A Secure Mobile Payment Framework Based On Face Authentication

Zhaomiao Xu, Tao Zhang, Yujun Zeng, Jia Wan, Wuyang Wu

***Abstract*—With the increasing market share of the smartphone, more and more people use m-payment (mobile payment) to pay for something in their daily life. In this paper, a brand new m-payment framework which based on face authentication is proposed after studying existing m-payment security frameworks. On the basis of traditional password authentication technology, this new face authentication based framework applies biological characteristics to ensure users' privacy. In technical level, it uses semi-3D vertical recovery technology and face feature extraction method which cope with 2D-PCA (two dimension principal component analysis) to verify users' face image. Besides, this framework applies a third-party to guarantee the legitimacy of the transaction process.**

***Index Terms*—m-payment, third-party guarantee to pay, 2D-PCA, face authentication**

I. INTRODUCTION

In September 26, 2013, "User research report of China mobile banking, 2013" released. The report shows users who preferred m-payment accounted for 46.97%, which slightly lower than the proportion of the PC, and the amount of users is growing rapidly. Thus, m-payment is a big trend, but for now, users' habit of using m-payment is still in training.

Manuscript received December 25, 2014; revised January 17, 2015. This research project was supported by National Undergraduate Training Programs for Innovation and Entrepreneurship of China (Program No. 201410699083). This research project was funded by NWPU.'S Key Graduation Design of Undergraduate on Bank Identity Verification System Based on Face Recognition.

Zhaomiao Xu is with School of Software and Microelectronics, Northwestern Polytechnical University, 127 West Youyi Road,Xi'an Shaanxi,710072,P.R.China (corresponding author to provide phone: 18792743581; e-mail: threewaterxzm@gmail.com).

Tao Zhang is with School of Software and Microelectronics, Northwestern Polytechnical University, 127 West Youyi Road,Xi'an Shaanxi,710072,P.R.China (corresponding author to provide phone: 159991789828; e-mail: tao_zhang@nwpu.edu.cn).

Yujun Zeng is with School of Software and Microelectronics, Northwestern Polytechnical University, 127 West Youyi Road,Xi'an Shaanxi,710072,P.R.China (corresponding author to provide phone: 18591986062; e-mail: zyj1994210@gmail.com).

Jia Wan is with School of Software and Microelectronics, Northwestern Polytechnical University, 127 West Youyi Road,Xi'an Shaanxi,710072,P.R.China (corresponding author to provide phone: 18740408875; e-mail: 554928577@qq.com).

Wuyang Wu is with School of Software and Microelectronics, Northwestern Polytechnical University, 127 West Youyi Road,Xi'an Shaanxi,710072,P.R.China (corresponding author to provide phone: 18792561764; e-mail: 937284436@qq.com).

People have done many investigations on the factors that influence uses' acceptance of m-payment, in many factors, safety is selected as the safety is the one that is worth most consideration [6-9]. There are two major m-payment risks currently, one of them is network data of mobile communication being captured, and another is verified path being uploaded [10].

At present, m-payment can be divided into near-field payment and remote payment. Near-field payment includes RFID-based m-payment framework and NFC-based m-payment framework. Currently, near-field payment is not popular and has limited use. Its protection of non-encrypted information in case of non-contact is still not efficient. Even more, some attackers transform NFC-enabled phone to a POS terminal in order to trade with non-contact card, which is similar to Portugal's NFC phone modes POS for frauds [17]. Meanwhile, there are lightweight m-payment protocols, third-party based m-payment frameworks and biometrics based m-payment frameworks in remote payment [4]. Some non-biometrics based frameworks always have a simple process, which easily causes data leakage or authentication errors. However, current biometric-based frameworks are not mature. It is hard for an immature framework to protect users' property. On the contrary, once safety and accuracy of a biometric-based framework can be guaranteed, the efficiency of payment will be greatly improved.

There are mainly two improvements in this new framework. First, it proposes a new m-payment framework which applies both face authentication and third-party supervision thoughts which combined the advantages of both. Second, in this paper, face authentication technology and m-payment security research are combined. According to the feature of m-payment, this paper makes some improvements on face authentication technology which make the efficiency and the accuracy of face authentication algorithm can meet requirements.

