

Perspective of Fingerprint Recognition Using Robust Local Feature

Pratibha H. Saini¹, Prof. Rakesh Suryawanshi²

¹PG Scholar, Dept of MCA, A.C Patil College of Engineering, Navi Mumbai, India

²H.O.D, Dept of MCA, A.C Patil College of Engineering, Navi Mumbai, India

Abstract: *There exist many human recognition techniques which are based on fingerprints. Most of these techniques use minutiae points for fingerprint representation and matching. However, these techniques are not rotation invariant and fail when enrolled image of a person is matched with a rotated test image. Moreover, such techniques fail when partial fingerprint images are matched. This paper proposes a fingerprint recognition technique which uses local robust features for fingerprint representation and matching. The technique performs well in presence of rotation and able to carry out recognition in presence of partial fingerprints. Experiments are performed using a database of 200 images collected from 100 subjects, 2 images per subject. The technique has produced a recognition accuracy of 99.46% with an equal error rate of 0.54%.*

Keywords: Biometrics, Fingerprint Recognition, Rotation and Occlusion Invariance, Partial Fingerprints

1. Introduction

Traditional Security Methods are based on things like Passwords and PINs. However, there are problems with these methods. For example, passwords and PINs can be forgotten or stolen. Use of biometrics has helped in handling these issues. Biometrics deals with the recognition of a person using his or her biometric characteristics. There are two types of biometric characteristics a person possesses. One is physiological characteristics where as another is behavioral characteristics. Physiological characteristics are unique characteristics physically present in human body. Examples of physiological biometric characteristics include face, fingerprint, iris, ear etc. Behavioral characteristics are related to behavior of a person. Examples of behavioral biometrics include signature, voice, gait (walking pattern) etc. The advantage of biometrics is that biometric identity is always carried by a person. So there is no chance of losing or forgetting it. Also, it is difficult to forge or steal biometric identity. Fingerprint is one of the popular biometric trait used for recognizing a person. Properties which make fingerprint popular are its wide acceptability in public and ease in collecting the fingerprint data. Many researchers have attempted to use fingerprints for human recognition for a long time. Most of them make use of minutiae based approach for representation and matching of fingerprints. Fingerprint matching based on minutiae features is a well-studied problem. This technique often makes assumption that the two fingerprints to be matched are of approximately same size. However, this assumption is not valid in general. For example, matching of partial fingerprints will not bind by this assumption. Even two fingerprints captured using two different scanners may have different size. Matching of two latent fingerprints may face the same problem. Moreover, two images with different orientation may fail to match in minutiae based techniques due to relative change in their minutiae locations.

2. What is a Fingerprint?

A fingerprint is the feature pattern of one finger (Figure 1). It is believed with strong evidences that each fingerprint is unique. Each person has his own fingerprints with the permanent uniqueness. So fingerprints have being used for identification and forensic investigation for a long time.



Figure 1: A fingerprint image acquired by an Optical Sensor

A fingerprint is comprised of ridges and valleys. The ridges are the dark area of the fingerprint and the valleys are the white area that exists between the ridges. Many classifications are given to patterns that can arise in the ridges and some examples are given in the figure 2 to the right. These points are also known as the minutiae of the fingerprint. The most commonly used minutiae in current fingerprint recognition technologies are ridge endings and bifurcations because they can be easily detected by only looking at points that surround them.



Figure 2: Fingerprints showing minutiae

3. Stages Fingerprint Recognition

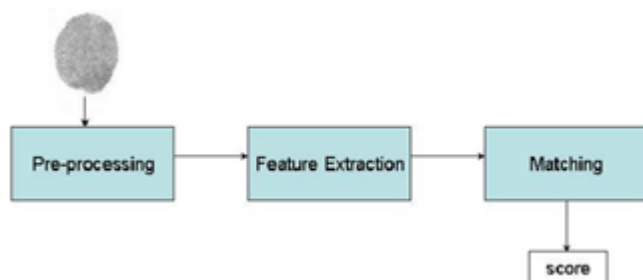


Figure 3: Main modules of a fingerprint verification system

The main modules of a fingerprint verification system (Figure 3) are: a) fingerprint sensing, in which the fingerprint of an individual is acquired by a fingerprint scanner to produce a raw digital representation; b) preprocessing, in which the input fingerprint is enhanced and adapted to simplify the task of feature extraction; c) feature extraction, in which the fingerprint is further processed to generate discriminative properties, also called feature vectors; and d) matching, in which the feature vector of the input fingerprint is compared against one or more existing templates. The templates of approved users of the biometric system, also called clients, are usually stored in a database. Clients can claim an identity and their fingerprints can be checked against stored fingerprints.

