# ACCURACY FINGERPRINT MATCHING FOR ALTERED FINGERPRINT USING DIVIDE AND CONQUER AND MINUTIAE MATCHING MECHANISM

A. Vinoth[1] and S. Saravanakumar[2]
[1]Department of Computer Science, Bharathiar University, Coimbatore, Tamilnadu, India
[2]Department of Computer Science Engineering, PR Engineering College Vallam, Thanjur, Tamilnadu, India
E-Mail: vino.asstprof@gmail.com

## ABSTRACT

Biometric traits never change in lifetime and probably reliable. There is various biometric traits lies in human body such as fingerprint, palm print, iris etc. Among them fingerprint traits are very common even it didn't matched for identical twins also. The verification of fingerprint is very smart in biometric but the real burden starts while creating unnatural finger (fake biometric) prints may be classified into fake or altered. The Biometrics devices should find out the acquiring fingerprint is natural or altered. But unlikethe issue of fingerprint alteration, the use of fake fingerprints has received lot of attention in the literature. In this paper the proposal will give solutions for altered fingerprint, which is the real finger print altered manually. The experimental sessions shows that the proposed method gave good results and works effectively than the existing methods.

**Keywords:** biometric traits, biometrics devices, fingerprint, minutiae matching mechanism.

## 1. INTRODUCTION

Now a day's finding out the identity is a vital role in all criteria such as banking insurance, passport etc. especially for security. Biometrics is the option to focus the identity. Biometric traits never change in lifetime and probably reliable. There is various biometric traits lies in human body such as fingerprint, palm print, iris etc. Among them fingerprint traits are very common even it didn't matched for identical twins also. The patterns of fingerprints are framed with ridges and valleys which flow parallel and create various shapes. The loop and delta portions in the fingerprint patterns are mainly used for fingerprint classification. The singular religions (macro-singularities) which were produced by ridge lines turn with peak curvature, known as loop and delta. The characterizations of ridges are derived from its frequency and orientation. The frequency and orientation are the global properties of the fingerprint pattern. The number of ridges which pass through a segment a defined length is known as frequency of ridges. The angle which was formed with horizontal axis of ridges known as orientation of ridges.

In natural finger print patterns the minutiae are nothing but small details which ridges lines were end. The ridges lines end in various ways and form different structures such as bifurcate, trifurcate or cross each other. Most of the time the ridges are broken, the usualis termination and bifurcation. During observation of the fine finger prints the observer can find other details such sweat pores, incipient ridges or creases (white lines).

The verification of fingerprint is very smart in biometric but the real burden starts while creating unnatural finger (fake biometric) prints may be classified into fake or altered. The fake finger prints made up of artificial materials like gelatin, silicone, latex and form a duplicate of the real fingerprint. The Other Category of Unnatural fingerprint is altered fingerprint, which is the real finger print altered manually. The manual changes or any uncertain able changes in real fingerprint made altered fingerprints. The ridge pattern's degradations may be classified into three categories such as obliteration, distortion and imitation. The distorted finger ridge patterns are made by plastic surgery which was turned from abrasion ridge patterns. Portions of the skin are removed from the finger and transplanted back on the same finger on different positions. The imitation of the finger ridge patterns are also made by plastic surgery but the real finger print transplanted into other biometric portions of the body such palm prints, toes and other finger's prints.

The real finger print pattern may be laid in any one of alteration such as obliteration, distortion and imitation but the reason behind this is the user want to mask their identity. Sometimes it may cause accidentally also. The Biometrics devices should find out the acquiring finger print is natural or altered. But unlikethe issue of fingerprint alteration, the use of fake fingerprints has received lot of attention in the literature.

## 2. LITERATURE SURVEY

An individual's fingerprint is unique and remains not changed during their lifetime. An impression of the pattern in the fingers represents an individual's fingerprint. The region between two adjacent ridges is defined as valley, and a single curved segment is defined as a ridge. The features that were used for identification are the local discontinuities in the ridge flow pattern are called minutiae. While performing minutiae extraction, details of the type, orientation, and location of the minutiae are considered into account.

