



A Review of Image Based Fingerprint Authentication Algorithms

Dr. Sunil Kumar Singla*

Electrical and Instrumentation Engineering Department,
Thapar University Patiala, India

Abstract— Fingerprints, because of their uniqueness and other related characteristics, are the most widely used & highly accepted biometrics. Fingerprint biometric systems are either minutiae-based or pattern image based. The minutiae-based algorithms depends upon the local discontinuities in the ridge flow pattern and are used when template size is important while image-based matching algorithm uses both the micro and macro feature of a fingerprint and is used if fast response is required. A lot of research has been done in minutiae based fingerprint authentication systems that is why they are being widely used by both human experts and machines. But, in the literature a very few algorithms for image based fingerprint authentication are available. So, in this paper a review of image based fingerprint authentication algorithms has been discussed.

Keywords— Image, Fingerprint, Authentication, Minutiae, algorithms

I. INTRODUCTION

Fingerprint is one of the important and most widely used biometric system in the modern automated world where machines are replacing the human in almost every aspect of life. Automatic fingerprint authentication systems can be broadly classified into two categories [1].

- Minutiae based systems
- Patter (Image) based systems

Minutiae based fingerprint authentication systems are widely used by both human experts and machines. These systems usually rely on “local discontinuities in the ridge flow pattern” called minutiae. According to the empirical study, two individuals will not have more than seven common minutiae [2, 3]. The set of minutiae are restricted into two types Ridge endings and Ridge bifurcations. Ridge endings are the points where the ridge curve terminates, and ridge bifurcations are the points where a ridge splits from a single path to two paths at a Y-junction as shown in Figure 1. The positions and angular orientations of these points within a fingerprint uniquely characterize the fingerprint.

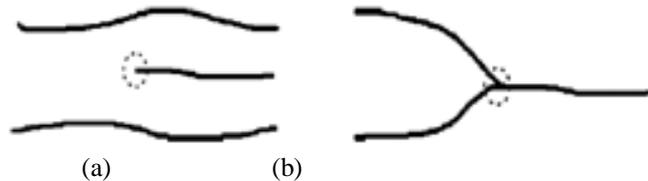


Fig. 1 Minutiae points (a) Ridge ending (b) Ridge bifurcation

Minutiae based algorithms which depend upon the local discontinuities in the ridge flow pattern and are used when template size is important as only a small part of finger image is required for verification in minutiae based systems. It would be ideal to use these algorithms where space restrictions impact the use and deployment of biometrics but this type of system requires high quality of fingerprint image. Also minutiae based approach requires extensive preprocessing operation and it is also required to reduce the number of false minutiae erroneously detected in noisy fingerprint images [4]. Image based matching algorithm use both the micro and macro features of a fingerprint [1]. The size of the image required for image based authentication must be larger as compared to minutiae based algorithm. This algorithm requires more of the image area to be present during verification. So, the memory requirement is more. But these algorithms are computationally more efficient because they can be directly applied to the gray scale fingerprint image without or very less preprocessing. Instead of using only the minutiae locations the image based system uses the gray level information which provides much richer and more discriminatory information than only the minutiae locations. In this paper a review of image based fingerprint authentication algorithms has been presented.

II. IMAGE BASED FINGERPRINT AUTHENTICATION SYSTEM

In image based fingerprint authentication system the fingerprint image itself is used as a template or reference image and the intensity values at each and every point of this template are compared with the intensity values of the query image. Depending upon the correlation between the intensity values of the two images the authenticity of the

person is determined. For a reference image (R) and query image (Q), the intuitive measure of diversity is the sum of squared difference between the intensity of the corresponding pixels [5]

$$\begin{aligned} SSD(R, Q) &= \|R - Q\|^2 \\ &= (R - Q)^T (R - Q) \\ &= \|R\|^2 + \|Q\|^2 - 2R^T Q \end{aligned} \quad (1)$$

Where, superscript "T" represents transpose of the vector.

Now, since the values of $\|R\|^2$ and $\|Q\|^2$ are constant so the value of $SSD(R, Q)$ depends upon the value of $R^T Q$. Greater the value of $R^T Q$ lesser is the diversity and vice versa. The $R^T Q$ is the cross correlation of the system representing the similarity between the two images. Hence, the authenticity of the person can be determined by calculating the cross correlation between the reference and query images.

Due to translation (both in x and y direction) and rotation between the two images the determination of cross correlation directly will not give the valid result. So, either some technique is required to be applied which will determine the translation and rotation between the two images before applying the cross correlation or one of the image is shifted in the given range of translation and rotation and cross correlation between the two images is determined and the maximum correlation among the group is taken as the similarity between the two images. For example, If δx , δy and $\delta \theta$ represents the range of probable translation in x, y- direction and rotation respectively, then similarity between the two images is given by

$$S(R, Q) = \max_{(\delta x, \delta y, \delta \theta)} cc(R, Q^{\delta x, \delta y, \delta \theta})$$

The direct application of the above equation is computationally very expensive. For example, If x and y both are sampled with a one pixel step in the range of $\delta x = \delta y = [-50, +50]$ and θ with a step size of 1° in the range of $[-20^\circ, +20^\circ]$ then the direct computation of above equation requires $101 \times 101 \times 41$ cross correlations and each correlation for a size of 400×400 pixel size images requires 1,60,000 multiplications and additions. Moreover, skin conditions, finger pressure etc. may cause brightness, contrast, ridge thickness etc. to vary significantly across the different impressions of the same finger. Also, nonlinear elastic distortions may cause the different impressions of the same fingerprint to be different.

