IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661, p- ISSN: 2278-8727Volume 13, Issue 5 (Jul. - Aug. 2013), PP 48-55
www.iosrjournals.org

A Challenge to Analyze and Detect Altered Human Fingerprints

Chandrakanth Biradar[1], Vijeth Rao[2]
[1] *Professor, Department of Computer Science and Engineering, Poojya Doddappa Appa College of Engineering, Gulbaraga, Karnataka, India,*
[2] *Department of Computer Science and Engineering, Poojya Doddappa Appa College* of *Engineering, Gulbaraga, Karnataka, India*,

Abstract: *The deployment of Automated Fingerprint Identification Systems (AFIS) in law enforcement and border control applications has escalated the need for ensuring that these systems are not compromised. Several problems related to fingerprint system security have been investigated carefully;, the problem of fingerprint alteration has received very scarce attention [1]. Fingerprint alteration refers to the deliberate alteration of the fingerprint pattern by a person for masking his/her identity. Several cases of fingerprint alteration have been reported previously. The main contributions of this paper is: 1) Analysis of the altered fingerprints 2) classifying the alterations into three major categories: Obliteration, distortion and imitation and suggesting possible countermeasures 3) Demonstrating by using an example of database, where based on matching score the person of interest is branded as guilty or not and then based on decrease in value of matching score[4][1] if below threshold value we can declare that the fingerprint is altered or not then combine fingerprint Image with person's UID(Unique Identity) comparing with that fingerprint with existing fingerprints showing if there is any match in the form of percentage and display his/her details with criminal record, 4) developing the above system by a technique to automatically detect altered fingerprints based on segmentation using Morphological operations, minutia marking with special considering the triple branch counting[11], minutia unification by decomposing a branch into three terminations[11][12], and matching in the unified x-y coordinate system orientation estimation[13], minutiae matching after a two-step transformation.*

Keywords: *Fingerprints, AFIS, alteration, orientation estimation, minutiae matching, threshold, UID.*

I. Introduction

Fingerprint recognition has been in use by law enforcement agencies to identify suspects and victims for almost 100 years. Since fingerprints are unique features for each individual, it keeps the each person's uniqueness for the life time There are many scenarios were lots of perpetrators has been identified by their fingerprints found in the crime scenes. Because of this, many perpetrators try avoiding their fingerprints to be found, either by spoofing or by alteration in order to mask their fingerprints In this paper we discuss about fingerprint alteration

The use of altered fingerprints to mask one's identity constitutes a serious "attack" against a border control biometric system since it defeats the very purpose for which the system was deployed in the first place,[7][8] i.e., to identify individuals in a watch list. It should be noted that altered fingerprints are different from fake fingerprints. The use of fake fingers—made of glue, latex, or silicone—is a well-publicized method to circumvent fingerprint systems. Altered fingerprints, however, are real fingers that are used to conceal one's identity in order to evade identification by a biometric system. While fake fingers are typically used by individuals to adopt another person's identity, altered fingers are used to mask one's own identity. In order to detect attacks based on fake fingers, many software and hardware solutions have been proposed. However, the problem of altered fingerprints has hitherto not been studied in the literature and there are no reported techniques to identify them. Furthermore, the lack of public databases comprised of altered fingerprint images has stymied research in this area. One of the goals of this paper is to highlight the importance of the problem, analyze altered fingerprints, and propose an automatic detect.ion algorithm for them.

