INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)

www.ijprems.com
editor@ijprems.com

Vol. 02, Issue 09, September 2022, pp : 126-130

e-ISSN : 2583-1062

Impact Factor : 2.265

ANALYSIS OF BIOMETRIC FACTOR RECOGNITION MECHANISM

Sheikh Ovais[*1], Dr. Siddharth Arora[*2], Tejbir Singh[*3]

[*1]M.Tech. Student, Department of Computer Engineering, GNIT, Mullana, Ambala-133 203, Haryana, India.

[*2]Associate Prof., Department of Computer Engineering, GNIT, Mullana, Ambala-133 203, Haryana, India.

[*3]Asst. Professor, Department of Computer Engineering, GNIT, Mullana, Ambala-133 203, Haryana, India.

DOI: https://www.doi.org/10.58257/IJPREMS1175

ABSTRACT

In today's world minutia matching is most popular and modern technology for fingerprint matching. If there is enough minutia point in one fingerprint image that are corresponding to other fingerprint image then it is most likely that both image are from same fingerprint. Minutiae are usually matched together by their distance relative to other minutiae around it. If multiple points in one image have similar distances between the multiple points in another image then the points are said to match up. But it is not an easy task to extract minutiae point in fingerprint. Also there may be some false minutiae point that makes the problem more difficult. Image quality is another problem to find the location and type of minutiae point in fingerprint. The quality of the input fingerprint image affects the performance and fingerprint matching methods. The quality of a fingerprint image measured corresponds to the clarity of the ridge structure in the fingerprint image. A fingerprint that contain high contrast and well defined ridges and valleys, are called as good quality image while a poor quality fingerprint is marked by low contrast and ill-defined boundaries between the ridges.

Keywords: Biometrics, Multimodal Biometrics, Recognition, Verification, Identification, Security.

1. INTRODUCTION

Fingerprints

A fingerprint is comprised of ridges and valleys. The ridges are the dark area of the fingerprint and the valleys are the white area that exists between the ridges. Figure 1.1 shows an example of fingerprint image. According to [1], the biological properties of fingerprint formation are well understood and fingerprints have been used for identification purposes from centuries. Fingerprint has been widely used for identification of criminals since 20th century. So most people do not feel comfortable in provide their fingerprints in many applications. Fingerprint-based authentication is very popular in a number of civilian and commercial applications such as, welfare disbursement, cellular phone access, and laptop computer log-in due to its many advantages such that fingerprint based biometric system provide high degree of confidence in positive identification and also it can be embedded in various system (e.g., cellular phones). The availability of cheap and compact solid state scanners as well as robust fingerprint matchers are two important factors in the popularity of fingerprint-based identification systems. There are also many disadvantages of fingerprint based authentication systems as compared to other biometrics. For example, approximately 4% of the population does not have good quality fingerprints, manual workers get regular scratches on their fingers which poses a difficulty to the matching system, finger skin peels off due to weather, fingers develop natural permanent creases, temporary creases are formed when the hands are immersed in water for a long time, and dirty fingers cannot be properly imaged with the existing fingerprint sensors. Also users should have a good knowledge to capture the fingerprint, so it is not suited for many applications such as surveillance. [1].

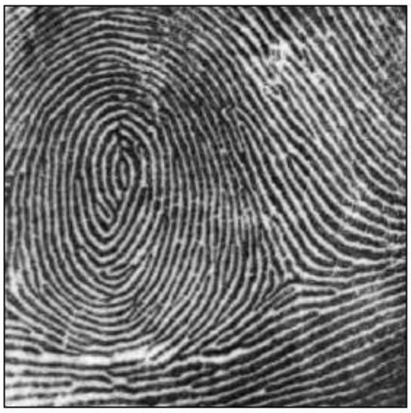

Figure 1.1: Fingerprint

2. BIOMETRIC SYSTEMS

A biometric system is essentially a pattern-recognition system that recognizes a person based on a feature vector derived from a specific physiological or behavioural characteristic that the person possesses [1]. That feature vector is usually stored in a database (or recorded on a smart card given to the individual) after being extracted. A biometric system based on physiological characteristics is generally more reliable than one which adopts behavioural characteristics, even if the latter may be more easy to integrate within certain specific applications. Biometric system can than operate in two modes: verification or identification. While identification involves comparing the acquired biometric information against templates corresponding to all users in the database, verification involves comparison with only those templates corresponding to the claimed identity. This implies that identification and verification are two problems that should be dealt with separately.

