Vidya Journal of Engineering & Technology
ISSN 2277-8978, Vol. 3, No. 1, Jan-Dec 2017, pp. 11-24

AN APPROACH FOR LATENT FINGERPRINT MATCHING FOR EXPLORING CRIME DETECTION BY USING AADHAAR DATABASE

Rajendra Kumar & Muhammad Aqeel Ashraf***

ABSTRACT

Latent Fingerprint Matching is an authentication technique that has widely helped law enforcement officials to identify potential criminals for decades, but recently it has gain wider usage. This paper investigates the new technique for latent fingerprint recognition and matching with the database of AADHAAR card (like social security number in India). Although the word Latent means “hidden or invisible”, but in modern usage for forensic science the term Latent Prints means accidental impressions left by friction ridge skin on a surface, regardless of whether it is visible or invisible at the time of deposition. The fingerprint obtained from the crime scenes is stored in the database to be matched with the central database containing the fingerprints of citizens (AADHAAR Database) in order to check whether the citizen may be a criminal or not. Several times investigators collect fingerprints captured through camera. The main problem with these fingerprints is that they are captured from different distances. As a result, the captured fingerprint is a zoomed image of the original one. Sometimes, fingerprints have a broken curve due to uneven surface and low finger pressure as these are left unintentionally. In this paper, we present an algorithm that implements the concept of M_join. Thus, our proposed approach eliminates the pseudo minutiae that connect broken curves in fingerprints.

Keywords: *Latent fingerprint, FFT, FRR, FAR, M_join, M_join, M_curve.*

* Vidya College of Engineering, Meerut,

** School of Environmental Studies, China University of Geosciences, Wuhan, P. R. China.

I. INTRODUCTION

Biometrics is the term that has gained a benchmark in the field of security for authenticating a person by analyzing their physical characteristics (like fingerprints) or behavior characteristics. The performance of the biometric system is governed by two rates i.e. high FRR (False Rejection Rate) and low FAR (False Acceptance Rate). False Rejection and Acceptance Rate are complementary in determining how severe a biometric system is in allowing access to individuals [1] depending on set threshold.

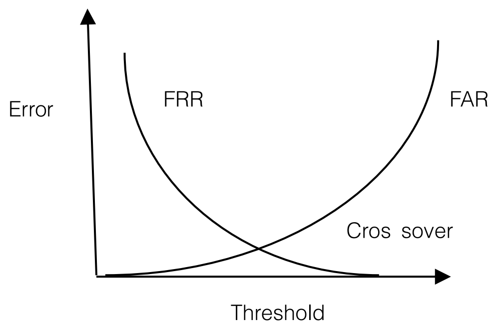

Fig. 1 Threshold level in fingerprint matching

The quantity and direction of the pressure applied by the user, the skin conditions and the projection of an irregular 3D object (the finger) onto a 2D flat plane introduce distortions, noise and consistencies in the captured fingerprint image [6]. Although the lexicon meaning of the word Latent means hidden or invisible but in modern usage for forensic science the term Latent Prints means accidental impressions left by friction ridge skin on a surface, regardless of whether it is visible or invisible at the time of deposition [2].

Each person has his/her own fingerprints with the permanent uniqueness. So, fingerprints are being used for identification and forensic investigation for the long time. It is composed of many ridges and furrows. The ridges and furrows present good similarities in each small local window like parallelism and average width. However, fingerprints are not distinguished by their ridges and furrows but by minutiae which are some abnormal points on the ridges. Fingerprints are not distinguished by their ridges and furrows but by minutia, which are some abnormal points on the ridges [3].

II. OBJECTIVE

The doctrine of the paper is to detect the person by matching the fingerprint impressions extracted from different distances, different finger pressures, uneven surfaces and dust particles with the fingerprints stored in the knowledge base in order to check whether the person is suspect or not. The law enforcement agencies worldwide have employed fingerprint recognition for two main purposes:

- Establish the identity of a suspect (or victim) based on partial prints, or lateens, left at a crime scene.
- Identify repeat offenders based on prints of all of their fingers.