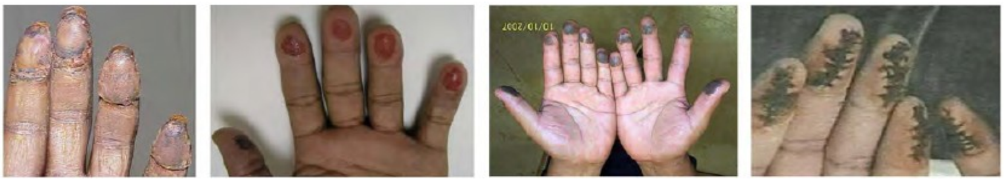


Figure 1 shows various cases of fingerprint obliteration

We divide the altered fingerprints into 3 types:
a) Obliteration,
b) Distortion,
c) Imitation

a) Obliteration

Friction ridge patterns on fingertips can be obliterated by abrading, cutting, burning, applying strong chemicals, and transplanting smooth skin. Further factors such as skin disease (such as leprosy) and side effects of a cancer drug can also obliterate fingerprints. Friction ridge structure is barely visible within the obliterated region, Obliteration most popular form of alteration. This may be because obliteration, which completely destroys ridge structures, is much simpler to perform than distortion/imitation, which requires a surgical procedure. Furthermore, detecting distorted or imitated fingerprints is much more difficult for human examiners than obliterated fingerprints.

Obliterated fingerprints can evade fingerprint quality control software, depending on the area of the damage. If the affected finger area is small, the existing fingerprint quality assessment software's may fail to detect it as an altered fingerprint, but AFIS is likely to successfully match the damaged fingerprint to the original mated fingerprint. But, if the altered area is sufficiently large, fingerprint quality control software can easily detect the damage. To identify individuals with severely obliterated fingerprints, it may be necessary to treat these fingerprints as latent images, perform AFIS search using manually marked features, and adopt an appropriate fusion scheme for ten print searches. In rare cases, even if the finger surface is completely damaged, the dermal papillary surface, which contains the same pattern as the epidermal pattern, may be used for identification.

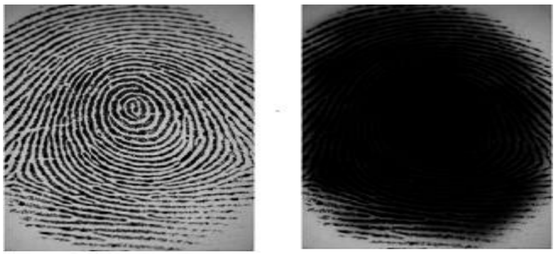

(a) (b)

Figure 2 (a) shows before alteration (b) shows after alteration (fingerprint is burnt)

b) Distortion

Friction ridge patterns on fingertips can be turned into unnatural ridge patterns by removing portions of skin from a fingertip and either grafting them back in different positions (Fig. 10a) or replacing them with friction ridge skin from the palm or sole. Distorted fingerprints have unusual ridge patterns which are not found in natural fingerprints. These abnormalities include abnormal spatial distribution of singular points or abrupt changes in orientation field along the scars. Note that orientation field discontinuity in natural fingerprints is usually observed only at singular points.

Distorted fingerprints can also successfully pass the fingerprint quality test since their local ridge structure remains similar to natural fingerprints while their global ridge pattern is abnormal. For instance, a distorted fingerprint as a result of swapping skin patches within the same finger retains the same ridge property (e.g., ridge frequency and width) over the entire fingerprint area.

Fingerprints altered by “Z” cut are of special interest since they retain their original ridge structure, enabling reconstruction of the original fingerprint before alteration. Therefore, it is imperative to upgrade current fingerprint quality control software to detect the distorted fingerprints. Once detected, the following operations may be performed to assist AFIS: 1) identify unaltered regions of the fingerprint and manually mark the features (i.e., the minutiae) in these regions and 2) reconstruct the original fingerprint as in the “Z” cut case.

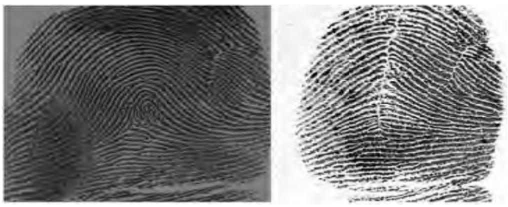

(a) (b)

