

Design of Biometric Fingerprint Image Enhancement Algorithm by using Iterative Fast Fourier Transform

Shiwani Dod

M.Tech Scholar

Department of Electronics and Communication Engineering
Rayat and Bahra Institute of Engineering, Kharar, Punjab, India

Email: shiwithakur@gmail.com

Abstract—Among all the minutia based fingerprint identification system, the performance depends on the quality of input fingerprint images. In this paper, we have designed and implemented an algorithm of fingerprint image enhancement by using Iterative Fast Fourier Transform (IFFT). We have designed an approach for removing the false minutia generated during the fingerprint processing and a method to reduce the false minutia to increase the efficacy of identification system. We have used fingerprint Verification Competition 2006 (FVC 2006) as a database for implementation of proposed algorithm. Experimental results show that the results of our enhancement algorithm are better than existing algorithm of fast Fourier transform.

Keywords: Iterative Fast Fourier Transform (IFFT), fingerprint Identification System (FIS), Image Enhancement, False Minutia, Broken Ridges, Fast Fourier Transform (FFT).

I. INTRODUCTION

Biometrics provides automated method to identify a person based on physiological or behavioural characteristics. Among the features measured are face, fingerprints, hand geometry, handwriting, iris, retina, vein, and voice. Biometric technologies are becoming the foundation of an extensive array of highly secure identification and personal verification solutions. As the level of security breaches and transaction fraud increases, the need for highly secure identification and personal verification technologies is becoming apparent. Each approach uses some aspect of an individual's physical or behavioral attributes as a means of authenticating the individual's identity. According to [4] the most pervasive biometric in use today is fingerprint, a physical biometric. [6] Had given the concept that fingerprints have a unique pattern of ridges and furrows. Fingerprint readers use this uniqueness to generate a pattern – rarely do they actually use the full print for identification – based on areas where line print lines merge, fork or loop – like the round “whorl” you can find in the finger prints. This pattern is stored in a database – either in a remote computer or in the device itself. When a person scans a print, this device compares the pattern generated by the print with one in the database to make a positive identification. [13] Discussed that there are various phases of fingerprint identification are in existence as image loading, image enhancement, normalization, thinning, minutia marking and minutia extraction. Fingerprint image quality is a vital issue to measure the performance of fingerprint identification system. So quality assessment of fingerprint data leads to identify the fingerprints in a better way. The main purpose of such procedure is to enhance the image by improving the clarity of ridge structure or increasing the consistence of the ridge orientation. In noisy regions, it is difficult to define a common orientation of the ridges. The process of enhancing the image before the feature extraction is also called pre-processing. According to [9] for this purpose generally two methods are used. First is normalization, this is a method to improve the image quality by eliminating noise and correcting the deformations of the image intensity caused by non-uniform finger pressure during the image capture. The idea of normalization consists in changing the intensity of each pixel. The normalization preserves the clarity and contrast of the ridges; however it is not able to connect broken ridges or improve the separation of the parallel ridges. Second is transformation. In particular, for detection of high or low frequencies. As the ridges have structure of repeated and parallel lines, it is possible to determine the frequency and the ridge orientation using transformation. According to [4]. Ridge Thinning is to eliminate the redundant pixels of ridges till the ridges are just one pixel wide. After the fingerprint ridge thinning, marking minutia points is relatively easy. In general, for each 3x3 window, if the central pixel is 1 and has exactly 3 one- value neighbors, then the central pixel is a ridge branch. If the central pixel is 1 and has only 1 one-value neighbor, then the central pixel is a ridge ending.

II. PREVIOUS WORK

This section summarizes the literature on fingerprint, palm and iris identification, elaborated with various normalization and enhancement techniques used for quality improvement of identification system. (Roger

