DOI: 10.24996/ijs.2021.SI.1.33

ISSN: 0067-2904

Network Authentication Protocol Based on Secure Biometric NIDN

Muntasser S. Falih [1]*, Fatima B. Ibrahim [2], Mahmood K. Ibrahem[1]

[1]College of Information Engineering, Al-Nahrain University, Baghdad-Iraq

[2]Department of Information and Communication Engineering, Al-Khawarizmy College of Engineering/University of Baghdad, Baghdad-Iraq

Abstract

In this paper an authentication based finger print biometric system is proposed with personal identity information of name and birthday. A generation of National Identification Number (NIDN) is proposed in merging of finger print features and the personal identity information to generate the Quick Response code (QR) image that used in access system. In this paper two approaches are dependent, traditional authentication and strong identification with QR and NIDN information. The system shows accuracy of 96.153% with threshold value of 50. The accuracy reaches to 100% when the threshold value goes under 50.

Keywords: Automatic Fingerprint Identification System, Fingerprint verification, QR, National Identification Number, Secure Socket Layer

Introduction:

The growth in the natural of applications especially in as e-government and e-business requires a new secured controlled authentication methods. The automatic identification of individuals plays an essential role in applications of that type where the identity of the person comes from his/her biometric and sometimes other personal information. User identification is known also as authentication or individual recognition in form of one – to – one verification. Authentication can be Token-based and/or Knowledge-based. The use of the term “something you have” is centered in the Token-based methods while the use of the term “something you know” is centered in the Knowledge-based methods. Both of these methods types suffer drawbacks of lost, forgetting, stolen, guessing by others and bad-using that makes the biometric technology takes an important range in applications. “Biometrics” is the term that overcomes the limitations mentioned above by using the individual properties both in physical and behavior form to identify persons. Biometrics can be finger print, Iris, face, palm, voice, handwriting, gait [1, 2].

Finger print (FP) biometric is considered the more reliable and useable that it is easy to capture, store and processed to generate a unique personal identification [3,4].

Section two expressed the architecture of the system where how the test of the system is done is expressed in section three. Section four gives the experiments results and tests. Conclusions are stated in section five. Finally, the references are listed as section six

System Architecture:

The framework system architecture that is suggested in this paper is illustrated in figure 1. It is depending on dividing the work into client/server sides. It is based on interaction system of client/server in Secure Socket Layer (SSL) protocol [5]. The client side afford complete interface helping user with totally system jobs, fingerprint scanner is accompanying in the client computer to capture the fingerprint image, and the QR code is generated and decoded. The server side affords services facilities for users of the system like registration procedure, and the generation of NIDN with the registration and

*Email: mntaser_almeahy@yahoo.com

authentication facilities for the user that needed from the users in both authentication types of normal such as normal and strong. Data transmission in both directions is traveling over SSL protocol module. The complete system structure and functions is expressed in figure 1 and the details of its functions are illustrated as follows:

1. Graphical User Interface (GUI): this component represents the front end interface for the system. The GUI interface is simple, clear and easy to be used by the user providing guiding in each step. .It is implementing using C# language compiler

2. FP capturing: to capture the fingerprint image, ZK 4500 FP optical scanner is used providing the system with a real time fingerprint image. In this module the fingerprint scanner will be compatible with the client program.

3. QR Generation: in this segment the QR image is produced for the produced NIDN. It is printed in a card that makes it available to use later in the accessing system [5].

4. QR Decoding: in this segment the web camera of the laptop is used to read the QR image, so it will work as a QR reader. Then it will recover the involved NIDN to be used later.

5. NIDN generation: this unit is work in the enrollment process to register a new user. Integration of the fingerprint feature and the personal identity user information like mane and birthday is used to generate the unique NIDN number. .flowchart of this process Figure 2 displays the