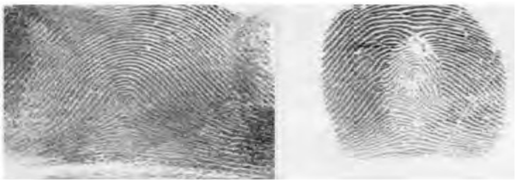
Figure 3 (a) shows before distortion (b) shows after distortion

c) Imitation

Friction ridge patterns on fingertips can still preserve fingerprint-like pattern after an elaborate procedure of fingerprint alteration: 1) a portion of skin is removed and the remaining skin is pulled and stitched together,

2) Friction ridge skin from other parts of the body is used to fill the removed part of the fingertip to reconcile with the remaining ridge structure, or 3) transplantation of the entire fingertip. As reported in, simply swapping the skin on fingertips between the left and right hands successfully evaded AFIS.

Imitated fingerprints can not only successfully pass the fingerprint quality assessment software; they can also confound human examiners. Fig. Shows pre-altered and post-altered fingerprint mates. The altered fingerprint has a very smooth orientation field over the entire fingerprint area (which looks like an arch-type fingerprint) and the only evidence of possible alteration is a thin scar.



(a) (b)

Figure 4 (a) shows before imitation and (b)after imitation

II. Related Work

Since existing fingerprint quality assessment algorithms are designed to examine if an image contains sufficient information for matching, they have limited capability in determining if an image is a natural fingerprint or an altered fingerprint. Depending on the area of the damage, If the affected finger area is small, the existing fingerprint quality assessment software may fail to detect it as an altered fingerprint. Even if they are there they only intimate whether the fingerprint is altered or not.

III. System Design

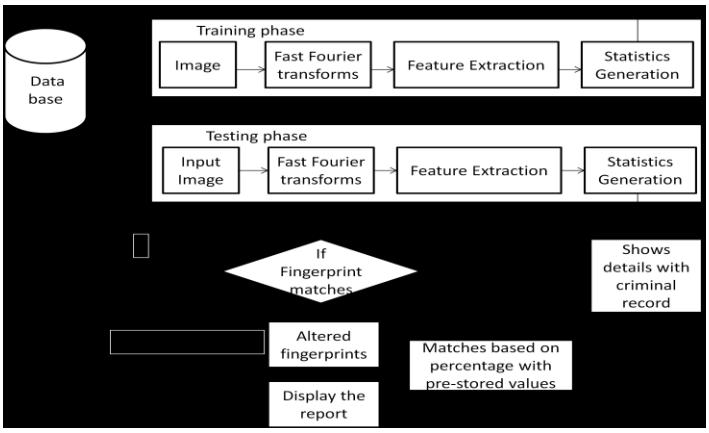


Figure 5 System Design

The different images of proper fingerprints are stored in database.

$I_{D=}\{i_{d1},i_{d2,}i_{d3}........................\}$ (1)

Where, I- Standard set

i- Individual image

D- Standard data set

d- Individual data set

In the training phase images are chosen from different data sets which are of different persons for the training purpose.

$T_{D=}\{t_{d1}, t_{d2,} t_{d3}........................\}$ (2)

Where, T- Standard training

t- Individual image

D- Standard data set

d- Individual data set

Training is done by taking individual images and by applying Fourier transforms and feature extraction- by applying histogram equalization, binarization, orientation flow estimation, region of interest, thinning, removing high breaks and spikes, applying minutiae extraction to extract minutiae, and finally removing spurious minutiae and finally saving the file as ID number as dat file. What we are doing is we are integrating image with ID number to extract the details of the person with criminal record along with altered [3][5] and non-altered fingerprint images.

The classifier used here is KBC (knowledge based classifier). The threshold set for altered fingerprint is 69.99% and below and for proper fingerprint is 70.01% and above.

