Secure Audio-CAPTCHA Authentication Method for Visually Impaired

Li Longhua

A Thesis Submitted in Partial Fulfillment of the Requirements for the Degree of

Master of Engineering in Computer Engineering

Prince of Songkla University

2014

Thesis Title Secure Audio-CAPTCHA Authentication Method for Visually Impaired

Author Mr. Li Longhua

Major Program Computer Engineering

Major Advisor:

……
(Asst. Prof. Dr. Suntorn Witosurapot)

Examining Committee:

……..……..……..……Chairperson
(Asst. Prof. Dr. Sangsuree Vasupongayya)

...……
(Asst. Prof. Dr. Suntorn Witosurapot)

...……
(Asst. Prof. Dr. Supachate Innet)

The Graduate School, Prince of Songkla University, has approved this thesis as partial fulfillment of the requirements for the Master of Engineering Degree in Computer Engineering.

.....……..……
(Assoc. Prof. Dr. Teerapol Srichana)
Dean of Graduate School

This is to certify that the work here submitted is the result of the candidate's own investigations. Due acknowledgement has been made of any assistance received.

……

(Asst. Prof. Dr. Suntorn Witosurapot)
Major Advisor

……..

(Mr. Li Longhua)
Candidate

I hereby certify that this work has not been accepted in substance for any other degree, and is not being currently submitted in candidature for any degree.

.....

(Mr. Li Longhua)
Candidate

Thesis Title Secure Audio-CAPTCHA Authentication Method for Visually Impaired

Author Mr. Li Longhua

Major Program Computer Engineering

Academic Year 2014

ABSTRACT

The most common approach for authenticating a computer user is done by means of username and password. However, when working on the mobile environment, this approach is clearly unsuitable for the visually impaired people and therefore needs to be enhanced so that it can be served in a more suitable manner. In this thesis, it is proposed that the One-Time Password (OTP) should be included in the password-based authentication for the visually impaired and worked in conjunction with audio-based CAPCHA playback and local Text-to-Speech (TTS) facility for preventing maliciously robotic attacks. It is in the sense that, after passing the validation process by a means of OTP, a human-verification process will be in action on some secret information that is encoded with the QR-code mechanism and is encrypted by RSA asymmetric cryptographic algorithm. Owing to the feature of twice encryption of information, we can prevent robotic attacking problem, and, at the same time, verify the mobile device being used through some device identity, e.g. IMEI number. The contribution of this thesis is then the design of authentication for the visually impaired on mobile, which is capable of preventing the anti-robotic attack problem in an efficient manner. In addition, we compare our proposed authentication method to the other related works and explain why it can achieve a higher level of security protection.

Key words: Authentication, OTP, QR-code, CAPTCHA, IMEI, TTS, RSA

CONTENTS

Page

LIST OF TABLES

Table Page

LIST OF FIGURES

Figure Page

CHAPTER 1

INTRODUCTION

1.1 Motivation

It becomes easy nowadays to connect any mobile device to computers by means of wireless links, either for the intent of sharing the information or gaining the access through the Internet. In those cases, it is usual that some authentication mechanism must be involved for verifying whether the users of mobile devices are authorized or not. To meet this requirement, the basic approach is often done by means of username and password verification as shown in Figure 1.1, due to its simplicity and popularity. Unfortunately, this password-based authentication approach is not directly applicable to the users who are visually impaired, and is also considered inadequacy on security [1, 2] if the fixed password is only required for authenticating users, especially in open network environments.

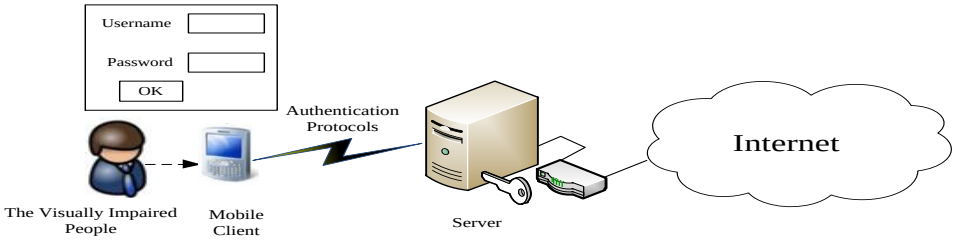


Figure 1.1 Typical password-based authentications for visually impaired people

A number of works have been attempted to alleviate the deficiency of fixed password in the recent years. However, only the works (such as [3-5]) that are related to the exploitation of One-Time Password (OTP) will be only interested. By enforcing different passwords to be used at each given time of authentication, the OTP-based solutions have been shown its effectiveness in handling various shortcomings found in the fixed password approach, such as Replay attack, Dictionary attack, and Phishing attack. Nevertheless, none of these studies have been solved for the issue of anti-robotic attack [5]. As a consequence, they are fail to deal with the interferences caused by some malicious programs that impersonate to be a human to fulfill the ongoing authentication process, e.g. sending some faked requests or responses periodically for degrading the server's performance. Therefore, it is interesting to investigate on how existing anti-robotic attack mechanisms can be included

to work in companion with the OTP-based solution for dynamic password authentication so that the facilitation for users with visually impairment on mobile devices can be realized.

However, in order to avoid complexity on OTP with anti-robotic attack mechanism under researched concern, user is expected to take part in the loop of operations by dialing whatever digits on the mobile device that are mandated from the authentication system. Therefore, any smart algorithm involved for detecting the anti-robotic attack (such as in [3]) is not needed, but can be replaced by somewhat less-complex security mechanism for generating digits and verifying them against the user inputs. By working in this manner, it seems that the audio-based CAPTCHA (Completely Automated Public Turing test to tell Computers and Humans Apart) mechanism [8] can be complement well to our research direction. Nevertheless, some other mechanisms for device authentication on mobile devices (e.g. International Mobile Equipment Identity number [6] and QR-Code [7]) will be also in consideration, since it will provide the arbitrary number of key lengths can be represented as a certain high degree of authentication approach.

In essence, a combined authentication method which is based on user and device authentication will be investigated for the visually impaired person on mobile phones, which can be capable of preventing the robotic attack problem in an efficient manner. Therefore a more secure, more practical and more useful authentication method can be made for the mobile users, who are the visually impaired during the access of computers through some mobile devices.

1.2 Objectives

1) To study the performance of security protection using encrypted codes obtained from some device authentication mechanisms.

2) To investigate the powerful combination of the OTP, the audio-based CAPTCHA mechanism, some selected device authentication methods and cryptographic algorithms for supporting the authentication process for the visually impaired through the mobile devices.

1.3 Scope of Work

1) The remote access of computers for the visually impaired through the mobile device is only considered in the research work.

2) The performance of security protection using encrypted codes obtained from some device authentication mechanisms such as the International

Mobile Equipment Identity and QR-Code algorithm will be carried out.

3) The combination of the OTP, audio-based CAPTCHA mechanism and some selected device authentication techniques will be investigated for enabling a suitable authentication technique for the visually impaired through the mobile devices.

1.4 Work Plan

1) To survey the literature related to the login authentication for the visually impaired and device authentication techniques on the mobile devices.

2) To investigate the performance of security protection using encrypted codes obtained from some device authentication mechanisms such as the International Mobile Equipment Identity and QR-Code algorithm.

3) To devise an anti-robotic mechanism working on the OTP and audio-based CAPTCHA mechanism and preferred device authentication techniques.

4) To submit the proposed papers to international conferences and write the final report.

1.5 Outline of the Thesis

This thesis is organized in 5 chapters as follow:

- Chapter 1 gives the motivation, objective and the scope of thesis. Then, the work plan for investigating the encrypted codes is given.
- Chapter 2 introduces the background of authentication techniques that will be investigated crucially in this thesis work. In addition, literature reviews on related work are provided in this chapter.
- Chapter 3 describes our proposed method that is aimed to devise an effective authentication protocol for people with visual disabilities, following with the comparison with the other works sharing the similar objective.
- Chapter 4 provides some practical experimental results and performance evaluation on some aspect of securing hidden information.
- Chapter 5 provides conclusion and discussion.

CHAPTER 2

BACKGROUND AND LITERATURE REVIEW

2.1 User Authentication Schemes for the visually impaired

User Authentication is a human verification process that uses one or more mechanisms to prove the identity of communicated users or being paired devices so that the privileged access of services or resources are granted afterward. It is, therefore, essential that the trust relationship under open network environments must be established through several forms of user identity. In this regard, two basic types of user authentication schemes [9] served for verifying ordinary people can be also applicable for the case of people with visual disabilities.

1) **User identity authentication** can be performed through various forms of user identity like: a) User preferences [10] (e.g. password, or personal identification (ID) number), b) User Identifications [11] (e.g. fingerprint, voice, or signature), and c) User personalization [12] e.g. security tokens and one-time password devices. It is noticed that only one or two forms will be chosen to work together in practice for verifying users (whether they are people with visual disabilities or not). The decision factors may be considered on the type and usage domain of certain application.
2) **User device authentication** can be validated through the validity of device identity which can be proved as secured device in order to ensure the access or require only come from the trusted devices.

   However, we argue that these two kinds of authentication must be used together, in order to obtain a higher degree of confidence. In this regard, not only legitimate users possess appropriate credentials, but also trusted devices, can be assured for legitimately accessing required resources or services. This is the particular case of supporting authentication for people of visual impairments that may need this facility for gaining the remote access (via mobile phones) of household devices or networked computers located within their smart homes.

2.2 Password-based Authentication Schemes

Authenticating users by simply verification of username and password inputted by the users is known as the password based authentication scheme. Besides its popularity, this authentication scheme may cause “Password vulnerabilities and threats [13]”

if weak passwords are attacked and resumed by illegal users or some malicious programs, who may seek for unauthorized accesses to a system. In response to common password threats, one possible solution is that encouraging users to use efficient passwords and change them on a regular basis. The other solution is to rely on dynamic passwords, such as One-Time Password (OTP), which are generated by some automatic mechanism, and are managed to send by some means to users so that they are enforced to use these passwords for the next authentication session.

2.2.1 One-Time Password

The One-Time Password (OTP) [14] is considered as one of the advanced techniques for the generation of dynamic passwords that can be set to valid once and only available within a short period of time. Therefore, when OTP works in conjunction to any password-based authentication schemes, OTP can prevent the vulnerabilities and threats according to the static password mentioned above well. Therefore, the OTP technique has been used widely in many e-business applications, especially for online transaction service or E-banking service by using trusted mobile devices.

The OTP is attractive to be implemented on mobile devices due to its low demand of power and memory requirements. However, the nature of OTP is still keeping on using the password style cannot protect the privacy of data when transmit. It is still incapable of preventing active attacks like the robotic attack. Although, it is claimed to be efficient for avoiding various shortcomings associated with traditional static password, such as Replay attack, Dictionary attack, and Phishing attack, these solutions are still incapable of anti-robotic-attack. As a result, when they are accommodated for the password-based authentication, those login processes can be then easily interfered by some malicious programs, e.g. sending some faked requests and responses periodically with the attempt to degrade the server's performance (hence, it is also known as the robotic attack problem).

2.2.2 Related Work

Liao et al. [15] described some incurred weaknesses, such as the risk of tampering and the high maintenance cost, when the password verification table was actively involved into the authentication process. With the adoption of OTP technique, these weaknesses was claimed to be resolved suitably. However, the encrypted form of QR-code is chosen to carry their new password codes, instead of sending in clear texts.

Jongpil et al. [16] studied an OTP-based user authentication scheme using smart cards for allowing only legitimate users to access home services. They showed the benefits of OTP technology for enhancing the security level in their authentication protocol by means of dynamic passwords, without a burden of high computation load in the system.

Zhu et al. [17] also studied an OTP-based identity authentication scheme for ensuring secure information, but in the mobile e-commerce domain. Two steps of authentication are performed their proposed scheme; the primary one verifies the legitimacy of user accessing the current mobile device, and the secondary one verifies the legitimacy of the mobile device with the server. This scheme represented a two-way authentication, and was claimed to overcome some weak points that occurred in similar other schemes (such as [14]).

In essence, these above-mentioned works can be seen as encouraging examples that give us a confidence on applying the OTP technology into our research work. Especially, the evidence from the last work that showed how the key weakness of OTP can be solved for preventing replay attacks and counterfeiting attacks.

2.3 QR-code based Authentication Schemes

2.3.1 Overview of QR-code

The QR-code (Quick Response-code) [7] is a kind of two-dimensional barcode, which is powerful not only for encrypting large number of information on small and limited district, but also capable of decrypting the encoded content at high speed. The content inside QR-code is encoded into binary format and represented as modules (square dots) in the QR-code tag. The dark module and white module mean a binary one and zero, respectively. Figure 2.1 depicts an instance of the QR-code symbol, which contains information in both vertical and horizontal directions, whereas a classical barcode has only one direction of data, as shown in Figure 2.2. Therefore, it has no doubt why QR-code can carry a higher capacity of data than the classical barcode. In Figure 2.3, the limitation of the message size in different message format is listed. In alphanumeric format, the maximum size of QR-code message can hold up to 4296 characters.

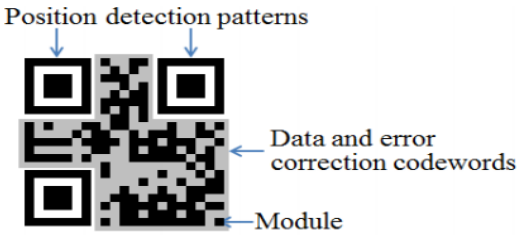


Figure 2.1 The QR-code module

Figure 2.2 Comparison of QR code with traditional bar code

Numeric	•7089 characters
Alphanumeric	•4296 characters
Binary (8 bits)	•2953 bytes
Kanji/Kana	•1817 characters
Chinese (Big-5)	•1800 characters
Chinese (UTF-8)	•984 characters

Figure 2.3 QR-code capacities [7]

In Figure 2.4, the general QR-code encoding and decoding diagram is shown. However, it does not necessary to rely on camera to capture the image of the QR-code, the direct feed of image file can be also applicable for the decoding program. The use of QR-code is free for any license, thus attracting many developers for the widespread uses in their applications.

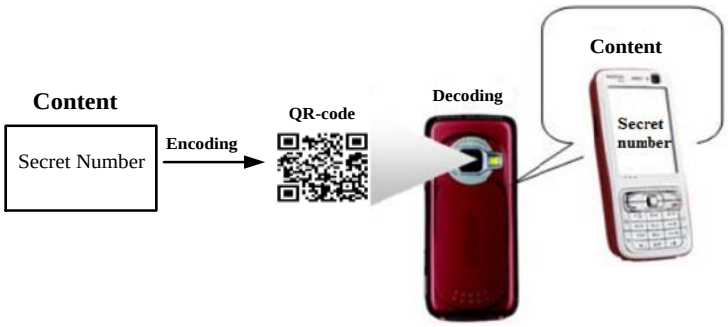


Figure 2.4 QR-Code encoding and decoding processes

2.3.2 QR-code Error Correction Functionality

QR-code supports error correction functionality in such a way that the higher rate of level are specified, the higher chance of error information can be restored, but on the expense of lower number of storage data. Figure 2.5 shows all possible choices of error correction levels that are allowed users to choose from. For instance, the level H mode, which is the highest error correction, allow up to 30% of errors or lost in the data codewords located inner-side of QR-code that can be restored successfully. Precisely, the restoration of data will be on those lost data that occurred in three different regions [18] and in the vertical or horizontal directions except the three finder patterns as depicted in Figure 2.6.

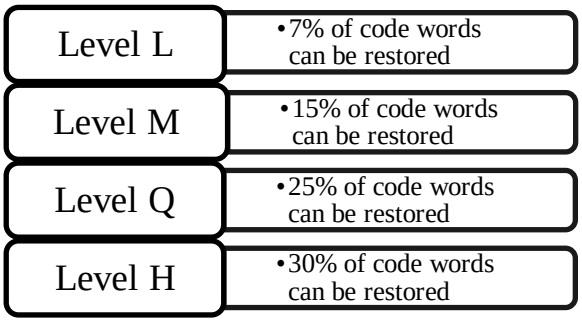


Figure 2.5 Error correction modes [7]

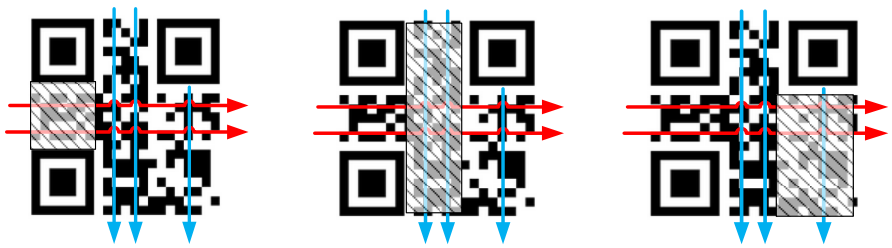


Figure 2.6 Three different regions of errors in vertical or horizontal directions

2.3.3 QR-code Techniques on Mobile Devices

The mobile phone as one of the mobile devices can be working as a secure hardware token and a new interface by its inbuilt-camera, not only due to its popularities in daily use and capabilities at reasonable prices, but also utilize a long serial numbers that is mobile's International Mobile Equipment Identity (IMEI) as secure proof of device identity. Figure 2.7 shows that a unique identity number is manufactured in mobile phone. Therefore with the help from IMEI numbers can greatly ensure the validity of accessing only derived

from some trusted devices. However, the compromise situation can be happened when the phone lost or stolen by some illegal users.