A simple biometric system consists of four basic components:

1) Sensor module witch acquires the biometric data;
2) Feature extraction module where the acquired data is processed to extract feature vectors;
3) Matching module where feature vectors are compared against those in the template;
4) Decision-making module in which the user's identity is established or a claimed identity is accepted or rejected.

Any human physiological or behavioural trait can serve as a biometric characteristic as long as it satisfies the following requirements:

1) Universality. Everyone should have it;
2) Distinctiveness. No two should be the same;
3) Permanence. It should be invariant over a given period of time;
4) Collectability.

In real life applications, three additional factors should also be considered: performance (accuracy, speed, resource requirements), acceptability (it must be harmless to users), and circumvention (it should be robust enough to various fraudulent methods).

3. LITERATURE REVIEW

There is a lot of work has been done in the field of fingerprint minutiae point detection. In this section, work done in the area of fingerprint and neural fuzzy set is reviewed and focus has been made on detecting the minutiae point of fingerprint. In this section detail of work has been done on fuzzy set and neural network in the field of fingerprint recognition is given:

Vijay Kumar Sagar et.al. [11], used neuro-fuzzy set technology in automated fingerprint recognition for minutiae point extraction. In contrast to the classical approach, the fuzzy approach makes use of the grayscale information for the extraction of minutiae. A grayscale fingerprint image consists of two distinct levels of gray pixels. The darker pixels, constituting the ridges, form one such level. The lighter pixels, constituting the valleys or furrows, form one other such level. Using human linguistics, these two levels of gray can be described as dark and bright levels correspondingly. By using fuzzy logic, these levels can be modelled and used along with the appropriate fuzzy rules to extract minutiae accurately. The fuzzy neural approach is essentially an extension of the fuzzy approach. The surrounding areas of a potential minutia can be considered as a pattern of dark and bright windows. Neural networks can then be used to recognize these patterns, and therefore, model the fuzzy rules of the system.

Tu Van et.al. [12], developed a fingerprint recognise system that was based on fuzzy evolutionary programming. A fingerprint recognizing system is built with two principal components: the fingerprint administrator and the fingerprint recognizer. Fingerprints are identified by their special features such as ridge endings, ridge bifurcation, short ridges, and ridge enclosures, which are collectively called the minutiae. The fingerprint administrator uses the method of gray scale ridge tracing backed up by a validating procedure to extract the minutiae of fingerprints. The fingerprint recognizer employs the technique of fuzzy evolutionary programming to match the minutiae of an input fingerprint with those from a database.

Vijayaprasad.PI, et.al. [13], proposed a new algorithm to improve fingerprint image quality by using Neuro-fuzzy technique. It was very difficult to detect minutiae point from bad quality fingerprint image. In this research a new method has been developed that was based on neural fuzzy set algorithm to enhancement the image. First give the membership function to each pixel according to its gray level and find image quality. After that a new membership function has been developed to enhance the fingerprint image and train the new image by neural network. In last by compare with many other image enhancement methods the result as neural fuzzy based technique gives batter result then others.

Benno Stain [14] introduced a particular form of fuzzy-fingerprints-their construction, their interpretation, and their use in the field of information retrieval. Though the concept of fingerprinting in general is not new, the way of using them within a similarity search as described here is: Instead of computing the similarity between two fingerprints in order to access the similarity between the associated objects, simply the event of a fingerprint collision is used for a similarity assessment. He has given a new approach by adding fuzzy hash function to compute fuzzy fingerprint for a given document to find similarity. The main impact of this approach is the small number of comparisons necessary to conduct a similarity search.

Later in 2005 G.Vert et.al. [15], used fuzzy logic and graphics point of reference for verifies to minutiae points. Fuzzy set theory used to verify fingerprint images in a database match with the scanned fingerprint of a user attempting to log into system. The idea behind the research that there may be different factor that affect efficiency and reliability of fingerprint verification system such as there may be different template of same fingerprint if it scan from different points. Because two templates obtained from the same fingerprint often can be difficult to match identically, so rules base on fuzzy set theory have been developed to perform matching on imprecise fingerprint templates. These rules allow for certain degree of error in the matching process.

