Person Identification using Multiple Fingerprint Matching

K.Sindhu
Student, M.E(CSE)
Kumaraguru College of Technology
Coimbatore

L.Latha
Associate Professor,CSE
Kumaraguru College of Technology
Coimbatore

ABSTRACT
In biometric security system still fingerprint authentication is a challenging task for the altered and compressed images. Apart from the Automatic Fingerprint Identification System(AFIS), the altered, blurred and compressed images are still having quality issues. This paper presents an efficient multi-model biometric system based on multiple fingerprint images which includes altered fingerprint images also. The system utilizes fingerprint scanner to simultaneously collect fingerprints of multiple fingers on a hand in one image. The collected multi-finger images are first segmented to get individual fingers. Quality of each individual finger is analysed and its minutiae points are extracted. The minutiae points of each finger is extracted from multiple fingerprint images and compared with the corresponding individual finger of the input fingerprint image to get matching score of that finger. Matching score between two or more fingerprint images is obtained by fusing matching scores of various fingers along with their respective image quality and relative accuracies. Prediction of genuine user or impostor user is based on the fused matching score.

General Terms
Person Authentication, Multiple Fingerprint..

Keywords
Fingerprint, Altered images, Fusion, Image Quality.

1. INTRODUCTION
Fingerprint is one of the well accepted biometrics in the current scenario. Although there are several biometrics traits such as Face, Palm, Ear, etc. [10] but fingerprint have the widest forensic application. Fingerprint comprises of a pattern of ridges, valleys that originates unique features called minutiae points such as ridge ending and bifurcation. It has been empirically determined that the fingerprint impression of identical twins are different. For a small fraction of the population, fingerprints may be unsuitable for automatic identification because of generic factors as aging, environmental or occupational reasons. In order to design an effective and accurate system which is based on fingerprints, one can think to make use of multiple fingers, instead of single finger. Acquisition of fingerprint images from multiple fingers using fingerprint scanner through which one can get all fingerprints of the hand simultaneously.

Figure 1.1 Fingerprint Image(adopted from crescentok.com)

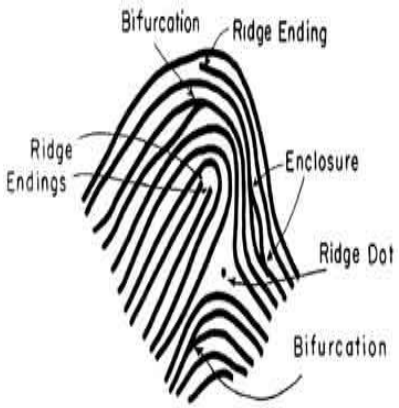

Figure 1.2 Minutiae Points(adopted from www.cis.rit.edu)

According to Fingerprint Verification Competition, they are particularly insisted on: wet, distortion, and dry fingerprints. Distortion of fingerprints seriously affects the accuracy of matching. There are two main reasons contributed to the fingerprint distortion. First, the acquisition of a fingerprint is a three-dimensional/two-dimensional warping process. The fingerprint captured with different contact centers usually results in different warping mode. Second, distortion will be introduced to fingerprint by the nonorthogonal pressure people exert on the sensor. How to cope with thesedistortions in the matching process is a challenging task.

