DESIGN OF A FINGERPRINT AUTHENTICATION SYSTEM FOR ACCESS CONTROL

Omoyele Ajoke Akinsowon, Olumide Sunday Adewale, Boniface Kayode Alese

Federal University of Technology, Akure, Department of Computer Science

ABSTRACT: With increasing use of the internet, there is increasing opportunity for identity fraud, organised crime, money laundering, theft of intellectual property and other types of cybercrime. There has also been an increase in reported biosecurity incidents, border control incidents and terrorism. The events of September 11 2001, the recent one that occurred here in Nigeria on the 24th of December, 2009 and many more occurrences have triggered increased response from governments, intelligence and law enforcement agencies world-wide. The structure of an automated fingerprint authentication system is described in this project work. The system completely eliminates the need for manual perusal of fingerprints to find a possible match.

KEYWORDS: Biometric, Security, Authentication, Fingerprint, Minutiae

1. INTRODUCTION

The word "biometric" is coined out of two Greek words 'bios' and 'metrikos', meaning 'life' and 'measure' respectively ([JP04]). It also means "measurement of life ". Biometrics is the method of utilizing a physical identifier such as fingerprints, facial geometry, iris scanning or other unique physiological feature to identify and authenticate an individual's credentials to access a facility, network or computer. True biometric authentication is the "holy grail" of credential management. Uniquely identifying an individual and authenticating access based upon criteria that cannot be duplicated virtually guarantees network and fazcility security. Biometry, as the science of studying mathematical or statistical properties in physiological and behavioural human characteristics, is widely used in forensic and non-forensic applications in security field such as remote computer access, access control to physical sites, transaction authorization. ([P+01]).

Biometric recognition, or biometrics, refers to the automatic authentication of a person based on his/her physiological or behavioral characteristics ([JP04]). Biometric recognition offers many advantages over traditional personal identification number (PIN) or password and token-based (e.g., ID cards) approaches; for example, a biometric trait cannot be easily transferred, forgotten or lost, the rightful owner of the biometric template can be easily identified, and it is difficult to duplicate a biometric trait. Some well-known examples of traits used in biometric recognition are fingerprint, iris, face, signature, voice, hand geometry, retina, and ear. A number of commercial recognition systems based on these traits have been deployed and are currently in use. Biometric technology has now become a viable and more reliable alternative to traditional authentication systems in many government applications. With increasing applications involving human-computer interactions, there is a growing need for fast authentication techniques that are reliable and secure. Biometric recognition is well positioned to meet the increasing demand for secure and robust systems.

There are many different types of biometric authentication methods with more being implemented every day. Among all the biometric techniques, fingerprint-based identification is the oldest method which has been successfully used in numerous applications. Everyone is known to have unique, immutable fingerprints. A fingerprint is made of a series of ridges and furrows on the surface of the finger. The uniqueness of a fingerprint can be determined by the pattern of ridges and furrows as well as the minutiae points. Minutiae points are local ridge characteristics that occur at either a ridge bifurcation or a ridge ending. The relative position of these minutiae is used for comparison, and according to empirical studies, two individuals will not have eight or more common minutiae. ([P+01]).

Several requirements that need to be met by a particular biometric trait when being considered for use in an authentication system are listed below:

(i) Universality: every individual should possess the trait,

(ii) Distinctiveness: the trait for two different persons should be sufficiently different to distinguish between them. The higher the degree of distinctiveness, the more individual the identifier is.

(iii) Robustness: refers to the extent to which the trait is subject to significant changes over time. These changes can occur as a result of age, injury, illness, occupational use or chemical exposure. A highly robust biometric does not change significantly over time while

a less robust one will change. For example, the fingerprint which does not change throughout a person's lifetime is more robust than one's voice,

(iv) Permanence: the trait characteristics should not change, or change minimally, over time, and

(v) Collectability: the trait can be measured quantitatively. This means that the trait can be easily presented to a sensor, located by it, and converted into a quantifiable digital format.

The following considerations are however important for practical biometric systems

(i) Are the performance and authentication rates of the system at acceptable levels (if implemented in different operational environments) when measured in terms of speed, recognition accuracy and robustness?

(ii) Will the biometric trait be widely accepted by the public for use in their daily lives, and

(iii) Will the system based on the trait be easily attacked or spoofed.

