Indian Journal of Information Sources and Services
ISSN: 2231-6094 (P) Vol.2 No.1, 2012, pp.34-37

DOI: https://doi.org/10.51983/ijiss.2012.2.1.348

Use of Fingerprint Recognition Systems in Libraries

S.Srinivasa Raghavan[1] and G.Sivakumar[2]
[1] *Department of Library and Information Science, Bharathidasan University, Trichirappalli - 620 024, Tamil Nadu, India*
[2]*Librarian, P.S.N.A College of Engineering and Technology, Dindigul - 624 622, Tamil Nadu, India*
E-mail : maduraiseenoo@yahoo.co.in,sivawins@gmail.com

(Received on 15 November 2011 and accepted on 18 March 2012)

Abstract **- This paper describes a comparative study on fingerprint recognition systems. The use of fingerprints for identification has been employed in law enforcement for about a century. A much broader application of fingerprints is for personal authentication, for instance to access a computer, a network, a bank-machine, a car, or a home. The following topics are covered: history, minutia types, image processing and methods, minutia extraction, enrollment and verification procedures, recognition rate, combination with other biometrics, and the future of fingerprint recognition system. AFIS is dramatically improving in the last decade. It can use in Library and Information Center for providing better security. The application of AFIS in Library and Information Center will protect from thief, mutilation of library materials and other unethical losses.**

Keywords: **Biometric, Fingerprint Alignment, Fingerprint Image Recognition, Fingerprint Verification, Image Enhancement, Minutia Extraction.**

I. Introduction

Library is a 'temple of learning', which play an important role in the development of an institutes and society. Library is not always safe and secure place. Books are often found on the library shelves with pages torn from the spine. Sometimes books are damaged beyond repair and almost all academic libraries are suffering from book or document theft by its member. So librarian need to aware from theft, mutilation of library materials and other unethical losses. The duty of the librarian is to keep the library buildings, shelves and stacks open and free without losing items to make available or putting individuals at unacceptable risk from the malicious, avaricious or senseless act of others. It is important to provide a safe and secure environment for library staff, library resources and equipment, and library users. In this regard, the fingerprint identification system is really useful for the library and information science professional. Biometric fingerprint recognition systems are the most commonly used biometric technology due to their long tradition. Fingerprint identification systems have been developed for more than hundred years and the identification of persons through their unique fingerprint is widespread in criminal investigations. The use of fingerprints as a biometric is both the oldest mode of computer-aided, personal identification and the most prevalent in use today. This paper contains an overview of fingerprint recognition system and related issues. We first describe fingerprint history and terminology. Digital image processing methods are described that take the captured fingerprint from a raw image to match result. Systems issues are discussed including procedures for enrollment, verification, spoof detection, and system security.

II. History Of Fingerprint Technology

There is archaeological evidence that fingerprints as a form of identification have been used at least since 7000 to 6000 BC by the ancient Assyrians and Chinese. In the mid-1800's scientific studies were begun that would established two critical characteristics of fingerprints that are true still to this day: no two fingerprints from different fingers have been found to have the same ridge pattern, and fingerprint ridge patterns are unchanging throughout life. These studies led to the use of fingerprints for criminal identification, first in Argentina in 1896, then at Scotland Yard in 1901, and to other countries in the early 1900's. Computer processing of fingerprints began in the early 1960s with the introduction of computer hardware that could reasonably process these images. Since then, automated fingerprint identification systems (AFIS) have been deployed widely among law enforcement agencies throughout the world. Now, in the late 1990s, the introduction of inexpensive fingerprint capture devices and the development of fast, reliable matching algorithms has set the stage for the expansion of fingerprint matching to personal use. Thus there is the experience of a century of forensic use and hundreds of millions of fingerprint matches by which we can say with some authority that fingerprints are unique and their use in matching is extremely reliable [1].

III. MINUTIA TYPES

The lines that flow in various patterns across fingerprints are called ridges and the spaces between ridges are valleys. It is these ridges that are compared between one fingerprint and another when matching. Fingerprints are commonly matched by one (or both) of two approaches. We describe the fingerprint features as associated with these approaches.

The more microscopic of the approaches is called minutia matching. The two minutia types that are shown in Figure 1 are

a ridge ending and bifurcation. An ending is a feature where a ridge terminates. A bifurcation is a feature where a ridge splits from a single path to two paths at a Y-junction. For matching purposes, a minutia is attributed with features. These are type, location (x, y), and direction (and some approaches use additional features).

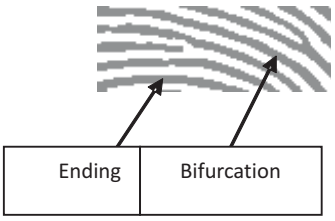

Fig. 1 Fingerprint minutiae: ending and bifurcation

IV. Image Processing And Verification

The ultimate objective of image processing is to achieve the best image by which to produce the correct match result. The image processing steps are the following: image alignment, image noise reduction and enhancement, feature detection, and matching. This section is organized to describe first the sequence of processing and verification via a "common" minutia-based approach.

