Improved Biometric Fingerprint Recognition System

Jyothi Silvester

PG Student

Department of ECE

Satyam College of Engineering

E-mail : jyothisilvester28@gmail.com

 Abstract- This system is to handle the problems such as false non-matching and distorted Fingerprints. Distorted Fingerprints are Detected and Rectified by using Novel algorithm and it will also used to detect the malicious users False non-matches due to limited capability of existing Fingerprint matchers. Malicious users will provide the duplicate and distort finger prints to escape from the identification process. 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.

Keywords: **Fingerprint, distortion, registration, nearest neighbor regression, PCA**

1 INTRODUCTION

Although automatic fingerprint recognition technologies have rapidly advanced during the last forty years, there still exists several challenging research problems, for example, recognizing low quality fingerprints [2]. Fingerprint matcher is very sensitive to image quality as observed in the FVC2006 [3], where the matching accuracy of the same algorithm varies significantly among different datasets due to variation in image quality. The difference between the accuracies of plain, rolled and latent fingerprint matching is even larger as observed in technology evaluations conducted by the NIST [4]. The consequence 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. In a positive recognition system, such as physical access control systems, the user is supposed to be cooperative and wishes to be identified. In a negative recognition system, such as identifying persons in watchlists and detecting multiple enrollments under different names, the user of interest (e.g., criminals) is supposed to be uncooperative and does not wish to be identified. In a positive recognition system, low quality will lead to false reject of legitimate users and thus bring inconvenience. The consequence of low quality for a negative recognition system, however, is much more serious, since malicious users may purposely reduce fingerprint quality to prevent fingerprint system from finding the true identity [6]. In fact, law enforcement officials have encountered a number of cases where criminals attempted to avoid identification by damaging or surgically altering their fingerprints [7].

Hence it is especially important for negative fingerprint recognition systems to detect low quality fingerprints and improve their quality so that the fingerprint system is not compromised by malicious users. Degradation of fingerprint quality can be photometric or geometrical. Photometric degradation can be caused by non-ideal skin conditions, dirty sensor surface, and complex image background (especially in latent fingerprints). Geometrical degradation is mainly caused by skin distortion.

To solve this problem, a 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 database of distorted reference fingerprints and the corresponding distortion field is used to rectify the input fingerprint. An important property of the proposed system is that it does not require any changes to existing fingerprint sensors and fingerprint acquisition procedures. Such property is important for convenient incorporation into existing fingerprint recognition systems. The proposed system has been evaluated on three databases, FVC2004 DB1 whose images are markedly affected by distortion, Tsinghua distorted fingerprint database which contains 320 distorted fingerprint video files, and NIST SD27 latent fingerprint database. Experimental results demonstrate that the proposed algorithms can improve the matching accuracy of distorted fingerprints evidently.

2 EXISTING METHOD

Due to the vital importance of recognizing distorted fingerprints, researchers have proposed a number of methods which can be coarsely classified into four categories.

2.1 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]. Fujii [18] proposed to detect distortion by detecting deformation of a transparent film attached to the sensor surface. However, 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; and
    (iii)   they cannot detect fingerprints distorted before pressing on the sensor.

2.1.1 Distortion-Tolerant Matching

The most popular way to handle distortion is to make the fingerprint matcher tolerant to distortion [20], [21], [22], [23], [24], [25]. In other words, they deal with distortion on a case by case basis, i.e., for every pair of fingerprints to be compared. For the most widely used minutiae-based fingerprint matching method, the following three types of strategies have been adopted to handle distortion: (i) assume a global rigid transformation and use a tolerant box of fixed size [20] or adaptive size [21] to compensate for distortion; (ii) explicitly model the spatial transformation by thin plate spline (TPS) model [22]; and (iii) enforce constraint on distortion locally [24]. Various methods for handling distortion during matching have also been used in image-based matcher [23] or skeleton-based matcher [25].
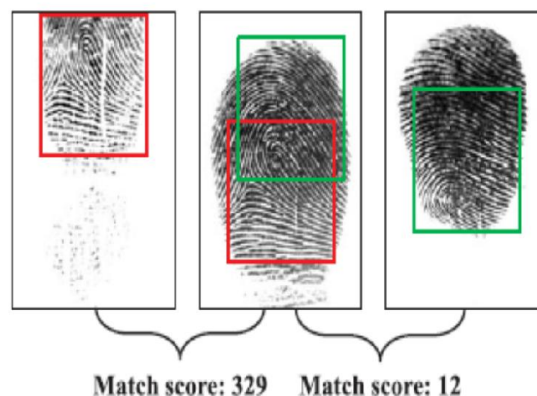

