Security Issues in Automated Fingerprint Identification Systems

Shahzad Memon, Nadarajah Manivannan, Azad Noor, and Celalettin Tigli

Abstract:

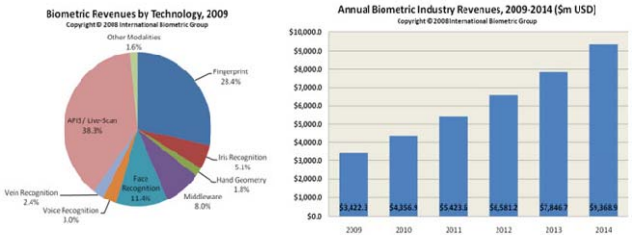
Automated electronic identification systems have been implemented in many sectors to provide identification and secure access. Although the widely accepted Automatic Fingerprint Identification systems (AFIS) have many potential applications in recent years, many published articles, reports and media news indicate that these systems are not fully secured and vulnerable to attacks at different levels. One of the most popular tests that have been carried out to spoof these systems was submission of fake fingertips or artificial fingers to the sensor. In many cases, these attacks have been successful. This paper discusses security issues with AFIS at various system levels. Furthermore, proposed solutions in literature and research articles have also been reviewed.

Index Terms: Fingerprint, AFIS, Security, Liveness Detection.

I. INTRODUCTION

Fingerprint biometrics based identification systems are so popular today and they have become the synonym for biometric systems. The use of Automatic Recognition and Identification Systems (ARIS) for maintaining security has increased globally in the last decade. These systems are practically implemented at various places such as airport, border and immigration control, cash machines and mobile devices. These ARIS uses physical and psychological traits of an individual (known as biometrics) for positive identification [1]-[5].

Among the available biometrics, the fingerprint as a biometric trait for personal identification is both the oldest mode of personal identification and the most prevalent in today use. Fingerprint has been used by law enforcement agencies since the late 1800s, and machine based fingerprint systems has been commonplace since the 1960s [6],[7] . In the recent years, the Automated Fingerprint Recognition Systems
(AFIS) has become an essential tool for many physical and logical access control and homeland security and border control [9, 10].



(a) (b)

Fig. 1 Market Share for Biometric Technologies [8]

Fig. 1 shows the market share of Biometric Technologies during the period 2009 – 2014[8]. As can be seen in Figure 1(a), in 2009, fingerprint biometric (fingerprint and AFIS) is leading by having market share of ~62% followed by face recognition (~11%). Figure 1(b) shows that revenue of biometric market will triple in 2014 compared to 2009.

This paper is structured into six sections. Fingerprint characteristics are explained in section two and main functioning of AFIS is discussed in section three. Issues with AFIS are presented in section four. Proposed solutions to overcome major issues with AFIS are discussed in section five and finally a conclusion is drawn in section six.

II. FINGERPRINT CHARACTERISTICS

A number of features are extracted from the captured and processed fingerprint image. There are three levels of features identified in a typical fingerprint image [10]-[12]. Level-1 features are ridges and valleys as shown in Fig. 2. As can be seen in this figure, ridge-valley forms a number of different patterns; loop, arch, whorl and tented arch. Level-2 features are shown in Fig. 2; 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).

Shahzad Memon, IEEE Member, Centre for Electronics Systems Research (CESR), Electronics and Computer Engineering, School of Engineering and Design, Brunel University, London, UK.
shahzad.memon@brunel.ac.uk

Nadarajah Manivannan, IEEE Member, Centre for Electronics Systems Research (CESR), Electronics and Computer Engineering, School of Engineering and Design, Brunel University, London, UK.
nadarajah.manivannan @brunel.ac.uk.

Azad Noor, PhD Student, Centre for Electronics Systems Research (CESR), Electronics and Computer Engineering, School of Engineering and Design, Brunel University, London, UK.
azad.noor @brunel.ac.uk.

Celalettin Tigli, Postdoctoral Research Fellow, Centre for Electronics Systems Research (CESR), Electronics and Computer Engineering, School of Engineering and Design, Brunel University, London, UK.
celalettin tigli, @brunel.ac.uk

Fig.2 Levels of Fingerprint Features

Level-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 active 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 [13]. However, level 3 features have been intensively used in forensic and high security applications which are mainly based on manual investigation of pores.