Clarke, 1994) identified need of identification and various factors required for human identification. According to this paper various identification measures as names, codes, knowledge-based, token-based and biometrics had taken into account. (Hong et al., 1996) emphasizes that Gabor filter has optimal joint resolution in both spatial and frequency domains. (Kansaei et al. 1997) used the concept of statistics to calculate the Dominant Ridge Direction (DRD) for each 16*16 block. After deriving the DRD, they rotate the block image according to the dominant orientation for image projection to enhance the local ridge veins. (Miao et al., 1997) proposed the method of minutiae extraction by tracing ridges on gray image. (Hong et al., 1998) used Gabor filters as band pass filters to remove the noise and prevent true ridge/valley structures because the filter has both frequency selective and orientation selective properties. (Wahab et al., 1998) define eight directional masks of spatial domain to find the local orientation of ridges in 8*8 block. (Abutaleb et al., 1999) used the fact that a fingerprint is made of white followed by black lines of bounded number of pixels in time domain. They use the genetic algorithm to generate black and white lines of different widths, and then translate the enhancement technique into the optimization problem while getting the best match with the original fingerprint. (Hong et al., 2000) introduced the method of Gabor filtering for fingerprint image. (Joachim Weickert et al., 2001) demonstrated the coherence enhancing diffusion filtering method, (N.K. Ratha et al., 2002) presented data hiding concept using wavelet transformation and WSQ compression techniques including the use of filters, with the assumption of secure image capture device. (Jianxin et al., 2003) described the Fast Fourier Transformation (FFT) method for fingerprint enhancement. (Marios Savvides et al., 2004) had shown the implementation of Min Avg. Co-relation Energy (MACE) filters for authentication while convolution (random no. generation + add it to the training images) provide irrevocability. (Ying-Han Pang et. al., 2005) proposed the concept of cancelable palmprint authentication system. This work is designed to transform palm print image into a lower dimensional compact feature representation. Cancelable verification key is generated with the help of random number generation. To generate the key wavelet based palm print features are hashed with a set of pseudo random data. (Eric Kukula et. al., 2006) dealt with the various factors i.e. technical as well as environmental (operational), current system characteristics of Hand Geometry software installing in the Purdue University. A performance analysis in terms of False Rejection Rate (FRR) and False Acceptance Rate (FAR) had shown in order to measure the efficiency of fingerprint identification system. As a result they got the fact that 93% people liked it, 98% interested to use it because of easiness and 87% preferred it than existing card-based. (Sharat et. al., 2006) demonstrated that core and Delta points are global features, represent intrinsic points of reference that can be used to align two prints and reduce computation complexity of the matcher. They provided an approach which reduces complexity from $O(n^3)$ or $O(n^2)$ to $O(n)$. Where n represent number of minutia. They used Fast Fourier Transformation for image enhancement. For singular point detection various steps are as image pre processing, complex filtering, and post-processing. (Nalini Ratha et al., 2006) demonstrated that biometrics is a method of enhancing the security and privacy of biometric authentication. Instead of using your real finger transformation used. Transformation means mapping the original finger into some different parameters and it can be done by various techniques as Cartesian Transformation, Radial Transformation, and Functional Transformation. (Eric Kukula et al., 2006) presented various factors i.e. technical as well as environmental (operational), current system characteristics of hand geometry software installing in the Purdue University and had done a performance analysis in terms of FRR and FAR. As a result they got the fact that 93% people are linked it, 98% interested to use it because of easiness and 87% preferred it than existing card-based. (Salil Prabhakar et al., 2003) reviewed various applications in the area of biometrics. (Kirat Pal Singh., 2015) proposed the technique to generate an irrevocable cryptographic key. This technique used bifurcation points and ending points for feature extraction. (Vince Thomas et al., 2007) represented iris texture feature for gender identification. Various steps as data acquisition, segmentation, feature extraction, geometric features, texture features were included. (Donald Monro et. al., 2007) had been proposed iris coding method based on Discrete Cosine Transform (DCT). This work demonstrated the use of novel patch encoding methods in capturing iris texture information. To model for matching and non- matching probability statistical analysis used in order to predict worst case equal error rates. (Guodong Guo et. al., 2007) proposed the concept that in case of iris pattern stolen or any other activity which force to compromise with the security of the iris identification system, cancellable iris biometric has been used. It can be achieved by the transformation of original iris pattern. They presented four techniques as gray-combo, bin-combo, gray-salt and bin-salt. (Emanuele Maio et al., 2008) provided on-line biometric authentication based on signature and for this purpose non-invertible transformation has been generated and convolution transformation has been used.

(Jinyu Zuo et. al., 2008) described that in case of Iris pattern stolen or any other activity which force to compromise with the security of the iris identification system, cancelable iris biometric has been used. It can be achieved by the transformation of original iris pattern and four techniques as gray-combo, bin-combo and gray salt, bin-salt. (Golamreza Amayeh et al., 2009) had given the approach in which hand is divided into different parts as parts related with fingers and confidence of each finger has analyzed by support vector data description. After the measurement of confidence of each finger consider the finger which has highest confidence and if this value is higher than threshold value then raise the confidence of other fingers also.