Match score: 329   Match score: 12

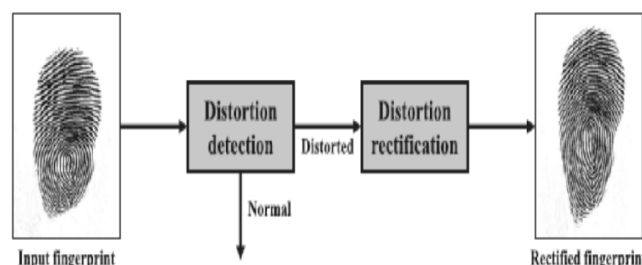*Figure 2.1: Three impressions of the same finger from FVC2004 DB1.*

Figure 2.2: Distortion detection and rectification system.

For example, if we increased the bounding zone around a minutia, many non-mated minutiae will have a chance to get paired. In addition, allowing larger distortion in matching will also slow down the matching speed.

### 2.1.2 Distortion Rectification Based on Finger-Specific Statistics

Compared to the other methods reviewed above, Senior and Bolle method has the following advantages: (i) it does not require specialized hardware; (ii) it can handle a single input fingerprint image; and (iii) it does not require a set of training images of the same finger. However, ridge density is neither fixed within a finger nor fixed across fingers. In fact, several researchers have reported improved matching accuracy due to incorporating ridge density information into minutiae matchers [29], [30]. Simply normalizing ridge density of all fingerprints will lose discriminating information in fingerprints and may improve impostor match scores. Furthermore, without any constraint on validity of orientation map, this method may generate fingerprints with fixed ridge period but strange orientation map. Compare to the first limitation, the second limitation is even more harmful, since it will reduces genuine match scores. These limitations were not found in [28] since the algorithm was tested only on a small database consisting of six fingers and finger rotation was not considered.

Our method shares the advantages of Senior and Bolle method over other methods, meanwhile overcomes some of its limitations. Our method is based on statistics learnt from real distorted fingerprints, rather than on the impractical assumption of uniform ridge period made in [28]. Distortion due to finger rotation can be handled by our method. In fact, the proposed method is able to deal with various types of distortion as long as such distortion type is contained in the training set. In addition, extensive experiments have been conducted to validate the proposed method. The current work is a significant update of our preliminary study in [1], which detects distortion based on simple hand-crafted features and has no rectification functionality.

3 PROPOSED SYSTEM

3.1 Fingerprint Distortion Detection

Fingerprint distortion detection can be viewed as a two class classification problem. We used the registered ridge orientation map and period map as the feature vector, which is classified by a SVM classifier. The distortion detection flowchart is shown in Fig. 3.
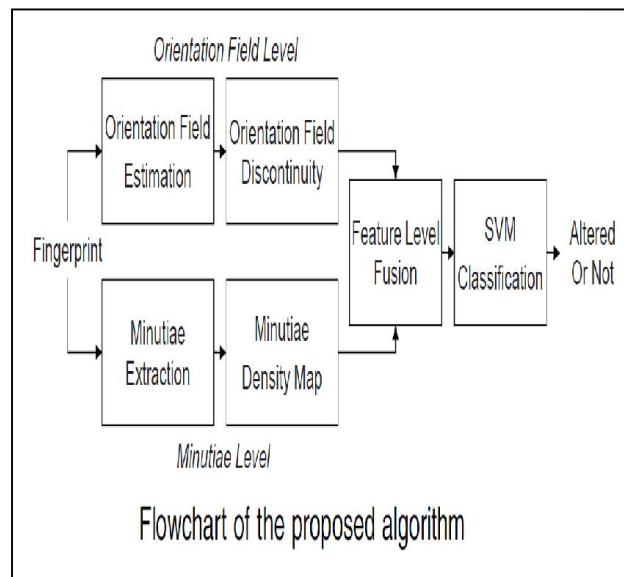
Figure 3.1: Flowchart of fingerprint distortion detection.

