Secure Identification System - SIS

by

Dr. Salah M. Rahal, Dr. Hatim A. Aboalsamh, Dr. Khaled N. Muteb

مؤتمر تقنية المعلومات والأمن الوطني
الرياض، المملكة العربية السعودية
٢١حتى٢٤_١١_١٤٢٨هـ الموافق ١حتى٤_١٢_٢٠٠٧م

Secure Identification System - SIS

by

Dr. Salah M. Rahal, Dr. Hatim A. Aboalsamh, Dr. Khaled N. Muteb

Abstract

The secure identification of a person was and still of great interest in different fields of human activities. The traditional identification methods such as PIN, passwords aren't capable to achieve a high level of secure identification. In the contrast, the biometrics allows to attain the suitable solution for this vital question.

Different types of biometrics are reviewed. Its characteristics are unique for each person either for physiological or behavioral biometrics. It is shown that the fingerprint recognition has a very good balance of all desirable properties.

The design of secure identification fingerprint-based system, in its hardware and software parts, is done. This system was implemented with the suitable features.

Keywords: Biometrics, Fingerprint, Fingerprint Features, Fingerprint Recognition, Identifier, Minutiae, Template.

1- Review

Biometrics refers to the automatic recognition of individuals based on their physiological and/or behavioral characteristics. Biometric technologies are becoming the foundation of an extensive array of highly secure identification and personal verification solutions. This technology acts as a front end to a system that requires precise identification before it can be accessed or used [1-3].

Utilizing biometrics for personal authentication is becoming more accurate than current methods (such as the utilization of passwords or Personal Identification Number - PINs) and more convenient (nothing to carry or remember). Thus, Biometrics is not just about *security*, it's also about *convenience.*

The need for biometrics can be found in a wide range of commercial and military applications. Thus, biometrics is set to pervade nearly all aspects of the economy and our daily lives.

2- Types of Biometrics

They involve two categories: *Physiological Biometrics & Behavioral Biometrics.*

2-1 Physiological Biometrics

In this category the recognition is based upon physiological characteristics. Some examples are: Fingerprint, Hand Geometry, Iris Recognition, Retinal Scanning, and Facial Recognition.

2-1-1 Fingerprint Recognition

Fingerprint is a unique feature to an individual. The lines that create fingerprint pattern are called *ridges* and the spaces between the ridges are called *valleys* or *furrows* (Figure -1). It is through the pattern of these *ridges* and *valleys* that the unique fingerprint is matched for authentication and authorization [4].

Figure -1

2-1-2 Hand Geometry Recognition [5]

This technology verifies a person's identity by the size and shape of the hand (Figure -2). The front part of the hand is used for hand geometry measurements. A set of features have been identified that could be used to represent a person's hand. These features include the lengths and widths of the fingers at various locations.

Figure -2

2-1-3 Iris Recognition [6]

Iris patterns (Figure -3) are complex and unique. In 1985 the concept that no two irises are alike was proposed. In 1994, was developed the sophisticated mathematical foundation that made automated iris recognition into reality.

Figure -3

This technology is known for it's *extreme accuracy: The probability of two individuals having the same iris pattern is 1 in* 10^{78}. The current population of the earth is 10^{10}. The size of the population of persons who have ever lived is 10^{11}.

2-1-4 Retinal Scanning [6]

Retinal scanning technology is used to measure the unique configuration of blood vessels contained in the retina (Figure -4).

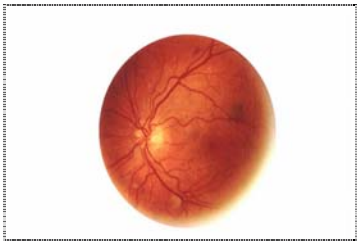


Figure -4

It does require the user to remove glasses, place his eye close to the device. A low intensity laser light source is used to illuminate the retina.

2-1-5 Facial Recognition [7]

Facial recognition analyzes the characteristics of a person's face images. It measures the overall facial structure (Figure –5). Measured features are retained in a database and used as a comparison when a user stands before the camera. In particular, an automated face recognition system is capable of capturing face images from a distance using video camera, and the face recognition algorithms can process the data captured: detect, track and do the recognition. Face recognition focuses on recognizing the identity of a person from a database of known individuals.