Figure 2.7 Unique IMEI number on mobile phone

As we know that the clear content of QR-code applications are encoding underlies the QR-code algorithm, then the image of cipher message will be exposed in the open network, so everyone can use QR-code reader application to obtain the original message without user's permission. Considering that without appearing clearly and directly over the air, through the way of hide the secret information via some encryption technologies can be efficient prevent the illegal user to intercepting and modifying the message during the transmission processing.

2.3.4 Related Work

The following works share the common objective of using QR-code or QR-code with some cryptographic algorithms to support the combined of user identity and user device authentication as that of our work.

Yang et al. [19] took the similar idea on Liao et al.'s work [20], but relied on the IMEI embedded in QR-code and managed the device authentication process on the authentication server. However, using IMEI alone is not safe for device authentication, especially when it is stolen by some illegal users. In the meantime, Won et al. [21] proposed a much more secure authentication scheme by equip with synchronized clocks between both parties in the network that repairs the security vulnerabilities in Liao et al.'s scheme.

In the works [22-25] are proposed secure user authentication with QR- code. They provide some new authentication method which can reduce the troubles come from phishing, man-in the-middle attack and eavesdropping attack.

In the study [26-29] are about RSA cryptographic algorithm and symmetric cryptosystem based on QR-code. We realized that with some encryption algorithms for enhance the security protection level can be prevent some potential attacks, but also can get

some problems as key length increase made the QR-code underlying encryption algorithm to be more complicated.

2.4 Audio-based Authentication Schemes

2.4.1 Overview

The CAPTCHA (Completely Automated Public Turing tests to tell Computers and Humans Apart) [8] is a simple mechanism which is often used to prevent automated "bot" from login procession or registry account. It seems to be applicable for identifying whether the being interact is a legitimate visually impaired human user or not. However, it is suitable in our usage scenario, where the user is visually impaired person and therefore, the audio version of CAPTCHA is preferred, shown in Figure 2.8.

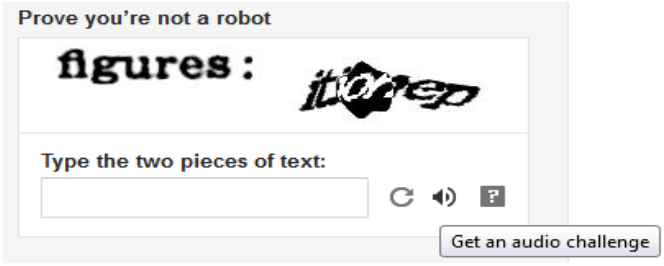
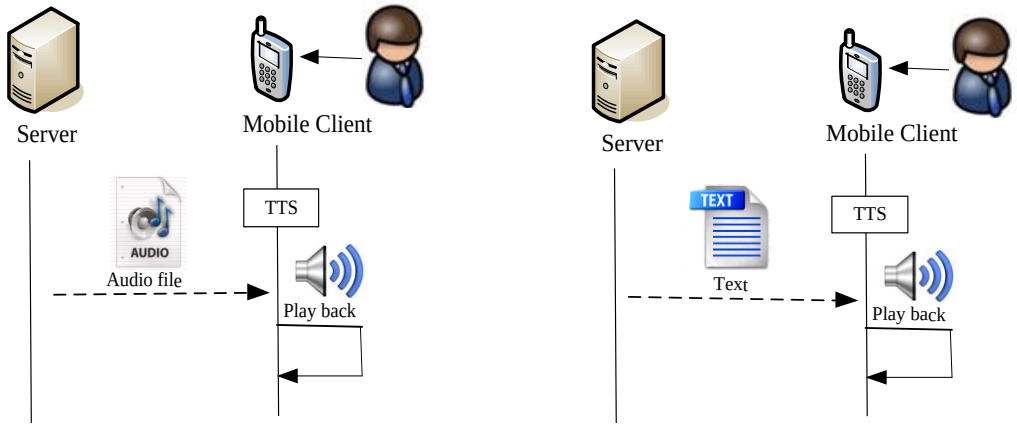


Figure 2.8 An example of audio-based CAPTCHA

In our scheme, through the local TTS engine inbuilt on mobile device for covert the successful decrypt of audio file or secret text into audio text are shown in Figure 2.9, by that way which required visually impaired user to listen and then to press the key number for obtain the given services or resources in order to guarantee human user is being interacted which can prevent anti-robotic attack from it.



(a) (b)

Figure 2.9 (a) Audio file and (b) Text is converted by inbuilt TTS engine on mobile

However, some weaknesses can be occurred when using audio file transmit over the air: (1) impossible to hide the secret information; (2) vulnerable to be attacked by fake audio; (3) resources consumption: e.g. long computing time; heavy workload; narrow bandwidth on CPU, RAM and data transmission. So ensure the safety of text in an encryption tunnel via some cryptographic algorithms should be realized.

2.4.2 Related Work

Hearing as one of the human senses is successfully applied in the authentication area. The three audio authentication techniques are proposed individually.

In [30-32], by use of audio channel for human-assisted authentication that is exchange both data and verification information among devices in order to provide human-verifiable secure.

Chang [33] applies hardware solution on a CAPTCHA image of OTP based smart card for guarantee human participation as a new way of authentication. Sound similar with Leung [34] utilized a moving CAPTCHA for input time restriction of OTP can be avoid attacking on information replying. In the sense that through the way of Audio version of CAPTCHA should be concern for guaranty the real human is being interaction in our scenario for the visually impaired, thereby can further depress robotic assisted attack which we called robotic attack.

2.5 Cryptographic Algorithms for the Mobile Phones

To ensure a secure communication over the public networks, especially on the mobile devices, the secret information or data can be protected by the approach of security cryptographic mechanisms on mobile phones for the visually impaired. The purpose of applying advanced cryptographic algorithms that are considering to the confidential information or data on security, identity and integrity for prevent unauthorized users from accessing and gaining the secret information or data in public networks. Cryptographic algorithms [35] can be categorized into two main groups: one is Public-key Cryptography (e.g. RSA); another one is Symmetric-key of Cryptography (e.g. AES) as shown in Figure 2.11.

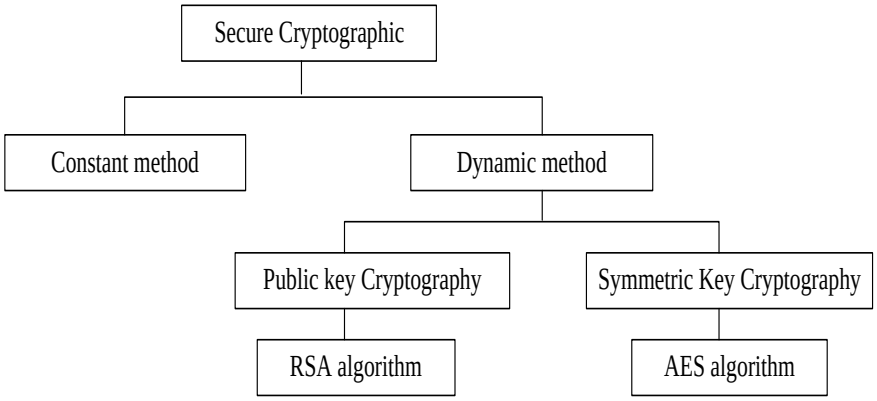


Figure 2.10 Classification of Cryptography

2.5.1 Asymmetric Cryptographic Algorithm

Asymmetric cryptographic algorithm (also called Public-key cryptography) is one of the Cryptographic algorithms which use a pair of two different keys for cryptography, e.g. the public and private keys [36]. Generally, one key is for encryption another one key is for decryption. So that unauthorized users cannot decrypt data by using public key because encrypted data can only be decrypted by theirs own private key. As shown in Figure 2.11, the public-key cryptography allows recipients and senders to use the secret key without previous agreement. In other words, the advantage of using public-key cryptography is to avoid the transmitting problem on session key.

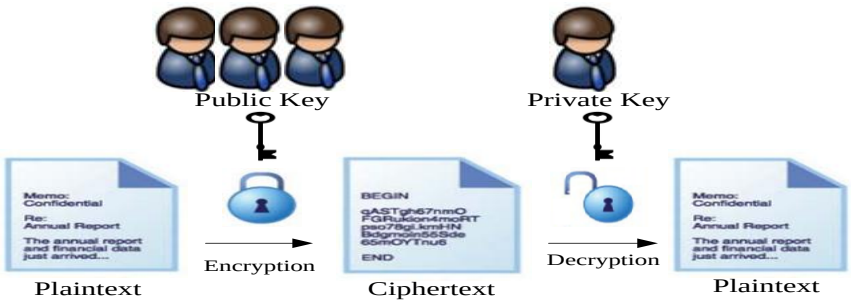


Figure 2.11 Process based on the public and the corresponding private key

Figure 2.11 shows the general procedure of public key cryptosystem. If the sender wants to deliver some information, by using public key cryptosystem, the receiver can publish his encoding key so that the sender can get it and then encodes the plaintext to cipher text. When the receiver gets the cipher text, he can use the corresponding decoding key to decode and get the original plain text.

If the third party try to grab the secret information, and we assume the third party got any what he can obtain as following [37] : (1) Stealing the encoding key when it is

delivered; (2) Obtaining the cipher text when it is transferred; (3) Public encoding algorithm using on this public encoding system.

Then the third party still cannot decode the cipher text even he got the encoding key and he can't derive the decoding key by encoding key. In other words, the third party cannot get the secret information even he has everything but decoding key. Nowadays, one of the most widespread used public key cryptosystem is RSA. We will introduce the RSA algorithm later and implement it into our system for hide and protect secret messages.

2.5.1.1 RSA Algorithm

RSA [27], as describing before, is one of the most well-known public key encryption algorithms. It was publicly described by Ron Rivest, Adi Shamir, and Leonard Adleman at MIT in 1978. RSA is widely trusted and used in electronic commerce protocols. In addition to the use of convenience, the most important reason is: RSA is based on complicated mathematical theory and is sufficient to protect the secure information of both transferor and receiver.

Now, the RSA public key cryptography for encryption and decryption process was introduced from following mathematical theory [27]:

1. Randomly select two distinct large prime p and q
2. Compute n = p * q
3. Choose encoding key e which is satisfied following condition GCD (e,φ(n))=1, φ is Eculer's Totient function, φ(n) is defined to be the number of positive integers less than or equal to n, we know that φ(n) = φ(pq) = (p-1)(q-1)
4. Derive decoding key d by computing d = e^(-1) mod φ(n)
5. Publish <e, n> as encryption key
6. The transferor can encode plaintext M to cipher text C by C = M^e (mod n)
7. The receiver can decode cipher text C to plaintext M by M = C^d (mod n).

As describing before, people can transfer the secret information by encoding with public key e, and the receiver can obtain the plaintext by decoding the cipher text from private key d.

2.5.1.2 Security of the RSA

RSA algorithm is based on mathematical functions rather than on substitution and permutation. Moreover, it is in the way of asymmetric, involve to using the two separate

keys. The use of two keys has profound consequences in the areas of confidentiality, key distribution, and authentication.

There are two wrong concepts on: 1. The asymmetric key encryption is more secure than conventional key encryption. 2. Replace of using key encryption by the asymmetric key encryption. Actually, the higher of security level depends on choosing the key length. Thereby, whether the symmetric or the asymmetric key encryption is more secure but still uncertain. Due to the overhead of computation on asymmetric key encryption schemes, so made symmetric key encryption still useful.

2.5.1.3 RSA Security Issue

If the third party wants to know the secret information and gets the cipher text so, should know n, e and d. In order to get decoding key d, he has to know the number of φ(n), in order to know φ(n), he has to factoring n to two prime p and q. Nowadays, there is no polynomial time algorithm to solve the problems of factoring a large number n into two prime number p and q, e.g. there is still no efficient algorithm to solve this problem of factoring large number. Therefore, the required time to factoring n is depends on the length of n if someone wants to factor it by brute-force method. Table 2.1 lists the relations of key length and break time.

Table 2.1 Relation between Key Length and Break Time [38]

Key length	Break time of 100 million 100MIPS,8MB Pentium
428	14.5 seconds
512	22 minutes
700	153 days
1024	280000 years

The following Table 2.2 shows the relationships of key length and the recommend key length on different standards.

Table 2.2 Recommended Key Length in each Level [38]

Year	Low standard	Average	High standard

		standard	
1995	405	579	1341
2000	425	619	1451
2005	447	661	1567
2010	469	705	1689
2015	493	751	1815
2020	515	799	1947

2.5.1.4 Key Selection Issue

Under certain conditions, RSA is also very fragile, so we must be carefully to avoid these issues. Actually, the weakness of RSA might happen if choosing e inappropriately; in some cases, inappropriate e might lead to M^e (mod n) = M. That is the ciphertext is equal to the plaintext so that the information need to be hidden is exposed. Besides, the public exponent for RSA must be sufficiently large. The values of public key such as 3 or 17 are no longer recommended, while the value like 65537 seems still safe [39]. Besides, there are lots of research works try to crack RSA. The Table 2.3 lists some problems under certain conditions [40].

Table 2.3 Current Known Attack Method on RSA [40]

Provenance	Weak Part	Condition	Result
Pollard	N	p-1 or q-1 is small enough	Derive p,q
Lehmanna	N	|p-q| is small enough	Derive p,q
Williams	N	p+1 or q+1 is small enough	Derive p,q
Knuth	N	p/q is a simple fraction	Derive p,q
λ（p-1）	N	p-1=ap', q-1=aq' and p'-1 or q'-1 is small enough	Derive p,q
Simmons-Norris	C (Ciphertext)	(1) p-1=ap', q-1=ap', and p'-1 or q'-1 is small enough (2) GCD(p-1,q-1) is big enough (3) The number of e mod (p-1)(q-1) is small enough	Derive M (plaintext)
Hastad	C (Ciphertext)	Encryption key, e , is small enough	Derive M (plaintext)
Wiener	e/N	(1) e < N (2) $d < \sqrt[4]{N}$	Derived d and p,q
		(1) e< N	

Chen	e/N	(2) $d < \sqrt[4]{N}$ or $(\lambda - d) < \sqrt[4]{N}$ or $\lvert \lambda/2 - d \rvert < \sqrt[4]{N}/2$ or $\lvert m\lambda/h - d \rvert < \sqrt[4]{N}/h$	Derived d and p,q

By Table 2.3, we found that if an inappropriate use of RSA will be a flaw in these attacks, particularly important is the choice of p and q so, the two values cannot be too small or too similar. In addition, the size of e and d are also important, because the majority of these attacks are originate from the too small of e or d.

2.5.2 Symmetric-key Cryptography

Symmetric cryptography (also called Private-key cryptography) is much more common than public-key cryptography which generally takes less time for key generation and less number of key (only a single key) for encryption and decryption algorithms [41]. Figure 2.12, shows the basic of method that the two members participate at one group must have the same key (secret key). Thus, both the sender and recipient can be able to obtain and know the cryptography information. The basic concept to transfer message must prior to reach an agreement and share the same secret key with the group of members through encryption and decryption process.

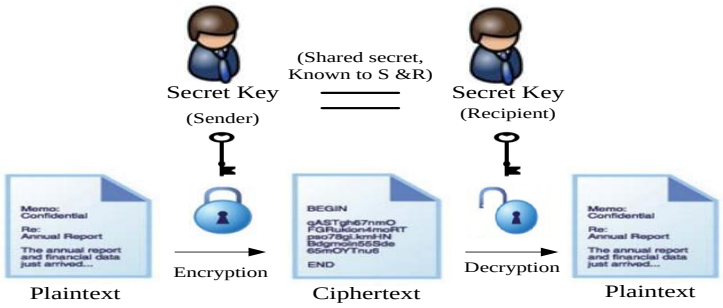


Figure 2.12 Cryptographic processing according to the private key (secret key)

2.5.2.1 Description of the AES

Advanced Encryption Standard (AES) [42] is a symmetric-key algorithm which keeps using the same key for encrypt and decrypt electronic data. Now, it is popular to be used in the all of the world.

