Trends in Bioinformatics

ISSN 1994-7941

science alert

ANSInet
an open access publisher
http://ansinet.com

OPEN ACCESS Trends in Bioinformatics

ISSN 1994-7941
DOI: 10.3923/tb.2016.52.58

Research Article
Fingerprint Biometric Systems

[1]Y. Faridah, [1]Haidawati Nasir, [2]A.K. Kushsairy, [2]Sairul I. Safie, [3]Sheroz Khan and [3]Teddy S. Gunawan

[1]Malaysian Institute of Information Technology, Universiti Kuala Lumpur, 1016, Jalan Sultan Ismail, 50250 Kuala Lumpur, Malaysia
[2]British Malaysian Institute (UniKL BMI), Universiti Kuala Lumpur, Malaysia
[3]Department of Electrical and Computer Engineering, International Islamic University, Malaysia

Abstract

One of the popular and widely practiced biometric systems is fingerprint. Fingerprint biometric systems are smaller in size, easy to use and has low power. It is available and deployed globally in law enforcement, such as immigration, banking sectors, forensics, health care and many more. This study reviewed fingerprint biometric systems and the methods used in each proposed system. Many studies have been done in the area of feature extraction and matching stages. The current techniques used in these stages are minutiae-based and euclidean distance-based. Application of the fingerprint biometric system in the industries has been accepted widely and used in the Europe and some developed country. Malaysia has also incorporated the use of this system in its administration for controlling the point of entry at the Kuala Lumpur International Airport. Generally, fingerprint biometric systems can be categorized into recognition, security, identification and control systems. Each system has their benefits and drawbacks that complemented each other.

Key words: Fingerprint, fingerprint biometric system, recognition, technologies, pattern, image

Received: June 11, 2016 Accepted: August 21, 2016 Published: September 15, 2016

Citation: Y. Faridah, Haidawati Nasir, A.K. Kushsairy, Sairul I. Safie, Sheroz Khan and Teddy S. Gunawan, 2016. Fingerprint biometric systems. Trends Bioinform., 9: 52-58.

Corresponding Author: Y. Faridah, Malaysian Institute of Information Technology, Universiti Kuala Lumpur, 1016, Jalan Sultan Ismail, 50250 Kuala Lumpur, Malaysia

Competing Interest: The authors have declared that no competing interest exists.

Data Availability: All relevant data are within the paper and its supporting information files.

INTRODUCTION

Biometric systems have been widely and in use long before the inception of computer in human activities. These systems make use of the physical or biological traits of human beings for recognition and authentication purposes. Most common biological traits or characteristics used are fingerprints, iris and face. The lists of development in this area are becoming longer which includes other biometrics such as palm print, retinal scan, signature, voice pattern, etc. It shows that the biometric is increasingly popular and here to stay.

Biological traits are much better in performances and are much more reliable as compared with behavioural traits such as signature, voice or keystroke. The latter are changeable over time, therefore the enrolled biometric references have to be updated every time it is used.

Biometrics are referred as biometric recognition due to the fact that a person can be automatically identified based on his/her physiological characteristics[1]. Each person has their own unique characteristics that explained "Who they are" rather than "What they have".

In the middle of the 19th century, the use of body parts to identify criminals has been developed and used. Fingerprint distinctiveness and its usage were discovered in the late of 19th century which dominate the findings of the later. From here, major law departments embraced the use of fingerprint system.

This system is mainly used in the process of identification, verification and security. In an identification, a person is being compared with the whole database of templates to find a match. One-to-many searches are conducted to establish the identity of the person.

While for verification process, the person has to claim his or her identity. An enrolment phase is involved where a person's biological traits are recorded and saved as a template in the system. Then this template is compared with the person's biometric traits. A one-to-one searches are made for the establishment of identity of a person.

Fingerprint systems and technologies: The old fingerprint systems, which was discovered in the late 19th century, stored the fingerprints of criminals in a database in the form of card filing. The fingerprints from the scene of the crime is taken and matched with this database to determine the identity of the criminals.

