Asian J. of Adv. Basic Sci.: 2(3), 50-56
ISSN (Online): 2347 - 4114
www.ajabs.org

Biometrics and Fingerprint Matching: A Study

Neha Walia

Department of Computer Science, St. Bede's College, Shimla (H.P.) INDIA
Email ID: walia04neha@gmail.com

ABSTRACT: "The future is in the palm of your hand." With the proliferation of biometric technology, it has never been truer. The future really is in the palm of your hand, but did you know it's also in the pattern of your iris, the minutiae of your fingerprint, and the structure of your face? Biometric recognition, or simply biometrics or life metrics, are base for a plethora of highly secure identification and personal verification solutions . A biometric system is fundamentally a pattern recognition system that recognizes a person by determining the authentication by using his different biological features i.e. Fingerprint, retina-scan, iris scan, hand geometry, and face recognition are leading physiological biometrics and behavioral characteristic are Voice recognition, keystroke-scan, and signature-scan. By using biometrics, iris possible to confirm or establish an individual's identity based on "who he/she is," rather than by "what he/she possesses" (e.g., an ID card) or "what he/she remembers" (e.g., a password). Fingerprint matching has been successfully used by law enforcement for more than a century. The technology is now finding many other applications such as identity management and access control. The papers give a brief overview of the field of biometrics, describe an automated fingerprint recognition system and identify key challenges in the field.

Key field: Biometrics, biometric techniques, identification, verification, fingerprint recognition.

INTRODUCTION

Biometrics is automated methods of recognizing a person based on a physiological or behavioral characteristic [1]. Biometric technique is now becoming the foundation of a wide array of highly secure identification and personal verification. As the level of security breach and transaction scam increases, the need for well secure identification and personal verification technologies is becoming apparent. There have different types of biometrics: Some are old or others are latest technology. Biometrics identify people by measuring some aspect of individual anatomy or physiology, some deeply ingrained skill, or other behavioural characteristic, or something that is a of the two . Biometric authentication technologies such as face, finger, hand, iris, skull ,odour, voice, gait recognition are commercially available today and are already in use[2]. A biometric system is essentially a pattern recognition system that operates by acquiring biometric data from an individual, extracting a feature set from the acquired data, and comparing this feature set against the template set in the database. Depending on the context, a biometric system may operate either in verification mode or identification mode: [3]

a) In the verification mode, the system validates a person's identity by comparing the captured biometric data with her own biometric template(s) stored in the system database.
b) In the identification mode, the system recognizes an individual by searching the templates of all the users in the database for a match.

FINGERPRINT RECOGNITION

Henry Faulds, Francis Galton, and Edward Henry, among others, established the scientific basis for using fingerprints as a method for person identification in the late 19th century. Since then, law enforcement agencies worldwide have employed fingerprint recognition for two main purposes:

a) Establish the identity of a suspect (or victim) based on partial prints, or *latents*, left at a crime scene.

b) Identify repeat offenders based on prints of all of their fingers (using 10 prints improves matching accuracy).

The main reasons for the popularity of fingerprint recognition are

a) Its success in various applications in the forensic, government, and civilian domains.
b) The fact that criminals often leave their fingerprints at crime scenes.
c) The existence of large legacy databases.
d) The availability of compact and relatively inexpensive fingerprint readers.

FRICTION RIDGE PATTERNS

Figure 1: Major Fingerprint pattern types: (a) loops, (b) whorls, and (c) arches

The overall pattern of the fingerprint is governed by the shape, size, and placement of volar pads[4.] Higher and symmetric volar pads tend to generate *whorls*, flatter and symmetric volar pads tend to generate *arches*, and asymmetric volar pads tend to generate *loops* as Figure 1 shows. Identification of the pattern type can facilitate faster search in large-scale fingerprint-recognition applications.

