

Review on Detection and Rectification of Distorted Fingerprint

Jinsha KS¹,Jeno Paul P²

¹ PG Student, CSE Dept, ASIET, Kalady, Kerala, India.

² Professor, EEE Dept, ASIET, Kalady, Kerala, India.

Abstract: False non-match is mostly caused by elastic distortion of fingerprints. Even though this issue affects all fingerprint recognition applications, watch list and duplicate applications are particularly vulnerable to it. Malicious users in these programs might intentionally alter their fingerprints in order to avoid detection. In this work, we presented new algorithms that use only one fingerprint image to identify and correct skin deformation. A SVM classifier is trained to handle the classification task, and distortion detection is seen as a two- class classification problem for which the registered ridge orientation map and period map of a fingerprint are employed as a feature vector. A distorted fingerprint is the input for distortion rectification (or equivalently, distortion field estimation), and the distortion field is the output. This can be thought of as a regression problem. The online stage finds the nearest neighbor of the input fingerprint in the reference database and uses the corresponding distortion field to change the input fingerprint into a normal one. This process is done on order to solve the problem, which involves building a database (referred to as the reference database) of various distorted reference fingerprints and corresponding distortion field in the offline stage.

Keywords: Elastic distortion, Rectification, SVM classifier.

I. INTRODUCTION

Over the past forty years, automatic fingerprint identification technologies have improved quickly, but there are still a number of difficult research difficulties to be solved. For instance, identifying poor- quality fingerprints.

The FVC2006 study shows that fingerprint matchers are highly sensitive to image quality, with matching of the same algorithm changing dramatically between datasets as a result of image quality variations. Based on NIST technology evaluations, there is an even greater discrepancy between plain, rolled, and latent fingerprint matching accuracy.

The impact of fingerprints with poor quality varies depending on the kind of fingerprint recognition technology. There are two types of fingerprint identification systems: positive systems and negative systems. The user is expected to cooperate and want to be identified in a positive recognition system such as physical access control systems. The user of interest (criminals, for example) in a negative recognition system is expected to be uncooperative and not want to be identified. Examples of this include recognizing individuals on watch lists and identifying numerous enrolment under different identities. In a positive recognition system, poor quality will cause erroneous rejections of valid users, causing discomfort. Malicious users may intentionally lower fingerprint quality in order to hinder the fingerprint system from determining the genuine identity, which makes the consequences of low quality for a negative recognition system even more severe. To prevent fraudulent users from jeopardizing the fingerprint system, it is crucial for negative fingerprint recognition systems to identify and enhance low-quality fingerprints.

II. BASIC CONCEPTS

The natural flexibility of fingertips, contact- based fingerprint capture techniques, intentional lateral force or torque, etc., all contribute to the introduction of elastic distortion. Because skin distortion makes it more difficult for existing fingerprint matchers to recognize highly distorted fingerprints, it increases intra-class variances (differences among fingerprints from the same finger) and causes misleading non-matches.

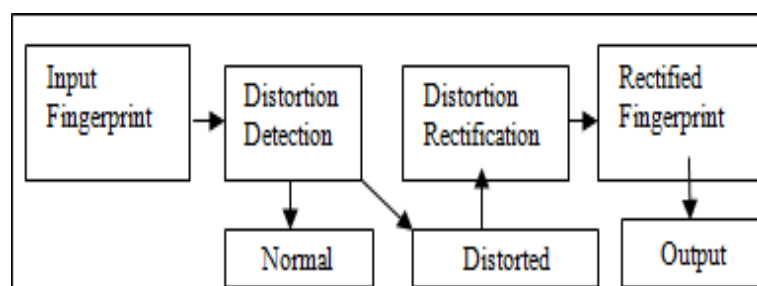


Fig 1: Basic concept

The flowchart for the suggested system is displayed in Figure1. A two-class SVM Classifier (Registered ridge orientation map and period map are used as feature vectors) is used to detect distortion when a fingerprint is given as input. If a distorted fingerprint is discovered, distortion rectification is used to make the damaged fingerprint appear normal. Regression analysis is used to analyze distortion field estimation. This will have a distorted fingerprint as the input and a similar distortion field as the output. In order to overcome this, an offline stage database is constructed that contains a variety of distorted fingerprints and the distortion fields that correlate to them. The virtual platform in order to correlate the input fingerprint, the nearest neighbor is located in the database of distorted reference fingerprints, and the matching distortion filed is utilized.