As the computer becomes the subject of rapid development, the fingerprint system also evolved and an automated biometric system is developed through extensive research and the use of computers.

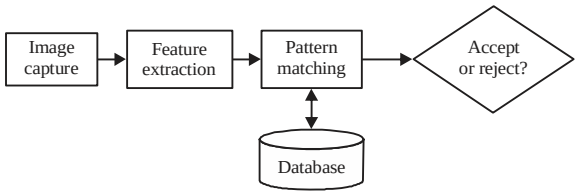

Fig. 1: Biometric system

The fingerprint system is a popular biometric system and actively researched area in biometric technologies. The fact that every person has a unique stamp of fingerprints helped the system to become "A much needed system". It is a low cost system as compared with others, e.g., iris and face recognition systems. It is also less intrusive of privacy as some people may not like their pictures be taken or speak into a microphone.

A typical fingerprint automated biometric system is shown in Fig. 1, consists of four major components. which consists of four major components. The components are image capture, feature extraction, pattern matching and database.

In image capture component in Fig. 1, a sensor captures biometric data in digital format for data acquisition. For feature extraction component, an algorithm is required to produce the feature vector which consists of numerical characterizations of the biometrics of interest. The third component, pattern matching, a matcher compares feature vectors to get a score, which shows the degree of similarity between the pair of biometrics data under investigation.

Results from this process is controlled by FAR and FRR[2]. False Acceptance Rate (FAR) is the rate where the system falsely accepted an unregistered or another registered user as a registered one compared to the total number of trials. While, False Rejection Rate (FRR) happened when the system falsely rejects a registered user over the total number of trials.

A high FRR indicated a low FAR and a high FAR indicated low FRR. The best and ideal system should have moderate values of both. The fingerprint technologies are being applied and used in identity management and access control.

Fingerprints consist of series of ridges and furrows on the surface of the finger and patterns such as swirls, loops or aches surrounded the core which make them distinctly different for each person.

Ridges are the outer layer segments of the finger while valleys are the lower layer segments. Both are identified by irregularities called as minutiae which become the basis of finger scanning technologies. Minutiae has the form of ridge ending, bifurcation and dot as shown in Fig. 2.

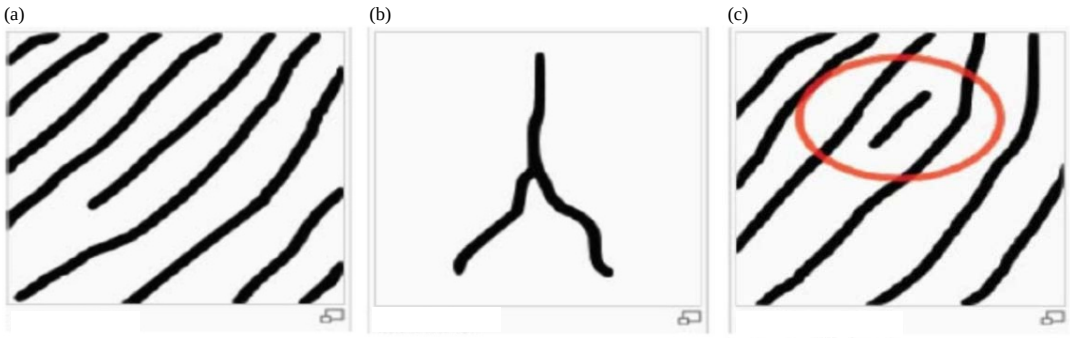

Fig. 2(a-c): Fingerprint minutiae forms (a) Ridge ending, (b) Bifurcation and (c) Short ridge (Dot)