AUTOMATED FINGERPRINT RECOGNITION

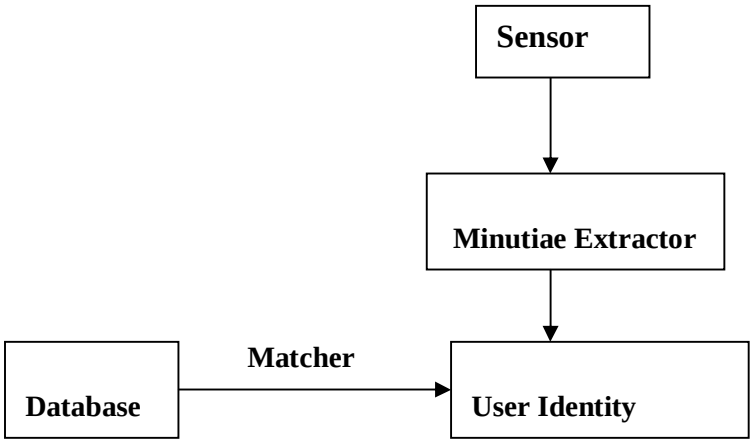


Figure 2: outlines a typical automated fingerprint recognition system.

During the *enrollment phase*, the sensor scans the user's fingerprint and converts it into a digital image. The minutiae extractor processes the fingerprint image to identify specific details known as *minutia points* that are used to distinguish different users. Minutia points represent locations where friction ridges end abruptly or where a ridge branches into two or more ridges. A typical good-quality fingerprint image contains about 20-70 minutiae points; the actual number depends on the size of the sensor surface and how the user places his or her finger on the sensor. The system stores the minutiae information—location and direction—along with the user's demographic information as a template in the enrollment database.

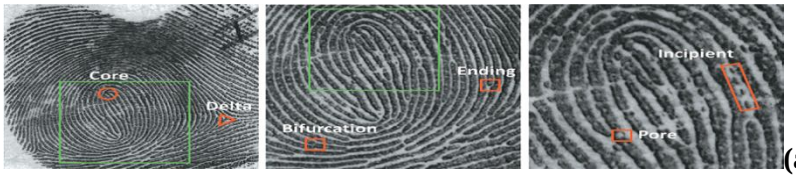
During the *identification phase*, the user touches the same sensor, generating a new fingerprint image called a *query print*. Minutia points are extracted from the query print, and the matcher module compares the query minutia set with the stored minutia templates in the enrollment pressure applied on the sensor,

the minutia points extracted from the template and query fingerprints must be aligned, or registered, before matching. After aligning the fingerprints, the matcher determines the number of pairs of matching minutiae—two minutia points that have similar location and directions. The system determines the user's identity by comparing the match score to a threshold set by the administrator.

Sensing: Fingerprints can be sensed using the traditional "ink and paper" method also called as offline technique [5], still used involves applying ink to the finger surface, rolling the finger from one side of the nail to the other on a card, and finally scanning the card to generate a digital image.or popular *live-scan* method, in which a digital image is directly obtained by placing the finger on the surface of a fingerprint reader.

Feature Extraction: Features extracted from a fingerprint image are generally categorized into three levels, as shown in Figure 3a. Level 1 features capture macro details such as friction ridge flow, pattern type, and singular points. Level 2 features refer to minutiae such as ridge bifurcations and endings. Level 3 features include all dimensional attributes of the ridge such as ridge path deviation, width, shape, pores, edge contour, and other details, including incipient ridges, creases, and scars. [6]

Level 1 features can be used to categorize fingerprints into major pattern types such as arch, loop, or whorl; level 2 and level 3 features can be used to establish a fingerprint's individuality or uniqueness. Higher-level features can usually be extracted only if the fingerprint image resolution is high. For example, level 3 feature extraction requires images with more than 500-ppi resolution.



(a)

(b)

Figure 3: Feature extraction. (a) Feature levels in a fingerprint. Note that the second and third images are magnified versions of the fingerprint regions indicated by green boxes in the corresponding preceding images. (b) Flow chart of a typical minutiae feature extraction algorithm.

