International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

Distortion Detection and Rectification in Fingerprint Based Security Systems

*V.SRAVANI **N.PRASAD

*M.TECH student, Dept of CSE, VAAGDEVI COLLEGE OF ENGINEERING
**Associate Professor, Dept of CSE, VAAGDEVI COLLEGE OF ENGINEERING

Abstract- Elastic distortion of fingerprints is the chief causes for fake mismatch. As this reason disturbs all fingerprint detection applications, it is particularly risk in negative identification applications, such as watch list and deduplication applications. In such applications, cruel persons may deliberately distort their fingerprints to hide recognition. In this paper, we recommended novel algorithms to identify and correct skin distortion based on a single fingerprint image. Distortion detection is demonstrated as a two-class classification problem, for which the registered ridge orientation map and period map of a fingerprint are helpful as the feature vector and a SVM classifier is educated to act the classification task. Distortion rectification (or equivalently distortion field estimation) is analyzed as a regression difficulty, where the input is a distorted fingerprint and the output is the distortion field. To simplify this problem, a database (called reference database) of various distorted reference fingerprints and matching distortion fields is built in the offline stage, and then in the online stage, the closest neighbor of the input fingerprint is planned in the reference database and the equivalent distortion field is used to change (Convert) the input fingerprint into a normal fingerprints. Capable results have been achieved on three databases having many distorted fingerprints, namely NIST SD27 latent fingerprint database, Tsinghua Distorted Fingerprint database, FVC2004 DB1,

Key words— Elastic distortion of fingerprints, SVM classifier, and Distortion detection

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

1. INTRODUCTION

Even though automatic fingerprint recognition technologies have quickly advanced during the last forty years, presently survive many demanding research problems, for example, identifying 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 differs significantly among different data-sets due to difference in image quality. The difference between the accuracies of plain, rolled and hidden fingerprint matching is even superior as found in technology assessment conducted by the NIST.The result of low quality fingerprints depends on the type of the fingerprint recognition system. A fingerprint recognition system can be classified as either a positive or negative system. If we observe in a positive recognition system, such as physical access control systems, the end-user is supposed to be cooperative recognition and desires to be recognized. When we have a look in a negative system, such as identifying persons in watch lists and discovering multiple enrollments under different names, the user of concern (e.g., thieves) is supposed to be unhelpful and does not want to be recognized. In a positive recognition system, low quality will points to false reject of justifiable persons and thus bring difficulty. The result of low quality for a negative recognition system, yet, is more serious, since cruel users may intentionally reduce fingerprint quality to stop fingerprint system from discovering the true identity. Hence it is especially important for negative fingerprint recognition systems to identify small quality fingerprints and raise their superiority so that the fingerprint system is not negotiated by cruel persons. Degradation of finger-print quality can be photometric or geometrical. Photometric degradation can be resulted by non-ideal skin circumstances, dirty sensor surface, and complex image background (in latent fingerprints). Geometrical degradation is primarily caused by skin distortion. On the converse, geometrical degradation due to skin distortion has not so far received sufficient notice, although of the importance of this problem. This is the problem this paper challenges to address. In Fig. 1. We are showing an example three impressions of the same finger. The left two are normal

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

fingerprints, whereas the right one includes severe distortion. The match score among the left two according to VeriFinger 6.2 SDK is much advanced than the match score among the right two. This huge dissimilarity is due to distortion slightly than overlapping area. Since demonstrated by red and green rectangles, the overlapping area is same in two

Situations.If we observe carefully in Fig. 1, the left two are normal fingerprints, while right figure contains greatest distortion. According to Veri-Finger 6.2 SDK, the match score in-between the left two is much superior than the match score between the right two. Hence the large contrast is due to distortion moderately than over-lapping area. Whereas it is likely to make the matching algorithms bear huge skin distortion, this will direct to more false matches and slow down matching speed.