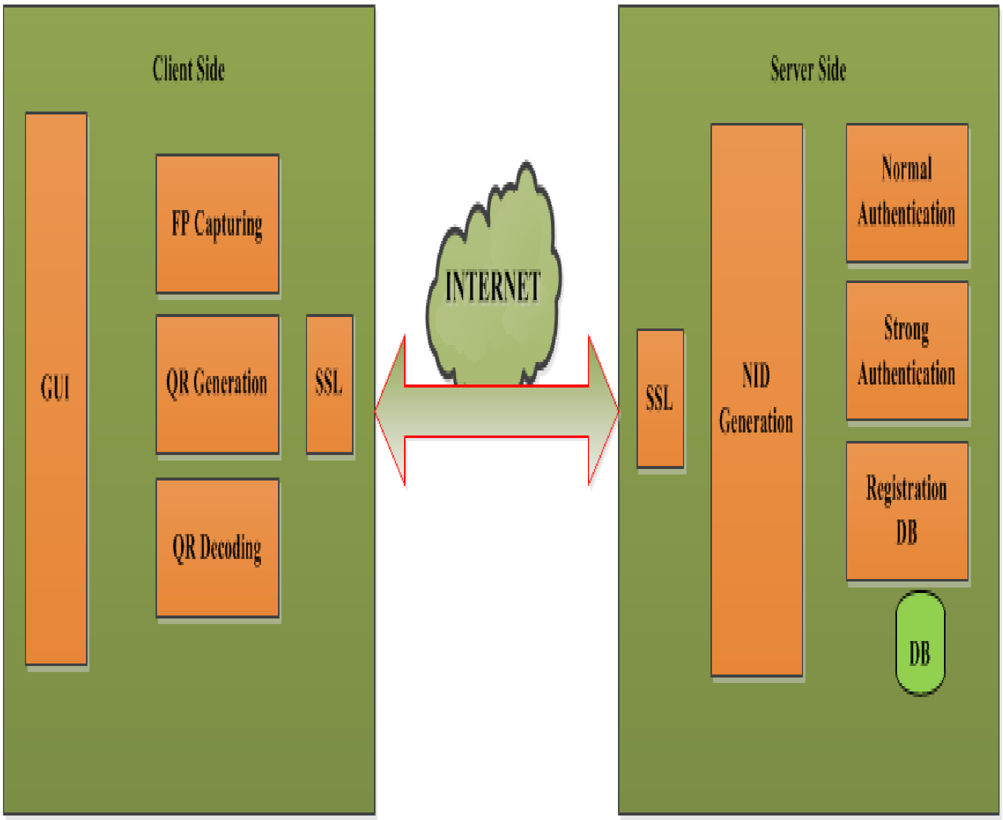


Figure1-The proposed system architecture

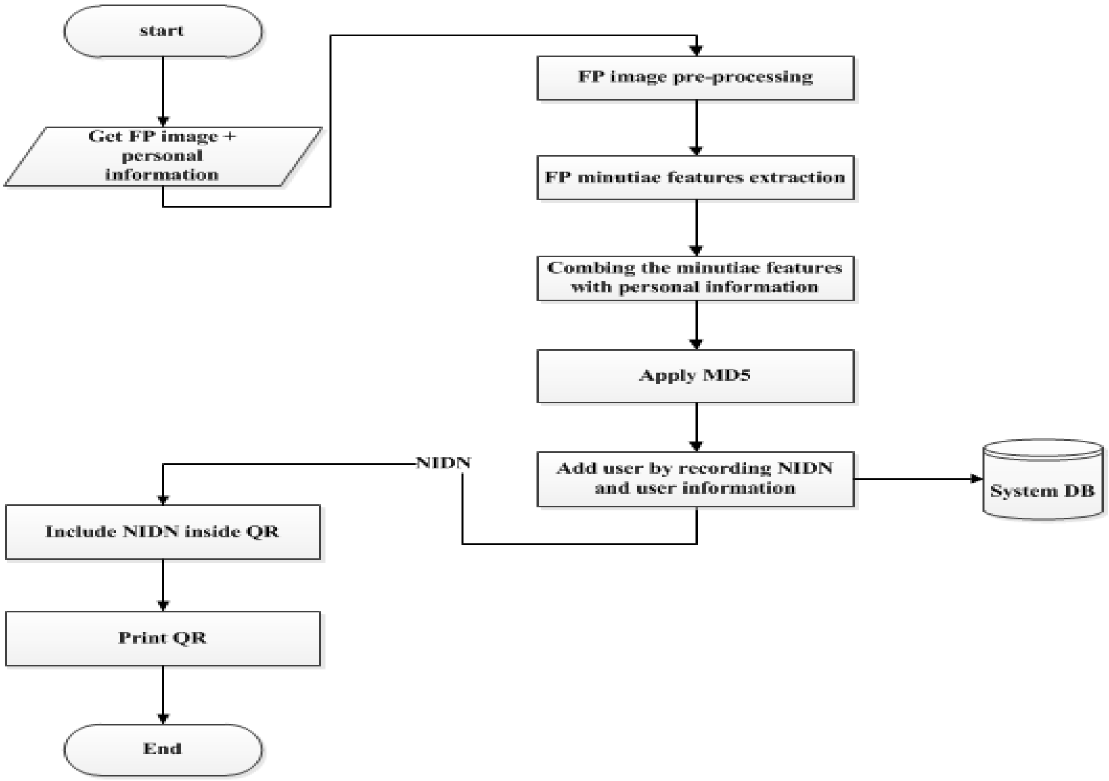

start
Get FP image + personal information
FP image pre-processing
FP minutiae features extraction
Combing the minutiae features with personal information
Apply MD5
Add user by recording NIDN and user information
System DB
NIDN
Include NIDN inside QR
Print QR
End

Figure 2-Flowchart of the registration system

The steps of generating the unique NIDN that are related with fingerprint and the personal information of the users are completed with hashing function to produce 128-bit hash value as an output, the steps are as follows:

a. FP pre-processing: to enhance the fingerprint image time domain Gabor filter is used, and as another preprocessing steps binarization and thinning are accomplished. The processes in this stage are useful to develop and enhance the feature extraction process.[6]

b. FP minutiae features extraction: Crossing Number (CN) algorithm is used in this stage to extract the minutiae fingerprint features as in equation (1) below:

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

Where *CN* is the crossing number, N_i is neighborhood pixels.

The value of *CN* is representing the minutiae type; that the value of (1) means that minutiae is in edge termination while the value of (3) means that it is in bifurcation [7].