Figure 3b shows the flow chart of a typical minutiae feature extraction algorithm. First, the algorithm estimates the friction ridge orientation and frequency from the image. Based on these values, it then performs contextual filtering to improve the image quality and facilitate ridge extraction. The algorithm then obtains binary ridge skeletons from the enhanced image by tracing the ridge lines. Ridge endings and bifurcation points are obtained from the ridge skeleton and referred to as minutiae. The algorithm employs some heuristic rules to detect and remove spurious minutiae resulting from an imperfect skeleton image.

Matching: A fingerprint matching module computes a match score between two fingerprints, which should be high for fingerprints from the same finger and low for those from different fingers. Fingerprint matching is a difficult pattern-recognition problem due to large intraclass variations (variations in fingerprint images of the same finger) and large interclass similarity (similarity between fingerprint images from different fingers). Intraclass variations are caused by finger pressure and placement—rotation, translation, and contact area—with respect to the sensor and condition of the finger such as skin dryness and cuts. Meanwhile, interclass similarity can be large because there are only three types of major fingerprint patterns (arch, loop, and whorl).

Most fingerprint-matching algorithms adopt one of four approaches: image correlation, phase matching, skeleton matching, and minutiae matching. Minutiae-based representation is commonly used, primarily because

- Forensic examiners have successfully relied on minutiae to match fingerprints for more than a century
- Expert testimony about suspect identity based on mated minutiae is admissible in courts of law.

Performance: A fingerprint matcher can make two types of errors: a *false match*, in which the matcher declares a match between images from two different fingers, and a *false nonmatch*, in which it does not identify images from the same finger as a match. A system's false match rate (FMR) and false nonmatch rate (FNMR) depend on the operating threshold; a large threshold score leads to a small FMR at the expense of a high FNMR. For a given fingerprint matching system, it is impossible to reduce both these errors simultaneously.

Fingerprint identification system performance is measured in terms of its *false positive identification rate* (FPIR) and *false negative identification rate* (FNIR). A false positive identification occurs when the system finds a hit for a query fingerprint that is not enrolled in the system. A false negative identification occurs when it finds no hit or a wrong hit for a query fingerprint enrolled in the system. The relationship between these rates is defined by FPIR = 1 - (1 - FMR)^{N}, where N is the number of users enrolled in the system. Hence, as the number of enrolled users grows, the fingerprint matcher's FMR needs to be extremely low for the identification system to be effective.

CHALLENGES

Numerous challenging problems in fingerprint recognition are there. The ever-increasing demand for reducing the error and failure rates of automated fingerprint recognition systems and the need for enhancing their security have opened many interesting research opportunities that encompass multiple domains such as image processing, computer vision, statistical modeling, cryptography, and sensor development.

New Sensors: The physical shape of fingers makes it difficult to capture a complete fingerprint pattern using touch-based sensors. In law enforcement applications, multiple impressions of the same finger are often recorded to obtain good-quality complete images of all the fingers. As most touch-based sensors are based on directly measuring the finger surface, they have difficulty sensing the fingerprints of elderly persons, whose fingerprints tend to be flattened, and manual laborers, whose fingerprints may contain many cuts. Rolling and improper pressure while using touch-based sensors also introduce distortion in the sensed images.

Low-Quality Images: Due to nonideal skin conditions, inherently low-quality fingers, and sensor noise, a significant percentage of fingerprint images are of poor quality. Extracting features from and matching low-quality fingerprints, like those shown in Figures 5a and 5b, is a challenging problem . In many government and forensic applications, human experts are available to encode low-quality fingerprints and verify associated hits found by the automated fingerprint recognition systems. In situations where human intervention is expensive or inconvenient, or fingerprints are unusable, a possible solution is *multibiometrics*[7] ,the fusion of multiple biometric traits such as fingerprint, palmprint, face, iris, and voice.

Small overlapping area and nonlinear distortion: Fingerprint sensors embedded in consumer electronic devices tend to have a smaller sensing area. This factor, combined with users improper placement of their finger on the sensor, results in a limited overlapping area between two impressions of the same finger, as Figure 5c shows. Given the very small number of minutiae in the overlapping area, it is difficult to determine if two fingerprints are from the same finger.