III. PROPOSED ALGORITHM

Proposed fingerprint enhancement algorithm is based on Iterative Fast Fourier transformation and used to enhance the intensity of pixels of the fingerprint images with maintaining its frequency and orientation selective properties. Various steps of this algorithm are shown as follows-

- Step1:** *Read the image*
- Step2:** *Calculate the size of image and save in a variable i.e. size.*
*size= imsize (length*width)*
- Step3:** *Define the blur operator ,i.e. blur*
- Step4:** *Adjust the blur operator with variance of pixels in image*
- Step5:** *Normalize the image with calculating the mean and variance with the following formula referred from (L. Hong et. al., 1998)*

$$N(x, y) = \left. \begin{array}{l} Ms + \sqrt{(Vs*(I(x, y) - M)^2)/V} \text{ if } I(x, y) > M, \\ Ms - \sqrt{(Vs*(I(x, y) - M)^2)/V} \text{ otherwise} \end{array} \right\}$$

Where M_s and V_s depict standard mean and variance correspondingly while M and V represent actual mean and variance respectively. $I(x,y)$ shows intensity at pixel with coordinates x and y .

- Step6:** *Binarize the image with the value assignment as*
Ridge=1 and Furrow=0
- Step7:** *B = zeros (size of image) */ Number of zeros can be calculated with the help of vanishing moments*/*
- Step8:** *x= blur x-size*
y= blur y-size
- Step9:** *To calculate the circular center, B*
B ((middle-y): (middle+y), (middle-x), (middle+x))= 1;
- Step10:** *B= fftshift (B);*
- Step11:** *B= B/sum (sum (B))*
- Step12:** *y= fftshift (ifft(fft(B)*fft(x)));*
- Step13:** *Enhanced image with iterative fast fourier transform*

PROPOSED ALGORITHM FOR FINGERPRINT ENHANCEMENT

IV. FALSE MINUTIA REMOVAL

If we match minutia based on matching points it may generate some extra minutia (false minutia) and erroneous matching points which can decrease the false rejection rate. So, it is necessary to remove false minutia as well as false matching points. Generally, fingerprint geometric variations are limited as rotations and translations. With the consideration of this fact set the k^{th} minutia as origin and align its direction to zero (along x) and then accommodate all other minutia points in the fingerprint to the new origin. The difference between minutia as origin and all other minutia origin direction is reflected as the orientation of each minutia and it is adjusted with the origin minutia. Minutia position value toward bottom right are positive while angle value are anti-clockwise from bottom to the top of the x axis on the right within $[0,\pi]$ and are clockwise from bottom to top of the x axis on the left within $[0,-\pi]$. Based on this observation, we select a value of majority orientation, length and keep the matching pairs that have the majority orientation and length. This reduces the number of false minutia and matching points. As earlier discussed in the previous section proposed technique can improve the quality of poor fingerprint images especially for light/dark fingerprint impressions by using the statistics of the global texture unit information. Sometimes for such situation, just using the texture filtering cannot give the satisfactory results. This may cause the erroneous false minutia in the minutia extraction process. As discussed above if we apply the orientation property of fingerprint the problem can be alleviated largely.

V. MINUTIA MATCH

Given two set of minutia of two fingerprint images, the minutia match algorithm determines whether the two minutia sets are from the same finger or not. An alignment-based match algorithm is used in our work. It includes two consecutive stages. First is alignment stage and second is match stage. In alignment stage two fingerprint images to be matched, choose any one minutia from each image, calculate the similarity of the two ridges associated with the two referenced minutia points. If the similarity is larger than a threshold (we have considered 90% in this paper), transform each set of minutia to a new coordination system whose origin is at the referenced point and whose x-axis is coincident with the direction of the referenced point. In Match stage, approach is to

elastically match minutia is achieved by placing a bounding box around each template minutia. If the minutia to be matched is within the rectangle box and the direction discrepancy between them is very small, then the two minutia are regarded as a matched minutia pair. Each minutia in the template image either has no matched minutia or has only one corresponding minutia.

VI. EXPERIMENTATION RESULTS

We have used four datasets DB1, DB2, DB3 and DB4 from the fingerprint database i.e. Fingerprint Verification Competition 2004 (FVC 2004). Each of these four disjoint datasets is collected by using different sensors. This database consists of 1800 fingerprint images those have been used in this research. In FVC2004, data collection is done with introducing difficulties as wet/dry impressions, rotated fingerprint, light/dark fingerprint impression etc. The performance of the proposed fingerprint enhancement algorithm has been evaluated on FVC2004 DB1, DB2, DB3, DB4 public domain fingerprint databases. Results of proposed enhancement algorithm are shown in figures 1.1 and 1.2.