c. Combining minutiae features with personal information: to avoid any conflict may be happened in minutiae feature extraction and to strength the system authentication, an integration with the personal identity information is done in this step.

d. Apply MD5: the integrated information in the previous sub-step will be the input to a one way hashing function that generate the NIDN which it is in a fixed 128-bit length. .[8]

At this point we get NIDN, to complete registration process a new user will be added to the dataset and production QR card that contain the NIDN to be used as token card in the access system.

6.DB registration: this component is clarified for registration procedure that comprises the computed NIDN and the other information of the user to the dataset of the system.

7. Normal Authentication: this part runs the traditional kind of authentication service that supplied by the system to guard the simple data that is public. In normal authentication the token QR card for individuals is only used in accessing the system as illustrated in the block diagram of Figure-3.

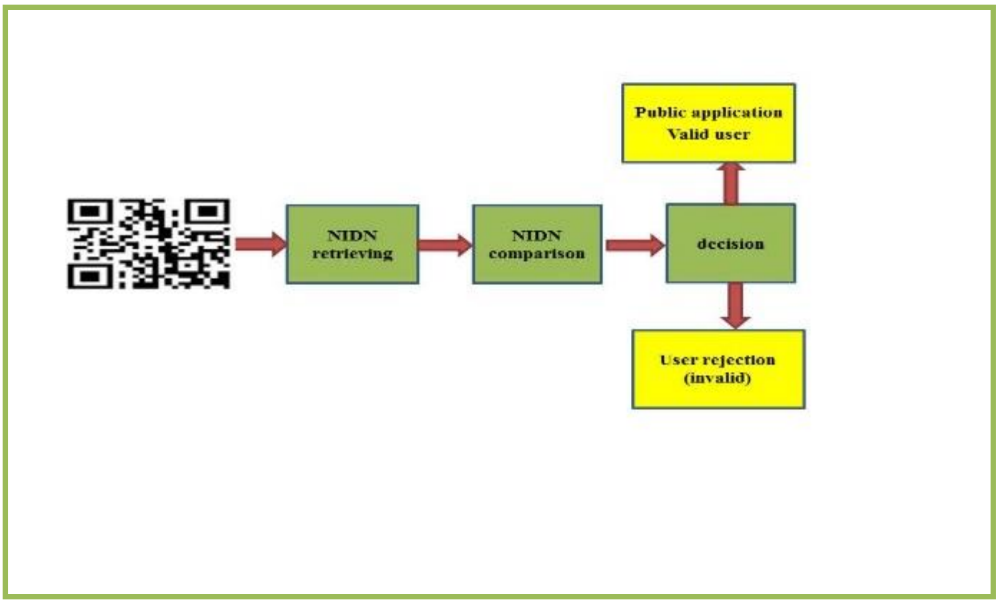


Figure 3-The basic block diagram for the normal authentication

A normal authentication gets QR card as input then matches it with the saved NIDN in the dataset. As a final point, the judgement is based on comparison to decide access or denied to the public application.