The main requirements of a practical biometric system are that it should have acceptable recognition performance rates, recognition speed and cost. In addition, it should protect the user from privacy intrusions and be robust with respect to various spoofing attacks. Among all the biometric traits used for authentication, fingerprint-based recognition has the longest history (almost 100 years) and has been successfully adopted not only in forensic applications, but in an increasing number of civilian applications. The reason behind this success is because fingerprints generally meet the requirements of a biometric trait discussed in the previous paragraph. ([UJR05]).

2. REVIEW OF RELATED WORK

There are several approaches to Fingerprint Authentication.

2.1 Using Genetic Algorithms

Using Genetic Algorithms: In automated fingerprint identification systems (AFIS), an efficient and accurate alignment algorithm in the preprocessing stage plays a crucial role in the performance of the whole system. In a previous study ([HT98]), it was concluded that the accuracy of registration in the preprocessing stage played a crucial role in determining the accuracy of the whole system. Most of the false rejection and false acceptance errors were results of inaccurate registration of the fingerprint image pair. In order to find the optimal registration, they had to try each point in the whole search space. Given a pair of images (F_n, F_m) that have a dimension of N x N and M x M (N>M) respectively, point (x_0, y_0) denotes the left-bottom corner coordinate of Fm and angle T denotes the rotation degree (see Figure 1). Both x_0 and y_0 can have a value within range of 0 to N (N is the size of larger image).

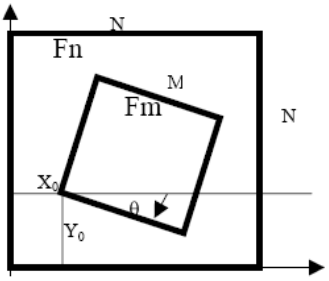

Fig. 1. Meanings of X_0, Y_0 and T

2.2 Using Back-propagation Neural Network

A neural network is an information processing system. It consists of massive simple processing units with a high degree of interconnection between each unit. The processing units work cooperatively with each other and achieve massive parallel distributed processing. The design and function of neural networks simulate some functionality of biological brains and neural systems. The advantages of neural networks are their adaptive-learning, self-organization and fault-tolerance capabilities. For these outstanding capabilities, neural networks are used for pattern recognition applications. Some of the best neural models are back-propagation, high-order nets, time-delay neural networks and recurrent nets.

The back-propagation neural network (BPNN) is a multi-layered, feed-forward neural network that is fully interconnected by layers. Thus, there are no connections that by-pass one layer to go directly to a later layer. The BPNN is called a mapping relationship between its input and output. The figure below shows the three-layer BPNN architecture.

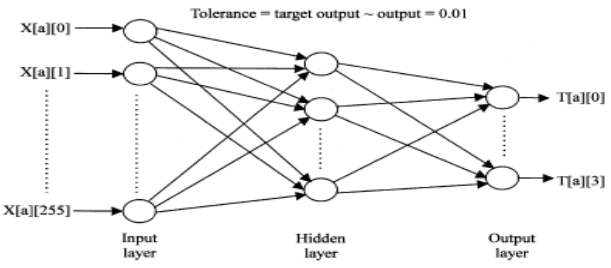

Fig 2. Three-layer neural network (Rashid et al, 2006)

2.3 Using Clusters Algorithm

This method of ANN achieves fingerprints' personal authentication in a short period of time. Neural

networks can be classified into recurrent and feed-forward categories. Feed-forward networks do not have feedback elements; the output is calculated directly from the input through feed-forward connections. In recurrent networks, the output depends not only on the current input to the network, but also on the current or previous outputs or states of the network. For this reason, recurrent networks are more powerful than feed-forward networks and are extensively used in control, optimization, and signal processing applications. ([Moh04]).

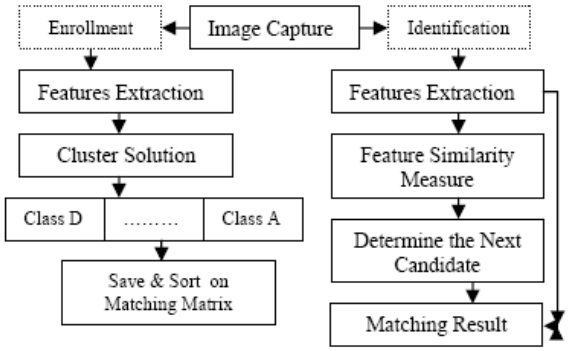

Fig.3. Chart of the Proposed Identification Algorithm ([Moh04])