III. AUTOMATIC FINGERPRINT IDENTIFICATION SYSTEM (AFIS)

Automatic Fingerprint identification System (AFIS) is based on four modules:

- Fingerprint Sensor
- Signal processing
- Software interface
- Fingerprint Template database

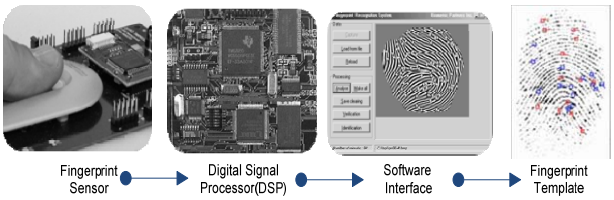


Fig.3 Automatic Fingerprint Identification System (AFIS)

In AFIS, sensor module is a basic and important module of system. There have various sensing technologies been introduced for performing fingerprint sensing. In general, they are divided into optical and solid state as shown in Figure 4. As shown in this figure, sensors based on optics include total internal reflection, optical fiber, sheet prism, electro-optical and In-finger light dispersion and solid state based sensors uses various techniques; capacitive, Thermal, pressure, acoustic and radiofrequency

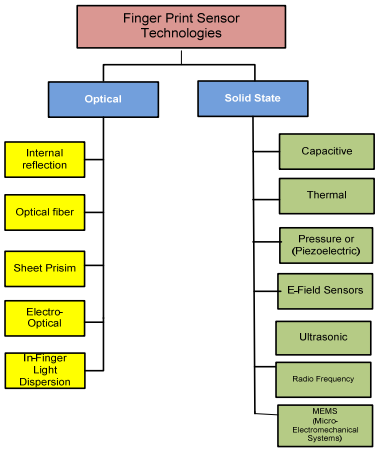


Fig.4 Fingerprint Sensor Technologies [14]

TABLE.1
VENDORS AND TECHNOLOGIES

Vendor	Technology	Model	DPI
Fujitsu http://www.fujitsu.com	Capacitive	MBF200	500
Atmel http://www.atmel.com	Thermal	AT77C104B	500
Ultra Scan http://www.ultra-scan.com	Acoustic (Ultrasonic)	Ultratouch Model 203	500
Biometric Fingerprint (BMF) http://www.bm-f.com	Pressure	BLP-100	500
Authentic http://www.authentec.com	Capacitive	TCS1	508
Biometrika http://www.biometrika.it	Optical	FX integrator	569
Mitsumi http://www.mitsumi.co.jp	Optical	SEF-A1F1	600
NEC http://www.nec.co.jp	Scattered light in the finger scanning system	PU900-10	1000
Light -On Semiconductor Corporation www.liteon-semi.com	Optical	FLB6100	1200

The performance of many of the existing fingerprint sensors is subject to spoofing (fake and dummy) and identification and authentication is limited to ~85%. For this purpose a critical literature review completed for this research to identify the problems in existing fingerprint sensing technologies. The information about the some vendors and their sensors are provided in following Table-1. Although various improvements to the existing technologies are still taking place, many problems still exit. Apart from their size, cost, their physical state and resolution, differentiation between real and gummy fingers is still a problem.

AFIS involves two stages; enrolment and recognition. Each stage is consists of a number of sub-stages. These two stages and their basic sub-stages are illustrated in Fig. 5

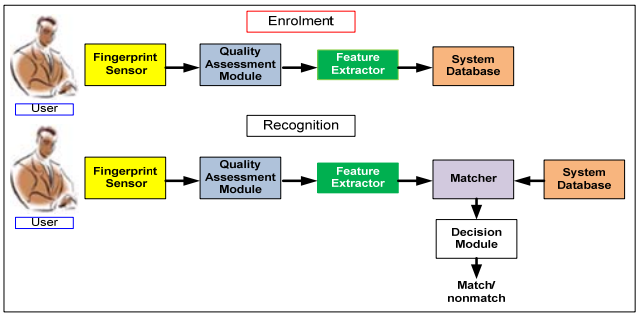


Fig 5. Stages of Fingerprint recognition

A. *ENROLMENT STAGE*

In this stage, each user enrolled their fingerprint as their unique ID. It is consist of five sub-stages as shown in figure 5. The fingerprint sensor captures the pattern of fingertip and the captured image passes through quality assessment module, which checks that quality of obtained image. If the quality of image is matches with the defined parameters then it will pass to feature extraction stage. If not the process of capturing is repeated for a pre-defined certain number of instances. Feature extracting stage enhances and extracts the features of the quality checked fingertip image. The resultant image of this module will be a binary image. Once features are extracted, then one or more templates are generated using the extracted features [1],[15]. These templates are then stored in a database for the use in the matching process. There are two type of matching process exist; 1:N matching and 1:1 matching. 1:N matching is performed for authentication (e.g.: access control) and 1:1 matching is performed for verification (e.g.: passport verification). There is a number of AFIS captures multiple fingerprints to increase the security and accuracy. The features obtained from the fingerprints are then fused and encrypted for efficient and secured storage [1], [16], [17].

B. *RECOGNITION STAGE*

In recognition stage, when user presented with his/her finger or fingers to the AFIS, it first captures the required fingers. Then captured image undergo same procedure and set of features are extracted same way as it is done in the enrolment stage. The extracted features are then matched against either the templates stored in the database for 1: N matching or the single identity stored on identity document (e.g.: passports or Identity cards) for 1:1 matching. Depending upon the predefined criteria, the final decision is made to either accept or reject the user as the user that claimed to be [17, 16].