AES can be fast used in software and hardware which based on design principle on substitution-permutation with a fixed block size of 128 bits and a key size of 128, 192, or 256 bits. Therefore with some rounds of repetition for convert the plaintext into ciphertext.

2.5.2.2 Security of the AES

Considering to the strength of key length on AES algorithm, e.g. 128, 192 and 256 key sizes can be affected by the security requirement. For the higher level of security protection so the higher key length should be selected. Table 2.4 lists that the longer key length will take a longer time to decrypt [42]

Table 2.4 Times for brute force attack on some symmetrical cryptography [42]

Key size (bits)	Number of alternative keys	Time required at 1 decryption/ μs	Time required at 10^6decryptions/ μs
32	2^{32} =4,3.10^9	2^{31} μs =35,8 min	2,15 ms
56	2^{56} =7,2.10^{16}	2^{55} μs = 1142 years	10 hours
128	2^{128} =3,4.10^{38}	2^{127} μs = 5,4.10^{24}years	5,4.10^{18} years
168	2^{168} =3,7.10^{50}	2^{167} μs =5,9.10^{36} years	5,9.10^{30} years

2.6 Selection of Cryptographic Algorithms

Through different of security protection level on the two cryptographic algorithms RSA and AES that according to the variety of key lengths to affect the speed of encryption, decryption process and the consumptions on memory with battery power usage during the information or data transmission via some mobile devices in public network .

Owing to the comparison study of the two cryptographic algorithms are easy to realize that the block sizes are equal to the key sizes of AES algorithms even the key sizes are encrypted. Instead, if apply to use the RSA algorithm, so the whole operation would be quite slow, especially when the n value is getting larger and larger, so that made the cipher size of secret information or data is larger than the original size of information or data several times. In the meantime, we are aware that RSA algorithm is used for solving the essential problem of key exchange on AES algorithm during transmission processing in the public environment.

As previous mentioned the comparison of the two cryptographic algorithms on security issue, according to the selection on different of key lengths (e.g. the prime numbers in RSA or the block sizes in AES) will be affected the level of security protection with the corresponding of performance improvement. Figure 2.13, shows that the comparison of the two cryptography algorithms of RSA and AES on mathematic computing, key generation, key transmission and key length.

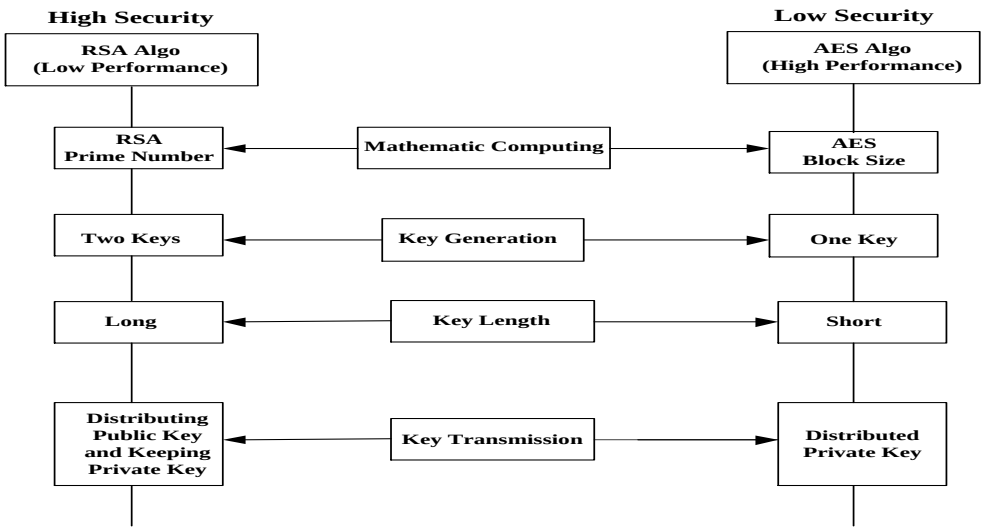


Figure 2.13 The comparison of RSA and AES cryptographic algorithms

2.7 Summary

In this chapter, user and device authentication are overviewed in terms of concept and QR-code technique with cryptographic algorithms are provided and discussed. By survey and investigate some of related works thus made us get more understanding the pros and cons from them. In our consideration for handling robotic attack issue on OTP from our proposed the combination of authentication method to establish a higher degree level in the manner of securely and friendly for the visually impaired people will be explain in the next chapter.

CHAPTER 3

PROPOSED METHOD & DESIGN

In this chapter, a newly proposed method can be realized which combines to use the user and device authentication, by the way of securely and friendly to establish a combined authentication method for helping the visually impaired person during the access of computers through some mobile devices.

3.1 Proposed Method for the Visually Impaired

Aforementioned that the user identity authentication is always occur whenever the users are intend to get into access a computing devices, so have to prove the devices that have been pre-established with the certain credentials.

In the meantime, the user device authentication should be taken into account as well, it is able to verify the devices identities in effect when they are via some unsecure communication channels for connecting and working with each other. However, the security problem can be occurred underlying wireless communication channels, so that some encryption technologies should be included.

To obtain the adequate level of security, so that a desired of authentication approach with the several combinations (show in Figure 3.1) should be fully consideration as follows:

1) One-time validation with OTP protocol;
2) Encryption/decryption the secret information through RSA public key cryptographic algorithm;
3) Stores the secret information into QR-code with inherent features;
4) Audio-based CAPTCHA playback with local Text-to-Speech (TTS) engine.

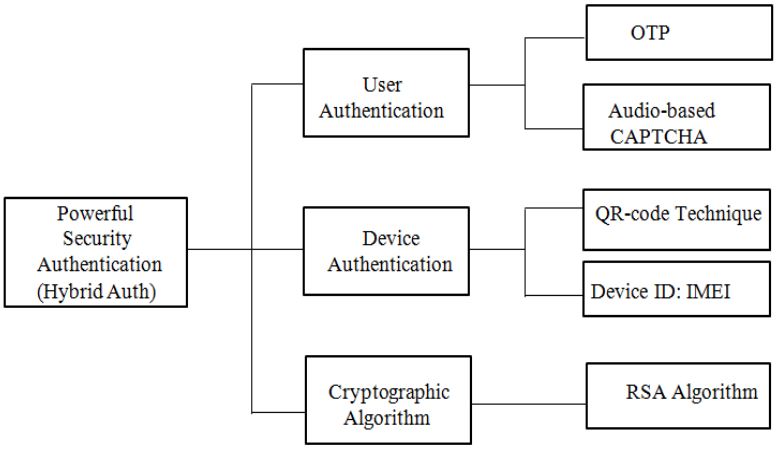


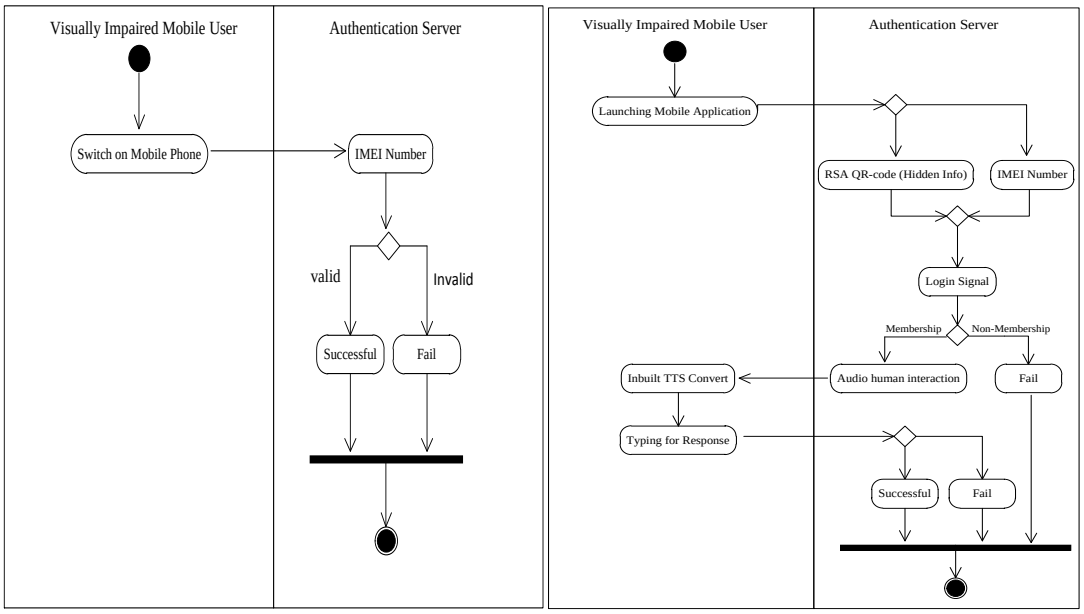
Figure 3.1 Our proposed authentication method for the visually impaired

By working towards this direction, we proposed a new authentication method that by using the common equipment of mobile phone with local TTS engine and RSA public-key cryptography algorithm encrypt on QR-code for the mobile users, who are visually impaired and may have the low level of computer skilled. As a result, the improved authentication not only can establish higher degree of security level on cryptographic technology, by identify the legitimate visually impaired mobile user is still being interacted to avoid robotic attack problem, but also can ensure that only the trusted mobile device can be authorized success to gain the services or resources, thereby, the whole combination for this authentication method will be realized.

3.2 Proposed System

As shown in Figure 3.2, we investigated the weaknesses of typical device authentication technique by means of unique mobile's International Mobile Equipment Identification (IMEI) and proposed to involve it with QR-Code based secret key in the Public Key Infrastructure (PKI) encryption scheme for improving the level of security since a much greater number of key lengths can be accommodated. However, it is likely that some audio-based CAPTCHA mechanism also need to be involved afterwards so that the full feature of anti-robotic attack can be realized. As a result, the improved authentication technique for the visually impaired on the access of computers through mobile devices can be obtained. To realize the efficiency of proposed mechanism, the performance study on the combination of Public Key Infrastructure security algorithms based on several degrees of combination between QR-Code and IMEI will be issued. Afterwards, a prototype will be implemented for

experimentation. This is to confirm the efficiency of the proposed system in some realistic environment.



(a) (b)

Figure 3.2 (a) Typical IMEI-based and (b) Our proposed authentication method

3.2.1 Architecture Overview

A simple and efficient manner is proposed in order to establish a higher level of security for support the authentication process to the visually impaired through the mobile devices. We proposed a powerful combination of users with device authentication method show in Figure 3.3 which is based on using OTP with QR-code technique and RSA algorithm. To make use of one-time validation of OTP in order that makes security on authentication getting much securer than the traditional username password scheme. The abilities for encrypt the secret information through RSA cryptographic algorithm and store it into QR-code. So that a combined of authentication method can be realized.

Our system is composed of two parts: a main server named (RSA OTP Server) and a mobile application named mobile QR-code generator (OTP QR-code Generator). The main server is provided by the functionality to register the user information and related services. The mobile QR-code generator is in charge of handling the (re)generate authentication QR-code images.

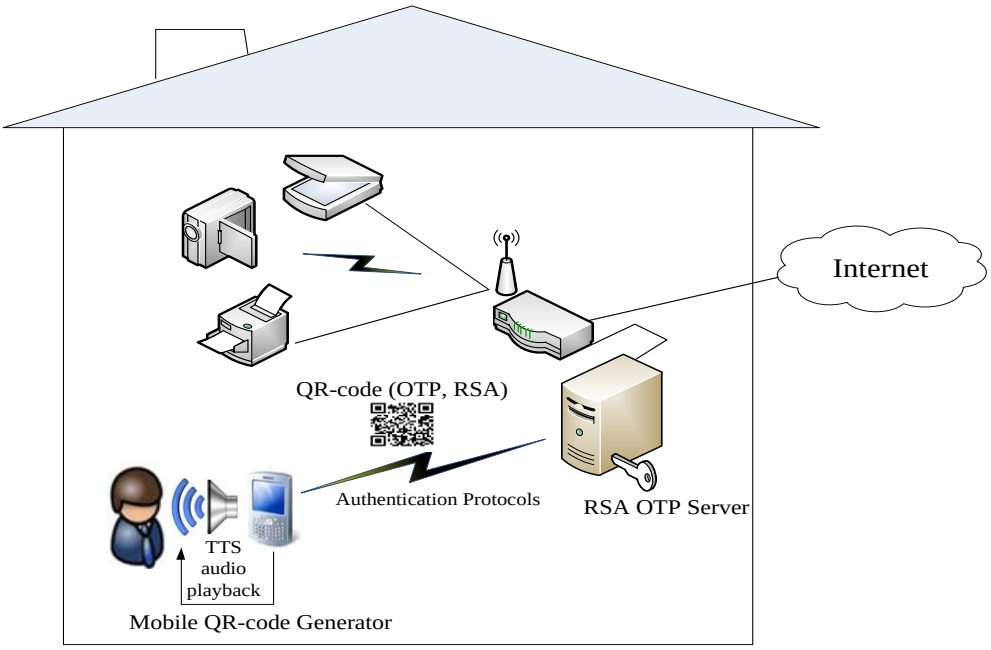


Figure 3.3 Overview of proposed system

Our proposed system can be widely utilize in many services and scenario e.g. web service, UPNP home appliance service, physic access scenario, prepay system and E-ticket scenario etc; which are required to do authentication. The main server is used to do authentication and verification of the request from VI mobile users. Figure 3.3 is an overview of proposed system. By considering to our scenario only a single VI mobile user conduct the authentication process which through the inbuilt smart engine (TTS) for helping the VI people fulfill the entire authentication and verification process to further improve the secure protection level on human verify and authenticate. By that way, apply only using a single object that is mobile phone, so without costing on extra specific hardware. Also easily to aware of phone lost than any other mobile devices and by using inbuilt smart engine which is suitable in our scenario for the VI people, so that makes the whole time length of authenticate processing can be cause injury shorter.

In the following sections, we will introduce each part of our system include the roles of they play and the functions of they provide.

3.2.2 Functional Blocks

In this section, through introduce the functions of mobile QR-code generator and main server, in the term of registration phase and authentication phase. The registration phase is to enable the VI mobile user to register the services depends on the requirements, so the proposed system can give out the correct response with the relative services. Another

phase is to introduce how our architecture combines with web service or UPNP home appliances service to implement an access service or an access control service.

Before introducing the functions, the notations are summarized as following:

E_{QR}(m): QR-code encoding processing function to encode message m to a QR-code image

D_{QR}(i): QR-code decoding processing function to decode a QR-code image I to a text

E_{RSA}(m, x): RSA encrypting processing function to encrypt message m by key x

D_{RSA}(m, x): RSA decrypting processing function to decrypt message m by key x

Pub_{OQG}: Public key of the mobile QR-code generator

Pri_{OQG}: Private key of the mobile QR-code generator

M_{OQG}: Modulus of the mobile QR-code generator

Pub_{ORS}: Public key of main server

M_{ORS}: Modulus of the main server

Pri_{ORS}: Private key of the main server

I: IMEI (Mobile's International Mobile Equipment Identification)

P_{No}: Phone number

S_{ID}: Service Id of the required service

OTP: One Time Password

F: From server flag equal to 1 if message generated from server

VI: Visually impaired mobile user

3.2.2.1 Registration Phase

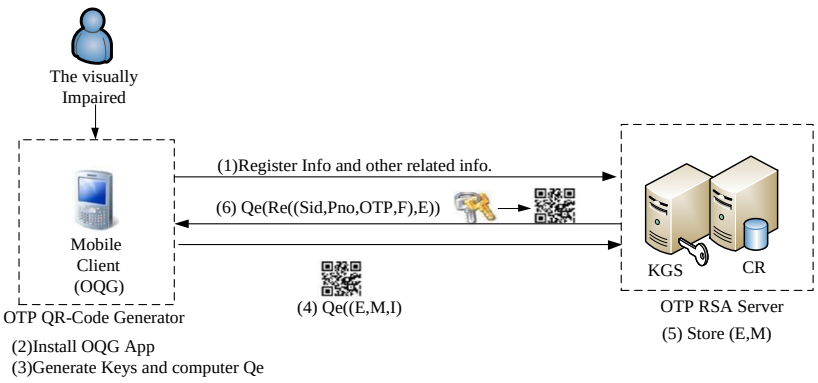


Figure 3.4 Registration phase

This phase introduces the registration phase as the first phase of the integrated framework. Its main purpose is to allow the VI mobile user to register the request services

and to create the RSA Key pairs by mobile QR-code generator, and then transfers the related key information to the main server for establish mutual secure authentication. Figure 3.4 shows the main structure of this phase:

1. When the mobile device initiates, it registers its IMEI, P_{No}, and required service to the main server of OTP.

2. Install the mobile QR-code generator of mobile application on the mobile.

3. Use the mobile application to generate the RSA keys (Pub_{OQG}, M_{OQG}, Pri_{OQG}) and to store the private key (Pri_{OQG}) into the database belonging to mobile QR-code generator at the first launch, get I of this mobile, and finally regenerates an image of QR-code by computing E_{QR} ((Pub_{OQG}, M_{OQG}, I)).