3. OUR APPROACH

The proposed automated fingerprint authentication system conceptualized in figure 4 below comprises the following phases:
a) Fingerprint Acquisition/ Enrollment
b) Fingerprint Image Enhancement
c) Minutiae Extraction
d) Minutiae Matching
e) Fingerprint Classification/Authentication

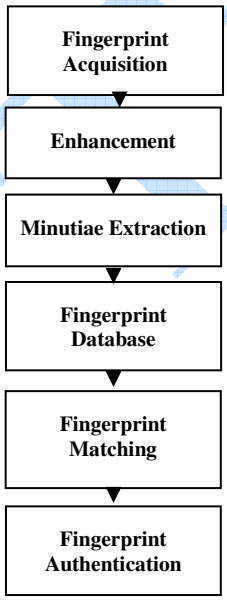

Fig. 4. Functional block diagram of the proposed Fingerprint Authentication system

3.1 Fingerprint Acquisition

The proposed method for this thesis is the live scan/on-line method because it is fast and easy to use without necessary need for expertise unlike the off-line method which is cumbersome, slow and returns large deformations due to the inherent nature of the rolled acquisition process despite the need for practice and skill for its use.

3.2 Fingerprint Sensing

There are two primary methods of sensing/acquiring a fingerprint image:
(a) **Inked scan (off-line):** The off-line approach is used to produce an impression of the finger on an intermediate medium such as paper.
(b) **Live scan (ink-less or on-line):** The live-scan fingerprint is a collective term for a fingerprint image obtained directly from the finger without the intermediate step of getting an impression on paper.

3.3 Fingerprint Storage

The features extracted during enrolment are saved in a formulated fingerprint database as fingerprint template (in binary format) for future comparison against other fingerprint templates. The database stores the fingerprints and other information peculiar to each fingerprint. For each fingerprint, the following information is stored in the database:

a. An identification number associated to the person whose fingerprint was captured
b. The fingerprint template
c. The fingerprint owner's name

Using the available information in the database, the following tasks could be performed:

a. Form an association between the fingerprint and the owner.

Associate extracted features to a particular fingerprint.

3.4 Fingerprint Classification

Fingerprint classification identifies the typical global representations of fingerprints. Global representations include locations of critical points (e.g., core and delta) in a fingerprint. A typical fingerprint classification scheme categorizes the prints into the following six major classes: whorl, right loop, left loop, arch, twin loop, and tented arch. Sometimes, a synthetic category called scars is included to classify fingerprints mutilated with scars, thus obscuring the possibility of accurately determining its true class. It is at this stage that the minutiae set obtained from an

individual's fingerprint is stored as a template for that subject. When analyzed at the global level, the fingerprint pattern exhibits one or more regions where the ridge lines assume distinctive shapes (characterized by high curvature, frequent termination, etc.). These regions (called singularities or singular regions) may be classified into three typologies: loop, delta, and whorl. Singular regions belonging to loop, delta, and whorl types are typically characterized by ∩, Δ, and O shapes respectively.

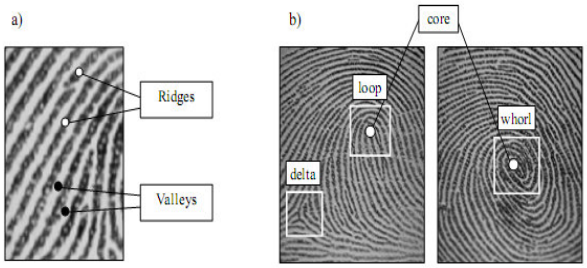

Fig.5. a) Ridges and valleys on a fingerprint image; b) singular regions (white boxes) and core points (small circles) in fingerprint images. ([JFR08])

3.5 Minutiae Extraction

Minutiae extraction is a process of studying and deriving useful information from filtered image patterns. The derived information may be general features which are evaluated to ease further processing. For example, in image recognition, the extracted features will contain information about gray shade, texture, shape or context of the image. This is the main information used in image processing. Extracting minutiae from the skeleton of the fingerprint requires a method that is able to distinguish and categorize the different shapes and types of minutiae.

At this stage of the proposed algorithm, the Crossing Number (CN) method will be employed. This concept would be adopted with the use of the skeleton image where the ridge flow pattern is eight-connected.

The following are the major tasks that would form this stage:

a) Minutiae extraction by scanning the local neighbourhood of each ridge pixel in the image using a 3x3 window.

b) Computation of CN value; which is defined as half the sum of the differences between pairs of adjacent pixels in the eight-neighbourhood.

c) Classification of the ridge properties into ridge ending, bifurcation or non-minutiae point.