According to Jain, A.K., and JianjiangFeng[1], during forensics observation the collected palm prints are of poor quality and covered only a few portions of palms with congested background. There is large number of minutiae founded in palms that too created another big issue. The author derived an algorithm to find the direction of ridges and its frequency in palm prints. It helps out to match minutiae even in poor quality. The author used minutiae descriptor and minutiae code to find out the data surrounds the minutiae. They used alignment based matching algorithm to watch the palm prints. The proposed system test with 10,200 full palm prints. (150 lives can partial palm prints and 1oo latents). The author achieved 78.7% and 69% respectively from rank 1 recognition rates for live palm prints. Although the proposal gave solution for poor quality palm prints, they are not proposed any solution for altered finger or palm prints.

Paulino, A.A., JianjiangFeng, and Jain, A.K.[2] proposes an algorithm to align fingerprints and measures similarity between fingerprints that uses a robust alignment algorithm. The orientation field is reconstructed from minutiae to be consistent with the latent matching in common practice manner. To be used in law enforcement applications, the proposed algorithm relies on manually marked minutiae. For improving matching accuracy, commercial fingerprint matchers and proposed algorithm are fused. When there is low number of matched area that is few number of similar patterns, two approaches fail.

Considering a very challenging pattern recognition issues, wide range of applications were used by fingerprint recognition which were discussed by Adina Petrovici and CorneliuLazăr [3]. By using fake fingerprints or altering their own fingerprints, individual trying to fool or evade the identification system because fingerprint system having security problems. A reduced set of key points are extracted at various scales are located on singular points and altered regions in an excessive number. On fingerprints images by applying SIFTS for altered fingerprints, new method is proposed. Altered can be identified but cannot be matched.

Criminals use to evade identification because new algorithm which detect changes to fingerprints due to mutilation and other similar measure are proposed by Jain, A.K., Soweon Yoon[4]. Web extra video features produced by Karl Ricanek, University of North Carolina Wilmington providing an overview of the 2011 International Joint Conference on Biometrics, and Charles Severance, Computer's multimedia editor, interviewing several conference attendees around the world.

In an image's pixel value histogram, the pixel value mappings leave behind statistical traces are showed by Stamm, M.C., and Liu, K.J.R [5]and referred as mapping's intrinsic fingerprint. For detecting general forms globally and locally applied contrast enhancement, we propose forensic method as well as for detecting features of each operation's intrinsic fingerprint, a method of detecting histogram equalization use by searching a method is proposed. A JPEG compressed image, a method is proposed to detect the global addition of noise that the intrinsic fingerprint of the specific mapping will be altered, if applied to image's pixel value after addition of noise. P. Velayutham and Dr.V.Vijayalakshmi[6] discusses in chronological order with some encounter fingerprint altered cases: by different law and enforcement and border security agencies, altered fingerprints analysis were used by available NIST SD 4 Database and types of alteration were recorded. This system can find whether the fingerprint is altered or not but cannot match altered fingerprints.

In Early approach, divide and conquer technique are used by Pal, Sanjukta; pal, Sucharita; and Paul, Pranam [7]. The whole image is fragmented into four segment and those segments DB image where checked one by one individually, four segments were chosen from previous different four segments. The neighboring pixel matching proceed further because of the matched value is greater than threshold value, If result is threshold value then fingerprint images match. The DB image were checked which would be traversed into four segments, better probability to get result above threshold value, only if one or two doesn't fulfill the criteria then remaining segment can.

Hoda A. Darwish, IhabTalkhan[9]present the idea of utilizing a spatial "geographical" Divide and Conquer technique in conjunction with heuristic TSP algorithms specifically the Nearest Neighbor 2-opt algorithm. The proposed algorithm has lower complexity than algorithms published in the literature which comes around 9% at a lower accuracy expense. The present approach welcomes the community for large problems when a reasonable solution reached in a fraction of the time.

## 3. PROBLEM STATEMENT

In today's world fingerprint alteration caused by accidents or malpractice leads to create unusual problems in automatic fingerprint verification. In past years many algorithm and methods were proposed to increase the accuracy of fingerprint analysis but these methods only works on minor cracks, cuts and minimum burned area. Some of the existing system can find whether the given fingerprint is altered or not but they cannot find the identity of that fingerprint which will be major problem in fingerprint identification system.