Figure 1.1 Fingerprint Images before Iterative Fast Fourier enhancement



Figure 1.2 Fingerprint Images after Iterative Fast Fourier enhancement

VII. EVALUATION INDEXES FOR FINGERPRINT RECOGNITION

False Rejection Rate (FRR) and the other is False Acceptance Rate (FAR). For an image database, each sample is matched against the remaining samples of the same finger to compute the False Rejection Rate. If the matching g against h is performed, the symmetric one (i.e., h against g) is not executed to avoid correlation. All the scores for such matches are composed into a series of Correct Score. Also the first sample of each finger in the database is matched against the first sample of the remaining fingers to compute the False Acceptance Rate. If the matching g against h is performed, the symmetric one (i.e., h against g) is not executed to avoid correlation. All the scores from such matches are composed into a series of Incorrect Score. Our algorithm tests all the images without any modification or fine tuning for the database. Proposed algorithm can better differentiate imposturous minutia pairs from genuine minutia pairs in a certain confidence level.

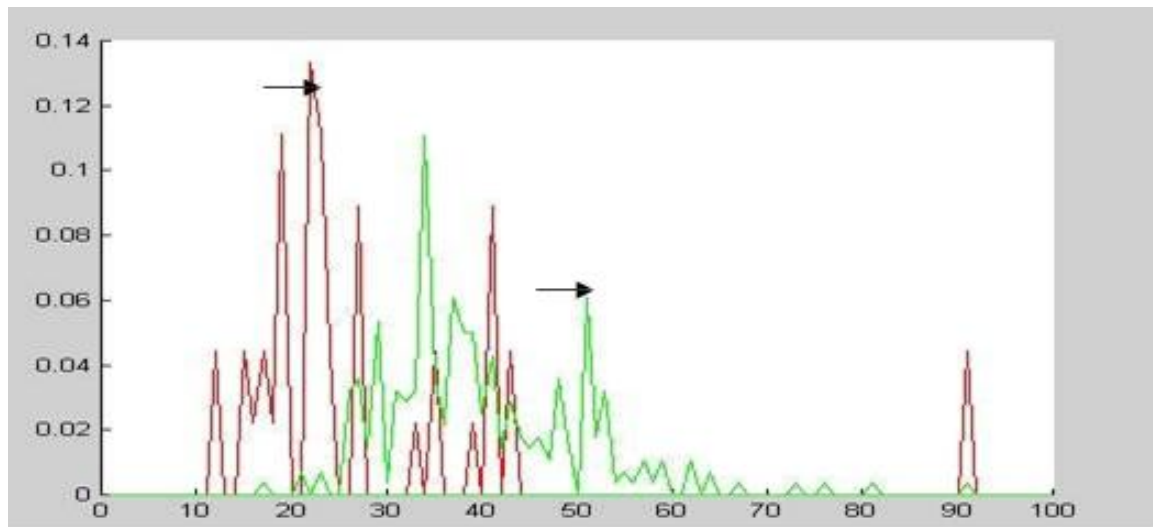


Fig. 1.3: Performance Evaluation of IFFT and FFT Enhancement Algorithm

- i. Red line: Iterative Fast Fourier Transform
- ii. Green line: Fast Fourier Transform

CONCLUSION

This paper describes a fingerprint enhancement method based on iterative fast fourier transformation. Image enhancement is critical to the quality of any fingerprint identification system. In this paper, we have shown the comparative study of fast fourier enhancement algorithm and iterative fast fourier enhancement algorithm. It has been shown with the help of a performance graph. Experiments on a public domain fingerprint database (i.e. FVC 2004) demonstrates that the use of minutia descriptors leads to an order of magnitude reduction in the false accept rate without significantly affecting the genuine accept rate. Based on the observation of good quality rolled images, the ridge and valleys intervals of each image are considered in order to select the Region of Interest (ROI) for effective enhancement. Sometimes, during fingerprint enhancement false minutia may be generated. In this paper, we have designed a method to remove the false minutia in order to maintain the efficacy of enhancement mechanism.

