International Journal of Industrial Engineering and Management (IJIEM), Vol. 2 No 2, 2011, pp. 39-44
Available online at http://www.ftn.uns.ac.rs/ijiem/
ISSN 2217-2661

Fingerprint Biometric for Identity management

Nadarajah Manivannan
Post Doctorial researcher, Nadarajah.Manivannan@brunel .ac.uk
Celalettin Tigli
Post Doctorial researcher, Celalettin.Tigli@brunel.ac.uk
Azad Noor
PhD Student, Azad.Noor@brunel.ac.uk
Shahzad Memon
PhD Student, Shahzad.Memon@brunel.ac.uk
Centre for Electronics Systems Research (CESR), School of Engineering and Design
Brunel University, London, United Kingdom

Received (02 March 2011); Revised (04 May 2011); Accepted (17 May 2011)

Abstract
In this paper a study of fingerprint biometric for Identity management is presented. Basic stages of automatic fingerprint systems are explained and a comparison study among three commercially available automatic fingerprint recognition systems is also presented. This study suggests that automatic fingerprint recognition systems performs reliably well as far as recognition is concerned, however there is a number of areas, such as liveness detection and unsupervised recognition, need to be tackled for high security applications, such as border control and anti-terror activities.

Key words: *Automatic Fingerprint Recognition Systems, Biometrics, Identity Management, Security*

1. INTRODUCTION

Identity management (IM) is establishing identity of a single person (subject) using one or more of the biometric or non-biometric features. Biometric trait is a biological and behavioural characterises of a subject, such as fingerprint, face, gait (the way the subject is walking) and signature. Non-biometric feature is anything other than biometric, such as pin number, password and name.

Fingerprint is a successful biometric for establishing identity of the subject for a very long time, more than a century. Fingerprint images were captured by manual impressions using ink and identification process was performed manually. This method of identification were limited by many factors, such as poor quality of capturing, short duration template of image, no-proper algorithm for matching the fingerprints, manual inspection lead for inaccuracies in matching process and time inefficient process.

In the digital age with high computing power at very low cost, Automated Fingerprint Recognition System (AFRS) has become part of our daily life at least in many developed countries like USA and Japan. Some of its applications are building access control, border control, computer & network access, e-government, e-commerce and forensic and criminology [1]. However it should be noted that manual inspection of fingerprints still exist in forensic and criminology as they need specialised ways analysing the fingerprints as finger prints are not captured by standard methods of fingerprint capturing technologies [2].

Automatic biometric based identity systems involve various stages, such as enrolment, recognition and integration. Enrolment is the stage where feature(s) of the subject is extracted and stored in a database or in a document such as Identity Document (ID) card and passport. Recognition is the process where features of the subject is matched and recognised against the database or identity document such as passport and Identity card. Recognition process can be classified into two, 1:1 matching (authentication) and 1: N matching (identification). 1:1 matching performed when a subject is matched and verified against his identity document using biometric traits. Verifying the picture in the passport against the holder of the passport is basically 1:1 matching. 1: N matching is performed when a subjects' biometric template is matched and checked against a database contains template of biometric traits of many subjects.

Nowadays government and commercial establishments are migrating their identification process from semi-automated systems to fully automated systems [3]. There are many reasons for such migrations and some of them are listed below:

1. More accurate: Fully automated systems have developed to a level so that they, in most of the cases, outperform manual or semi-automated systems. Algorithms developed to perform the recognition are very advanced and take care of the

variability in the biometrics due to various reasons, such as ageing in face, damage in fingerprints and so on [3]. Fingerprint sensing technologies have advanced to a level so that high quality imaging of finger print is now possible [4].

2. Better time efficiency: As ultra fast computing is becoming nowadays commonly available, fast identification processing is now practical. Due to that fingerprint matching algorithms now work with very large database to establish identification. Very interesting example is 'unique Indian ID Project', which is currently underway and aimed at enrolling India's whole population of 1.2 billion on its central data base with their biometrics and demographic details and each Indian citizen will be given with a unique ID.

