International Journal of Engineering & Technology, 3 (3) (2014) 391-395
©Science Publishing Corporation
www.sciencepubco.com/index.php/IJET
doi: 10.14419/ijet.v3i3.2368
Research Paper

An analysis of issues in biometric finger identification

V. Nandakumar

Programmer SG, Computer Centre, Alagappa University, Karaikudi, Tamilnadu, India
E-mail: vnkumar62@yahoo.com

Abstract

A Person's identity is an essential factor in this vastly connected society. Biometric Finger has wide acceptance as a genuine method for determining an individual’s identity. Biometric Finger authentication is reliable, since physical characteristics in humans are difficult to forge, harder to change or make copies. Biometric fingerprinting is one of the most popular and legally accepted biometrics used in person identification. Finger print authentication applications include Computer Applications, Network Access, Data Protection, Transaction Security, and Web Security. E-commerce and E-governments can carry out strong authentication rules. This paper analyzes issues related to Fingerprint identification to suggest viable alternatives.

Keywords: *Fingerprint Identification, Optical Sensors, Ultrasound Sensors, Issues in Finger Print Identification*.

1. Introduction

Biometrics fingerprinting is a good way to protect information and data. Biometric Finger printing can play the key role of personal authentication in enterprise network environments to protect digital contents. Finger printing systems are standalone systems or integrated with other technologies like smart cards and digital signatures. Biometric system attributes help gauge their effectiveness. Most biometric systems may not cater to the basic necessary attributes, making Fingerprint verification a challenging area in pattern recognition of biometric systems [1]. This technology is the base for numerous new inventions.

Biometrics Fingerprinting has its applications in different fields like hospitals for patient's identity, at the airports to verify people, help governments keep track of citizen’s movements or find criminals and terrorists. Existing applications include verification of pass holders at amusement parks, Internet banking or users’ authentication in a variety of social services [2]. Network security authentication systems rely on passwords, renewed after a certain time for security. Passwords may be copied and used by unauthorized people. Biometric identification in network security is more logical as it verifies a person's identification for secure network services allowing access control to the system [3]. User’s unique biometric characteristics like retina, fingerprint, and face can be collected in many ways.

Fingerprint authentication is verifying human fingerprints with previously stored samples. The fingerprint is scanned electronically for creating a reference template. This template is derived from either a minutiae element like the pattern of the fingerprint, or simply the image of the fingerprint. The inside surfaces of the hands and feet of all primates contain minute ridges of skin, with furrows between each ridge. Fingerprints are distinctive to a person and even identical looking twins have differences in fingerprints [4]. It is widely believed that no two people have identical ridge details.

Fingerprinting for person identification had an advantage over most other biometrics in that fingerprint acquisition has been possible for centuries in the form of impressions of inked fingers on paper and direct impressions in materials like clay. Fingerprints can be acquired without the use of ink. The basic principle of the inkless methods is to sense the Ridges of a finger using a Scanner. The image is called a “live scan” and the Scanners are known as “live scan” Fingerprint Scanners [5], [6].

The data acquisition mechanism requires special set of devices and instruments to capture the fingerprint images. Scanners scan the fingerprint images in a digital representation composed of M × N pixels and a discrete 2D function f(x, y), where x = 0, 1, 2… M and y = 0, 1, 2… N, which denotes the spatial co-ordination. The value of f in any (x, y) corresponds to the grey level in that point [7] and scanned images are processed.

The scanned images are stored within an enrolment database. The main goal of a biometric system is to verify a person's identity. Biometric Identification has two distinct phases namely Verification and Identification. Identification is based only on biometric measurements and compares measurements within an entire database of the people enrolled, instead of a single record, selected by some identifier.

Biometric data needs to have the basic attributes like Universality (Individual biometric characteristic), Uniqueness (No repetition of biometric characteristics), Permanence (Invariant biometric characteristic), Collectability (measuring characteristics) and Acceptability. It is the combination of these attributes that determines the effectiveness of a biometric fingerprint system. The similarities in verification point out the degree of fitness between the features and template/s compared. The system uses the score to declare, as per the decision policy, the case a Match/Non-Match..

2. Fingerprint biometric system

The Fingerprint recognition is a technology actively studied and verifies the identity of a person, since every person’s fingerprints are unique. The chance of any two persons having the same finger print identification is nearly zero [8]. The cost of a fingerprint based biometric system is comparatively quite low with other identification techniques like iris and facial recognitions.

