautified QR code for D_j |
| s | The secret provided by S |
| K | The secret key shared among all departments |
| $g(\cdot)$ | The Lagrange interpolating polynomial |
| $h(\cdot)$ | A collision-free one-way hash function |
| \parallel | The string concatenation operation |

3.3 The Initialization Phase

This phase allows the server to generate a share in the form of a beautified QR code for each department. As-

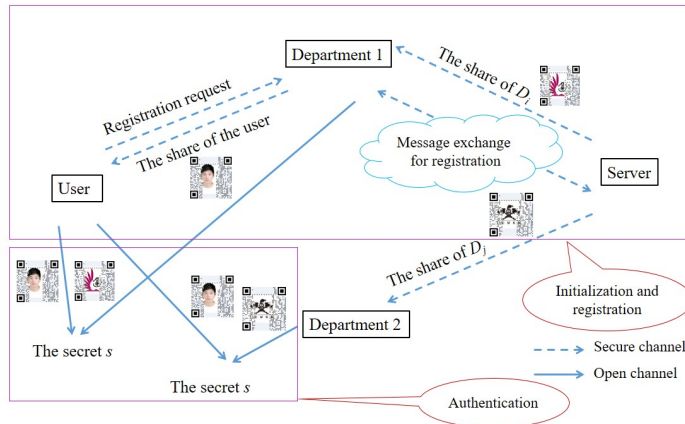


Figure 3: Architecture of the proposed protocol

assume that all of the N departments within the organization share a secret key K . Firstly, the department D_j computes $x_{D_j} = h(ID_{D_j} \parallel K)$ and sends it to the server S . Then, S selects a secret s , a number a_1 and a prime number p to generate a one-degree-polynomial function g as

$$g(x) = s + a_1x \pmod{p}. \quad (1)$$

For each department, S computes $y_{D_j} = g(x_{D_j}) = s + a_1x_{D_j} \pmod{p}$. Finally, S creates a beautified QR code Q_{D_j} for the department D_j as the share of D_j by using the information (x_{D_j}, y_{D_j}) and D_j 's logo.

Here, we briefly explain how the beautified QR code for a department is generated. The information (x_{D_j}, y_{D_j}) is first placed into modules of the message region to produce a QR code. Then, a beautification algorithm on the QR code is made for efficient management. There are many available beautification algorithms and we use the one presented in [10]. In this algorithm, the modules in the padding region of the QR code is first modified to keep "clean" with the help of a basis vector matrix, and then, the department's logo is embedded into the padding region by a synthetic strategy. Interested readers can refer to [10] for a better understanding.

3.4 The Registration Phase

In this phase, a user can register at any department and acquire his/her own share, also in the form of a beautified QR code. This phase is described in detail as follows and demonstrated in Figure 4.

Step 1. The user U_i sends his/her identity number ID_{U_i} to the department D_j .

Step 2. D_j computes $x_{U_i} = h(ID_{U_i} \parallel K)$ and sends x_{U_i} to the server S .

Step 3. S computes $y_{U_i} = g(x_{U_i}) = s + a_1x_{U_i} \pmod{p}$ by Equation (1).

Step 4. S generates a beautified QR code Q_{U_i} for the user U_i as the share of U_i by using the information (x_{U_i}, y_{U_i}) and U_i 's photo. The method of generating the beautified QR code for the user is the same as that for the department as mentioned in the initialization phase.

Step 5. S sends Q_{U_i} to D_j .

Step 6. D_j sends Q_{U_i} to U_i .

3.5 The Authentication Phase

The authentication is conducted by an authentication device within a department which is equipped with a QR code reader and has a copy of the secret s . The authentication device verifies the identity of the user by recovering the original secret s through the collaboration of the user's QR code and the department's QR code. If the user passes the authentication, he/she can gain services provided by this department. The steps of this phase are addressed as follows and illustrated in Figure 5.

Step 1. The user U_i shows the beautified QR code Q_{U_i} to the authentication device.

Step 2. The authentication device scans the QR code Q_{U_i} of U_i and extracts (x_{U_i}, y_{U_i}) .

Step 3. The authentication device scans the QR code Q_{D_j} of the department D_j where it is located and retrieves (x_{D_j}, y_{D_j}) .

