

## SECURED ACCESS TO E-HEALTH RECORDS USING MINUTIA-BASED FINGERPRINT MATCHING ALGORITHM

<sup>1</sup>G.Niranjana, <sup>2</sup>V.Arumugam, <sup>3</sup>M.Balaji

<sup>1</sup>Department of Computer science engineering

<sup>2,3</sup>Department of Information Technology  
SRM University

**Abstract:** The most commonly used method for user authentication in ICT (information and communications technology or technologies) services are passwords or personal identification numbers (PINs). The latest development in ICT technology has allowed the use of several biometric characteristics including voice and fingerprints with the aim to improve the security. In this project, we are maintaining the e-health records of the patients including their personal information, medical history and recent vital measures. Vital measures include ECG, blood glucose, Temperature, Blood Pressure and cardiac activity. This information is stored in the database along with their fingerprint as user identification. Once the details are stored they can be accessed by using the fingerprint of the patient as authentication. A minutia-based fingerprint matching algorithm is used for authenticating the user. It eases the effort of the patient to carry the medical records and assist the physician to review their previous history of visits. This project provides secured and easy access to e-health records of the patients

### 1. Introduction

Technological developments in medical field pave way for huge collection of healthcare data that include data about patients, changing conditions, treatments prescribed, drug protocols, outcomes, etc. Normally, these data make it difficult to capture and analyze using traditional methods. E-health data sets are so large and complex and they are difficult to manage with traditional software and/or hardware; nor can they be easily managed with traditional or common data management tools and methods.

Fingerprint recognition is an active research area nowadays. An important component in fingerprint recognition systems is the fingerprint matching algorithm. According to the problem domain, fingerprint matching algorithms are classified in two categories: **fingerprint verification algorithms and fingerprint identification algorithms**. The aim of fingerprint

verification algorithms is to determine whether two fingerprints come from the same finger or not. On the other hand, the fingerprint identification algorithms search a query fingerprint in a database looking for the fingerprints coming from the same finger.

There are more number of papers concerning to fingerprint verification but, there is not any framework for fingerprint verification available on the web. So, we must implement our own tools in order to test the performance of our fingerprint verification algorithms. This motivates us to put our fingerprint verification framework available for everyone.

Our framework is implemented using ASP .Net Framework, SQL Database.

We implement the fingerprint verification algorithms proposed by Tico and Kuosmanen,[2] Jiang and Yau,[3] Medina-Pérez et al. and Qi et al. It is important to highlight that, despite the algorithm of Qi et al. is a combination of a minutiae matching algorithm with an orientation based algorithm, we implement only the **minutiae matching algorithm**.

Matching is an important process in the current fingerprint system. The aim of fingerprint matching is to achieve a high trustworthy in comparing two fingerprint image. The different impressions of the same finger make reliable matching fingerprint and most difficult problem. In this paper, a Minutiae-Based Algorithm (MBA) for fingerprint pattern recognition and matching is proposed, which is essentially a point pattern matching method. This proposed algorithm demonstrates effective recognition and matching performance of minutiae based algorithms.

The advantages of the fingerprint medical information system over other systems are:

- Low power consumption
- Improves security formats in the hospital
- We can add new patient users
- Patient database maintained individually so that we can avoid the man-made error

- Used in emergency medical situation when a patient is unconscious

This paper is organized as follows.

1. Overview of fingerprint matching algorithms.
2. Describes the databases
3. Result and Discussion.
4. Conclusion of this paper.

## 2. Overview of Minutiae Matching Algorithm

### Method 1: Using bifurcation, ridge ending

The fundamental data elements used for minutiae-based representation of a fingerprint are: the type of the ridge (bifurcation, ridge ending), the coordinates (x,y) (in pixels), the direction  $\theta$  (in radian).

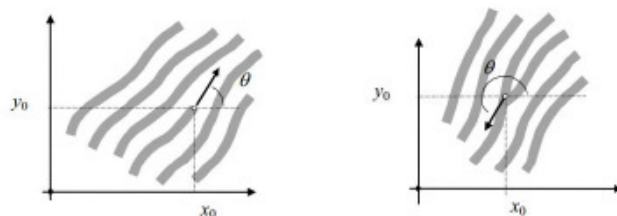


Figure 1. Minutiae representation models

The figure 1, presents the information related to two types of minutiae most used: ridge ending (to the left), bifurcation (to the right). The minutiae-based approaches uses firstly local minutiae descriptors to coarsely align two fingerprints and then computes a global matching score based on minutiae correspondences as shown in figure 2