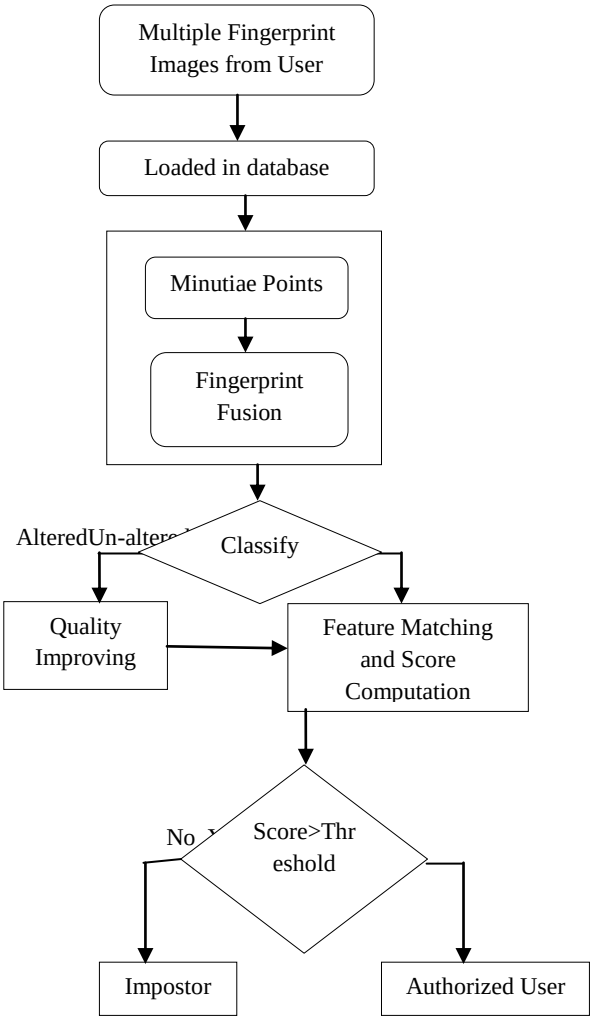

Figure 1.3 Flow Chart for proposed fingerprint matching

2. RELATED WORK

2.1 Related Work

Anil K. Jain(2012) discuss an Analysis and Detection based on Altered Fingerprints. The primary purpose of fingerprint alteration is to evade identification using techniques varying from abrading, cutting, and burning fingers to performing plastic surgery. The use of altered fingerprints to mask one's identity constitutes a serious "attack" against a border control biometric system since it defeats the very purpose for which the system was deployed in the first place, that is to identify individuals in a watch list.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 analysis of altered fingerprints, first determine the impact of fingerprint alteration on the matching performance, second categorize altered fingerprints into three types: obliteration, distortion, and imitation , and finally assess the utility of an existing fingerprint quality measure in terms of altered fingerprint detection. The proposed algorithm was evaluated at two levels: finger level (one finger) and subject level (all 10 fingers). The Finger Level Evaluation is done through orientation field discontinuity.

AdityaNigam(2012) discuss fusion of multiple fingerprint images based on score level fusion. In order to design an effective and accurate system which is based on fingerprints, one can think to make use of multiple fingers, instead of single finger. In this paper by normalizing the fingerprint image, foreground and background areas are identified.The extracted foreground image is rotated from −45degreeto +45 degree.Connected components are obtained in each for the rotated images and fingertip enclosing boxes are formed. Based on the ratio of number of black and white pixels in these enclosing boxes, a vertically aligned image is obtained.To classify the fingers into one of the 4 categories viz. index, middle, ring and little finger, clusters containing fingertips are selected using geometric characteristics of a finger.

Dario Maio(2006) discuss about discriminating fake fingers from real ones,based onthe analysis of skin distortion. The main potential threats for fingerprint-based systems are attacking the communication channels, including replay attacks on the channel between the sensor and the rest of the system, attacking specific software modules (e.g., replacing the feature extractor or the matcher with a Trojan horse), attacking the database of enrolled templates, and presenting fake fingers to the sensor. Fake fingerprint detection approach uses a sequence of frame as input. In that some subsequent steps are followed. First one is discarding the fingerprints which does not satisfies the amount of rotation condition. Second the input which satisfies the condition are allowed inside for next processing. The main stage in fake fingerprint detection is computation of the optical flow. Block wise correlation technique is used in this optical flow calculation. Next to this is computation of distortion map. An effective solution to the distortion map problem is to perform a temporal-integration of the distortion map, resulting in an integrated distortion map. The temporal integration is simply obtained by block-wise summing the current distortion map to the distortion map "accumulated" in the previous frames. Final step is distortion code. In this, Comparing two sequences of integrated distortion maps, both acquired under the same movement trajectory, is the basis of this fake finger detection approach.

YilongYin(2009) discussed about the fusion of multiple impression of same finger for fingerprint verification. This novel method is of score level fusion using multiple enrolled impressions to achieve higher verification accuracy of existing fingerprint systems. The main idea of the method is to build a representation of the biometric reference as a polyhedron by taking into account the matching results of multiple enrolled impressions. The verification step consists in measuring a distance between the centroid of the polyhedron and the acquired image. Score level fusion method involves two stages: enrollment and verification. During enrollment, multiple enrolled impressions of the same user's finger are acquired and stored as templates, and these relativities in multidimensional space are extracted through matching them between every pair of impressions. During verification, a new impression is acquired and compared to the stored templates to verify the user's claimed identity by computing a distance from the query fingerprint to the centroid of templates in multidimensional space.

