DOI: https://doi.org/10.24113/ijoscience.v7i4.386

Application of Machine Learning in Fingerprint Image Enhancement and Recognition: A Review

Kshitij Singh
M.Tech Scholar
Department of CSE
Oriental Institute of Science & Technology
Bhopal, M.P, India

Dr. Gireesh Kumar Dixit
Professor
Department of CSE
Oriental Institute of Science & Technology
Bhopal, M.P, India

Abstract: **Biometric characteristics helps to recognize an individual among others. Each individual has a unique biometric feature. So, an automated system is designed to recognize an individual. In today's growing AI development, biometric recognition is applied in many security systems. One of oldest and widely used authentic biometric methodology is fingerprint recognition. Many fingerprint recognition algorithms are designed and developed in order to reduce error rate and to improve accuracy. In this paper, a comprehensive review is presented on various techniques used for fingerprint recognition system along with their performance and their limitations. The purpose of this paper is to review various recent work on the fingerprint recognition system, to explain step by step the steps for recognizing fingerprints, and to provide summaries of the fingerprint databases with functionality.**

Keywords: **Fingerprint, Pre-processing, Image Enhancement, Machine Learning, Matching.**

I. INTRODUCTION

With advancement of network and multimedia technologies there increases the security threats which leads to development of more secure transmission system. In order to develop such security algorithm, biometrics contributes the most. Conventional protection systems for image content use extrinsic approaches such as watermarks or fingerprints. In many circumstances, protection of extrinsic content is not possible. Therefore, there is a great deal of interest in developing forensic tools that use intrinsic fingerprints to solve these problems [1].

Biometrics can have physiological or behavioral characteristics [2]. The physiological properties are contained in the physical part of the body (such as fingerprints, handprints, iris, face, DNA, hand geometry, retina etc.). Behavioral characteristics are based on an action performed by a person, e.g. B. (speech recognition, key scan and signature scan). Any biometric system comprising two phases is the first phase the registration phase and the second the detection phase. The recognition of a person through his body and the subsequent connection of this body with an "identity" established from the outside constitutes a very powerful tool for identity management with enormous potential positive and negative consequences. Consequently, biometrics is not only a fascinating problem in model recognition research, but if applied with care, it is a technology that can make our society safer, less fraudulent and more user-friendly. Numerous biometric authentication systems have been used, but each type of unimodal biometrics has its disadvantages depending on the characteristics, the recording device, the database and the characteristics of these characteristics [3].

Fingerprints are a popular identifier, but can be easily falsified with false fingerprints sensitive to dirt, moisture and aging [1,2].

Facial recognition depends on facial expression and age [3].

Speech recognition also depends on environmental conditions and is not safe for recorded speech [4].

A step of operations is performed during biometric recognition or while designing such applications. Generally, it is composed of four basic steps or operations which are discussed as below [5]:

i. Sensor: Sensors are any physical devices that has capabilities to sense data. In fingerprint biometrics, fingerprint sensor is used to capture fingerprint images or templates for further processing. The optical devices are inbuilt in such sensors. Sometimes UV technologies are also included but in general fingerprint sensors optical technologies are used.

ii. Feature Extraction: After capturing images from sensor, features such as minutiae's, pores, bifurcation or ridge information are extracted by applying algorithms.

iii. Database: Further, a template or feature containing database is created. This database is basically collection of several individuals fingerprint features along with their class label. This is used during verification or decision-making process. For security reasons, raw data is not stored here.

iv. Decision Making: This operation is performed during verification phase. In this phase fingerprints are matched with stored templates and gives a matching score with all stored feature and output that have highest matching probability is considered to be output.

v. Given the challenges of today's detection system, the time has come to develop a robust single-mode detection system to protect privacy. A comparative evaluation of the most important biometric methods is described in

Table 1. Each mode has its advantages and disadvantages.

Given the challenges of today's detection system, the time has come to develop a robust single-mode detection system to protect privacy. A comparative evaluation of the most important biometric methods is described in Table I. Each mode has its advantages and disadvantages.