In previous approaches, various methods were implemented to find out whether the fingerprint is altered or not. But those approaches got major drawbacks. If there is any cut mark or injuries then the device will result it as fake fingerprint and not as altered one. Even its real fingerprint and got spoiled with known hazards they are not addressed here. Moreover if any scar or major damages on the real fingerprint didn't match with fingerprint's database. So it's very hard to find out whether this was done by purpose or not?

## 4. PROPOSED METHODOLOGY

The over view architecture of proposed system is shown in Figure-x. In which the fingerprint image segmented initially to separate the foreground and background images because the fingerprint information lies only at foreground regions. The resultant image get smoothed and sharpened by using Gabor, Gaussian and statistical calculations. Due to this segmentation and noise reduction (image enhancement - smoothening andsharpening) the image is get ready for minutiae extraction. The minutiae extraction algorithm process extracted the features that are minutiae's of fingerprint. The false minutiae's such bifurcation, spur, loop, bridge are removed by using previous mentioned algorithm in literature. The resultant images will stored in database during acquisition process or get ready for authenticate matching while checking the same with database image. The matching takes place using minutiae matching algorithm which will be explained in below section. The result percentage analyzed and if it is less than 80% the divide and conquer method applied for the unmatched fingerprint. The non-matching position will finds out. Due to this the non-matching position will predicted and its percentage was matched with non-matching fingerprint's missing percentage. If it's matched then it denoted as altered fingerprint.

## 5. SEGMENTATION

Segmentation is the process which divides the image into required regions and non-required regions. Here in fingerprint the author separate it into two regions foreground and background. The ridges and valleys are present in the foreground regions of fingerprint. The background region contains border area which does not contain any valid fingerprint information. As per the proposal's calculation we won't need any unusual portion to verify the fingerprint. So we segment it into foreground and background. Even though we applied our minutiae algorithm to these background regions which will give results as noisy and false minutiae.

The foreground regions have very high variance value whereas the background regions exhibit very low grey-scale variance value in fingerprint image. To perform segmentation, variance threshold method is used. First of all, the image is divided into blocks and grey-scale value calculated for each block in the image. If variance is less than global thresholds then block are assigned to background image otherwise it is assigned to part of foreground. The grey-level variance for a block of size W x W is defined as:

$$V(k) = \frac{1}{w^2}\sum_{i=0}^{w-1}\sum_{j=0}^{w-1}(I(i,j)-M(k))^2,$$

Where V (k) is the variance for block k, I (i, j) is the grey-level value at pixel (i, j), and M (k) is the mean grey-level value for the block k.

## 6. IMAGE ENHANCEMENT

The first step in the development of an algorithm for fingerprint image segmentation is the selection of useful *pixel* or *block features*. Note that the term 'feature' is used here to refer to properties of individual pixels whereas it was used earlier to refer to properties of the entire (foreground) image. In the rest of this chapter, the correct meaning of 'feature' should become clear from the context. For each pixel or block in the fingerprint image, the pixel features are extracted, and each block is classified according to the extracted feature values. From many alternatives, we have selected four features that contain useful information for segmentation. These features are the coherence, the local mean, the local variance or standard deviation, and the Gabor response of the fingerprint image. Instead of using pure block-wise processing, the smoothing window that is used for noise reduction and the block size are decoupled. For noise reduction, the features are averaged by a Gaussian window *W* with *σ* = 6, providing a combination of both localized and smoothly changing features.

1. The coherence gives a measure how well the gradients are pointing in the same direction. Since a fingerprint mainly consists of parallel line structures, the coherence will be considerably higher in the foreground than in the background. In a window *W* around a pixel, the coherence is defined as:

$$Coh = \frac{\left|\sum_W (G_{s,x}, G_{s,y})\right|}{\sum_W \left|(G_{s,x}, G_{s,y})\right|} = \frac{\sqrt{(G_{xx}-G_{yy})^2+4G_{xy}^2}}{G_{xx}+G_{yy}} \qquad (4.1)$$

where $(G_{s,x}, G_{s,y})$ is the squared gradient, $G_{xx} = \sum_W G_x^2$, $G_{yy} = \sum_W G_y^2$, $G_{xy} = \sum_W G_x G_y$ and $(G_x, G_y)$ is the local gradient.

