Biometric Security Technique: A Review

N. K. Sandhu and R. Kaur

Department of Computer Science, Lovely Professional University, Phagwara – 144411, Punjab, India;
rupinder.88@outlook.com, navneet_150@yahoo.co.in

Abstract
The objective of this paper is to present different techniques of the fingerprint recognition. Two significant techniques Minutia based technique and the correlation based technique are reviewed. Both have their own significance. Minutia is working on specific part of the finger image called ridge and bifurcation. Correlation works on the gray level image data that extract from the finger image. Minutia based technique used different algorithm to extract the features and to check the accuracy and reduce the error rate. Ransac (random sample census) algorithm is tries to work on some random transformation and find the good one. Algorithm for local correlation based on the Markov random field modal which is used to smooth the orientation field. The main finding is to get the better authentication system with a better strength.

Keywords: Biometric, Fingerprint, Image, Minutia, Ridge

1. Introduction
The word “biometric” is derived from the two Greek words ‘bios’ and ‘metrikos’ where bios represents ‘life’ and metrikos represents ‘measure’. Biometrics system identifies the individuals based on the corresponding features thereby providing the authentication when ever needed with better security mechanisms. In addition to this it is used to distinguish the people in a large gathering who are under observation. The biometric techniques are used to measure and analyze the personal characteristics. These characteristics includes both physiological and behavioral.

a. Physiological
   i. Face
   ii. Fingerprint
   iii. Hand
   iv. Iris

b. Behavioral
   i. Keystroke
   ii. Signature
   iii. Voice

A fingerprint comprises of pattern of ridges and valleys upon the surface of finger of a person. A ridge can be defined as a single curved segment, whereas the region between two adjacent ridges forms a valley.

Validation of a person which is based upon biometric check is turning out to be progressively well known in different applications like managing an account, aeronautics, monetary exchanges and so on. There are two functions used by a biometric system, one is identification and the other is verification. Verification system relies on comparing the presented biometric with a biometric reference that is already stored in the system which generates result much faster and accurate than the conventional identifi-
Figure 1. Process involved in fingerprint recognition.

Figure 2. Verification process.
cation systems, even with the increase in the size of the database.

Biometric provides better security in every field. There are many biometric techniques (palm, fingerprint, iris, ear, speech etc.) provides more accuracy and more security. Research is still going on in the area of fingerprint identification biometric technique and in the past, different types of work have been done.

The authors D. Binu and P. Malathi proposed a Multi Model based Biometric Image Retrieval for Enhancing Security. In this work they introduced the multimodal biometric authentication which recognize the human being with the consideration of four models fingerprint, face, palm, iris and improves the accuracy.

The authors Manvjeet Kaur, Mukvinder Singh and Parvinder S. Sindhu presented a Fingerprint Verification System using Minutiae Extraction Technique. This system introduced combined methods to build a minutia extractor and a minutia matcher using two techniques, one is Histogram Equalization and FFT for fingerprint image enhancement and the other is Crossing Number Perception for Minutiae Extraction. For improving thinning process, removal of false minutiae, and for marking of minutia, they used Segmentation with Morphological operations.

The authors Karthik Nandakumar and Anil K. Jain proposed Local Correlation based on Fingerprint Matching. This paper describes a correlation-based fingerprint matching which utilizes correlation of regions locally around the minutiae to identify the degree of matching between more than one fingerprint images.

2. Advantages of Biometrics

2.1 Security

One of the major advantages of this framework is that they cannot be presumed or stolen. The issues regarding effective watchword frameworks are such that frequently there exists grouping of letters, numbers, images, which makes it hard to recollect every time. The problem with these tokens is they could be effortlessly stolen or missed where both of these expected strategies include the risk of data being shared. However that would not be the situation with the biometric attributes, and does not
need (it is not required) to handle the risk of sharing, replication, and misrepresentation.

2.2 Accurate Identification Process
The traditional security frameworks are based on passwords, radiant cards, it can accomplish an irregular state of precision with biometrics frameworks. On the off chance when we have effectively set up the framework, we can make use of natural attributes such as filters for fingerprints and iris, which offers one of a kind and accurate strategies of recognizable proof. These elements cannot be easily and effortlessly copied that provides safety and security by just approving an authorized individual to get access.

2.3 Ease of use and Safety
The privileged thing about the utilization of biometrics for identification is advanced frameworks are assembled and developed to be simple and more over to safe to use. The innovation in biometrics yields accurate results with negligible obtrusiveness as a straightforward output or a photo that is generally required. In addition the product as well as the equipment can be utilized effortlessly and anybody can implement with no requirement of advance preparation.

3. Errors in Biometric System
There are two basic types of errors:

3.1 False Match (FM)
A false match error in biometric system is the one which wrongly declares a correct match among the input pattern and the existing stored template pattern.

3.2 False non Match (FNM)
It describes the situation where the biometric system wrongly declares as a failure between input pattern and stored template pattern. A false rejection error occurs when a matching pair of biometric data is wrongly rejected by the system.