1. Distortion Detection Based on Special Hardware

For the purpose of rejecting significantly distorted fingerprints, it is desirable to automatically detect distortion during fingerprint acquisition. A number of researchers have suggested utilizing specifically made hardware to identify incorrect force. The use of a force sensor was suggested by Bolle et al. to identify excessive force and torque. Controlled fingerprint acquisition improves matching performance, as they demonstrated.

By monitoring the deformation of a transparent film affixed to the sensor surface, Fujii suggested detecting distortion. Dorai et al. suggested examining the mobility of a fingerprint in a video to identify distortion. These approaches have the following drawbacks: (i) they need specialized force sensors or fingerprint sensors that can record video. (ii) they cannot identify distorted fingerprint images in database that already exist; and (iii) they cannot identify distorted fingerprints that were applied prior to pressing on the sensor.

2. Distortion-Tolerant Matching

To deal with distortion, the most common approach is to make the fingerprint matcher distortion tolerant. Put differently, each pair of fingerprints is compared, thus they address distortion on an individual basis. Three different sorts of techniques have been developed to mitigate distortion for the most popular minutiae-based fingerprint matching method: To account for distortion, one can (i) assume a global rigid transformation and employ a tolerant box of constant size [20] or adaptive size; (ii) explicitly represent the spatial transformation using a thin plate spline (TPS) model; and (iii) impose local constraints on distortion. In image-based matchers or skeleton-based matchers, other techniques have also been employed to manage distortion during matching. But a higher false match rate is an inevitable consequence of allowing more distortion in matching. An increase in the bounding zone surrounding a minutia, for instance, increases the likelihood that several non-mated minutiae will be coupled. The pace of matching will likewise decrease if greater distortion is allowed.

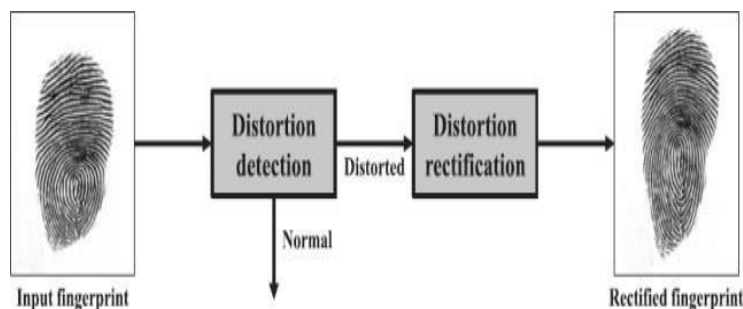


Fig 2: Distortion tolerance matching

3. Distortion Rectification Based on Finger-Specific Statistics

Applying a number of training images of the same finger, Ross et al. identify the deformation pattern and apply the averaged deformation to the template. They demonstrate that this increases the accuracy of minutiae matching. But the following are the approaches limitations: Existing fingerprint databases often only have one image per finger, thus (i) getting multiple pictures of the same finger can be complicated in some circumstances; (ii) even with many images per finger, they might not be sufficient to cover different skin defects.

4. Distortion Rectification Based on General Statistics

An interesting method to remove distortion before to the matching stage was created by Senior and Bolle. This technique is predicated on the idea that a fingerprint's ridges are consistently spaced apart. In order to prevent distortion, they equalize the ridge density throughout the fingerprint to a set value. They use the distortion rectification method to each fingerprint since they lacked a distortion detecting algorithm.

The Senior and Bolle technique has the following advantages over the other methods mentioned above: It can process a single input fingerprint image; (ii) it does not require trained hardware; and (iii) it doesn't need a set of training images of the same finger. Ridge density, however, is neither constant within a finger nor constant among fingers. In fact, adding ridge density data to minutiae matchers has been demonstrated by multiple researchers to improve matching accuracy. All fingerprints will lose their ability to differentiate one another if the ridge density is simply normalized, while this might boost impostor match scores. Furthermore, this method could yield fingerprints with a fixed ridge period but an odd orientation map if there are no restrictions on the validity of the orientation map. The second restriction is considerably more damaging than the first since it lowers actual match scores. Since finger rotation was not taken into account and the algorithm was assessed only on a small database of six fingers, these drawbacks were not identified.

Our method shares the advantages of Senior and Bolle method over other methods, while addressing some of its limitations.

