

A systematic review on Fingerprint based Biometric Authentication System

Hemalatha S

School of Information Technology

VIT University

Vellore, Tamil Nadu, India

lshemalatha@gmail.com

Abstract—Finger print recognition system is a security concern to enter through our nger print. The nger print is identified by nger print scanner like Microsoft Fingerprint Reader. Finger print recognition is regarded as the most reliable and accurate biometric identification system available. Every person is identified by their individual attendance, lock opened through their own unique nger prints. It is most actively studied as a biometric technology. The ngerprint recognition problem is regarded as ngerprint verication and ngerprint identification. The nger print pattern matching is widely used in areas like security lock door system, house entries, mobile screen locks etc., The goal of this paper is to exhibit the journey of modern fingerprint recognition systems with their merits and demerits.

Index Terms—Fingerprint, Munutiae, Feature extraction, Thinning, Matching

I. INTRODUCTION

Nowadays, password kind of authentication methods are not precise to safeguard ones belongings whether it be touchable or virtual and thus, biometric authentication systems are used. There exist 2 classes of human-biometrics i.e. biometrics of behavior and biometrics of physiology. Every human has their own biometrics characteristics and can be identified through these characteristics. Fingerprint-based authentication is one of the most significant technologies of the biometric authentication and is gaining its popularity in day-to-day life. The construction of an authenticating fingerprint-recognition system is of great importance nowadays and has drew the attention of lot of researchers.

The feasibility of using fingerprints recognition system for authenticating individual human-beings was explored by Yuan et al., [8]. The fingerprints recognition systems are now broadly used for 1:1 matching (authentication) or 1:N searching (identification) around the world. They are capable of reliably recognizing individuals for the sensitive real-world applications like banking transactions, computer/cellphone security, forensics and international border-crossing.

Primarily, fingerprint recognition system has a process of matching of fingerprint to be authenticated with the existing database of fingerprints [9]. Then, it may also be used as a device for security [3]. In general, the system involves four phases i.e. Collection, extraction, comparison, identification or recognition. Considering fingerprint-based authentication

systems, it is found that fingerprint is a union of number of ridges and valleys on the image surface.

Nowadays, image-processing systems use cutting-edge technologies for ngerprint recognition. In order to identify gaps and get higher accuracy, existing fingerprint recognition systems are to be analyzed in a detailed manner. The ultimate aim of this paper is to describe the journey of authentication systems of using fingerprint recognition, analyze the gaps and list the future enhancements.

II. LITERATURE REVIEW

A. A Real-time Fingerprint Recognition System

The fingerprint-recognition system presented by [8] in 2007 contained tiny fingerprint-sensors and hence found to be apt to use with modern embedded systems. This system, in general contained four major modules: 1. Fingerprint image pre-processing, 2. Feature extraction, 3. Fingerprint matching and 4. Fingerprint database management. In the pre-processing module, normalization, mask approximation, computing the orientation of ridges and frequency estimation are included. Then, filtering with Gabor filters, followed by adaptive binarization and parallel thinning processes are applied in order to prepare the fingerprint images for feature extraction.

Feature extraction is started by first applying the algorithm of ridge width estimation to get the average width of fingerprint ridge and finding the false minutiae features. Then, the fingerprint minutiae features are obtained as ends and bifurcations of ridges through cross-number computation algorithm. Finally, the extracted minutiae features are combined with fingerprint directional details from the pre-processing module and feature vectors are obtained. The fingerprint matching process is considered to be the matching of 2 different vector point data-sets, which is done through vector alignment to align the input image to template image and then feature matching process with different scales. Also, a local area matching is applied to overcome false matching.

The fingerprint database management system includes registration and search of fingerprint images as well the database maintenance It was quoted by the authors that the future plan is to enlarge the database with additional functions for fingerprint indexing and classification. The computational speed and accuracy of the system was justified with the experiments on FVC2002 database for the fingerprint-based authentication.

The domestic hundreds are connected, as in most cases, in a very single-phase. For the matter during this paper, it's assumed that every feeder contains fifty domestic hundreds or connections to that, following average domestic load flow studies in Republic of South Africa. So, the full load to the 3 phases is a hundred and fifty connections. Every load is through the switch selector connected solely to the one among the 3 phases.