Face recognition has several advantages over other biometric technologies: it is natural, of "passive" nature[1], and easy to use that makes it more suitable for wide range surveillance and security applications.

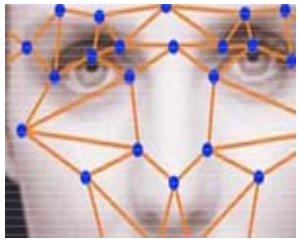


Figure -5

To prevent a fake face or mold from faking out the system, many systems now require the user to smile, blink, or otherwise move in a way that is human before verifying [4].

2-2 Behavioral Biometric [5,6]

Behavioral biometrics is traits that is learned or acquired over time as differentiated from physiological characteristics. Some examples are: VoiceRecognition, Signature Recognition and Keystroke Recognition.

[1] In contrast, fingerprint, hand and iris recognition are examples of "active" biometric tasks. They require people's cooperation to place hands on a fingerprint or hand reader, or to look into iris scanner.

2-2-1 Voice Recognition

Voice is a behavioral biometrics. The features of an individual's voice are based on the shape and size of the appendages (e.g., vocal tracts, mouth, nasal cavities, and lips) that are used in the synthesis of the sound.

These physiological characteristics of human speech are invariant for an individual, but the behavioral part of the speech of a person changes over time due to age, medical conditions (such as common cold), emotional state, etc.

2-2-2 Signature Recognition

The way a person signs his name is known to be a characteristic of that individual. Signature (Figure -6) requires contact with the writing instrument and an effort on the part of the user. They have been accepted in government, legal, and commercial transactions as a method of verification.

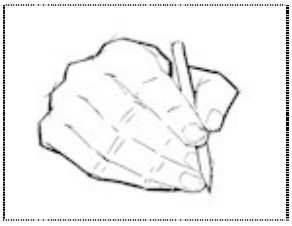


Figure -6

2-2-3 Keystroke Recognition

It is hypothesized that each person types on a keyboard (Figure -7) in a characteristic way. This behavioral biometric is not expected to be unique to each individual but it offers sufficient discriminatory information to permit identity *verification*. Keystroke dynamics is a behavioral biometric; for some individuals, one may expect to observe large variations in typical typing patterns. Further, the keystrokes of a person using a system could be monitored unobtrusively as that person is keying in information.

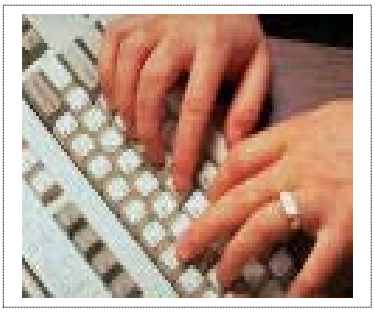


Figure -7

4- Comparison of Various Biometrics

Based on the main factors that are used for comparison i.e. *Universality, Distinctiveness, Permanence, Collectability, Performance, Acceptability, Circumvention* [4], The various biometric identifiers described above are compared in Table -1 where it is shown that *fingerprint recognition has a very good balance of all desirable properties.*

Table-1

Biometric identifier	Universality	Distinctiveness	Permanence	Collectability	Performance	Acceptability	Circumvention
Face	H	L	M	H	L	H	H
Hand geometry	M	M	M	H	M	M	M
Fingerprint	M	H	H	M	H	M	M
Iris	H	H	H	M	H	L	L
Retina	H	H	M	L	H	L	L
Keystroke	L	L	L	M	L	M	M
Signature	L	L	L	H	L	H	H
Voice	M	L	L	M	L	H	H

H: High M: Medium L: Low

The fingerprint recognition is one of the most mature biometric technologies and is suitable for a large number of recognition applications. It occupies 48.8% of the market share of identity verification systems (Figure –8).