Rather than depending on the unrealistic assumption of a constant ridge period, our approach is based on statistics extracted from real distorted fingerprint data. Our approach can handle distortion caused by rotation of the fingers. Indeed, the suggested approach may effectively handle diverse forms of distortion, providing that the particular distortion type is present in the training dataset. Furthermore, an extensive amount of testing has been performed to confirm the suggested strategy.

5. Fingerprint Distortion Detection

It would be feasible to think of fingerprint distortion detection as a two-class classification problem. The registered ridge orientation map and period map, which are identified utilizing an SVM classifier, served as the feature vector. Fig. 3 shows the distortion detection flowchart.

The force or torque directions are indicated by the blue arrows, and the distortion grids, which are calculated by matching minute details between the normal and distorted fingerprints, are shown by the red grids.

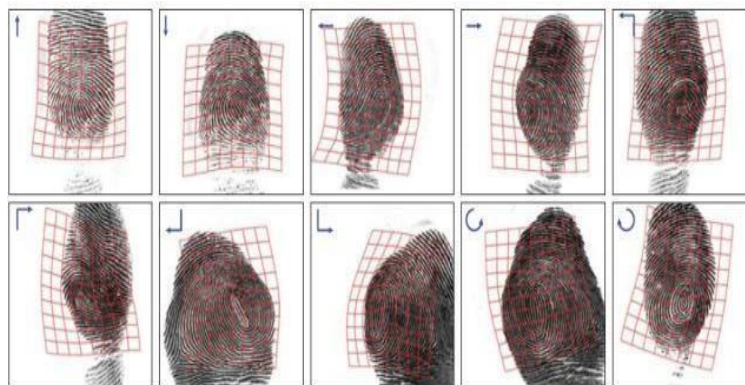


Fig 3: Fingerprint distortion detection

6. Feature Vector Extraction

By sampling the registered orientation map and period map, we are able to extract a feature vector. In Fig. 3, the sample grid is shown along with the finger center. Keep in mind that the two sampling grids are not the same. While the orientation map's sample grid only covers the fingerprint's upper region, the period map's sampling grid includes the entire fingerprint. This is because of the reality that, even in typical fingerprints, the orientation maps below the finger center are extremely different. Thus, they are not helpful in order to differentiate between distorted and normal fingerprints.

7. Classification

Training samples are derived from the reference fingerprints. It is believed that distorted fingerprints are positive samples and that regular fingerprints are negative samples. A quadratic polynomial kernel Support Vector Classifier was trained using LibSVM. In LibSVM, all parameters are utilized as defaults. To be more precise, the SVM type is C-SVC, the kernel function's coef0 value is 0, and the kernel function's g value is $1/L$, where L is the feature vector's length.

8. Distorted Fingerprint Rectification

One way to conceptualize a distorted fingerprint is as an unknown distortion field d applied on an unknown normal fingerprint. The distorted fingerprint can be readily rectified into the normal fingerprint by applying the inverse of d , provided we are able to estimate the distortion field d from the given deformed fingerprint. Thus, even with a block-wise distortion field, we still have to deal with the challenging regression problem caused by the large dimensionality of the distortion field. The closest neighbor regression method is applied to this job in this research.

An offline stage and an online stage make up the suggested distorted fingerprint rectification algorithm. Several normal reference fingerprints are transformed with different distortion fields sampled from the statistical model of distortion fields in order to create a database of distorted reference fingerprints in the offline stage. When a distorted input fingerprint is presented online, we first locate its closest neighbor in the distorted reference fingerprint database. Next, we use the inverse of the matching distortion field to correct the distorted input fingerprint.

9. Statistical Modelling of Distortion Fields

To acquire knowledge of the statistical fingerprint distortion model, we must be aware of the distortion fields, also called deformation fields, that exist between paired fingerprints in the training set, which are the first and last frames of each film. Based on the matching details of the two fingerprints, the distortion field between them can be approximated. Unfortunately, existing minutiae matchers are unable to reliably detect corresponding minutiae because of the high distortion between paired fingerprints.

Thus, we do minutiae tracking in each movie and use VeriFinger to extract minutiae in the first frame. Reliable minutiae correspondences between the first and last frames can be found using this method because of the little relative motion between neighboring frames.