Identification of ridge pixel with three-ridge pixel neighbors as ridge bifurcations and those with one-ridge pixel neighbors as ridge endings.

The CN for a ridge pixel P is given by

$$CN = 0.5 \sum_{i-1}^{8} |P_i - P_{i+1}| \quad P_9 = P_1$$

where P_i is the pixel value in the neighbourhood of P. For a pixel P, its eight neighbouring pixels are scanned into an anti-clockwise direction.

3.6 Feature Matching

Extracted minutiae from the fingerprint are together forming a point pattern in plane. Therefore matching two minutiae point patterns with each other is considered a 2-D point pattern problem. Hence, an algorithm that localizes the maximum number of mutual points in the two point patterns is adopted for this research. A minutia is determined by its attributes. Matching the minutia is to match its three attributes. In this algorithm, noting that the three attributes are independent, we can separately calculate the possibility of matching one attribute. After casting grids on two fingerprints, namely A and B, only the "effective area" is considered as shown below.

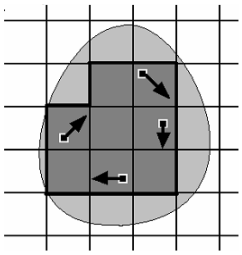

Fig.6. Grids on a fingerprint ([Sto88])

Distribution Fitting

Side length of grid r:

In an actual fingerprint image, the value of M is related with r - the side length of the grids. r should be so large that the same minutia point in different images can fall in the same grid, meanwhile r should be small enough to contain at most one distinct minutia. So the value of r should be determined with great caution. The approach here is to fit the distribution of position distance of the same minutia in different impressions along x and y axes separately, from which we can choose a proper lower bound of r.

This algorithm involves the following:

a. Detection of a minutia by its attributes.
b. Matching the 3 attributes (number, direction and type/class) of each minutia.

i) Matching in grid number
ii) Matching in direction
iii) Matching in type

iv) Matching of minutiae

Considering the assumption that the three attributes are independent, the probability that two minutiae are matched in both direction and type is obtained from the product of the two separate probabilities:

$$P = P_{\alpha} x P_{t} = \frac{1}{8} x \frac{1}{2} = \frac{1}{16}$$

4. SYSTEM IMPLEMENTATION

The technological approach for the implementation of this system is based on Java as the front-end and Mysql relational database running on windows operating system as the back-end.

The design of the proposed fingerprint authentication system is illustrated in the flowchart below as follows. It is based on four major steps:

- Initializing the Fingerprint System's library,
- Capturing images from a fingerprint reader or loading them from files,
- Extracting a template for each captured image,
- Choosing between enrolling a template (that is, a new one) or matching it against others in the database.

Usually the processes of capturing, extracting, enrolling or matching are repeated until the application is finished.

Once the capture module is initialized, and a supported fingerprint reader is plugged into the system, a corresponding image capture event is activated on the fingerprint reader. Also, as the fingerprint image is captured, another event is triggered. Finally, when the finger is removed from the fingerprint reader, the corresponding sets of events are started as well.

4.1 The Fingerprint Application

The finger is placed on the fingerprint scanner or reader with much pressure so that the captured image is of high quality. The system determines the quality of the image in order to ensure that only the best quality fingerprint template is stored into the database by using fingerprint image quality determination during enrollment.

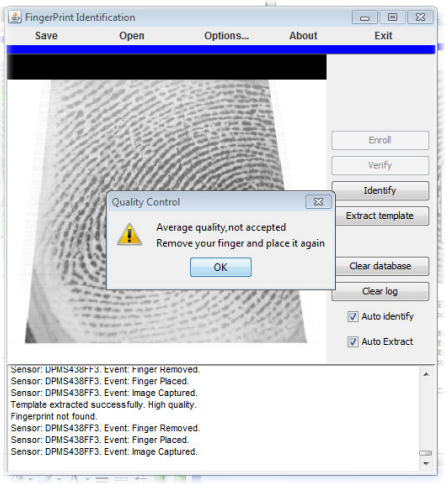

Fig. 7. Fingerprint Quality Assessment

This phase must be satisfied before the system allows Enrollment of the fingerprint image.

