FINGERPRINT RECOGNITION TIME & ATTENDANCE SYSTEM DEVELOPMENT

Dr. Salah M. Rahal*[1], Dr. Hatim A. Aboalsamah*[2], Dr. Khaled N. Muteb*[3]

Computer Technology Dept. College of Computer and Information Sciences, King Saud University, P.O. Box 51178, Riyadh11543, KSA, Fax: +966(1) 4675630

Rahal@ccis.ksu.edu.sa*[1], Hatim@ccis.ksu.edu.sa*[2], Kmutib@digi.net.sa*[3]

Keywords: Biometrics, Identification, Minutiae, Template, Verification.

Abstract

Biometrics refers to the automatically identifying humans by means of distinctive and behavioral characteristics called identifiers. Biometric recognition forms a strong link between a person and his identity because biometric traits cannot be easily shared, lost, or duplicated. Furthermore they are convenient and secure. For these reasons, they are preferred over traditional methods because of convenience and security.

Due to high accuracy, inexpensive equipments and ease of installation, fingerprint identifier is the best of biometrics types and in this paper is focused on it.

In the first part, the fingerprint pattern, its structures at global and local levels and fingerprint recognition phases are described.

In the second part the developed Time & Attendance System is described. The system is developed around a fingerprint module and personal computer.

1- Review

Biometrics refers to the automatically identifying humans by means of distinctive physiological (such as fingerprints, face, iris, retina) and behavioral (such as signature, gait) characteristics, called biometric identifiers [7].

This method of identification is preferred over traditional methods involving passwords and PINs (Personal Identification Numbers) because of convenience (nothing to remember or to carry) and security (can't be shared, stolen, or forged). A biometric system can operate either in A verification mode (1-to-1) or in an identification mode (1-to-N) [1,4,8].

Due to high accuracy, inexpensive equipments and ease of installation, fingerprint identifier is an attractive type of biometrics and it is used in our actual work.

Fingerprints are fully formed at about seven months of fetus development and finger ridge configurations do not change throughout the life of an individual except due to accidents such as bruises and cuts on the fingertips [4,10].

2- Fingerprint Pattern

A fingerprint pattern is composed of a sequence of ridges and valleys that run next to each other. The ridges are the raised skin; while the valleys are the lowered skin. In fingerprint image, the ridges appear as dark lines while the valleys are the light areas between the ridges. Many characteristics can describe the ridges. The two most prominent of them, called "minutiae", are ridge termination and ridge bifurcation (Figure-1). Typically, a fingerprint image may contain between 20 to 70 minutiae depending on the fingerprint sensor characteristics (e.g., sensor area) and the position of the user's finger on the sensor [2,4].

Figure-1

Storing raw fingerprint images may be problematic for large AFISs - Automatic Fingerprint Identification Systems. Each fingerprint card, when digitized at 500 dpi requires about 10 MB of storages. The image-based representation requires a considerable amount of storage and the digital archive could become extremely large [4].

3- Fingerprint Recognition [1,12]

3-1 Enrollment Phase

This phase involves the fingerprint scanning, image enhancement, feature extraction and classification as shown in the figure-2. The processing in this phase is performed off-line.

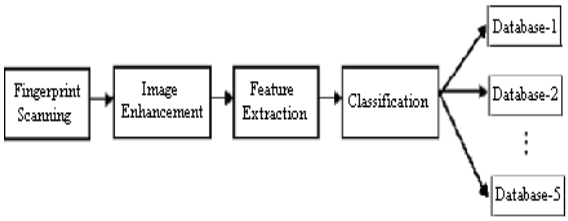


Figure-2

3-2 Authentication Phase

This phase, on-line processing, is similar with the previous phase except the final step where a minutiae matching is performed (figure-3).

Figure-3

a- Fingerprint Scanning

The acquisition of fingerprint images is performed by a fingerprint scanner.
There are a number of different ways to get the fingerprint image. The most common methods today are optical scanning and capacitance scanning [13].

b- Image Enhancement

The fingerprint recognition techniques rely heavily on the quality of the input fingerprint images. A significant percentage of fingerprint images (approximately 10%) is of poor quality.
Usually, the input of the enhancement algorithm is a gray-scale image. The output may either be a gray-scale or a binary image, depending on the algorithm.

