Altered Fingerprints: Identification and Analysis

Reji R
SAINTGITS College of Engineering
Kottayam,
India.

Akhil Mathew Philip
SAINTGITS College of Engineering
Kottayam,
India.

ABSTRACT
Automated Fingerprint Identification Systems (AFIS) is deployed in law authorization and fringe control applications. This has elevated the requirement for guaranteeing that these frameworks are not traded off. A few issues identified with finger print analysis frameworks security have been explored. This includes the utilization of fake fingerprints for disguising personality. The issues of finger print alteration or jumbling has gotten almost no consideration. Fingerprint Obfuscation alludes to the planned change of the finger print pattern of a single person with the goal of veiling his personality. A few instances of unique finger print Obfuscation have been reported so far. Finger print image quality assessment software can't generally identify adjusted fingerprints. This paper highlights the significance of the issue by analyzing altered fingerprints and proposes an effective algorithm for them.

Keywords
fingerprints, Obfuscation, Alteration, Minutia

1. INTRODUCTION
FINGER print Analysis and recognition has been effectively utilized by law authorization organizations to recognize suspects and exploited people for many years. Late advances in computerized Finger print analysis, coupled with the developing requirement for dependable individual distinguishing proof, have brought about an expanded utilization of fingerprints in both government and Citizen Applications [3]. For example, Border control, historical verifications, and secure office access. The utilization of changed fingerprints to veil one's character is a serious issue[6]. It is noticed that altered fingerprints are not quite the same as fake fingerprints. The utilization of fake fingers—made of paste, latex, or silicone—is a decently plugged system to evade finger print analysis frameworks.

The finger print analysis system is evaluated at two levels finger level and at the subject level [1]. At the finger level, we assess the execution of recognizing regular and adjusted fingerprints. At the subject level, we assess the execution of recognizing subjects with fingerprint characteristics and those with modified fingerprints. The main contributions of this paper are:

1) Each pixel of a fingerprint is stored in matrix format so it makes easy analysis and detection process.

2) Mean algorithm can be used for removing noise from fingerprint image.

3) Zhang suen algorithm is capable of handling matrix information more accurately and efficiently.

4) In matching process given fingerprint is matched with every fingerprint in the database, after checking with every fingerprint some fingerprint image are extracted from database and give rank to everyone. Ranking starts from 0-3 and Percentage of matched pixel is more in rank-0 image than other one. And the information of the corresponding person will be extracted from database.

2. ALGORITHM USED
The algorithms used in this approach are mean algorithm and Zhang- Suen algorithm [3]. A region is extracted from fingerprint image that having some discontinuity in its fingerprint lines. Zhang Suen algorithm is capable of handling matrix information more accurately and efficiently. This algorithm can be used for creating a Skeleton image of fingerprint. It can handle matrix information very easily and helps us to find out eight neighboring pixels. So we can easily find out region that having discontinuity. The noise embedded in the color regions in each image is removed by a modified version of K means algorithm. The Euclidean Distance is calculated and is used to determine which cluster a pixel belongs to. Every pixel is put into a cluster, which produces the minimum Euclidean Distance between the pixel and the centroid. The minimum number of pixels in the clusture is 8.The proposed method for altered fingerprints analysis and detection produces more accurate result. Results show the feasibility of the proposed algorithms. The algorithm is based on the extracted features from the minutia and orientation field. The requirements for the detection algorithm are

1) Fast operational time.
2) High true positive rate at low false positive rate.
3) Ease of integration into AFIS.

3. FEATURE EXTRACTION OF FINGER PRINT
The captured image can have a range of specifications. The pixels are 8-bit values, and intensity range from 0 to 255.

a) Binary matrix formation

Feature extraction is the most difficult stage of altered finger print identification. For feature extraction, after taking finger print image we want to calculate length and breadth of finger print image, then store each pixel of finger print image in a matrix format. By using this matrix format we can easily manipulate finger print information.

b) Smoothing

In feature extraction, smoothing plays a vital role. For making smoothed finger print image K means algorithm is used.