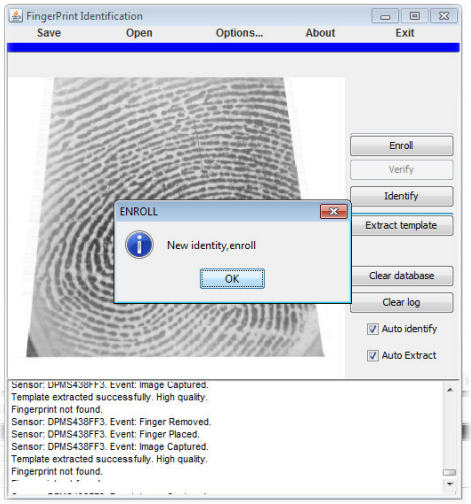

Fig. 8. Fingerprint Capture

Hence, the system requires a fresh capture of the finger until a satisfactory quality image is acquired. When the system is satisfied with the quality of the image, it prompts the need to go ahead with the enrollment.

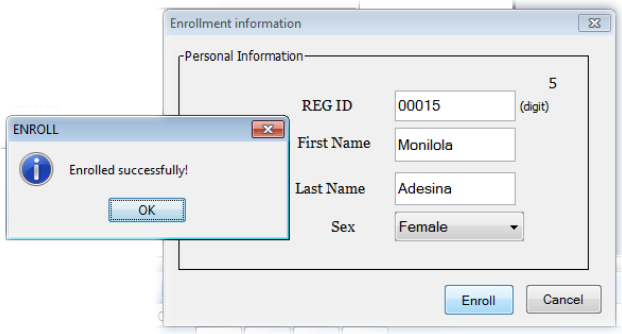

Fig. 9. Fingerprint Enrollment

By clicking the "Enroll" button, the "Enrollment information" dialog box comes up.

At this prompt, details of the owner of the finger are registered against the image. Duplicate enrollment is controlled. This option is used to protect the application from enrolling duplicate fingerprint images.

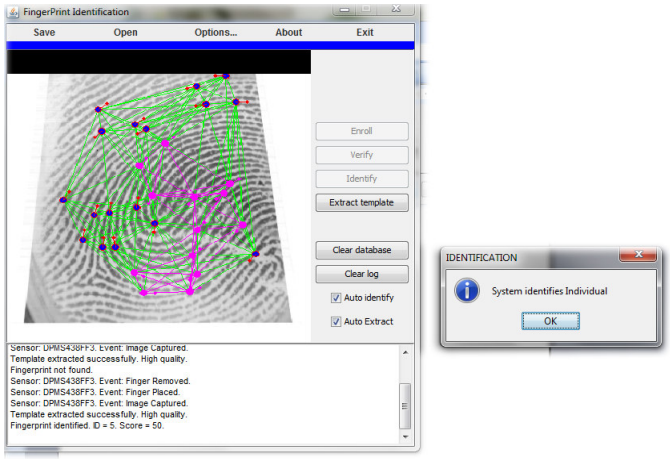

Fig. 10. Fingerprint Identification

By checking the "Auto identify" option, whenever a finger is placed over the reader, the sample will try to automatically identify the fingerprint; the result will be shown in the log box. Once the finger is placed on the scanner, the system identifies the fingerprint. It does this by displaying the details of the individual who owns the fingerprint. This feature ensures that duplicates of the same image are not enrolled.