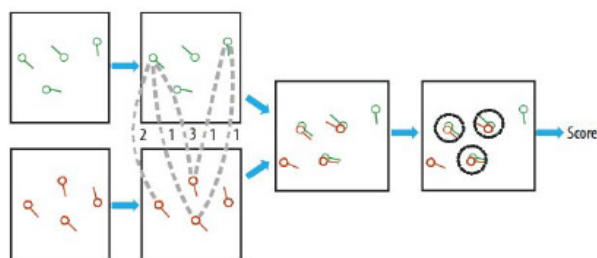


Figure 2. Minutiae representation models

The major of comparative approaches fingerprints are based on the comparison of minutiae. We have to develop effective methods for minutiae detection and extraction, in order to establish a reliable recognition system.

### Method 2: Using Binarization and Thinning

Binarization of fingerprint image which is a process to transform the image from 256 levels to two levels (0, 1) refers to (black and white) respectively. In this paper we used locally adaptive binarization method, the steps are followed:

1. The image is divided into blocks with size 16x16.
2. Mean intensity value for each block is calculated.
3. For each pixel the following rule is applied.

$$\text{pixel} = \begin{cases} 1 & \text{if intensity value} > \text{mean intensity value for the current block} \\ 0 & \text{if intensity value} < \text{mean intensity value for the current block} \end{cases}$$

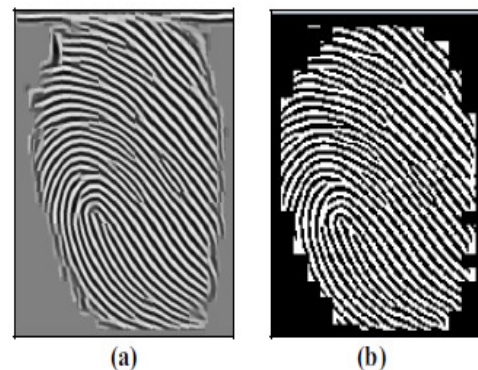


Figure 3.a. Enhancement Image  
Figure 3.b. Binarization

### 2.1 Thinning

To enhance the binary image the thinning algorithm is used to reduce the ridges of fingerprint images.

- Thinning is iterative to erode away successively the foreground pixels until they are one-pixel wide.
- Each iteration examines the 8 neighborhood of each pixel in the binary image, and checks whether the pixel can be deleted or not Minutiae Extraction
- The minutiae are extracted by scanning the local neighborhood of each ridge pixel in thinned image using a 3X3 window.
- The (Crossing Number) CN value is then computed, which is defined as half the sum of the differences between pairs of adjacent pixels in the eight neighborhood

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

Where  $P_i$  is the pixel value in the neighborhood of P

### 3. Result and Discussion

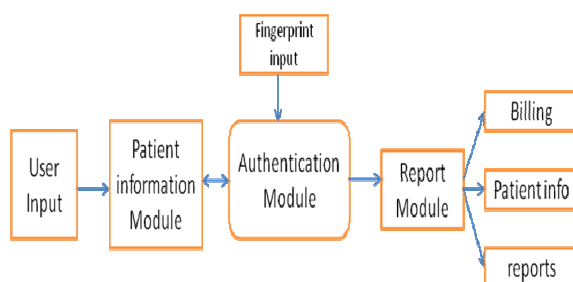
The Patient database representing the Medical Information System is created. The following parameters are included in the database creation:

- Patient's personal details
- Age and Gender
- Blood group
- Family History
- Type of Disease
- Symptoms
- Tests done and results obtained
- Doctor's comments
- Medicines prescribed

**Advantages of using this medical information system are:**

- Database can be used during emergency condition
- High security of using fingerprint
- More convenient for user authentication
- Online accessibility
- Reduction of Medical record errors

#### 3.1 System Architecture



**Figure 4.** Minutiae Matching Algorithm

#### 3.2 System modules

- Data collection (Patient Data Gathering)
- Patient information module
- Authentication module(Multi Access Control)
  - Admin Account
  - Patient Account
  - Doctor Account
- Reports module

##### A. Patient Data Gathering

In this module, patient details are collected during the first visit of the patient for consultation.

Patient data includes date of birth, date of last negative and first positive tests, root of infection, alcohol and drug usage. Clinical data are collected on a continuous basis every time the patient consults the treating physician. Data includes information such as the treatments suggested, symptoms of disease, reaction to the prescribed drugs and laboratory results.