It is possible to deploy Fingerprint readers in any kind of environment. It is less intrusive, more user-friendly and has the versatility of enrolling multiple fingers. The uniqueness of a fingerprint is determined by ride and furrow patterns along with their minutiae points. Ridges are upper skin segments and valleys are lower segments in the finger [9]. The ridges have two minutiae points namely ridge ending and ridge bifurcation. Two main algorithms recognize fingerprints namely minutiae matching and pattern matching. Minutiae matching’s compare the details of the extracted minutiae to recognize the differences between user fingerprints. Minutiae images previously stored in a database are compared with the one provided at the time of access [9].

Pattern matching compares the surfaces and concentrates on thickness and density of finger's surface. The images around a minutiae point have areas with low curvature radius or unusual combinations of ridges [9]. Five basic patterns make up the fingerprint. The arch covers 5% of a fingerprint, both left and right loop cover 60% of fingerprints, whorl 34% and accidental whorls cover 1% of fingerprints [10]. Fingerprint images are depicted in Fig. 1.

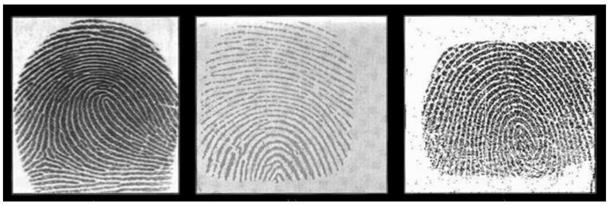

Fig. 1: Fingerprint Types

3. Identification and verification

Identification and verification, called authentication, is used to declare the identity of a user. The system verifies the Finger print of a person from a profile or template containing the biometric fingerprints stored (enrollment) [11] for matching results. Factors of Evaluation in Fingerprint matching are as follows.

1) Success rate in Fingerprint identification is the rate at which successful verification or identification made compared to the total number of trials [12].
2) False Rejection Rate (FRR) is the rate at which a system falsely rejects a registered user compared to the total number of trials [12].
3) False Acceptance Rate (FAR) is the rate at which the system falsely accepts an unregistered user, FAR measures if a user is accepted under a false claimed identity [12].
4) Equal Error Rate (EER) is the common value of the FAR and FRR when the FAR equals the FRR and has to be kept low as possible. A low EER value indicates a high accuracy of the system [13].

4. Issues in biometric fingerprints

The fingertip is a small part from which finger print images are captured. Fingers can undergo wear and tear. Fingerprint images of such fingers are a complicated task. People with improper minutia points cannot use the system. The minutia point’s count can be a limiting factor while in use. Results can also be improper due to false minutia points appearing out of low-quality enrollment, imaging, or fingerprint ridge details. Biometric fingerprinting systems have specific issues as detailed below.

4.1. Technology concerns

One of the key technology issues is interoperability. Multiple international standards which are not interoperable in e-based fingerprint templates increase the issue of interoperability. Key Problems have been noticed in Converting Finger Minutiae between Formats like ISO/IEC 19794-2, ILO-SID and ANSI/NIST-ITL 1-2007 Type-9. Vendor-neutral fingerprint biometric templates do not guarantee flawless integration or exchange of information between vendors. Biometric databases contain personal information of the public, raising questions on maintenance. The general concern is about authorized people who can track the public when required. To achieve privacy and security cryptographic techniques can be used called biometric encryption [14]. A key can be derived from the biometric data and be embedded into the template. The key can be decrypted only with a biometric image of the enrolled person making it secure.

4.2. Sensing equipment issues

Sensing equipment is prone to errors due to many factors like installed equipment, climate or contamination in the finger.