To be discussed later of this paper in the following aspects. The second part describes some related research. In the third part, our framework will be proposed. In the fourth part, m-

ISBN: 978-988-19253-2-9
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

payment face authentication algorithm will be introduced. Then, the fifth part will discuss the verification of this algorithm's reliability. The sixth part will validate the proposed framework. Last, there will be a conclusion in the seventh part.

II. Related work

At present, m-payment can be divided into near-field payment and remote payment. When it comes to remote-payment, it can be divided into biometric based remote m-payment framework and non-biometric based remote m-payment framework according to whether it uses biological characteristics to authenticate. The following contents will describe some related work from these three aspects.

1) Near-field payment. Reference [3] proposed RFID-based m-payment system, it injects RFID information card into mobile to ensure the authenticity of the registration information. However, RFID is not universal and it cost a lot to popularize this system. NFC technology combined with CDC (Citizen Digital Certificate) is proposed in [5]. To improve safety performance, this framework uses PKI (Public Key Infrastructure) to encrypt information. However, this framework is NFC functionality required and its process is tedious.

2) Biometric based remote m-payment framework. Reference [11] proposed a biometric based secure m-payment framework. It gathers fingerprint recognition technology, WPKI (Wireless Public Key Infrastructure) and UICC (Universal Integrated Circuit Card) to ensure the confidentiality of the transaction process. However, it's based on fingerprint recognition which made it requires mobile devices possess fingerprint function. At present case, most mobile devices have difficulty to have this feature which made it hard to promote. An android-based m-payment service protected by 3-factor authentication is proposed in reference [13]. This services use text authentication, card authentication and face authentication as its key factors to verify users' identification. But it requires the use of specific USIM card (USIM card) to authenticate users, which limits the promotion of this service.

3) Non-biometric based remote m-payment framework. In order to take care of mobile performance, improve the efficiency of the program, reference [1] proposed a lightweight m-payment protocol based on symmetric encryption. This protocol takes into account the performance of the phone, and enhances the enforceability of the program. However, it reduces the security of m-payment. Reference [2] abandons the traditional Client - Bank - Customer payments and proposed a brand new third-party based m-payment model. However, in its proposed model, it fails to propose a suitable authentication mechanism.

Based on the above work, this paper proposes a secure mobile payment framework based on face authentication.

III. M-payment security mechanism

Confidentiality, authentication, integrity and non-repudiation are the most critical four factors for m-payment. To meet these four requirements, proposed framework in this paper is based on following assumptions.

1) Assuming a third-party supervision agency has reached an agreement with banks that third-party has rights to call the users' bank card number CardId and saves user transaction information. In this way, feasibility of this framework can be improved.

2) Assuming the all the interactive data was encrypted based on symmetric encryption mechanism.

3) When there are data exchanges in each part of the system, to ensure the timeliness of data, a timestamp will be added to the data packet. It is used to prevent replay attacks.

A. Mobile Payment Security Framework

As is shown in Fig 1, proposed framework is composed of three parts: mobile client, server-side and transaction interface.

1) Mobile client. As an application is needed to accomplish users' operation, it is marked as client app and merchant app in Fig 1. These two apps are used to implement the payment process, thus they have the same software architecture. The architecture is showed in Fig 2.

