Improved Fingerprint Matching by Distortion Removal

B. Abhinethri
M. tech 2nd year, IT, MGIT, Hyderabad, India.

Dr.V. Ramesh
Professor, IT, MGIT, Hyderabad, India.

Abstract – Elastic distortion of fingerprints is one of the major causes for false non-match. While this problem affects all fingerprint recognition applications, it is especially dangerous in negative recognition applications, such as watch list and deduplication applications. In such applications, malicious users may purposely distort their fingerprints to evade identification. In this paper, we proposed novel algorithms to detect and rectify skin distortion based on a single fingerprint image. Distortion detection is viewed as a two-class classification problem, for which the registered ridge orientation map and period map of a fingerprint are used as the feature vector and a SVM classifier is trained to perform the classification task. Distortion rectification (or equivalently distortion field estimation) is viewed as a regression problem, where the input is a distorted fingerprint and the output is the distortion field. To solve this problem, a database (called reference database) of various distorted reference fingerprints and corresponding distortion fields is built in the offline stage, and then in the online stage, the nearest neighbor of the input fingerprint is found in the reference database and the corresponding distortion field is used to transform the input fingerprint into a normal one. Promising results have been obtained on three databases containing many distorted fingerprints, namely FVC2004 DB1, Tsinghua Distorted Fingerprint database, and the NIST SD27 latent fingerprint database.

Index Terms – Fingerprint, distortion, registration, nearest neighbor regression.

1. INTRODUCTION

FINGERPRINT recognition has been successfully used by law enforcement agencies to identify suspects and victims for almost 100 years. Recent advances in automated fingerprint identification technology, coupled with the growing need for reliable person identification, have resulted in an increased use of fingerprints in both government and civilian applications such as border control, employment background checks, and secure facility access [2]. Examples of large-scale fingerprint systems in the US government arena include the US-VISIT's IDENT program [3] and the FBI's IAFIS service [4].

The primary purpose of fingerprint alteration [5] is to evade identification using techniques varying from abrading, cutting, and burning fingers to performing plastic surgery (see Fig. 1).

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 [10] and hardware [11] solutions have been proposed

Fig. 1. Photographs of altered fingerprints. (a) Transplanted friction ridge skin from sole [6]. (b) Fingers that have been bitten [7]. (c) Fingers burnt by acid [8]. (d) Stitched fingers [9].

Localized dictionaries based orientation field estimation for latent fingerprints:

Dictionary based orientation field estimation approach has shown promising performance for latent fingerprints. In this paper, we seek to exploit stronger prior knowledge of fingerprints in order to further improve the performance. Realizing that ridge orientations at different locations of fingerprints have different characteristics, we propose a localized dictionaries-based orientation field estimation algorithm, in which noisy orientation patch at a location output by a local estimation approach is replaced by real orientation patch in the local dictionary at the same location. The precondition of applying localized dictionaries is that the pose of the latent fingerprint needs to be estimated. We propose a Hough transform-based fingerprint pose estimation algorithm, in which the predictions about fingerprint pose made by all orientation patches in the latent fingerprint are accumulated. Experimental results on challenging latent fingerprint datasets show the proposed method outperforms previous ones markedly.

Orientation field estimation for latent fingerprint enhancement:

Identifying latent fingerprints is of vital importance for law enforcement agencies to apprehend criminals and terrorists. Compared to live-scan and inked fingerprints, the image quality of latent fingerprints is much lower, with complex image background, unclear ridge structure, and even overlapping patterns. A robust orientation field estimation algorithm is indispensable for enhancing and recognizing poor quality latent. However, conventional orientation field estimation algorithms, which can satisfactorily process most live-scan and inked fingerprints, do not provide acceptable results for most latent. We believe that a major limitation of conventional algorithms is that they do not utilize prior knowledge of the ridge structure in fingerprints. Inspired by spelling correction techniques in natural language processing, we propose a novel fingerprint orientation field estimation algorithm based on prior knowledge of fingerprint structure. We represent prior knowledge of fingerprints using a dictionary of reference orientation patches. Which is constructed using a set of true orientation fields, and the compatibility constraint between neighboring orientation patches. Orientation field estimation for latents is posed as an energy minimization problem, which is solved by loopy belief propagation. Experimental results on the challenging NIST SD27 latent fingerprint database and an overlapped latent fingerprint database demonstrate the advantages of the proposed orientation field estimation algorithm over conventional algorithms.