1) Sensor mounting height: Positioning the fingerprint scanner at the correct height for the user makes it considerably easier and improves the recognition capability of the device. The scanner should be fitted in a way that it guarantees, the scanner can be used in a relaxed manner. If the user has to strain in any way to work on the scanner, the scanning results have a lesser impact. The scanner should be mounted in a minimum height of 135 cm's so that the middle finger or index finger can be comfortably placed over the sensor in a straight line. In the case of children, this height makes it easier for them to operate the scanner correctly.
2) Sensor: The sensor is a thin strip on the finger guide of the fingerprint scanner. The sensor should not be scratched with fingernails or exposed to any added mechanical stresses or come into contact with the abrasive side of objects like sponge or keys. A damaged sensor cannot function properly.
3) Capacitive Sensors: Capacitive sensors use capacitor plates to image fingerprints. Ridges have higher capacitance while valleys have a lower capacitance. Application of a small voltage enhances the signal and creates a better image. Capacitive sensors are insensitive to ambient lighting and resist contamination issues in the finger.
4) Thermal Sensors: Thermal sensors use pyro-electric material. A fingers contact temperature is measured when it comes in contact with the sensor surface. The valleys cannot be measured as they do not make contact. The image is built from the skin-temperature on ridges and ambient temperature for valleys. The drawback in the system is due to constant changes in temperature and the finger temperature gets adjusted with the sensor's temperature in less than a second.
5) Optical Sensors: Optical sensors have Photo-transistor detectors that convert the light energy into electrical charge. They use an LED (light-emitting-diode) to illuminate the finger. The detectors can be coupled-devices (CCD) or CMOS based optical imagers. Low lights are detected by CCD and are capable of creating good quality pictures in grayscale. CCD fabrication is expensive in contrast to CMOS imagers which are cheaper. Neither low-light sensitivity nor grayscale imaging generated by CCD is required for fingerprint recognition. Optical sensors can be affected by many factors. Common contaminates that weaken image quality include scratches on the sensor surface or layer formations on the surface like ice, dirt.etc. Problems are more while attempting to image a dry finger, an oily finger or imaging in a very low humidity. If ridge structure is irregular, causing air gasps between ridge and platen if finger is contaminated with dirt, newsprint, pen or pencil markets, paint, etc. If the scanner platen becomes coated with oil or if dirt accumulates, they limit the use of optical scanners in identification as depicted in Fig. 2.

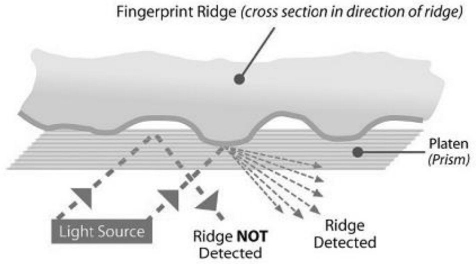

Fig. 2: Effects of Rough Ridge Structure on the Sensing

6) Ultrasound Scanners: Ultrasound imaging can overcome the limitations of optical fingerprint scanners. It is a rapidly growing imaging technology with acoustic energy. An ultrasonic scanner relies upon differences in acoustic impedance between the finger ridge or valley and the platen to form an image. Sound waves get partly reflected and transmitted at each interface level producing return signals at successive depths. Ultrasound permits

imaging beyond air gaps and surface contamination into the true ridge structure of the finger. The finger print scan is analogous to optical system resolution with 500 dpi sensitivity and an 8 bit grey scale contrast. The achieved image quality is very high and is unaffected by common contaminants or skin dryness. No pre-conditioning is required in image enhancement and processing time is reduced to a great extent compared to optical images. The quality of enhanced image is depicted in Fig. 3.

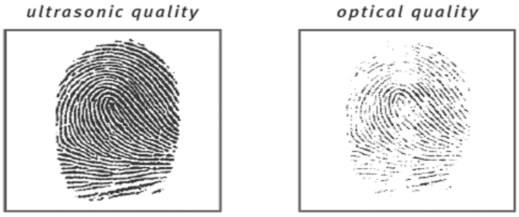

Fig. 3: Fingerprint Image from Ultra-Scan Ultrasonic Scanner

4.3. Fingerprint algorithms

Algorithms form the base in developing Fingerprint Recognition Systems that return relevant results to a query fingerprint image in a relevant time [15]. The general shape of the fingerprint is used in pre-processing images and reducing the search time in large databases. Several categories of minutiae have been defined and algorithms use these minutiae points in matching fingerprints. Some algorithms count the number of ridges between particular points. Pattern matching algorithms use ridges, valleys and minutiae. Image of the fingerprint is divided into smaller sectors and the details extracted and stored. Very often, algorithms use a combination of all techniques. Pankanti of IBM) estimated a 6.10-8 probability for 12 minutiae matching among 36 samples. [16]. Fingerprint Algorithms need to cater to a lot of factors like efficiency, speed, accuracy in addition to simplicity in implementing the algorithm in a system.