4. The main server gets the message from the decoded image of QR-code, computed by $D_{QR}(E_{QR}(Pub_{OQG}, M_{OQG}, I))$.

5. Store (Pub_{OQG}, M_{OQG}) into the database relative to mobile client whose IMEI equal to I.

6. QR-code is generated with OTP and secret message (S_{ID}, P_{No}, OTP, F) from main server via local wireless home network by computing E_{QR} (E_{RSA} (S_{ID}, P_{No}, OTP, F)Pub_{OQG}). If the illegal users intercept and decode this secret message from wireless communication channel, they can only see the big integers, because they do not have the private key of the mobile QR-code generator of mobile application.

3.2.2.2 Authentication Phase

In this section, we introduce how our architecture combines the web service or UPNP home appliance services to implement an access service or an access control service and regenerate a new QR-code image from the image received in phase 1 to be used as the authentication token to execute authentication. The graph shown in Figure 3.5 gives the main structure of phase 2.

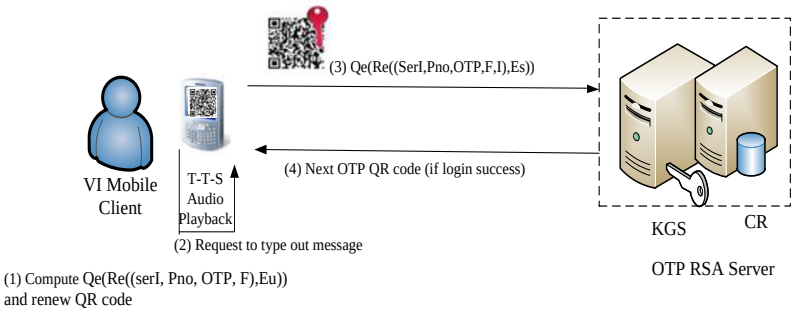


Figure 3.5 Authentication phase

1. Use the mobile QR-code generator of mobile application to generate a usable one-time password QR-code from the transfer message at main server, in order to do that, mobile QR-code generator compute D_{RSA} ($D_{QR}(E_{QR}(E_{RSA}((S_{ID}, P_{No},$ OTP, F), Pub_{OQG}), Pri_{OQG})) to get secret information ($S_{ID}, P_{No},$ OTP, F) at first and the mobile QR-code generator will change F flag from 1 to 0 and add I into the secret information set as the response so that the new secret information is ($S_{ID}, P_{No},$ OTP, F, I). The mobile QR-code generator has to regenerate this secret information into a QR-code image for authentication by computing $E_{QR}(E_{RSA}((S_{ID}, P_{No},$ OTP, F, I), Pub_{ORS}).
2. The main server computes D_{RSA} (E_{RSA} (($S_{ID}, P_{No},$ OTP, F,I), Pub_{ORS}), Pri_{ORS}) to get plaintext ($S_{ID}, P_{No},$ OTP, F,I), identifying if this is a valid of OTP for this user by checking these information stored in the database before, thus wait for a authentication result (login signal) to enter the request OTP code.
3. With embedded local TTS smart engine in audio-based CAPTCHA mechanism to convert the successful decryption of secret message about random value into a voice version of digit numbers (should less than eight digits) which is mandated by Text-To-Speech (TTS) engine and required the VI user to press then can obtain the services or resources as the VI user wants.
4. After get services, then the main server generates a new QR-code image and transfers it to the mobile device via wireless communication channel which is used for the next authentication.

3.3 Main Hidden Information

- The key information QR code (show in Figure 3.6)

When the 512, 1024, 2048 bits RSA keys are generated from OTP QR-code Generator, we have to send the public key and modulus to the server. Because the public key and modulus are publishable, we do not have to worry if someone tries to steal the information. We use the QR-code to encode the information and make the server to be able to scan the QR-code to get keys information and store it directly for avoiding typing error. The information contains modulus, public key, and International Mobile Equipment Identify number.

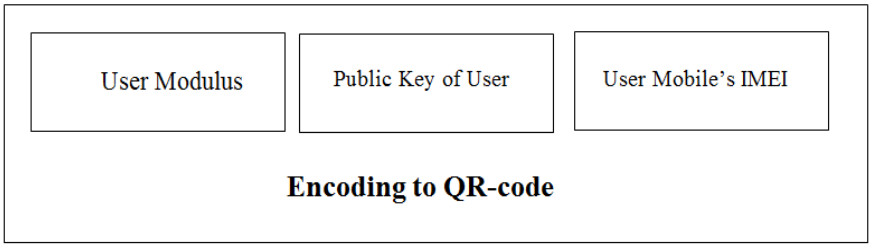


Figure 3.6 Format of keys message

We will encode two times for the fact of main server described above, first time is encoded these factor into RSA message using RSA algorithm by client public key which was stored before, and second times is encoded the RSA message into QR-code so that we can transfer this QR-code Via Wi-Fi. The authentication of QR-code from the main server shows in Figure 3.7.

There are four required fact for the main server in this image:

(1) Service ID: An integer number for Service

(2) User Mobile: The mobile number of receiver phone

(3) OTP: A sequence of 6 bytes numeric string generated from server

(4) CAPTCHA: A digital number should less than 4 or 6 numbers

(5) From Server: An integer factor always I if this QR-code is created by server.

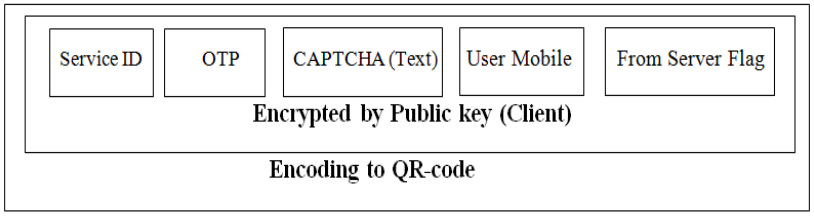


Figure 3.7 Format of authentication image from the main server

The Server side will add text messages (directly encrypt by RSA public key from user) we still need to consider, then make a choice shown in Figure 3.8.

- The authentication QR-code regenerated from mobile QR-code generator. After receiving the authentication QR-code from server, OTP QR-code Generator will decode the QR-code and get plain message by RSA decoding. OTP QR-code Generator will regenerate a new OTP RSA QR-code by modifying the plaintext.

(1) Modify 'fromServer=0' to 'fromServer=1', it is treat as a response data to server.

(2) Add user Mobile IMEI factor into plain text so that server can assure the new OTP RSA QR-code is generated from OTP QR-code Generator registering in phase1.

(3) Utilize TTS smart engine to convert OTP digit numbers to audio voice which require the VI to type it out for assure the human user still interact this ongoing authentication processing.

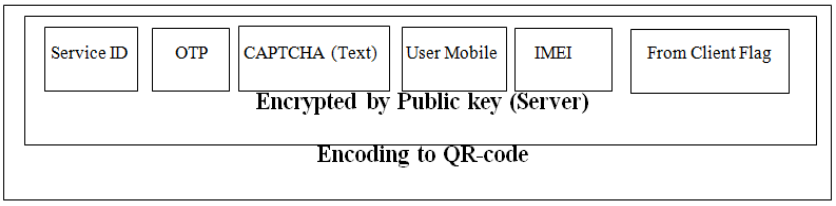


Figure 3.8 Format of authentication Image from mobile QR-code generator

3.4 Security Analysis

In this section, we will list several common network attacks below, and discuss the influence to the proposed mechanism in accordance with the attacks:

(1) Anti-robotic-attack:

The audio-based CAPTCHA mechanism can be applicable for identifying whether the being interaction come from the user who is a legitimate (visually impaired) human or not, in order to mitigate the weakness of vulnerable to be interfered by some malicious computer programs on OTP based login authentication processing.

(2) Man-in-the-middle attack:

Even if the illegal user can intercept the transmission messages, it's useless because the secret message is encrypted by the RSA cryptography algorithm.

(3) Message modification attack:

The role of RSA algorithm of public-key cryptology is used to protect the secret information, thereby it's useless to tamper with the encrypted message on it. The mobile client takes an active connection to main server and it does not open a fixed port to

wait for a response, therefore even an attacker attempt to destroy our scheme by this attack is very difficult.

(4) Replay attack:

One-time password is an effective mechanism can avoid tradition static password issues. In our scheme, the certified QR-code image are all one-time validation used, even the third party grabbed the certification in our scheme through this attack is still not useful.

(5) Masquerade attack:

a. Malicious of the mobile client: The feigned of mobile client does not work in deed, because it cannot successful to decode the image of QR-code, even if it intercepts one, there has no way to obtain the correct of secret key. In other words, it cannot obtain any valid of information at all.

b. Malicious of the main server: With the protection from RSA cryptography algorithm, a fake main server cannot decode the receiving information, because it has no private key of real main server. In addition, a fake main server without the ability of sending message easily with a special application.

c. Malicious of mobile QR-code generator: The user needs to register the service at registration phase so a fake OTP QR-code Generator cannot receive the authentication of QR-code image via wireless communication channel. In addition, the specific of secret message was generated according to the register service and mobile phone number associate with mobile's IMEI. Not any of the QR image can be used in any OTP RSA QR-code Generator, even if the message is intercepted by the illegal users are still meaningless for them.

3.5 Comparison with the Other Works

Many authentication methods are introduced in this thesis which including [5], [19], [20], [24] and our proposed mechanism. All of them have somewhere in common and different as well. Therefore, through compare of them and give out the difference between all of them in the Table 3.1.

In the scheme [24] uses QR-code as authentication method in mobile, working on trust carrier network for make sure the great service and protection. In schemes [19] and [20], each of them takes four times and two times separately to communicate between client and server in the authentication and verification procedure.

The scheme [5] by use of user authentication method for authenticates user and provides service directly through the home server of home network, each time to transfer the data always after be encoded with the mutual time synchronization method between OTP module and home server to generate a random parameter.

Table 3.1 Comparison of related authentication schemes

	Our Proposed	[19]	[24]	[5]	[20]
Authentication Method	RSA OTP QR-code	QR-code Counter based OTP	Nijigen code	QR-code Time based	OTP Scheme
Device Authentication	Yes	Yes	No	Yes	No
Access Control	Yes	Yes	No	Yes	No
Anti-Robotic Attack	Yes	No	No	No	No
Network for Authentication	Wireless Network	Mobile Network	Mobile Network	Mobile Network	N/A
Communication times each authentication	2	4	6	2	2
Encryption Algorithm	RSA	Hash Function	Hash Function	Hash Function	Hash Function
Mutual Authentication	Yes	Yes	No	Yes	No

In our proposed method, by use of the RSA encryption algorithm can establish higher security level and avoid disposing secret information in public. It can be seen that our mechanism is comparable to the other works, but is dominant at the feature of anti-robotic attack. This is due to the exploit of the audio-based CAPTCHA mechanism for allowing the human-verification to be occurred over the same communication network. In addition, it is also a friendly manner to do authentication for the visually impaired mobile user during the access of computers through some mobile device.

3.6 Security Consideration of Design Criterial

A combined authentication method is proposed with the RSA cryptographic algorithm for establish a higher security level for the visually impaired through some mobile devices. As the main concern of the RSA algorithm is to make sure the data security which is fully rely on the key's generation and transmission, so that we have to keep the private key for safety. As we knew that if the key sizes of RSA are getting larger, the longer cipher message and the more adequate of security level we can obtain, therefore a suitable value n (two prime number p*q) and key length should be considered, after measure the computing

time on several of key lengths generation (see Figure 3.9), hence the 1024 bits of key sizes can be selected for using in this work.

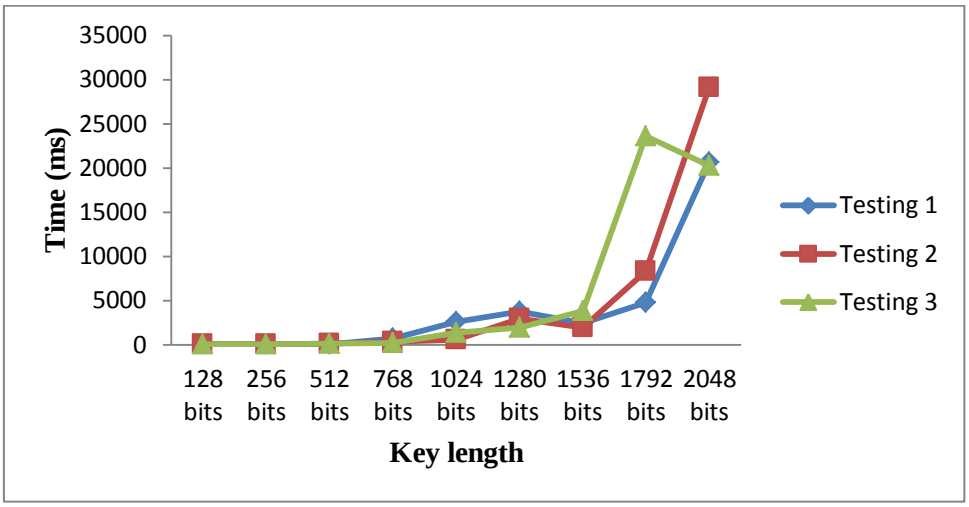


Figure 3.9 Time taken vary of key lengths on RSA algorithm

For securely and effetely hidden the confidential information as we wanted, thereby the widespread of QR-code technique should be included, in the regards to the QR-code algorithm which divides the content of QR-code into the required numbers of blocks to enable the error correction algorithms (see Figure 3.10).

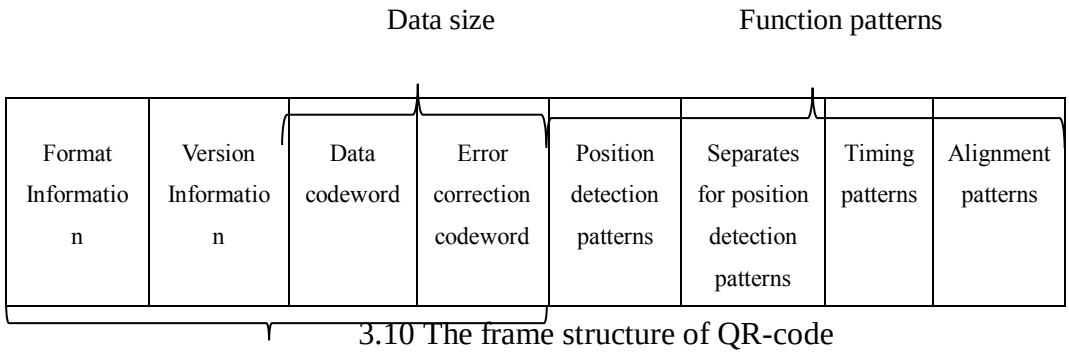
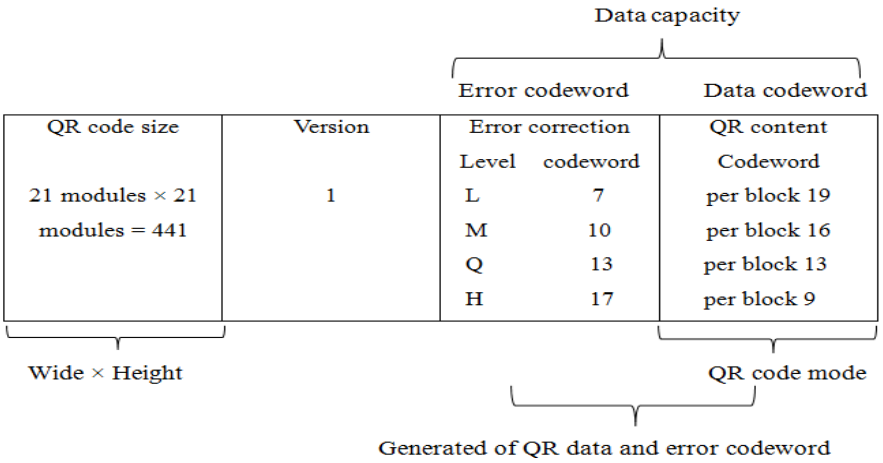


Figure 3.10 The frame structure of QR-code

For the specification of QR code should take to use, following this to better understanding during the loss of QR-code on transmission process or damage situation, in Table 3.2 shows a sample of version 1 QR-code what are the data codeword and error code words should include.