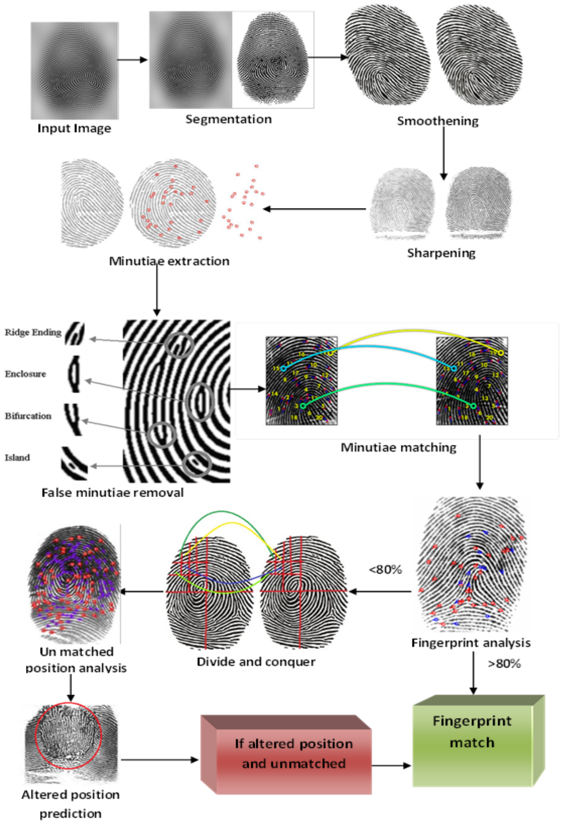


**Figure x overview of proposed system**

a) The average gray value is the second pixel feature that is useful for the segmentation of fingerprint images. Most sensor uses white color for ridge-valley structure and black for background, where the finger does not touch the sensor, is rather white. This means that the mean gray value in the foreground is in general lower, i.e. darker gray, than it is in the background. Using *I*as the intensity of the image, the local mean for each pixel is given by:

$$Mean = \sum_W I \qquad (4.2)$$

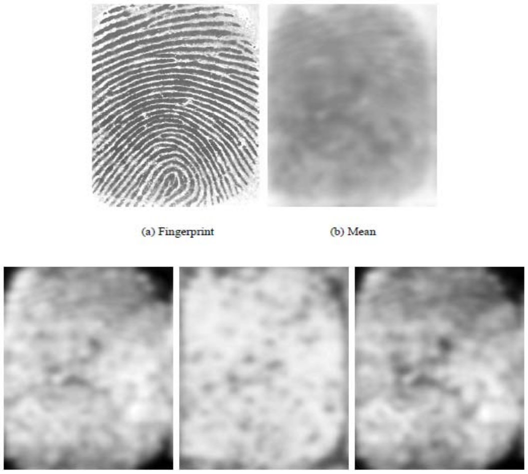
b) The variance or standard deviation is the third pixel feature that can be used. In general, the variance of the ridge-valley structures in the foreground is higher than the variance of the noise in the background. The variance is for each pixel given by:

$$Var = \sum_W (I - Mean)^2 \qquad (4.3)$$

and the standard deviation by

$$Std = \sqrt{Var} \qquad (4.4)$$

c) The Gabor response is the smoothed sum of the absolute values of the fingerprint images that have been filtered by the complex Gabor filter. It can be interpreted as the local standard deviation of the fingerprint image after enhancement. Therefore, the Gabor response is expected to be higher in the foregroundregion.



(a) Fingerprint (b) Mean

(c) Standard deviation (d) Coherence (e) Gabor response

1st, Read 5 or 6 fingerprint images from different angle.

1a: Images from database are converted into grayscale images

1b: These gray scale images are then converted into binary images

Finally, fingerprints are matched one by one.