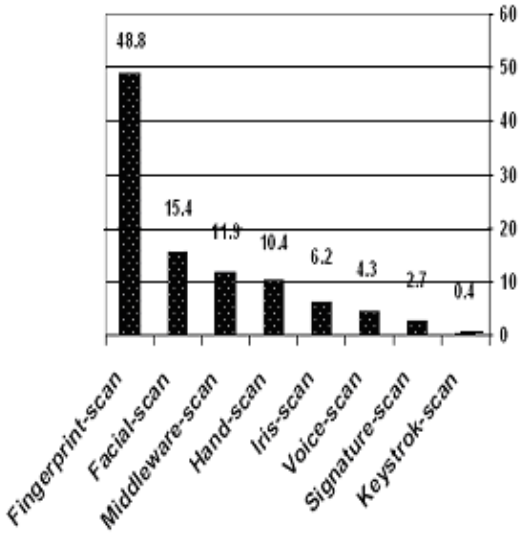


Figure –8

On the other hand, the growth of biometrics industry, in the last five years, is of an exponential form (Figure –9) [1].

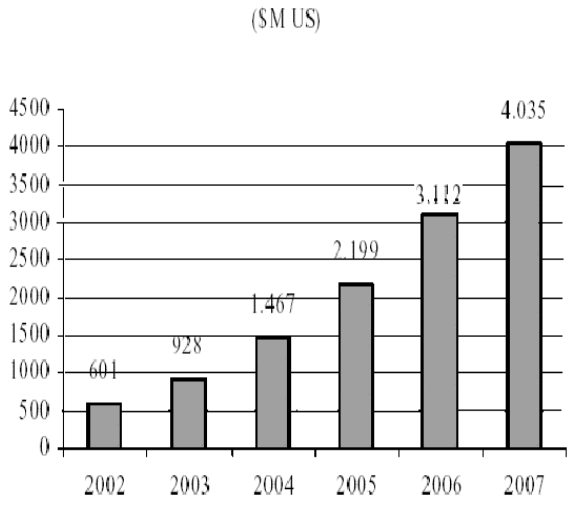


Figure –9

4- Fingerprint Recognition

4-1 Fingerprint Patterns

The pattern o a fingerprint is consisted of *ridges* and the spaces between them- *valleys* or *furrows* (Figure -10). It is through the pattern of these ridges and valleys that a unique fingerprint is matched for authentication. Fingerprints are universal and unique. In other words, everyone has them and no two have ever been found to be identical.

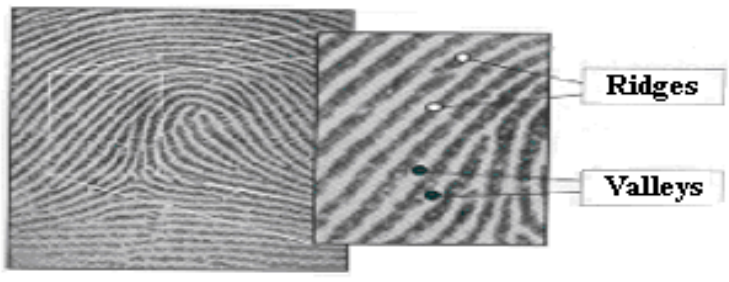


Figure –10

Fingerprints are also unchangeable. They are formed before birth and remain until decomposition of the skin that occurs some time after death. Although some deformities may result from aging, manual labor, or scarring, the overall pattern always remains distinguishable. What make fingerprints preferable are that they can be easily attained, quickly classified, and are very likely to be found at crime scenes. Not only can they identify criminals but also casualties of disasters such as plane crashes.