IV. Algorithm

1. Initially take first image from the database, which is stored in the form of queue, and train that image apply Fast Fourier transforms by dividing the image into small processing blocks (32 by 32 pixels) and perform the Fourier transform.
2. To enhance a specific block by its dominant frequencies, multiply the FFT of the block by its magnitude a set of times. Get the enhanced block accordingly.
3. Apply Histogram equalization, Region of interest and extract minutiae and finally remove false minutiae.
4. Repeat steps 1-3 on rest of the image.
5. Generate and Store the statistical value in database.
6. Give a fingerprint image from outside, in testing phase and repeat steps 1-3 on that image.
7. Generate the statistical value out of that image.
8. Compare both trained and Testing phase's statistical values if they match 100% Go to step 9 otherwise go to step 10
9. Display Database guide with person's details along with criminal background.
10. Display altered fingerprint guide with person's matching details along with criminal background. Also display, altered and non-altered fingerprint of same person.
11. Generate a report and display the same for any of the case.

V. Processing and Feature Extraction

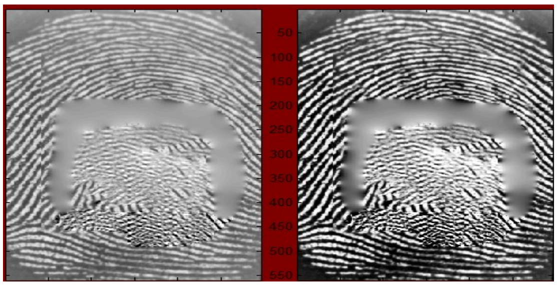


Figure 6 shows images of before and after applying histogram equalization

Two Methods are adopted in my fingerprint recognition system: the first one is Histogram Equalization; the next one is Fourier Transform.

Histogram equalization is to expand the pixel value distribution of an image so as to increase the perception information. The original histogram of a fingerprint image has the bimodal type [Figure 7], the histogram after the histogram equalization occupies all the range from 0 to 255 and the visualization effect is enhanced [Figure 6]

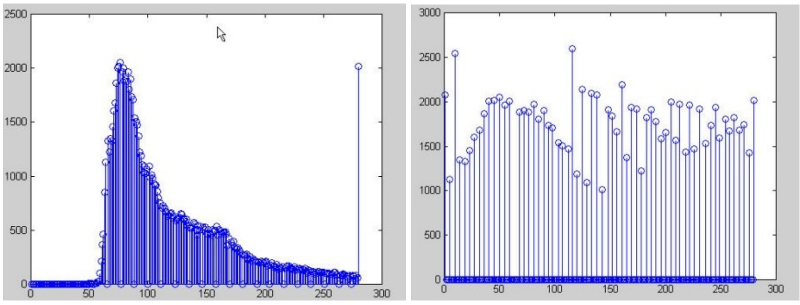


Figure 7 the Original histogram of a fingerprint image and after histogram equalization

We divide the image into small processing blocks (32 by 32 pixels) and perform the Fourier transform according to:

$$F(u,v)=\sum_{x=0}^{M-1}\sum_{y=0}^{N-1} f(x,y)\times\exp\left\{-j2\pi\times\left(\frac{ux}{M}+\frac{vy}{N}\right)\right\}(1)$$

For u = 0, 1, 2, ..., 31 and v = 0, 1, 2, ..., 31.

In order to enhance a specific block by its dominant frequencies, we multiply the FFT of the block by its magnitude a set of times. Where the magnitude of the original FFT = abs (F (u, v)) = |F(u, v)|.

Get the enhanced block according to

$$g(x,y)=F^{-1}\{F(u,v)*|F(u,v)|^{k}\}\ (2)$$

Where F^{-1}(F (u,v)) is done by:

$$f(x,y)=\frac{1}{MN}\sum_{x=0}^{M-1}\sum_{y=0}^{N-1} F(u,v)\times\exp\left\{j2\pi\times\left(\frac{ux}{M}+\frac{vy}{N}\right)\right\}\quad(3)$$

For x = 0, 1, 2,…. 31 and y = 0, 1, 2, ..., 31.