4. DETECTIONOFALTERED FINGERPRINTS

a) Normalization

The input fingerprint image is normalized by taking a small rectangular region from the centre of the fingerprint. The extracted features are invariant to translation and rotation [1].

b) Orientation field estimation

The fingerprint orientation field is calculated using the gradient-based method [14][15]. The initial field is obtained by smoothed average filter, followed by averaging the orientations in pixel blocks. A foreground mask is created for filling local blocks and morphological process is performed.

c) Orientation field approximation

The orientation field is approximated by a polynomial model [17][18].

d) Feature extraction

The error map is computed using the absolute difference and is used to construct the feature vector [1].

5. ANALYSIS OF MINUTIA DISTRIBUTION

The ridge characteristic in the image is indicated by the minutia [16] .In most finger print approaches minutia is used in the matching process. In addition to the orientation field abnormalities of altered finger prints there are differences in the minutia too.

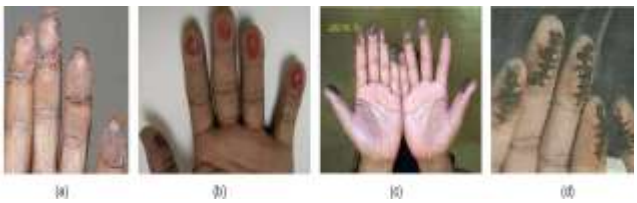

Figure 1: Altered Fingers

(a) Transplanted friction ridge skin from sole [7]

(b) Fingers that have been bitten [8]

(c) Fingers burnt by acid [9]

(d) Stitched fingers [10]