3. Cost effective: As computing and digital processing become cheaper, the fully automated fingerprint identification systems, in principle, are cost effective in the long run.

4. Adaptability: Computer programs and embedded systems are always updatable and therefore AFRSs are also updatable. It is very useful feature as any developments/improvements in any part of the AFRS can be in cooperated in to the existing system without interrupting the other parts of the AFRSs.

The goal of this is paper is to carry out a study on usability of automatic fingerprint recognition in modern world applications. For this study three commercially successful AFRSs is chosen and using their specifications the systems are compared and contrasted. Weakness of these systems are also identified as a way forward for future work.
Structure of the paper is as fellow; Section 2 discusses biometrics technology in general and compares a number commonly used biometrics traits. Sections 3 explain the basic stages involved in a typical fingerprint based biometric recognition system and briefly discusses recent developments in AFRS. Section 4 compare and contrast three fingerprint based recognition systems and finally the paper is summarized in section 5.

2. BIOMETRICS TECHNOLOGIES

As mentioned already, the term "biometrics" can be described as a characteristic or as a process [3]. As a characteristic it is a measurable biological (Anatomical or Physiological) and behavioural characteristic that can be used to recognise or identify a person. As a process it is a method of identifying a person based on the person's measurable biological (Anatomical or Physiological) and behavioural characteristic.

Physiological characteristics involve face recognition, handprints and fingerprints, veins in hands, capillary vessels in eyes, voice, iris and hand and finger geometry while behavioural characteristics includes voice modulations, hand drawing, signature style, gait and keystroke dynamics. These distinctive characteristics usually do not change during the adult life of a person.
A typical automated biometric system consists of five components such as

i) A sensor or transducer system to collect the biometric data and convert it into digital format.
ii) Signal processing modules that build a template with the collected data using certain algorithms.
iii) A database system where these template are stored.
iv) A matching algorithm (either 1:1 or 1:N) which compares the new template with the template/templates stored in the database.
v) A decision process (either fully automated or human assisted) which makes a system level decision based on the result from matching algorithm outcome.

The matching algorithm process as mentioned above can be used as 1:1 matching where the subject is checked against their own template stored in the identify document. The algorithm is posed with the question, "Is this template belong to Mr Smith or not?"
Whereas in 1: N matching, the claimants' template is checked against all the templates stored in the database until a match is found. If no match is found, the claimant is denied the authentication or passkey. This time the algorithm is posed with "Who does this biometric data belong to?"
Table 1 compare most popular biometric traits used in commercial recognition systems; fingerprint, Hand Geometry, vein, iris, face and voice. The table list typical applications, advantages and disadvantages. As can be seen, each biometric has got its own advantages and disadvantages. Fingerprint has got long history in AFRS fairly easy to use, high performance has seen in AFRS, economical but suffer from spoof attacks as it is easy to make artificial fingerprints using commonly available cheap materials such as gelatine and silicon and fingerprints requires full cooperation from the user. Face has also got long history in AFRS, user friendly, able to use without cooperation from the user. However face suffers from low performance and easy spoof attack. While iris shows very high performance and high distinctiveness, it is not user friendly and can be expensive. Therefore its really type of application, social and economical factors decide what type of biometrics is best.