4. Fingerprint Matching Techniques

The large number of approaches to fingerprint matching can be coarsely classified into three families.

- Correlation-based matching: Two fingerprint images are superimposed and the correlation between corresponding pixels is computed for different alignments (e.g. various displacements and rotations).
- Minutiae-based matching: This is the most popular and widely used technique, being the basis of the fingerprint comparison made by fingerprint examiners. Minutiae are extracted from the two fingerprints and stored as sets of points in the two dimensional plane. Minutiae-based matching essentially consists of finding the alignment between the template and the input minutiae sets those results in the maximum number of minutiae pairings
- Pattern-based (or image-based) matching: Pattern based algorithms compare the basic fingerprint patterns (arch,

whorl, and loop) between a previously stored template and a candidate fingerprint. This requires that the images be aligned in the same orientation. To do this, the algorithm finds a central point in the fingerprint image and centers on that. In a pattern-based algorithm, the template contains the type, size, and orientation of patterns within the aligned fingerprint image. The candidate fingerprint image is graphically compared with the template to determine the degree to which they match.

5. Issues and Challenges with Existing Techniques

One of the open issues in fingerprint verification is the lack of robustness against image quality degradation. The performance of a fingerprint recognition system is heavily affected by fingerprint image quality. Several factors determine the quality of a fingerprint image: skin conditions (e.g., dryness, wetness, dirtiness, temporary or permanent cuts and bruises), sensor conditions (e.g., dirtiness, noise, size), user cooperation, etc. Some of these factors cannot be avoided and some of them vary along time. Poor quality images result in spurious and missed features, thus degrading the performance of the overall system.

Therefore, it is very important for a fingerprint recognition system to estimate the quality and validity of the captured fingerprint images. We can either reject the degraded images or adjust some of the steps of the recognition system based on the estimated quality. Several algorithms for automatic fingerprint image quality assessment have been proposed in literature. Also, the benefits of incorporating automatic quality measures in fingerprint verification have been shown in recent studies.

Most of the existing fingerprint techniques in literature are based on minutiae points which are represented using their co-ordinate locations in the image. When test fingerprint image is rotated with respect to enrolled image or partially available, these techniques face problem in matching due to change in the co-ordinate locations of the minutiae points and perform very poorly. These two cases are discussed below. A. Rotated Fingerprint Matching: An example of a rotated fingerprint image is shown in Figure 4(b). We can see that it is difficult to match minutiae of two images because due to rotation, coordinate locations of all the minutiae points in Figure 4(b) with respect to Figure 4(a) are changed. B. Partial Fingerprint Matching: An example of partial fingerprint is given in Figure 5(b). We can see that it is difficult to match minutiae of two images because due to missing part of the fingerprint, coordinate locations of all the minutiae points in Figure 5(b) with respect to Figure 5(a) are changed. Figure 4 (a) Normal Fingerprint Image, (b) Rotated Fingerprint Image Figure 5(a) Full Fingerprint (b) partial Fingerprint Image Concisely, matching of rotated or partial fingerprints to full enrolled images present in the database face several challenges: (a) If test image is rotated, the co-ordinate locations of minutiae points may change even with slight rotation, (b) the number of minutiae points available in partial fingerprints are relatively less, leading to less

discrimination power (c) co-ordinate locations of minutiae points are also bound to change due to change in reference point in case of partial fingerprints.