5. Conclusion

Biometrics is a means of verifying personal identity measuring and analyzing unique characteristics like fingerprints. Fingerprint biometric system is used in all fields except chemical industries because the finger print of Chemical industries workers is often affected. Though biometric authentication offer high security, they need to be perfected. A human expert can identify errors with an error rate of 1%, but systems are tested against skilled forgeries, even the best system is able to deliver error rates less than 5% [17]. This can be overcome by identifying and compensating sources of errors in the algorithm, since cost of an error in biometric verification is very high. User acceptance, level of security required, accuracy, Cost and Implementation are the basic parameters that need to be considered while designing a biometric verification system [18]. Experience shows that the middle finger, index finger, ring finger, thumb and the little finger are most suitable for fingerprint scanners in the same order. Moist or wet fingers problem can simply be overcome by rubbing the finger dry. Dry fingers problem can be overcome by wiping it quickly across the eyebrow or by increasing the pressure when operating the scanner. It can be concluded that Finger print biometrics is one of the efficient, secure, cost effective, ease to use technologies for user authentication in spite of the infant level problems.

References

[1] Hemanta Saikia, Kanak Chandra Sarma Approaches and Issues in Offline Signature Verification System International Journal of Computer Applications (0975 – 8887) Volume 42– No.16, March 2012

[2] R. Sanchez-Reillo, C. Sanchez-Avila, and A. Gonzales-Marcos, “Biometric identification through hand geometry measurements,” IEEE Trans. Pattern Anal. Mach. Intell., Volume 22, Issue. 10, Oct. 2000, pp. 1168–1171. International Journal of u- and e- Service, Science and Technology Vol. 2, No. 3, September, 2009

[3] Paul Reid, "Biometrics for network security", Pearson Education Inc., 2004, ISBN 0131015494

[4] S. Pankanti, S. Prabhakar, and A.K. Jain, “The Individuality of Fingerprints,” in Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition, Kauai, Hawaii, December 2001, pp. I: 805 -812

[5] Ruud M. Bolle, Jonathan H. Connell, Sharath Pankanti, Nalini K. Ratha, and Andrew W. Senior, Guide to Biometrics. Springer Science + Business Media, Inc, NY 10013, USA, 2004, pp 3 – 6, 31 – 45, 146 – 148

[6] Julian Ashbourn, Practical Biometrics: From Aspiration to Implementation. Springer-Verlag London, 2004, p. 2.

[7] Batista, L., Rivard D., Sabourin R., Granger E., Maupin P. 2007. State of the art in off-line signature verification. In: Verma B., Blumenstein M. (eds.), Pattern Recognition Technologies and Applications: Recent Advances, (1e). IGI Global, Hershey (2007.)

[8] Massimo Tistarelli and Marks Nixon, "Advances In Biometrics", Springer-Verlag Berlin Heidelberg 2009, ISBN 03029743

[9] "Biometrics new portal" UK 2011 http://www.biometricnewsportal.com/

[10] Department of Health, New Mexico, “Fingerprint Techniques Manual what.pmd" http://dhi.health.state.nm.us/elibrary/ cchspmanual/ fingerprint_manual.pdf

[11] T. van der Putte and J. Keuning. Biometrical Fingerprint recognition: don't get your fingers burned. In Proceedings of IFIP TC8/WG8.8 Fourth Working Conference on Smart Card Research and Advanced Applications, pages 289-303.Kluwer Academic Publishers, September 2000.

[12] J. Blomme. Evaluation of biometric security systems against artificial fingers. Master's thesis LITH-ISY-EX-3514- Department of Electrical Engineering, LinkÄoping University, LinkÄoping, Sweden, October 2003

[13] Jr. J. D. Woodward, N. M. Orlands, and P. T. Higgins. Biometrics: Identity assurance in the information age. McGraw-Hill/Osborne, Berkeley, California, USA, 2003.

[14] IEEE Conferences On biometric encryption using fingerprint and its security evaluation, February 2009

[15] Rahul Sharma, Nidhi Mishra, Sanjeev Kumar Yadav, Fingerprint Recognition System and Techniques: A Survey , International Journal of Scientific & Engineering Research, Volume 4, Issue 6, June-2013 1670 ISSN 2229-5518

[16] http://fingerchip.pagesperso-orange.fr/biometrics/types/fingerprint_algo.htm

[17] Kovari B, Toth B, Charaf H. 2009. Classification Approaches in Off-Line Handwritten Signature Verification. WSEAS TRANSACTIONS on MATHEMATICS Issue 9, Volume 8, September 2009

[18] Jain A K, Ross A and Prabhakar S. 2004. An Introduction to Biometric Recognition, IEEE Transactions on Circuits and Systems for Video Technology, Vol. 14, No. 1, January 2004.