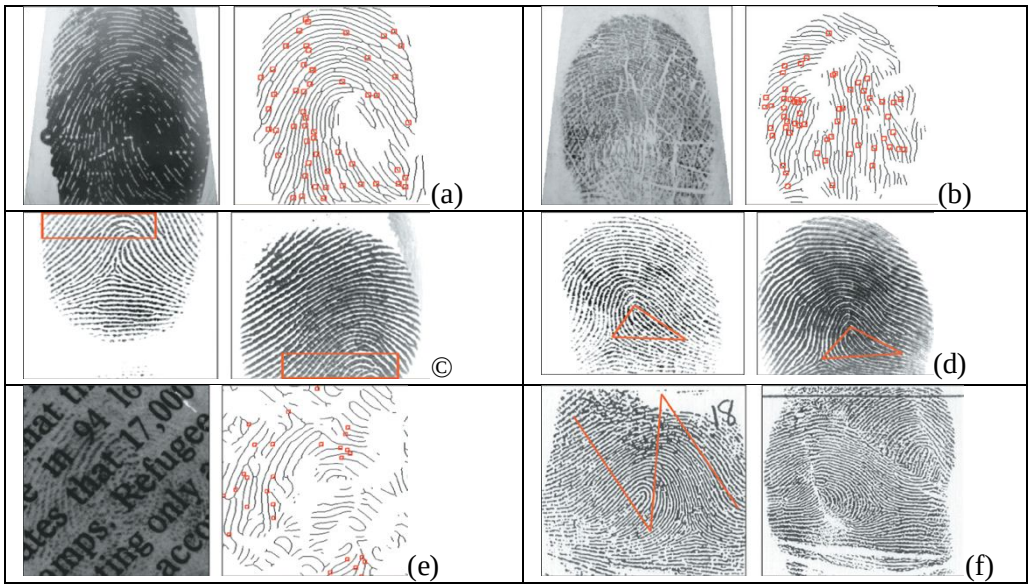


Figure 4: Challenges in automated fingerprint processing: (a) wet fingerprint (left) and extracted features (right); (b) fingerprint with many cuts (left) and extracted features (right); (c) small overlapping area as marked by rectangles; (d) large nonlinear distortion in fingerprint patterns as indicated by the corresponding triangles; (e) latent fingerprint with overlapping letters (left) and the extracted features (right); (f) altered fingerprint: a criminal made a Z-shaped incision into each of his fingers (left), switched two triangles, and stitched them back into the finger (right).[5]

One way to alleviate this problem is to utilize level 3 features to improve the matching accuracy in cases where there is only a small overlapping area between the two impressions. However, level 3 features may not be suitable for commercial applications because the sensors used in such applications usually provide only low-resolution images. A more feasible solution may be *fingerprint mosaicking*, which combines multiple smaller images into a larger image, and more ergonomic and intuitive interfaces that can guide users to properly place the central (pattern) area of their finger on the sensor.

Pressing soft finger skin on a sensor always introduces some distortion, which is generally not repeatable. Matched fingerprints may appear very different under severe distortion, as Figure 5d shows. Ergonomic sensors and appropriate feedback to users can alleviate this problem. Another option is to match fingerprints locally—for example, using local minutiae descriptors4—before aggregating these local matches globally.

Latent Fingerprints: Latent fingerprints generally suffer from low image quality, small overlapping area, and nonlinear distortion as well as the presence of a complex background, as Figure 5e shows. To overcome this problem, current automated fingerprint ID systems require extensive manual intervention in latent encoding (feature extraction) and in verifying a candidate list returned by the system. With the increase in latent matching transactions for civilian, law enforcement, and homeland security applications, automated latent processing and matching are receiving more attention.

Altered/Fake Fingerprints: People may alter their fingerprints in different ways for many reasons. For example, an unauthorized user may use a fake finger that imitates a legitimate user's fingerprint template to access a computer system. Criminals may cover their fingers with fake fingerprints made of substances like glue or they may intentionally mutilate their fingers to avoid being identified by automated systems or even human experts, as Figure 5f shows.