B. Fingerprint Verification using Minutiae Matching

The fingerprint recognition system suggested by [7] in 2008 is considered here. Most of the fingerprint recognition systems work with minutiae matching that has been well prepared for authentication. Minutiae-based matching is being used in different fingerprint recognition algorithms. Yet, they suffer from the issue of dealing poor quality thumb impressions. One such issue is distortion which changes geometric location as well as alignment, and raises complications in determining a match between different impressions obtained with the same thumb. Another issue is that is still under research is accurate marking all minutiae and eliminating false minutiae. The authors of this work claimed that a minutia extractor and matcher were constructed by combining many techniques and this combination arrived from broad analysis of different research works. It is also claimed that the usage of morphological operators for segmentation, advanced thinning method, removal of fake minutia, marking of minutia with triple branch counting, uniting minutia by decomposition method led to overcome the issues mentioned above.

C. Edge Detection for Fingerprint matching

In 2008, the authors of [5] considered that the edge detection is very much required for fingerprint recognition as it has a considerable impact on thinning and feature extraction and also influences the matching process. The crucial idea is to apply edge-enhancing algorithm to improve local edges, define the edge intensity of every pixel in the image and then derive the edge strength by setting an appropriate threshold. Also, it is required to develop an operator that detects edges and contours considering them equally in arbitrary directions.

Some conclusions on different edge detection operators to be used with fingerprint images were obtained by the authors through experiments: Though the Sobel, Roberts and Prewitt operator give good performance for even noisy images, locating edges is not that much accurate and the edges found contain multi-pixels. The LOG operator detected edges are much wide and is delicate to noise. The Canny and zero-cross operators do not respond to noise and could detect the edges to be thin and have higher accuracy.

D. Normalized Cross-correlation Method

Karna D. K. et al., in 2008, contemplated that the utilization of the count of matching minutia pairs for recognizing fingerprints and proposed for the same [6]. However, it was found that the methodology was not that much effective for the purpose with the fingerprints of less-quality. The authors

thought of overcoming this problem, by making use of correlation method as these techniques were used by the previous researchers and found to provide improved results.

Also, the correlation method was modified to be normalized cross-correlation method so as to reduce the computational cost and errors from the traditional minutiae-matching technique. Cross-correlation concept is massively used digital signal processing field to compute the amount of correlation i.e. relationship between two signals. Therefore, it can be used to compare two fingerprint-images and figure out the similarity. It was concluded that even though the method worked well with the less-quality images, the outcome is dependent on the fingerprint-registration process.

E. Thinning Algorithm

In 2013, Al-Ani M S et al., made a detailed analysis on previous works on fingerprint-based-authorization systems and considered to improve the process of thinning [1]. Then, it was claimed by the authors that the feature extraction and the recognition process was improved by the so-called optimal thinning.

F. An Integrated Approach

In 2017, Cao K. and Anil K. Jain suggested an indexing methodology for fingerprint recognition based on convolutional neural network [2]. This was done by assuming that each fingers impressions were captured for multiple number of times in a very large database. The suggested methodology uses all 3 levels of features in fingerprint-images and is able to overcome the limitations with other indexing methods that use level-1 and level-2 features. The authors claimed that this is possible because neural network concept is used to train different orientations and align the fingerprints in a unique co-ordinate system. It is also claimed that the fusion of index-scores from 2 major benchmark-databases, namely, NIST and COTS SDK databases enhances the accuracy of recognition and the search efficiency.

G. Multifactor based Authentication Scheme

The work was developed in 2018 to improve the security of ATM and aimed to merge fingerprint matching, PIN code and QR-code schemes [3]. In the beginning, the bankers get fingerprint phone numbers from their customers and grant customer-only-access through fingerprint-matching. When the customer touches the fingerprint-sensor available on the machine, the fingerprint-image gets saved in SRAM and then sent to biometric-data server for further process. The two main steps followed are recognition and enhancement of fingerprint-images.