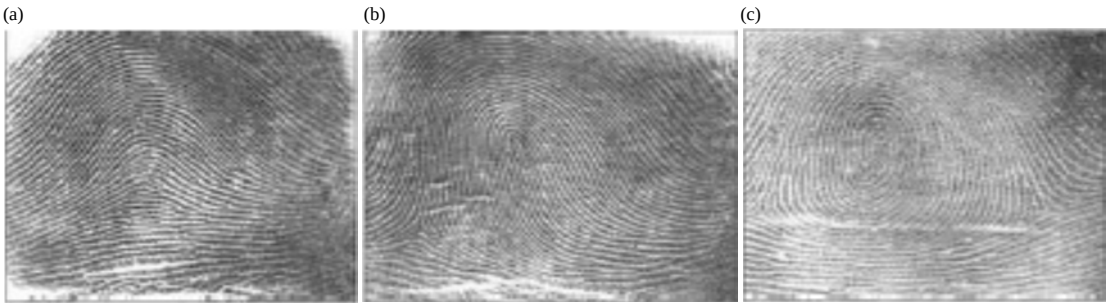

Fig. 3(a-c): Fingerprint patterns (a) Arch, (b) Loop and (c) Whorl

The ridge ending is where the ridge terminates. While, bifurcations happen when a single ridge splits into two ridges and dots are ridges which are significantly shorter than the average ridge length on the fingerprint. Other forms of minutiae which are not explained here, included islands, ponds or lakes, spurs, bridges and crossovers.

The minutia points are identified, with their relative positions to each other and their directions during the enrollment process. In the matching stage, the image is digested to differentiate its minutia point, which are then compared with the registered template.

Another basis for the scanning technology is through pattern detection. In fingerprint ridges, there are three basic patterns known as the arch, loop and whorl[3] as depicted in Fig. 3. It was reported that family members do share similar general fingerprint patterns[4].

In the process of matching, all characteristics of fingerprints are compared, not focusing on individual points only. The characteristics can contain sub-areas of certain interest such as ridge thickness, curvature or density. Small sections of the fingerprint and their relative distances are differentiated in the enrollment process.

The area around the minutia point, areas with low curvature radius and areas with an unusual combination of ridges are the areas of interest.

Current biometric systems used optical, silicon, thermal and ultrasound technologies to capture the real-time fingerprint images using readers, instead of getting the images using the conventional ink method.

EXISTING FINGERPRINT BIOMETRIC SYSTEMS

Fingerprint identification in biometric security systems: In this system that is designed and proposed by Lourde and Khosla[5], focused in selecting an optimal algorithm for performance and accuracy. They looked into the fingerprint matching techniques which is to detect the sameness between two given fingerprint images.

The three existing categories of matching techniques minutiae-based, correlation-based and euclidean-based are discussed.

Two freeware software based on MATLAB are chosen-minutiae-matching algorithms developed by Hong Kong Baptist University used Histogram Equalization and Fourier Transform while the Fingerprint Recognition System 5.1 built by S. Prabhaker and A. Jain from Michigan State University was published by Luigi Rosa employed the euclidean-base distance between the two corresponding FingerCode vectors and also filter-based algorithm (Gabor Filters).

The NIST database-4 are used where 25 pairs of fingerprint images are sampled as test data. These images are submitted, first, to the minutiae-based matcher then to the filter-bank based matcher. The FAR and FRRs are captured and compared.

They found that none of the two algorithms was the winner in terms of performance. They proposed a combination of two or more established algorithms due to the fact that all algorithms have their advantages and disadvantages, these will completed each other.

Biometrics security systems: Fingerprint and speech technology: Orsag and Drahansky[6] from Czech Republic proposed and designed an architecture of biometric security systems which make use of cryptographic data derived from the biometric traits and joint by a splitting of a private cryptographic key.

The objective is to divide up the key over all biometric systems used. A limited amount of vectors should be generated by each biometric systems, which is used as the key. A hash function is then derived for each of these keys and stored in hardware storages. A combination of two biometrics are used: Fingerprint system and speech system.

Method of designing the system is ambiguous. Both biometric systems involved a lot of techniques in each stage of the component system. Though, for the first system, Gabor filters are used for performance while minutiae algorithm for extraction and verification.

