Secure Network Authentication Based on Biometric National Identification Number

Dr. Mahmood K. Ibrahem
College of Information Engineering
Al-Nahrain University/ Baghdad-Iraq

Muntasser S. Falih
College of Information Engineering/ Department of Networks Engineering
Al-Nahrain University/ Baghdad-Iraq

Abstract- This paper present a proposed authentication system based on fingerprint as biometric type and some of static credential personal information such as name and birth date. The system generate a Unique National Identification Number (NIDN) by combining fingerprint minutiae features with user's personal information (name and birthdate) printed in Quick Response code (QR) image to be used as a token card in system accessing. Fingerprint one-to-one verification is used to verify the user's identity for the application that needs high security level. The proposed system provides two authentication services; first is normal authentication service, to protect the public application that contain public data such as billing payments application, this authentication service needs only the user's NIDN or QR for the system access. Second is strong authentication service, to protect the private application that contains sensitive data such as banking systems, this authentication service needs user's NIDN or QR as well as fingerprint of the same user for system access. The experimental work of the proposed system shows that, with threshold value under (50), user's acceptance accuracy is 100%, and with threshold value equal to (50), user's acceptance accuracy is 96.153.

Keywords- Biometric, Fingerprint, Authentication, QR, hash function.

I. INTRODUCTION

The presence of modern sensitive applications such as e-government, banking transaction and smart card and assurance on the protection of the information saved in multiple Databases (DB). Automatic personal identification become most important issue, broad range of civilian applications is needed accurate automatic personal identification. Personal identification is the process of binding a specific individual for an identity. Identification sometimes came in the form of verification which also refer to (authentication) or (recognition), which mean of defining the user identity from DB of users known to the system. Two personal identification techniques have wide range of usage are Token-based and Knowledge-based. Token-based techniques use of "something you have" to generate a personal identification, examples on these technique such as passport, ID card, driver's license, credit card or keys. Knowledge-based technique use of "something you now" to generate a personal identification, examples on these technique such as password or a Personal Identification Number (PIN). The two techniques have some drawbacks; lost, stolen, forgotten or mislays are associated with token, guessing and forgetting are associated with a password or PIN. A more reliable and secure approach can be used to support person's identity instead of the traditional approaches is called "Biometrics" [1]. Biometrics is a technology by which the data become more secure, define all the users by method of their personal physical or behavioral properties. Fingerprint (FP), face, iris, speech, handwriting or hand geometry and so on are the biometrics information that can be used to completely identity the people. Using biometric identifiers presents several advantages over other identifiers (token and knowledge based) [2].

From all biometrics types, FP has one of the highest security and authenticity levels. FP is the best biometrics to be easily captured, stored and compared to verify the identity of an individual. A FP is an active proof of a person's identity as a part of the fingerprint uniqueness and universality [3, 4].

This work presents a client-server interaction system with secure socket layer protocol (SSL) [9]. Client side is dealing with user interface for data capturing and result returning. Server side is dealing with processing the main system functions.

The reset of paper is organized as follow. The system architecture is explained in section II. System testing is presented in section III. Results of system implementation and testing are presented in section IV. Section V and VI gives the conclusion and references respectively.

II. SYSTEM ARCHITECTURE

The proposed system architecture is illustrated in figure 1. The client side provide full interface for system's user with all system functions, FP scanner is also connected in the client machine for FP capturing and QR code generation and decoding. The server side provides services for system user such as registration process, NIDN generation, user recording and authentication service that requested by users such as normal authentication and strong authentication. Each side transmit its data using the SSL module, each module for each side can be explained as follow:

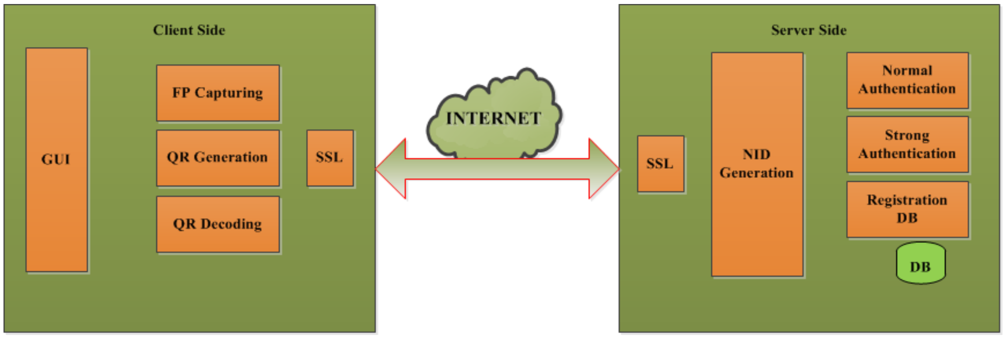

Figure1. The proposed system architecture.