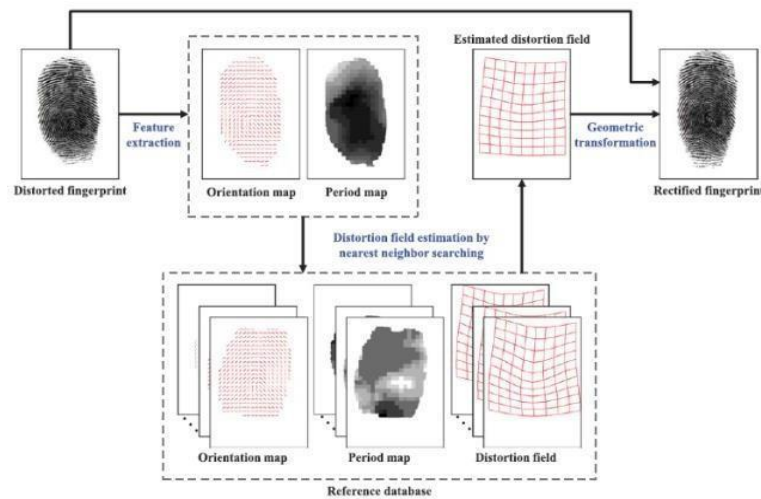


Fig 4: Statistical Modelling of Distortion Fields

10. Generation of Distorted Reference Fingerprint Database

The first two main components span a subspace, which is evenly sampled to create the distortion fields. Eleven points in the interval $[-2, 2]$ are consistently sampled for every basis. To improve performance, numerous reference fingerprints are employed in practice. Moreover, take note that we save each fingerprint's ridge orientation map and period map in the reference database rather than the fingerprint picture.

III. SYSTEM ANALYSIS

The suggested distortion detection algorithm is initially assessed in this section. Next, we conduct matching experiments on three databases to assess the suggested distortion rectification algorithm. The effect of the quantity of reference fingerprints on distorted fingerprint rectification is finally covered.

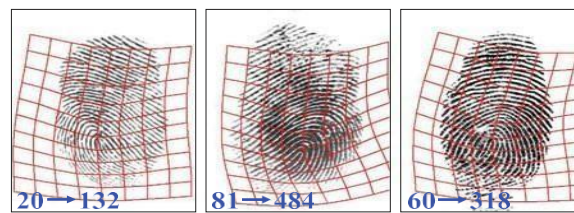


Fig 5: Three distorted examples

We consider distortion detection to be a problem of two-class classification. It is believed that distorted fingerprints are positive samples and that regular fingerprints are negative samples. A real positive happens when a fingerprint that has been altered is identified as positive. The occurrence of a false positive is when a typical fingerprint is identified as positive. The receiver operating characteristic (ROC) curve can be obtained by varying the decision threshold.

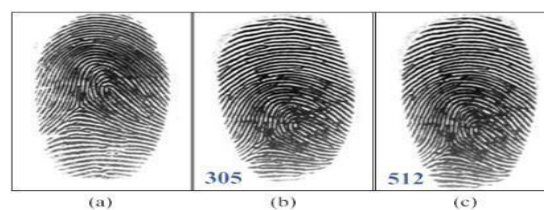


Fig 6: An example of false negative due to slight distortion



Fig 7: An example of false positive due to low quality and small area

Visual analysis of the photos reveals that FVC2004 DB1 has 89 warped fingerprints in addition to 791 regular fingerprints. This figure shows that the performance of the current method is significantly better. The improved detection performance of the present approach over our old algorithm is further illustrated with three distorted instances.

While the majority of fingerprints may be accurately recognized, occasional false positives and false negatives do occur. The primary reason for false negatives is a small distortion. Luckily, fingerprint matchers can successfully match slightly deformed fingerprints, therefore we found that this is not a serious issue. Fig. provides one such example. VeriFinger reports that the matching score between the query and gallery fingerprints is 305, which is a very high matching score. However, the proposed detection algorithm is unable to identify the query fingerprint as distorted due to its tiny distortion.

If this query fingerprint is rectified by the the matching score can be raised to 512 with the suggested rectification procedure.

The main causes of false positives are small finger areas, non-frontal finger poses, and poor image quality. In many situations, the available data is insufficient to accurately align and classify the fingerprint. Rerectification of normal fingerprints, for instance, may result in lower matching scores.