##### B. Multi Access Control

In this module three different levels of access controls are implemented to support for three different retrieval levels.

###### Admin Account

Users having this access right will be able to add details about patients that are collected from the hospital and can also modify the patient's personal details.

###### Patient Account

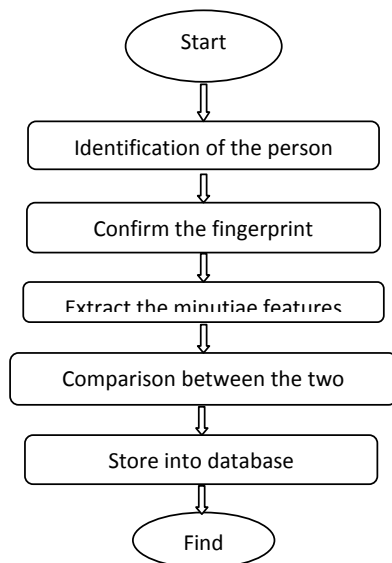
In this patient account, patients can view their medical records, drugs prescribed for them and progress in their recovery process. Patients can search or monitor their own details.

###### Doctor Account

In this doctor can view the patient disease, symptoms and their test levels, analyze and identify the disease and suggest the drug for the disease discovered.

##### C. Registration process

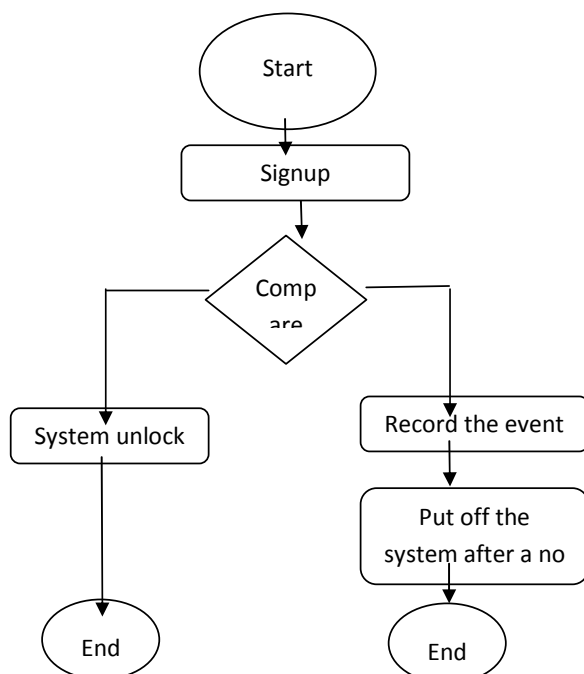
This method consists of taking a person's fingerprint using a fingerprint capturing device. During this process, the system stores the person's fingerprint into a database. The following figure shows the registration process.



**Figure 5.** Registration process Flow diagram

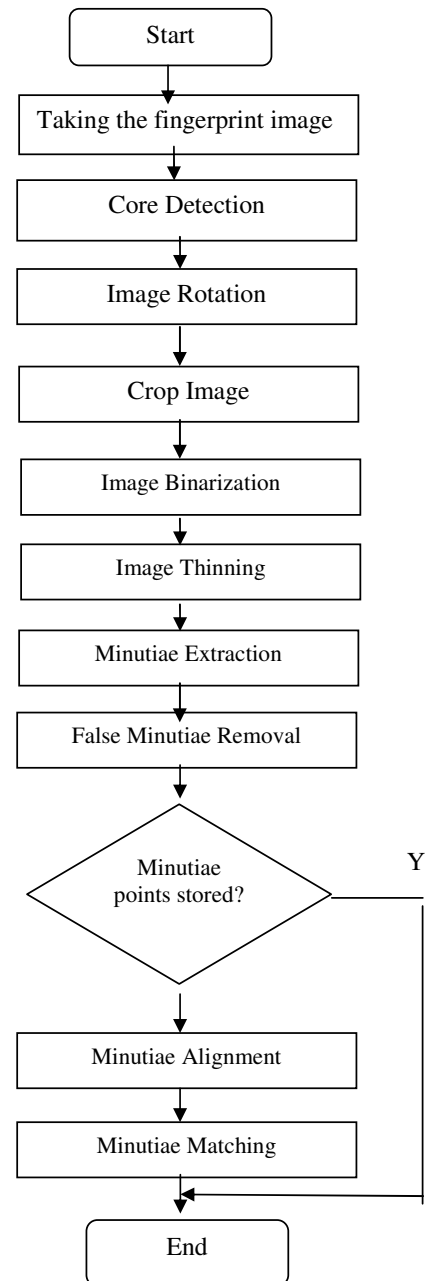
#### D. Authentication module

This module consists of comparing a captured fingerprint from the device to stored fingerprint obtained in the registration process. The following figure shows the authentication module.