3.1.1 Fingerprint Registration

In order to extract meaningful feature vector, fingerprints have to be registered in a fixed coordinate system. For this task, we propose a multi-reference based fingerprint registration approach. In the following,

we describe how the reference fingerprints are prepared in the offline stage, and how to register an input fingerprint in the online stage.

3.1.2 Reference Fingerprints

In order to learn statistics of realist fingerprint distortion, we collected a distorted fingerprint database called Tsinghua distorted fingerprint database. A FTIR fingerprint scanner with video capture functionality was used for data collection. Each participant is asked to press a finger on the scanner in a normal way, and then distort the finger by applying a lateral force or a torque and gradually increase the force.

We use 500 fingerprints as reference fingerprints which consist of 100 normal fingerprints from FVC2002 DB1_A, 200 pairs of normal and distorted fingerprints from the training set of Tsinghua DF database. Note that there are no common fingerprints between training and testing data. A large number of references are used in order to properly register fingerprints of various pattern types, while distorted fingerprints are also used as references in order that new distorted fingerprints can be properly registered.

3.1.3 Online Fingerprint Registration

In the online stage, given an input fingerprint, we perform the registration w.r.t. registered reference fingerprints. Level 1 features (orientation map, singular points, period map) are extracted using traditional algorithms [11], [31]. According to whether the upper core point is detected or not, the registration approach can be classified into two cases. If the upper core point is not detected, we do a full search to find the pose information, namely solve the following optimization formula:

$$\arg\max_{x,y,\alpha,i} \|\mathrm{OrientDiff}(RO_i(x,y,\alpha),O) \le \theta_t\|_0, \qquad (1)$$

where x and y denote the translation parameters, a denotes the rotation parameter, i denotes the corresponding reference fingerprint ID, O is the orientation map of the input fingerprint, ROi denotes the orientation map of the ith reference fingerprint, function Orient computes the difference of two orientation maps at each location, k X k0 counts the number of nonzero elements, and ut is the threshold, which is empirically set as 10 degrees. Note that the ridge orientation map is defined on blocks of 16 X 16 pixels.
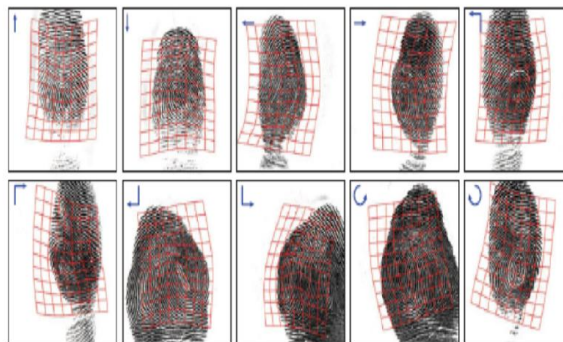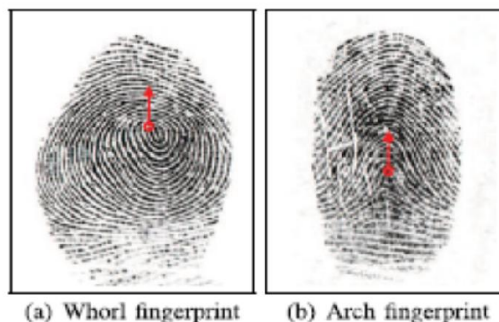

Figure 3.2: Examples of 10 distortion types in Tsinghua DF database.

The blue arrows represent the directions of force or torque, and red grids represent the distortion grids which are calculated from matched minutiae between the normal fingerprint and the distorted fingerprint.

(a) Whorl fingerprint   (b) Arch fingerprint

Figure 3.3: The center (indicated by red circle) and direction (indicated by red arrow) of two fingerprints.