8. Strong authentication: it is another authentication service that the system is provided. By this service the safeguard to a sensitive data is applied. The data may be for banking application. In strong authentication QR card and real time fingerprint is required to access the system. Figure 4 illustrates the flowchart of this strong authentication service.

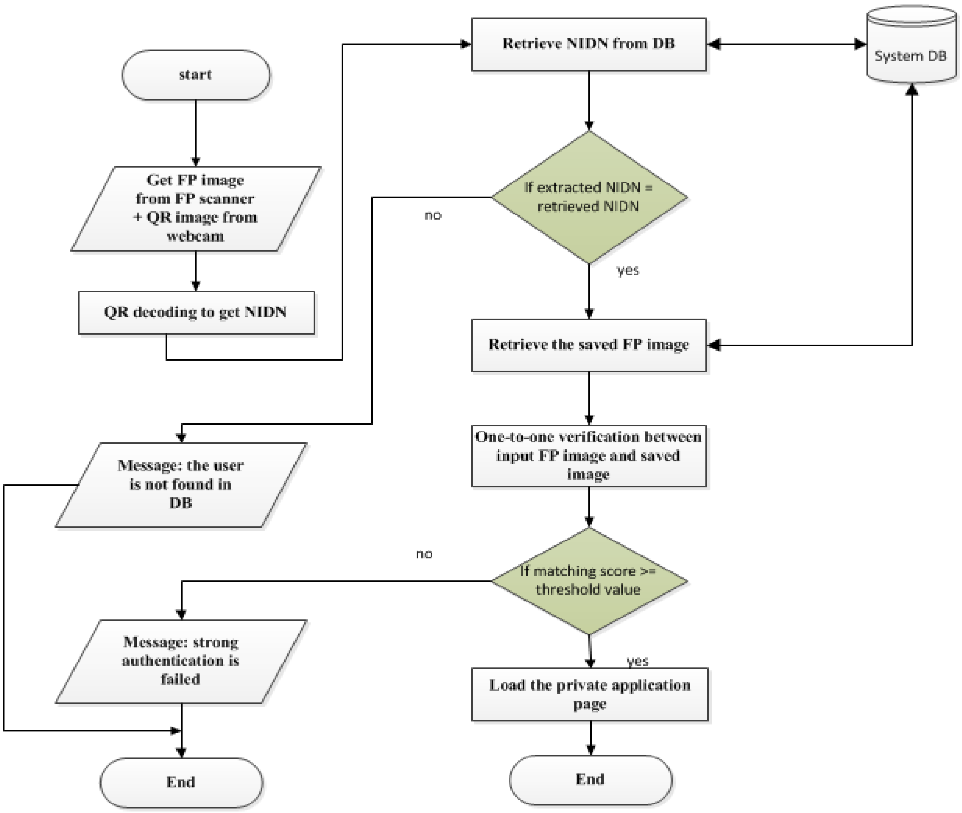

start
Get FP image from FP scanner + QR image from webcam
QR decoding to get NIDN
Retrieve NIDN from DB
System DB
If extracted NIDN = retrieved NIDN
no
yes
Retrieve the saved FP image
Message: the user is not found in DB
One-to-one verification between input FP image and saved image
no
If matching score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

Figure 4-“Strong authentication flowchart”

"In strong authentication; user identification has been accomplished by examining the user NIDN with the total NIDNs in the saved dataset". The dependence of user verification in FP one-to-one is based on the comparison between saved FP image of data set and real time captured image [9]. "Automatic Fingerprint Identification System (AFIS) algorithm, called (AFIS engine) is used to implement the verification" [7], which is a robust matching algorithm that can solve some of the complications connected with fingerprint images such as "rotation and shifting. The difference between two fingerprint images defines the user's receipt by the system".

Testing ways of System:

"The system has been weighed using the following methodologies":

1. **"FP matching system testing:** this check demonstrates the trustworthiness of AFIS engine" with some changing of impressions circumstances of fingerprint images. Figure 5 shows the fingerprint shifting conditions to test the system. "Table-1 shows the results matching score values results for these conditions".