In The Fig.2 we are demonstrating the flowchart of the proposed system. Given that an input finger-print, distortion detection of fingerprint is achieved first. If it is determined to be distorted, distortion rectification is carrying out to translate the supply input fingerprint into normal fingerprints. A distorted fingerprint is similar to a face with expression, which change the matching competence of face recognition systems. Resolving a distorted fingerprint into a normal fingerprint is similar to converting a face with expression into a impartial face, which can progress face recognition presentation

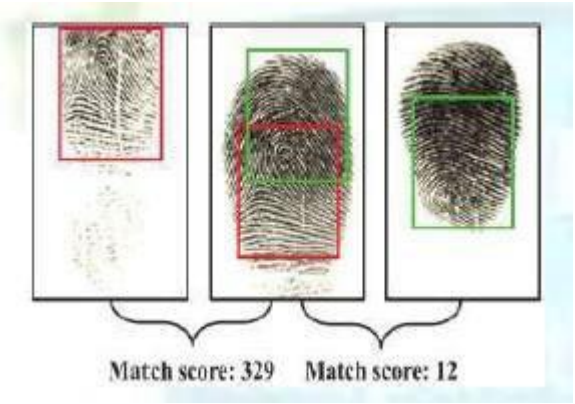

Fig 1: Three impressions of the same finger

2. RELATED WORK: Due to the main significance of recognizing distorted fingerprints, a variety of proposed method can be divided into four groups. **Distortion-Tolerant Matching:**

1. The major suitable way to hold distortion is to make the matcher to understand the distortion. [8]– [10]. On the other hand, they deal with

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

2. Fig2: Flow chart of the proposed distortion detection and rectification system

3. Distortion for each pair of fingerprints to be measured. For example, the subsequent three groups of approaches to hold distortion:

4. Imagine a universal inflexible transformation and utilize a tolerant box of fixed size to recompense for distortion[8];

5. Openly using the spatial transformation [9] by Thin-Plate Spline model; and

6. Only impose limitation on distortion locally [10].

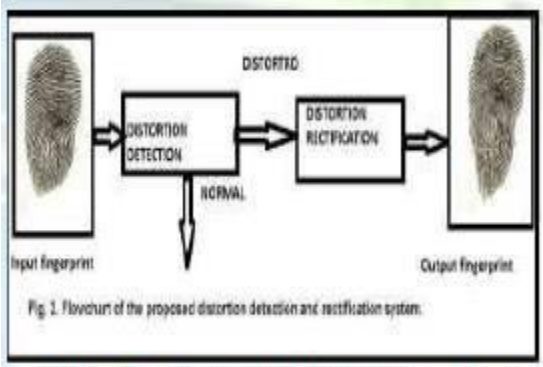

Fig 1. Flowchart of the proposed distortion detection and rectification system.

On the other hand, permitting enormous distortion details will have a possibility to acquire paired.

2.1 Fingerprint Adjustment

Senior and Bolleconcern explained the distortion by standardizing ridge thickness in the whole fingerprint to a fixed value [11]. They illustrated this by boost real match scores. On the other hand, ridge thickness is known to include discriminating data and many researchers have reported to boost matching accuracy due to incorporating ridge density [12], [13] in information into detailed matchers. Just combining ridge density of all fingerprints will drop discriminating information in fingerprints and may raise false match rate. Ross et al discovered the deformation pattern from a set of training images of the same finger and alter the template with the least deformation via the moderate deformation with other images. They prove this leads to larger than detailed matching correctness. But this technique has the following limitations:

(i) Obtaining multiple images of the same finger is difficult in some applications and existing fingerprint databases usually hold only one image per finger; and

(ii) yet if multiple images per finger are obtainable, a cruel user can still adopt unusual distortion, which is not reflected in the training data, to deceive the matcher.

2.2 Distortion Detection Based on Special Hardware It is essential to routinely detect distortion through Fingerprint attainment so that tremendously distorted fingerprints can be discarded. Various researchers have suggested identifying improper force by means of particularly planned hardware [14], [15], [16]. Bolle et al. [14] projected to detect extreme force and torque exerted by using a force sensor. They exhibit that restricted fingerprint attainment guides to improved matching presentation [15]. Fujii projected to detect distortion by detecting deformation of a crystal clear film [16] attached to the sensor surface. Doraiet al. [17] designed to identify distortion by examining the alter in video of fingerprint. On the other hand, the above techniques have the subsequent boundaries: They require to extraordinary force sensors or fingerprint sensors with attached video capturing ability; (ii)They cannot identify distorted fingerprint images in original existing fingerprint databases; and (iii) They cannot discover fingerprints distorted before pressing on the sensor.

2.3 Distortion Rectification Based on Finger-Specific Statistics Ross et al. [17] studied the deformation pattern from gathering of training images of the same finger and transform the template with the modest deformation. They illustrated this leads to enormous details of matching correctness. But this technique has the following limitations: (i) By considering the multiple images of the same finger it is not convenient in some applications and existing fingerprint databases usually hold only one image per finger; and Still if multiple images per finger are obtainable, it is not essentially sufficient to cover a variety of skin distortions.