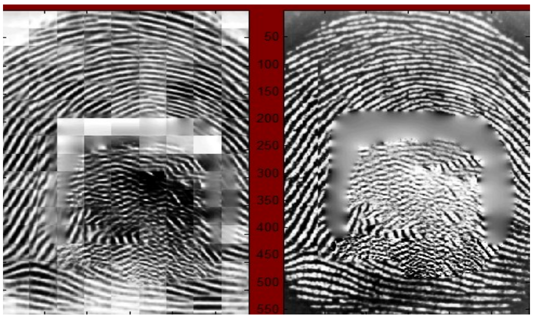


Figure 8 shows the application of FFT on left hand side of the image

The k in formula (2) is an experimentally determined constant, which we choose k=0.45 to calculate. While having a higher "k" improves the appearance of the ridges, filling up small holes in ridges, having too high a "k" can result in false joining of ridges. Thus a termination might become a bifurcation. The enhanced image after FFT has the improvements to connect some falsely broken points on ridges and to remove some spurious connections between ridges. The side effect of each block is obvious but it has no harm to the further operations because I find the image after consecutive binarization operation is pretty good as long as the side effect is not too severe.

Fingerprint Image Binarization is to transform the 8-bit Gray fingerprint image to a 1-bit image with 0-value for ridges and 1-value for furrows. After the operation, ridges in the fingerprint are highlighted with black colour while furrows are white.

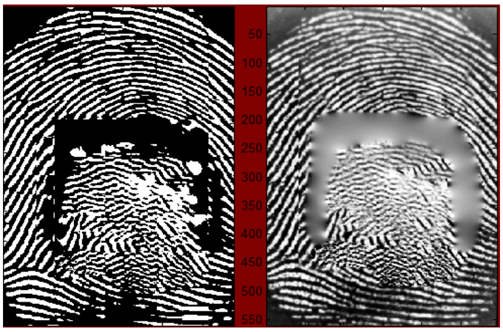


Figure 9 shows how the image changes after applying binarization (the left image**)**

In general, only a Region of Interest (ROI) is useful to be recognized for each fingerprint image. The image area without effective ridges and furrows is first discarded since it only holds background information.[7] Then the bound of the remaining effective area is sketched out since the minutia in the bound region is confusing with those spurious minutias that are generated when the ridges are out of the sensor. To extract the ROI, a two-step method is used. The first step is block direction estimation and direction variety check, while the second is intrigued from some Morphological methods.

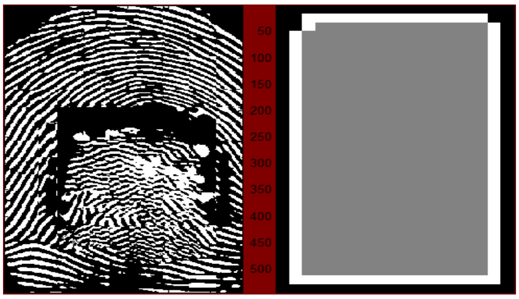


Figure 10 shows how Region of Interest is being selected (right image)

Extraction of minutiae and false minutiae removal: In general, for each 3x3 window, if the central pixel is 1 and has exactly 3 one-value neighbours, then the central pixel is a ridge branch [8]. If the central pixel is 1 and has only 1 one-value neighbour, then the central pixel is a ridge ending. Suppose both the uppermost pixel with value 1 and the rightmost pixel with value 1 have another neighbour outside the 3x3 window, so the two pixels will be marked as branches too. But actually only one branch is located in the small region. So a check routine requiring that none of the neighbours of a branch are branches is added. Together with the minutia marking, all thinned ridges in the fingerprint image are labelled with a unique ID for further operation. The labelling operation is realized by using the Morphological operation: BWLABEL.

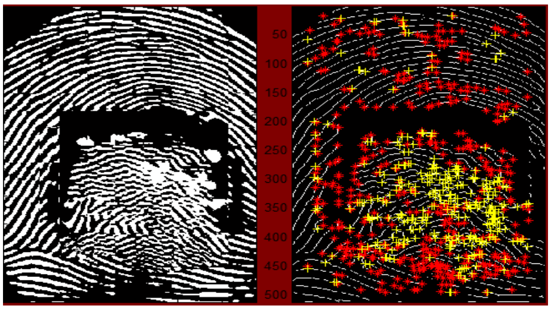


Figure 11 shows the minutiae points marking (right image)

The false minutia will significantly affect the accuracy of matching if they are simply regarded as genuine minutia. So some mechanisms of removing false minutia are essential to keep the fingerprint verification system effective.