1. *Graphical User Interface (GUI):* this module provides the front end interface between the system and the user, designed to be simple and guide the users for each functions. This has been implemented using C#.

2. *FP capturing:* this module deals with capturing the FP image by ZK 4500 FP optical scanner to feed the system with real time FPs. The module work to make the FP scanner compatible with the client program.

3. *QR Generation:* this module generates a QR image of the generated NIDN. QR image printed in card to be used in the system access [9].

4. *QR Decoding:* this module is used to retrieve the included NIND from the QR image during system access. Web camera of the Laptop is used as QR reader in this module.

5. *NIDN generation:* this module will be active in the registration of new user (enrollment process). NIDN is a unique number generated by combining the FP minutiae feature with some of static user credentials such as name and birthdate. Figure 2 shows the registration and NIDN generation flowchart.

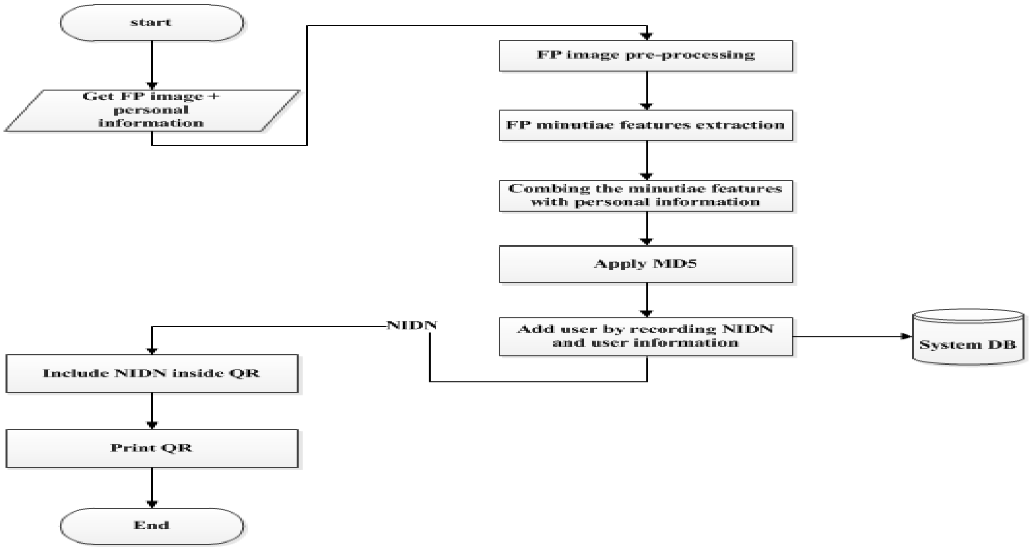
start
Get FP image + personal information
FP image pre-processing
FP minutiae features extraction
Combing the minutiae features with personal information
Apply MD5
Add user by recording NIDN and user information
System DB
NIDN
Include NIDN inside QR
Print QR
End

Figure 2. System Registration flowchart.

NIDN generation steps combine the FP and user information as input value and produce 128-bit hash value as output, these steps are:

a. **FP pre-processing:** this step is used to enhance the clarity of the FP image and achieve some process as preparing before features extraction. Gabor filtering algorithm is used in FP enhancement, binarization and thinning are also performed in this step [5].

b. **FP minutiae features extraction:** in this step the minutiae features have been extracted by using Crossing Number algorithm (CN) as described in the following equation:

$$CN = \sum_{i=1}^{8} |N_{i+1} - N_i|, N_9 \ldots\ldots\ldots(1).$$

Where CN is crossing number, N_i is neighborhood pixels.
The CN value determined the minutiae type; for CN equal (1) minutiae is edge termination and for CN equal to (3) minutiae type is bifurcation [6].

c. **Combining minutiae features with personal information:** after minutiae extraction, these features will be combined with user credential information to avoid the conflict in FPs if it happens, finally we get a mixed block of FP features and user information.

d. **Apply MD5:** the mixed block will be feed to one-way hash function to compress this block and produced fixed length NIDN (128-bit) [10].

At this point we have NIDN, to complete registration process new user will be added to the DB and issues QR card contain the NIDN to be used as token card in system access.

6. **DB registration:** this module explained in the registration process which includes recording the NIDN and user information in system DB.

7. **Normal Authentication:** this module provides the first type of authentication service that provided by the system to protect the public data such as bills payment systems. In normal authentication the user need his token card (QR) only for system access. Figure 3 illustrates normal authentication functional block.