The whole procedure advances in the following manner:

- Extracting the fingerprint left unintentionally which are analyzed with the help of the chemical spray.
- Enhancing the extracted image by using the techniques like FFT (Fast Fourier Transformation), and filtering (Gaussian and Butterworth filters), then matching the enhanced image with the image stored in the knowledge base.
- Finally analyzing the result.

III. PREVIOUS WORK

The online fingerprint matching systems are 99.94% [15] accurate therefore a very little scope is available for improvement but in case of offline (latent taken from crime scene) fingerprints a lot of work is being done to make system near to perfect.

The fingerprints obtained from the crime scenes are of bad quality because these are captured unintentionally from an uneven surface. Such fingerprints are called latent fingerprints [1]. Latent fingerprint impressions left at the crime scenes require manual “lifting” techniques like dusting [4]. [19] have proposed a framework that matches fingerprints on pressure variation. They have given AAN based algorithm for filling the small breaks in the latent fingerprints created because of uneven surface and uneven pressure.

Poor quality fingerprint image lead to missing and spurious minutiae that degrade the performance of fingerprint matching system. The poor-quality image produces many spurious minutiae and many genuine minutiae may be ignored. Therefore, an image enhancement algorithm is necessary to increase the performance of the minutiae extraction algorithm. The present algorithm for minutiae extraction implements either the M_connect [17] or M_curve [3] technique but their fusion can be even more effective.

The latent fingerprints contain partial area of a finger, and often have smudged or blurring ridges due to which the performance rate of the minutiae extraction degrades.

There is a great issue of how the fingerprints can be sensed. The traditional "ink and paper" method which is still in use involves applying ink to the finger surface, rolling the finger from one side of the nail to the other on a card, and finally scanning the card to generate a digital image. In the more popular live-scan method, a digital image is directly obtained by placing the finger on the surface of a fingerprint. Optical sensors [17] based on the frustrated total internal reflection (FTIR) technique are commonly used to capture live-scan fingerprints in forensic and government applications, while solid-state touch and sweep sensors-silicon based devices that measure the differences in physical properties such as capacitance or conductance of the friction ridges and valleys.

A. Manipulations with fingerprint image

The quality of the input fingerprint images greatly influence efficacy of a fingerprint image-matching system. Acquisition of good quality images is very important especially in the case of latent fingerprints but due to some environmental factors or user's body condition, a significant percentage of acquired images are of unacceptable quality for a computerized identification system in practice [5].

The Binarization and the Thinning operations form some of the structures like the triangles, bridges, spurs, opposing minutiae and ladders which leads to invalid minutiae extraction when the feature is extracted.

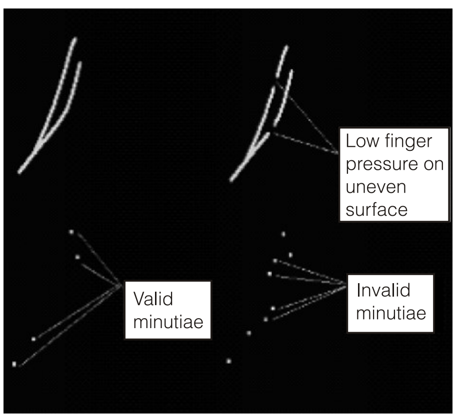

Fig. 2 Extraction of invalid minutiae due to presence of dust particles or cut on finger.

B. Extraction of valid and invalid minutiae

The primary reason with pseudo (false) minutiae is the presence of dust particles, oily fingers, dry fingers, and cut on finger. Dry finger may fail to produce a complete line/curve up to the actual end points. As a result, the break points create pseudo minutiae as seen in the figure 3.

1	0	0	0	0	0	1	0
0	1	0	0	0	1	0	0
0	0	1	0	1	0	0	0
0	0	0	0	0	0	0	0
1	0	0	0	0	0	0	0
0	1	0	0	0	1	0	0
0	0	1	0	0	0	1	0
0	0	0	1	0	0	0	1

Fig. 3 Thinned image with false minutiae

IV. NEED OF GOOD QUALITY FINGERPRINT IMAGES

Quality of a fingerprint image has a great impact on the matching process and influences the result obtained. A good quality fingerprint images will result in high match up performance resulting into the correct recognition of a person [7]. Accurate minutiae extraction from fingerprint images is heavily dependent on the quality of the fingerprint images. In order to improve the performance of the system, much effort has been made on the image enhancement algorithms [17]. If the preprocessing is adaptive to the fingerprint image characteristics in the image enhancement step, the performance gets to be more robust [8].