TABLE I
COMPARATIVE EVALUATION OF THE BIOMETRIC TECHNOLOGIES

Biometrics	Accuracy	Data Size	Cost	Security Level
Fingerprint	Medium	Small	Low	Low
Face	Low	Large	High	Low
Iris	High	Large	High	Medium
Voice	Low	Small	Mediu m	Low
Hand Geometry	Low	Large	High	Low

II. FINGERPRINT

A fingerprint contained many types of small things such as the tip of the comb, the fork, the bow, the double ring, the vortex, the right ring, the left ring, the short comb, the spur, the core, the delta, the islet, etc. [2].

Figure 1. Samples of Fingerprint

There are several approaches for fingerprint verification. Some of them are used in crime scene detection. Others use minutiae that join devices; and others are a bit more unique, including things like moiré stripe patterns and ultrasound properties. A wider range of fingerprint devices is available than any other biometric technology [6]. Fingerprint systems translate illuminated fingerprint images into digital code for other software such as registration (fingerprint registration) and verification (authentication or verification of registered users). The scanner uses an advanced CMOS image sensor to acquire high contrast and high contrast fingerprint images that are practically undistorted. A series of powerful algorithms extracts the image data and maps the distinctive characteristics of the fingerprint.

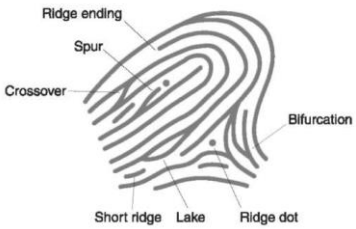

Fig. 2. Features of Fingerprint

III. FINGER PRINT RECOGNITION

A fingerprint shows the patterns on the fingertips. There are several approaches for fingerprint verification. Some emulate the traditional police method of matching models. Others are currently using minute matching devices; and others are more unique, including moiré stripe patterns and ultrasound. There is a greater selection of fingerprint devices than any other biometric device [4]. Fingerprint verification can be a good choice for internal systems where adequate explanations and training can be provided to users and where the system is used in a controlled environment.

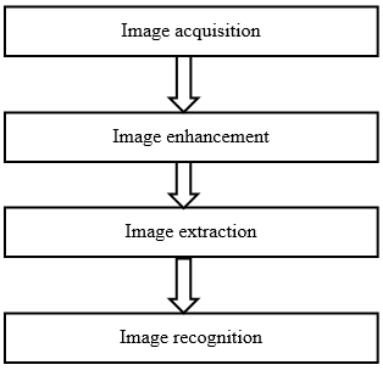

Fig. 3 Steps to identify fingerprint image

A. Image acquisition

The image sensor acquires digital images in relation to the problem area. First of all, it is a physical device sensitive to the energy emitted by the object. The second, called a digitizer, is a device for converting the output of the physical acquisition device into figures [5]. Specialized image processing equipment consists of the digitizer and equipment that performs other primitive operations. The computer is an image processing system that runs from a PC to a supercomputer. The image processing software consists of special modules that perform certain activities. Mass storage capacity is a must in image processing applications.

B. Image Enhancement

The purpose of this phase is to provide a high-quality image. A good quality fingerprint image has a high contrast between ridges and valleys. Poor quality fingerprint image is low contrast, noisy, broken or complacent, which leads to small wrong and missing things. Techniques such as grayscale

leveling, contrast stretching, histogram compensation and Wiener filter can be used as preprocessing steps before applying a sophisticated fingerprint enhancement algorithm. The purpose of an enhancement algorithm is to improve the clarity of the peak structures in a fingerprint. The image is analyzed in local neighborhoods to estimate the ridge model attributes such as ridge width, alignment and noise and image quality.

C. Feature Extraction

Once a sharp image is acquired, the characteristics of the minutia, as well as their attributes and relationships, can be extracted from the image. The whole process is divided into three phases:

- Thinning the structure of the reconstructed binary peak that is obtained after the improvement of the image.
- The elimination of all structural defects of the diluted image.
- Extraction of minutiae.