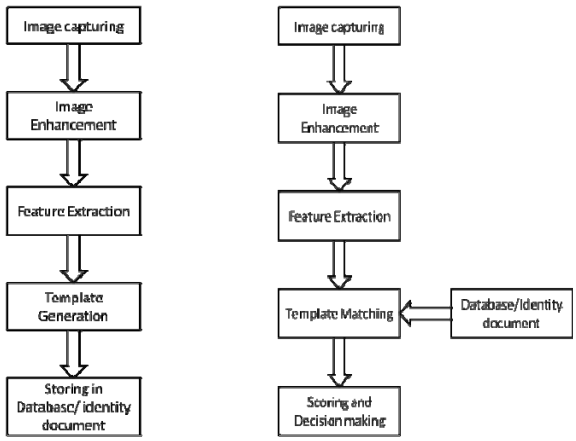
Table 1. Comparisons among various biometric traits

Biometric Trait	Application	Advantages	Disadvantages
Fingerprint	• Access Control • ATM • Border Enforcement Agency • Check out at retail	• High distinctiveness • High performance • Low cost • Short processing time • small storage • Easy integration	• Higher chance of finger image degradation by occupation, age or trauma • Can be easily fooled by using fake fingerprints
Hand Geometry	• Access Control • Immigration Control	• Easy to use • Easy to integrate • Invariant to age • Can work with dirty hands	• Accuracy is low • Fairly expensive • Doesn't work well for people with arthritis • Possibility of degradation from injury or trauma.
Hand Vein	• Login control • Bank & Financial services security • Military installation	• Invariant to age • Highly secure because it is hard to copy or even read	• Fairly new, the effect of heart attack or other medical problems is not clear.
Iris	• In law enforcement such as in prison • Airport security	• High distinctiveness • High performance • Distance recognition • Low FRR • Remains almost unaffected by environmental change • Left and right iris patters are completely different even in identical twins	• Not easy to use • Not easy to integrate with other system • The position of the eye can be problematic • It requires specialised devices so can be very expensive
Face	• Law enforcement agencies • Banks	• Can be placed on a smart card for added security • More suited for authentication • Easy to use • High acceptability	• Low distinctiveness • Low performance • Sometimes background can cause problem • Can be easily fooled as by wearing a mask
Voice	• Ecommerce transaction	• Vocal tract is not affected by cold • Can be used with telephones • Low invasiveness • High acceptability	• Local acoustics can throw off the biometric system • Age and illness can affect the voice • High false acceptance rate
Signature	• Online signature verification	• Reasonably accurate • Easy for user	• Can be fooled by imitation signature
Keystroke	• Access control to company documents	• User friendly • Fairly unique between people • More suitable for verification • Low cost	• Less suitable for identification • Can be hacked and password can be stolen.
Gait	• In hospitals to determine medical issues	• Can be obtained from a distance • Can be used to determine medical illness	• Invasion of privacy as can be obtained from distance

Among the biometrics (e.g. face, fingerprint, iris, gait and voice) fingerprint has got many advantages such as high degree of distinctiveness, permanence, performance and acceptability [1]. Due these inherent advantages, fingerprint has been dominating biometric market in recent years. A study by Wenture Digital of China estimates that the fingerprint industry leads the biometric industry with 45% market share followed by face (19%) in 2010 [11]. Another study by Acuity Management Intelligence of USA predicts that overall biometric industry will treble in 2020 with fingerprint still hold major market share in 2020 [12].

3. AUTOMATIC FINGERPRINT RECOGNITION SYSTEM

As already mentioned AFRS involves two stages; enrolment and recognition. Each stage consists of a number of sub-stages. These two stages and their basic sub-stages are illustrated in Fig. 1.



(a) Enrolment stage (b) Recognition stage

Figure 1. Stages of Fingerprint recognition

3.1 Enrolment Stage

This is the stage where each user is enrolled their fingerprint as a unique ID to use services/access of the enroller. This stage consists of five sub-stages as illustrated in Fig. 1. a).

Image of the fingerprint of the subject is first captured using one of fingerprint capturing technologies [4]; {E.g. optical, capacitive and Radio Frequency (RF)}. The captured fingerprint images are then processed at the image enhancement stage so that the following stages can be performed. The resulting image will generally be of binary.