In Roshini Velamuri [16] submitted a report in University of Texas El Paso on the topic of Fingerprint recognition using Fuzzy inference techniques. She develops the fingerprint recognition system using fuzzy inference techniques. The two principle components in this recognition system are the administrator, where templates are stored and the fingerprint recognizer. Here do not use the intermittent steps of Image processing techniques like enhancement the image and reduction of the noise. This technique based on extracts true minutiae point by fuzzy rules and then matching fingerprint by these minutiae points. In comparison to other recognition systems designed, this approach has an advantage that is the proposed system is cost effective.

A. Montesanto, et.al. [17], given a fuzzy approach for fingerprint recognition by minutiae point extraction. He proposed the fingerprint verification method based on local ridge discontinuities features (minutiae) only using grey scale images. He extracts minutiae using two algorithms those following ridge lines and then recording ridge endings and bifurcations. His approach is based on the fuzzy logic and combines the results obtained using three different methods of minutiae extraction: the sequential method, the reactive agent and the neural classification system. These methods does not guarantee the same performances in the minutiae extraction phase, producing sometimes too many false minutiae due to the noisy images considered in the experimental phase. The sequential method run after the ridge line on the grey scale image of the fingerprint until it does not meet a ridge ending or a point of intersection with another ridge line. In order to establish if the intersection identifies a bifurcation, a fixed threshold is used. During the experiment this method is able to correctly recognize the ridge endings, unlike the bifurcations. In the second method the fingerprint image is very similar to a maze, in which a reactive agent moves avoiding the ridge line that identifies the walls. This approach, using an association between the sensorial profiles and the path is the most efficient in the minutiae extraction. Moreover this method is an interesting and a novel application for this specific problem. Finally the neural classification system consists of a MLP based on a supervised learning that elaborates a grey scale normalized matrix representative of the fingerprint image. The idea of this approach was to resort to the fuzzy logic for joining the results of the three different methods, in order to improve the identification percentage of the fingerprint. For this purpose the minutiae are identified not only by the (x,y) coordinates and the orientation but also by the level of belonging to the OR Fuzzy set produced by the three method.

Dr.Rosalina Abdul Salam [18], presented a project on fingerprint recognition system using neuro-fuzzy set. This system was based on neuro-fuzzy clustering. He proposed that Clustering of fingerprints can help to reduce the complexity of the search process in a database. This can be done by grouping fingerprints with the same characteristic in the same group. The matching algorithm can compare stored fingerprint codes with only one cluster instead of the entire database. In his research, he classified fingerprints into five categories which are arch, left loop, right loop, whorl, and others. The last category is use to categorize fingerprint pattern other then the four categories. Finally, experiments were carried out to show that clustering can reduce the recognition time. Experiments were carried out using neural network classifier, fuzzy logic and Neuro-fuzzy and showed that neural network classifier is the best among the three.

4. IMPLEMENTATION AND RESULT

The process to extract minutiae point in fingerprint and their location. All the work has been implemented in MATLAB 7.0. MATLAB is a software package developed by Maths Work. It integrates computation, visualisation and programming in easy to use environment. MATLAB toolbox allows learning and applying specialized technology. Areas in which toolboxes are available include signal processing, image processing, control systems, neural networks, fuzzy logic, wavelets, simulation, and many others.

The process to extract fingerprint minutiae points contains five steps. First step is image acquisition step to obtained fingerprint image from different sensor. The second step is to enhance the contrast of image by using fuzzy logic. Image binarisation step is done after enhancement of image. Fourth step is to convert the binary image into thinned image and then minutiae point extraction method has been implemented in step five. Neural network training are describes in step six.

Step 1 Image Acquisition

The first step is to acquire fingerprint image. The fingerprint image acquire either by offline or by an online process. The fingerprint acquired by online is called “live-scan” whereas offline fingerprint image are known as “inked” fingerprint. Inked fingerprint are of three types: rolled, dab and latent. In the rolled method of fingerprint acquisition, ink is applied to the finger and then rolled on a paper from one side of the nail to the other to form an impression. This paper is then scanned at 500 dpi resolution by a standard grayscale. In the Dab method ink is applied on fingerprint and then presses it onto paper. In the online process there is no need of paper. In this process fingerprint image directly obtain from person. In this thesis offline images are used.