An essential counter measure to thwart the use of inanimate or fake fingers is *liveness detection*—checking if the finger is "live" by measuring and analyzing various vital signs of the finger such as pulse, perspiration, and deformation. While software-based liveness detection solutions that complement existing fingerprint scanners may be more cost-effective, they have not yet shown much promise.

Interoperability: Interoperability problems can occur in all three main modules of a fingerprint recognition system: sensor, feature extractor, and matcher. Different sensors may output images that exhibit variations in resolution, size, distortion, contrast, background noise, and so on. Different encoders may extract different features or adopt varying definitions of the same feature. This diversity makes it difficult to build a fingerprint system with principal components sourced from different vendors.

System on device: An important security issue in fingerprint recognition systems is the tampering or modification of the hardware/software components and interception of fingerprint data passing through the communication channels—for example, the wireless interface between a passport reader and the chip on a passport that contains the user's fingerprint template. This problem can be overcome by employing system-on-device technology in which the sensor, feature extractor, matcher, and even the templates reside on a tamper-resistant device.

Figure 5: Cancellable fingerprint. Applying a noninvertible mathematical transformation to the fingerprint template on the left produces the template on the right. Even if the transformed template is revealed, the real fingerprint cannot be gleaned easily.

5.8. Template Security: While system-on-device technology may be a useful security measure in verification applications, fingerprint ID systems require centralized storage of fingerprint information in large enrollment databases. The unauthorized use or disclosure of fingerprint template information from such databases constitutes a serious security and privacy threat. Not only can a stolen fingerprint template be reverse-engineered to construct a fake finger[8] or replayed into the system, it can be used for cross-matching across different databases to covertly track people without their consent, thereby compromising their privacy Another issue is that unlike credentials such as passwords or ID cards that can be easily revoked and reissued, people cannot arbitrarily replace their fingerprint template—disclosure of fingerprint information results in permanent loss. Two strategies have been proposed to secure fingerprint templates. A) cancellable fingerprint, as Figure 6 shows. B) biometric cryptosystems.

CONCLUSION

Automated fingerprint identification systems have been successfully deployed around the globe and new fingerprint-matching applications continue to emerge. The fingerprint biometric is the dominant biometric trait, and many identity management and access control applications will continue to rely on fingerprint recognition because of its proven performance, the existence of large legacy databases, and the availability of compact and cheap fingerprint readers. Further, fingerprint evidence is acceptable in courts of law to convict criminals.

While fingerprint recognition technology has been under development for nearly half a century, new research problems have accompanied the wide deployment of fingerprint technology.. Issues such as fingerprint recognition at a distance, real-time identification in large-scale applications with billions of fingerprint records, developing secure and revocable fingerprint templates that preserve accuracy, and scientifically establishing the uniqueness of fingerprints will likely remain as grand challenges in the near future.

REFERENCES

1. Bhatia Rana(2013),Biometrics and face recognition techniques, *International Journal of Advanced Research in Computer Science and Software Engineering* ,3(5), 93-99.
2. Fernando L. Podio: "Personal Authentication Through Biometric Technologies"
3. Anil K. Jain, Arun Ross and Salil Prabhakar (2004) "An Introduction to Biometric Recognition" IEEE Transactions on Circuits and Systems for Video Technology, Special Issue on Image- and Video-Based Biometrics, Vol. 14,No. 1.
4. M. Kücken and A.C. Newell (2005), "Fingerprint Formation," *J. Theoretical Biology*, 235(1), 71-83.
5. Maltano David,MaioDario,Jain A.K., Prabhakhar S, "Hankbook of Fingerprint Recognition",Springer,2nd ed.
6. JainA.K,, Feng Jianjiang Nandakumar Karthik (2010) , "Fingerprint Matching",*IEEE*.
7. Ross A.A. Nandakumar K. and. Jain A.K. (2006), *Handbook of Multibiometrics*, *Springe*r.
8. R. Cappelli et al.(2007), "Fingerprint Image Reconstruction from Standard Templates," *IEEE Trans. Pattern Analysis and Machine Intelligence*, 1489-1503.
9. http://e2e.ti.com/blogs_/b/thinkinnovate/archive/2012/11/07/the-future-of-biometrics-technology.aspx.