International Journal of Innovative Research in Computer and Communication Engineering

Survey on Detection and Rectification of Distorted Fingerprint Using SVM Classifier by PCA Algorithm

Nishi Garg[1,] Akhil Pratap Singh[2,] Neha Vaishampayan[3]

Student, Dept of Electronic and Communication, Vindhya Institute of Technology and Science, Satna, MP, India

Prof, Dept of Electronic and Communication, Vindhya Institute of Technology and Science, Satna, MP, India

Asst. Prof, Dept of Electronic and Communication, Vindhya Institute of Technology and Science, Satna, MP, India

ABSTRACT: One of the open come outs in fingerprint confirmation is the lack of robustness against image quality degradation. Poor-quality images result in specious and missing features, thus degrading the performance of the overall system. Therefore, it is very important for a fingerprint acknowledgement system to estimate the quality and validity of the captured fingerprint images. Also the elastic distortion of fingerprints is one of the major causes for false non-match. While this problem impacts all fingerprint acknowledged applications, it is especially unsafe in negative recognition applications, such as watch list and reduplication applications. In such applications, malicious users may purposely distort their fingerprints to elude identification. In this paper, we proposed novel algorithms to detect and rectify skin distortion based on a individual fingerprint image. Distortion notification 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 prepared to perform the classification task.. Distortion detection is displayed as a two-class categorization problem, for which the registered ridge orientation map and period map of a fingerprint are beneficial as the feature vector and a SVM classifier is trained to act the classification task. Distortion rectification (or equivalently distortion field estimation) is viewed as a regression complication, where the input is a distorted fingerprint and the output is the distortion field. To clarify 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 closest neighbor of the input fingerprint is organized in the reference database and the corresponding distortion field is used to transform (Convert) the input fingerprint into a normal fingerprints. Promising results have been obtained on three databases having many distorted fingerprints, namely FVC2004 DB1, Tsinghua Distorted Fingerprint database, and the NIST SD27 latent fingerprint database.

KEYWORDS: Fingerprint, distortion, registration, nearest neighbor regression, rectification, classifiers, SVM.

I.   INTRODUCTION

Although automatic fingerprint recognition technologies have briskly advanced during the last forty years, there still exists many challenging research problems, for example, recognizing low quality fingerprints [2]. Finger-print matcher is very sensitive to image quality as seen in the FVC2006, where the matching accuracy of the same algorithm varies significantly among different data-sets due to variation in image quality. The variation between the accuracies of plain, rolled and latent fingerprint matching is even larger as found in technology evaluations conducted by the NIST. The consequence of low quality fingerprints depends on the type of the fingerprint recognition system. A fingerprint recognition system can be categorized as either a positive or negative system. In a positive recognition system, such as physical access control systems, the end user is supposed to be cooperative recognition and wishes to be identified. In a negative system, such as identifying persons in watch lists and detecting multiple enrollments under different names, the user of concern (e.g., criminals) is supposed to be uncooperative and does not want to be identified. In a positive recognition system, low quality will points to false reject of legitimate persons and thus bring inconvenience. The effect of low quality for a negative

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 2, February 2016

Recognition system, however, is more serious, since malicious users may purposely reduce fingerprint quality to prevent fingerprint system from finding the true identity. In fact, law

Enforcement officials have encountered a number of cases where criminals attempted to avoid identification by damaging or surgically altering their fingerprints. Hence it is especially important for negative fingerprint recognition systems to detect small quality fingerprints and increase their quality so that the fingerprint system is not compromised by malicious persons. Degradation of finger-print quality can be photometric or geometrical. Photometric degradation can be effected by non-ideal skin conditions, dirty sensor surface, and complex image background (in latent fingerprints). Geometrical degradation is mainly caused by skin distortion. On the contrary, geometrical degradation due to skin distortion has not yet received sufficient attention, despite of the importance of this problem. This is the problem this paper attempts to address. Note that, for a negative fingerprint recognition system, its security level is as low as the lowest point. Thus it is urgent to develop distorted fingerprint (DF) detection and rectification algorithms to fill the hole. Elastic distortion is introduced due to the inherent flexibility of fingertips, contact-based fingerprint acquisition procedure, and a purposely lateral force or torque, etc. Skin distortion increased the intra-class variations (difference among fingerprints from the same finger) and thus leads to false unmatched due to limited capability of existing fingerprint matchers in recognizing severely distorted finger-prints.
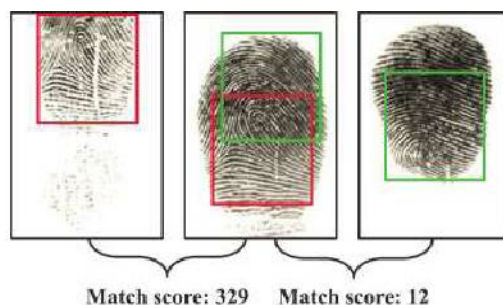

Match score: 329   Match score: 12
Fig. 1.Three impressions of the same finger.