When an inked imprint of a finger is made, the impression is created of the ridges while the furrows are the uninked areas between the ridges. Although the manner in which the ridges flow is distinctive, other characteristics of the fingerprint (called ***Minutiae***[2]) are what is most unique to the individual. Minutiae features (Figure -11) are particular patterns consisting of [1,4]:

- ***Ridge ending (Termination)***- a ridge that ends abruptly;
- ***Bifurcation*** - a single ridge that divides into two ridges;
- ***Lake or enclosure*** - a single ridge that bifurcates and reunites shortly afterwards to continue as a single ridge;

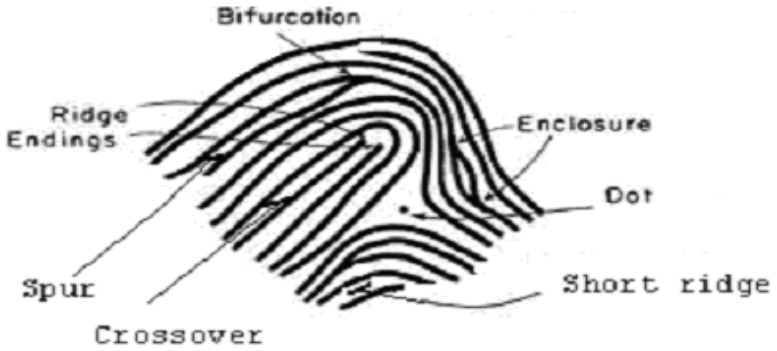


Figure -11

[2] Minutiae points are local ridge characteristics that occur at either a ridge bifurcation or a ridge ending.

- ***Short ridge (independent ridge)*** - a ridge that commences, travels a short distance and then ends;
- ***Dot (point or island)*** - an independent ridge with approximately equal length and width;
- ***Spur*** - a bifurcation with a short ridge branching off a longer ridge; and
- ***Crossover or bridge*** - a short ridge that runs between two parallel ridges.

It is these features that AFIS extract and compare for determining a match.

4-2 Fingerprint Classifications

Large volumes of fingerprints are collected and stored everyday in a wide range of applications including forensics, access control, and driver license registration. An automatic recognition of people based on fingerprints requires that the input (fingerprint) has to match with a large number of fingerprints in a database. To reduce the search time and computational complexity, it is desirable to classify these fingerprints in an accurate and consistent manner so that the input fingerprint is required to be matched only with a subset of the fingerprints in the database.

Consequently, the fingerprint classification is a technique to assign a fingerprint into one of the several pre-specified types already established in the literature, which can provide an indexing mechanism. There are four basic fingerprint classes: a. Arch, b. Tented arch, c. Loop, and d. Whorl [1,7].

a. Arch (a plain arch): it is that type of pattern in which the ridges enter on one side of the impression and flow or tend to flow out the other side with a rise or wave in the center (Figure -12).

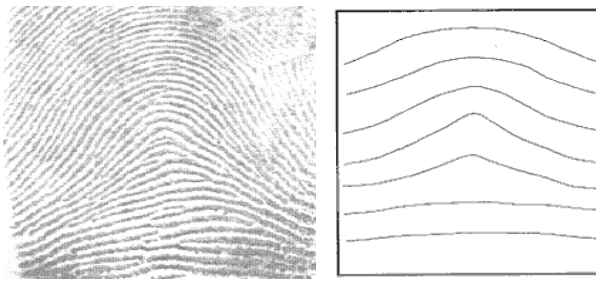


Figure -12

b. Tented Arch: It is that type of pattern where the ridges enter upon one side of the impression and flow or tend to flow out upon the other side, as in the plain arch type, except that at least one ridge exhibits a high curvature and one loop and one delta are present (Figure -13).

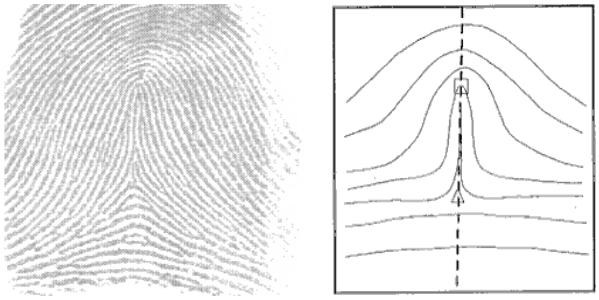
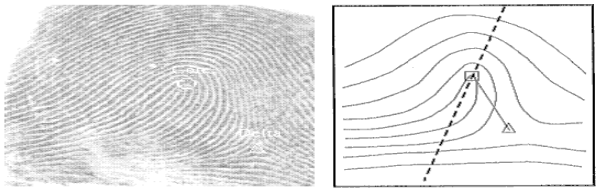
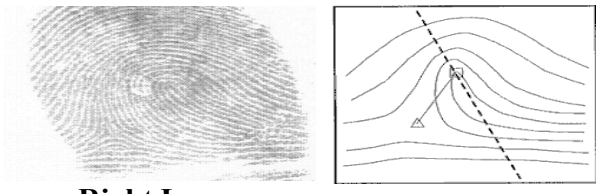