Figure 4: (a) Normal Fingerprint Image, (b) Rotated Fingerprint Image



Figure 5 (a) Full Fingerprint (b) partial Fingerprint Image

6. Proposed Technique

To overcome the issues faced by minutiae based techniques, we propose the use of local robust features for fingerprint representation and matching. Among various local features such as SIFT [1], SURF, GLOH etc. available in literature, SURF (Speeded up Robust Features) have been reported to be robust and distinctive in representing local image information. SURF is found to be rotation-invariant interest point detector and descriptor. It is robust with scale and illumination changes and occlusion. A. Key-Point detection SURF identifies important feature points commonly called key-points in the image. It uses hessian matrix for detecting key-points. For a given point in an image I , the hessian matrix is defined as: where, L_{xx} , L_{yy} , and L_{xy} are filter matrices defined as follows where gray pixels represent 0.

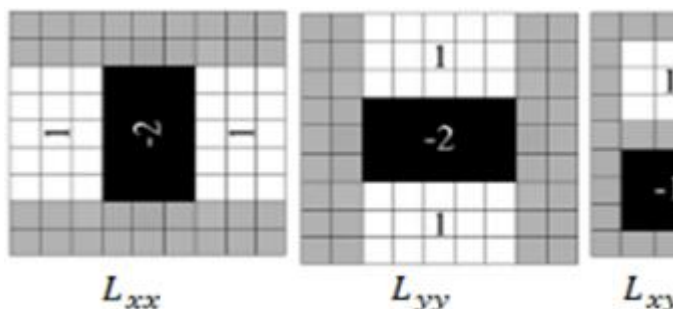


Figure 6: Flow chart of the proposed Technique

Key-points at different scales are detected by considering filters at various scales. In order to localize interest points in the image and over scales, maximum filter in a

neighborhood is implemented. B. Computation of Descriptor Vector In order to generate key point descriptor vector, a region around the key-point is considered and Haar wavelet filter responses in horizontal () and in vertical () directions are computed. These responses are used to obtain the dominant orientation in the circular region. Feature vectors are measured relative to the dominant orientation resulting the generated vectors invariant to image rotation. A square region around each key-point is considered and it is aligned along the direction of dominant orientation. The square region is further divided into sub-regions and Haar wavelet responses are computed for each sub-region. The sum of the wavelet responses (and) in horizontal and vertical directions and of their absolute values (and) for each sub-region is used as feature values. Thus, the feature vector for sub-region is given by SURF feature vector of a key-point is obtained by concatenating feature vectors () from all sixteen sub regions around the key-point resulting a vector of elements.

7. Steps Involved in Proposed Technique

There are three basic modules in the proposed technique. Various modules of the proposed technique are discussed below. Figure 6 shows the block diagram of the technique.

A. Image Acquisition: This module is used to read fingerprint images. We collect the data using SecuGen Fingerprint scanner and images are collected at 500 dpi. **B. Image Enhancement** In this module, image enhancement is carried out to remove the noise from fingerprint image. We use Gaussian smoothing filter for noise removal. We also used average and median filter for noise removal, however found the best result in case of Gaussian filter. **C. Feature Extraction** In the feature extraction module, features from the enhanced fingerprint image are extracted. We have used SURF for feature extraction. The reason behind using SURF is that it is robust against rotation. Also, since SURF represents image using local features, it also works well in presence of occlusion i.e. for partial fingerprint image. **D. Matching** In matching module, two fingerprint images are matched with the help of extracted local features. Depending upon the obtained matching score, two fingerprints are declared as matched or not-matched. **V. RESULTS** Experiments have been performed on a database of 200 images collected from 100 subjects, 2 images per subject. Few sample images from the database are shown in Figure 7.



Figure 7: Few samples of fingerprint images from the database

Figure 8 shows the score distribution for genuine and imposter matches. It is clear from the figure that these scores are quite distinguishable. This shows that the proposed technique would be efficiently able to differentiate between genuine and imposter matches. Performance of the proposed technique is presented in TABLE I. Threshold vs. FAR; FRR curves are shown in Figure 9 whereas Receiver Operating Characteristics (ROC) curve and accuracy curves are shown in Figures 10 and 11 respectively.