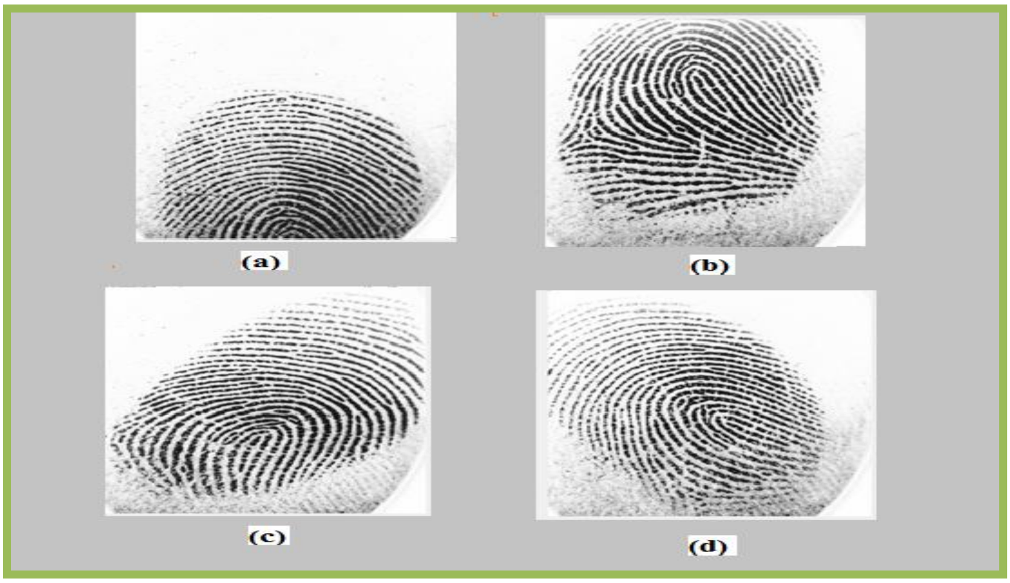
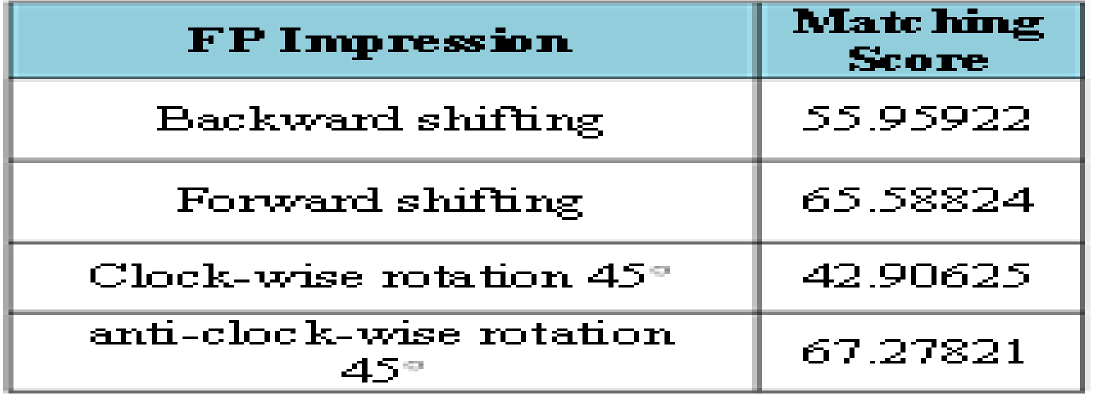


Figure 5-(a) Fingerprint backward shifting, (b) Fingerprint forward shifting, (c) Fingerprint clock-wise rotation and (d) Fingerprint anti-clock-wise shifting.

Table 1-The matching scores for different impression conditions of fingerprint



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

1. **Traffic analysis:** this check confirms the reliability of Secure Sockets Layer to prevent sniffing attack for the transmitted data. This testing is achieved by the wire shark which is a software tool developed with the system to deal with the traffic sniffing. With Secure Sockets Layer the users can get encrypted data that is useless and unmeaning when the secret keys are unknown.

Experiments and Results:

This section demonstrates the effects and outcomes of implementing the system, demonstrations the features in stages of processing fingerprint images, normalization of the fingerprint images, the minutiae feature extraction, and for each user generating NIDN to be used in strong authentication access to the system, then the precision rate for the system is computed depending on some real and faked users. Figure 6 displays the steps and results of fingerprint processing on a sample image.