Figure -13

c. Loop: It is that type of a pattern in which one or more of the ridges enter on either side of the impression, recurve, touch or pass an imaginary line drawn from the delta to the core, and terminate or tend to terminate on or toward the same side of the impression from which they entered (Figure -14).



Left Loop



Right Loop

Figure -14

. ***d. Whorl***: The whorl is that type of a patterns in which contains at least one ridge making a complete circuit, and two deltas are present with a recurve in front of each (Figure -15). The whorl class is quite complex and in some classification schemes, it is further divided into two categories: twin loop and plain whorl.

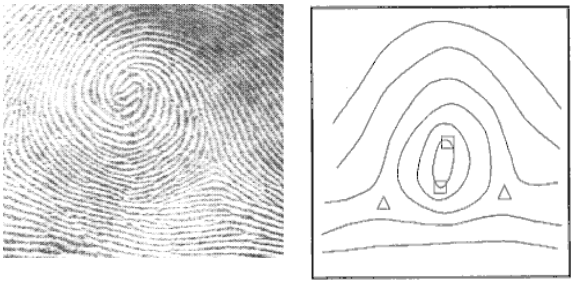


Figure -15

Loops constitute about 65% of the total fingerprint patterns; whorls make up about 30%, and arches/tented arches together account for the other 5% [6].

4-3 Fingerprint Matching

A fingerprint system may be called either a verification system or an identification system [4]:

- A ***verification system*** authenticates a person's identity by comparing the captured fingerprint characteristic with his own fingerprint template(s) pre-stored in the system. It conducts one-to-one (1 to 1) comparisons to determine whether the identity claimed by the individual is true. This mode is recommended when the number of users is large.
- An ***identification system*** recognizes an individual by searching the entire template database for a match. It conducts one-to-many (1 to N) comparisons to establish the identity of the individual.

  A fingerprint matching algorithm compares two given fingerprint images and returns either a degree of similarity or a binary decision. Only a few matching

algorithms operate directly on grayscale fingerprint images; most of them require that an intermediate fingerprint representation be derived through a feature extraction stage.

The fingerprint feature extraction and matching algorithms are usually quite similar for both fingerprint verification and identification problems. This is because the fingerprint identification problem (i.e., searching for an input fingerprint in a database of N fingerprints) can be implemented as a sequential execution of N one by one matches between pairs of fingerprints. The fingerprint classification techniques are usually exploited to speed up the search in fingerprint identification problems.

Generally speaking, it is significantly more difficult to design an identification system than a verification system. For an identification system, both speed and accuracy are critical.

5- System Design & Implementation

5-1 System Block Diagram

The major issues in designing a fingerprint authentication system include: defining the working mode, selecting hardware and choosing software components, making them work together, and defining effective administration policy.

Based on this, the proposed system shown in figure –16 is designed. It can be for general purposes applications for secure identification through fingerprint. Our system is specially designed for Access Control Application. It consists of the following parts [1]:

- Fingerprint part functioning in “verification mode” and consisting mainly of sensor unit and Fingerprint Recognition Unit.

- PC that is mainly used as Administrator PC, and for providing Database-2; where all users info (entering time, leaving time, break time,…) are stored.