JieTian(2006) discuss about the novel algorithm to deal with the nonlinear distortions. The proposed algorithm has two main steps. First, the template and input fingerprints were aligned. In this process, the local topological structure matching was introducedto improve the robustness of global alignment. Second, the method Normalized Fuzzy Similarity Measure was introduced to compute the similarity between the template and input fingerprints. Fuzzy theory to deal with the nonlinear distortion in fingerprint images. The algorithm was defined to deal with the spurious minutiae. Then the algorithm aligns the template and input fingerprints using the registration method and local topological structure matching was introduced to improve the robustness of global alignment. Finally a novel similarity computing method based on fuzzy theory, was conducted to compute the similarity between the template and input fingerprints.

3.PROPOSED WORK

3.1 Image Acquisition: Image Collection can be done in different ways. The image is obtained from the multiscan basic SDK 2.6 scanner. Gathering two samples of all the ten fingerprint for an each individual. Likewise collecting multiple fingerprint samples from different persons.

3.2 Pre-Processing:

In pre-processing having two stages called binarization and thinning.Binarization[6] is nothing but the process of converting the gray scale image into black and white image. In that the gray levels of pixels belonging to the object are quite different from the gray levels of the pixels belonging to the background. So moving to an effective tool thresholding to separate objects from the background. The next stage thinning is a process of reducing the width of each ridge to one pixel.

3.3 Feature Extraction:

The major part in the Feature Extraction is Minutiae Marking and False Minutiae Removal. The first stage Minutiae Marking is done by locating the end points and bifurcation points on the thinned ridge skeleton image based on the number of neighboring pixels.The end points are selected if they have a single neighbor and the bifurcation points are selected if they have more than two neighbors.Crossing Number (CN) algorithm is using for extracting the minutiae points[12].

$$C_n(\mathrm{P}) = \left(\frac{1}{2}\right)\sum_{i=1}^{8} |P_{i-} P_{i+1}|$$

$C_n(\mathrm{P})$is equal to half of cumulative successive difference between pairs of adjacent pixels belonging to the 8-neghiborhood of pixel. The second stage False Minutiae Removal is a combination oflocating termination and bifurcation points.

3.4 Fusion Scheme for Combination of Multiple Impressions:

Feature Level Fusion is used for the combination of multiple fingerprint images.[2] A fusion of multiple fingerprint can be achieved at the feature level by simply concatenating the feature vectors from multiple fingers. Some features like ridge flow map, ridge wavelength is calculated from each individual fingerprint and concatenating the features of individual finger to get the sum fusion value of multiple fingerprints. Ridge flow map is nothing but the similarity between the flow at two sample points and ridge wavelength map is the similarity between the wavelengthof two sample points.

3.5 Matching:

The matching process starting with the baseline matching algorithm, which uses only minutiae, reference points, overall image characteristics and skeleton are incrementally used. In Local Minutiae Matching the similarity[16] between each minutia of a finger print and each minutia of altered fingerprint is computed. The neighborhood of a minutia is defined to be a circular region of radius 80 pixels. All minutiae lying in this neighbourhood are called the neighbourhood minutiae. In Global Minutiae Matching the one-to-one correspondence between minutiae is established. When fewer than three minutiae are matched [11] [3], the matching score is set as 0; otherwise *SM* is the product of a quantitative score *Smn*and a qualitative score *Smq*. The main algorithm used in matching is K-means which is known to be efficient in clustering large data sets. The K-means algorithm partition a set of objects, based on their features into k clusters where k is a predefined or user defined constant. The main idea is to define *k* centroids, one for each cluster. The centroid of a cluster is formed in such a way that it is closely related (in terms of similarity function; similarity can be measured by using different methods such as cosine similarity, Euclidean distance,Extended Jaccard) to all objects in that cluster.

3.6 Quality Measure:

A quality measure is in effect a rule (or the result of a rule) that assigns numeric values to a specific quality indicator. The important distinction between quality indicators and quality measures is that quality measures take on numeric values, while quality indicators refer only the unquantified attributes which is related to quality. The proposed work presents a novel methodology Global Clarity Score (GCS) and Global Orientation Quality Score (GOQS)[7][8] for fingerprint image quality measurement.

4. EXPERIMENTAL RESULTS

The proposed algorithm is tested with six fingerprints collected from each persons and have been fused together. These fused fingerprints are tested for Matching accuracy at intra-level, inter-level and with the fingerprints that have been altered. Four impressions of six fingerprints have been collected from 25 subjects and put it under training set. And six impressions of six fingerprints have been collected from 25 subjects and put it under testing set. In most of the paper altered fingerprint authentication is done with the help of public database. But in this paper the fingerprint is collected with the help of multiscan SDK 2.6 scanner and just converting the real-time fingerprint image into altered by applying some simulations and accuracy of the altered fingerprint is checked.