If the upper core point is detected in the input fingerprint, we align the upper core point to the center point of reference fingerprints. Namely, ðx; yÞ is known. We find the optimal rotation parameter for Eq. (1). Finally, we register the ridge orientation map and period map of the input fingerprint to the fixed coordinate system by using the obtained pose information. The flowchart in Fig. 3 shows an example of registration.

3.2 Feature Vector Extraction

We extract a feature vector by sampling registered orientation map and period map. The sampling grid is shown in Fig. 3, where finger center is also marked. Note that the two sampling grids are different. The sampling grid of period map covers the whole fingerprint, while the sampling grid of orientation map covers only the top part of the fingerprint. This is because the orientation maps below finger center are very diverse even within normal fingerprints. See Fig. 6 for examples. So they are not good features for distinguish distorted fingerprints from normal fingerprints. The feature vector is defined, where O denotes the orientation vector on sampling grids, and P denotes the period vector on sampling grids. Feature value at sampling points outside fingerprint region is set as 0.

3.3 Classification

The 500 reference fingerprints that we mentioned in Section 3.1, were used as training samples. Distorted fingerprints are viewed as positive samples while normal fingerprints are viewed as negative samples. LibSVM [32] was used to train a Support Vector Classifier with quadratic polynomial kernel.

3.4 Distorted Fingerprint Rectification

A distorted fingerprint can be thought of being generated by applying an unknown distortion field d to the normal fingerprint, which is also unknown. If we can estimate the distortion field d from the given distorted fingerprint, we can easily rectify it into the normal fingerprint by applying the inverse of d. So we need to address a regression problem, which is quite difficult because of the high dimensionality of the distortion field (even if we use a block-wise distortion field). In this paper, a nearest neighbor regression approach is used for this task.

The proposed distorted 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.

3.4.1 Statistical Modeling of Distortion Fields

In order to learn statistical fingerprint distortion model, we need to know the distortion fields (or deformation fields) between paired fingerprints (the first frame and the last frame of each video) in the training set. The distortion field between a pair of fingerprints can be estimated based on the corresponding minutiae of the two fingerprints. Unfortunately, due to the severe distortion between paired fingerprints, existing minutiae matchers cannot find corresponding minutiae reliably. Thus, we extract minutiae in the first frame using VeriFinger and perform minutiae tracking in each video. Since the relative motion between adjacent frames is small, reliable minutiae correspondences between the first frame and the last frame can be found by this method.
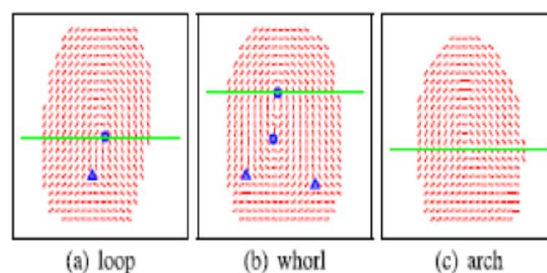
(a) loop   (b) whorl   (c) arch

Figure 3.4: Orientation maps of three patterns: (a) loop, (b) whorl, and (c) arch.

3.4.2 Generation of Distorted Reference Fingerprint Database

To generate the database of distorted reference fingerprints, we use nref ¼ 100 normal fingerprints from FVC2002 DB1_A which are same to what we described in Section 3.1. Note that, these fingerprints have been registered following the procedure described in Section 3.1. The distortion fields are generated by uniformly sampling the subspace spanned by the first two principle components. For each basis, 11 points are uniformly sampled in the interval [_2,2].