Then for matching purpose,

**Minutiae extraction**

- **Input:**

  Binary image as a 256*256 array from the previous module

- **Output:**

  Set of minutiae points with (x, y) and their relative displacement

Minutiae Extraction (Image Segment)

**Step1:**Consider the inner 236*236 array

**Step 2:**Scrutinize the image from its upper portion to bottom portion, left portion to right portion by following only ridges.

**Step 3:**Find out the 0 -1 transition, the ridge's width is calculated by noting the 1- 0 transition

**Step 4:**The analysis move to next row and follow the same ridges.

**Step 5:**If the P >= Q then Call bifurcation () to check if there is any minutiae point since there may be bifurcation from top to bottom.

Where P –> current Row width, Q –> previous row width

Else

If the P =< Q then Call bifurcation () to check if it is a minutiae point since there is bottom to top ridge bifurcation

**Step 6:**

Continue with the next row and repeat these for all the ridges in the given image or until 90 minutiae points have been obtained.

**Minutiae matching**

**Minutiaematching (SEGminupoints)**

**Step 1** Pick a minutia in one of templates.

**Step** [[[[[2Compare SEGminupoints formed by its neighborhood against all possible neighborhoods in the second template. (Distance between minutiae and their orientations)

**Step 3** Use a distance measure to calculate similarity.

**Step 4** if matching ratio is more than 80%

Fingerprint match

Else

Fingerprint not match

Call divide_and_conquire();

Step 4 Return match score.

**Divide and conquer**

**divide_and_conquire()**

**Step 1:** Calculate the number of pixels along width and in length (say m and n) from Final Image.

**Step 2:** Using m, n derive the centre position (p, q) of Final Image by (m+1/2, n/2) or by (m/2, n+1/2) or by (m+1/2, n+1/2) or by (m/2, n/2).

**Step 3:** Using (p, q) as centre position break the image into four segments.

**Step 4:** Take the south east corner image segment (say A) of Final Image.

**Step 5:** If the number of pixel along width and length of the image segment A is greater than 10 then go to step1 and repeat step2 and step3.

**Step 6:** Take the North West corner image segment (say A1) of the previous image segment A.

**Step 6a:** If the number of pixel along width and length of previously selected image segment A1 is greater than 10 then go to step5.

**Step 6b:** If the number of pixel along width and length of previously selected image segment A1 is less or equal to 10 then go to step7.

**Step 7:** Take the North East corner image until every segment is reached doMinutiaeextraction (Image Segment)

**Step 8:** Take the North East corner of Minutiaepoints of segment doMinutiaematching (SEGminupoints)

**Step 9:** StoreMatched and unmatched percentage of each area

**Step 10:** If there is image still in db choose next image and go to step 1 Else take the highest percentage of matching image and go to step-11

**Step-11** Find the unmatched area and altered finger area

If position (unmatchedarea) = Position (Altered finger area)

Then fingerprint match

Else fingerprint not match

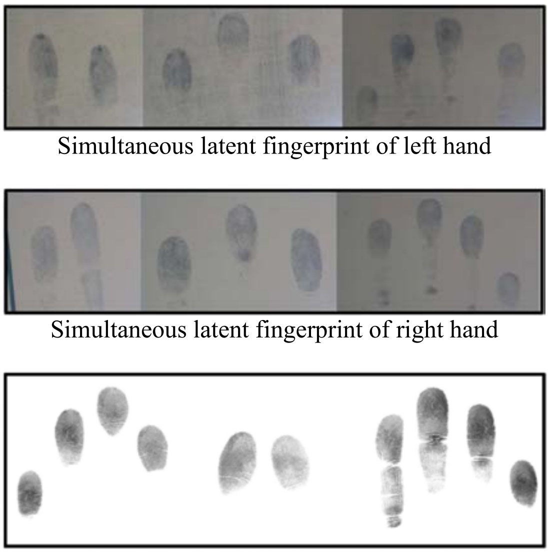
**Dataset description**

The fingerprint database s taken from IIIT-D Simultaneous Latent Fingerprint Database which is found in the website "https://research.iiitd.edu.in/groups/iab/fpdatabases.html" Lack of availability of simultaneous latent fingerprint database for research is one of the main reasons for limited research in this domain. To motivate research in this area and to encourage researchers to publish results on a common database, we have prepared IIITD SLF database1, which is the largest and only publicly available database up till now.