Table 3.2 Specification of QR-code



Through taking into account the entire proposed system, which can be divided into two different security layers (see Figure 3.11), the outer security layer is according to RSA cryptographic algorithm which is used for verify the original data really being transmitted from the place they claim to be, also can be avoid by some illegal ways attacking, e.g. MITM, message changed, replay attack etc. Another one is the inner security layer is based on QR-code self-recovery algorithm which is applied to using the popularity of quick manner for detecting and decoding with its dominant characteristics and en/decoding algorithm to obtain the original information. Finally, the two security layers to be establish the higher level of security on our proposed authentication method.

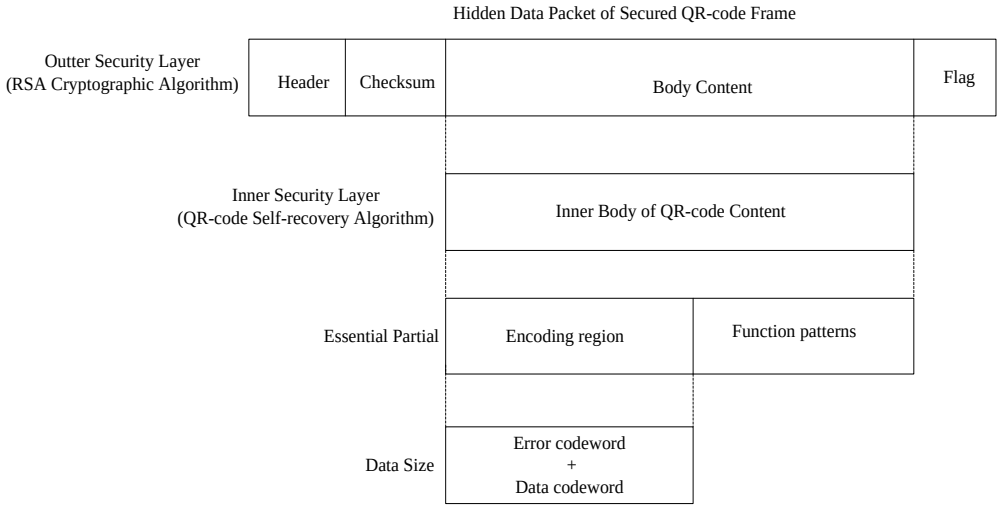


Figure 3.11 The frame of data segmentation for the two different security layers

In the previous parts, we mentioned that the tradition static password's weakness which by use of dynamic style of One-time password to handle it, due to OTP's dominant features on one-time validation, also use 15 bytes of numeric string as the

maximum size of OTP. Nevertheless, we realized that it still cannot efficient verify the active process is coming from the really human user. Thereby, the audio-version of CAPTCHA should be utilized in our scenario which is required the visually impaired to type it out, considering to the friendly manner should be used so that the digital number of audio-CAPTCHA should within 1 to 15 numeric number, if it is too long, the visually impaired will be difficulty to recognized each of them and unable to successful type out, if it is too short and easy will be vulnerable to be attacked by the keylogger. The whole of data frame structure is showed in Figure 3.12 and 3.13.

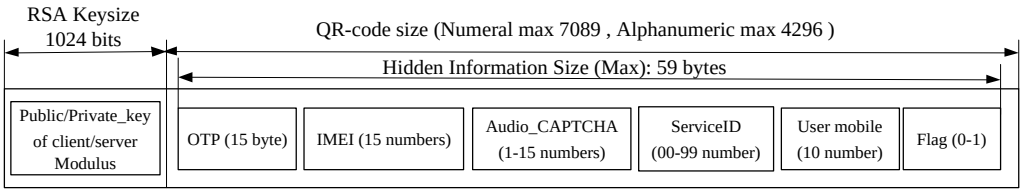


Figure 3.12 The entire of frame structure of secured data size

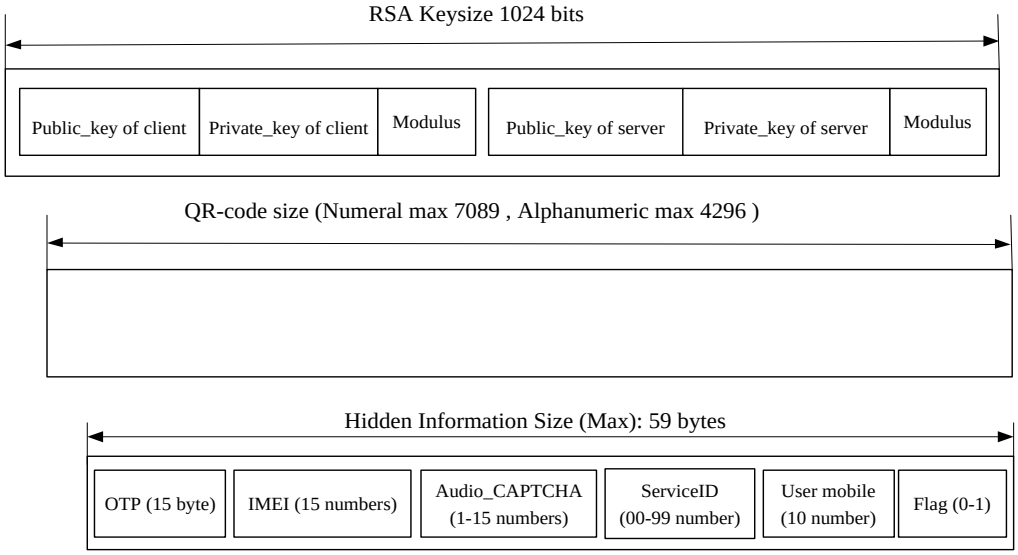


Figure 3.13 The separate frame structure of secured data size

3.7 Summary

In this section, to obtain an adequate security level by combined user identity authentication and user device authentication for design a desired authentication method in the manner of securely and friendly for helping the low level of computer skilled of visually impaired mobile user during the access of computers through some mobile devices. With analysis and discuss the security of proposed system which regarding to the consideration of design criteria. Also give out some comparisons with some other relevant works.

CHAPTER 4

EXPERIMENTAL RESULTS AND DISCUSSIONS

As we previously proposed a hybrid authentication method which can be establish a higher security protection level for the visually impaired person via mobile devices, underlying the security algorithms, such as RSA, AES etc. So to evaluate the time consuming on data size encryption and decryption will made our method more reasonable and more selectable. Apply the selected security algorithm into the widespread QR-code algorithm, so that the two-level of security can be realized.

4.1 Robustness of Proposed System

The objective of this proposed system is to examine whether the QR-code with some errors can still be read out or not. Based on the property of QR-code, to evaluate the three error position areas occurred on QR-code images also to measure the capacity of error correction level and changed QR-code area ratio.

4.1.1 Exprimental Set Up

Table 4.1. Experimental conditions

Content		Detail
QR code	Data	Alphanumeric mode 10 numbers
	Version	3
	EC Level	4 Levels: L, M, Q, H
Display Tool		Dell E2011H (20 inch)
Reading Software		Codetwo QR-code Desktop Reader
Editor Software		Gimp 2.8.0
Error areas		Exception of the finder pattern

In this experiment, the free open source of ZXing library is used to encoding and decoding QR-code as software development platform. Application of QR-code PC decoder can be used as a QR-code reader without taking a picture. Consider to use the RSA cryptographic algorithm, so evaluate the time for encryption and decryption on data size.

4.1.2 First-Level of Security (QR-code Security Level)

Previously in Figure 3.11 mentioned the frame of data segmentation for the two different security layers. Through study some others works related to the level of security on QR-code are:

On Huang and Weng's [26-27] are apply to use QR-code technique on high speed reading with encryption technology on RSA public-key cryptography for confidentially store information on QR-code. We can found that using longer key size of RSA algorithm not only can secure encrypt message but also will make the cipher message much longer than before. However, the RSA QR-code will be more complicated on decoding problem. As we know that the QR-code have a variety of modes (L, M, Q, H) are suitable in different conditions, if choose the higher rate of error correction level, the more chance can get information recover success, but the complex QR-code problem will be happen.

4.1.3 Second-Level of Security (RSA + QR-code Levels)

According to the RSA algorithm is selected for the primary of higher security cryptographic algorithm on our proposed method. It is not only protect the confidential information avoid altering arbitrarily, but also verify the data owner in precisely.

For the most important points of RSA algorithm are key generation and key transmission. For the key generation of RSA is computed by the two prime numbers of p and q, which required to be as larger as better in order to obtain a higher level of security. As we known that there is no polynomial time algorithm to solve the problems of factoring a large number n value into two prime numbers and required time to factoring based on the length of n value [27].

Considering the following choice of the length of n value: (1) If the value n is too small then security issue will happen. (2) If the value n is too big the problems will be occurred on heavy calculation burden of RSA en/decryption on mobile devices and made the encrypted QR code image too complex to let it cannot be decoded.

Regarding to ensure the key transmission successful, so a pair of two different keys will be utilized, so that keep the private key safety is quite important. To consider that the different sizes of key length will affect the security level of cryptographic algorithm. If choose to use small length of key size on RSA algorithm, thus made the security level is vulnerable to be attacked. To en/decrypt the vary of data sizes underlying the two different keysizes 512 bits and 1024 bits, the same like the given data size as the time taking longer when the key lengths are gradually increase (shown in Figure 4.1 and 4.2).

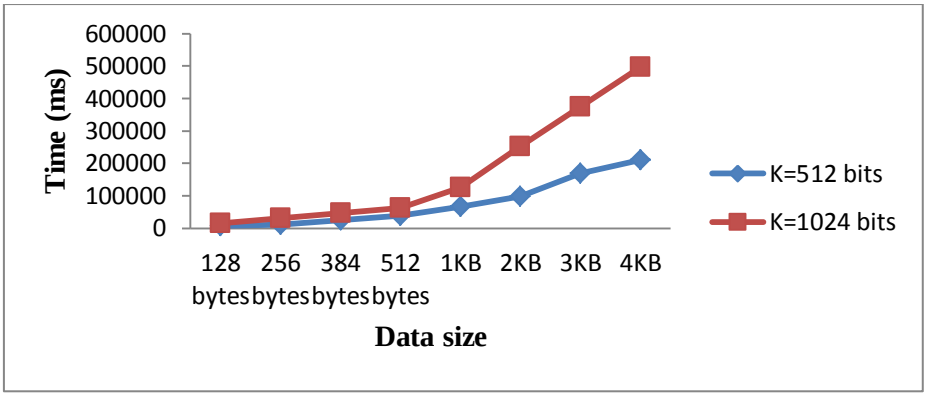


Figure 4.1 Execution time for encryption with different datasizes

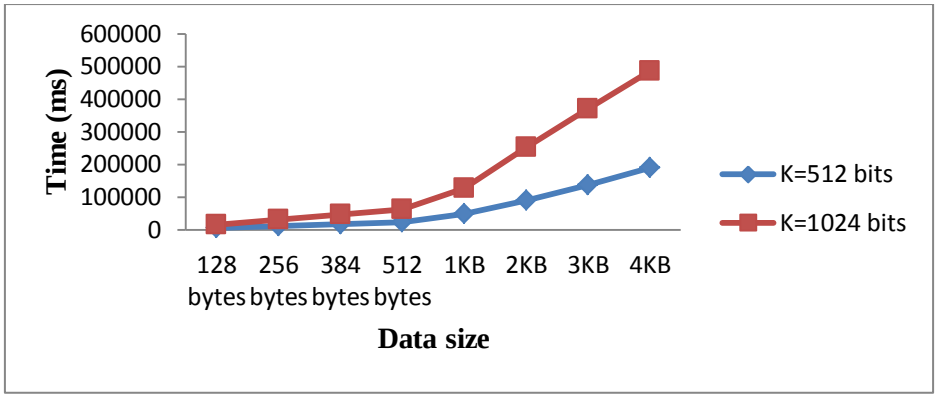


Figure 4.2 Execution time for decryption with different datasizes

4.1.4 Error Occurred Position on QR-code

Through measure the error correction levels at some errors are occurred areas on QR-code image. The table 4.2 is the experimental result show that the error position of center-left with the best reading capability if compare with the other two areas, due to the error areas are mainly take up on the part of reminder bits, timing pattern and format information. In the fact, the best reading capability should be on the center part of QR-code, because this part include a large number of data codewords and error codewords, so that means if error happened in this region can be have much more percentages to recover the lost information back.

Table 4.2 The results of errors occurred at three positions

Error Correction Level	The Errors Occurred area (width × height = cells)		
	Center	Center-Left	Right-Bottom

L	√	√	×
M	√	√	×
Q	√	√	×
H	×	√	×

(√ Show a success reading by QR-code reader)

(× Show a failure reading by QR-code reader)

4.1.5 Secret Information of QR-code

The higher rate of error correction, the more error codewords can be accommodated, but the data that can be stored is relatively less (see Table 4.3). Through version 1 to 40, as QR-code size increase made each version of error correction level will be changed. In Figure 4.3 represents the Table 4.3 that as the higher version of QR-code and higher error correction level can be obtain larger space of error codewords in the meantime the whole space for encoding data size will be less and less.

Table 4.3 Different versions and error correction levels on QR-code

Version	QR code size	Error correction level (Secret payload bits)			
		L	M	Q	H
1	$21^2 = 441$	28	40	52	68
5	$37^2 = 1369$	104	192	288	352
10	$57^2 = 3249$	288	520	768	896
15	$77^2 = 5929$	528	960	1440	1728
20	$97^2 = 9409$	896	1664	2400	2800
25	$117^2 = 13689$	1248	2352	3480	4200
30	$137^2 = 18769$	1800	3248	4800	5760
35	$157^2 = 24649$	2280	4256	6360	7560
40	$177^2 = 31329$	3000	5488	8160	9720

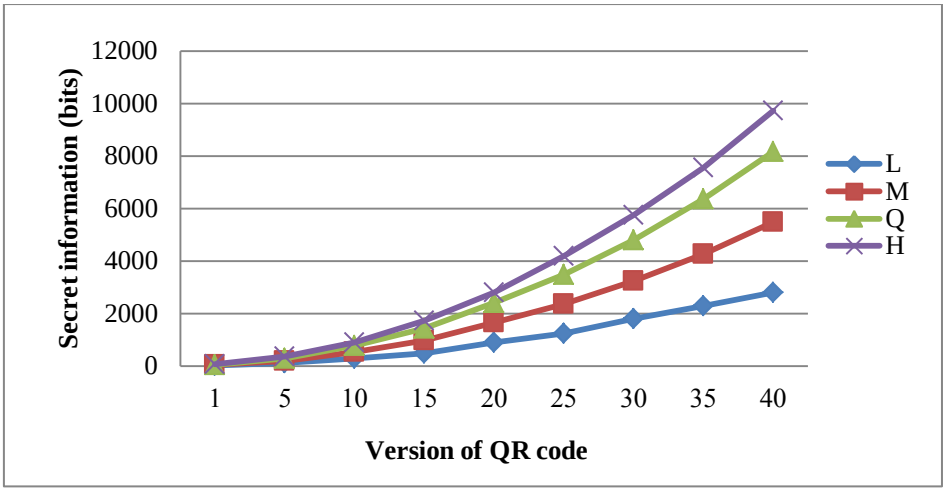


Figure 4.3 Different versions and error correction levels on QR-code

4.1.6 Error Correction Level on QR-code

According to the standard of QR-code, so the error correction characteristics for version 1 to 40, we can simply calculate the number of error correction capacity divide total number of codewords (see Table 4.4 and Figure 4.4). To ensure the error correction capacity = $\frac{\text{Error correction code per block}}{Total\ number\ of\ codewords}$ ×100%. Then will obtain each version of error correction level which approximates the idea percentage of error correction level.