The left two are normal fingerprints, while the right one contains severe distortion. The match score in-between the left two according to VeriFinger 6.2 SDK is much higher than the match score in-between the right two. This large difference is due to distortion rather than overlapping area. As displayed by red and green rectangles, the overlapping area is same in two cases. In Fig. 1, the left two are normal fingerprints, while right figure contains maximum distortion. According toVeri-Finger 6.2 SDK, the match score in-between the left two is much higher than the match score between the righttwo. This large difference is due to distortion rather thanover-lapping area. While it is possible to make the matchingalgorithms tolerate huge skin distortion, this will lead tomore false matches and slow down matching speed. Providing aninput finger-print, distortion detection of fingerprint isperformed first. If it is determined to be distorted, distortionrectification is performed to convert the provided input fingerprint into normal fingerprints. A distorted fingerprint is analogous to a face with expression, which alter thematching efficiency of face recognition systems. Rectifying a distorted fingerprint into a normal fingerprint is analogous to converting a face with expression into a neutral face, which can improve face recognition performance.
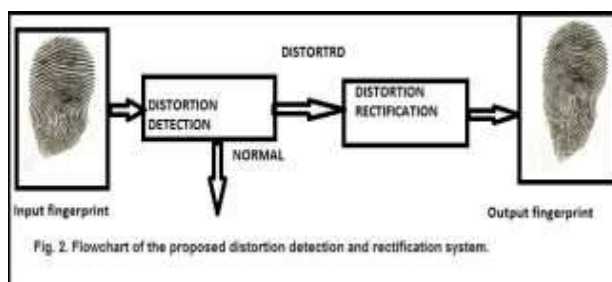

Fig. 2. Flowchart of the proposed distortion detection and rectification system.

Fig. 1.Flow of the System.

International Journal of Innovative Research in Computer and Communication Engineering

II.   RELATED WORK

Due to the major importance of recognizing distorted fingerprints, the various proposed method can be classified into four categories

2.1 Distortion-Tolerant Matching:

The most suitable way to handle distortion is to make the matcher tolerant to distortion. [8]– [10].In another words, they deal with distortion for each pair of fingerprints to be compared. For example, the following three types of strategies to handle distortion: (i) Assume a global rigid transformation and use a tolerant box of fixed size to compensate for distortion[8]; (ii) explicitly model the spatial transformation [9] by Thin-Plate Spline model; and (iii) only enforce constraint on distortion locally [10]. However, allowing huge distortion in matching will inevitably outcomes in higher false match rate. For example, if we enhanced the bounding zone around a minutia, many no matched minutiae will have a chance to get paired.

2.2 Fingerprint Adjustment

Senior and Bolleconcern with distortion by normalizing ridge density in the whole fingerprint to a fixed value [11]. They showed this can boost genuine match scores. However, ridge density is known to contain discriminating information and numbers of researchers have reported to boost matching accuracy due to incorporating ridge density [12], [13] in information into minutiae matchers. Simply unifying ridge density of all fingerprints will lose discriminating information in fingerprints and may increase false match rate. Ross et al learn the deformation pattern from a set of training images of the same finger and transform the template with the least deformation using the moderate deformation with other images. They show this leads to larger than minutiae matching accuracy. But this method has the following constrains: (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, a malicious user can still adopt unusual distortion, which is not reflected in the training data, to cheat the matcher.

2.3 Distortion Detection Based on Special Hardware

It is necessary to automatically detect distortion during Fingerprint acquisition so that extremely distorted fingerprints can be rejected. Many researchers have recommended detecting improper force using specially designed hardware [14], [15], [16]. Bolle et al. [14]
Proposed to detect excessive force and torque exerted by using a force sensor. They display that controlled fingerprint acquisition leads to enhanced matching performance [15]. Fuji proposed to detect distortion by detecting deformation of a transparent film [16] attached to the sensor surface. Doraiet al. [17] planned to detect distortion by analyzing the change in video of fingerprint. However, the above methods have the following restrictions :(i) they need to special force sensors or fingerprint sensors with attached the video capturing capability; (ii) they cannot detect distorted fingerprint images in original existing fingerprint databases; and (iii) they cannot detect fingerprints distorted before pressing on the sensor.