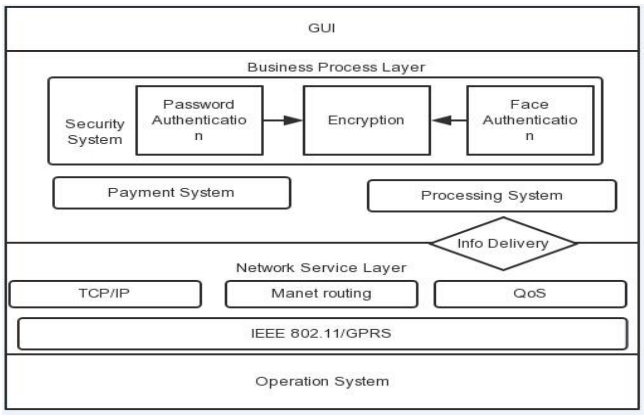

Fig 2. Software Architecture of Mobile Client

ISBN: 978-988-19253-2-9
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

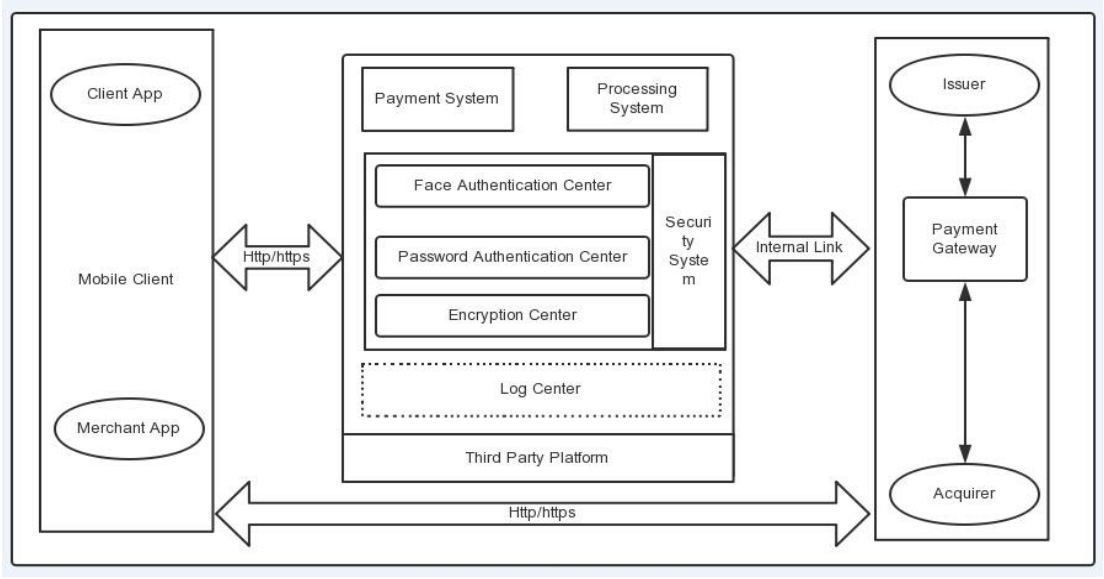

Fig 1. System Framework

As shown in Fig 2, mobile client software is divided into four layers, namely, the underlying operating system, network service layer, business process layer, GUI interface presentation layer. Among them, operating system provides the underlying support for the realization of software. Network service layer provides interfaces which have the ability to connect with outside world for software. Simultaneously, there is information exchange between network service layer and business process layer. Business process layer includes three main parts, payment systems, security systems, logic systems. Payment system is related to payment functions and its work is directed by logic system. At the same time, to complete payment process, it need to cooperate with security system. Security system is responsible for encryption, user authentication and user account authentication. Last, GUI is responsible for interacting with users.

2) Server-side. As shown in Fig 1, third-party agency composed of the server-side of proposed framework. It is used to response to user actions, complete a variety of requests and give feedbacks. Payment system, processing system, security system and log center is included in server-side. In order to ensure the security of m-payment framework, security systems including face authentication center, password authentication center and encryption center.

3) Transaction interface. As is shown in Fig 1, it is consisted of issuer, acquirer and payment gateway. It is used to complete users' financial transactions.

In the proposed m-payments framework, the most core elements is the payment function. Structure of mobile client payment function is showed in Fig 3 and mobile server side payment function is showed in Fig 4.

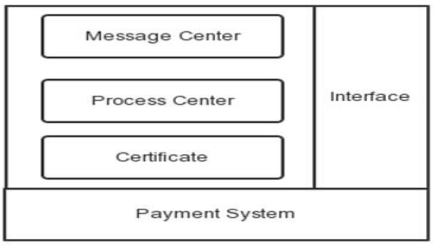

Fig 3. Structure of Mobile Client Payment Function

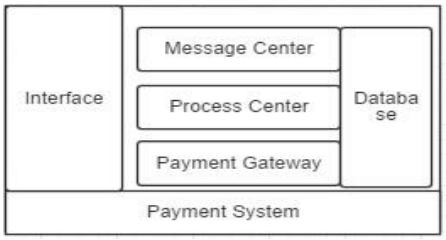

Fig 4. Structure of Server-Side Payment Function

As is shown in Fig 3, mobile client payment system consists of four parts, message center, process center, certificate center and interface. Among them, message center is used to transmit information with the outside. Process center is responsible for parsing and dealing received information. Certificate is a certification mark of software and it's used to verify users' identity. All the results will interact with the outside world via the interface. As is shown in Fig 4, server side payment function consists of five parts, message center, processing center, payment gateway, interface and database. Among them, message center, processing center and interface's function is as same as what they are in mobile client. Payment gateway is used to interact with bank which enables funds circulation and normal execution of the transaction. Last, database responses for storing customer information and interaction information.