III. LITERATURE REVIEW

In the literature different authors proposed the different solutions to the problems of image based fingerprint authentication systems. Bazen et al. [6] proposed a three step correlation based fingerprint verification system. In the first step small size templates are selected in the primary reference fingerprint. In the second step template matching is used to find the position in the secondary (query) fingerprint image at which the template match the best. Finally, the third step aims to compare the template position in both the fingerprints to make the decision regarding the authenticity. Since in this method small templates are used which means the correlation is computed locally i.e. for the local position, which is much more stable than the global correlation so this method can tolerate the non-uniform local shape distortions in the fingerprint. But this method is computationally more expensive and is not capable to deal with rotations of more than 10 degree. Nandkumar et al. [7] proposed a local correlation based fingerprint matching algorithm. In the proposed algorithm the author used a window size of 42×42 pixels around the minutia locations in the template image and 32×32 pixels size windows around the corresponding location in the query image. The normalized cross-correlation between the query window and template window is computed and peak is detected. If the peak lie outside 10 pixels from the centre, the correlation between template and query window is zero otherwise this is the absolute value of correlation between the query and template window. The local correlation of all template windows with the corresponding regions in the query image are computed and mean correlation value is found. In this way all the possible correspondence from the alignment stage are tested and maximum correlation value over all the correspondence is taken as the matching score between the query and template image. In the proposed method minutiae points are required to be extracted so all the problems related to minutiae extraction remains with this system. Moreover, the proposed system depends upon the alignment algorithm used before matching and system is computationally expensive. Cavusoglu et al. [8] proposed a robust correlation based fingerprint matching algorithm. The proposed algorithm requires segmentation, ridge orientation, reference point detection and normalized operation before the application of correlation algorithm. During the enrollment stage starting from the selected reference (core) point of the template image a set of features is obtained with deferent radius (r) and angle θ . For the authentication purpose the features of the input query image are obtained by rotating the query image with an incremental size of 1° in the given range of -15° to $+15^\circ$. For each rotation the normalized cross correlation values of both images are calculated. The maximum value of cross correlation in the given range, determine the similarity of the query and template image. This method is efficient in terms of storage since instead of template (reference image or part of reference image) the features of the template are stored but this method requires the accurate detection of core point which is a trivial task. Moreover, this method also fails in case the core point is not present in the fingerprint image.

Owang et al. [9] proposed a correlation based matching method using local Fourier-Mellin descriptor (FMD) and phase only correlation (POC) function. In the proposed method most likely FMD pair is calculated from the reference and query fingerprint images. According to the information obtained from the pair two fingerprints are aligned and other corresponding FMD pairs are checked if they are matched or Not. The symmetric phase only correlation function (which is shift and brightness invariant and is robust against noise) is used during the calculation of similarity of the two FMDs and the alignment parameters. The proposed method does not require any minutiae or core information

while taking rotation into account. The proposed system is fast but requires efficient method for the extraction of local FMDs to improve the performance of the system. Ito et al. [10] proposed a band limited phase only correlation (BLPOC) based image matching algorithm. BLPOC method is more robust to the noise and provides a sharper peak to distinguish between the genuine and imposter matching than POC. In the proposed algorithm the translational displacement is obtained using the positions of the core points (if present) in both query and reference images. The rotational alignment is determined by evaluating the similarity between the rotated replicas of the reference image (in the range of -40° to $+40^\circ$) and the query image using BLPOC function. If either reference or query image do not have the core point then firstly rotational displacement is determined using the above said method and translational displacement between the rotational –normalized image & query image is obtained using the POC function. In the next step, the common effective image area of the same size is extracted from the two images for matching using BLPOC function. The proposed technique is particularly effective for verifying low quality images that cannot be identified accurately but the detection of the core point and larger number of computations involved for rotation restricts the use of this method. Moreover, the presence of elastic deformations in the image further degrades the system performance.

Zhang et al. [11] proposed another correlation based fingerprint matching method using both Fourier-Mellin transform and band limited phase only correlation. In the proposed algorithm FMT is used to determine the rotational angle between the reference and query images. The proposed system calculates three different angles (depending upon the local maximum values) instead of one in the FMT algorithm and then selects the most appropriate angle using the following verifying steps

- (i) Extend the two aligned images
- (ii) Compute the correlation of two extended images using POC and maximum of the correlation
- (iii) Compute the position of maximum
- (iv) If the position is near the origin, two images are well aligned. Otherwise alignment is false and repeat step (i) to (iv) for other two angles.