2. RELATED WORK

1.1 Distortion Detection Based on Special Hardware

It is desirable to automatically detect distortion during fingerprint acquisition so that severely distorted fingerprints can be rejected. Several researchers have proposed to detect improper force using specially designed hardware [16], [17], [18]. Bolle et al. [16] proposed to detect excessive force and torque exerted by using a force sensor. They showed that controlled fingerprint acquisition leads to improved matching performance [17]. Fuji [18] proposed to detect distortion by detecting deformation of a transparent film attached to the sensor surface.

The above methods have the following limitations: (i) they require special force sensors or fingerprint sensors with video capturing capability; (ii) they cannot detect distorted fingerprint images in existing fingerprint databases;

1.2 Distortion Rectification Based on Finger- Specific Statistics:

Ross et al. [26], [27] learn the deformation pattern from a set of training images of the same finger and transform the template with the average deformation. They show this leads to higher minutiae matching accuracy. But this method has the following limitations: (i) acquiring multiple images of the same finger is inconvenient in some applications and existing fingerprint databases generally contain only one image per finger; and (ii) even if multiple images per finger are available, it is not necessarily sufficient to cover various skin distortions.

DISADVANTAGES

- Distortion rectification (or equivalently distortion field estimation) is viewed as a regression problem, where the input is a distorted finger print and the output is the distortion field.
- They require special force sensors or fingerprint sensors with video capturing capability
- They cannot detect distorted fingerprint images in existing fingerprint databases.

They cannot detect fingerprints distorted before pressing on the sensor.

3. PROPOSED MODELLING

This paper described a novel distorted fingerprint detection and rectification algorithm. For distortion detection, the registered ridge orientation map and period map of a fingerprint are used as the feature vector and a SVM classifier is trained to classify the input fingerprint as distorted or normal. Distortion rectification (or equivalently distortion field estimation) is viewed as a regression problem, where the input is a distorted fingerprint and the output is the distortion field. A nearest Neighbor regression approach is used to predict the distortion field from the input distorted fingerprint and then the inverse of the distortion Field issued to transform the distorted fingerprint into a normal one

A. NORMALIZATION

An input fingerprint image is normalized by cropping a rectangular region of the fingerprint, which is located at the center of the fingerprint and aligned along the longitudinal direction of the finger, using the NIST Biometric Image Software (NBIS). This step ensures that the features extracted in the subsequent steps are invariant with respect to translation and rotation of finger.

B. ORIENTATION FIELD ESTIMATION

The orientation field of the fingerprint is computed using the gradient-based method. The initial orientation field is smoothed averaging filter, followed by averaging the orientations in pixel blocks. A foreground mask is obtained by measuring the dynamic range of gray values of the fingerprint image in local blocks and morphological process for filling holes and removing isolated blocks is performed.

C. ORIENTATION FIELD APPROXIMATION

The orientation field is approximated by a polynomial model to obtain.

D. FEATURE EXTRACTION

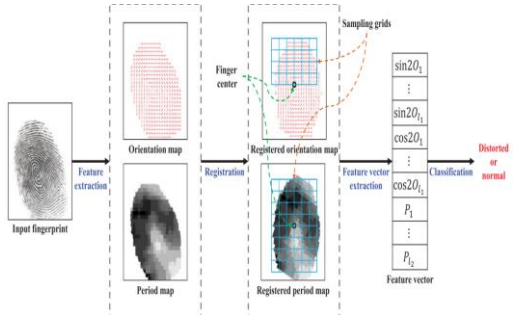
The error map is computed as the absolute difference between and used to construct the feature vector.

False non-match frequency of fingerprint matchers is relatively high in severely distorted fingerprints. It creates a security hole in automatic fingerprint detection systems that could be used by criminals and terrorists. So, building up of fingerprint distortion scrutiny and reformation algorithms to fill the hole is a must.