ISBN: 978-988-19253-2-9
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

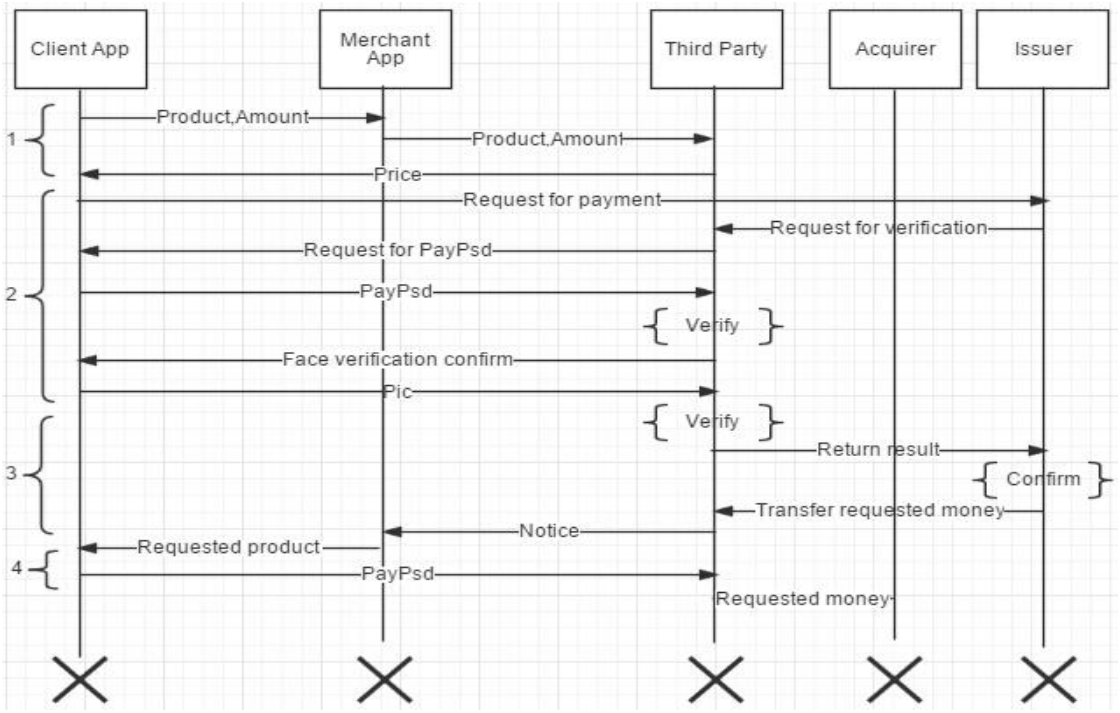

Fig 5：Payment Process

B. Mobile Payment Security Processes and Interfaces Design

Proposed framework added the idea of face authentication to ensure the security of user account [12]. Simultaneously, a third-party supervision agency is added to operate users' property. In the condition that the user has used Uname and Psd login system, payment process of this proposed framework is shown in Fig 5.

1) A client finds what they need, and confirms the order to the merchant. Once the merchant received an order from client, he need to send the order to third-party supervision agency, the order is consisted of commodity name, unit price, amount and so on. After a third-party verification, the total price will be sent to the client.

2) After the client receiving and verifying the total price, a payment password PayPsd should be provided by client. Once payment password is verified by third-party, a request from third-party for face image will be sent to client. In this case the client needs to open the camera immediately and shoot face image Pic. Then, Pic will be upload to third-party

For the convenience of mobile applications integrates and calls face authentication technology mentioned in this framework, 4 necessary API interfaces are shown in Table I. and waits for authentication.