If none of the three angles will give the satisfactory response then maximum one of the three correlation values will be used to determine the alignment. In the matching step the BLPOC is used to find the correlation between the two images. The proposed method combines the advantages of BLPOC (sharpness of correlation peak and robustness) and FMT (Rotation and translation) but the performance of the system degrades if the query and reference image contains much noise and that too of different types. Arora et al.[12] proposed an image based fingerprint verification algorithm which has been developed using LabVIEW (Laboratory Virtual Instrument Engineering Workbench) 6i software. The proposed verification algorithm consists of enrollment and authentication as two steps. The proposed method uses a learning phase during the enrollment step, which is not present in conventional image-based systems. In the learning phase a pseudo random sub-sampling is performed in which pixels are analyzed by checking their surrounding neighborhood for uniformity and each pixel is classified according to how large the uniformity of its surrounding neighborhood is (e.g. 3×3 , 5×5 and so on)[13]. This step will reduce the amount of calculations in the matching stage. The features of the reference image are extracted using the edge detection operation and the information is stored in a file along with the circular intensity profile of the reference image used in finding the rotated version of the image in the search/query image. In the verification step, the name and password of the user is first checked. If they are incorrect the system stops. If this stage is passed then the system demands for the fingerprint image in question and, after the preprocessing step, compares the two images (one in the reference pallet and the other the preprocessed image in question) and calculates the threshold value. If the threshold value lies within the accepted limit the system will accept the identity of the user; otherwise, it will reject it. As pointed out by the authors the size of the extracted template is very critical for the accuracy of the system. Too small template may not provide enough distinction; on the other hand if the entire fingerprint is taken as a template then the elastic deformation of the query image may cause serious errors. The authors conducted the experiments on FVC2002/Db1_a database by considering the template sizes of 50×50 , 100×100 and 200×200 pixels extracted from the center of the image. The authors concluded that the false rejection rate (FRR) increases with the increase in the value of threshold and for smaller learning size images the false rejection is less however, false acceptance rate (FAR) increases with decrease in learning size image. The authors concluded that a moderate 100×100 learning image size and a threshold value of 700 (1000 being the perfect match) is a good compromise for the false acceptance and false rejection rate. Although good results have been obtained by using this method at a threshold of 70% but this method can't be applied to the systems of high security.

IV. Conclusion

Fingerprint biometric systems are of minutiae-based and image based. In this paper various algorithms of image based fingerprint authentication systems have been described. Although good results have been obtained in the image based fingerprint authentication system but still a lot of work is required to be done to make this system fool proof.

References

1. P. Reid, "Biometric for Network Security", 1st Indian Reprint, Pearson Education, New Delhi, 2004.
2. E. Spinella, "Biometrics Scanning Technologies: Finger, Facial and Retinal Scanning", SANS Technology Institute, San Francisco, Dec., 2002.
3. D. Maio and D. Maltoni, "Direct Gray-Scale Minutiae Detection in Fingerprints", IEEE Transactions on Pattern Analysis and Machine Intelligence, vol.19, no.1, pp. 27-40, 1997.
4. <http://www.questbiometrics.com/biometric-history.html>

5. R. C. Gonzalez and R. E. Woods, "Digital Image Processing", Second Edition, Pearson Education, 2005.
6. A. M. Bazen and S. H. Gerez, "Directional Field Computation for Fingerprints based on the Principal Component Analysis of Local Gradients", Proceedings of 11th Annual Workshop on Circuits, Systems and Signal Processing, Veldhoven, Netherlands, pp. 1-7, November, 2000.
7. K. Nandakumar and A. K. Jain, "Local Correlation-based Fingerprint Matching", Proceedings of Indian Conference on Computer Vision, Graphics & Image Processing, pp.1-6, Kolkata, December, 2004.
8. A. Cavusoglu and S. Gorgunoglu, "A Robust Correlation based Fingerprint Matching Algorithm for Verification", Journal of Applied Sciences, vol. 7, no. 21, pp. 3286-3291, 2007.
9. Z. Ouyang, J. Feng, F. Su and A. Cai, "Fingerprint Matching with Rotation Descriptor Texture Features", Proceedings of 18th International Conference on Pattern Recognition, Hong Kong, vol. 4, pp. 417-420, Aug., 2006.
10. K. Ito, A. Morita, T. Aoki, T. Higuchi, H. Nakajima, and K. Kobayashi, "A Fingerprint Recognition Algorithm using Phase-based Image Matching for Low Quality Finger prints", Proceedings of IEEE International Conference on Image Processing, Genoa, Italy, vol. 2, pp. 33-36, September, 2005.
11. J. Zhang, Z. Ou and H. Wei, "Fingerprint Matching using Phase only Correlation and Fourier-Mellin Transforms", Proceedings of the 6th International Conference on Intelligent Systems Design and Applications, Jian, China, pp. 379-383, 2006.
12. S. Arora and S. K. Singla, "Image Based Fingerprint Verification System using LabVIEW", Majeo International Journal of Science and Technology, vol.2, no.3, pp. 489-501,2008.
13. "IMAQ VISION CONCEPTS MANUAL", NATIONAL INSTRUMENTS CORPORATION, AUSTIN, **2000**.