D. Pattern Recognition

A model is an arrangement of descriptors. It is characterized by the order of the elements that compose it, rather than by the nature of these elements. Recognition of the model is divided into two main areas: decision theory and structure. Decision theory treats the models described using quantitative descriptors, such as length, area and plot. The structural category deals with models best described by qualitative descriptors, such as relational descriptors [6].

The recognition of machine models involves techniques to assign the models to their respective classes, automatically and with the least human intervention possible. Three common patterns used in practice are vectors, chains and trees. The recognition process aims to determine whether fingerprint patterns were produced by the healthy finger or not.

The patterns are lined up before pairing the fingerprints. Then, a score is defined to measure the similarity between two models. The simplest approach is the minimum distance classifier which, as the name suggests, calculates the distance between the unknown and each of the prototype vectors [7]. The elastic technique used allows a certain margin of adaptive spatial tolerance to compensate for nonlinear elastic formations.

Some of the contribution of different researchers are illustrated in table II.

IV. MEASURING BIOMETRIC EFFECTIVENESS

There are two commonly used methods for measuring the effectiveness of biometrics matching technology.

1. False Rejection Rate (FRR) as known as False Non-Match Rate (FNMR). FRR is a value that measures the frequency with which a biometric sample is associated with one or more biometric models if a biometric model is available, but the similarity between the sample and the model is less than the specified decision threshold, therefore none occurs. In other words, it is the frequency with which people are not identified when they should be identified.
2. False Accept Rate (FAR) also known as False Match Rate (FMR). FAR is a value that measures the percentage of correspondence of a biometric sample with one or more biometric models when there is no biometric model, but the similarity between the sample and the model is greater than the decision threshold, which translates into a delay.

TABLE II
REVIEW ON FINGRPRINT RECOGNITION TECHNIQUES

Ref.	Technique Used	Enhancement Used	Classifier Used	Result	Limitations
[8]	Wavelet transform and singular value decomposition	Wavelet Filter	-	Accuracy = 95%	Need to decompose the singular value.
[9]	Supervised Neural Network and minimum distance features between singularities for fingerprint	Hong's Algorithm	Neural Network	EER = 5.1%	Needs sufficient number of training set and improvement in EER.
[10]	Fuzzy based fingerprint enhancement technique based on adaptive thresholding	Fuzzy logic based on thresholding	-	PSNR = 38.24	Requires defuzzy

[11]	Contrast Enhancement	Block wise histogram equalization based on gap detection and gap similarity measures	-	Similarity measure = 0.88	Random detection rate
[12]	Rule based classifier for flat fingerprints with missing singular point	-	Rule based	Accuracy = 91%	Needs additional Rules for enhancement of image
[13]	Deep neural network	-	Convolution neural network	Accuracy = 90% (wet fingerprint)	Accuracy rate is quite low in dry and blurred condition
[14]	Fingerprint image enhancement processing for impulse noise removal	Adaptive Median Filter	-	PSNR= approx. 38	With increase in impulse noise there is steep decrease in PSNR value
[15]	Fingerprint liveness detection using deep learning		Deep Residual Convolutional Neural Network	Accuracy = 97%	Computational complexity of network is high.
[16]	Enhancement based on super resolution	Deep Convolution Neural Network (DCNN)	-	-	Need More exploration for classification

V. CONCLUSION

Fingerprint recognition is a very reliable recognition system. The above implementation was an attempt to understand how fingerprint recognition is used as a form of biometrics to recognize human identity.

It includes all stages, from extracting minutiae from fingerprints to comparing minutiae, which generates an evaluation of correspondence. In this paper, different approaches used in fingerprint recognition are reviewed and analyzed. After reviewing these research works, several factors can be identified which have further scope for advancement. These factors include, type of data, image enhancement techniques, noise removal, minutiae extraction, etc. By applying advancement to these factors leads to improvement in system performance and accuracy rate.