3) Once the face authentication and password verification is confirmed, issuer will transfer required payment amount in this transaction to third-party's account. Then, third-party will send a receipt notification to merchant which notice the merchant to deliver the client's commodities.

4) Once client receives the commodity of online shopping, a confirmation should be given to third-party. Then, third-party will transfer required payment amount to acquirer. At this point, the transaction ended.

Table 1：Necessary API for Face Authentication

API Name	Function Description
Face Detection API	Detect human faces in images, then the detected face will be marked
PCA Processing API	Do 2DPCA to existing data
Face Matching API	Compare two processed face images
Grayscale Conversion API	Put color image convert into gray images

IV. Face Recognition Algorithm

A. General Description of Algorithm

In order to improve the accuracy of face authentication and reduce FAR, proposed algorithm takes three steps to

ISBN: 978-988-19253-2-9
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

achieve this goal.

1) When the mobile device is acquiring face images, various factors like shooting angle and camera shake will results in face is not parallel to the camera during shooting. At this point, the photo effect will greatly affect the accuracy rate. So, a semi-3D vertical pose recovery technology is applied in this framework to make the face images become vertical and parallel to camera [13]. It is presented clearly in [13] and here will not elaborate it again.

2) On the basis of a vertical face images, use feature extraction method [16] to obtain human being's face feature, such as eyes, nose, lips and so on. After obtaining the facial feature vector, they should be added to sample to increasing the dimension of the sample space.

3) On the basis of the above two steps, use 2DPCA to deal with face images to obtain its projection matrix. Then, use this matrix to make dimension reduce of the whole sample space. Last, an eigenvector of the images will be obtained, which can help us to verify users.

B. Feature Extraction Method

A combination of gray feature and face feature is proposed in this paper. Add the position between the eyes, the width of the lips and some other features to sample space will increasing the dimension of the sample space [16].

The first step of extract facial features is seeking the second derivative of the gray scale image.

$$d(x,y)=\sum g(x+i,y+j)-9g(x,y) \quad i,j=-1,0,1 \qquad (1)$$

Then, binaries the gray scale image. According to the projection histogram of each line to obtain the position of eyes, mouse and other features. For example, projection histogram of human eyes is shown in Fig.6.

Fig.6: Projection Histogram of Human Eyes

By analyzing projection histogram, a q-dimensional facial feature vector can be obtained. It will be added to sample space and then have a 2DPCA operation to get the whole sample space's projection matrix.

C. 2DPCA

The basic idea of using 2DPCA to identify face is that in a m*n image matrix A,making X be an n-dimensional unit of the column vector, projecting the image matrix A to the X through linear transformation $Y = AX$. Then, we get an m-dimensional column vector Y and we call it as the projection eigenvector of A [14-15].

Assuming that our training samples have c classes (containing c different pictures of people): $w_1,\ldots,w_n$, each training sample contains n_i pictures, $A1, A2, \ldots A_M \left(M=\sum_{i=1}^{c} X_i \right)$ stands for the whole training images, each sample's image can be expressed in a m*n matrix. Then the overall scatter matrix G of samples is:

$$G_t=\frac{1}{M}\sum_{i=1}^{M}\left(A_i-\overline{A}\right)^T\left(A_i-\overline{A}\right) \qquad (2)$$

In this formula $\overline{A}=\frac{1}{M}\sum_{i=1}^{M}A_i$ is the average of all training samples. It's easy to prove that G_t is n-dimensional non-negative definite matrix. The Criterion function is

$$J(X)=\frac{X^T G_t X}{X^T X} \qquad (3)$$

According to relative matrix knowledge, G_t has orthogonal unitized eigenvectors. Assuming $G_i X_i=\lambda_i X_i$,and $\lambda_1\geq\lambda_2\geq\cdots\geq\lambda_n\geq 0$. Then the best projection eigenvector $X_1,\ldots,X_d$ can be the orthogonal unitized eigenvectors when G_t get d largest eigenvalues. Making $P=[X_1,\ldots,X_d]$, then P is the best projection matrix.

Projecting the face image to be identified W onto the feature space and principal component vector. At the same time, we project the face image stored in the system to the feature space and principal component vector too.