Table II: Performance of the Proposed Technique

Parameter	Result
Accuracy	99.46%
Equal Error Rate (EER)	0.54 %

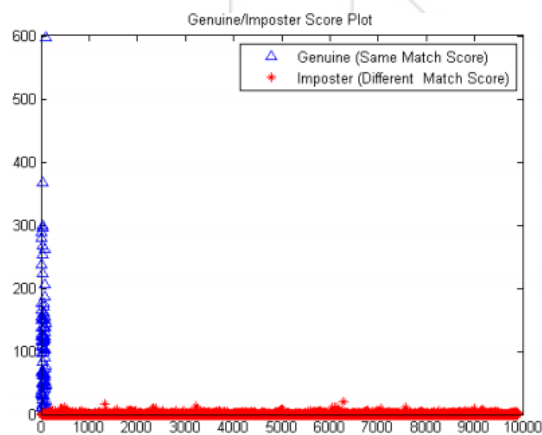


Figure 8: Genuine and Imposter Match Score Distribution (100 genuine score points against 9900 imposter score points)

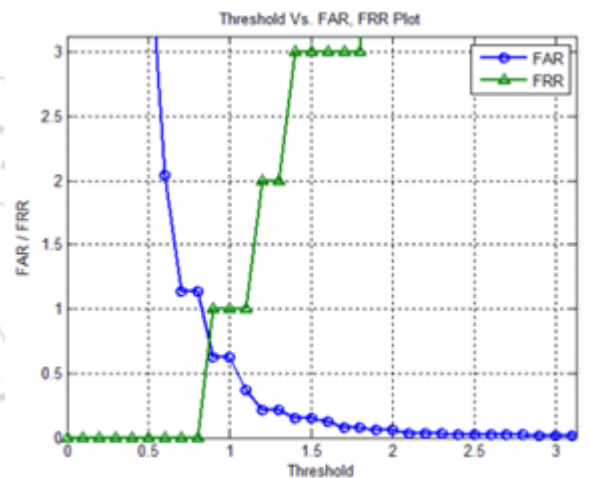
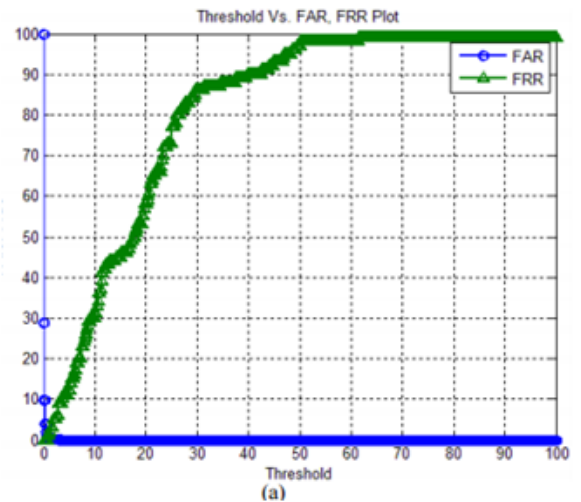


Figure 9 (a) Threshold vs. FAR, FRR plots, **(b)** Close View of Plots

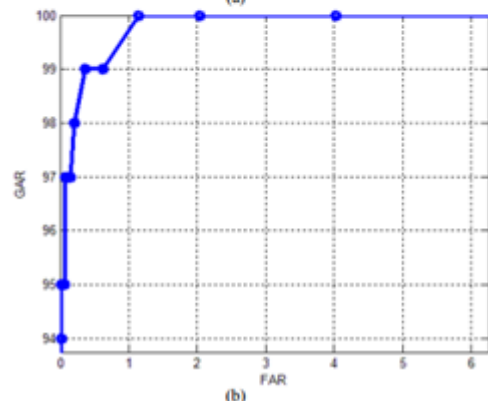
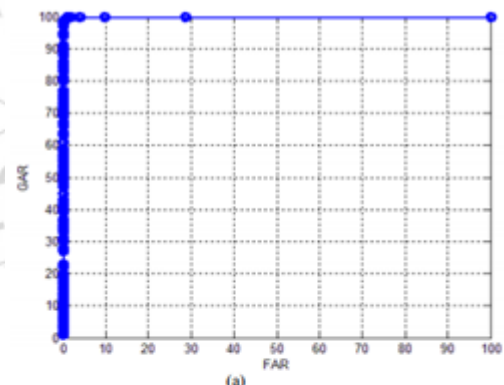


Figure 10 (a) ROC curve, **(b)** Close View of ROC Curve

A. Experiment to Show Rotation Invariance

All 200 images from the database are used in this experiment. 100 images are used for enrollment and 100 for testing. To test robustness against rotation, test images are rotated before matching. We have used rotation angles of 5°, 10°, 15° and 20° in the experiments. Rotated images for few angles for a subject are shown in Figure 9. Obtained experimental results are presented in Table II. From the table, we can observe that even after a rotation of 10°, recognition accuracy is more than 99%.