(a) First Component with a Negative Coefficient

(b) First Component with a Positive Coefficient

(c) Second Componen-t with a Negative Coeffi-cient

(d) Second Componen-t with a Positive Coeffi-cient
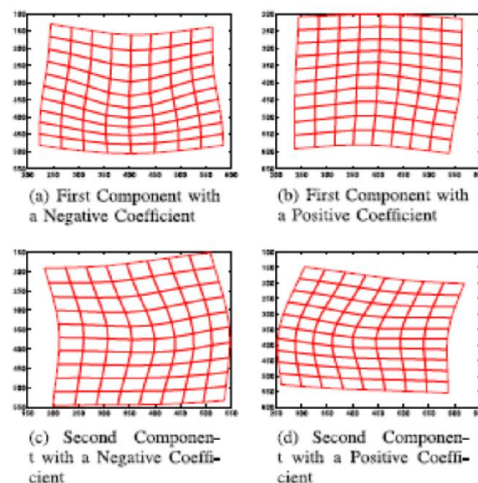
Figure 3.4: First two principal components of distortion fields from the training set of Tsinghua DF database.

Here, for visualization purpose, only one reference fingerprint (the fingerprint located at the origin of the coordinate system) is used to generate the database of distorted reference fingerprints. In practice, multiple reference fingerprints are used to achieve better performance.

3.5 Performance of Distortion Detection

We view distortion detection as a two-class classification problem. Distorted fingerprints are viewed as positive samples and normal fingerprints as negative samples. If a distorted fingerprint is classified as a positive sample, a true positive occurs. If a normal fingerprint is classified as a positive sample, a false positive occurs. By changing the decision threshold, we can obtain the receiver operating characteristic (ROC) curve. Fig. 10 shows the ROC curves of the proposed algorithm and our previous algorithm [1] on FVC2004 DB1 and the test set of Tsinghua DF database.
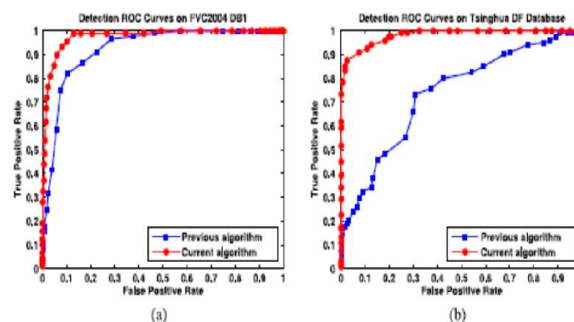

Figure 3.7: The Detection ROC curves of our previous algorithm [1] and current algorithm on the (a) FVC2004 DB1 and (b) Tsinghua DF database.

The red transformation grids estimated by the proposed algorithm are overlaid on them. The blue numbers show the matching scores without/with rectification. It shows the importance of detecting them as distorted fingerprints. First two examples come from FVC2004 DB1, while the last one comes from Tsinghua DF database.
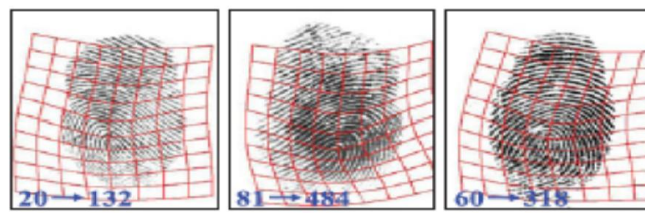
Figure 3.8: Three distorted examples. Our previous algorithm [1] fails to detect their distortion, while the current algorithm can detect their distortion correctly.
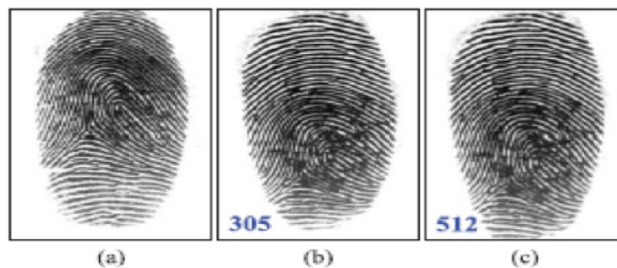

Figure 3.9: An example of false negative due to slight distortion. (a) Gallery fingerprint, (b) query fingerprint, and (c) query fingerprint rectified by the proposed rectification algorithm.

Fortunately, we found that this is not a severe problem since fingerprint matchers can successfully match slightly distorted fingerprints. Such an example is given in Fig. 12. As the query fingerprint contains slight distortion, the proposed detection algorithm fails to detect it as distorted one, but the matching score between the query fingerprint and the galley fingerprint is 305, a very high matching score according to VeriFinger.