Step 4. The authentication device uses (x_{U_i}, y_{U_i}) and (x_{D_j}, y_{D_j}) as two shares to restore a secret s' . If $s' \neq s$, the authentication device terminates the phase and the authentication fails; otherwise, it executes Step 5.

Step 5. The authentication device computes $x'_{U_i} = h(ID_{U_i} \parallel K)$ and then checks whether x'_{U_i} equals x_{U_i} . If it holds, the authentication device confirms

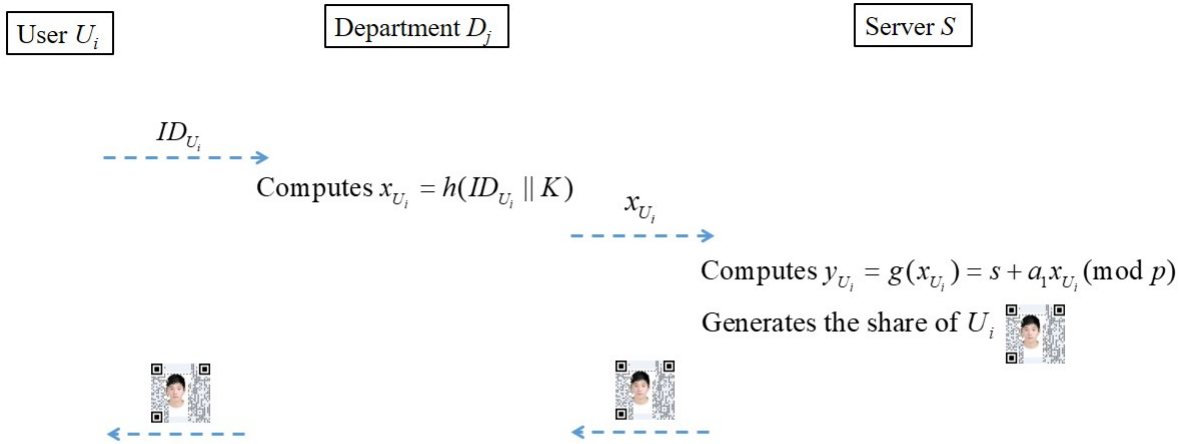


Figure 4: The registration phase of the proposed protocol

that the user is legal; otherwise, the phase is terminated and the authentication fails.

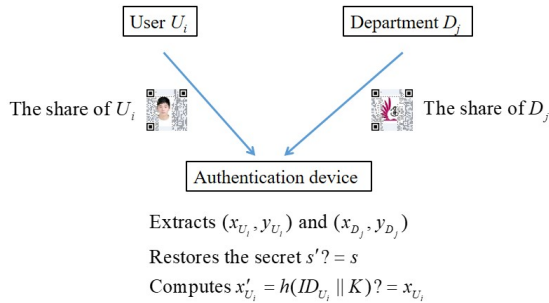


Figure 5: The authentication phase of the proposed protocol

In the authentication phase, it is worth noticing that if the restored secret s' is different from the original secret s by Step 4, the user is definitely illegal. However, if s' is equal to s , it cannot confirm that the user is legal. This is because if an attacker impersonates a user to embed fake values of x''_{U_i} and y''_{U_i} that satisfy $y''_{U_i} = g(x''_{U_i}) = s + a_1 x''_{U_i} \pmod p$ into the QR code, the correct secret s can still be obtained by the two points (x_{D_j}, y_{D_j}) and (x''_{U_i}, y''_{U_i}) on the function g . Therefore, Step 5 is added to check whether x''_{U_i} equals $h(ID_{U_i} || K)$ when $s' = s$ to ensure that x''_{U_i} is real.

4 Experimental Results

To evaluate the performance of our proposed protocol, our experiments were implemented by the open source computer vision library OpenCV and C++ program language. In this section, three users and two departments

are involved into a concrete example to illustrate the experimental results. In the following example, we select $s = 1024, a_1 = 21, p = 1237$ and $K = "@MSNLAB"$. Thus, the function g generated by the server S for the initialization becomes $g(x) = 1024 + 21x \pmod{1237}$. The beautified QR code Q_{D_j} for each of the two departments is generated in the initialization phase and shown in Table 2, where the department's logo, the identity number ID_{D_j} and the information (x_{D_j}, y_{D_j}) used for the generation of Q_{D_j} are also provided. After the registration on the department D_1 or D_2 , each of the three users obtains a beautified QR code Q_{U_i} by using the user's photo, the identity number ID_{U_i} and the information (x_{U_i}, y_{U_i}) , as shown in Table 3. In addition, the departments' logos in Table 2 are provided by Feng Chia University and the users' photos in Table 3 come from the Yale Face Database [2].