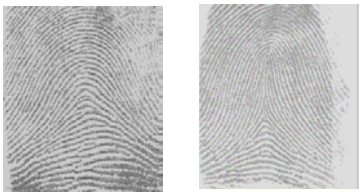
c- Feature Extraction

Although some fingerprint matching techniques directly compare images through correlation-based methods, the gray-scale image intensities are to be an unstable representation. Most of the fingerprint recognition and classification algorithms require a feature extraction stage for identifying salient features [4].
The feature extracted from fingerprint images often have a direct physical counterpart (e.g., singularities or minutiae), but sometimes they are not directly related to any physical traits (e.g., local orientation). Features may be used either for matching or their computation may serve as intermediate step for the derivation of other features. For example, some preprocessing and enhancement steps are often performed to simplify the task of minutiae extraction.

d- Fingerprint Classification

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. According to the ridges flow structure there are five basic fingerprint classes: Loop (left & right), Whorl, Arch and Tented Arch (figure-4) [3,5,7].

a. Left Loop b. Right Loop c. Whorl



d. Arch e. Tented arch

Figure -4

The natural portion for these classes is: 33.8 % for Left Loop; 31.7 % - Right Loop, 27.9 % - Whorl, 3.7 % - Arch and 2.9 for Tented Arch [2,4].

e- Fingerprint Matching

Fingerprint matching is a difficult problem due to the large intra-class variations (variations among different impressions of the same finger) and the small inter-class variations (images of different fingers may appear quite similar) [4].
There are mainly three-class categorization of fingerprint matching techniques [4]: Minutiae-based matching, Correlation-based matching and ridge feature-based matching.

❖ Minutiae-Based Matching

It is based on extracting and matching minutia points between two fingerprint images: The actual fingerprint image (input) and the previously stored template. Each minutia is represented by a feature vector of fixed length. The features (attributes) representing a minutia point typically consist of its location, orientation, type (e.g.,

* For example, there are more than 81 million fingerprints currently in the FBI Fingerprint database, and every day approximately 7000 new individual records are added to the files [7].

ridge-ending or ridge-bifurcation), and other local information like the ridge count and the quality of the fingerprint region around the minutia point. The matching of two minutiae sets is usually posed as a point pattern matching problem and the similarity between them is proportional to the number of matching minutia pairs [5].
Most fingerprint matching systems are based on this method of matching. Generally, minutiae-based methods require a significant amount of preprocessing to produce accurate results [4].

❖ **Correlation -Based Matching**

Two fingerprint images are superimposed and the correlation (at the intensity level) between corresponding pixels (of the input image and the template) is computed for different alignment (e.g., various displacement and rotation since the input image might be oriented differently than the template image). The maximum correlation value produced in this process relates to the best possible alignment between the input and the template. Main advantages of these techniques [4,6]:

- Better results than minutiae extraction methods for low quality fingerprint images where it may be difficult to reliably extract the actual minutiae points.
- A better computational efficiency than the standard minutiae-based techniques: The amount of pre-processing to produce acceptable results isn't significant (the only pre-processing methods that are applied are a binarization and thinning phase).

❖ **Ridge Feature-Based Matching**

Here, the ridge features such as local orientation and frequency, ridge shape, texture information are used in these approaches. These features of the input image and the template are used for the matching.
The basic ridge features are obtainable from any quality image. Since minutiae-based methods require an image of good quality, ridge features offer an alternative for poor images. Furthermore, ridge feature-based techniques do not have to be limited to images of poor quality. They can be used in conjunction with minutiae-based techniques to increase the accuracy and robustness of the recognition system [4].