Practically the quality of a fingerprint image depends on the clearness of the separated ridges by valleys and the uniformity of the separation. However, the change in the physical conditions such as temperature and pressure might manipulate a fingerprint image in many ways; the humidity and oily finger dominate the overall quality of the fingerprint [5].

Extracting fingerprint impressions holds great importance in the whole matching process as it is the initial process in which the fingerprint needs to be the finest quality because the quality deteriorates gradually in the consecutive steps. Also, it results into high FRR (False Rejection Rate).

V. HIGH FALSE REJECTION RATE CASES

The False Rejection Rate is the measure of the likelihood that the biometric security system will incorrectly reject an access attempt by an authorized user [9].

Possible reasons for high FRR cases

- **Physiological Problems:** These cannot be solved by the user alone and thus have mainly to be addressed by the system developer. These are:
    - **Wet Fingers:** Specially, capacitive sensors may have problems with wet fingers. They often occur with young users or in warm environment.
    - **Dry fingers:** They often happen with elder users. The situation with dry fingers may partially be diffused by the user (increase pressure and weight longer).
    - **Minutiae scarcity:** Some users may have too few minutiae to be detected without problems, depending on sensor area.
    - **Skin disease:** Some kind of skin disease may destroy or disturb the natural finger structure.
    - **Skin abrasion:** Depending on sensor type many handcraft activities may decrease the ridge heights such that many sensors deliver only small contrast pictures. This effect is reversible.
- **Operational Problems:** These problems arise from wrong usage and can be solved by system design and user behavior. This is due to wrong Finger pressure, if is the pressure on the sensor is too high the image quality mat degrades.
- **Wrong finger positioning:** Usually rotation and translation is limited because of limited sensor area and because of fake protection. Sometimes a finger guide is not accepted by a user because it may be insufficient or too difficult to be understood.
- **Software Problems:** During feature extraction, there are possibilities to have too many minutiae, to have too few minutiae, inaccurate minutia position, inaccurate minutia type, inaccurate Minutia angle, etc. to affect the recognition process.

Measures to improve FRR

- **Physiological problems:**
  - **Wet Fingers:** For capacitive the amplitude resolution in the region of water seems to show high potential of improvement. The problem may be diffused by drying fingers.
  - **Dry Fingers:** For capacitive sensors low noise and high resolution in the region of air is important. The problem may be solved by increase pressure and waiting longer.
  - **Minutia Scarcity:** Increase sensor area.
  - **Skin disease:** No remedy known.
- **Hardware problems:** Major problem is related to Sensor. Spatial resolution should be greater than 500 dpi, gray level resolution at least 200 steps, Surface resistance against contaminations, noise less than 1 LSB and sensor area greater than 150 mm2.

VI. PROPOSED MODEL

In order to reduce crimes, our proposed model collects the latent fingerprints from the crime scenes captured by the high-quality camera. The image being captured may or may be of a good quality on which the further operations are performed, so the initial step is to enhance the fingerprint image being captured followed by filtering (Gaussian and Butterworth filters).

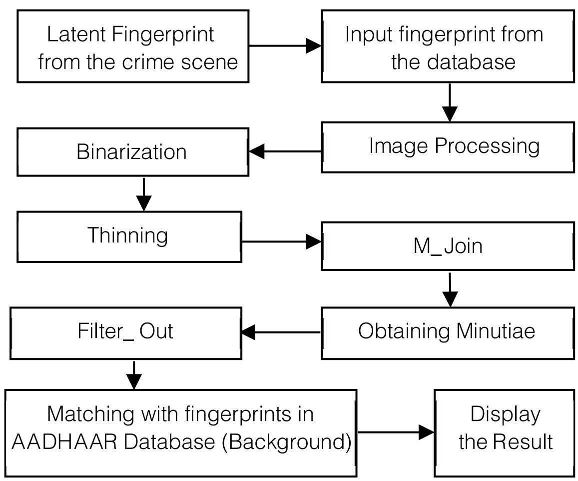

Fig. 4 Model of proposed system

- **Image Enhancement:** Once the image has been extracted from the spot, enhancement is required to improve its quality using the techniques such as:

- **Fast Fourier Transformation (FFT):** It is the technique used in the frequency domain and is defined as an efficient algorithm to compute the Discrete Fourier Transform and its inverse. A FFT computes the DFT (Discrete Fourier Transform) and produces exactly the same result as evaluating the DFT definition directly [11]. It is defined by the formula:

  for u = 0, 1, 2, 3, ... , 31 and v = 0, 1, 2, ..., 31
- **Filtering:** Image filtering is useful for many applications like smoothening, Sharpening, Removing noise and edge detection. In our proposed mode either of the two filtering techniques may be used i.e., Gaussian Low Pass Filter or Butterworth Low Pass Filter.
- A Low-Pass Filter is the basis for most smoothing methods. An image is smoothed by decreasing the disparity between the pixel values by averaging nearby pixels.

Fig. 5 (a) Original Gray Image, (b) Filtered Image

Butterworth Low Pass Filter: The transfer function of Butterworth Low Pass Filter of order n with cut-off frequency at distance D0 from the origin is defined by:

Gaussian Low Pass Filter: The transfer function of Gaussian Low Pass Filter of order n with the cut-off frequency at D0 from the origin is defined by:

- **Inverse Fast Fourier Transform:** It is defined by the formula:
- **Image Binarization:** The binarization process enhances the image and converts it into the binary form (0 and typically the two colors (Black and White) are used. Thus image binarization converts an image up to 256 gray levels to a black and white image. Frequently binarization is used as a pre-processor before OCR (Optical Character Recognition) [13].

  The simplest way to use image binarization is to choose a threshold value, and classify all pixels with the values above the threshold as white, and all other pixels as black. Now the problem arises that how to select the correct threshold. In many cases, finding one threshold compatible to the entire image is very difficult, and in many cases even impossible. Therefore, adaptive image binarization is needed where an optimal threshold is chosen for each image area.

Fig. 6 Binarized Image

- **Image Thinning:** The binary image obtained is now converted into the one-pixel wide skeleton which is known as Thinning. It is based on spatial domain method and considers each pixel with its neighbors. The process of thinning includes two processes.
- **Ridge Thinning:** It eliminates redundant pixels of ridges till the ridges are 1 pixel wide. In each scan of the full fingerprint image, the algorithm marks down the redundant pixels in each small image window of (3×3) matrix and finally removes all those marked pixels after several scans.
- **Skeleton Refinement:** This operation takes thinned image as the input and produces refined skeleton image by converting small straight lines to curve to the maximum possible extent.

Fig. 7 Thinned Image

- **M_join:** The M_join is the combination of M_Connect and M_Curve. The M_Curve combined with M_Connect gives thinned fingerprint to make matching system more robust.

This manipulation increases length of curve by adding white pixels at each end. The final result FRR is improved due to elimination of some false minutiae.

- **M_Connect:** It is further used to refine the skeleton of the thinned image. The procedure of M_Connect is as follows:

```
for i, j
        if (out(i, j) == 1) && (out(i+1, j+1) == 1)
        then out(i+1, j) = 0 and out(i, j +1) = 0
        (if out(i, j) == 1) && (out(i-1, j+1) == 1)
        then out(i, j +1) = 0 and out(i-1, j) = 0
end
```

- **M_Curve:** It adds one white pixel at the broken ends. Although the minutiae marking positions are diverted one pixel far away from the actual position, but as a final result FRR is improved due to elimination of some invalid minutiae as shown in fig. 8.

***i*-1,*j*-3**			
	***i*,*j*-2**		
		***i*+1,*j*-1**	
	i*, *j		

Fig. 8 M_curve Identification

There exist sixteen such conditions as explained above which increase the length of the curve. After this operation some of the cases appear which are eliminated by filtering. The fingerprint image segment after M_Curve operation is shown in fig. 9.