Here, we only take the user authentication process performed by the department D_1 as an example. Now let us demonstrate how the department D_1 verifies the identity of the user U_1 in the proposed protocol. Firstly, the authentication device in D_1 scans D_1 's beautified QR code Q_{D_1} (See in Table 2) and U_1 's beautified QR code Q_{U_1} (See in Table 3), respectively. Secondly, the information (x_{D_1}, y_{D_1}) and (x_{U_1}, y_{U_1}) are extracted from Q_{D_1} and Q_{U_1} , respectively, and then used as two shares to reconstruct a function g' as

$$g'(x) = y_{U_1} \frac{x - x_{D_1}}{x_{U_1} - x_{D_1}} + y_{D_1} \frac{x - x_{U_1}}{x_{D_1} - x_{U_1}} \pmod{1237} = 1024 + 21x \pmod{1237}.$$

Then, a secret s' is derived by $s' = g'(0) = 1024$, which is equal to the original secret s . Finally, we compute $x'_{U_1} = h(ID_{U_1} || K)$ and find that x'_{U_1} equals x_{U_1} . This indicates that the user U_1 passes the authentication.

In the following, we also show how the department D_1 detects an illegal user Bob by the proposed protocol. Assume that Bob uses $x_B =$

Table 2: The beautified QR codes for the departments

| | Department D_1 | Department D_2 |
|-------------------------------------|---|---|
| Logo |  |  |
| ID_{D_j} | http://lib.fcu.edu.tw | http://www.sa.fcu.edu.tw |
| $x_{D_j} = h(ID_{D_j} \parallel K)$ | dc1cf84361a4986424325645bef5be802344dc55 | 742b34c092beb4ea998a104509635fe32c394f3 |
| $y_{D_j} = g(x_{D_j})$ | 607 | 107 |
| Q_{D_j} |  |  |

6ed3693a3ef2fa0421cd0d1bd36750691522ce29, $y_B = 671$ and his photo to forge his QR code Q_B and then shows Q_B to the authentication device. The authentication device uses (x_B, y_B) extracted from Q_B and (x_{D_1}, y_{D_1}) derived from Q_{D_1} to reconstruct a function g'' as

$$g''(x) = y_B \frac{x-x_{D_1}}{x_B-x_{D_1}} + y_{D_1} \frac{x-x_B}{x_{D_1}-x_B} \pmod{1237} = 287 + 16x \pmod{1237}.$$

Obviously, a secret s' is derived by $s' = g''(0) = 287 \neq 1024$, which implies that Bob is an illegal user.

5 Analyses

In this section, we give the security and performance analyses of the proposed protocol, respectively.

5.1 Security Analysis

The proposed protocol can efficiently protect the user's privacy and resist various typical attacks, such as the impersonation attack, the collusion attack and the replay attack. The detailed security analysis from the theoretical aspect is given as follows.

5.1.1 Privacy Protection

One property of the QR code is that the information embedded in the message region of the QR code can be decoded and extracted by any QR code reader. As a result, a malicious attacker must be prevented from retrieving any personal knowledge about the user from the extracted information. To achieve this goal, the user U_i 's identity number ID_{U_i} is not embedded directly into the

QR code, but first encrypted by a one-way hash function as $x_{U_i} = h(ID_{U_i} \parallel K)$, and then, the encrypted message x_{U_i} and the corresponding value y_{U_i} computed via x_{U_i} by Equation (1) are used to generate the user U_i 's QR code Q_{U_i} . When a malicious attacker scans the QR code Q_{U_i} through a QR code reader, he/she only gets the messages x_{U_i} and y_{U_i} but has no idea of the user's identity number ID_{U_i} . By this way, the user's personal information will not be disclosed so that privacy protection is achieved. Besides, it doesn't matter that the photo embedded on the QR code reveals the appearance of the user since it is useless for the user authentication.







