CHAPTER 1

Introduction

Biometric refers to the use of distinctive anatomical and behavioral characteristics, called biometric identifiers or traits or characteristics for automatically recognizing individuals. Biometrics are becoming an essential component of effective personnel identification solution, because biometric identifiers cannot be shared or misplaced and they intrinsically represent the individual's bodily identity. Recognition of people by their body, then linking that body to an externally established "identity", forms a very powerful tool of identity management with tremendous potential consequences, both positive and negative. The word biometrics is derived from the Greek words bios (meaning life) and metron (meaning measurement); biometric identifiers are measurements from living human body.

Biometrics offer several advantages over traditional security measures. These include:

1. Non-repudiation: With token and password based approaches, the perpetrator can always deny committing the crime pleading that his/her password or ID was stolen or compromised even when confronted with an electronic audit trail. There is no way in which his claim can be verified effectively. This is known as the problem of deniability or of 'repudiation'. However, biometrics are indefinitely associated with a user and hence it cannot be lent or stolen making such repudiation infeasible.

2. *Accuracy and Security*: Password based systems are prone to dictionary and brute force attacks. Furthermore, such systems are as vulnerable as their weakest password. On the other hand, biometric authentication requires the physical presence of the user and therefore cannot be circumvented through a dictionary or brute force style attack. Biometrics has also been shown to possess a higher bit strength compared to password based systems [1] and are therefore inherently secured.
3. *Screening*: In screening applications, we are interested in preventing the users from assuming multiple identities (e.g. a terrorist using multiple passports to enter a foreign country). This requires that we ensure a person has not already enrolled under another assumed identity before adding his new record into the database. Such a screening is not possible using traditional authentication mechanisms and biometrics provides the only available solution.

There is one biometrics that has been systematically used to make identifications for over 100 years. This is a biometric that has been measured, copied and examined extensively, a biometric that does not change and is relatively easy to capture. It is a biometric that is not invasive and does not require sophisticated hardware for analysis, making it relatively inexpensive on a per search level. Because of these properties, the biometric has received the most attention and this biometric is the fingerprint.

The Fingerprint Recognition System has become a widely used technology in civilian/ commercial and forensic application. Despite this widespread use of fingerprint over the decades, which has been used as individual’s proof of identity, a reliable, fully automated recognition is still an unsolved challenging problem. In particular, the issue of how many minutiae point should be used for matching is unresolved.

1.1 Motivation Behind the Present Work

Due to the persistence need of the law enforcement and interest from the developers of biometric systems, efficient fingerprint identification systems are becoming increasingly used and an extensive research work is being carried out by the pattern recognition community. It is a common misconception that automated fingerprint identification is a solved problem. Despite significant research efforts over the past four decades, state-of-the-art fingerprint matching technology is nowhere near the theoretical upper bound on performance [2].

The general framework for fingerprint identification systems is well established in the scientific literature. The vast majority of the studies were being published and attempts were made to update and improve to the specific algorithms in use at the various levels of processing. This approach is beneficial, and these minor improvements do contribute to the overall trend towards higher accuracies. However, as the state-of-the-art is still far from its theoretical potential, it may be worth exploring radically different approaches from those currently in fashion.

1.2 Objective of the Thesis

- To conduct a thorough survey of the fingerprint recognition system.
- To developed an efficient technique for removing noise or unwanted information.
- To developed a novel fingerprint matching system which is robust against rotation.
- To developed a novel fingerprint indexing system which is efficient in terms of time complexity and image attack like rotation, noise and scaling.

1.3 Thesis Contribution

The following listed is the main contribution of the thesis:

- Introduction of primary and secondary enhancement of the fingerprint in the preprocessing stage. The primary enhancement is performed on the input fingerprint image to remove the noise from the ridge and furrow structures using Fast Fourier transformation (FFT). The Secondary enhancement is required to reduce the “hairy” (spikes) structures which lead to spurious ridge bifurcations and endings. Moreover the mismatch or alignment of the blocks in FFT is removed by Gaussian filter.
- A novel fingerprint matching algorithm using MinHeap and Euclidean distance between the core point and minutiae points is proposed. In this algorithm, a hit count and an error

tolerance, ϵ, are used for determining the level of similarity between the nodes in MinHeap which is constructed from two fingerprint images for comparison. The comparision is done only at the root node of the MinHeap, H_a and H_b , where the deletion of the root node and heapify operations are performed after comparision. The algorithm is also rotation invariant and yields better matching rate.

- The system proposed a novel indexing technique for fingerprint database. It is based on the distance feature from core to minutiae. It performs consistently on different kind of image quality. It requires less space as it deals only with a numerical value and also considers error tolerance ‘k’ as the fingerprint has elastic properties. The proposed indexing algorithm has gone through with scaling test, rotation test and noise test. The high hit rate achieved at a low penetration rate indicates that the proposed distance feature indexing technique is satisfactory.

1.4 Thesis Outline

The thesis has been organized in the following order:

Chapter 2: Literature review

Chapter 3: Overview of Fingerprint

This chapter presents an overview on the history of fingerprint, It also discusses about the different fingerprint pattern and different levels of fingerprint features, requirement of the automatic system over the manual identification system.

Chapter 4: Fingerprint Recognition System

This chapter presents the previous methods and the proposed fingerprint recognition system which is discussed about preprocessing and post processing stage, development of distance feature, heap based fingerprint matching and fingerprint database indexing using distance feature.

Chapter 5: A preprocessing stage and post-processing stage

This chapter presents the proposed fingerprint enhancement algorithm for preprocessing stage. It also shows the different stages of preprocessing and post processing.

Chapter 6: Fingerprint Matching based on hFPM

This chapter presents the proposed Heap based Fingerprint matching (hFPM). It shows how to construct distance features using core point and minutiae.

Chapter 7: Indexing of Fingerprint Database

This chapter presents about fingerprint database and the proposed fingerprint indexing technique using distance features. It also discusses about how distance features are stored in a database.

Chapter 8: Experimental results and discussions

This chapter discusses about standard fingerprint database and also presents the experimental results of preprocessing and post processing stages, fingerprint matching algorithm and database indexing.

Chapter 9: Conclusions and future works

Finally, this chapter presents the conclusion. Summary of the work and contributions are outlined along with a discussion on the scope of future research work.