4- Time & Attendance System Development

Generally the major issues in designing a fingerprint authentication system include: defining the system working mode (verification or identification), choosing hardware and software components and making them work together, dealing with exceptions and poor quality fingerprint images, and defining effective administration and optimization policy.
A fingerprint-based system may operate either in verification or identification mode. When the number of users is large it is recommended that the system designer choose the verification mode unless identification is strictly necessary. In fact, it is significantly more difficult to design an identification system than a verification system. For an identification system, both speed and accuracy are critical.
Time & Attendance System consists of both hardware and software. Hardware captures the user fingerprint features. Software interprets the resulting data and determines acceptability [9,11].

a- Hardware: It is consisted of the following (figure-5):

➢ *Time & Attendance Device* that includes:

- Optical fingerprint sensor that is used for the user's finger scanning.
- Fingerprint Recognition Module, which includes verification algorithm and templates.
- Indicators and additional circuits that include LEDs (for indicating the status of the verification process: success or failure), Keypad (for entering user Personal Identification Number – PIN), Buzzer (for generating sound signals "beep") and Power supply unit (110 VAC – 5 Volt DC, 800 mA).

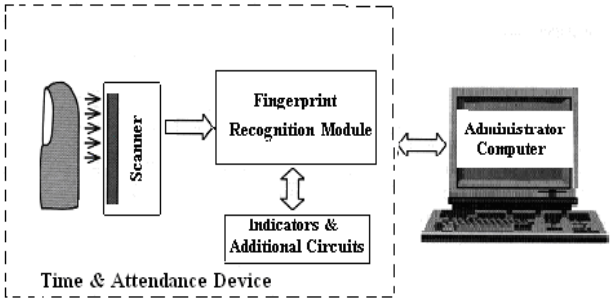


Figure-5

➢ *Personal Computer* that is mainly used:

- As administrator PC.
- For providing database where all users info (attendance, leaving time, out-work and break times) are stored.

b- Software: The system software is consisted of tow main parts:

- The system program that performs the system functions.
- The system database, which contains the system user information.

System Main Functions: The main functions are:

- Recording user attendance, leaving, out-work and brake times.
- Displaying weekly form for all users.
- Performing various reports: Absent, Late hours and Vacation.
- Administrator system monitoring.
- Performing interfacing tasks.

5- Conclusion

This paper presents the development of a biometric prototype aimed to be used as Time & Attendance system. It functions in the mode 1:1 i.e. in the verification mode. The selection of adequate hardware and software subcomponents was completed.

The system software permitting to issue different reports in Arabic, system assembly, system test and fulfillment of the aimed specifications were also completed.

References

[1] Anil K. Jain
Biometric authentication, Scholarpedia, 6/2008

[2] David H. Chahg,

Fingerprint Recognition Through Circular Sampling, http://www.cis.rit.edu/research/thesis/bs/1999/chang/thesis.html

[3] Jun Lia, Wei-YunYaub, HanWanga
Combining singular points and orientation image information for fingerprint classification, Pattern Recognition Journal 41 (2008) 353 – 366

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

[5] Qinzhi Zhang, Kai Huang and Hong Yan
Fingerprint Classification Based on Extraction and Analysis of Singularities and Pseudoridges, School of Electrical and Information Engineering University of Sydney, NSW 2006, Australia.

[6] S. Prabhakar, A. Jain,
Fingerprint Identification,
http://biometrics.cse.msu.edu/index.html.

[7] 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.

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

[9] Dr. Salah M. Rahal, Dr. Hatim A. Aboalsamh, Dr. Khaled N. Muteb
Secure Identification System – SIS, Information Technology & National Security Conference, Riyadh, K.S.A., 121/2007.

[10] Sharath Pankanti Salil Prabhakary Anil K. Jain
On the Individuality of Fingerprints, IEEE Computer Society Conference On Computer Vision and Pattern Recognition (CVPR) , pp. 805-812, Hawaii, 12/2001.

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

[12] Evaluation of Fingerprint Recognition Technologies – BioFinger; Public final Report, Bundesmat fur Sicherheit in der Informationstechnik, 8/2004.

[13] HowStuffWorks
Fingerprint Basics, 2008,
http://computer.howstuffworks.com/fingerprint-scanner1