A brief introduction of biometrics and fingerprint payment technology: This study is done by Dileep Kumar and Yeonseung Ryu of South Korea[3] providing a glance on the fingerprint biometric systems in payment technology. The proposed biometric systems technology is safe, secure and economical as perceived by the respondents through survey results conducted by Unisys (www.Unisys.com).

They suggested the use of fingerprint recognition by using circular sampling. In this method, the image is sampled through a pattern consisting of concentration circles, i.e., in polar coordinate space, the image is considered as a two-dimensional continuous signal. The sampling resolutions are the distance from the concentric circles of the sampling interval within the circumference of the circles. A high magnitude showed a likeness between two sources of signals. The magnitude is the total area of the product of the two signals. They employed the minutiae-based and correlation-based techniques in the matching process.

Fingerprint recognition using extraction of connected boundaries

Components edge detection: The method proposed in this study is due to the fact that there are problems in detecting likeness for fingerprints which are related to discontinuities, spots, independent ridges, etc.

Nazera *et al.*[7] proposed a recognition method using extraction of connected boundaries components edge detection.

In this method, they suggested to create a connected boundaries components using the local features minutiae points in fingerprint image as objects image.

The objective is to produce a line drawing of an image or similar to it. Practically, it involved search of places with the intensity changes rapidly. They proposed minutiae extraction algorithm which make use of Crossing Number (CN). Local neighborhoods are scanned using a 3 by 3 window. The CN consisted of the x and y raw coordinates.

Detailed experimental comparison is done on fingerprint image database from Al-Sder Hospital, Iraq and images was obtained from the Internet (SIGGRAPH). The system is based on region and results showed success in the testing done.

Edge detection and feature extraction in automated fingerprint

Identification systems (AFIS): Boldischar and Moua[8] concentrated on two components of an automated fingerprint identification systems. They focused on the feature extractor component which involved the use of gray scale normalization, thinning process and edge detection. Edge detection can be done based on process of convolution.

Researchers discussed on existing AFIS but not much explanation was provided.

Efficient fingerprint recognition system using pseudo 2D hidden

Markov model: The existing biometric systems combined both Bayes and Henry classifier in order to speed up the authentication stage. In the real time implementation stage, the system proved difficult and takes time to process data.

Parvathi and Saravanan[9] proposed a new method by using pseudo 2D Hidden Markov Model (HMM). This model take each types of fingerprint as separate states with different level of Markov chain. The HMM is used in the recognition process, where it verifies every super states to detect which types of fingerprint in order to match the given fingerprint image with the image kept in the database.

The 1-D HMM consists of a state transition probability matrix, an initial state probability distribution and a set of probability density functions associated with the observations for each state. The 1-D HMM states structure are extended to become the 2D HMM.

The pseudo HMM is built by taking different samples of the same fingerprints and implementing a training process. It did not perform the ridge image thinning stage and minutiae selection.

Fingerprint classification using fast fourier transform and non-linear

Discriminant analysis: A new way of fingerprint classification by adopting Discrete Fourier Transform (DFT) and Non-linear discriminant analysis (NDA). The images are re-constructed by using DFT and NDA is applied to the new image.

Park and Park[10] used directional filters and explored the DFT technique, fast Fourier transform. The NDA is used during the feature extraction stage.

System is tested using NIST database 4 consist of 4000 images. The results were compared with other published results and proved to be better.

BIOMETRIC PERFORMANCE TESTING STANDARDS

The standard activities for biometric systems are not discussed in-depth in this study as it focused more on the application of the biometrics system and how the combination of biometric traits can be done.