Step 2 Image Enhancement by Fuzzy Set

Fingerprint is the pattern of ridges and valleys. Every individual has a unique fingerprint. This uniqueness is determined by the local ridge characteristics. Minutiae points are the prominent ridge characteristic. A good quality fingerprint typically contains about 40 - 100 minutiae points [19, 20].

Fingerprint Image enhancement is to make the image clearer to the further operations. Since the fingerprint images that have been acquired from sensors or other media are not assured with perfect quality, so any enhancement method, for increasing the contrast between ridges and valleys and for connecting the false broken points of ridges due to insufficient amount of ink, is very useful to keep a higher accuracy to fingerprint recognition. For this purpose, fuzzy logic is used to enhance the fingerprint image by increase the contrast between ridge and valleys.

Fuzzy logic is not just new method for image enhancement. Many kinds of enhancement methods of the fingerprint image have been proposed [21-25]. Most are based on image finalisation, while others enhance the image directly from gray-scale images. In the gray-scale images approach, the enhancement algorithm includes the following steps [26]: (i) normalization, (ii) local orientation estimation, (iii) local frequency estimation, and (iv) filtering by a bank of the designed filters. In the normalization step, an input fingerprint image is normalized to decrease the dynamic range of the gray scale between ridges and valleys of the image in order to facilitate the processing of orientation image estimation and the tuning of the filter parameters.

Following are some of the methods used for enhancement of fingerprint images, (i) Enhancement algorithm based on image normalization and Gabor filter [21]. (ii) Fourier domain filtering of fingerprint images [22]. (iii) Fingerprint .image enhancement using CNN Gabor -type filters [23]. (iv)Adaptive normalization based on block processing [24]. (v) Enhancement of fingerprint image using M-lattice [25]**.**

Lin presented a fast fingerprint enhancement algorithm, which can adaptively improve the clarity of ridge and valley structures of input fingerprint images based on the estimated local ridge orientation and frequency [26, 27].

Some of fuzzy rule for image enhancement are such as

- If pixel level is dark then output is darker.
- If pixel level is gray then output is gray.
- If pixel level is bright then output is brighter.

5. CONCLUSION

Biometrics refers to an automatic recognition of a person based on her behavioural and/or physiological characteristics. Many business applications (e.g. banking) will in future rely on biometrics since using biometrics is the only way to guarantee the presence of the owner when a transaction is made. For instance, fingerprint-based systems have been proven to be very effective in protecting information and resources in a large area of applications. Although companies are using biometrics for authentication in a variety of situations, the industry is still evolving and emerging. At present, the amount of applications employing biometric systems is quite limited, mainly because of the crucial cost-benefit question: supposing biometrics do bring an increase in security, will it be worth the financial cost? The future probably belongs to multimodal biometric systems as they alleviate a few of the problems observed in unimodal biometric systems. Multimodal biometric systems can integrate information at various levels, the most popular one being fusion at the matching score level. Besides improving matching performance, they also address the problem of nonuniversality and spoofing. Finally, the use of biometrics raises several privacy questions. A sound trade-off between security and privacy may be necessary; but we can only enforce collective accountability and acceptability standards through common legislation [1]. For example, if and when face recognition technology improves to the point where surveillance cameras can routinely recognize individuals, privacy, as it has existed in the public sphere, will be wiped out. Even today, in some major cities, you are recorded approximately 60 times during the day by various surveillance cameras. In spite of all this it is certain that biometric-based recognition will have a great influence on the way we conduct our daily business in near future.

This study is carried out by the authors as we are working on a framework for biometrics security.