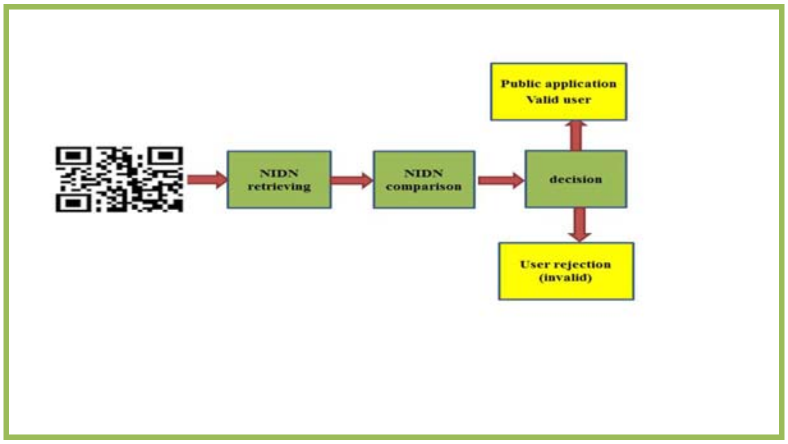

Figure 2. The normal authentication functional block.

Normal authentication takes QR card as input and compare it with the retrieved NIDN from database. Finally, the decision is based on comparison, which either access the user to public application or denied from it services.

8. Strong authentication: this is the second authentication service that provided by the system. This service is used to protect the sensitive data such as banking application. This authentication service needs the QR card and the real time captured FP image for system access. Figure 3 illustrates strong authentication flowcharts.

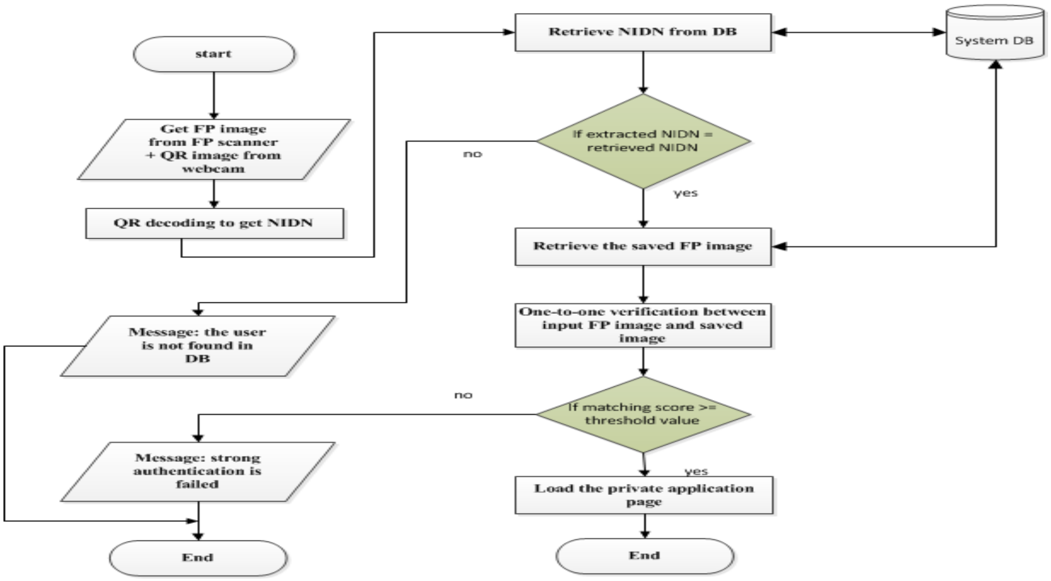
start
Get FP image from FP scanner + QR image from webcam
QR decoding to get NIDN
Retrieve NIDN from DB
System DB
If extracted NIDN = retrieved NIDN
no
yes
Retrieve the saved FP image
Message: the user is not found in DB
One-to-one verification between input FP image and saved image
If matching score >= threshold value
no
yes
Message: strong authentication is failed
Load the private application page
End
End

Figure 3. Strong authentication flowchart.

In strong authentication user identification has been achieved by checking the user NIDN with the whole NIDNs that is saved in DB. User verification is depending on FP one-to-one verification between the saved FP image and real time captured image [8]. One-to-one FP verification is implement by using an algorithm proposed by Automatic Fingerprint Identification System (AFIS) called (AFIS engine) [7], which is a powerful matching algorithm and solved some of problems related with FP image like rotation and shifting. The matching value between the two FPs images determines the user's acceptance by the system.