However, there are multiple parts of standards for biometric performance testing and reporting developed by INCITS M1 and ISO/IEC JTC 1/SC 37. This standards follow the American National Standard that were approved by ANSI on 25th October, 2005. The standards are:

- INCITS 409.1-2005 known as American national standard for information technology biometric performance testing and reporting, part 1: Principles and framework. This standard develops a common set of methodologies and procedures to be allowed for conducting technical performance testing and evaluations. Included in this are guidelines that address issues regarding required test sizes, performance statistics, error reporting and presentation of performance results. These procedures can be incorporated in an "end-to-end' system approach or from an individual technical component perspective
- INCITS 409.2-2005, American national standard for information technology, part 2: Technology testing and reporting. This standard specifies procedures for conducting offline tests of the performance of biometric technologies
- INCITS 409.3-2005, American national standard for information technology, biometric performance testing and reporting part 3: Scenario testing and reporting. This standard specifies requirements for scenario-based biometric testing and reporting

There are other standards which are under developed at the international level, ISO/IEC FDIS 19795-1:2005, based from two NIST primary source documents developed earlier by NIST. Several international players shown in Fig. 4, in the development of biometrics standards are:

- Standards Development Organizations (SDO): ISO/IEC, ITU-T, CEN, ANSI
- Industry consortia: BioAPI Consortium, Biometric Consortium, OASIS
- Other organizations: ICAO, ILO

DISCUSSION

The researches worked done in the area of fingerprint biometric systems becoming more extensive and it opens unknown door to new future full of technologies. From the reviews, it proves that fingerprint biometric systems is dominant and popular among researcher. The systems are most popular in the area of recognition.

Table 1 showed the comparison of performance among favorites biometric characteristics, based on FAR, FRR and EER parameters. The EER is the Equal Error Rate. In comparison with other biometric technologies, fingerprint showed the lower EER rate as compared with the number of subjects tested and used.

Table 1 showed the data collected for different types of biometric technologies for the EER, FAR and FRR rates. It represented the technologies performances base on this three index categories.

The published ratings plays a vital role for industry for example e.g., forensic science community, general public, security to choose systems that suit their needs and functions. This leads to development of high quality acquisition devices and future technology.

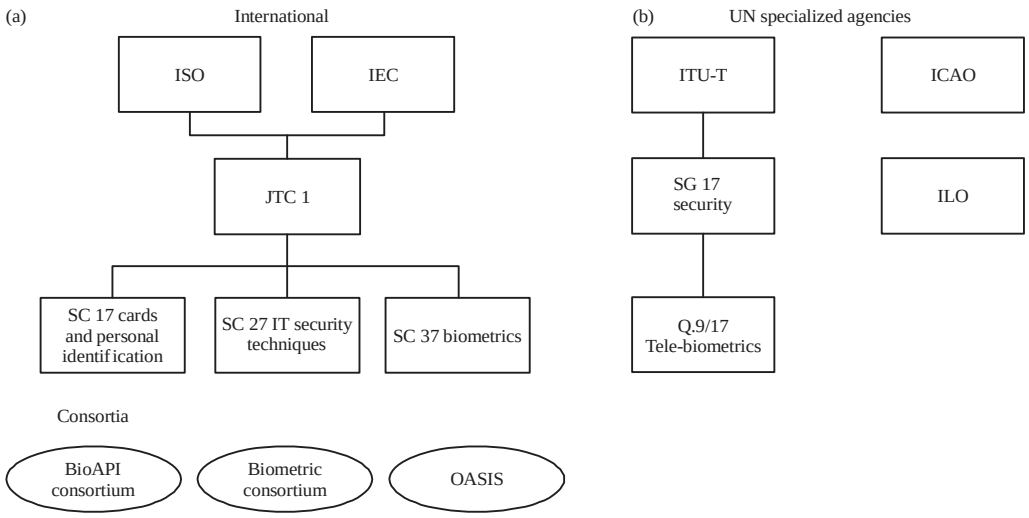

Fig. 4(a-b): Biometric standardization landscape (a) International and (b) Consortia