Table 4.4 The percentage of error correction level on different version

Version	QR code size	Error correction level (Error correction capacity)			
		L	M	Q	H
1	21^2= 441	7.69%	15.4%	23.1%	30.8%
5	37^2= 1369	9.70%	17.9%	26.9%	32.8%
10	57^2= 3249	10.4%	18.8%	27.7%	32.4%
15	77^2= 5929	10.1%	18.3%	27.5%	33.0%
20	97^2= 9409	10.3%	19.2%	27.6%	32.3%
25	117^2= 13689	9.8%	18.5%	27.4%	33.1%
30	137^2 = 18769	10.3%	18.6%	27.5%	33.0%
35	157^2 = 24649	9.91%	18.5%	27.6%	32.9%
40	177^2= 31329	10.1%	18.5%	27.5%	32.8%

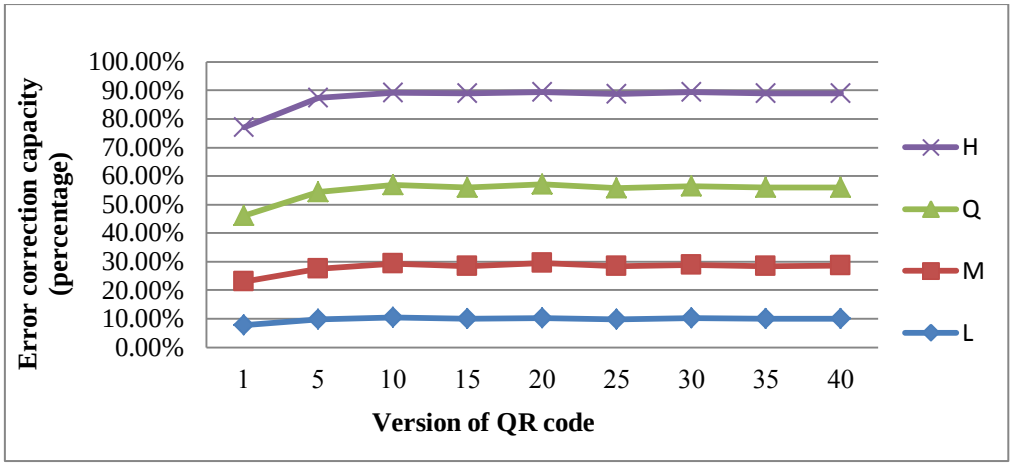


Figure 4.4 The percentage of error correction level on different version

4.1.7 Change Ratio of Secret QR-code

If the large version and error correction level of a QR code we chose, the large codewords we can obtain, so the more secret capacity can hide into a QR code (see Table 4.5). To evaluate the modified ratio of a marked QR code, the change ratio σ is used to ascertain the changed modules of the marked QR code, $\sigma = \sum b_{i\_j} \Big/ \text{QR code size}$ b_{i_j} : the j-th changed module of i-th block, generally, the amount of the changed modules is half of secret payload (see Figure 4.5).

Table 4.5 Vary of secret payload C (bits) and the change ratio σ(%) on QR-code

Version	QR codesize (modules)	Error correction level			
		L σ(%)	M σ(%)	Q σ(%)	H σ(%)
1	$21^2 = 41$	3.17%	4.54%	5.90 %	7.71%
5	$37^2 = 1369$	3.80%	7.01%	10.52%	12.86%
10	$57^2 = 3249$	4.43%	8.00%	11.82%	13.79%
15	$77^2 = 5929$	4.12%	8.10%	12.14%	14.57%
20	$97^2 = 9409$	4.76%	8.84%	12.75%	14.88%
25	$117^2 = 13689$	4.56%	8.59%	12.71%	15.34%
30	$137^2 = 18769$	4.80%	8.65%	12.79%	15.34%
35	$157^2 = 24649$	4.62%	8.63%	12.90%	15.34%
40	$177^2 = 31329$	4.47%	8.76%	13.02%	15.51%

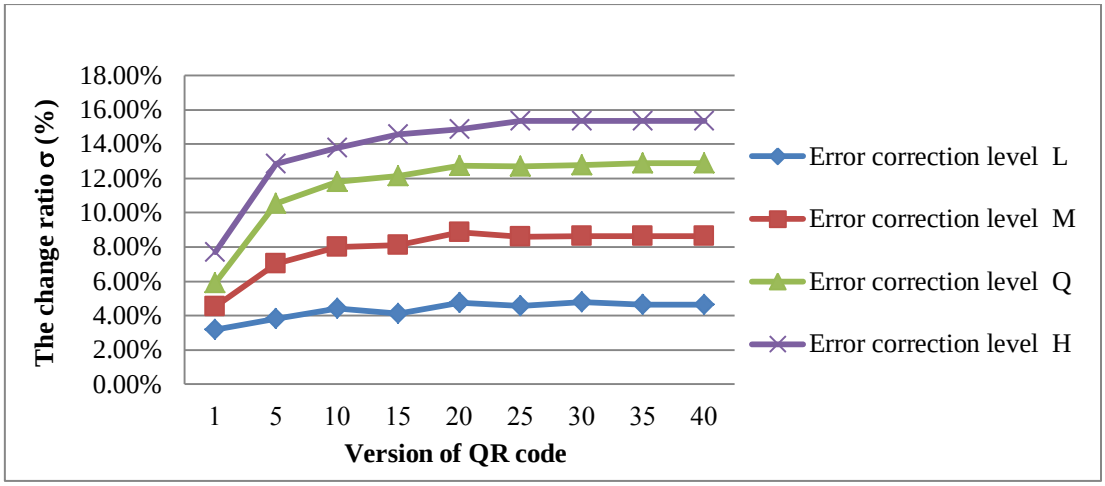


Figure 4.5 Vary of secret payload C (bits) and the change ratio σ(%) on QR-code

4.1.8 Suitable Length of QR-code

According to the QR-code ISO/IEC 18004 standard, four levels of error correction are available. The higher of the level, the greater of the error correction result will be obtained, but also the larger version of the QR Code will be generated. The characters and input data capacity from version 1 to 40. It easy to know that the data sizes from high to low: (1-L: 25 to 1-H: 10), (40-L: 4296 to 40-H: 1852) from low to high: (1-L: 25 to 40-L: 4296), (1-H: 10 to 40-H: 1852). Considering to the main hidden information express in total length of secret information in QR-code calculating roughly:

1. Key information in QR-code;

Key size of RSA encryption algorithm selection on 304 bits, 448 bits, 512 bits, 576 bits, 640 bits, 704 bits, 768 bits, 832 bits, 896 bits, 960 bits, 1024 bits and 2048 bits will be used. For the IMEI number should include 15 digital numbers.

2. Authenticated QR-code image;

A service Id is expressed in an integer number for service (two digits from 00 to 99). OTP is a sequence of (15 bytes or selected random generated) numeric string, we can design it becomes as shorter as our wish. So the frame structure of total length of QR-code conducts in Table 4.6.

Table 4.6 Frame structure of hidden information on QR-code

RSA key sizes (304bits - 2048 bits)	IMEI number (15 digits)	Service ID (2 digits)	OTP (4 digits)	User mobile (10 digits)

3. In the previously, we mentioned that 512 bits of key sizes is the minimum key length of RSA encryption algorithm, in our case the suitable key length 1024 bits should be used, considering the limitation of computing on mobile devices. If use 512 bits of RSA key length, so the final data size should take up 760 bits, if use 1024 bits of RSA key length, so the data size will hold 1272 bits.

4. Through calculate the 512 bits of RSA key size the suitable data size take 760 bits. Based on the QR-code standard get to know that accommodate in version 5-L, version 6-L, 6-M, version 7-L, 7-M, version 8-L, 8-M, 8-Q, until version 9 (see table 4.6. Due to before the data size of version 5 is not in the range of data capacity of QR-code so ignore them (see in Figure 4.6).

Table 4.7 760 bits of error correction level on different version of QR-code

		Error correction level			
Version	Data sizes	L	M	Q	H
1	760 bits	-	-	-	-
2	760 bits	-	-	-	-
3	760 bits	-	-	-	-
4	760 bits	-	-	-	-
5	760 bits	104	-	-	-
6	760 bits	144	256	-	-
7	760 bits	160	288	-	-
8	760 bits	192	352	528	-
9	760 bits	240	440	640	768
10	760 bits	288	520	768	896

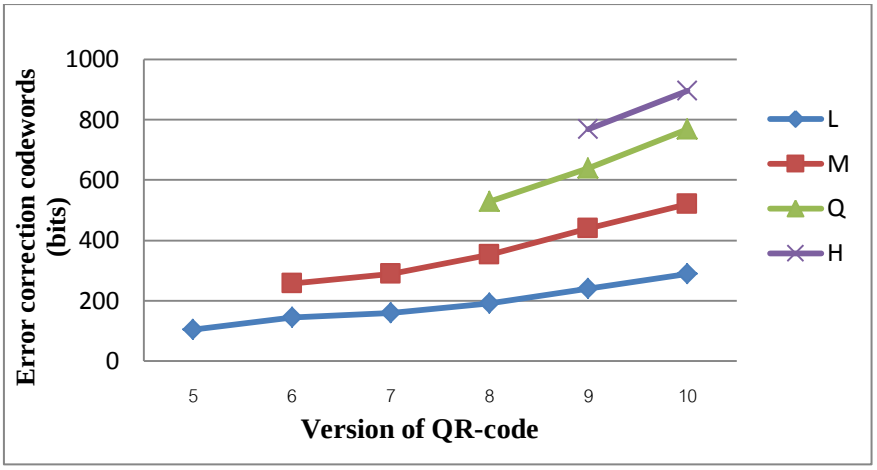


Figure 4.6 Error correction level of code words on different of QR-code version

5. Through calculate the 1024 bits of RSA key size the suitable data size take 1272 bits. Based on the QR-code standard get to know that accommodate in version 8-L, version 9-L, 9-M, version 10-L, 10-M, version 11-L, 11-M, 11-Q, version 12-L, 12-M, 12-Q until version 13 (see Table 4.8). Due to before the data size of version 5 is not in the range of data capacity of QR-code so ignore them (see in Figure 4.7).

Table 4.8 1272 bits of error correction level on different version of QR-code

		Error correction level			
Version	Data sizes	L	M	Q	H
1	1272 bits	-	-	-	-
2	1272 bits	-	-	-	-
3	1272 bits	-	-	-	-
4	1272 bits	-	-	-	-
5	1272 bits		-	-	-
6	1272 bits	-		-	-
7	1272 bits	-	-	-	-
8	1272 bits	192	-	-	-
9	1272 bits	240	440	-	-
10	1272 bits	288	520	-	-
11	1272 bits	320	600	896	
12	1272 bits	384	704	1040	
13	1272 bits	416	792	1152	1408
14	1272 bits	480	864	1280	1536

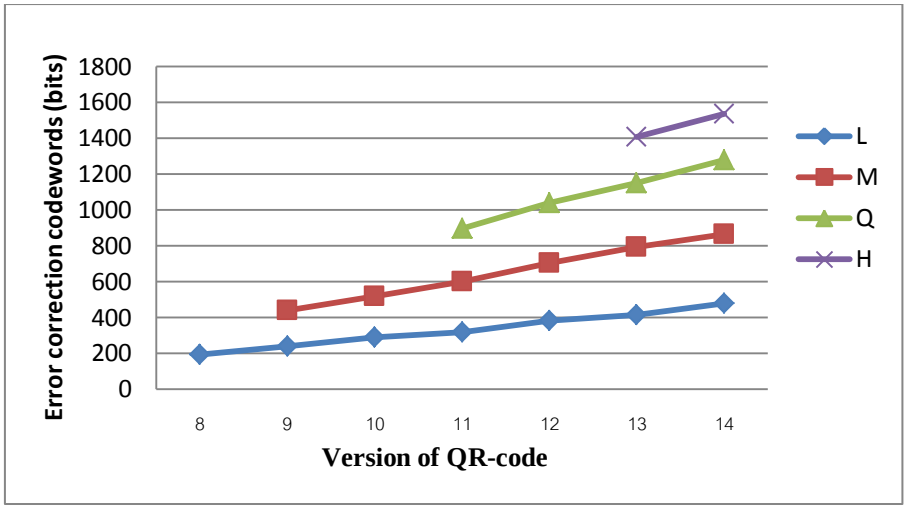


Figure 4.7 Eerror correction level of code words on different of QR-code version

4.2 Summary

By taking the advantage of RSA encryption algorithm, made the hidden information hardly to be obtained and modified, with considering to its key selection issue and suitable environment, so 1024 bits of RSA key length can be used in our case, at the meantime, take into account the specification of essential QR-code during the loss on the three part regions, we got to know that if choose the larger version so that the space for data size will become more and more density, that means each error correction level of codewords will be increase as well, so the L level should be chose, due to use the higher level of error correction which means the secret QR-code also will getting more and more complicated.

CHAPTER 5

CONCLUSION AND DISCUSSION

5.1 Conclusion

In this thesis, we proposed a securely and friendly authentication method which integrates user identity and user device authentication as combined approach to successful do the authentication for the VI mobile users via mobile phone. Since the mobile phone has become so ordinary in ours daily life not only for conduct calling and sending message function, but also sound as indispensable of multi-utilities carry-on device. Compare with traditional authentication solution by using of smart access card or traditional USB key token, in this work, utilize mobile phone as authentication token, one hand, without carrying on other objects and costing on extra specific hardware requirement, on the other hand, with inbuilt smart engine TTS for covert text message into audio version to require type out correctly in order for distinguish robot with human users. It is easy to aware of the mobile phone get lost if compare with using some other hardware tokens suck like: access control card or USB keys.

Through use of OTP as user identity authentication, made this security authentication method get more secure, due to it is only valid once time. To considering establish higher level of security protection, so that make use of the public key of RSA encryption algorithm, made the authenticated QR-code hard to be modified, therefore this combined authentication method can be applied to many services which are required to do authentication. In addition, with the capability of prevent the anti-robotic attack problem in an efficiency and friendliness manner in our considering scenario by audio-based CAPCHA mechanism to verify the on-going valid active process derive from the human user who are the visually impaired mobile users.

5.2 Discussion

In this work, it can be implemented on some other different scenarios. There we list some of applications for further describe them.

(1) To apply in the public places, such as: E-ticket of train or airplane or some other transportation system or E-ticket of cinema system as well.

(2) To use the concept on the prepay system, which allows the users to buy some stuffs without paying cash or credit card. Without modifying on the system architecture, but slightly change the hidden information still working. The system architecture does not require some modifications; only slightly made some changes on the hidden contents then can work.

(3) To utilize this work at housing access control system. Only the system administrator can send the regenerate QR-code image, but the customers apply using one-time application on mobile replace of using the real keychain.

The proposed authentication method gets lots of advantages based on the combined authentication method to working together. However, it gets several limitations discussed as follow.

5.2.1 Advantages

1) One-time validation with OTP as user identity authentication.
2) Encryption/decryption the secret information through RSA public-key cryptographic algorithm, the secret information is stored into QR-code by inherent feature.
3) Audio-based CAPTCHA playback with local TTS engine to be included in the verification process with the capability to prevent the anti-robotic attack problem in an efficient manner.
4) Our proposed authentication method not only is able to achieve the effect of twice time encryption, but also is capable of preventing the robotic attack problem in an efficient manner which is suitable in our scenario for the VI mobile users.

5.2.2 Limitations

1) By use of RSA algorithm can increase the higher level of secure protection; however, the cipher message will become longer and will make the QR-code image get more complicated than before.
2) The large key sizes of RSA algorithm will have longer cipher message which will lead to decoding problem on complicated RSA QR-code issue.
3) As we known that the transmission way are executed via wireless communication channel which is still vulnerable to be attacked, so the illegal users still have chance to detect and intercept the hidden

information.

4) If choosing longer length of key sizes then made the whole consuming time on encryption and decryption processing will be increase longer and longer, also should select the key sizes careful when considering to working on some memory constraint of mobile devices.

5.2.3 The future work

1) Make some changes on OTP, let it can be valid in several times or available permanently which can be according to the design or demand on portable and cost.
2) Replace of the RSA algorithm with other cryptographic methods (such as AES or DES) or to consider using hybrid of cryptographic algorithms which is more secure and more fast on power and memory constrained of mobile phone is part of our future work.
3) Use some manners to transmit a QR-code image such as: via WiFi or Bluetooth or near field communication transmission channel to reduce the time taking on key message transfer and the entire of authentication.
4) Handle the problem on concurrent users simultaneously send request and use this authentication method therefore take into account how long of key length should be taken and fulfill the whole processing how much time will be satisfied by the users.

REFERENCE

[1] L. Lamport, "Password authentication with insecure communication," Communications of ACM, Vol. 24, No. 11, pp. 770-772, Nov 1981.

[2] T. Tsuji, and A. Shimizu, "Simple and secure password authentication protocol ver.2 (SAS-2)," *IEICE Technical Report, OIS. 2002-30, Vol. 102, No. 314, September 2002.*

[3] J. Jeong, M. Y. Chung and H. Choo, "Integrate OTP-based User Authentication Scheme Using Smart Cards in Home Networks," *in Proceeding of the 41st Hawii International Conference on System Sciences, pp.294–299, Hawii, United State of American, Jan 2008.*

[4] W. B. Hsieh, and J. S. Leu, " Design of a time and location based one-time password authentication scheme," *7th International Wireless Communications and Mobile Computing Conference (IWCMC), pp. 201-206, 12 Aug 2011.*

[5] J. O. Park, and S. G. Kim, "OTP Authentication Module and Authentication Certificate Based User Authenticating Technique for Direct Access to Home Network and Resource Management," *International Journal of Smart Home, Vol.4, No. 3, July 2010*.