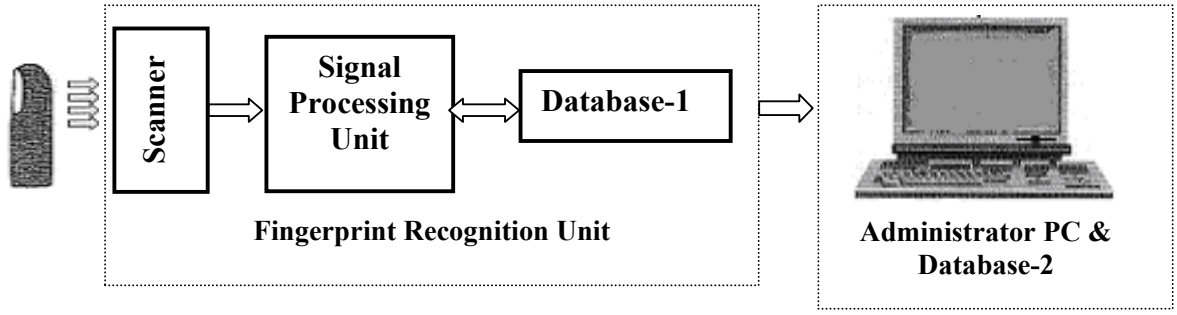


Figure- 16

5-2 System Software

The system software is consisted of tow main parts:

- The system program for which the flowchart is shown in Figure -17.
- The system database, which contains the system user information.

Flowchart Description

- **PIN Input:** The use of the system starts by entering the user PIN.
- **Processing-1:** Verifying the user inputs (fingerprint and PIN) with templates in database.
- **User Authentication:** the entered PIN allows to checking the match between the template in the database, which is related to this PIN, and the actual fingerprint data. In the case of the matching, the Pass signal is generated; otherwise the Fail signal formed.
- **Processing-2:** the main system functions (recording the attendance and leaving time, recording the out-work and brake time, performing administrator operations,..) will be performed.
- **Administrator Alert:** in case of mismatching (between template and actual fingerprint data) the administrator will be alerted.

- **Performing command of access control** & sending it to the access point.