Table 1: Biometric technologies comparison based on EER, FAR and FRR

Biometric	EER (%)	FAR (%)	FRR (%)	Subject	Comments
Face	NA	1.00	10.00	37437	Varied light, indoor/outdoor
Fingerprint	2.00	2.00	2.00	25000	Rotation and exaggerated skin distortion
Hand geometry	1.00	2.00	2.00	129	With rings and improper placement
Iris	0.01	0.94	0.99	1224	Indoor environment
Key stokes	1.80	7.00	0.10	15	During 6 months period
Voice	6.00	2.00	10.00	30	Text dependent and multilingual

Source: Subban and Mankame[11]

CONCLUSION

This study presented works published by researchers for fingerprint biometric systems. It reviews and studies the methods used in related system. From the finding, it can be concluded that the best methods for matching process for fingerprint biometric system are minutiae-based and correlation-based. While euclidean distance-based is more suitable for feature extraction process. The review on the International standard of biometric testing and reporting is not discussed as it concentrated on the application of the fingerprint systems and the method used for extracting images of fingerprints to make it clearer for the process of verification and identification of a person.

Research study were mostly done in the feature extraction and matching stages. Both stages have lots of room to be improved and explored. There are many more algorithms that can be developed and used. The use of existing matching and feature methods can also be done in this area.

The reviews concentrate on the uni-modal biometric systems, therefore it is a good idea, if multi-modal system to be explored. For example, combination of iris and fingerprint, fingerprint and voice, naming a few.

The review also found that not one method of fingerprint biometric systems is superior that the other. Mostly new approaches have been designed for the feature extraction and matching stages of the fingerprint biometric systems. As of to date, there are minimal but continuous development in this area.

Biometrics proved to be at an advantages over the conventional ink method, password and token-based security.

ACKNOWLEDGMENTS

We would like to acknowledge the IEEE and ICETE committee for allowing us to amend the template giving the opportunity to participate in the conference.

REFERENCES

1. Jain, A.K., A. Ross and S. Prabhakar, 2004. An introduction to biometric recognition. IEEE Trans. Circuits Syst. Video Technol., 14: 4-20.
2. Sravya, V., R.K. Murthy, R.B. Kallam and B Srujana, 2012. A survey on fingerprint biometric system. Int. J. Adv. Res. Comput. Sci. Sofware Eng., 2: 307-313.

3. Kumar, D. and Y. Ryu, 2009. A brief introduction of biometrics and fingerprint payment technology. Int. J. Adv. Sci. Technol., 4: 25-38.
4. Jain, A., U. Uludag and A. Ross, 2003. Biometric template selection: A case study in fingerprints. Proceedings of the International Conference on Audio-and Video-Based Biometric Person Authentication, June 9-11, 2003, Guildford, UK., pp: 335-342.
5. Lourde, R.M. and D. Khosla, 2010. Fingerprint identification in biometric security systems. Int. J. Comput. Electr. Eng., 2: 852-855.
6. Orsag, F. and M. Drahansky, 2003. Biometric security systems: Fingerprint and speech technology. http://www.fit.vutbr.cz/~orsag/IICAI-03.pdf
7. Nazera, K.D., R.M. Hind and A.M. Noora, 2013. Fingerprint recognition using extraction of connected boundaries components edge detection. UNIASCIT, 3: 340-346.
8. Boldischar, M. and C.P. Moua, 2007. Edge detection and feature extraction in automated fingerprint identification systems. http://www2.uwstout.edu/content/rs/2007/Edge%20Detection.pdf
9. Parvathi, R. and D.S. Saravanan, 2013. Efficient fingerprint recognition system using pseudo 2D hidden Markov model. Int. J. Soft Comput. Eng., 3: 169-173.
10. Park, C.H. and H. Park, 2005. Fingerprint classification using fast Fourier transform and nonlinear discriminant analysis. Pattern Recognit., 38: 495-503.
11. Subban, R. and D.P. Mankame, 2013. A study of biometric approach using fingerprint recognition. Lecture Notes Software Eng., 1: 209-213.