**Table-1.**

| | |
|---|---|
| Number of subjects | 30 |
| Number of classes | 60 (2 hands persubject) |
| Number of simultaneous latent samples per class | 6 |
| Total Number of simultaneous Impressions | 360 |
| Total number of latent fingerprints | 1080 |
| Number of optical slap impressions (4 + 4 + 2 prints) | 60 |

A sample fingerprint of the database is provided in Figure-y. Multiple samples of various finger combinations are collected from30 subjects in a semi-controlled environment with a ceramic tile as the background, i.e. Fingerprints are deposited on a ceramic tile. The database gathering process confirms that both latent fingerprint deposition and lifting is done simultaneously. Hence, similarity is established as a ground truth in this database. Further, two sets of mated optical slap fingerprints (4 + 4 + 2 fingers) are captured using Crossmatch L-Scan Patrol at 500 dpi for all 30 subjects. The database provides scope of research in both matching simultaneous latent fingerprints and establishing simultaneity automatically. Detailed statistics of the IIITD SLF database are given in Table-1.



Simultaneous latent fingerprint of left hand

Simultaneous latent fingerprint of right hand

Fingerprint captured using crossmatch

**Figure.**Sample fingerprint of one subject in the databaseFigure-y.

## 7. CONCLUSIONS

This system uses minutiae matching algorithm to compare the finger print and divide and conquer method to find matched and unmatched areas (Altered area). By combining both processes it can able to find the altered fingerprint as well as to verify the identity of the altered fingerprint which works effectively. To increase the accuracy various steps like segmentation smoothening (Fingerprint enhancement) and sharpening process takes place these process removes unwanted noise as well as other data which increases quality and performance.

## REFERENCES

[1] Jain, A.K.,andJianjiangFeng. 2009. Latent Palmprint Matching.Pattern Analysis and Machine Intelligence, IEEE Transactions on.31(6): 1032-1047, DOI:10.1109/TPAMI.2008.242.

[2] Paulino A.A., JianjiangFeng and Jain A.K.2013. Latent Fingerprint Matching Using Descriptor-Based Hough Transform.Information Forensics and Security, IEEE Transactions on.8(1): 31-45, DOI:10.1109/TIFS.2012.2223678.

[3] Adina petroviciand corneliulazăr. 2012. Altered fingerprints analysis based on siftkeypoints"echnicaluniversity "gheorgheasachi" of iasitome lviii (lxii) fascia. 3, 2012 section automation and computers.

[4] Jain, A.K., Soweon Yoon. 2012. Automatic Detection of Altered Fingerprints. Published in:Computer (Volume: 45, Issue: 1) Biometrics Compendium, IEEE, pp. 79 - 82, DOI: 10.1109/MC.2012.6.

[5] Stamm M.C. and Liu K.J.R. 2010. Forensic detection of image manipulation using statistical intrinsic fingerprints. Information Forensics and Security, IEEE Transactions on.(5(3): 492-506, DOI: 10.1109/TIFS.2010.2053202.

[6] P. Velayutham and Dr.V.Vijayalakshmi. 2012. Automatic Detection of Altered Fingerprints.International Journal of Advanced Research in Electronics and Communication Engineering (IJARECE). 1(5).

[7] Pal, Sanjukta; pal, Sucharita; and Paul, Pranam. 2013. Matching of Fingerprint Geometry by Advanced Divide and Conquer Technique. International Journal of Advanced Research in Computer Science. 4(2): 337.

[8] Pal, Sanjukta; pal, Sucharita and Paul, Pranam. 2013. Fingerprint Geometry matching by Divide and Conquer Strategy. International Journal of Advanced Research in Computer Science. 4(2): 179.

[9] Hoda A. Darwish, IhabTalkhan. 2014.Reduced Complexity Divide and Conquer Algorithm for Large Scale TSPs. Article Published in International Journal of Advanced Computer Science and Applications (IJACSA), 5(1). DOI:10.14569/IJACSA.2014.050110.