4. Techniques for Fingerprint Recognition
Fingerprint recognition technique is the most commonly used and established biometric method and is the simplest to use for a higher security level. Even it is easy to install and it consumes less time and effort in acquiring one's fingerprint. It is a very secure technique in each and every field where security of data is demanded.

4.1 Minutiae Based Technique
The process of scanning minutiae needs to work on gathering specific points in a finger image. Additionally there are two major specifications, ridges and bifurcation. Minutia mean little points of interest, and this to the conduct of the edges discontinuities, for example,
Table 1. Principle categories of minutia are

| Name                          | Represents                                                                 |
|-------------------------------|---------------------------------------------------------------------------|
| Ridge ending                  | end of a ridge                                                             |
| Ridge bifurcation             | single ridge that divides into two ridges                                  |
| Short or independent ridge    | a ridge that begins, travels a small distance and then it ends             |
| Island                        | a single small ridge within a short ridge or a ridge ending which is not connected to the remaining ridges |
| Ridge enclosure               | A ridge that bifurcates and then reunites later to continue as one ridge   |
| Spur                          | Denotes a bifurcation that has a short ridge branching off a bigger ridge  |
| Crossover or bridge           | A short ridge which runs among parallel ridges                             |
| Delta                         | It is a Y-shaped ridge meeting                                             |
| Core                          | It is a U-shaped ridge pattern                                           |

Figure 5. Different points in figure image.
end, bifurcation and trifurcation or different elements, for example, pores (little openings inside the edges), lake (two shut bifurcations), spot (short edges), and so forth. Most frameworks use just the end and bifurcations. With the goal of coordinating the fingerprints we have to extricate the unique finger impression elements, for example, details and peculiarity focuses.

4.2 Correlation-Based Technique

To deal with some of the issues of minutiae-based

![Local correlation based algorithm.](image)

**Table 2.** Comparison of finger identification techniques

| Technique Parameters | Minutiae | Correlation |
|----------------------|----------|-------------|
| Works on | Length, height and density of fingerprint | Gray-level image |
| Preprocessing | More | Less |
| Image quality | Capable of dealing with good image quality only | Capable of dealing with bad image quality also |
| Computation complexity | Less | High |
| Performance | Good | Better |
methodology, one should have to choose an alternative methodology. Correlation-based approach makes use of the gray-level data that is extracted from the fingerprint image. This is a promising approach to fingerprint matching where the new generations of fingerprint sensors are being used. The main limitation of this method is its high complexity of computation as well as low tolerance to nonlinear distortion and contrast variation. Hence there should have been another alternative proposals which are able to compute the correlation locally rather than computing it globally, in which only the regions of interest (for example, minutiae and regions of singularity) are to be selected and matched. Such kind of algorithms use simple approaches for alignment of two images of fingerprints and subtract the input image from the template image to check whether the ridges corresponds.

5. Conclusion

In this paper, two fingerprint techniques are compared based on various parameters. Both the techniques have their advantages and disadvantages. Minutiae technique produces best result on good quality images and correlation method produces best result with the richer gray level data of fingerprint identification. This technique is capable of dealing with bad quality images as well as high resolution images. Both have their own significance.

6. References

1. Bazén M, Verwaaijen GTB, Gerez SH, Veelenturf LPJ, Van Der Zwaag BJ. A Correlation-Based Fingerprint Verification System. 11th Annual Workshop on Circuits Systems and Signal Processing, Netherland. 2000 November. p. 1–8.
2. Binu D, Malathi P. Multi Model based Biometric Image Retrieval for Enhancing Security. Indian Journal of Science and Technology. 2015; 8(35):1–10.
3. Gaur S, Shah VA, Thakker M. Biometric Recognition Techniques: A Review. Journal of the International Association of Advanced Technology and Science. 2012 Nov; 15.
4. He Y, Tian J, Luo X, Zhang T. Image enhancement and minutiae matching in fingerprint verification. Pattern Recognition Letters. 2003; 24(9,10):1349–60.
5. Jain AK, Ross A, Prabhakar S. An Introduction to Biometric Recognition. IEEE Transactions on Circuits and Systems for Video Technology. 2004; 14(1):4–20.
6. Lakkoju PK, Shankar TN. Detection of Fingerprints in Advanced Biometric System Design. Indian Journal of Science and Technology. 2016 9(May).
7. Nandakumar K. Local Correlation-based Fingerprint Matching. 2004 December.
8. Noor, A New Algorithm for Minutiae Extraction and Matching in Fingerprint School of Engineering and Design. 2012; July.
9. Orság F, Drahanský M. Biometric Security Systems: Fingerprint and Speech Technology Design of Biometric Security System [PhD thesis].
10. Parra P. Fingerprint minutiae extraction and matching for identification procedure.
11. Pawar S, A Survey of Minutiae Extraction from Various Fingerprint Images. 2016; 6(6):169–73.
12. Thai LH, Tam HN. Fingerprint recognition using standardized fingerprint model. 2010; 7(3).
13. Finger comparison guide.