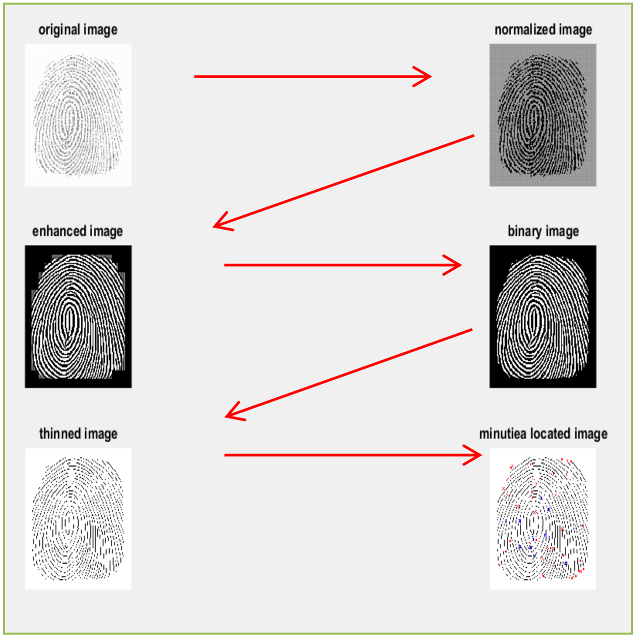


Figure 6-Steps of fingerprint processing

Table-2 expresses for number users of the system their NIDN. Table 3 displays or number of both authenticated and unauthenticated users of the system their matching scores value in the strong authentication service.

To conclude results, the precision matching of system is calculated with different thresholding values. The following formula outlines the computing of percentage precision.

Precision rate (%) = $\frac{TM}{TN} \times 100\%$.

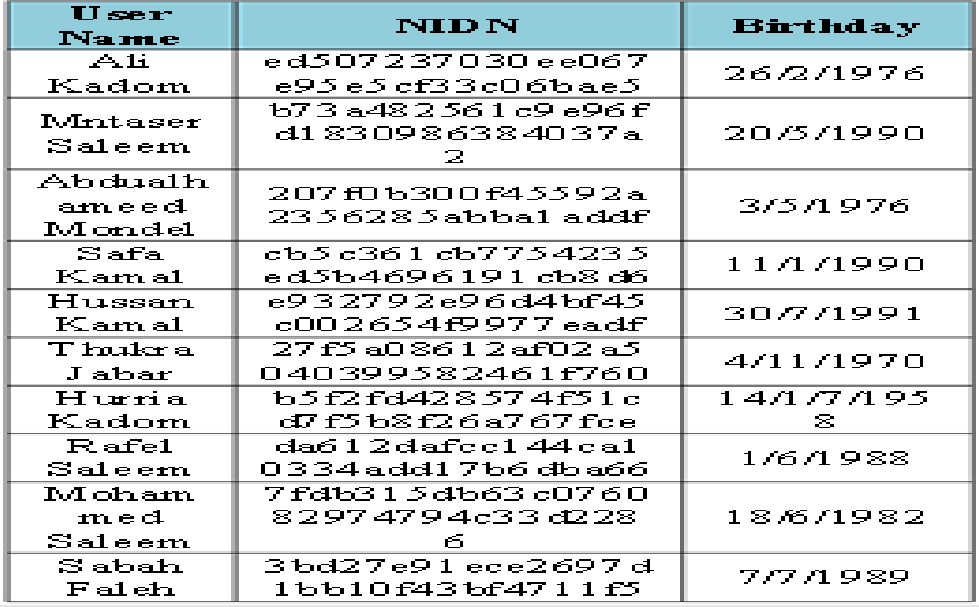
Where

TM: True Matching trails.

TN: Total Number of trails.