III. SYSTEM TESTING

The system has been evaluated using the following approaches:

1. **FP matching system testing:** this test shows the reliability of AFIS engine at different impressions conditions of FP image. Figure 4 illustrates the FP condition for system testing; table 1 shows the matching score values results for these conditions.

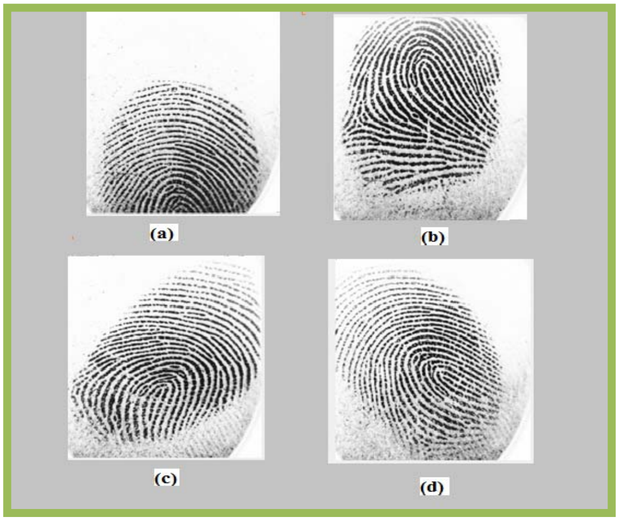

Figure 4. (a) FP backward shifting, (b) FP forward shifting, (c) FP clock-wise rotation and (d) FP anti-clock-wise shifting

Table – 1 Matching score at different FP impression conditions

FP Impression	Matching Score
Backward shifting	55.95922
Forward shifting	65.58824
Clock-wise rotation 45°	42.90625
anti-clock-wise rotation 45°	67.27821

2. **Traffic analysis:** this test shows the reliability of the SSL in the prevention the transmitted data from any sniffing attack. This testing done by using software tool for traffic sniffing called (Wire shark). With SSL the eavesdroppers can get encrypted data which is meaningless without knowing the secrets keys.

IV. RESULTS

This section shows the result of system execution. the results illustrates the following features; the FP image processing steps from normalization to minutiae extraction, the generated NIDN for number of users, strong authentication accessing for valid and invalid users and finally, the accuracy rate. Figure 4 shows the output of FP image processing.

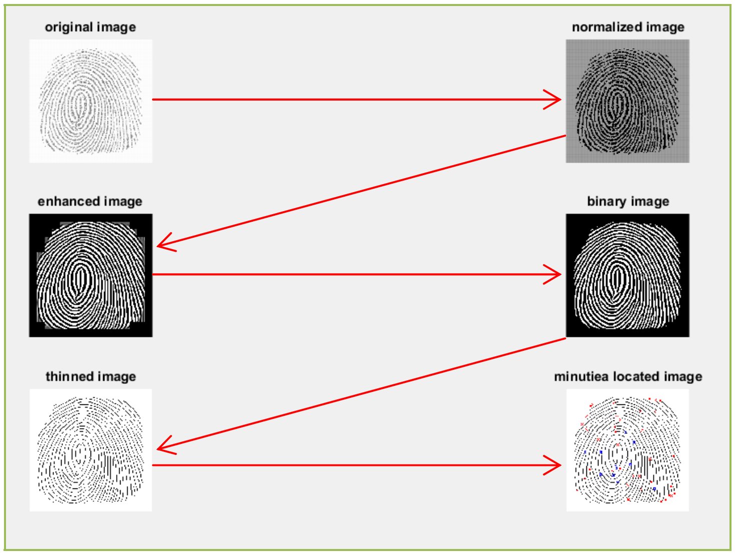

Figure 4. FP image processing steps.

Table 2 shows the NIDN for number of system users. Table 3 shows the matching score value in strong authentication service for a valid and invalid users.

Table – 2 The generated NIDN.

User Name	NIDN	Birthdate
Ali Kadom	ed507237030ee067e95e5cf33c06bae5	26/2/1976
Mntaser Saleem	b73a482561c9e96fd1830986384037a2	20/5/1990
Abdualhameed Mondel	207f0b300f45592a2356285abba1addf	3/5/1976
Safa Kamal	cb5c361cb7754235ed5b4696191cb8d6	11/1/1990
Hussan Kamal	e932792e96d4bf45c002654f9977eadf	30/7/1991
Thukra Jabar	27f5a08612af02a5040399582461f760	4/11/1970
Hurria Kadom	b5f2fd428574f51cd7f5b8f26a767fce	14/1/7/1958
Rafel Saleem	da612dafcc144ca10334add17b6dba66	1/6/1988
Mohammed Saleem	7fdb315db63c076082974794c33d2286	18/6/1982
Sabah Faleh	3bd27e91ece2697d1bb10f43bf4711f5	7/7/1989

Table – 3 valid and invalid (faked) FP matching score.