[6] Y. R. Tsai and C. J. Chang, "SIM-based subscriber authentication mechanism for wireless local area networks," *Computer Communication, Vol. 29*, pp. 1744-1753, *2006.*

[7] ISO/IEC 18004:2000. Information technology-Automatic identification and data capture techniques-Bar code Symbology-QR Code, 2000.

[8] A. Hindle, M. W. Godfrey and R. C. Holt, "Reverse Engineering CAPTCHAs," WCRE'08. 15th Working Conference, pp. 59-69, Oct 2008.

[9] *N.Saxena and H. W. James, "Authentication Technologies for the Blind or Visually Impaired," in Proc. the 4th USENIX conference on Hot topics in security, pp:7-7, Montreal, Canada, Aug 2009,.*

[10] S.Furnell, "An assessment of website password practices," *Computers and Security, vol. 26, pp. 445-451, 2007.*

[11] F. Deane, K. Barrelee, R. Henderson, D. Mahar, "Perceived acceptability of biometric security systems," *Computers and Security, vol. 1, pp.225-231, 1994.*

[12] C. Warner, J. R. Hedrick. United States Patent (NO. 6,629,591): Smart token.

[13] Melissa Walters, "Assessing password threats: implications for formulating university password policies" *Journal of Technology Research, vol.2, p1, Sep 2010.*

[14] Aviel D. Rubin, "Independent One-Time Passwords," *in SSYM'95 proceedings of the 5th conference on USENIX UNIX Security Symposium, vol. 5, pp. 15-15, 1995.*

[15] K. C. Liao, W. H. Lee, and M. H. Sung, "A One-Time Password Scheme with QR-Code Based on Mobile Phone," INC, IMS and IDC, 2009, NCM'09. Fifth International Joint Conference, pp. 2069-2071, *Aug 2009.*

[16] J. Jongpil, M. Young and C. Hyunseung, "Integrate OTP-based User Authentication Scheme Using Smart Cards in Home Networks," *in :proceeding of the 41st Hawaii International Conference on System Sciences, pp:294-294, Hawaii, United of American, Jan 2008.*

[17] X. M. Zhu, X. P. Shang, C. C. Wang, and J. R. Su, "Study on an OTP Identity Authentication Scheme in Mobile Commerce," *Journal of Computational Information Systems, vol. 6, no. 11, Nov 2010, pp. 2517-3525.*

[18] Samretwit. D. "Measurement of Reading Characteristics of Multiplexed Image in QR Code," *in: Intelligent Networking and Collaborative Systems (INCoS), pp:* 552-557, Fukuoka, Japan, Dec 2011.

[19] M. Yang, R. Zhang, and Q. Wang, "New Authentication Scheme for M-commerce Based on Two Dimension Bar Code," IEEE International Conference on Service Operations, *Beijing, pp. 1029-1034, Oct 2008.*

[20] K. C. Liao, "A Novel User Authentication Scheme Based On QR-code," *Journal of Networks, Vol.5, No. 8, Aug 2010, pp. 937-941.*

[21] Y. Lee, J. Kim, W. Jeon, and D. Won, " Design of a Simple User Authentication Scheme Using QR-Code for Mobile Device," *Information Technology Convergence, Secure and Trust Computing, and Data Management, Lecture Notes in Electrical Engineering, Vol. 180, 2012, pp. 241-247.*

[22] M. Lee, B. K. Ku, and J. B. Kim, " Easy Authentication Using Smart Phones and 2-D Barcodes," in Proc. *IEEE International Conference on Consumer Electronics (ICCE), Las vegas, NV, Jan 2011, pp. 139-140.*

[23] H. S. Al-Khalifa, " Utilizing QR Code and Mobile Phones for Blinds and visually Impaired People," in Proc. 11th International Conference, ICCHP 2008, *Linz, Austria, Jul 2008, pp. 1065-1069.*

[24] M. Tanaka and Y. Teshigawara, " A Method and Its Usability for User Authentication by Utilizing a Matrix Code Reader on Mobile Phones," *in Proc. WISA'06 proceedings of the 7th international conference on information security application, Jeju Island, Korea, pp. 225-236, Aug 2006.*

[25] Y. G. Kim and M. S. Jun, " A design of user authentication system using QR code identifying method," *in Proc. 6th International Conference on Computer Sciences and Convergence Information Technology (ICCIT), Seogwipo, Korea, pp. 31-35, Nov 2011.*

[26] Y. K. Huang, Y. W. Kao, H. T. Lin, and S. M. Yuan, *"Physical Access Control Based on QR Code," in Proc. International Conference on Cyber-Enabled distributed Computing and Knowledge Discovery, Beijing, China, pp. 285-288, Oct 2011.*

[27] J. F. Weng, "The Study of RSA Algorithm on QR Code Design," *M.S. thesis, Dept. Computer Sci. Eng., Tatung University, Taiwang. 2008.*

[28] M. X. Li, Z. X. Ping, K. Feng, and W. P. Zhu, "Matrix barcode authentication scheme based on public key cryptosystem," *in Proc. 2ed International Conference on Applied Robotics for the Power Industry (CARPI), Zurich, Switzerland, pp. 696-698. Feb 2012.*

[29] C. L. David, C. M. Enrique, J. G. Francisco, and G. C. Felipe, " Secure eTickets Based on QR-Codes with User-Encrypted Content," *in Proc. IEEE International Conference on Consumer Electronics (ICCE), Las vegas, NV, Jan 2010.*

[30] T. G. Michael, S. Michael et.al, "Loud and Clear: Human-Verifiable Authentication Based on Audio," *in Proc. 26th IEEE international Conference on Distributed Computing Systems (ICDCS'06), p. 10, Jul 2006.*

[31] C. Soriente, G. Tsudik and E. Uzun, "HAPADEP: human-assisted pure audio device paring," *in Proc. 11th information security conference, Taipei, Taiwan, pp. 385-400, Sep 2008.*

[32] S. Shirali-shahreza, "Spoken captcha: A captcha system for blind users," *in Proc. Computing, Communication, Control, and Management, Sanya, China, pp.221-224, Aug. 2009.*

[33] T. L. Chang, "Captcha based one-time-password authentication system," Master's Thesis, Graduate Institute of Information Engineering. Feng Chia University, Taiwan, Jul 2006.

[34] C. M. Leung, " Depress Phishing by CAPTCHA with OTP," *in Proc. 3rd international conference on Anti-counterfeiting, security, and identification in communication, Hongkong, China, pp. 187-192.*

[35] P. K. Yuen, Practical Cryptology and Web Security, England: Addison Wesley Longman, 2005. [E-book]. *Available through: British Library www.Pearsoned.co.uk/yuen [Accessed: 12 Dec 2010*].

[36] W. Stallings, Cryptography and network security: principles and practice, 4th ed. Prentice Hall, 2006.

[37] R. Javidan, and M. A. Pirbonyeh, " A New Security Algorithm for Electronic Payment via Mobile Phones," *in Proc. 3rd International Symposium on Applied Sciences in Biomedical and Communication Technologies (ISABEL), Rome, Italy, pp.1-5, Nov 2010.*

[38] S. Shiuhpyng, "网络安全-理论与实务," 第5章 公开金匙密码系统. [online]. Available: http://140.113.210.231/ssp/2010-Spring-NetSec-book/Chap05.pdf. (Chinese version) [accessed: 01-June-2012].

[39] A. K. Lenstra and E. R. Verheul, "Selecting cryptographic key sizes," Journal of Cryptology, 14(4):255293, 2001.

[40] D. Boneh, "Twenty years of attacks on the RSA cryptosystem", *Notices of the American Mathematical Society (AMS), Vol. 46, No. 2, pp. 203--213, 1999.*

[41] G. J. Simmons, "Symmetric and asymmetric encryption," *ACM Computing Surveys, volume 11, Issue 4, pp. 305-330, 1979.*

[42] Inga. Martin D, "Biometric Security Systems Fingerprint Recognition Technology," *PH.D. Dissertation, Dept. Computer Sci. Eng., Brno University of Technology, Czech Republic, 2005.*

APPENDIX

Appendix

Published papers

KKU-IENC2012

"Driving Together Towards ASEAN Economic Community"

May 10-12, 2012

Kosa Hotel Khon Kaen, Thailand

Proceedings

The 4th KKU International Engineering Conference 2012

Agricultural Machinery and Postharvest Technology Research Center

EMCO

AERD-KKU

IEEE

THAILAND SECTION

turnitin

Paper: H12_044

The 4th KKU International Engineering Conference 2012 (KKU-IENC 2012)
"Driving together towards ASEAN Economic Community"
Faculty of Engineering, Khon Kaen University, Thailand, May 10-12, 2012

A Design of OTP-based Authentication Scheme for the Visually Impaired via Mobile Devices

Li Longhua[1] Suntorn Witosurapot[2]
[1]Department of Computer Engineering, Faculty of Engineering, Prince of Songkla University,
Hatyai, Songkhla 90110
E-mail: lhlee0929@gmail.com
[2]Department of Computer Engineering, Faculty of Engineering, Prince of Songkla University,
Hatyai, Songkhla 90110
E-mail: wsuntorn@coe.psu.ac.th

***Abstract*—The most common approach for authenticating a computer user is done by means of username and password. However, when working on the mobile phone environment, this approach is inversely unsuitable for the visually impaired that may have low level of computer skilled. In this paper, we argue that a suitable authentication protocol can be designed in a friendly manner. Regarding this, we advocate the use of One-Time-Password (OTP) protocol for enhancing password-based authentication for the visually impaired, but demanding some extra mechanism (such as those of audio-based CAPCHA schemes) to be included in the verification process so that it cannot be interfered by maliciously robotic attacks. We discuss such a desired OTP-based authentication in this paper, which combines the use of a) one-time validation with OTP protocol, b) encryption/decryption on the secret information with QR-code algorithm, and c) audio-based CAPCHA playback with local Text-to-Speech (TTS) engine. This would be contributed to the design of authentication for the visually impaired on mobile device, which is capable of preventing the anti-robotic attack problem in an efficient manner.**

Keywords: Authentication for the visually impaired; OTP; QR-code; CAPTCHA.

I. INTRODUCTION

With the advance of computer network technology, it becomes easy now to connect mobile devices (such as smart phones) to computers by means of wireless links, either for the intent of sharing the information or gaining the access through the Internet. In such scenarios, it is usual that some authentication mechanism must be involved for verifying the mobile device's user whether they are authorized or not. While the password-based authentication scheme is likely to be implemented due to its simplicity and popularity, it is considered inadequacy for security [1, 2], due to the static password inputted by users during the authentication process.

In order to mitigate the deficiency of static password, many solutions have been proposed in the Internet. However, the solutions [3, 4, 5] relying on the mechanism of One-Time Password (OTP) is particularly interested, due to the salient feature that enforces different passwords to be used for each time of authentications. By working in this manner, it is claimed to be efficient for avoiding various shortcomings associated with traditional static password, such as Replay attack, Dictionary attack, and Phishing attack. Nevertheless, these solutions are still incapable of anti-robotic-attack. As a result, when they are accommodated for the password-based authentication, those login processes can be then easily interfered by some malicious programs, e.g. sending some faked requests and responses periodically with the attempt to degrade the server's performance (hence, it is also known as the robotic attack problem).

In order to mitigate the weakness of lacking the anti-robotic-attack of OTP described above, the audio based CAPTCHA mechanism seems to be applicable for identifying whether or not the being interacted user is a legitimate (visually impaired) human. However, to obtain the adequate level of security, we argue the combination of these two user authentication mechanisms that are OTP and audio-based CAPTCHA but still inadequate, unless some mechanism for "Device Authentication" (e.g. Mobile's Subscriber Identification Module (SIM) number [6] or QR-Code [7]) is exploited. In this paper, by working towards this direction, we propose a design of authentication for the visually impaired that by using the common equipment of mobile phone with local Text-to-speech (TTS) engine and the QR-code technique for the mobile users, who are visually impaired and may have the low level of computer skill.

The rest of this paper is organized as follows. In section II, we give some background information about protocol and mechanisms concerned in our design. In section III, we summarize the related works in the literature. In section IV, we describe the full information about our design proposed in this paper, following with the analytical security with other authentication schemes in section V. Finally, we conclude the paper in section VI.

II. BACKGROUND INFORMATION

A. One-Time Password (OTP)

OTP [8] is a well-known mechanism for generating random and dynamic of password with some cryptographic algorithm in such a way that it will be only available for one time. Therefore, the OTP is invulnerable to replay attack and sniffing. In addition, it is also proof against prediction of a possible password in use for next time from the one currently being used. This can solve a lot of problems occurred by using static password chosen by users. Factors that can be used in OTP generation are names, time, seed, etc. As we known that the two of the most popular authentication systems using OTP are Secure ID and S/KEY [9]. The Secure ID is a hardware solution, while the S/KEY works in software way. Both of them have advantages and disadvantages, so make what to use depend on user's decision.

B. QR-Code (Quick Response-Code)

QR Code [7] is a kind of high density two-dimension barcode, which is powerful not only for encrypting much information on a small and limited district, but also decrypting the decoded content at high speed.

In this paper, we proposed to replace using extra of secure hardware and reducing the requirement of infrastructure with the widely adopted QR-code technique with mobile's International Mobile Equipment Identity (IMEI for short) on it for secured proof of the device identity in this novel authentication scheme. In addition, without using the clear original form of QR-code image so that the RSA algorithm of public-key cryptology should considers to employ into RSA QR-code to further enhance the authentication security, even the illegal user intercept it still useless for them. The greater increase the security level of authentication, the more conveniences to be easy detected and decrypted for the visually impaired during the access of computers through some mobile devices. The QR-code encoding and decoding diagram is shown in Figure 1.

Figure 1. QR-code encoding and decoding processes.

C. Audio-based CAPTCHA (Completely Automated Public Turing tests to tell Computers and Humans Apart)

The CAPTCHA [10] is a simple mechanism which is often used to prevent automated "bot" from login procession or registry account. It seems to be applicable for identifying whether the being interacted users are legitimate (visually impaired) humans or not. However, it is suitable in our usage scenario, where the user is visually impaired person and therefore, the audio version of CAPTCHA is preferred (see Figure 2.) in our scheme which through the local TTS engine in mobile device to covert the successful decrypted of secret OTP key into digit numbers which required visually impaired user to listen and then to press the key number for obtain the given services or resources in order to guarantee human users are being interacted which can prevent anti-robotic attack from it.

Figure 2. An example of audio-based CAPTCHA with noise background to differentiate human with robot's interaction.

III. RELATED WORKS

As discussed in the previous section, password based authentication schemes are still not enough to reinforce the level of security for user authentication, especially in the ubiquitous computing environment with mobile devices. So a possible approach can be that of mutual authentication, which combine the use of mechanisms for user authentication and device authentication altogether.

With the popularity of QR-code, many authentication schemes working based on QR-code with OTP have been proposed. Yang's "Two-way Authentication by Two-dimension barcode and OTP" (TABTO for short) [11] provides a new OTP authentication method based on the two-dimension barcode and adapts it into M-commerce environment. It takes the counter which contains the information has the increased counter for next round of authentication as the important factor of authentication so that the password doesn't need to preserve directly in the database of server. It uses the IMEI as the secret information. It can not only provide the mutual authentication between the server and user, but also resist the man-in-the-middle attack. M. Tanaka's secure user authentication with nijigen code (SUAN for short) [12] "Nijigen" (In Japanese means two dimension) code. It provides a new authentication method which can reduce the troubles come from phishing and eavesdropping attack. Some advantages are established on this method: (1) High rate of installation 2D barcode reader and popularity of use in Japan. (2) More secure working on the carrier network than public open network.

In [13] Liao and Lee's "A Novel User Authentication Scheme Based on QR-Code" (AUSQ for short) makes use of the deployed widespread QR-code techniques in order to eliminate the drawbacks of the prior one-time password schemes. It is the first to propose a QR-code based one-time password authentication protocol, which not only eliminates the usage of the password verification table, but also is a cost effective solution since most cyber users already hold mobile phones.

The RSA cryptographic algorithm based on QR-code is also found in the literature. Huang and Yuan in [14] proposed a RSA encryption algorithm with OTP to be used as a security authentication scheme for preventing illegal user to access, modify and copy service contents. It can be

applied to many services of required authentication. Weng in [15] proposed a 2D barcode integrate with the cryptology of RSA algorithm on public-key cryptography which employed into RSA QR-code to fulfill a guide system. This method can not only enhances the security of the information, but also enables diversified service levels for different users.