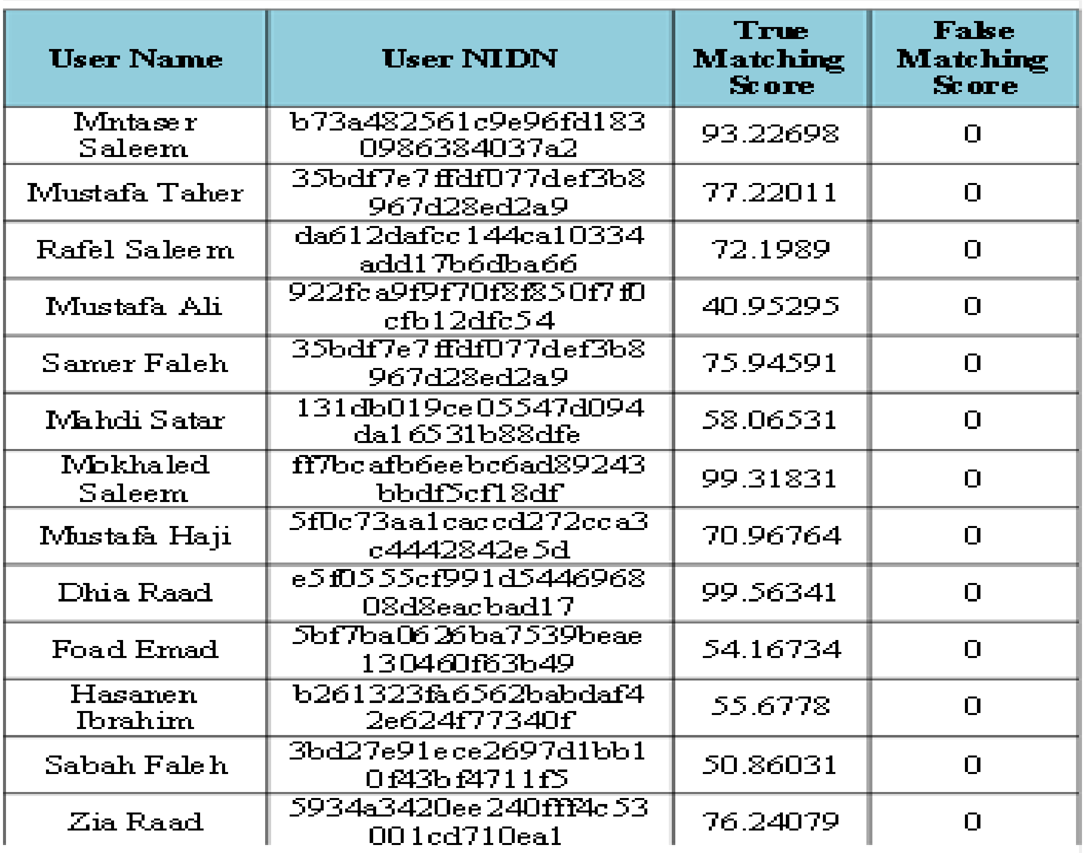
The results of computing the accuracy for different threshold values is shown in Table-4.

Table 2-The generated NIDN



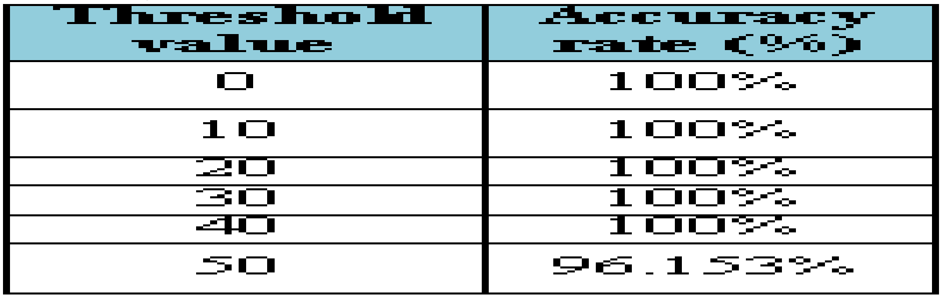
User Name	NIDN	Birthday
Ali Kadom	ed507237030ee067e95e5cf33c06bae5	26/2/1976
Mntaser Saleem	b73a482561c9e96fd1830986384037a2	20/5/1990
Abdualhameed Mondel	207f0b300f45592a2356285abba1addf	3/5/1976
Safa Kamal	cb5c361cb7754235ed5b4696191cb8d6	11/1/1990
Hussan Kamal	e932792e96d4bf45c002654f9977eadf	30/7/1991
Thukra Jabar	27f5a08612af02a5040399582461f760	4/11/1970
Hurria Kadom	b5f2fd428574f51cd7f5b8f26a767fce	14/1/7/1958
Rafel Saleem	da612dafcc144ca10334add17b6dba66	1/6/1988
Mohammed Saleem	7fdb315db63c0760829747 94c33d2286	18/6/1982
Sabah Faleh	3bd27e91ece2697d1bb10f43bf4711f5	7/7/1989