Table II: Performance of the Proposed Technique in presence of Rotation

Rotation Angle	Accuracy
0	99.46
5	99.22
10	99.13
15	98.15
20	94.85

B. Experiment to Show Robustness against Partial Fingerprints In this experiments also all 200 images from the database are used for experimentation. 100 images are used for enrollment while 100 for testing. To test robustness against occlusion (partial fingerprint), test images are partially presented during matching. Few examples of occluded (partial) fingerprint images are shown in Figure 10. We have experimented by considering partial fingerprint with 5%, 10%, 15%, 20%, 25%, 30% and 40% occlusion. Experimental findings are presented in Table III. From the table, we can observe that even by using fingerprint with 15% occlusion, recognition accuracy value is more than 90%. Also in presence of 30% occlusion, recognition accuracy is around 97%.



Figure 12: Examples of Rotated Fingerprint Images



Figure 13: Examples of Occluded (Partial) Fingerprint Images

Table III: Performance of the Proposed Technique for Partial Fingerprint Images

%age Occlusion	Accuracy
0	99.46
5	99.45
10	99.22
15	99.02
20	98.69
25	97.88
30	96.94

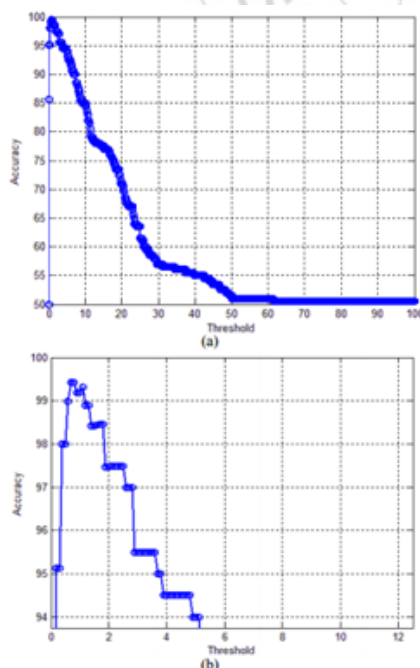


Figure 11 (a) Accuracy curve, **(b)** Close View of Accuracy Curve at Maximum Accuracy Point

8. Conclusions

This paper has proposed an efficient fingerprint recognition technique which is based on local robust features. It has used Speeded-up Robust Features (SURF) as local robust features as it has been found to be superior as compared to other local features in terms of accuracy and speed. The technique has performed well in presence of rotation and partial fingerprint images. Experimental validation has been performed on a database of 200 images collected from 100 subjects, 2 images per subject. The performance of the technique has been found to be very

encouraging. It has produced a recognition accuracy of 99.46% with an equal error rate of 0.54%.

References

- [1] A.K. Jain, A. Ross, S. Prabhakar, An introduction to biometric recognition, IEEE Transactions on Circuits and Systems for Video Technology, Special Issue on Image- and Video-Based Biometrics 14 (1), pp. 4–20, 2004.
- [2] Nalini Ratha and Ruud Bolle, Automatic Fingerprint Recognition Systems, Springer-verlag, 2003.
- [3] Davide Maltoni, Dario Maio, A. K. Jain and Salil Prabhakar, Handbook of Fingerprint Recognition, Second Edition, Springer, 2009.
- [4] Herbert Bay, Andreas Ess, Tinne Tuytelaars and Luc Van Gool, Speeded-Up Robust Features (SURF). Computer Vision and Image Understanding, 110(3), pp. 346-359, 2008.
- [5] Herbert Bay, Tinne Tuytelaars and Luc Van Gool, SURF: Speeded up robust features, In Proceedings of 9th European Conference on Computer Vision (ECCV'06), pp. 404-417, 2006.
- [6] David G. Lowe, Object recognition from local scale-invariant features, Proceedings of the International Conference on Computer Vision. 2. pp. 1150–1157, 1999