Fig. 9 Image after M_Join

End Points: End points find out all the minutiae in a fingerprint image. It also includes invalid points due to injury, involvement of dust particles, bad surface in case of fingerprint captured through camera. If the sum of neighboring pixel is 0 or 1 then it is an End point. If the sum of the neighboring pixel is 3 or more then it is a Branch point.

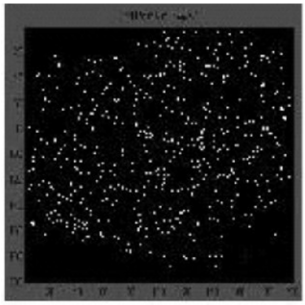

Fig. 10 End Points

- **Real End Points:** Once the end points and branch points are obtained, the list is maintained which after filtering using the End_Track method helps in obtaining the valid minutiae.
- **End_Track:** This method examines each end point in such a manner that if there exist a path of minimum 25 pixels corresponding to that end point, then that end point is considered relevant and is a Real End Point.

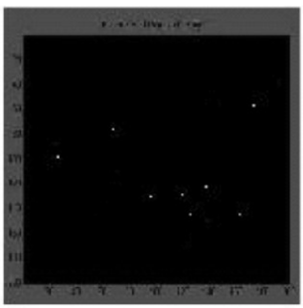

Fig. 11 Real End Point

- **Matching:** Once the real end points of the latent image are being calculated, the final process of matching is done between the two images, one fetched from the database and another taken from crime scene. The matching process takes place in the following manner:
  (i) The valid center of the image being obtained from the knowledge base is that minutiae which is closest to the resolution center of the image.

(ii) The Eigen values and eigenvectors [16] are calculated for each minutiae of the image with respect to the valid center of the image.

(iii) PCA (Principle Component Analysis) [18] allows finding the projection of the real ends of the latent image onto the Eigen vectors of the image obtained from knowledge base.

(iv) The extent to which the real points obtained from the first image are projected on the Eigenvectors of the Second image gives the percentage of the matching

V. EXPERIMENTS AND RESULTS

The various experiments were conducted on the fingerprints (complete and fractional) that were gathered at different twenty pressures and improvement in the results has been found that gradually enhances the performance as part of our experiments. Consider the two images:

(a) L402 gm **(b) L306 gm**

Fig. 12

The percentage of matching from the preexisting model was 16.3275% whereas the percentage of matching has improved to 24.5796%.

Similarly, the experiments have been conducted on 200 different images and the percentage of matching has enhanced from 8.9738% to 11.2548% by applying M_Curve.

VI. CONCLUSION

Our proposed model could be used to categorize the suspect more vigorously and reduce crimes globally. The performance of the fingerprint matching relies critically on the quality of the image. Therefore, the more efficient way of extracting the valid minutiae and their matching has been proposed which is helpful in improving the overall performance. Also, the algorithms that have been implemented from the image extraction to the image enhancement and from minutiae extraction to minutiae matching are refined from the preexisting model which gives us a better and proficient approach in matching process. The research of our paper is the use of EigenValues and EigenVectors in the matching of the valid minutiae that has reduced the overhead of matching in the preexisting model.

VII. FUTURE SCOPE

Biometrics is gaining its importance day by day in every fields related to the authentication of the person that act as a proof to identify the right suspect in case of crimes. The proposed alignment method performs very well on latent that contain small number of minutiae. Further we plan to incorporate extended features which are automatically extracted from the image into the current matcher to further improve the matching accuracy. Also, improvements of current representations through robust and reliable domain-specific image processing techniques such as: Model-based Orientation Field Estimation and Robust – image Enhancement and masking. Feature based indexing schemes (minutiae triplets) can be introduced that will surely enhance the performance.

REFERENCES

[1] **K. Asai, H. Izumisawa, H. Owada, S. Kinoshita, and S. Matsuno**, (1987), "Method and Device for Matching Fingerprints with Precise Minutia Pairs Selected from Coarse Pairs", US Patent 4646352.