The works in [3] [4] [5] are related to the study about OTP based user authentication. Park's "OTP Authentication Module and Authentication Certificate Based User Authentication Technique for Direct Access to Home Network and Resource Management" (OAUM for short) [5] proposed a user authentication method for home network that operates on the server that is served for both authentication and service provisioning. This is contrast to many existing authentication methods. In [3], Jongpil et al., proposed to use smart cards based on one-time-password protocol as a new user authentication scheme. However, compared to our work, their work did not concern on preventing the OTP from the robotic attack problem.

Hearing (as one of the human senses) can support well to the authentication process. In [16], Michael et al., proposed "Loud and Clear: Human-Verifiable Authentication Based on Audio", by relying on the verification (by human) on the spoken language transmitted over a secure communication channel. Nevertheless, it still contains a drawback of Man-In-The-Middle (MITM) attack (also called "Fake Audio" attack).

In [17] Uzun et al., proposed "HAPADEP: human-assisted pure audio device paring", which is in similar with the Loud-and-Clear technique, but demand only one communication channel for supporting both digitized audio transmission and verification information between devices.

It is clear that all of works mentioned above ignore the anti-robotic attack issue. Therefore, they are much different to our work proposed in this paper, where some selected device authentication technique is bring to work in combination with the OTP and audio-based CAPTCHA mechanism. Details will be described in the next section.

IV. The Proposed Scheme

Our proposed scheme aims to make the use of widely deployed QR-code technique with RSA public-key cryptography algorithm to achieves the effect of the twice encryption, to combine working together with the OTP and audio-based CAPTCHA mechanism in order to eliminate the drawbacks of prior one-time password schemes. So that made our scheme can be more secure, more practical and more useful.

In our proposed scheme, it involves two parties: a remote mobile client and a main server (OTP RSA Server, ORS for short). Only authorized user can obtain the service after be successful encrypted and decrypted by mobile application (OTP QR-code Generator, OQG for short) and ORS, all of them are organized under a Public Key Infrastructure (PKI) system [18]. In addition, with the inbuilt mobile application to encode and decode QR-code image underlying RSA cryptographic algorithm, also embedded smart agent in the mobile device which means audio-based CAPTCHA. The whole authentication process of proposed scheme is shown in Figure 3. our scheme can be divided into two phases: registration and verification phases.

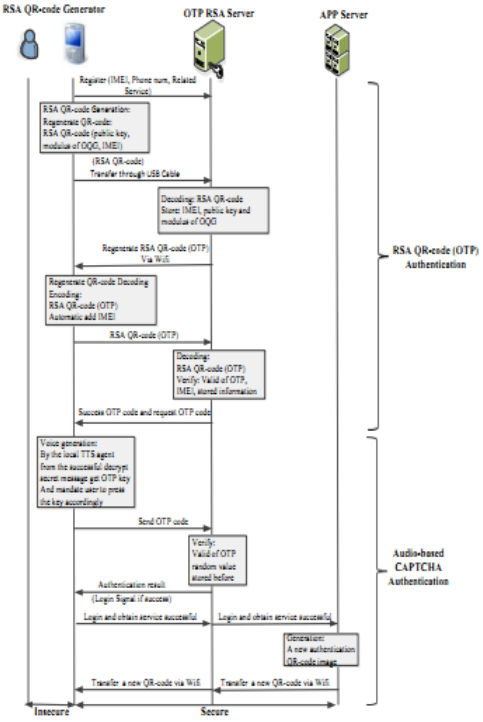


Figure 3. A proposed Authentication Scheme.

We define notation in Table 1. that will be used throughout of this paper.

TABLE 1. NOTATION

Notation	Description
$E_{QR}(.)$	QR-code encoding processing function to encode message to a QR-code image
$D_{QR}(.)$	QR-code decoding processing function to decode message to a QR-code image
$E_{RSA}(m, x)$	RSA encoding processing function to encode message m by key x
$D_{RSA}(m, x)$	RSA decoding processing function to decode message m by key x
Pub_{OQG}	Public key of OQG
M_{OQG}	Modulus of the OQG
Pri_{OQG}	Private key of the OQG
Pub_{ORS}	Public key of ORS
M_{ORS}	Modulus of the ORS
Pri_{ORS}	Private key of ORS
I	IMEI (Mobile's International Mobile Equipment Identification)
P_{NO}	Phone number
S_{ID}	Service ID of the required service

A. Phase 1: Registration phase

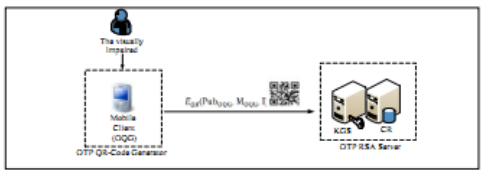


Figure 4. Mobile device sends its IMEI, public key of OQG encrypted by QR-code to the server.

Step 1: When the mobile device initiates, it registers its IMEI, P_{NO}, and required service to the OTP server as shown in Figure 4.

Step 2: Install the OQG application on the mobile.

Step 3: Use the application to generate the RSA keys and to store the private key into the database belong to OQG at first launch, finally regenerate an image of QR-code by computing the following equation (1).

$$E_{QR}(\mathrm{Pub}_{OQG}, \mathrm{M}_{OQG}, \mathrm{I}) \quad (1)$$

Step 4: ORS get the message from the decoded image of QR-code, computed by the equation (2).

$$\mathrm{D}_{QR}(\mathrm{E}_{QR}(\mathrm{Pub}_{OQG}, \mathrm{M}_{OQG}, \mathrm{I})) \quad (2)$$

Then, we can store $(\mathrm{Pub}_{OQG}, \mathrm{M}_{OQG})$ into the database relative to mobile client whose IMEI equal to I.

Step 5: QR-code is generated with OTP and secret messages from ORS through multimedia message system (MMS), compute through equation (3).

$$\mathrm{E}_{QR}(\mathrm{E}_{RSA}(S_{ID}, P_{NO}, \mathrm{OTP}), \mathrm{Pub}_{OQG}) \quad (3)$$

If the illegal users intercept and decode this secret message from wireless communication channel, they can only see the big integers, because they not have private key of the OQG.

B. Phase 2: Verification phase

Step 1: Use the mobile application OQG to generate a usable one-time password QR-code from the transfer message at ORS as shown in Figure 5. To get the secret information is computed by (4).

$$\mathrm{D}_{RSA}(\mathrm{D}_{QR}(\mathrm{E}_{QR}((S_{ID}, P_{NO}, \mathrm{OTP}), \mathrm{Pub}_{OQG}), Pri_{OQG})) \quad (4)$$

Figure 5. Mobile device sends the secret information within IMEI and OTP encrypted by a public key.

Then, OQG will add I into the secret set as the response, so that the new secret information is $(S_{ID}, P_{NO}, \mathrm{OTP}, \mathrm{I})$. Regenerate this secret information into a QR-code image for authentication as (5).

$$\mathrm{E}_{QR}(E_{RSA}((S_{ID}, P_{NO}, \mathrm{OTP}, \mathrm{I}), Pub_{ORS}) \quad (5)$$

Step 2: ORS identify and authenticate by computing is shown as (6).

$$D_{RSA}(E_{RSA}((S_{ID}, P_{NO}, \mathrm{OTP}, \mathrm{I}), Pub_{ORS}) \quad (6)$$

The procedure of decryption is shown in Figure 6. to get a plaintext, identify if this is a valid of OTP for this user by checking these information stored in the database before, after that wait for a authentication result (login signal) to enter the request OTP code.

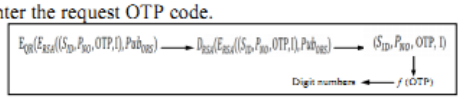


Figure 6. The Procedure of decryption at the OTP RSA Sever.

Step 3: With embedded local TTS smart agent in Audio-based CAPTCHA mechanism to convert the successful decryption of secret message about random value into a voice version of digit numbers (should less than eight digits) which is mandated by Text-To-Speech (TTS) engine and required visually impaired user to press then can obtain the services or resources as the visually impaired wants. As Figure 7. show.

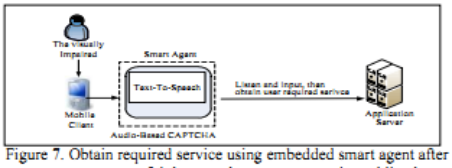


Figure 7. Obtain required service using embedded smart agent after successful decrypted secret message in mobile phone.

Step 4: After get service, then ORS generates a new QR-code image and transfers it to the mobile via wireless communication channel which is used for next authentication.

V. Analytical Security Of The Proposed Scheme

A. The security analysis of our proposed scheme

In this sub-section, we discuss the security issue which influences on our proposed scheme. In this attack approach, there are several different parts are discussed as following:

- Masquerade attack:

  Malicious mobile client: The feigned of mobile client doesn't work in deed, because it cannot successful to decode the image of QR-code, even if it intercepts one, there has no way to obtain the correct of secret key. In other words, it can't obtain any valid of information at all.

  Malicious ORS: With the protection from RSA cryptography algorithm, a fake ORS can't decode the receiving information, because it has no private key of

real ORS. In addition, a fake ORS without the ability of sending message easily with a special application.

Malicious OQG: The user needs to register the service at registration phase so a feigned OTP QR-code Generator can't receive the authentication of QR-code image via wireless communication channel. In addition, the specific of secret message was generated according to the register service and mobile phone number associate with mobile's IMEI. Not any of the QR image can be used in any OTP RSA QR code Generator, even if the message is intercepted by the illegal users are still meaningless for them.

- Replay attack: One-time password is an effective mechanism can avoid tradition static password issues. In our scheme, the certified QR-code image are all one-time validation used, even the third party grabbed the certification in our scheme through this attack is still not useful.
- Message modification attack: The role of RSA algorithm of public-key cryptology is used to protect the secret information, thereby it's useless to tamper with the encrypted message on it. The mobile client takes an active connection to ORS and it does not open a fixed port to wait for a response, therefore even an attacker attempt to destroy our scheme by this attack is very difficult.
- Man-in-the-middle attack: Even if the illegal user can intercept the transmission messages, it's useless because the secret message is encrypted by the RSA cryptography algorithm.
- Anti-robotic-attack: The audio-based CAPTCHA mechanism can be applicable for identifying whether legitimate (visually impaired) human or not, in order to mitigate the weakness of vulnerable to be interfered by some malicious computer programs on OTP based login authentication processing.

B. A comparison of authentication schemes

Previously, we have introduced lots of authentication methods in this paper, which includes TABTO, SUAN, AUSQ, OAUM and our schemes. All of them have somewhere in common and different as well. Therefore, through compare of them and give out the difference between all of them in the table 2.

In the TABTO and SUAN scheme, both of them combine to use mobile device and QR-code as authentication method also take the advantage of using carrier network, which should be more secure and more trust compare with home network. Because the carrier network for ensure the security of service and communication not directly open to the public network. In the experiment of SUAN, the time length take average between 18.3 seconds and 10.0 seconds when start authentication on the mobiles, then send authentication result back to the mobile devices.

In the TABTO and AUSQ scheme, each of them takes four times and two times to communicate separately between client and server in the authentication and verification procedure. For TABTO scheme, two times for updated 2D bar code transmission and the other two times for transmission the result value after computing, while for AUSQ scheme, one times for store secret key from server, anther one for compute and derive by one way hash function.

In the OAUM scheme by use of user authentication method for authenticates user and provides service directly through the home server of home network, each time to transfer the data always after be encoded with the mutual time synchronization method between OTP module and home server to generate a random parameter.

TABLE 2. COMPARSION OF RELATED AUTHENTICATION SCHEMES

	Our proposed	TABTO	SUAN	AUSQ	OAUM
Authentication Method	RSA OTP QR-code	QR-code Counter based OTP	Nijigen code	QR-code Time based OTP	X 509 v3-based Certificate
Device Authentication	Yes	Yes	No	Yes	Yes
Access Control	Yes	Yes	No	Yes	Yes
Anti-Robotic Attack	Yes	No	No	No	No
Network for Authentication	General network	Carrier network	Carrier network	Carrier network	General network
Communication times each authentication	2	4	6	2	4
Encryption algorithm	RSA	Hash function	Hash function	Hash function	Symmetric key
Mutual Authentication	Yes	Yes	No	Yes	Yes
Authentication times	≤10 s	N/A	Average 18.3 s-10 s	N/A	N/A

It can be seen that our scheme is comparable to the other work, but is dominant at the feature of Anti-Robotic Attack. This is due to the exploit of the audio-based CAPTCHA mechanism for allowing the human-verification to be occurred over the same communication network. As a result, it can take less time than the other schemes, where the other network (such as the GSM carrier network for general mobile phones).

VI. CONCLUSIONS

In this paper, an authentication mechanism for visually impaired users with the mobile phones has been presented. It works mainly on the OTP protocol, but includes device authentication techniques (QR-code and Mobile's IMEI) and audio-based CAPTCHA mechanism for handling the Anti-robotic-attack problem in the efficient manner. Hence, it demands for some text-to-speech engine to be existed in the mobile phone and visually impaired users to be followed the numbers under the mandate and pressed them accordingly.

REFERENCES

[1] L. Lamport, "Password authentication with insecure communication," Communications of ACM, Vol. 24, No.11, pp. 770-772, Nov 1981.
[2] T. Tsuji, and A. Shimizu, "Simple and secure password authentication protocol ver.2 (SAS-2)," IEICE Technical Report, OIS. 2002-30, Vol. 102, No.314, September 2002.
[3] J. Jong, M. Y. Chung, and H. S. Choo, "Integrated OTP-based User Authentication Scheme Using Smart Cards in Home Networks," Proceeding of the 41st Hawaii International Conference on System Sciences, Hawaii, USA, pp. 294–313, Jan 2008.
[4] W. B. Hsieh, and J. S. Leu, "Design of a time and location based one-time password authentication scheme," 7th International wireless communications and Mobile Computing Conference (IWCMC), pp. 201–206, 12 Aug 2011.

[5] J. O. Park, and S. G. Kim, "OTP Authentication Module and Authentication Certificate Based User Authenticating Technique for Direct Access to Home Network and Resource Management," International Journal of Smart Home, Vol. 4, No. 3, July 2010.
[6] Y. R. Tsai and C. J. Chang, "SIM-based subscriber authentication mechanism for wireless local area networks," Computer Communication, Vol. 29, No. 10, pp. 1744-1753, 2006.
[7] Denso Wave Inc. QR Code.com (http://www.qrcode.com)
[8] A. Fadi, and Z. Syed, "Two Factor Authentication Using Mobile phones," Internation Conference on Computer Systems and Applications, AICCSA, pp.641-644, May 2009.
[9] H. Neil, "The s/key(tm) one-time password system," Symposium on Network and Distributed System Security, PP.151-157, Feb 1994.
[10] A. Hindle, M. W. Godfrey and R. C. Holt, "Reverse Engineering CAPTCHAs," WCRE'08. 15th Working Conference, pp.59-68, Oct 2008.
[11] M. Yang, R. Zhang, and Q. Wang, "New Authentication Scheme for M-commerce Based on Two Dimension Bar Code," IEEE International Conference on Service Operations, Beijing, pp. 1029–1034, Oct 2008.
[12] M. Tanaka, and Y. Teshigawara, "A Method and Its Usability for User Authentication by Utilizing a Matrix Code Reader on Mobile Phones," Workshop on Information Security Application (WISA), Vol. 4298, pp. 225–236, Aug 2006.
[13] K. C. Liao, and W. H. Lee, "A Novel User Authentication Scheme Based on QR-Code," Academy Publisher, 2010, pp. 937–941.
[14] Y. K. Huang, and S. M. Yuan, "Physical Access Control Based on QR Code," International Conference on Cyber-Enabled distributed Computing and Knowledge Discovery, Beijing, China, pp. 285–288, Oct 2011.
[15] J.F. Weng, "The Study of RSA Algorithm on QR Code Design," Master degree.Tatung University, 2008.
[16] T. G. Michael, S. Michael et.al, "Loud and Clear: Human-Verifiable Authentication Based on Audio," in: proceedings of the 26th IEEE international Conference on Distributed Computing Systems (ICDCS'06), pp.10-10, Jul 2006.
[17] C. Soriente, G. Tsudik and E. Uzun, "HAPADEP: human-assisted pure audio device paring," in: 11th information security conference, pp.385-400, 2008.
[18] W. Diffie, and H. Martin, "New directions in cryptography," IEEE Transactions on Information Theory, vol. 22, Issue 6, PP. 644–654, Nov 1976.