6. REFERENCES

[1] S. Prabhakar, S. Pankanti, A. K. Jain, "Biometric Recognition: Security and Privacy Concerns", IEEE Security & Privacy, March/April 2003, pp. 33-42

[2] A. K. Jain, A. Ross, S. Prabhakar, "An Introduction to Biometric Recognition", IEEE Trans. on Circuits and Systems for Video Technology, Vol. 14, No. 1, pp 4-19, January 2004

[3] D. Maio, D. Maltoni, R. Cappelli, J. L. Wayman, A. K. Jain, "FVC2002: Fingerprint verification competition" in Proc. Int. Conf. Pattern Recognition (ICPR), Quebec City, QC, Canada, August 2002, pp. 744-747

[4] M. Golfarelli, D. Maio, D. Maltoni, "On the error-reject tradeoff in biometric verification systems," IEEE Trans. Pattern Anal. Machine Intell., Vol. 19, pp. 786-796, July 1997

[5] J. Daugman, "How Iris Recognition Works", IEEE Trans. on Circuits and Systems for Video Technology, Vol. 14, No. 1, pp. 21-30, January 2004

[6] L. O'Gorman, "Seven issues with human authentication technologies," in Proc. Workshop Automatic Identification Advanced Technologies (AutoID), Tarrytown, NY, Mar. 2002, pp. 185-186

[7] L. Hong, A. K. Jain, S. Pankanti, "Can multibiometrics improve performance?," in Proc. AutoID'99, Summit, NJ, October 1999, pp. 59-64

[8] L. I. Kuncheva, C. J. Whitaker, C. A. Shipp, R. P. W. Duin, "Is independence good for combining classifiers?," in Proc. Int. Conf. Pattern Recognition (ICPR), Vol. 2, Barcelona, Spain, 2001, pp. 168-171

[9] L. Hong, A. K. Jain, "Integrating faces and fingerprints for personal identification," IEEE Trans. Pattern Analysis Machine Intell., Vol. 20, pp. 1295-1307, December 1998

[10] A. K. Jain, A. Ross, "Multibiometric Systems", Appeared in Communication of the ACM, Special Issue on Multimodal Interfaces, Vol. 47, No.1, pp. 34-40, January 2004

[11] Boyce, A. Ross, M. Monaco, L. Hornak, and X. Li, “Multispectral iris analysis: a preliminary study,” Proc. of IEEE Computer Society Workshop on Biometrics at CVPR, pp. 51-59, 2006.

[12] J. S. Pierrard and T. Vetter. Skin detail analysis for face recognition. In Proc. CVPR, pages 1–8, 2007.

[13] Usher, Y. Tosa, and M. Friedman, “Ocular biometrics: simultaneous capture and analysis of the retina and iris,” Advances in Biometrics: Sensors, Algorithms and Systems, Springer Publishers, pp. 133-155, 2008.

[14] B. Fernando, M. Glasston, L. Eduardo, H. C. Paulo, and A. Gaurda, “Exploring the scalability of multiple signatures in iris recognition using GA on the acceptance of frontier search,” in 2017 IEEE Congress on Evolutionary Computation (CEC), pp. 1843–1847, San Sebastian, Spain, 2017.

[15] S. Velmurugan and S. Selvarajan, “A multimodal authentication for biometric recognition system using hybrid fusion techniques,” Cluster Computing, vol. 22, no. S6, pp. 13429–13436, 2019.

[16] S. Viriri and J. Tapamo, “Iris pattern recognition based on cumulative sums and majority vote methods,” International journal of Advanced Robotics Systems, vol. 14, no. 3, p. 172988141770393, 2017.

[17] N. Malarvizhi, P. Selavarani, and P. Raj, “Adaptive fuzzy genetic algorithm for multi biometric authentication,” Multimedia Tools and Applications, vol. 79, no. 13-14, pp. 9131– 9144, 2020.

[18] M. Saracevic, S. Adamovic, and E. Bisevac, “Applications of Catalan numbers and lattice path combinatorial problem in cryptography,” Acta Polytechnica Hungarica, vol. 15, no. 7, pp. 91–110, 2018.

[19] S. Velmurugan and S. Selvarajan, “A multimodal authentication for biometric recognition system using hybrid fusion techniques,” Cluster Computing, vol. 22, no. S6, pp. 13429– 13436, 2019.

[20] B. K. Gul and Ç. Kurnaz, “The impact of coding and noise on iris recognition system performance,” in 2016 24th Signal Processing and Communication Application Conference (SIU), Zonguldak, Turkey, 2016