A number of features are then extracted from the processed image. Three levels of features are identified in a typical fingerprint image [5]. Level-1 features are ridges and valleys as shown in Fig. 2. As can be seen in this figures, ridge-valley forms a number of different patterns; loop, arch, whorl and tented arch. Level-2 features are shown in Fig. 3; ridge endings, bifurcation (two ridges join), ridge ending or terminations, cross-over (two ridges are connected by a small ridge), point/island (isolated very small ridge) and spur (short branch in a ridge).

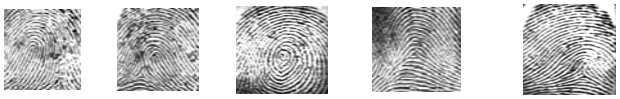


Figure 2. Level-1 features

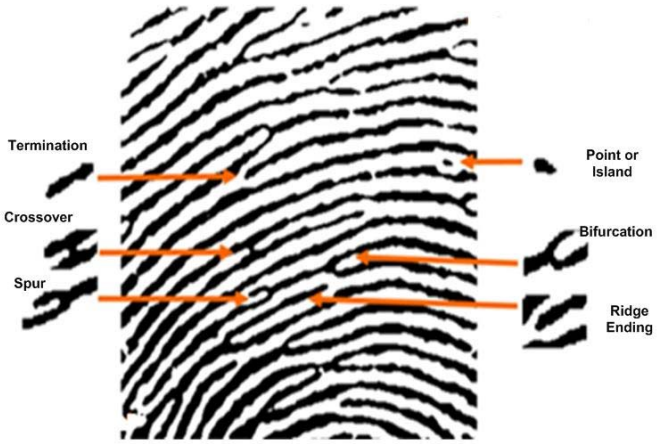


Figure 3. Level-2 features

Leve-3 features are basically pores, their shape, size and distribution and width of ridges. Pores are very small openings distributed on ridges and they become open to discharge sweat liquid to keep thermal balance of the body. While Level 1 and level 2 features are currently used in commercially available AFRSs, level 3 features is still under research and development stage as it requires high-resolution image capturing to extract and process [6]. However, level 3 features have been intensively used in forensic and high security applications which are mainly based on manual investigation of pores.

Once features are extracted, then one or more templates are generated using the extracted features. These templates are then stored in a database for the use in matching process for 1: N matching or in an identity document such as identity card or passport for 1:1 matching.

There is a number AFRS uses more than one fingerprint for increased security and accuracy. The features obtained from the fingerprints are then fused and encrypted for efficient and secured storage [6,7].

3.2 **Recognition Stage**

Recognition stage is illustrated in Fig.1b. When the subject is presented with his finger/fingers to the AFRS, the AFRS first captures the required fingers. The captured fingerprint images are then undergo same image processing procedure as done in the enrolment stage and the same set of features are extracted same way as it is done in enrolment stage. The extracted features are then matched against either the templates stored in data base for 1: N matching or the single template stored in the identity document (e.g.: identity card or passport) for 1:1 Matching.

Depending upon the criteria used, the results from the template matching are scored and final decision is arrived to accept or reject the subject as the subject that claimed to be.

3.3 **Recent developments in AFRS**

The two typical measures used in assessing fingerprint are FAR (False Acceptance Rate) and FRR (False Rejection Rate). The fist one indicates the percentage of wrongly accepted fingerprint and second one indicates the percentage of wrongly rejected fingerprint. Ideally both figures should be zero. However, there are number of reasons theses figures are not zero and some of the reasons are low quality of image capturing technology, inherent pressure applied on the image capturing device when presenting the finger, orientations of finger, permanent or temporary damage in fingers, in ability to exact the features more accurately.

There have been number of developments attained over a decade not only to bring FAR and FRR to very close to zero but also to make the recognition process more reliable, robust, highly secured, user friendly and robust [1]. These developments include (but not limited to) high-resolution image capturing sensors, touch-less capturing technology, multi-finger recognitions through fusions and encryption of templates [8].