False positives are mainly due to low image quality, small finger area, or non-frontal pose of finger. In such cases, there is no sufficient information for correctly aligning and classifying the fingerprint. Such an example is shown in Fig. 13. Applying rectification to normal fingerprints may reduce matching scores.
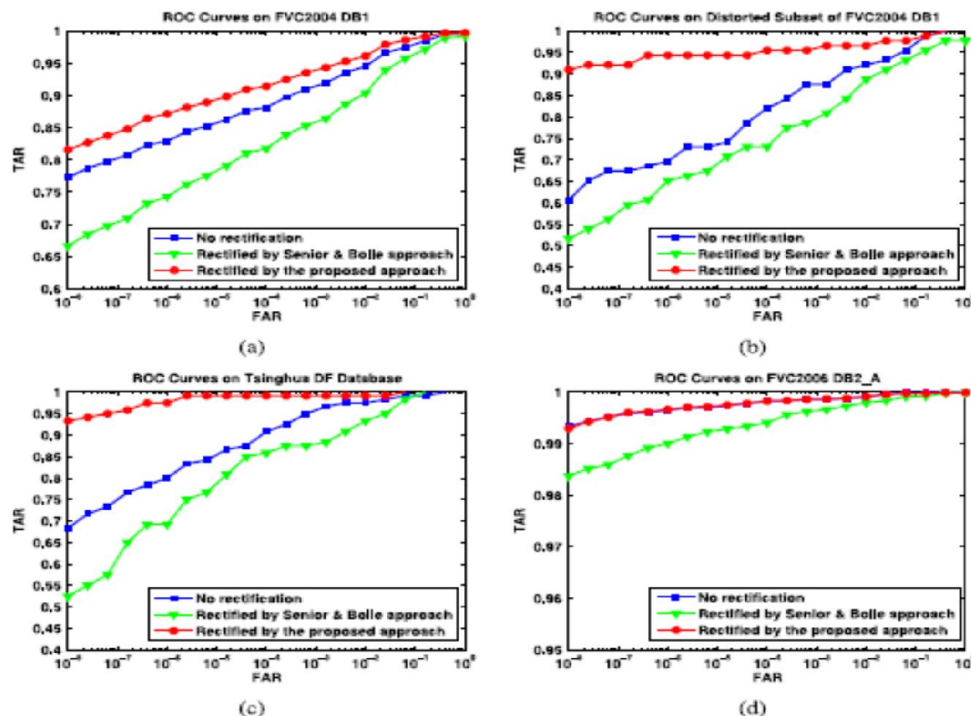

Figure 3.10: The ROC curves of three fingerprint matching experiments on each of the following four databases: (a) FVC2004 DB1, (b) distorted subset of FVC2004 DB1, (c) Tsinghua DF database, and (d) FVC2006 DB2_A.

We have examined all detection errors on FVC 2004 DB1 and Tsinghua DF database and have categorized the reasons into four types. Note that this classification is not exclusive and one example might be attributed to multiple reasons (such as both low quality and small area).

3.6 Performance Of Distortion Rectification

The final purpose of rectifying distorted fingerprints is to improve matching performance. To quantitatively evaluate the contribution of the proposed rectification algorithm to the matching accuracy, we conducted three matching experiments on each of the following four databases:

FVC2004 DB1, distorted subset of FVC2004 DB1, Tsinghua DF database, and FVC2006 DB2_A. VeriFinger 6.2 SDK was used as the fingerprint matcher. The input images to VeriFinger in the three experiments are original fingerprints, rectified fingerprints by Senior and Bolle approach, and rectified fingerprints by the proposed algorithms, respectively.

VeriFinger was used as the fingerprint matcher. The cumulative match characteristic (CMC) curve is commonly used to report latent matching accuracy. To make the experiment more realistic, we use all 27,000 file fingerprints in the NIST SD14 database as the background database.