H. Fingerprint spoof buster

Chugh, T et al., in 2018 attempted to deal with the issue of spoofing attack on fingerprints by a deep learning based methodology [4]. This methodology involves minutiae feature detection and local patch extraction using convolutional neural network concept. After representing fine-grained fingerprint-images, spoofing score is presented to prove the efficacy. A

GUI, namely, FINGERPRINT SPOOF BUSTER, was presented to subjectively analyse the local areas in the image so as not to depend on only one measure as in conventional methods.

I. Gabor Wavelet and DCT Transforms

A frequency-domain based fingerprint-recognition methodology was suggested by Zheng, B et al., in 2018 [9]. The improvisation of fingerprint-images are taken care of by Gabor filters and an advanced thresholding algorithm. The DCT method and Gabor WT were combined in order to get the features extracted from the images and for the dimensionality reduction. Then, the classification is performed using nearest neighbour algorithm. The authors proved that the identification time was considerably reduced with the help of simulation experiments.

III. FINGERPRINT RECOGNITION SYSTEM

The basic intention of fingerprint-recognition is to carry on with authentication using fingerprint-impressions. This is mostly done by minutiae-features of fingerprint images. And the general flowchart is shown in Fig.1.

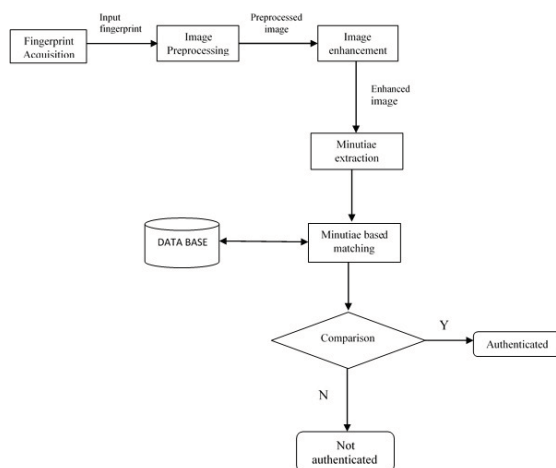


Fig. 1. Fingerprint Recognition System - General Methodology

In common, the process involves the following stages: Gather numerous fingerprint-images of the same set of persons

- i Build a database for the gathered images.
- ii Apply classification on them using apt features.
- iii Develop a methodology to identify the features.
- iv Finally, verify the method by measuring accuracy.

A. Preprocessing

The ultimate aim of this process is to make the input images get prepared for further tasks in the overall system. Especially, some pre-processing tasks such as noise removal, enhancement and thinning need to be applied before feature extraction. These are done in order to obtain sufficient accuracy in the end result. It involves the following:

- i Image sensing.

- ii Changing to 8-bit image.

- iii Convert the image-orientation to apt position

The variations in the alignments of fingerprint-images of the original and database-images leads to the distortion in the matching process which in turn leads to a collapse in the original purpose. In order to get rid of this, this step is required before feature extraction and matching processes.

- iv Image enhancement & denoising

These two are to be done with utmost care so that these do not affect the basic pattern of images to be processes.

- v Image normalization

This is done to match the size of original image to template image.

B. Thinning

It is the process by which the width of ridges in fingerprint-images are decreased while trying to keep the loss of information the least one. It is considered to be the vital process as it helps to distinguish the pattern of requirement in fingerprint-images.

While thinning process is carried on, the following points must be kept in mind as far as possible:

- i The width of ridges be one-pixel wide.
- ii The ridges to contain no kind of breaks.
- iii All kinds of noises and repetitions to be eradicated.

C. Feature Extraction

This is said to be the process of focus in the complete system and is largely dependent on preprocessing and thinning. It is also considered to be a sensitive one and is expected to extract minutiae characteristics. Minutiae are defined to be the key points in any fingerprint-image and are possibly classified to be the ends of ridges and bifurcations. Thus, these features are found to be suitable for fingerprint recognition and currently available as the backbone of many existing systems. The key points are indeed selected from original image as well as the datasets by using the function called cpselect that yields a set of matching points. There are many different key points present in fingerprint-images and the chosen points determine how the original image is oriented with respect to the template image.