There are still number of areas needs improvement in AFRS and two of such areas are liveness detection and recognition without the cooperation of the subject. Liveness detection is when fingerprint is presented to the AFRS, it should be able to detect if the finger is real or an artificial one. There have been a number reports that artificial fingerprint have been used to fool the AFRS [9].

Currently AFRS needs the subject to willingly present to the system to perform the recognition. The image capturing is performed in a controlled manner. However it may be useful to capture and process the fingerprints without any cooperation the subject, possibly at a distance, known as unsupervised recognition. Liveness detection and unsupervised recognition can be useful in high-security applications such as border control, homeland security, forensic and criminology and anti-terror activities [10].

4. APPLICATIONS OF ARFS

In this section three products performing automatic fingerprint recognition for identity management are compared and contrasted. DERMALOG AFIS from Dermalog, Germany, MiY-ID from Cogent systems, USA and Morpho (Safran group), USA are chosen for the case studies. The pictures of these products are shown in Fig. 4. [13,15].

A number of technical attributes of these products are summarized in the Table 2. These data are collected from the technical specifications sheet of the products as posted on their website [14,15].

The first two systems only uses fingerprints and the last one use both fingerprint and smart card for recognition process. Derlog and MorphoSmart can be applicable in a number of various situations based on PC and other operating systems whereas MiY-ID is designed to use only for access control device. All three products is regulated by globally accepted such as American National Standards Institute (ANSI), National Institute of

Standards and Technology (NIST), Federal Information Processing Standard (FIPS) and Federal Bureau of Investigation (FBI).

(a)

(b)

(c)

Figure 4. Three commercially available AFRSs used in the study (a) DERMALOG AFIS (b) MiY-ID and (c) Morpho

All three use optical technology for image capturing. All three products capture images with 500 ppi resolution which allow the systems to extract and use level-1 and level-2 features in the fingerprint. In terms of orientations, Dermalog has capability of handle a variation of up to 3600 whereas MiY-ID can only cope with a variation of up to 900. Though MorphoSmart is not designed to handle variation in orientation, it instructs the user for precise orientation as well as right pressure applied on to the scanner. All three products can perform identification process (1: N matching). However DERMALOG and MarphoSmart can also be used for authentication (1:1 matching). When the speed of the matching processing is concerned, DERMALOG performs exceptionally well with 100,000 matches per second compare to MorphoSmart with only 12500 matches per second. This large difference may be due to the fact that DERMALOG is run on PC or UNIX computer system whereas MorphoSmart is run on dedicated standalone device. Miy-ID and MophoSmart provides security for template by having encryption whereas DERMALOG does not provide any encryption methods for template storage. None of these product support spoof attack.

Table 2. Summary of three ARFS

No	Product name	DERMALOG AFIS	MiY-ID	The MorphoSmart™ 1300 Series
1	**Vendor**	Dermalog, Germany	Cogent system, USA	Morpho (Safran group), USA
2	**Description**	Automatic Fingerprint identification system	Multi-functional outdoor access control reader	A family of multi-factor authentication peripherals using fingerprint and smart card technologies.
3	**Standards**	ANSI/NIST	FIPS 140-2, FIPS 201	FIPS 201, NIST, FBI
4	**Application**	Police and Civilian applications	Access control	logical access control to highly secured desktop PC applications,
5	**Scanning technology**	Standard flat bed scanner optical scanning and chip live scanner	Optical scanner	Optical sensor
5	**Image resolution**	500 ppi	500 ppi	500 ppi
	Rotation angle variation	360^0	+/-45 ^{o}	None. User guided through instruction
6	**Platforms**	MS Windows/solarise/Linux	Stand alone	Standard alone
7	**Database**	Oracle, SQL Server, Informix,	PACS	Local and remote
8	**Matching**	1:1 and 1:N	1:N	1:1 and 1:N
9	**Matching speed (minimum)**	100,000 matches / second	Not available	1250 matches/second
11	**Security of template**	No	yes	yes
12	**Liveness included**	No	No	No

This comparison study extracts the fact that AFRS has many variations in its specifications which depend on the type of use.