User Name	User NIDN	True Matching Score	False Matching Score
Mntaser Saleem	b73a482561c9e96fd1830986384037a2	93.22698	0
Mustafa Taher	35bdf7e7ffdf077def3b8967d28ed2a9	77.22011	0
Rafel Saleem	da612dafcc144ca10334add17b6dba66	72.1989	0
Mustafa Ali	922fca9f9f70f8f850f7f0cfb12dfc54	40.95295	0
Samer Faleh	35bdf7e7ffdf077def3b8967d28ed2a9	75.94591	0
Mahdi Satar	131db019ce05547d094da16531b88dfe	58.06531	0
Mokhaled Saleem	ff7bcafb6eebc6ad89243bbdf5cf18df	99.31831	0
Mustafa Haji	5f0c73aa1caccd272cca3c4442842e5d	70.96764	0
Dhia Raad	e5f0555cf991d544696808d8eacbad17	99.56341	0
Foad Emad	5bf7ba0626ba7539beae130460f63b49	54.16734	0
Hasanen Ibrahim	b261323fa6562babdaf42e624f77340f	55.6778	0
Sabah Faleh	3bd27e91ece2697d1bb10f43bf4711f5	50.86031	0
Zia Raad	5934a3420ee240fff4c53001cd710ea1	76.24079	0

Finally the accuracy of matching is computed with some of different thresholding values. The following formula defines the calculation of percentage accuracy.

Accuracy rate (%) = $\frac{SA}{TU}$100%.

Where

SA: successful matched count.

TU: total number of submitted users.

Table 4 shows the accuracy rate in different thresholding values.

Table – 4 Accuracy rate.

Threshold value	Accuracy rate (%)
0	100%
10	100%
20	100%
30	100%
40	100%
50	96.153%

V. CONCLUSIONS

Through the system design and implementation phase, some conclusions are drawn, these are:

1. Strong authentication service is a good method to protect the private application that contains sensitive data from access by unauthorized users, but will cost more computation time.
2. Some applications such as electronic libraries (e- libraries) and billing payment systems needs a normal authentication method with light weight computation efforts, so the normal authentication is a more appropriate for this purpose.
3. Including NIDN in QR image is more feasible to be secured and fast retrieved by capturing device during system access comparing with using the plain NIDN.
4. SSL is a good security protocol in providing a secure data transfer between the client and server sides.

5. Using of time domain Gabor filtering method for fingerprint quality enhancement is more appropriate enhancement method for minutiae features extraction algorithms.
6. A minutia features are a good features in comparing among fingerprints and differ from one person to another but suffering from instability against scaling and rotation of fingerprint.

REFERENCES

[1] A. Jain, L. Hong and S. Pankanti, **"Biometric Identification",** Communications of The ACM, Vol. 43, No. 2, February, 2000.

[2] A. K. Ojha, **"ATM Security using Fingerprint Recognition"**, International Journal of Advanced Research in Computer Science and Software Engineering Research Paper, Vol.5, No.6, June 2015.

[3] A. Jain, A. Ross and S. Prabhakar, **"Fingerprint Matching Using Minutiae and Texture Features"**, Int'l Conference on Image Processing (ICIP), pp. 282-285, October 2001.

[4] C. C. Ho and C. Eswaran, **"Consodilation of Fingerprint Databases: A Malaysian Case Study"**, 11th International Conference on Hybrid Intelligent Systems (HIS), 2011.

[5] R.Thai, **"Fingerprint Image Enhancement and Minutiae Extraction"**, phD. Thesis, University of Western Australia, 2003.

[6] Y. Li-qiang and G. Ling, **"Feature Extraction of Fingerprint Image Based on Minutiae Feature Points"**, International Conference on Computer Science and Service System, IEEE, 2011.

[7] http://www.sourceafis.org/, last access on 2nd January 2015.

[8] S. Ambadiyil, K. Soorej and V. Pillai, **"Biometric based Unique ID Generation and One to One Verification for Security Documents"**, International Conference on Information and Communication Technologies (ICICT), 2014.

[9] A. Johny and Jayasudha J. S, **"Secure Socket Layer Implementations-A Review"**, International Journal of Computer Science & Engineering Technology (IJCSET), Vol. 4 No. 2, Feb 2013.

[10] P. Gupta and S. Kumar, **"A Comparative Analysis of SHA and MD5 Algorithm"**, International Journal of Computer Science and Information Technologies (IJCSIT), Vol. 5, No. 3, 2014.