Table II: Experimental Data of Face Identification

Threshold	Recognition Rate	False Reject Rate	False Accept Rate
0.6	99.2%	0.8%	17.4%
0.7	97.3%	2.7%	12.8%
0.8	95.6%	4.4%	4.7%
0.9	91.9%	8.1%	0.3%

After getting the projection matrix, add q facial characteristic dimension into samples feature space and get d+q dimensional feature space. While verification, treat the unverified images in the same way and gain their eigenvectors and facial features dimensions. Then compare these data with information stored in sample feature space.

ISBN: 978-988-19253-2-9
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

D. 2DPCA Face Authentication

In this m-payment framework, face authentication is used to verify users. Thus, we only need to judge if the people who upload the photo is the user whose information has already been stored in our system. Through the method mentioned before, we could combine two feature vectors and get the Euclidean distance D $D = \sqrt{\sum_{i=1}^{d+q} (x_i - y_i)^2}$ （4）

D is the threshold of verification. When D stays in a specific range, the framework determine the identity authentication. On the contrary, authentication fails.

V. Verification Experiment

In the experiment, we tested the stability and efficiency of the algorithm by using 40*10 photos in orl face database. According to the principle made by the framework, we selected one photo from each different face images and compared it with the rest nine photos. Meanwhile, we set the threshold to 0.6 that stood for successful recognition at the beginning with 0.1 plus every time later. Since when the threshold is 1 two images are the same, there is no need to set the threshold to 1. Thus, the threshold in the testing should range from 0.6 to 0.9. The table below shows three types of referenced date gained in different situations.

According to Table II, following the increasing of threshold, the Recognition Rate and the False Accept Rate will decrease and the False Reject Rate will increase. We hope to diminish the False Accept Rate in the framework since a framework can't guarantee it's security if it isn't able to identify the difference between two users. At the same time, because of the need of diminishing the False Accept Rate, the False Reject Rate will rise. Considering when people fails to pass the verification, they could verify again, we allow this diminishment even though it seems inconvenient, since it's good for security.

According to the above analysis, the security and efficiency of the framework can be guaranteed when the threshold is set to 0.9. So this framework could be used.

VI. Security Threat Analysis

This part will elaborate the security and availability of the framework by considering two aspects: the advantage of Face Authentication and resistance of framework when facing common attack.

A. The Advantage of Face Authentication

There are three major methods to authenticate identity: identifying through private information such as password; identifying through private things such as ID; identifying through physical feature, such as face or fingerprint [11]. Traditional authentications need private information or specific possession to make the judgment. However, information like password or things like certifications could easily lose. Thus, framework has difficulties in ensuring the person is a user himself. Because of these deficiencies in the traditional authentications, we started to consider the possibility of using physical feature in authentication.

In the biometric-based m-payment frameworks, there are some mature technologies such as the face authentication, the fingerprint authentication, the iris authentication, etc. However, the fingerprint authentication and the iris authentication need specific equipment to collect biological information. While it's almost impossible currently to add these devices into mobile terminals, most mobile terminals possess a good camera. Thus, the face authentication is much easy to spread.

According to the above analysis, the face authentication has the following advantages：

1) Can't be duplicated. There is litter possibility of illegal verification.

2) Can easily spread. Current mobile devices ensure that m-payment based on face authentication could be availed widely.

3) Have high precision. The algorithm of face authentication based on semi-3D and 2DPCA could retain the Identified Rate in a relative high level. At the same time, it will also decrease the Misidentified Rate.

B. Resistance Under Common Attack

There are three common attacks in m-payment, which includes replay attack, disguised attacks and Man-in-the-Middle attacks. Proposed m-payment framework in this paper will have an effective resistance for different attacks. The following content will focus on the analysis of proposed m-payment framework's ability to resist common attacks.

1) Replay attacks. If an attacker keeps sending a valid date on purpose, the framework could detect and boycott the attack according to the delivery time in the timestamp contained in packet.

2) Disguised attacks. When an attacker tries to simulate a users' operation, the third-part will verify the identification through camera and forestall the attack.

ISBN: 978-988-19253-2-9
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

3) Man-in-the-Middle attacks. When attackers try to steal users' information through the Man-in-Middle attack, the third-party oversight institution will verify the certification in the m-payment before authorizing the operation. Since attackers are difficult to get the certification form hardware, the attack could be prevented.