ADVANTAGES

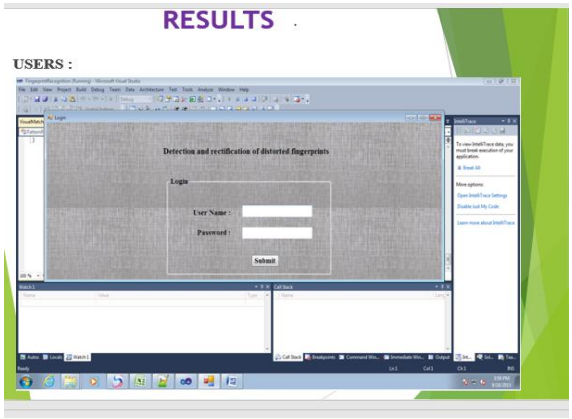
- Fingerprint rectification algorithm consists of an offline stage and an online stage. In the offline stage, a database of distorted reference fingerprints is generated by transforming several normal reference fingerprints with various distortion fields sampled from the statistical model of distortion fields.
- The proposed distortion rectification algorithm by performs well by performing matching experiments on various databases.
- The proposed algorithm can improve recognition rate of distorted fingerprints evidently.

SYSTEM ARCHITECTURE



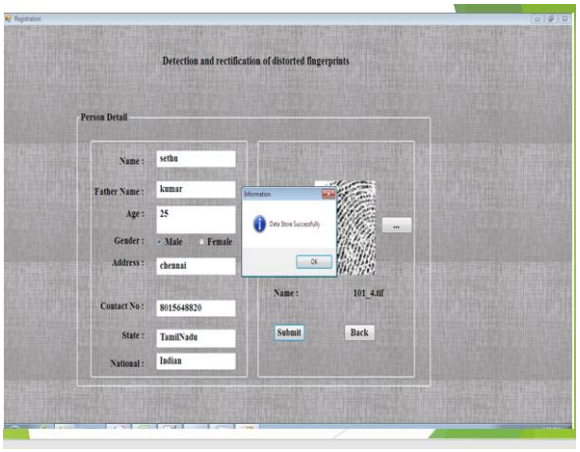
4. RESULTS AND DISCUSSIONS

Fig 1. USER login page



The user should login through username and password in order to perform registration process

Fig 2. Person details



After entering the user details, fingerprint image the data will be stored successfully in the database.

Fig 3. LAB login page

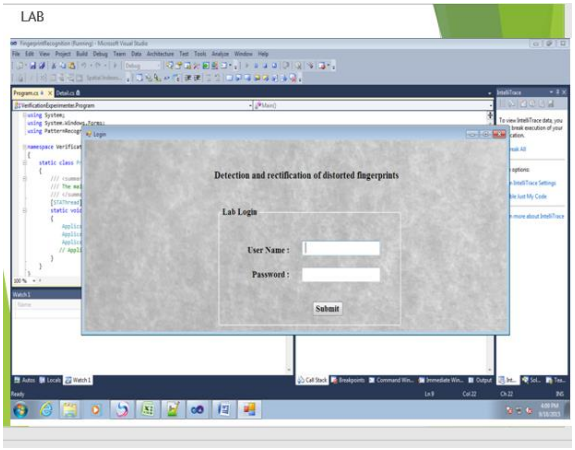
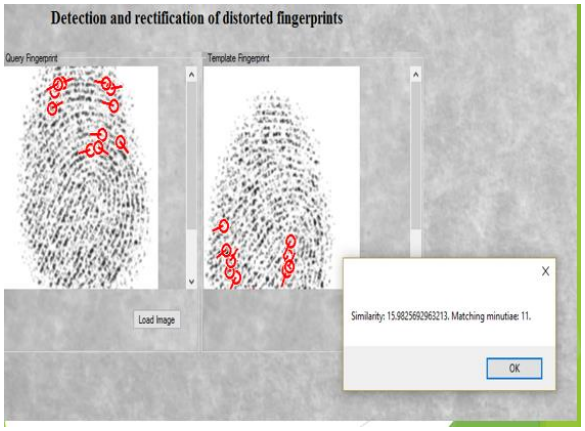


Fig. 4



Similarity between two fingerprints will be calculated.