2.4 Distortion Rectification Based on Finger-Specific
Statistics

Ross et al. [17] learn the deformation pattern from collections of training images of the same finger and transform the template with the moderate deformation. They show this leads to huge minutiae matching accuracy. But this method has the following restrictions: (i) to taking the 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.

III.   PROPOSED SYSTEM MECHANISM

In Proposed System was evaluated at two levels of plane: finger level and subject level. At the finger level, we estimate the performance of differentiating between natural and changed fingerprints. At the subject level, we estimate the performance of differentiating between subjects with natural fingerprints and those with changed fingerprints. The

International Journal of Innovative Research in Computer and Communication Engineering

proposed algorithm is based on the characteristics extracted from the orientation field and minutiae perform or satisfy the three required requirements for alteration detection algorithm: 1) speedy operational time, 2) Huge true positive rate at small false positive rate, and 3) Ease of integration into AFIS.

IV.   METHODOLOGY

4.1 Detection of Altered Fingerprints
4.1.1 Normalization:-
An input fingerprint image which is provided is normalized by cropping or cutting a rectangular region of the input image fingerprint, which is located at the center of the fingerprint and aligned along with the longitudinal direction of the fingerprints, using the NIST Biometric Image Software (NBIS). This step insures that the features extracted in the subsequent steps are invariant with respect to translation and rotation of finger.
4.1.2 Orientation Field Estimation
The orientation field of the fingerprint is estimated using the gradient-based method. The starting orientation field is smoothed moderating filter, followed by moderating the orientations in pixel blocks. A foreground mask is earn 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**.**

4.1.3 Orientation Field Approximation
The orientation field is near by a polynomial model to obtain.
4.1.4 Feature Extraction
The error map is counted as the absolute difference in-between and used to construct the feature vector.
4.2 Analysis of Minutiae Distribution:
In this methodology, a minutia in the fingerprint implies the ridge characteristics such as ridge ending or ridge bifurcation. Almost all the fingerprint recognition systems usage minutiae for matching. The abnormality observed in orientation field also noted that minutiae distribution of altered fingerprints often differs from that of natural fingerprints. On the basis of minutiae extracted from a fingerprint by the open source minutiae extractor in NBIS, a minutiae density map is composed by using the Parzen window method containing uniform kernel function.

V.   METHODS WE USED

Algorithm
1.   Support Vector Machines (SVM)
An SVM classifies data by finding the best hyperplane that separates all data points of one class from those of the other class. The best hyperplane for an SVM means the one with the largest margin between the two classes. Margin means the maximal width of the slab parallel to the hyperplane that has no interior data points.
The support vectors are the data points that are closest to the separating hyperplane; these points are on the boundary of the slab. The following figure illustrates these definitions, with + indicating data points of type 1, and – indicating data points of type –1.

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

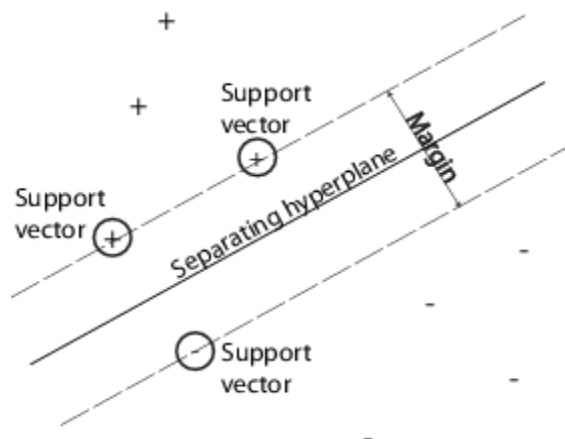**Vol. 4, Issue 2, February 2016**

Fig 15. Support Vector Machine

The advantages of support vector machines are:
- Effective in high dimensional spaces.
- Still effective in cases where number of dimensions is greater than the number of samples.
- Uses a subset of training points in the decision function (called support vectors), so it is also memory efficient.
- Versatile: different Kernel functions can be specified for the decision function. Common kernels are provided, but it is also possible to specify custom kernels.