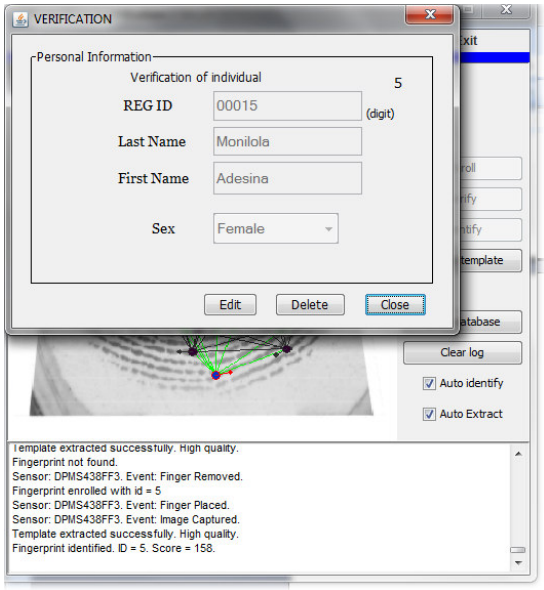

Fig. 11. Verification of Fingerprint

4.2 Fingerprint Database

As the fingerprint is being captured, its details are stored in a database. This system uses the Mysql database as its back-end.

```
mysql> select * from data;
+------+-----------+-----------+-----------+--------+
| ID   | matricNo  | LastName  | FirstName | sex    |
+------+-----------+-----------+-----------+--------+
|    1 | 0001      | Adelaide  | Atkins    | Female |
|    2 | 0002      | Philomena | Rodriguez | Female |
|    3 | 0010      | Adebola   | Olupitan  | Male   |
|    4 | 00017     | Salewa    | Dipeolu   | Female |
|    5 | 00015     | Monilola  | Adesina   | Female |
+------+-----------+-----------+-----------+--------+
5 rows in set (0.00 sec)
```

Fig. 12. Fingerprint database

4.3 System Performance Analysis

Table 4.1 Analysis of the Fingerprint Authentication System

Fingerprint ID	False Acceptance Rate (FAR)	False Rejection Rate (FRR)
1	0.01%	1.0%
2	0.012%	4.0%
3	0.03%	3.0%
4	0.02%	0.5%
5	0.01%	1.0%
6	0.05%	3.0%
7	0.01%	4.5%
8	0.018%	5.0%
9	0.03%	1.0%
10	0.02%	3.0%

The accuracy of the system is quantified in terms of false acceptance ratio (FAR) and the false rejection ration (FRR). An FAR of 1% was obtained for an FRR of 7% for this database. The Equal error rate (FAR=FRR) for the system was found to be 5%. This implies an accuracy of 95%. The main reason for the rate of FRR is the low pressure of the finger on the scanner. Hence, it is essential that some pressure is exerted on the scanner so that the fingerprint can be captured well in order that it may be authenticated. The finger should be held down on the scanner until the red light blinks but it should be noted that a dry skin takes longer. If the error continues after all the listed methods have been used, then the fingerprint may need to be re-registered. Also, in the event that there is difficulty acquiring a scan of the fingerprint, the reader window may need cleaning.

5. DISCUSSIONS AND FUTURE WORK

The critical factor for the widespread use of fingerprints is in meeting the performance (e.g, matching speed and accuracy) standards demanded by emerging civilian identification applications. Unlike an identification based on passwords or tokens, performance of the fingerprint-based identification is not perfect. There will be a growing demand for faster and more accurate fingerprint matching algorithms which can (particularly) handle

poor quality images. Some of the emerging applications (e.g., fingerprint-based smartcards) will also benefit from a compact representation of a fingerprint. The design of highly reliable, accurate, and foolproof biometrics-based identification systems may warrant effective integration of discriminatory information contained in several different biometrics and/or technologies. The issues involved in integrating fingerprint-based identification with other biometric or non-biometric technologies may also constitute another important research topic.

REFERENCES

[HT98] **Ammar Hany, Yongyi Tao** – *Fingerprint Registration Using Genetic Algorithms*, Retrieved from citeseerx.ist.psu.edu, 1998

[JP04] **A. Jain, S. Pankanti**, *Fingerprint Classification and Matching,* Retrieved from citeseerx.ist.psu.edu, 2004

[JFR08] **A. K. Jain, P. J. Flynn, A. Ross** - *Handbook of Biometrics***,** ISBN-13: 978-0-387-71040-2, e-ISBN-13: 978-0-387-71041-9, Springer Science + Business Media, 2008

[Moh04] **M. A. A. Mohamed** - *Artificial Neural Networks Based Fingerprint Authentication With Clusters Algorithm*, Minia University, Faculty of Engineering, Department of Electrical, Communications and Electronics section, Egypt, 2004

[P+01] **M. Poulos, E. Magkos, V. Chrissikopoulos, N. Alexandris** - *Secure Fingerprint Verification Based On Image Processing Segmentation Using Computational Geometry Algorithms,* 2001

[RA06] M. Rashid, A. K. M. Akatar Hossain - Fingerprint Verification System Using Artificial Neural Network, Information Technology Journal 5 (6): 1063-1067, ISSN 1812-5638, 2006

[Sto88] **D. Stoney** - *Distribution of Epidermal Ridge Minutiae,* Am. J. Physical Anthropology, vol. 77, pp. 367-376, 1988

[UJR05] **U. Umut, A.K. Jain, A. Ross** – *Biometric Template Security: Challenges And Solutions,* Appeared in the Proceedings of the European Signal Processing Conference (EUSIPCO), (Antalya), Turkey, 2005