[2] **Anil K. Jain, Jianjiang Feng, Abhishek Nagar, Karthik Nanda Kumar,** (2007), "On Matching Latent Fingerprints", ARO grant W911NF-06-1-0418 and NIJ grant-RG-CX-K183.

[3] **Saurabh Sharma, Rajendra Kumar**, (2011), "Modeling and Simulation: Latent Fingerprint Matching", M. Tech. Dissertation, KSOU.

[4] **Anil K. Jain,** (2011), Fellow, IEEE, and Jianjiang Feng, "Latent Fingerprint Matching", IEEE Transactions on Pattern Analysis and Machine Intelligence, Vol. 33(1).

[5] **Eun_kyung Yun, Jin_Hyung Hong, and Sung-Bae Cho,** "Adaptive Enhancing of fingerprint Image with Image Characteristics Analysis", http://citeseerx.ist.psu.edu/ viewdoc/download?doi=10.1.1.100.8895&rep=rep1&type=pdf

[6] **D. Maltoni, D. Maio, Anil Kumar Jain, and S. Prabhakar,** (2009), "Handbook of Fingerprint Recognition", Second Ed. Springer.

[7] **T. Y. Jea and V. Govindaraju,** (2005), "A Minutia-Based Partial Fingerprint Recognition System", Pattern Recognition, Vol. 38(10), pp. 1672-1684.

[8] **E. Tabassi, C. Wilson, and C. Watson,** "Fingerprint Image Quality," NISTIR 7151, http://fingerprint.nist.gov/NFIS/ ir_7151.pdf

[9] **T. Van der Putte and J. Keuning,** (2001), “Biometrical fingerprint recognition: Don’t get your fingers burned. Smart Card Research and Advanced Applications”, IFIPTC8/W68.8 Fourth Working Conference on Smart Card Research and Advanced Applications, pp. 289–303.

[10] **D. Maio, D. Maltoni,** (1997) “Direct Gray-scale Minutiae Detection in Fingerprints”, IEEE Trans. Pattern Anal. Mach. Intell.19, pp.27-39.

[11] **J. W. Cooley, P. A. Lewis, and P. D. Welch,** (1967), “History of the fast Fourier transform”, In Proc. IEEE, Vol. 55, pp. 1675.1677.

[12] **L. Hong, Y. Wan, and A. Jain,** (1998), “Fingerprint Image Enhancement: Algorithm and Performance Evaluation”, IEEE Trans. Pattern Analysis and Machine Intelligence, Vol. 20(8), pp.777-789.

[13] **Bolle et al.,** (1986), “System and methods for determining the quality of fingerprint images”, United States patent number US596356, 1999.

[14] **W. Niblack,** (1986), “An introduction to digital image processing”, Prentice (Hall) Englewood Cliffs NJ, pp. 115-116.

[15] **Anil Jain, Lin Hong, Ruud Bolle,** (1997), “On-Line Fingerprint Verification”, IEEE Transactions on Pattern Analysis and Machine Intelligence, Vol. 19(4), pp. 29-38.

[16] **Xudong Jiang,** (2005), “On Orientation and Anisotropy Estimation for Online Fingerprint Authentication”, IEEE Transactions on Signal Processing, Vol. 53(10), pp. 15-20.

[17] **Rajendra Kumar,** (2007), “Variaion in Biometric Data: Modeling and Simulation”, M. Tech. Thesis, UPTU.

[18] **Ernande F. Melo, H. M. De Oliveira,** (2015), “A Fingerprint-based Access Control using Principal Component Analysis and Edge”, Signal Processing Group, Federal University of Pernambuco C.P., Brazil.

[19] **Rajendra Kumar, Saurabh Sharma,** (2009), Paradigm Shift on Finger-print Recognition on Pressure Variation and Impact of Information System in Crime Reduction, Global Journal of Enterprise Information System, Vol. 1(1), pp. 88-93.

[20] **Jugal Kishor Gupta, Rajendra Kumar,** (2010), “An efficient ANN Based approach for Latent Fingerprint Matching”, IJCA, Vol. 7(10), pp. 18-21.