**Figure 6.** Authentication Flow diagram

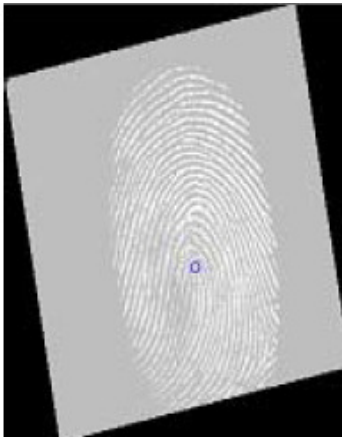
The model of fingerprint minutiae matching algorithms.



**Figure 7.** Fingerprint minutiae matching Flow diagram



**Figure 8.a.** Original image



**Figure 8.b.** Core Detection



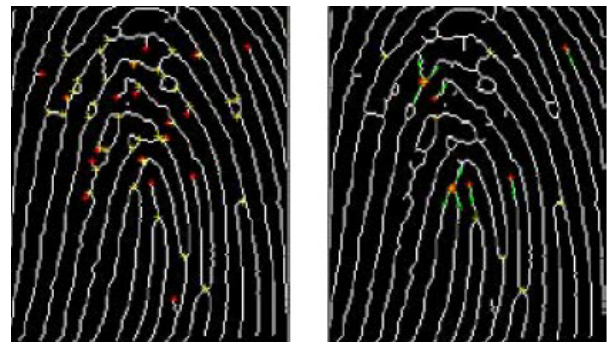
**Figure 8.c.** Rotated and cropped image



**Figure 8.d.** Image Binarization



**Figure 8.e.** Image Thinning



**Figure 8. f.** Minutiae Extraction **Figure 8. g.** Result of False Minutiae Removal

#### 4. Conclusion

This system improves the reliability of medical treatment. Fingerprint verification is considered to protect the medical information transmitted and to guarantee both the integrity and the confidentiality of the data. Patient data can be stored and retrieved by connecting to the hospital database, and thus it can be accessed globally. The main advantage of this project is online accessibility of patient database. Another crucial advantage is that it is applicable during emergency conditions. The patient need not carry the ID card with them as such there is no possibility of losing them. Medical record errors can be reduced using the finger print technique. Since fingerprint cannot be lost or forgotten like passwords, fingerprints have the potential to offer high security and more convenience for user authentication. The fingerprints are significantly more difficult to copy, share, distribute than passwords which make fingerprint recognitions the most convenient method while maintaining sufficiently high security. Furthermore, large fingerprint data need not be memorized. The emergency data such as his/her blood group and type and contact person information can be accessed during his/her finger in the emergency. Our long term goal is to create a sustainable, secure solution that allows doctors to more efficiently utilize patient data to improve the overall quality and efficiency of care. In future, the Patient database can be modified with images like X-ray, CT, MRI and graphs such as ECG, EEG, EMG, etc. The system had analyzed the symptoms and diagnosed the exact disease and also the suitable drug is suggested for the diagnosed disease. This diagnosed disease and the best suitable drugs for a patient will aid the physician in analyzing and making decisions about the kind of treatment and medication for a patient with certain health conditions. Thus minutiae matching scheme is suitable for an online processing of Health records due to its high processing speed.

#### References

- [1] Nandakumar K., Anil.K. J., and Ross A., "Introduction to biometrics", Springer, 2011.
- [2] M. Tico, P. Kuosmanen. "Fingerprint matching using an orientationbased minutia descriptor", In IEEE Trans. Pattern Anal. Mach. Intell. 25 (2003) 1009-1014
- [3] X. Jiang, W.Y. Yau. "Fingerprint minutiae matching based on the local and global structures", International Conference on Pattern Recognition (ICPR), 2000, pp. 6038-6041
- [4] Anil K. Jain, Jianjiang Feng, and Karthik Nandakumar. "Biometrics: Fingerprint matching", IEEE Comput. Soc. 2010.
- [5] A.K.Jain, A.Ross, and S.Prabhakar, "An introduction to biometric Recognition", IEEE Transaction on Circuits and Systems for Video Technology, vol. 14, no. 1, pp. 4-20, January 2004.