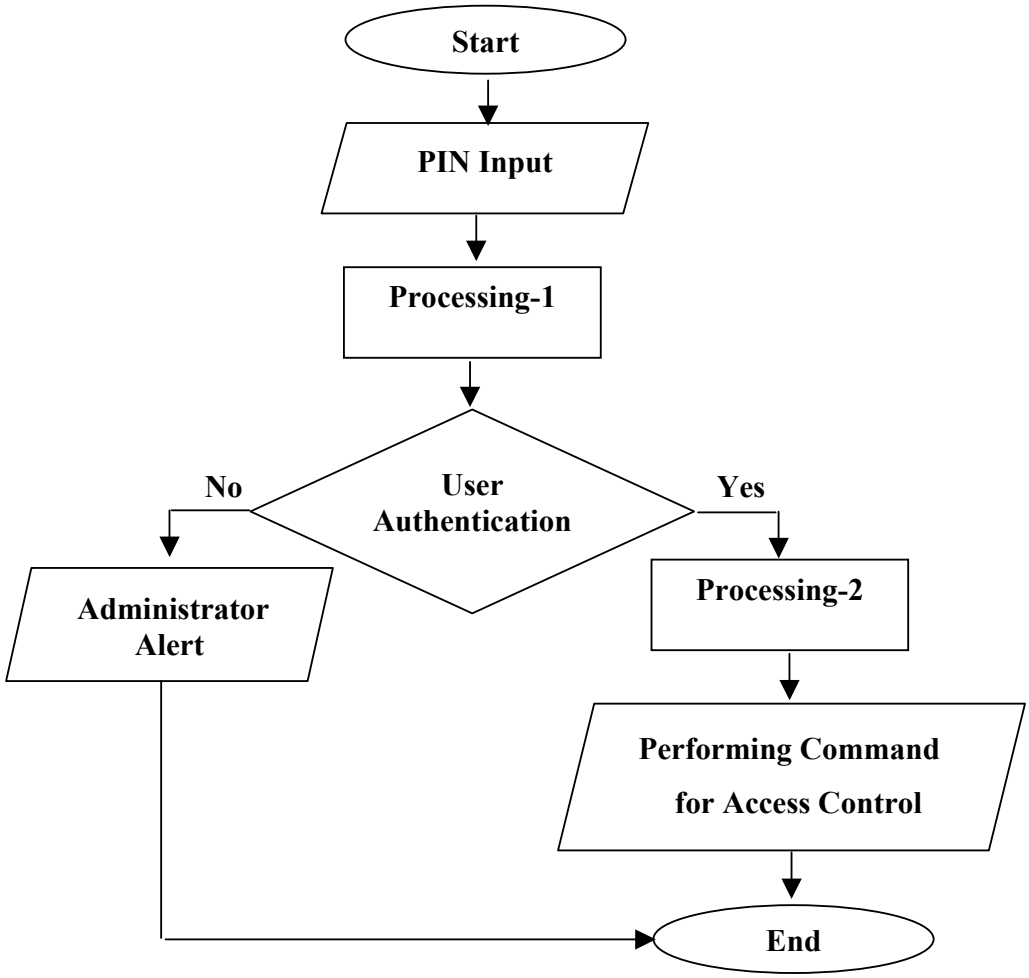


Figure -17

5-3 System usage: There are two phases:

1- **Enrollment phase:** The user fingerprint is, for the first time, stored using the sensor, in the database-1 as "user template". It is assigned with Personal Identification Number, which is entered by the keypad unit.

2- Normal usage: The user enters his PIN by the keypad; the sensor capture his fingerprint; the finger recognition unit compares the fingerprint features with the stored, in database-1, user fingerprint template. The possible cases are:

- **Match (of Fingerprint):** Captured user fingerprint features are matched with stored fingerprint templates: The user is allowed to enter/to go out to/from the establishment. The pass indicator will be lighted for short delay. A control signal (for opening /closing a virtual door) will be formed.
- **Non-match (of Fingerprint):** The user is not accepted. The fail indicator will be lighted for short delay.

In all these cases the user data will be stored in the database-2 for reference. They will be used for issuing different reports: daily, weekly, monthly,..

6- Conclusion

In the first phase of this research work, a very brief review about the biometrics, biometric types, the identifiers of each type, and a comparison between the identifiers was done. The selection of the fingerprint identifier was justified.

The second phase focused on the system design and implantation. The system worked in the verification mode (i.e. 1:1) was designed. The system software permitting to manage the system and to issue different reports in Arabic was done. The aimed system specifications were achieved.

Acknowledgement: The authors thank Mr. Abdullaziz Ahmed Assiri & Mr. Abdulrhman M. AL Hothaily for their valuable efforts.

References:

[1] S. Rahal
Authentication Fingerprint System, First National Information Technology Symposium (NITS 2006): Bridging the digital Divide: Challenges and Solutions, College of Computer & Information Sciences, King Saud University – 2006.

[2] Dr. Salah M. Rahal, Dr. Hatim A. Aboalsamah, Dr. Khaled N. Muteb
Multimodal Biometric Authentication System – MBAS; IEEE 2d International Conference on Information & Communication Technologies : From Theory to Applications - ICTTA'06; 24 – 28 April 2006, Damascus, Syria.

[3] Java Card Special Interest Group
JCSIG- Introduction to Biometrics
http://www. javacard. org/others/ biometrics_intro.htm

[4] D. Maltoni, D. Maio, A. K. Jain, S. Prabahakar
Handbook of Fingerprint Recognition, Springer - 2003

[5] Anil K. Jain, Arun Ross and Salil Prabhakar
An Introduction to Biometric Recognition
IEEE Transactions on Circuits and Systems for Video Technology, Special Issue on Image- and Video-Based Biometrics, August 2003

[6] Dave Mintie's
http://www.biometricwatch.com/ Copyright © 2003

[7] Arun Ross, Salil Prabhakar and Anil Jain
http://biometrics.cse.msu.edu/index.html

[8] New numerical methods of fingerprints' recognition based on mathematical description arrangement of dermatoglyphics and creation of minutiae.
http://www.optel.com.pl/software/english/method.htm,

[9] Components of biometrics
http://securitysa.com/Article.ASP pklArticleID=3316&pklIssueID=487, 12/2004.

[10] J. Wayman, A. Jain, D. Maltoni, D. Maio
Biometric Systems, Technology, Design and Performance Evaluation, Springer – 2005.