Figure 2: Registering Finger Print

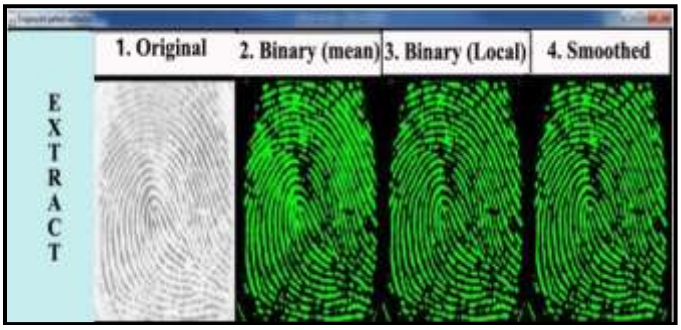

Figure 3: Finger Print Extraction

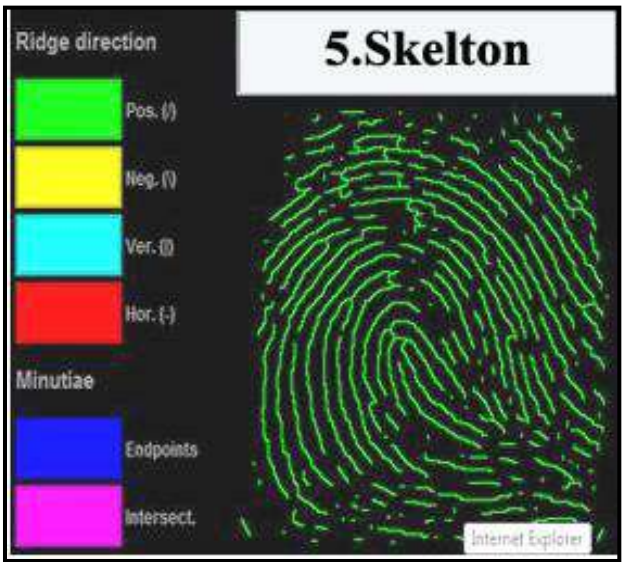

Figure 4.1 a

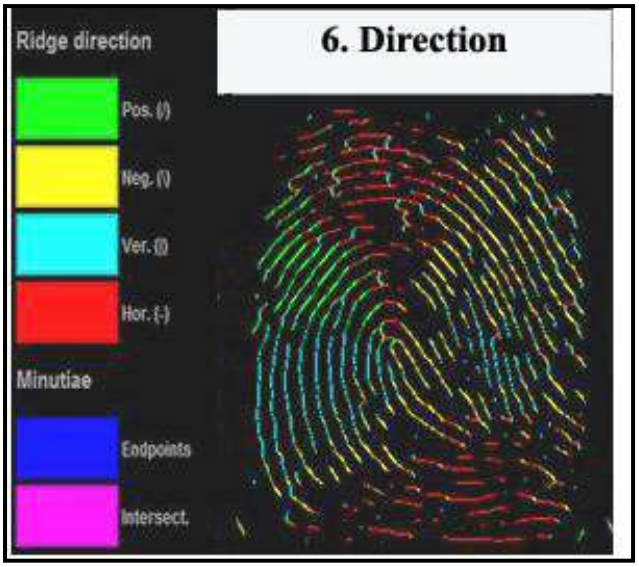

Figure 4.1 b

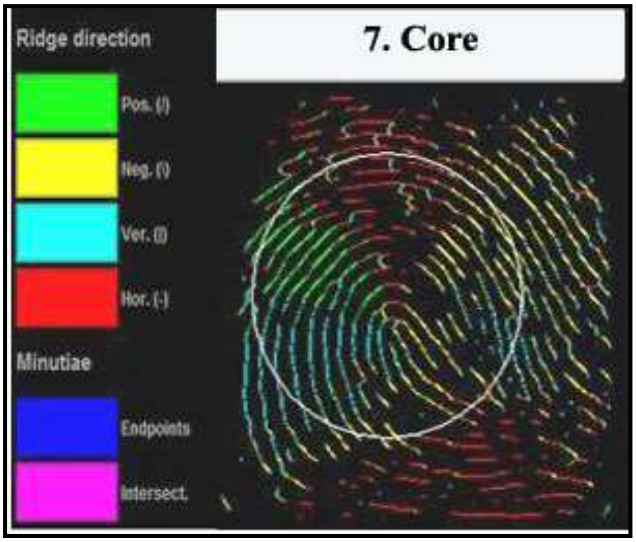

Figure 4.1 c

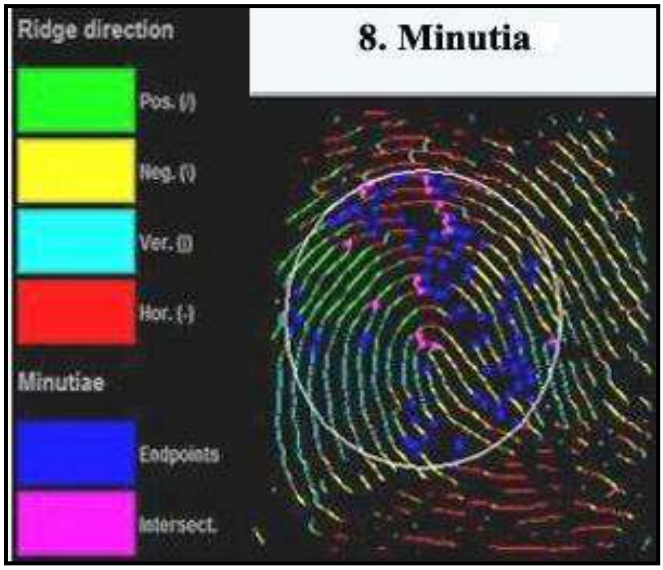

Figure 4.1 d

Figure 4: Extracted Finger Print

Figure 5: Similarity Measure

Figure 6: Match Details

6. CONCLUSION

The advantage and effectiveness of AFIS have prompted many people around the world to evade idfentification by altering the finger prints. . Fingerprint Obfuscation alludes to the planned change of the finger print pattern of a single person with the goal of veiling his personality. Finger print Obfuscation is different from fingerprint spoofing. Now a day's fingerprint spoofing has got much attention but obfuscation we need to move a lot. Obfuscation may be encountered even with face and iris .

This work can be further extended to

1. Automatic detection of the type of alteration.
2. Reconstruction of altered finger prints.
3. Matching process between altered and its unaltered mates.
4. Using multimodalities.

7. REFERENCES

[1] Yoon, Feng, A.K. Jain, "Altered Fingerprints analysis and detection,"IEEE transaction on pattern analysis and machine intelligence 2012.

[2] J. Feng, A.K. Jain, and A. Ross, "Detecting Altered Fingerprints,"Proc. 20th Int'l Conf. Pattern Recognition, pp. 1622-1625, Aug. 2010.

[3] D. Maltoni, D. Maio, A.K. Jain, and S. Prabhakar, Handbook of Fingerprint Recognition, second ed. Springer-Verlag, 2009.