Procedures in removing false minutia are:

1. If the distance between one bifurcation and one termination is less than D and the two minutias are in the same ridge (m1 case). Remove both of them. Where D is the average inter-ridge width representing the average distance between two parallel neighbouring ridges.
2. If the distance between two bifurcations is less than D and they are in the same ridge, remove the two bifurcations.
3. If two terminations are within a distance D and their directions are coincident with a small angle variation. And they suffice the condition that no any other termination is located between the two terminations. Then the two terminations are regarded as false minutia derived from a broken ridge and are removed.
4. If two terminations are located in a short ridge with length less than D, remove the two terminations.

My proposed procedures in removing false minutia have two advantages. One is that the ridge ID is used to distinguish minutia and the seven types of false minutia are strictly defined comparing with those loosely defined by other methods. The second advantage is that the order of removal procedures is well considered to reduce the computation complexity. It surpasses the way adopted by [12] that does not utilize the relations among the false minutia types.

Unify terminations and bifurcations

Since various data acquisition conditions such as impression pressure can easily change one type of minutia into the other, most researchers adopt the unification representation for both termination and bifurcation. So each minutia is completely characterized by the following parameters at last: 1) x-coordinate, 2) y-coordinate, and 3) orientation.

The orientation calculation for a bifurcation needs to be specially considered. All three ridges deriving from the bifurcation point have their own direction, [11] represents the bifurcation orientation using a technique proposed in [13][10] Simply chooses the minimum angle among the three anticlockwise orientations starting from the x-axis. Both methods cast the other two directions away, so some information loses. Here I propose a novel representation to break a bifurcation into three terminations. The three new terminations are the three neighbour pixels of the bifurcation and each of the three ridges connected to the bifurcation before is now associated with a termination.

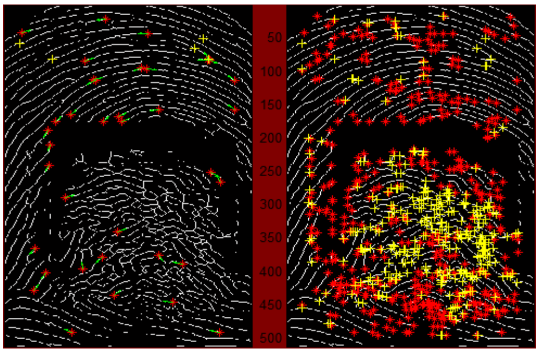
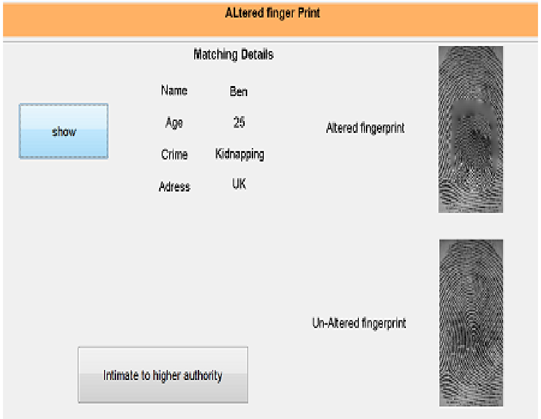


Figure 12 shows the removal of false minutiae by considering combinations of bifurcations and termination (left image)

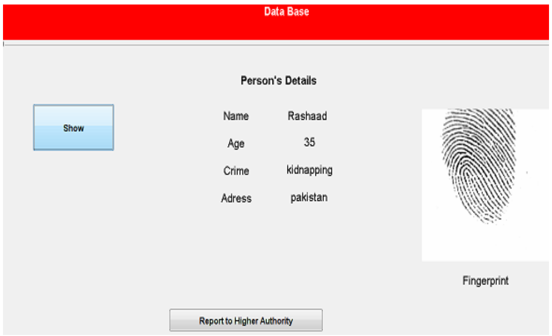
And finally when the guide opens for the respective cases (i.e. if matching 70 and above normal database or below 70 altered) as it is already integrated with person's UID number with the figure 13 and 14 shows the details of the person in both cases if the person has any criminal charges then only we intimate to higher authority by pressing the button below in each guide. Then the report will be generated accordingly.