Figure 4.1 GAR and FAR GRAPH

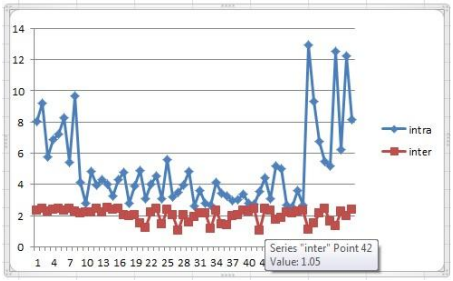

Figure 4.2 Matching Score for proposed system

The performance evaluation of the proposed algorithm results 89.5 percent of the subjects with altered fingerprints (these percentages are calculated based on the threshold value).

5. CONCLUSION AND FUTURE WORK

The fusion of multiple fingerprints plays major role in person authenticationand also it helps to reduce the false positive acceptance of a person.This study can further extended in reconstruct of altered fingerprints. That is for some types of altered fingerprints where the ridge patterns or ridge structure are damaged locally, reconstruction is indeed possible. Hence some fuzzy algorithm is needed to solve this problem.

6. ACKNOWLEDGEMENT

The authors would like to thank DRDO, Government of India for funding this project.

7. REFERENCES

[1] A.Antonelli, R. Cappelli, D. Maio, and D. Maltoni, *"Fake Finger detection by skin distortion,"* in IEEE Transactions on Information Forensic and Security, Vol. 1,No.3,Sep 2006.

[2] Anil K .Jain, "*Latent Fingerprint Matching:Fusion of Rolled and Plain Fingerprints*," Department of Computer Science and Engineering, Michigan State University.

[3] A. M. Bazen and S. H. Gerez," *Elastic Minutiae Matching by Means of Thin-Plate Spline Models*," Proc. 16th Int'l Conf. Pattern Recognition, pp. 985-988, 2002.

[4] Almansa, A., Lindeberg, T.: "*Fingerprint enhancement by shape adaption of scale-space operators with automatic scale selection"*. IEEE Transactions on Image Processing, Vol 9, No. 12 pp. 2027–2042 (2000).

[5] Chaohong Wu, Sergey Tulyakov and VenuGovindaraju,"*Image Quality Measures for Fingerprint Image Enhancement*,"Center for Unified Biometrics and Sensors (CUBS) SUNY at Buffalo, USA.

[6] D. Maltoni, D. Maio, A.K. Jain, and S. Prabhakar, Handbook offingerprint recognition, New York: Springer, 2003.

[7] E. Lim, X. Jiang, W. Yau, "*Fingerprint quality and validity analysis*", IEEE International Conference on Image Processing (ICIP 2002), 1 2002 pp. 22–25.

[8] H. Chen, J. Tian, and X. Yan, "*Fingerprint matching with registration pattern inspection*," in *Proc. AVBPA*, 2003, pp. 327–334.

[9] JianjiangFeng, Anil K. Jain, Arun Ross, "*Detecting Altered Fingerprints*," in 2010 International Conference on Pattern Recognition.

[10] K. Jain, "*Biometric recognition: Q&A*", Nature, Vol. 449, pp. 38-40,Sept. 6, 2007.

[11] M. Tico and P. Kuosmanen," *Fingerprint Matching Using an Orientation-Based Minutia Descriptor*," IEEE Trans. Pattern Analysis and Machine Intelligence, vol. 25, no. 8, pp.1009-1014, Aug 2003.

[12] RoliBansal, Pritisehgal and punambedi, "*Minutiae Extraction from FingerprintImages*," in IJCSI International Journal of Computer Science Issues, Vol. 8, Issue 5, No 3, Sep 2011.

[13] Tong, X., Tang, X., Shi, D."*Adjacent orientation vector based fingerprint minutiae matching system"*, In: IEEE Proceedings of the 17th International Conference on Pattern Recognition (ICPR '04), vol. 1, pp. 528–531 (2008).

[14] Tai Pang Chen, Xudong Jiang and Wei Yun Yau,"*Fingerprint Image Quality Analysis*," Institute for Infocomm Research.

[15] Xinjian Chen, JieTian and Xin Yang, "*A New Algorithm for Distorted Fingerprints Matching Based on Normalized Fuzzy Similarity Measure*," in IEEE Transactions on Image Processing, Vol. 15,No.3, March 2006.