The CMC curves on NIST SD27 shown in Fig. 16 correspond to the following three cases: no rectification, latent fingerprints rectified by Senior and Bolle approach, and latent fingerprints rectified by the proposed approach. From Fig. 16, we can see that both rectification algorithms can improve the recognition rate and the proposed algorithm performs better.
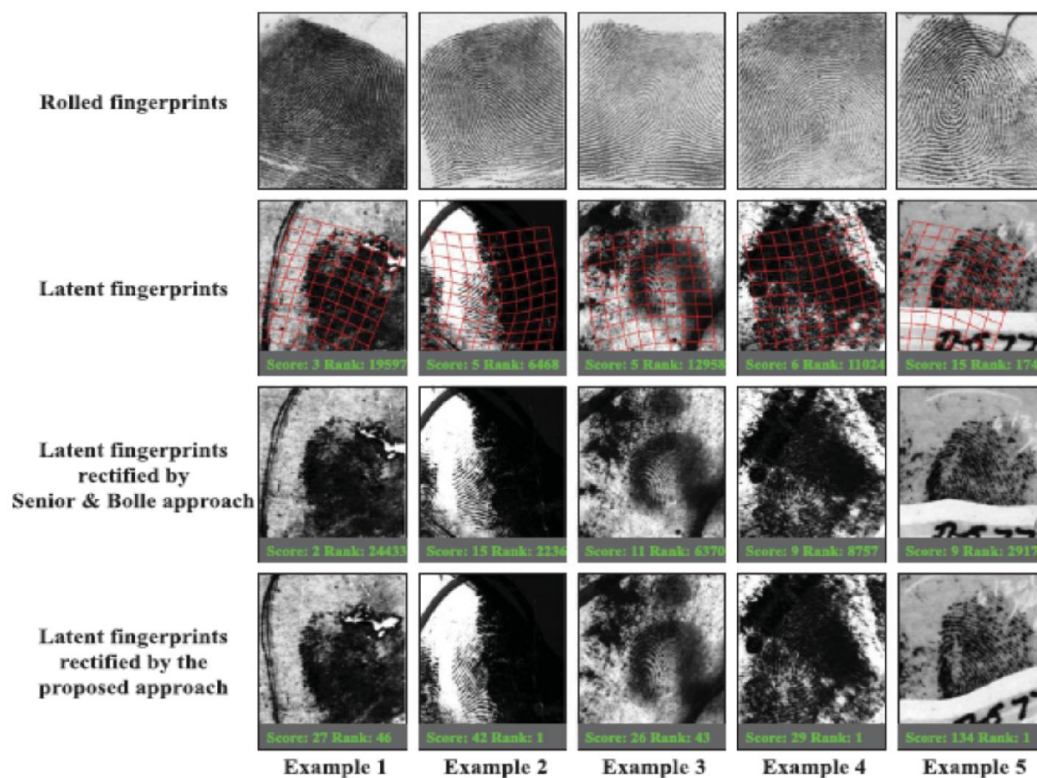
Figure 3.11: Genuine match scores and ranks of original latent fingerprints and latent fingerprints rectified by two different approaches for five examples from NIST SD27.

The red transformation grids estimated by the proposed approach are overlaid on the original latent fingerprints to visualize the distortion.
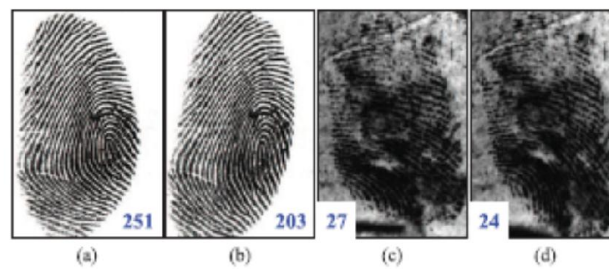
Figure 3.12: Two examples of unsuccessful rectification due to non-frontal pose and low image quality.

Although the genuine match scores of most distorted fingerprints are improved after rectification, there are some examples whose matching scores dropped after rectification. Unsuccessful rectification can be classified into two categories: (1) a normal fingerprint is incorrectly detected as a distorted one and then undergoes the rectification process, and (2) the rectification for a distorted fingerprint is incorrect. False positive of distortion detection is discussed in Section 5.1.