REFERENCES

- [1] Amayeh, G. B., "Improving Hand Based Verification Through Online Finger Template Update Based on Fused Confidences", IEEE Transactions on Pattern Recognition , pp. 978-984, 2009.
- [2] Ayers, T. F., "Modeling fingerprints: Components for the task of synthesis", Proceeding of Introduction to Modeling and Simulation on Biometric Technologies, pp. 155-162, Calagary, 2004
- [3] Bolle, R. C., "Biometrics perils and patches", Transaction of Pattern Recognition , pp. 2727-2738, 2002.
- [4] Chikkerur, S. G., "Minutia Verification in Fingerprint Images Using Steerable Wedge Filters", IEEE Transactions on Pattern Recognition and Machine Intelligence , pp. 45-51, 2005.
- [5] Clarke, R., "Human Identification in Information Systems: Management Challenges and Public Policy Issues", Information Technology & People , pp. 6-37, 1994.
- [6] S. A. Cole, R. McNally, and K. Jordan, "Truth Machine: the Contentious History of DNA Fingerprinting", Chicago: The University of Chicago Press, 1995.
- [7] Kirat Pal Singh, Shivani Parmar, "VHDL Implementation of a MIPS-32 Pipeline Processor", International Journal of Applied Engineering Research, Research India Publication, pp. 1952-1956, 2012.
- [8] Gerez, A. M., "Systematic methods for the computation of the directional fields and singular points of fingerprints", IEEE Transactions on Pattern Analysis and Machine Intelligence , pp. 905-919, 2002.
- [9] Guo, G. J., "Iris Extraction Based on Intensity Gradient and Texture Difference", IEEE workshop on Applications of Computer Vision, pp. 211-216, 2008.
- [10] Hong, L. W., "Fingerprint Image Enhancement: Algorithm and Performance Evaluation", Transactions on Pattern Analysis and Machine Intelligence , pp. 777-789, 1998.
- [11] L. Hong, Y. Wan and A. K. Jain, "Fingerprint Image Enhancement: Algorithm and Performance Evaluation", Transactions on Pattern Analysis and Machine Intelligence, Vol. 20, No. 8, pp. 777-789, 1998.
- [12] Chikkerur, S. G., "Minutia Verification in Fingerprint Images Using Steerable Wedge Filters", IEEE Transactions on Pattern Recognition and Machine Intelligence , pp. 45-51, 2005.
- [13] Hong, L. W., "Fingerprint image enhancement: Algorithm and performance evaluation", IEEE Transaction of Pattern Analysis and Machine Intelligence , pp. 670-781, 2000.
- [14] Kirat Pal Singh, Shivani Parmar, Dilip Kumar, "Design of High Performance MIPS Cryptography Processor", Proceedings of 9th International Conference Heterogeneous Networking for Quality, Reliability, Security and Robustness (GBU, Noida, U.P, India), Springer LNCS Publication, pp. 778-793, 2013.
- [15] Jain, A. H., "Biometrics: Promising frontiers for emerging identification market", ACM Communications , pp. 91-98, 2000.

- [16] Kansaei, M. B. "Fingerprint Feature Enhancement Using Block-Direction on Reconstructed Images", International Conference on Information, Communications and Signal Processing, pp. 721-725, 1997.
- [17] Kukula, E. E., "Implementation of Hand Geometry at Purdue University's Recreational Center: An Analysis of User Perspectives and System Performance", 2005.
- [18] Maio, D. M., "FVC2002: Fingerprint verification competition", IEEE Pattern Analysis Machine Intelligence , pp. 402-412, 2008.
- [19] Monro, D. M., "DCT Based Iris Recognition", IEEE Transactions on Pattern Analysis and Machine Intelligence , pp. 586-593, 2007.
- [20] Peng Wang, Q. J., "Modeling and Predicting Face Recognition System Performance Based on analysis of Similarity Scores", IEEE Transactions on Pattern Analysis and Machine Intelligence, pp. 665-670, 2007.
- [21] Prabhakar, S. J., "Learning Fingerprint Minutiae Location and Type", Transactions of Pattern Recognition , pp.1847-1857, 2003.
- [22] Ratha, N. C., "Cancelable Biometrics", IEEE Conference on Pattern Recognition, pp. 48-51, 2006.
- [23] Savvides, M. V., "Cancelable Biometric Filters for Face Recognition", Proceedings of the IEEE conference on Pattern Recognition, pp. 51-54, 2004.
- [24] Sharat, C. R., "Impact of Singular Point Detection on Fingerprint Matching Performance", IEEE Transactions on Pattern Recognition and Machine Intelligence , pp. 64-70, 2006.
- [25] Kirat Pal Singh, "Biometric based Network Security using MIPS cryptography Processor, International Journal of Exploration in Engineering and Technology, researchgate, pp. 33-37, 2015.
- [26] Takahashi, K. H., "Generating Provably Secure Cancelable fingerprint Templates based on Correlation-invariant Random Filtering", IEEE Transactions on Pattern Recognition , pp. 978-984, 2009.
- [27] Thomas, V. C., "Learning to predict gender from iris images", IEEE Transactions on Pattern Analysis and Machine Intelligence , pp. 11-418, 2007.
- [28] Zuo, J. R., "Cancelable Iris Biometric", IEEE Conference on Pattern Recognition, pp. 244-248, 2008.