D. Fingerprint Matching







This process facilitates the comparison of original images with dataset images for the purpose of actual recognition using minutiae features extracted. Other features such as whorl, loop or arch can also be extracted and used for this purpose. The basic necessity is that both original and template images are to be oriented in the similar direction and to this end a focal-point in the fingerprint-image is found and further processed. Basically, the geometry-correspondent algorithms are used for this purpose. In this algorithm, the template-structure consists of size and orientations as well as type of features in the properly-aligned manner. And the input image is graphically matched with the template-image for recognition.

The advantage of using other features than minutiae is that minutiae features are sometimes corrupted by corrosion. But there are disadvantages such as using other features is much dependent on orientation and also has a huge memory requirement for dataset images.

IV. RESULTS OF ILLUSTRATION

In order to demonstrate the fingerprint-recognition process, FVC2002 database is used in our experiments. This database is widely used for illustrating fingerprint-identification works and it comprises of 4 internal databases. The experimental results are encouraging and the database is extensively used by many researchers. A matching and a non-matching results are shown in Table I.

TABLE I
ILLUSTRATIVE RESULTS

	
Input image (103-6 from FVC2002)	Input image (101-7 from FVC2002)
	
Minutiae feature extracted	Minutiae feature extracted
	
Result authenticated	Result NOT authenticated

V. CONCLUSION

In the process of analyzing fingerprint-based authentication systems, multiple works have been considered. The ultimate goal is to understand the needs of fingerprint-based recognition systems and study the merits, demerits and shortfalls of existing systems. It is understood that biometric-templates like fingerprints are highly robust and reliable for the purpose of authentication when compared with passwords, PINs or highly stuffed keys. It is also noted that there exists a significant difference between the fingerprint-samples of a single person captured at different occasions. Thus, the comparison task is considered to be a probabilistic one which is really a vice-versa of strict matching of passwords or keys.

The probabilistic matching may lead to errors like false rejection rate (FRR) and false acceptance rate (FAR) that depend on many influences, specifically, on the matching algorithm. The core of the system is characterized by two main phases: enhancing fingerprint-images and validating the identity of a human-being. Hence, in future, it must be aimed to improve the enhancement process and to build a better identification algorithm with reduced FAR and FRR.

REFERENCES

- [1] Muzhir Shaban Al-Ani. A novel thinning algorithm for fingerprint recognition. *International Journal of Engineering Sciences*, 2(2):43–48, 2013.
- [2] Kai Cao and Anil K Jain. Fingerprint indexing and matching: An integrated approach. In *2017 IEEE International Joint Conference on Biometrics (IJCB)*, pages 437–445. IEEE, 2017.
- [3] Chioma Chigozie-Okwum. Implementation of multifactor based authentication scheme for enhanced atm security. *International Journal of Computer Applications*, 975:8887.
- [4] Tarang Chugh, Kai Cao, and Anil K Jain. Fingerprint spoof buster: Use of minutiae-centered patches. *IEEE Transactions on Information Forensics and Security*, 13(9):2190–2202, 2018.
- [5] Wei Cui, Guoliang Wu, Rongjin Hua, and Hao Yang. The research of edge detection algorithm for fingerprint images. In *2008 World Automation Congress*, pages 1–5. IEEE, 2008.
- [6] Deepak Kumar Karna, Suneeta Agarwal, and Shankar Nikam. Normalized cross-correlation based fingerprint matching. In *2008 Fifth International Conference on Computer Graphics, Imaging and Visualisation*, pages 229–232. IEEE, 2008.
- [7] Manvjeet Kaur, Mukhwinder Singh, Akshay Girdhar, and Parvinder S Sandhu. Fingerprint verification system using minutiae extraction technique. *World Academy of Science, Engineering and Technology*, 46:497–502, 2008.
- [8] Wang Yuan, Yao Lixiu, and Zhou Fuqiang. A real time fingerprint recognition system based on novel fingerprint matching strategy. In *2007 8th International Conference on Electronic Measurement and Instruments*, pages 1–81. IEEE, 2007.
- [9] Bo-wen Zheng, Jie-sheng Wang, Yan-lang Ruan, and Shu-zhi Gao. Recognition method based on gabor wavelet transform and discrete cosine transform. *Engineering Letters*, 26(2), 2018.