3.6.1 Impact of the Number of Reference Fingerprints

The number of reference fingerprints used in distortion rectification is an important parameter. Fig. 3.15 shows the impact of the number of reference fingerprints on matching accuracy on FVC2004 DB1. As we can see from this figure, a larger number of reference fingerprints lead to higher matching accuracy. But a larger number of reference fingerprints also mean longer process time.
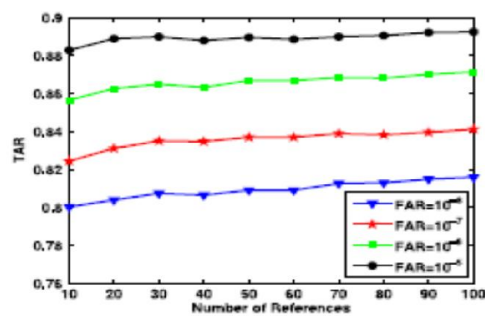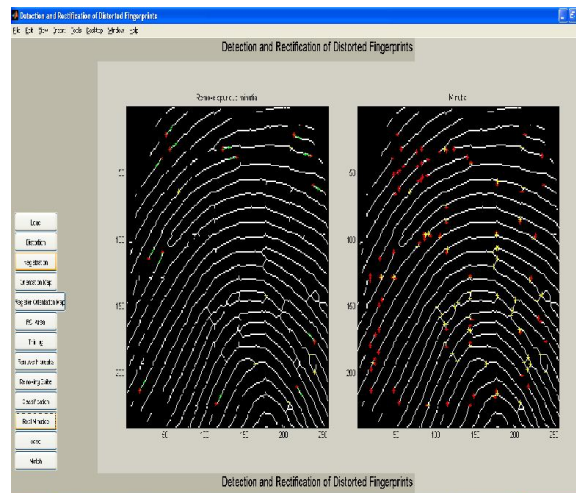

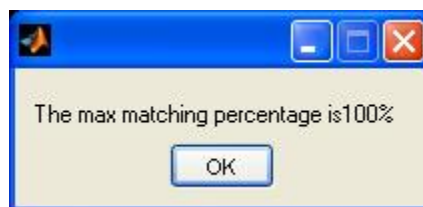***Figure 3.13: The impact of the number of reference fingerprints on matching accuracy on the whole FVC2004 DB1.***

4 RESULTS
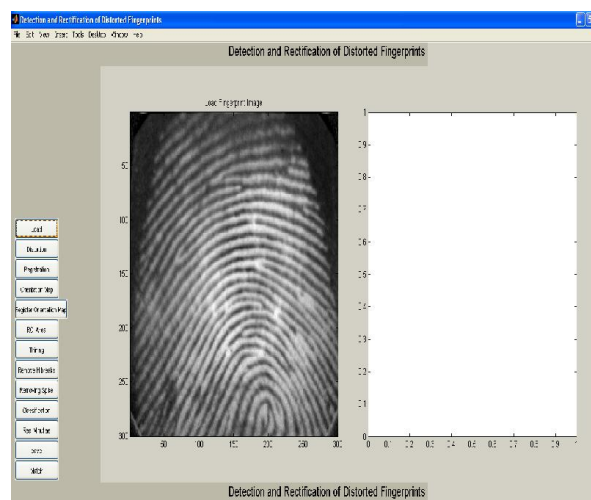
Figure 4.1: Input Image

Figure 4.2: Match File

Figure 4.3: Output Recognition and Detection

6 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, 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.

Finally a classifier framework has been developed and found that cost sensitive classifier produces better results. The system has been evaluated on fingerprint database and the experimental result shows that system produces a verification rate of 98%.

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. Garris, "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. 2003.

[9] F. Alonso-Fernandez, J. Fi_errez-Aguilar, J. Ortega-Garcia, J. Gonzalez-Rodriguez, H. Fronthaler, K. Kollreider, and J. Big€un, "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. Fi_errez-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. 213–220.