REFERENCES

[1] Mouad .M.H.Ali, Vivek H. Mahale "Overview of Fingerprint Recognition System" *International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT)*, pp. 1334- 1338, 2016.

[2] Umesh Singh Tomar, Abhinav Vidwans "A Review of Fingerprint Recognition by Minutiae's Analysis" International Journal of Engineering and Information Systems (IJEAIS), Vol. 1 Issue 8, pp. 182-185, October 2017.

[3] Priyanka Rani, IIPinki Sharma "A Review Paper on Fingerprint Identification System" *International Journal of Advanced Research in Computer Science & Technology (IJARCST 2014)* Vol. 2, Issue 3 July - Sept. 2014.

[4] Ritu, Matish Garg "A Review on Fingerprint-Based Identification System" *International Journal of Advanced Research in Computer and Communication Engineering*, Vol. 3, Issue 3, March 2014.

[5] Cynthia D'Souza N , Leeda Jovita Rodrigues "A Survey On Fingerprint Recognition Techniques" *International Journal of Latest Trends in Engineering and Technology Special Issue SACAIM*, pp. 441-447, 2016.

[6] R. Kumar, B.R.D. Vikram, "Fingerprint matching using multidimensional ann", *Eng. Appl. Artif. Intell*. Vol. 23 pp. 222–228, 2010.

[7] Khalil-Hani, Mohamed, Muhammad N. Marsono, and Rabia Bakhteri. "Biometric encryption based on a fuzzy vault scheme with a fast chaff generation algorithm." *Future Generation Computer Systems* vol. 29, issue 3 pp. 800-810, 2013.

[8] Jing-Wein Wang, Ngoc Tuyen Le, Chou-Chen Wang, and Jiann-Shu Lee, "Enhanced Ridge Structure For Improving Fingerprint Image Quality Based On A Wavelet Domain," *IEEE Signal Processing Letters*, Vol. 22, No. 4, pp. 390-395, April 2015.

[9] AlaBalti , MounirSayadi and Farhat Fnaiech, "Supervised Neural Network And Minimum Distance Features Between Singularities For Fingerprint Verification," 2013 10th *IEEE International MultiConference On Systems, Signals & Devices (Ssd) Hammamet*, Tunisia, March 18-21, 2013.

[10] M. Selvi and Aloysius George, "FBFET: Fuzzy Based Fingerprint Enhancement Technique based on Adaptive Thresholding," *ICCCNT* – 2013.

[11] Gang Cao, Yao Zhao, Rongrong Ni, and Xuelong Li, "Contrast Enhancement-Based ForensicsIn Digital Images", *IEEE Transactions On Information Forensics And Security*, Vol. 9, No. 3, pp. 515-526, March 2014.

[12] Leandra Webb and Mmamolatelo Mathekga, "Towards A Complete Rule-Based Classification Approach for Flat Fingerprints," *IEEE Second International Symposium On Computing And Networking*, 978- 1-4799-4152-0/14, pp. 549-556, 2014.

[13] P. Tertychnyi, C. Ozcinar and G. Anbarjafari, "Low-quality fingerprint classification using deep neural network," in IET Biometrics, vol. 7, no. 6, pp. 550-556, 11 2018.

[14] K. Han, Z. Wang and Z. Chen, "Fingerprint Image Enhancement Method based on Adaptive Median Filter," 2018 24th Asia-Pacific Conference on Communications (APCC), Ningbo, China, 2018, pp. 40-44.

[15] Y. Zhang, D. Shi, X. Zhan, D. Cao, K. Zhu and Z. Li, "Slim-ResCNN: A Deep Residual Convolutional Neural Network for Fingerprint Liveness Detection," in *IEEE Access*, vol. 7, pp. 91476-91487, 2019.

[16] A. Muhammed and A. R. Pais, "A Novel Fingerprint Image Enhancement based on Super Resolution," *International Conference on Advanced Computing and Communication Systems (ICACCS)*, Coimbatore, India, 2020, pp. 165-170.