5.1.2 Withstanding Impersonation Attack

According to the proposed protocol, the impersonation attack refers to an attack that a malicious intruder forges a QR code and then impersonates a user with the intention of passing the authentication. To launch this kind of attack, the intruder must produce fake values of x_{U_i} and y_{U_i} and use them to forge the QR code. There is a strong possibility that the fake x_{U_i} and y_{U_i} do not satisfy the equation $y_{U_i} = g(x_{U_i}) = s + a_1x_{U_i} \pmod{p}$, thus the secret s restored by the cooperation of the two shares (x_{U_i}, y_{U_i}) and (x_{D_j}, y_{D_j}) is different from the original secret s . This implies that the impersonation attack is successfully detected in this situation. However, there also exists a situation that the intruder knows the function $g(x) = s + a_1x \pmod{p}$ and produces fake x_{U_i} and y_{U_i} satisfying the function g such that the correct secret s can still be obtained. Since under this case the value of s cannot determine whether the user is legal, the proposed protocol will further compute $x'_{U_i} = h(ID_{U_i} \parallel K)$. The value x_{U_i} created by the intruder will not equal x'_{U_i} because the intruder does not know the value of K , which indicates that x_{U_i} is fake and the impersonation attack fails.

5.1.3 Withstanding Collusion Attack

The proposed protocol must be collusion-resistant. The collusion attack in the proposed protocol means that, if multiple authorized users collude, they can obtain important information and use it to help an attacker to pass the authentication. Since it is sufficient for any two shares working together to restore the secret s , two authorized users can release their shares and collude to recover the function $g(x) = s + a_1x \pmod{p}$. The two users may share the function g with an attacker who attempts to impersonate a legal user. The attacker can create the values of x_{U_i} and y_{U_i} satisfying the function g and the correct secret s can be obtained in the authentication phase. Nevertheless, the attacker cannot pass the authentication since the created value x_{U_i} will not equal x'_{U_i} ($x'_{U_i} = h(ID_{U_i} \parallel K)$) as addressed in Subsection 5.1.2. Therefore, the collusion attack cannot be launched successfully.

Table 3: The beautified QR codes for the users

| | User U_1 | User U_2 | User U_3 |
|------------------------------|---|---|---|
| Photo |  |  |  |
| ID_{U_i} | WangJiaQing#M0557591 | ZhuZhaoHua#M0419274 | LiJing#P0361138 |
| $x_{U_i} = h(ID_{U_i} K)$ | a2e5bc07294a34caaffcc79 264e0f2aec912b37a | 3cf5b5fffb9153545bd8bbf1 f0edb154ec2691fc1 | 53132e6ffe935538492e213f 9c232d308c9c0488 |
| $y_{U_i} = g(x_{U_i})$ | 788 | 709 | 565 |
| Photo |  |  |  |

5.1.4 Withstanding Replay Attack

In a replay attack, a valid data transmission is repeated or delayed by a malicious attacker without detection. The proposed scheme can withstand such attack by the following way. An attacker can steal or duplicate a valid QR code and tries to use it to pass the authentication. One method to prevent it happening is that we can periodically change the value of the secret key K and accordingly update the QR codes for the users and departments based on the function g . Therefore, the QR code held by the attacker always expires since the attacker can never get the latest version of the user's QR code.

5.2 Performance Analysis

To evaluate the performance of the proposed protocol, we analyze the decoding rate and robustness of the QR codes for users and departments in this subsection.

5.2.1 Decoding Rate of Beautified QR Codes

To evaluate the decoding rate of the beautified QR code, we conduct experiments on both Apple's iOS and Google's Android mobile operation system. As shown in Table 4, several applications from Apple APP store and Google Play APP store were installed on two different mobile phones (iPhone 7, XiaoMi 4) and twenty beautified QR codes synthesized from users' authentication information with their photos were used to test the decoding rate of beautified QR codes. All these 20 users' photos are from Yale face database [2] and AT&T Cambridge face database [1]. From Table 4, we can see that all the APPs in these two selected phones can successfully decode the beautified QR code messages at the decoding rate of 100%.