A. Image Specifications/Acquisition

Depending upon the fingerprint capture device, the image can have a range of specifications. Commonly, the pixels are 8-bit values, and this yields an intensity range from 0 to 255. The image resolution is the number of pixels per unit length, and this ranges from 250 dots per inch (100 dots per centimeter) to 625 dots per inch (250 dots per centimeter), with 500 dots per inch (200 dots per centimeter) being a common standard. The image area is from 0.5 inches square (1.27 centimeter) to 1.25 inches (3.175 centimeter), with 1 inch (2.54 centimeter) being the standard.

B. Image Registration / Alignment

The captured image is registered or aligned first. This is an important process before image enhancement. For image alignment we can use Mutual information technique or any other clustering based algorithm. The aligned image takes very less time for matching.

C. Image Enhancement

A fingerprint image is one of the noisiest of image types. This is due predominantly to the fact that fingers are our direct form of contact for most of the manual tasks we perform: finger tips become dirty, cut, scarred, creased, dry, wet, worn, etc. The image enhancement step is designed to reduce this noise and to enhance the definition of ridges against valleys. The registered image must be enhanced before extracting the minutia points. We can use few image enhancement techniques like image histogram, Fast Fourier Technique, Gabor filter technique etc. *T*he stages of image enhancement, feature detection, and matching are illustrated in Figure 2. Image enhancement is a relatively time-consuming process.

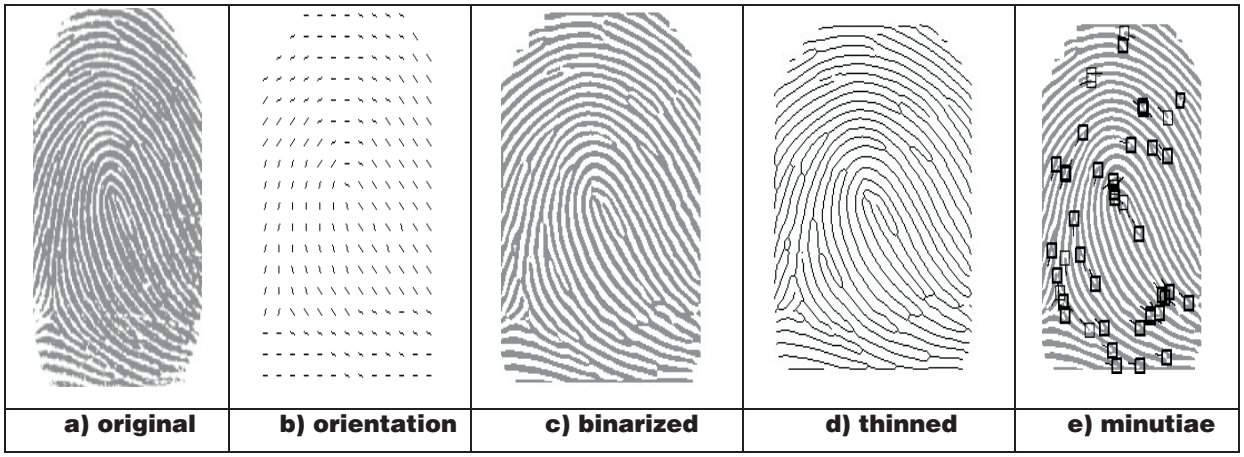

Fig. 2 Sequence of fingerprint image processing steps

V. Minutia Extraction

The fingerprint minutiae are found at the feature extraction stage. Operating upon the thinned image, the minutiae are straight forward to detect. Endings are found at termination points of thin lines. Bifurcations are found at the junctions of three lines. See Figure 2(e).

The result of the feature extraction stage is what is called a minutia template. This is a list of minutiae with accompanying attribute values. An approximate range on the number of minutiae found at this stage is from 10 to 100. If each minutia is stored with type (1 bit), location (9 bits each for x and y), and direction (8 bits), then each will require 27 bits – say 4 bytes – and the template will require up to 400 bytes.

VI. Verification

At the verification stage, the template from the claimant fingerprint is compared against that of the enrolled fingerprint. This is done usually by comparing neighborhoods of nearby minutiae for similarity. A single neighborhood may consist of three or more nearby minutiae. One result of the verification stage is a match score, usually a number between 0 and 1 (or 10 or 100). Higher values in the range indicate higher confidence in a match. This match score is then subject to a user-chosen threshold value. If the score is greater than the threshold, the match result is said to be true (or 1) indicating a correct verification, otherwise the match is rejected and the match result is false (or 0). This threshold can be chosen to be higher to achieve greater confidence in a match result, but the price to pay for this is a greater number of false rejections. Since one of the most vexing challenges of fingerprint processing is obtaining a clean image upon which to perform matching, there are various methods proposed to perform image enhancement. Most of these involve filtering that is adaptively matched to the local ridge orientations [2,3,4,5,6,7,8,9].