VII. Conclusion

This m-payment framework has high-level security and efficiency. However, because of the complication in the technology and the disturbance from circumstance, the accuracy and efficiency will be influenced to the extent when users take photos at different direction or under different lights. Thus, after the construction of the framework, our group will further explore the face authentication algorithm in order to increase the framework's stability and accuracy.

References

[1] Fun T S, Beng L Y, Likoh J, et al. A lightweight and private mobile payment protocol by using mobile network operator[C]//Computer and Communication Engineering, 2008. ICCCE 2008. International Conference on. IEEE, 2008: 162-166.

[2] Xu Y, Liu X, Yao R. A payment model of mobile phone based on Third-Party security[C]//Management of e-Commerce and e-Government, 2009. ICMECG'09. International Conference on. IEEE, 2009: 400-403.

[3] Qadeer M A, Akhtar N, Govil S, et al. A Novel Scheme for Mobile Payment Using RFID-Enabled Smart SIMcard[C]//Future Computer and Communication, 2009. ICFCC 2009. International Conference on. IEEE, 2009: 339-343.

[4] Javidan R, Pirbonyeh M A. A new security algorithm for electronic payment via mobile phones[C]//Applied Sciences in Biomedical and Communication Technologies (ISABEL), 2010 3rd International Symposium on. IEEE, 2010: 1-5.

[5] Chen W D, Mayes K E, Lien Y H, et al. NFC mobile payment with Citizen Digital Certificate[C]//Next Generation Information Technology (ICNIT), 2011 The 2nd International Conference on. IEEE, 2011: 120-126.

[6] Dewan S G, Chen L. Mobile payment adoption in the USA: a cross-industry, cross-platform solution[J]. Journal of Information Privacy & Security, 2005, 1(2): 4-28.

[7] Kreyer N, Pousttchi K, Turowski K. Mobile payment procedures: scope and characteristics[J]. e-Service Journal, 2003, 2(3): 7-22.

[8] Teo E, Fraunholz B, Unnithan C. Inhibitors and facilitators for mobile payment adoption in Australia: A preliminary study[C]//International Conference on Mobile Business, ICMB 2005. IEEE, 2005: 663-666.

[9] Zmijewska A. Evaluating wireless technologies in mobile payments-a customer centric approach[C]//Mobile Business, 2005. ICMB 2005. International Conference on. IEEE, 2005: 354-362.

[10] Dawei Li. Issues of security of mobile payment technology[J]. Gansu Science and Technology, 2014, 2: 011.

[11] Ahamad S S, Sastry V N, Nair M. A Biometric based Secure Mobile Payment Framework[C]//Computer and Communication Technology (ICCCT), 2013 4th International Conference on. IEEE, 2013: 239-246.

[12] Gordon M, Sankaranarayanan S. Biometric security mechanism in Mobile payments[C]//Wireless And Optical Communications Networks (WOCN), 2010 Seventh International Conference On. IEEE, 2010: 1-6.

[13] Hu J Y, Sueng C C, Liao W H, et al. Android-based mobile payment service protected by 3-factor authentication and virtual private ad hoc networking[C]//Computing, Communications and Applications Conference (ComComAp), 2012. IEEE, 2012: 111-116.

[14] Zhang Q R. Two-Dimensional Parameter Principal Component Analysis for Face Recognition[C]//Advanced Materials Research. 2014, 971: 1838-1842.

[15] Zhang D, Zhou Z H. (2D) 2PCA: Two-directional two-dimensional PCA for efficient face representation and recognition[J]. Neurocomputing, 2005, 69(1): 224-231.

[16] Hadid A, Heikkila J Y, Silvén O, et al. Face and eye detection for person authentication in mobile phones[C]//Distributed Smart Cameras, 2007. ICDSC'07. First ACM/IEEE International Conference on. IEEE, 2007: 101-108.

[17] Liu Y, Kostakos V, Deng S. Risks of Using NFC Mobile Payment: Investigating the Moderating Effect of Demographic Attributes[J]. Effective, Agile and Trusted eServices Co-Creation, 2013: 125

.

ISBN: 978-988-19253-2-9
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)