5.2.2 Robustness of the Proposed Protocol

In the application scenario, when the beautified QR code was printed in the plastic card to be an ID card or scanned by a camera in the absence of adequate lighting condition, it usually suffers from several image degradation factors, such as pixel distortion, geometric distortion, noise, blur, and so on. These factors can be considered as a kind of image attack. Sometimes the quality of the QR code image being attacked has degraded significantly. Figure 6(a) shows the result of the beautified QR code Q_{U_i} of user U_1 in Table 3 suffering from the print-and-scan attack. The beautified QR code was printed in 600dpi with the HP LaserJet 500 color M551 printer, and scanned by the 200dpi with HP LaserJet M2727nf scanner. Figure 6(b) shows the result of Q_{U_i} suffering from Gaussian blur with the parameter $\sigma = 5$. Figure 6(c) shows the result of Q_{U_i} suffering from Gaussian noise with parameters $M = 0, V = 0.05$.

The authentication information embedded in these attacked beautified QR codes could still be decoded by any standard QR code reader. It demonstrates that the beautified QR code is tolerant to common attacks and the one-code-pass user authentication protocol is practically usable in the real-world applications.

6 Conclusions

In this paper, we proposed a novel "one-code-pass" user authentication protocol based on QR code and secret sharing such that an authorized user can successfully use only one QR code to access various services from all departments within an organization. In the proposed protocol, a secret is divided into many shares in the form of QR codes held among different departments and users. Each user can register at any department and acquire his/her

Table 4: Decoding rate in different applications

| Mobile Phone | Applications (Developer) | Decoding Rate |
|---------------------------|---|---------------|
| iPhone 7 (iOS 10.3.2) | WoChaCha QR code (WoChaCha Information Technology) | 100% |
| | Quick scan (iHandy Inc.) | 100% |
| | Quick QR code reader & creator (Fellow Software) | 100% |
| | QR code kit (Sima Biswas) | 100% |
| | QuickMark (SimpleAct Inc.) | 100% |
| XiaoMi 4 (Android 7.0) | WoChaCha QR code (WoChaCha Information Technology) | 100% |
| | QR code extreme(FancyApp) | 100% |
| | QR code reader (Scan.me) | 100% |
| | Free QR code scanner (TWMobile) | 100% |
| | QuickMark (SimpleAct Inc.) | 100% |



Figure 6: Results of beautified QR code of user U_1 in Table 3 after image degradation processes. (a) After Print-and-Scan attack; (b) After adding the Gaussian blurring with $\sigma = 5$; (c) After adding the Gaussian noise with parameters $M = 0, V = 0.05$

share including authentication information from the department. When a user wants to access services of any of the departments, the user is authenticated by recovering the original secret through the cooperation of both the department's share and the user's share. Theoretical analyses and experimental simulations show that the proposed protocol can efficiently protect the user's privacy and resist various typical attacks, such as the impersonation attack, the collusion attack and the replay attack.

References

- [1] *At&t Face Database*, accessed 31 Oct. 2017. (<http://www.cl.cam.ac.uk/research/dtg/attarchive/facedatabase.html>)
- [2] *Yale Face Database*, accessed 31 Oct. 2017. (<http://cvc.yale.edu/projects/yalefaces/yalefaces.html>)
- [3] G. R. Blakley, "Safeguarding cryptographic keys," in *Proceedings of the National Computer Conference*, vol. 48, pp. 313–317, 1979.
- [4] Denso-Wave Inc. *QR code standardization*, accessed 31 Oct. 2017. (<http://www.qrcode.com/en/index.html>)
- [5] P. C. Huang, C. C. Chang, Y. H. Li, and Y. Liu, "Efficient access control system based on aesthetic QR code," *Personal and Ubiquitous Computing*, vol. 22, no. 1, pp. 81–91, 2018.
- [6] Q. Jiang, J. Ma, G. Li, and X. Li, "Improvement of robust smart-card-based password authentication scheme," *International Journal of Communication Systems*, vol. 28, no. 2, pp. 383–393, 2015.
- [7] S. Kumari, S. A. Chaudhry, F. Wu, X. Li, M. S. Farash, and M. K. Khan, "An improved smart card based authentication scheme for session initiation protocol," *Peer-to-Peer Networking and Applications*, vol. 10, no. 1, pp. 92–105, 2017.
- [8] L. Lamport, "Password authentication with insecure communication," *Communications of the ACM*, vol. 24, no. 11, pp. 770–772, 1981.
- [9] C. T. Li, "A new password authentication and user anonymity scheme based on elliptic curve cryptography and smart card," *IET Information Security*, vol. 7, no. 1, pp. 3–10, 2013.
- [10] L. Li, J. Qiu, J. Lu, and C. C. Chang, "An aesthetic QR code solution based on error correction mechanism," *Journal of Systems and Software*, vol. 116, pp. 85–94, 2016.
- [11] P. Y. Lin, "Distributed secret sharing approach with cheater prevention based on QR code," *IEEE Transactions on Industrial Informatics*, vol. 12, no. 1, pp. 384–392, 2016.
- [12] S. S. Lin, M. C. Hu, and T. Y. Lee, C. H. Lee, "Efficient QR code beautification with high quality visual content," *IEEE Transactions on Multimedia*, vol. 17, no. 9, pp. 1515–1524, 2015.
- [13] Y. Liu and C. C. Chang, "A one-card-pass user authentication scheme using image morphing," *Multimedia Tools and Applications*, vol. 76, no. 20, pp. 21247–21264, 2017.
- [14] Q. Mao, K. Bharanitharan, and C. C. Chang, "Edge directed automatic control point selection algorithm for image morphing," *IETE Technical Review*, vol. 30, no. 4, pp. 343–243, 2013.