Matching Details

Name	Ben
Age	25
Crime	Kidnapping
Adress	UK

Figure 13 shows the guide for altered fingerprint with person's details along with criminal background

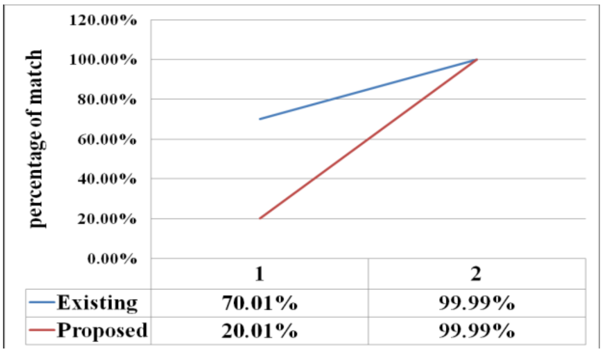


Person's Details

Name	Rashaad
Age	35
Crime	kidnapping
Adress	pakistan

Figure 14 shows the guide for proper fingerprint with person's details along with criminal background

VI. Graph



	1	2
Existing	70.01%	99.99%
Proposed	20.01%	99.99%

Figure 15 shows the graph between existing and proposed systems red represents proposed and blue represents existing system

VII. Conclusion

We have combined many methods to build a minutia extractor and a minutia matcher like Fast Fourier Transforms, Binarization, Histogram Equalization, and Region of Interest. The combination of multiple methods comes from a wide investigation into research paper. Also some novel changes like segmentation using Morphological operations, minutia marking with special considering the triple branch counting, minutia unification by decomposing a branch into three terminations, and matching in the unified x-y coordinate system after a two-step transformation are used. Also a program coding with MATLAB going through all the stages of the altered fingerprint recognition is built. It is helpful to understand the procedures of altered fingerprint recognition. By use of this method along with knowledge based classifier, the person with altered fingerprint can be identified and by also giving his Id number we can club fingerprint as well as his details along with criminal record to find out whether the person is criminal or not. Based on this knowledge people who seek asylum and try to hide their identity can be easily identified.

References

[1] Altered Fingerprints: Analysis and Detection by Jianjiang Feng (2012)
[2] Yi (Alice) Wang and Jiankun Hu “Global Ridge Orientation Modelling for Partial Fingerprint Identification” (2011)
[3] Jianjiang Feng “Detecting Altered Fingerprints” (2010)
[4] Anil k jain “Fingerprint Alteration” 2009
[5] Kajal Singh “Altered Fingerprints” 2009
[6] Fingerprint Recognition Using Minutia Score Matching by RAVI. J, K. B. RAJA 2009
[7] Systematic Methods for the Computation of the Directional Fields and Singular Points of Fingerprints by M. Bazen (july 2002)
[8] Sweden refugees mutilate fingers BBC news
[9] Journal of the American Institute of Criminal Law and Criminology
[10] Lin Hong. "Automatic Personal Identification Using Fingerprints", Ph.D. Thesis, 1998.
[11] Image Systems Engineering Program, Stanford University. Student project By Thomas Yeo, Wee Peng Tay, Ying Yu Tai
[12] L.C. Jain, U.Halici, I. Hayashi, S.B. Lee and S.Tsutsui. Intelligent biometric techniques in fingerprint and face recognition. 1999, the CRC Press.
[13] M. J. Donahue and S. I. Rokhlin, "On the Use of Level Curves in Image Analysis," Image Understanding, VOL. 57, pp 652 - 655, 1992.