Support vector machines (SVMs) are a set of supervised learning methods used for classification, regression and outlier's detection.

The advantages of support vector machines are:
- Effective in high dimensional spaces.
- Still effective in cases where number of dimensions is greater than the number of samples.
- Uses a subset of training points in the decision function (called support vectors), so it is also memory efficient.
- Versatile: different Kernel functions can be specified for the decision function. Common kernels are provided, but it is also possible to specify custom kernels.

The disadvantages of support vector machines include:
- If the number of features is much greater than the number of samples, the method is likely to give poor performances.
- SVMs do not directly provide probability estimates, these are calculated using an expensive five-fold cross-validation (see Scores and probabilities, below).
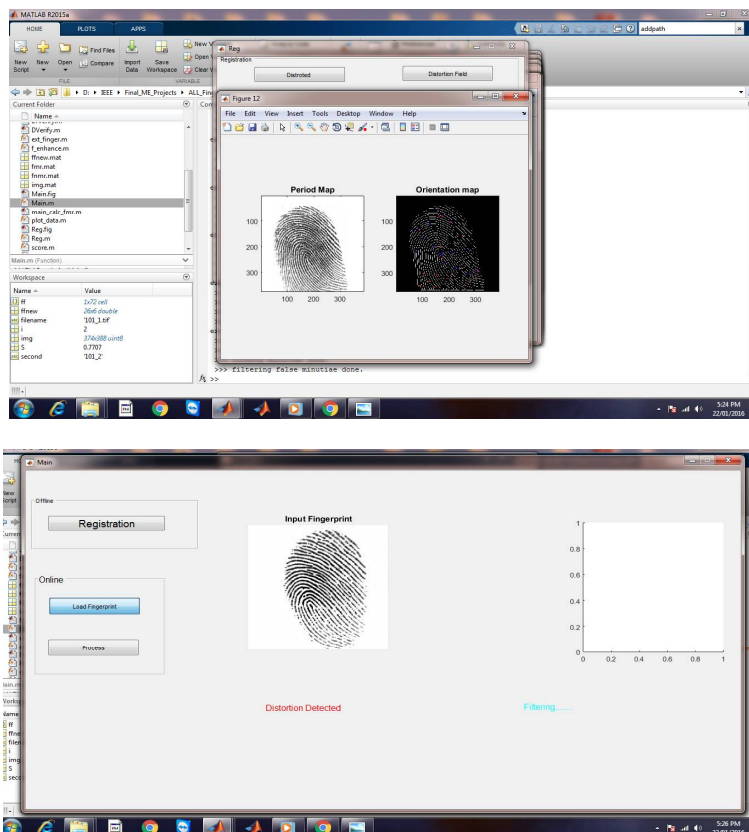
VI.   RESULT
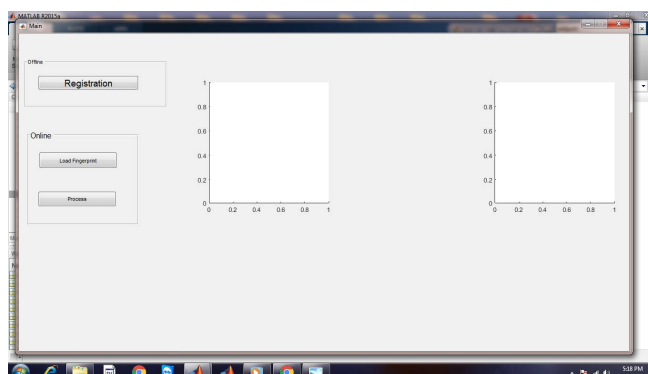
International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 2, February 2016

VII.   CONCLUSION

Wrong non-match rates of fingerprint matchers are very huge in the case of critically distorted fingerprints. This creates a security hole in automatic recognition of fingerprint systems which can be utilized by criminals and terrorists. For this reasoning, it is required to develop a fingerprint distortion detection and rectification algorithm, to fill the hole. The distorted fingerprint detection and rectification paper described a novel distorted fingerprint detection and rectification algorithm. For distortion detection, the ridge orientation map and period map of a fingerprint are needed as the feature vector and a SVM classifier is skilled to categorize the input fingerprint as distorted or normal. (Not distorted). For distortion rectification a close neighbor regression approach is used to conclude the distortion field from the provided input distorted fingerprint and then the converse of the distortion field is used to convert the distorted fingerprint into a normal one (un-distorted). The experimental results on FVC2004 DB1, Tsinghua DF database, and NIST SD27 database displayed that the scheduled algorithm can increase the recognition rate of distorted fingerprints manifestly. The proposed algorithm based on the features derived from the orientation field and minutiae amuse the three necessary requirements for change detection algorithm:

REFERENCES

[1] B. Sotomayor, R. S. Montero, I. M. Llorente, and I. T. Foster, Virtual infrastructure management in private and hybrid clouds," IEEE Internet Computing, vol. 13, no. 5, pp. 14–22, 2009.
[2] D. Maltoni, D. Maio, A. K. Jain, and S. Prabhakar, Handbook of Fingerprint Recognition, 2nd ed. Berlin, Germany: Springer-Verlag, 2009.
[3] A. Juels and B. S. K. Jr., "Pors: proofs of retrievability forlarge files," in ACM Conference on Computer and Communications Security, P. Ning, S. D. C. di Vimercati, and P. F. Syverson, Eds. ACM, 2007, pp. 584–597.
[4] G. Ateniese, R. D. Pietro, L. V. Mancini, and G. Tsudik, "Scalable and efficient provable data possession," in Proceedings of the 4th international conference on Security and privacy in communication netowrks, SecureComm, 2008, pp. 1–10.

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 2, February 2016

[5] C. C. Erway, A. Küpç¸ü, C. Papamanthou, and R. Tamassia, "Dynamic provable data possession," in ACM Conference on Computer and Communications Security, E. Al-Shaer, S. Jha, and A. D. Keromytis, Eds. ACM, 2009, pp. 213–222.

[6] H. Shacham and B. Waters, "Compact proofs of retrievability," in ASIACRYPT, ser. Lecture Notes in Computer Science,J. Pieprzyk, Ed., vol. 5350. Springer, 2008, pp. 90–107.

[7] Q. Wang, C.Wang, J. Li, K. Ren, and W. Lou, "Enabling public verifiability and data dynamics for storage security in cloud computing," in ESORICS, ser. Lecture Notes in Computer Science, M. Backes and P. Ning, Eds., vol. 5789. Springer, 2009, pp. 355–370.

[8] N. K. Ratha, K. Karu, S. Chen, and A. K. Jain, "A Real- Time Matching System for Large Fingerprint Databases," IEEE TPAMI, vol. 18, no. 8, pp. 799–813, 1996.

[9] A. M. Bazen and S. H. Gerez, "Fingerprint Matching by Thin-Plate Spline Modelling of Elastic Deformations," Pattern Recognition, vol. 36, no. 8, pp. 1859–1867, 2003.

[10] Z. M. Kovacs-Vajna, "A Fingerprint Verification System Based on Triangular Matching and Dynamic Time Warping," IEEE TPAMI, vol. 22, no. 11, pp. 1266–1276, 2000.

[11] A. Senior and R. Bolle, "Improved Fingerprint Matching by Distortion Removal," IEICE Trans. Information and System, vol. 84, no. 7, pp. 825–831, July 2001.

[12] D. Wan and J. Zhou, "Fingerprint Recognition Using Model-based Density Map," IEEE TIP, vol. 15, no. 6, pp. 1690–1696, 2006.

[13] J. Feng, "Combining Minutiae Descriptors for Fingerprint Matching," Pattern Recognition, vol. 41, no. 1, pp. 342–352, 2008. [14] A. Ross, S. C. Dass, and A. K. Jain, "Fingerprint Warping Using Ridge Curve Correspondences," IEEE TPAMI, vol. 28, no. 1, pp. 19– 30, 2006.

[14] R. M. Bolle, R. S. Germain, R. L. Garwin, J. L. Levine, S. U. Pankanti,N. K. Ratha, and M. A. Schappert, "System and method for Distortion control in live-scan inkless fingerprint images," U.S.Patent No. 6 064 753, May 16, 2000.

[15] N. Ratha and R. Bolle, "Effect of controlled image acquisition on Fingerprint matching," in Int. Conf. Pattern Recognit., 1998, vol. 2,pp. 1659–1661.

[16] Y. Fujii, "Detection of fingerprint distortion by deformation of elastic film or displacement of transparent board," U.S. Patent No. 7 660 447, Feb. 9, 2010.

[17] A. Ross, S. C. Dass, and A. K. Jain, "A deformable model for fingerprint matching," Pattern Recognition., vol. 38, no. 1, pp. 95–03, 2005