- [15] Q. Mao, K. Bharanitharan, and C. C. Chang, "A proxy user authentication protocol using source-based image morphing," *The Computer Journal*, vol. 58, no. 7, pp. 1573–1584, 2014.
- [16] V. Odelu, A. K. Das, and A. Goswami, "A secure biometrics-based multi-server authentication protocol using smart cards," *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 9, pp. 1953–1966, 2015.
- [17] A. Shamir, "How to share a secret," *Communications of the ACM*, vol. 22, no. 11, pp. 612–613, 1979.
- [18] H. M. Sun, Y. H. Chen, and Y. H. Lin, "oPass: A user authentication protocol resistant to password stealing and password reuse attacks," *IEEE Transactions on Information Forensics and Security*, vol. 7, no. 2, pp. 651–663, 2012.
- [19] I. Tkachenko, W. Puech, C. Destruel, O. Strauss, J. M. Gaudin, and C. Guichard, "Two-level QR code for private message sharing and document authentication," *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 3, pp. 571–583, 2016.
- [20] J. Yu, G. Wang, Y. Mu, and W. Gao, "An efficient generic framework for three-factor authentication with provably secure instantiation," *IEEE Transactions on Information Forensics and Security*, vol. 9, no. 12, pp. 2302–2313, 2014.
- [21] L. Zhang, Y. Zhang, S. Tang, and H. Luo, "Privacy protection for e-health systems by means of dynamic authentication and three-factor key agreement," *IEEE Transactions on Industrial Electronics*, vol. 65, no. 3, pp. 2795–2805, 2018.
- [22] Q. Zhao and C. H. Hsieh, "Card user authentication based on generalized image morphing," in *2011 3rd*

International Conference on Awareness Science and Technology (iCAST'11), pp. 117–122, Sep. 2011.

Biography

Yanjun Liu received her Ph.D. degree in 2010, in School of Computer Science and Technology from University of Science and Technology of China (USTC), Hefei, China. She has been an assistant professor serving in Anhui University in China since 2010. She currently serves as a senior research fellow in Feng Chia University in Taiwan. Her specialties include E-Business security and electronic imaging techniques.

Chin-Chen Chang is a professor in Feng Chia University. He received the BS degree in Applied Mathematics in 1977 and the M.S. degree in Computer and Decision Sciences in 1979, both from the National Tsing Hua University, Taiwan. He received the Ph.D. degree in Computer Engineering in 1982 from the National Chiao Tung University, Taiwan. He is the author of more than 900 journal papers and has written 36 book chapters. His research interests include computer cryptography, data engineering, and image compression.

Peng-Cheng Huang is a lecturer at the Xiamen University of Technology. He received his BS degree from Xiamen University of Technology in 2007, the MS degree in Computer Architecture from the Fuzhou University in 2010. He is currently pursuing the Ph.D. degree from the Feng Chia University. His current research interests include multimedia security, image processing, and Internet of thing.