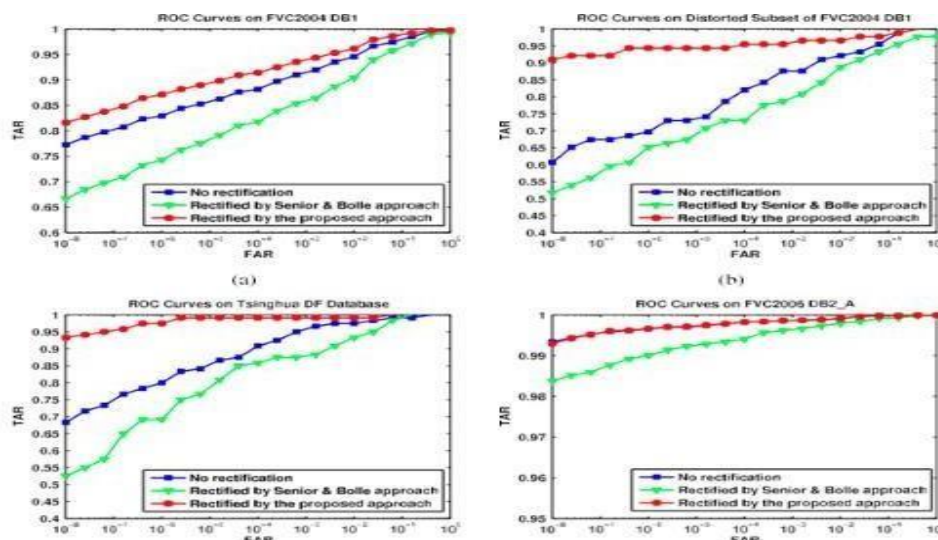


Fig 8: The ROC curves of three fingerprint matching experiments on each of the following four databases

IV.CONCLUSION

When fingerprints are significantly deformed, the false non-match rates of fingerprint matchers are extremely high. This results in an automated fingerprint recognition system security flaw that terrorists and criminals can exploit. To close this gap, techniques for the identification and correction of fingerprint distortion must be developed.

An innovative algorithm for distorted fingerprint identification and rectification was presented in this paper. The registered ridge orientation map and period map of a fingerprint are utilized as the feature vector for distortion detection, and an SVM classifier is trained to distinguish between normal and deformed input fingerprints. In order to perform distortion rectification, or more accurately, distortion field estimation, the distorted fingerprint is first converted into a normal one using the inverse of the distortion field, which is predicted from the input distorted fingerprint using a nearest neighbor regression technique.

REFERENCES

1. 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.
2. D. Maltoni, D. Maio, A. K. Jain, and S. Prabhakar, *Handbook of Fingerprint Recognition*, 2nd ed. Berlin, Germany: Springer-Verlag, 2009.
3. FVC2006: The fourth international fingerprint verification competition. (2006). [Online]. Available: <http://bias.csr.unibo.it/fvc2006/>
4. V. N. Dvornychenko, and M. D. Garriss, "Summary of NIST latent fingerprint testing workshop," *Nat. Inst. Standards Technol.*, Gaithersburg, MD, USA, Tech. Rep. NISTIR 7377, Nov. 2006.
5. Neurotechnology Inc., VeriFinger. (2009). [Online]. Available: <http://www.neurotechnology.com>
6. L. M. Wein and M. Baveja, "Using fingerprint image quality to improve the identification performance of the U.S. visitor and immigrant status indicator technology program," *Proc. Nat. Acad. Sci. USA*, vol. 102, no. 21, pp. 7772–7775, 2005.
7. S. Yoon, J. Feng, and A. K. Jain, "Altered fingerprints: Analysis and detection," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 34, no. 3, pp. 451–464, Mar. 2012.
8. E. Tabassi, C. Wilson, and C. Watson, "Fingerprint image quality," *Nat. Inst. Standards Technol.*, Gaithersburg, MD, USA, Tech. Rep. NISTIR 7151, Aug. 2004.
9. F. Alonso-Fernandez, J. Fierrez-Aguilar, J. Ortega-Garcia, J. Gonzalez-Rodriguez, H. Fronthaler, K. Kollreider, and J. Biguñ, "A comparative study of fingerprint image-quality estimation methods," *IEEE Trans. Inf. Forensics Security*, vol. 2, no. 4, pp. 734–743, Dec. 2007.
10. J. Fierrez-Aguilar, Y. Chen, J. Ortega-Garcia, and A. K. Jain, "Incorporating image quality in multi-algorithm fingerprint verification," in *Proc. Int. Conf. Biometrics*, 2006, pp. 213