5. CONCLUSION

Automatic Fingerprint Recognition System has been used for many identity management applications and has evolved over the decade very rapidly. The need for automatic fingerprint identification has increased over a decade, both commercial and government applications. Image capturing technologies, image enhancement and image matching algorithms have advanced to a state where the fingerprint recognition can be performed with high accuracy and low FAR and FRR. These advancements have been varified through a comparison study among three commercially available AFRSs and presented in this paper. From this study and literature, it can also be concluded that future work should include liveness detection and unsupervised identification in order to make the AFRS more appropriate in modern-world high security applications.

Overall AFRS has simplified the complex identification process to a single point (a fingerprint) with many advantages in terms of economy, reliability, robustness, user-friendly, and efficiency.

6. REFERENCES

[1] Maltoni, D., Maio, D., Jain, A.K., and Prabhakar, S. (2009), *Handbook of fingerprint recognition-second edition*, Springer, New York.

[2] Gupta, A., Buckley K., and Sutton R. (2008), "*Latent fingermark pore area reproducibility*", Forensic Science International, Vol. 179, No. 2-3, pp. 172–175.

[3] Chellappa, R., Phillips, J. and Reynolds, D. (2006), "*Special Issue on Biometrics: Algorithms and Applications*", Proceedings of the IEEE, Vol. 94, No. 11, pp. 1912-1914.

[4] Memon, S., Sepasian, M. and Balachandran, W. (2008), "*Review of Finger Print Sensing Technologies*", Proceeding of the 12th IEEE International Multitopic Conference - INMIC 2008, pp. 226-23.

[5] Jain, A., Chen, Y. and Demirkus, M. (2006), "*Pores and Ridges: Fingerprint Matching Using Level 3 Features*", Pattern Recognition, ICPR 2006. 18th International Conference on Pattern Recognition (ICPR), Vol. 4, pp. 477-480.

[6] Manivannan, N., Memon, S. and Balachandran, W. (2010), "*Automatic detection of active sweat pores of fingerprint using high- pass and correlation filtering*", Electronics Letters, Vol. 46, No. 18, pp. 1268-1269.

[7] Barni, M., Bianchi, T., Catalano, D., Di Raimondo, M., Labati, R.D., Failla, P., Fiore, D., Lazzeretti, R., Piuri, V., Piva, A., and Scotti, F. (2010), "*A privacy-compliant fingerprint recognition system based on homomorphic encryption and Fingercode templates*", Biometrics: Theory Applications and Systems (BTAS), Fourth IEEE International Conference on Biometrics: Theory Applications and Systems (BTAS), pp. 1-7.

[8] Xiaohui, R., Jinfeng, Y., Henghui, L. and Renbiao, W. (2009), "*Multi-fingerprint Information Fusion for Personal Identification Based on Improved Dumpster-Shafer Evidence Theory*", Electronic Computer Technology, International Conference on Electronic Computer Technology, pp. 281-285.

[9] Nixon, K.A., Robert, V.A. and Rowe, R.K. (2007), *Spoof Detection Schemes*, Handbook of Biometrics, Springer.

[10] http://www.planetbiometricts.com/article-details/i/459 (accessed 27/01/2011)

[11] http://www.wenturedigital.com/component/content/article/ 35-latest-headlines/46-fingerprint-biometric-market-growth.html. (accessed 27/01/2011)

[12] http://acuity-mi.com/Future_of_Biometrics.html (accessed 27/01/2011)

[13] http://www.dermalog.de/english/3/38/AFIS.html (accessed 27/01/2011)

[14] http://www.cogentsystems.com/MiY-ID.asp (accessed 27/01/2011)

[15] http://www.morphotrak.com/MorphoTrak/MorphoTrak/IM/ mt_mso1300_ser.html (accessed 27/01/2011)