[4] The U.S. Department of Homeland Security, US-VISIT, http://www.dhs.gov/usvisit, 2011.

[5] The Fed. Bureau of Investigation (FBI), Integrated Automated Fingerprint Identification System(IAFIS), http://www.fbi.gov/hq/cjisd/iafis.htm, 2011.

[6] H. Cummins, "Attempts to Alter and Obliterate Finger-prints,"J. Am. Inst. Criminal Law and Criminology, vol. 25, pp. 982-991, 1935.

[7] [Surgically Altered Fingerprints, http://www.clpex.com/images/FeetMutilation/L4.JPG, 2011.

[8] K. Singh, Altered Fingerprints, http://www.interpol.int/Public/ Forensic/fingerprints/research/alteredfingerprints.pdf, 2008.

[9] M. Hall, "Criminals Go to Extremes to Hide Identities," USA Today, http://www.usatoday.com/news/nation/2007-11-06-criminal-extreme_N.htm, Nov. 2007.

[10] Criminals Cutting off Fingertips to Hide IDs,http://www.thebostonchannel.com/news/15478914/detail.html, 2008.

[11] A. Antonelli, R. Cappelli, D. Maio, and D. Maltoni, "Fake Finger Detection by Skin Distortion Analysis," IEEE Trans. Information Forensics and Security, vol. 1, no. 3, pp. 360-373, Sept. 2006

[12] K.A. Nixon and R.K. Rowe, "Multispectral Fingerprint Imaging for Spoof Detection," Proc. SPIE, Biometric Technology for Human Identification II, A.K. Jain and N.K. Ratha, eds., pp. 214-225, 2005

[13] E. Tabassi, C. Wilson, and C. Watson, "Fingerprint Image Quality," NISTIR 7151, http://fingerprint.nist.gov/NFIS/ir_7151.pdf, Aug. 2004.

[14] C. Watson, M. Garris, E. Tabassi, C. Wilson, R.M. McCabe, S. Janet, and K. Ko, "NIST Biometric Image Software," http://www.nist.gov/itl/iad/ig/nbis.cfm, 2011.

[15] A.M. Bazen and S.H. Gerez, "Systematic Methods for the Computation of the Directional Fields and Singular Points of Fingerprints," IEEE Trans. Pattern Analysis and Machine Intelligence,vol. 24, no. 7, pp. 905-919, July 2002.

[16] F. Alonso-Fernandez, J. Fierrez, J. Ortega-Garcia, J. Gonzalez- Rodriguez, H. Fronthaler, K. Kollreider, and J. Bigun, "A Comparative Study of Fingerprint Image-Quality Estimation Methods," IEEE Trans. Information Forensics and Security, vol. 2,no. 4, pp. 734-743, Dec. 2007.

[17] J. Zhou and J. Gu, "A Model-Based Method for the Computation of Fingerprints' Orientation Field," IEEE Trans. Image Processing, vol. 13, no. 6, pp. 821-835, 2004.

[18] S. Huckemann, T. Hotz, and A. Munk, "Global Models for the Orientation Field of Fingerprints: An Approach Based on Quadratic Differentials," IEEE Trans. Pattern Analysis and Machine Intelligence, vol. 30, no. 9, pp. 1507-1519, Sept. 2008.

[19] Y. Wang and J. Hu, "Global Ridge Orientation Modeling for Partial Fingerprint Identification," IEEE Trans. Pattern Analysis andMachine Intelligence, vol. 33, no. 1, pp. 72-87, Jan. 2010.

8. AUTHOR PROFILE

Reji R. is a Ph.D Research Scholar at School of Computer Sciences, Mahatma Gandhi University – Kottayam, Kerala, India. He received his Masters in Computer Applications (MCA) from M S University, Tirunelveli and his MTech in Computer Science and Information Technology from Centre for Information Technology and Engineering. Currently working as an Assistant Professor in the Department of Computer Applications, SAINTGITS college of Engineering, Kottayam, Kerala, India. His research interests include Image Registration, Face Recognition, 3D Face Recognition, Artificial Neural networks, and DataMining.

Akhil Mathew Philip. Is Currently working as an Assistant Professor in the Department of Computer Applications, SAINTGITS college of Engineering, Kottayam, Kerala, India. His research interests include Image Registration,Information Security and Data Mining.