VII. Recognition Rate

The ultimate measure of utility of a fingerprint system for a particular application is recognition rate. This can be described by two values. The false acceptance rate (FAR) is the ratio of the number of instances of pairs of different fingerprints found to (erroneously) match to the total number of match attempts. The false rejection rate (FRR) is the ratio of the number of instances of pairs of the same fingerprint are found not to match to the total number of match attempts. FAR and FRR trade off against one another. That is, a system can usually be adjusted to vary these two results for the particular application, however decreasing one increase the other and vice versa.

VIII. Multi-modal Biometrics

Multi-modal biometrics refers to the combination of two or more biometric modalities into a single system. The most compelling reason to combine different modalities is to improve recognition rate. The different modalities listed in Table I, it is likely that each is largely independent from the other. Fingerprint and eye features remain consistent for a lifetime, whereas the others change with growth.

Table I Features Of Different Biometric Modalities

Biometric	Matching 1-to-1, 1-to-many	Variation: Lifetime, Day-to-Day	Maximum Independent Samples per Person	Sensor Size
Fingerprint	Yes, Yes	None, Little	10	Very Small
Eye	Yes, Yes	None, Very Little	2	Medium
Hand	Yes, No	Much , Very Little	2	Medium
Face	Yes, No	Much, Medium	1	Small
Voice	Yes, No	Much, Medium	1	Very Small
Signature	Yes, No	Much, Medium	1	Medium

IX. Control Access To Library Books

Implementation of fingerprint as a library borrower cards will be one of the positive steps to make library a digital environment. Every applicant of library cards will get enrollment of their fingerprint image and get stored in the database. And at the time to borrow book, the person need to scan their fingerprint in the fingerprint scanner. If the fingerprint is matched with the template in the database, the person can be allowed to borrow book from the library because fingerprint is unique to every individual. This will release the burden of forgetting, stealing and missing of library cards. Introducing a fingerprint as a library card will reduce the workload of making cards of each and every authorized member.

X. Limitation And Problems Of Fingerprint Application

Though the biometrics technology provides a number of advantages, there are some disadvantages too.The following are a select list of problems associated with the system.

1. Fingerprint Identification System is inherently individuating and interface easily to database technology, making privacy violation easier and more damaging.
2. Fingerprint Identification System are useless without a well considered threat model.
3. Fingerprint Identification System are no substitute for quality data about potential risks.
4. Fingerprint Identification System accuracy is impossible to assess before deployment.

XI. Conclusion

Fingerprint Identification System are really very useful for Library and Information Science professionals to ensure better safety and security to the valuable collections which consist of information resource base. Though there are few limitation, the technology could be used in our libraries in a phased manner. The academic libraries can make use of the benefits of the technology to ensure better safety and security to their invaluable information resource base and human resources as well.

References

[1] J. Berry, "The history and development of fingerprinting," in Advances in Fingerprint Technology, (H. C. Lee and R. E. Gaensslen, ed.s), CRC Press, Florida, 1994, pp. 1-38, 1994.

[2] A. K. Jain, L. Hong, and R. Bolle, "On-line fingerprint verification," *IEEE Trans. Pattern Analysis and Machine Intelligence,* Vol. 19, No. 4, pp. 302-313, 1997.

[3] H. E. Knutsson, R. Wilson, and G. H. Granlund, "Anisotropic Nonstationary Image Estimation and its Applications: Part I – Restoration of Noisy Images," *IEEE Trans. Communications,* Vol. 31, pp. 388-397, 1983.

[4] B. M. Mehtre, N. N. Murthy, and S. Kapoor, "Segmentation of Fingerprint Images Using the Directional Image," *Pattern Recognition,* Vol. 20, No. 4, pp. 429-435, 1987.

[5] O. Nakamura, K. Goto, and T. Minami, "Fingerprint Classification by Directional Distribution Patterns," *Systems, Computers, and Controls*, Vol. 13, pp. 81-89, 1982.

[6] L. O'Gorman and J. V. Nickerson, "An approach to fingerprint filter design", *Pattern Recognition,* Vol. 22, No. 1, pp. 29-38, 1989.

[7] N. K. Ratha, S. Chen, and A. K. Jain, "Adaptive Flow Orientation-Based Feature Extraction in Fingerprint Images," *Pattern Recognition,* Vol. 28, No. 11, pp. 1657-1672, 1995.

[8] N. K. Ratha, K. Karu, S. Chen, and A. K. Jain, "A Real-Time Matching System for Large Fingerprint Databases", IEEE Trans. *Pattern Analysis and Machine Intelligence,* Vol. 18, No. 8, pp. 799-813, 1996.

[9] B. G. Sherlock, D. M. Munro, and K. Millard, "Algorithm for Enhancing Fingerprint Images," *Electronics Letters,* Vol. 28, No. 18, pp. 1720-1721, 1992.