5. CONCLUSION

False non-match rates of fingerprint matchers are very high in the case of severely distorted fingerprints. This generates a security hole in automatic fingerprint recognition systems which can be utilized by criminals and terrorists. For this reason, it is necessary to develop a fingerprint distortion detection and rectification algorithms to fill the hole. This paper described a novel distorted fingerprint detection and rectification algorithm. For distortion detection, the registered ridge orientation map and period map of a fingerprint are used as the feature vector and a SVM classifier is trained to classify the input fingerprint as distorted or normal. For distortion rectification (or equivalently distortion field estimation), a nearest neighbor regression approach is used to predict the distortion field from the input distorted fingerprint and then the inverse of the distortion field is used to transform the distorted fingerprint into a normal one.

6. FUTURE ENHANCEMENT

The major limitation of the current approach does not support rolled fingerprints. It is difficult to collect many rolled fingerprints with various distortion types and meanwhile obtain accurate distortion fields for learning statistical distortion model. It is ongoing work to address the limitation.

REFERENCES

[1] Yang, J. Feng, and J. Zhou, "Localized dictionaries based orientation field estimation for latent fingerprints," IEEE Trans. Pattern Anal. Mach. Intell., vol. 36, no. 5, pp. 955–969, May 2014.
[2] Maltoni, D. Maio, A.K. Jain, and S. Prabhakar, Handbook of Fingerprint Recognition, second ed. Springer-Verlag, 2009.
[3] J. Feng, J. Zhou, and A.K. Jain, "Orientation field estimation for latent fingerprint enhancement," IEEE Trans. Pattern Anal. Mach. Intell., vol. 35, no. 4, pp. 925–940, Apr. 2013.
[4] The Fed. Bureau of Investigation (FBI), Integrated Automated Fingerprint Identification System (IAFIS), http://www.fbi.gov/ hq/cjisd/iafis.htm, 2011
[5] J. Feng, Zhou, and A.K. Jain, "Orientation field estimation for latent fingerprint
[6] N. Ratha and R. Bolle, "Effect of controlled image acquisition on fingerprint matching, "inInt.Conf. PatternRecognit.,1998,vol.2,pp.1659–1661.
[7] Y. Fuji, "Detection of fingerprint distortion by deformation of elastic film or displacement of transparent board," U.S. Patent No. 7 660 447, Feb. 9, 2010.
[8] 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.
[9] C.-C. Chang and C.-J. Lin, "LIBSVB: A Library for support vector machines", *ACM Trans. Intell. Syst. Technol.*, vol. 2, pp. 27:1-27:27, 2011.
[10] J. Dai, J. Feng and J. Zhou, "Robust and efficient ridge-based palm print matching", *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 34, no. 8, pp. 1618-1632, Aug. 2012.
[11] A. Ross, S. C. Dass, and A. K. Jain, "Fingerprint warping using ridge curve correspondences," IEEE Trans. Pattern Anal. Mach. Intell., vol. 28, no. 1, pp. 19–30, Jan. 2006.
[12] X. Si, J. Feng, and J. Zhou, "Detecting fingerprint distortion from a single image," in Proc. IEEE Int. Workshop Inf. Forensics Security, 2012, pp. 1–6.

Author

Dr. V. Ramesh, Professor in the Department of Information Technology, obtained B.Tech in CSE from S.V. University , M.Tech and PhD in Computer Science and Engineering from Sathyabama University, Chennai. He has 12 years of teaching experience. He has authored two books "Principles of Operating Systems" by University Science Press, New Delhi. & " Preemptive DSR for Mobile Ad Hoc Networks" by Lambert Lap Publishers, Germany. He has published 48 research papers in various refereed International Journals and Conference Proceedings. He is the Editorial Board member for International Journal of Computer Engineering and Applications, Honorary Reviewer for Global Journal of Computer Science and Information Technology, Reviewer for IET Journal of Networks, IEEE Transactions of Mobile Computing and many more. He served for many conferences as session chair, advisory board member and technical committee member. He is the member of CSI, ISTE, IAENG, IACSIT, ASDF, GARD, etc.