Table 3-matching fingerprint scores for both real and faked cases



User Name	User NIDN	True Matching Score	False Matching Score
Mntaser Saleem	b73a482561c9e96fd183 0986384037a2	93.22698	0
Mustafa Taher	35bdf7e7ffdf077def3b8 967d28ed2a9	77.22011	0
Rafel Saleem	da612dafcc144ca10334 add17b6dba66	72.1989	0
Mustafa Ali	922fca9f9f70f8f850f7f0 cfb12dfc54	40.95295	0
Samer Faleh	35bdf7e7ffdf077def3b8 967d28ed2a9	75.94591	0
Mahdi Satar	131db019ce05547d094 da16531b88dfe	58.06531	0
Mokhaled Saleem	ff7bcafb6eebc6ad89243 bbdf5cf18df	99.31831	0
Mustafa Haji	5f0c73aa1caccd272cca3 c4442842e5d	70.96764	0
Dhia Raad	e5f0555cf991d5446968 08d8eacbad17	99.56341	0
Foad Emad	5bf7ba0626ba7539beae 130460f63b49	54.16734	0
Hasanen Ibrahim	b261323fa6562babdaf4 2e624f77340f	55.6778	0
Sabah Faleh	3bd27e91ece2697d1bb1 0f43bf4711f5	50.86031	0
Zia Raad	5934a3420ee240fff4c53 001cd710ea1	76.24079	0

Table 4- Accuracy rate



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

Conclusions

Over and done with the stages of designing and implementing the system, some points are concluded; they are seen in the natural of the system flow work like the trade of strong authentication service method for protection the privacy of the application including sensitive data from unauthorized access. Also the time cost of extra computations is considered. And for less sensitive applications including e-libraries a less weight computation authentication which it is considered normal authentication method is proposed. Combining NIDN with QR image can be secure and quick properly. It is planned to capture the QR image by the device in accessing time in and compare it with the plain NIDN. For transmission data, SSL protocol is used. Gabor filter is used to enhanced the performance of fingerprint with the minutiae feature extraction technique.

The future work is to implement the developed the biometric recognition system in a reconfigurable hardware (10-16).

References

1. Jain, A., Hong, L. and Pankanti, S. **2000**. “Biometric Identification” *Communications of The ACM*, **43**(2), February.
2. Ojha, K. **2015**. “ATM Security using Fingerprint Recognition”, *International Journal of Advanced Research in Computer Science and Software Engineering Research Paper*, **5**(6), June 2015.
3. Jain, A. Ross and Prabhakar, **S. 2001**. “Fingerprint Matching Using Minutiae and Texture Features”, Int’l Conference on Image Processing (ICIP), pp. 282-285, October.
4. Ho, C. and Eswaran, C. **2011**. “Consodilation of Fingerprint Databases: A Malaysian Case Study”, 11th International Conference on Hybrid Intelligent Systems (HIS).
5. Hasan, S. **2016**. "Performance-Aware Architectures for Parallel 4-D color fMRI Filtering Algorithm: A Complete Performance Indices package", *IEEE Transactions onParallel and Distributed Systems,* **27**(7).
6. Hasan, S. **2016**. "Performance-vetted 3-D MAC processors for parallel volumetric convolution algorithm: A 256×256×20 MRI filtering case study", Multidisciplinary in IT and Communication Science and Applications (AIC-MITCSA) Al-Sadeq International Conference on, pp. 1-6, 2016.
7. Hasan, S. **2013**. FPGA implementations for parallel multidimensional filtering algorithms, Newcastle upon Tyne, UK : University of Newcastle, 2013.
8. Amjad J. Humaidi, Sami Hassan and Mohammed A. Fadhel. **2018**. “FPGA-based lane-detection architecture for autonomous vehicles: A real-time design and development,” *The Asian International Journal of Life Sciences*, **16**(1): 223-237.
9. Amjad J. Humaidi, Sami Hassan and Mohammed A. Fadhel. **2018**. “Rapidly-fabricated nightlydetected lane system: An FPGA-implemented the architecture,” *The Asian International Journal of Life Sciences*, **16**(1): 343-355.