3. PROPOSED APPROACH:

The Proposed scheme was estimated at two levels of plane: finger level and subject level. At the finger level, we analyze the performance of distinguishing between natural and changed fingerprints. At the subject level, we guess the performance of discrimination between subjects with natural fingerprints and those with altered fingerprints. The proposed algorithm is based on the uniqueness take out from the

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

orientation field and details to perform or satisfy the three required necessities for modification detection algorithm: 1) speedy operational time, 2) Huge true positive rate at small false positive rate, and 3) Ease of integration into AFIS.

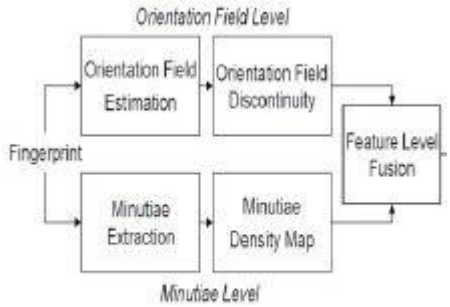

Fig 3.System Architecture

4. METHODOLOGY:

4.1 Detection of Altered Fingerprints

4.1.1 Normalization:- An input fingerprint image which is supplied is normalized by cutting a rectangular region of the input image fingerprint, which is situated at the center of the fingerprint and associated along with the longitudinal direction of the fingerprints, using the NIST Biometric Image Software (NBIS). This step assures that the features take out in the following steps are invariant with respect to conversion and rotation of finger.

4.1.2 Orientation Field Estimation The orientation field of the fingerprint is analyzed using the gradient-based method. The starting orientation field is smoothed moderating filter, pursue by modest the orientations in pixel blocks. A foreground mask is produced by measuring the dynamic range of gray values of the fingerprint image in local blocks and morphological method for filling holes and eliminating isolated blocks is achieved.

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 calculated as the absolute difference between and used to build the feature vector.

4.2 Analysis of Minutiae Distribution: In this method, a minutia in the fingerprint involves the ridge personality such as ridge ending or ridge junction. Almost all the fingerprint detection systems use minutiae for matching. The irregularity observed in orientation field also celebrated that minutiae distribution of altered fingerprints frequently change from that of natural fingerprints. On the beginning of minutiae

take out from a fingerprint by the open source minutiae extractor in NBIS, a minutiae thickness map is collected by using the Parzen window method including uniform kernel function.

5. CONCLUSION

Incorrect mismatch rates of fingerprint matchers are very enormous in the case of seriously distorted fingerprints. This produces a safety whole in routine recognition of fingerprint systems which can be make use of by thieves and terrorists. For this logic, it is necessary to expand a fingerprint distortion detection and rectification algorithm, to fill the hole. In this distorted fingerprint detection and rectification paper we described a novel distorted fingerprint detection and rectification algorithm. For distortion detection, the edge orientation map and period map of a fingerprint are desirable as the feature vector and a SVM classifier is skilled to classify the input fingerprint as distorted or normal. (Not distorted). For distortion rectification a close neighbor regression method is used to terminate the distortion field from the supply input distorted fingerprint and then the reverse of the distortion field is used to translate the distorted fingerprint into a normal one (un-distorted). The experimental results on FVC2004 DB1, Tsinghua DF database, and NIST SD27 database shows that the scheduled algorithm can increase the recognition rate of distorted fingerprints noticeably. The proposed algorithm based on the features derived from the orientation field and minutiae amuse the three essential necessities for change detection algorithm: A major limitation of the current approach is competence. Both i.e. detection and rectification steps can be considerably speed up if a rough and properly fingerprint register algorithm can be created. Another limitation is that the current approach is not supported rolled fingerprints. It is vital to collect many rolled fingerprints with numerous distortion categories and for the time being to get exact distortion fields for learning statistical distortion model.

6. REFERENCES

[1]Prof. Bere S.S. and Mr. Ganesh V. Kakade, “Identify and Rectify the Distorted Fingerprints”, International Journal on Recent and Innovation Trends in Computing and Communication” Volume: 3 Issue: 12.

[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 ACMConference 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.

[5] C. C. Erway, A. K¨upc¸ ¨u, 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. Jain, "Fingerprint Warping Using Ridge Curve Correspondences," IEEE TPAMI, vol. 28, no. 1, pp. 19– 30, 2006