IV. SECURITY ISSUES IN AFIS

Once a systems' weakness has been found, it gives intruders the ability to use, alter or destroy data stored on system. In AFIS, it is possible that hackers can gain access in system using hardware and software methods at three possible levels.

- Sensor level
- Processing level
- Template database

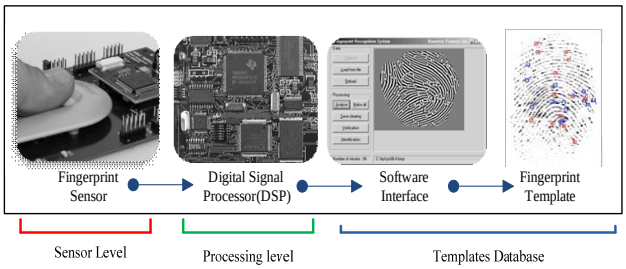


Fig.6 Levels of possible security issues with AFIS

A. *SENSOR LEVEL ISSUES*

The rapid developments in device fabrication technology facilitate to design and develop finger print capture devices with various technologies such as optical, thermal, capacitive, pressure, acoustic and radio frequency (RF). Parallel to improving the fingerprint sensing technologies, various types of attack and forge at sensor level is also improving. However, according to many recent research based on commercially available fingerprint sensing modules, indicates the possibilities of attacks with artificial or gummy fingerprints. Most of the AFIS are compact in size, has adequate resolution and has fast image processing capabilities, but they are not capable to detect liveness of the finger placed onto it. In addition, they have a high value of False Acceptance Rate (FAR) and False Rejection Rate (FRR)[1]-[3], [18],[19]. The FAR is a measure of the possibility that the access system will mistakenly accept an access attempt; that is, will allow the access attempt from an unauthorized user.

$$(\%)FAR = \frac{fa}{n} \times 100 \qquad (1)$$

fa = Number of incidents of false acceptance
n = Total number of Samples

and FRR is a measure the percentage of authorized users that have not been able to enter the system

$$(\%)FRR = \frac{fr}{n} \times 100 \qquad (2)$$

fr = Number of incidents of false rejection
n = Total number of Samples

In the following section the preparation of fake finger prints and tests on fingerprint modules are explained.

Fingerprint Stamps and Artificial Finger

Fingerprint stamps are easy to make to duplicate a real fingertip. Most fake fingerprint stamps are made from gelatin and silicon. However, preparation of fake finger stamps is different and depends on the fingerprint sensing technology used by AFIS. Figure 7 illustrates four common methods for preparation of fake finger stamps that has been successfully tested with commercial AFIS systems[20-23].

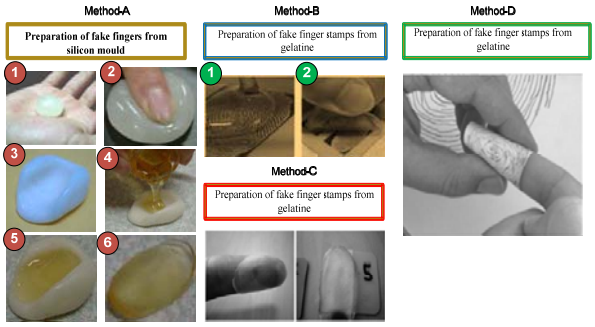


Fig.7 Methods A-D for preparing of fake fingerprint stamps

Method A

This method uses original fingerprint either by directly making a mold of user's finger fingerprint to make an artificial fingerprint as shown in figure 7 (Method A). After making mold from silicon or rubber, it filled with liquid gelatin. The molded fingers are rather transparent and amber while having ridges and valley similar to those of live finger in terms of outside appearance [21]. These duplicate finger stamps have been successfully tested on commercially available optic ' and capacitive technology based fingerprint sensors [21ı. These sensors were successfully deceived by fake finger stamps created with a simple procedure. This study proved that AFIS are not capable to distinguish between fake and real fingerprints.

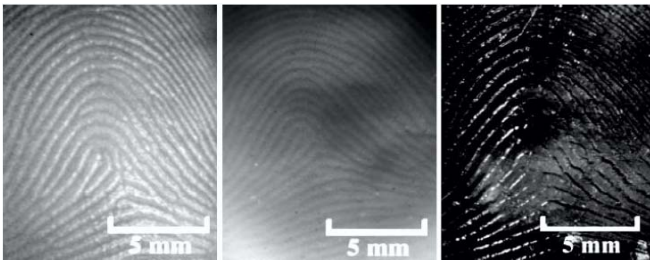
Method B

In this method, a residual fingerprint can be taken from sensor surface or other surface. The gummy finger was produced from a residual fingerprint on a glass plate, enhancing it with a cyanoacrylate adhesive. After taking picture of outside appearance it is scanned and enhanced with image processing software. The final image is further imposed on a printed and etched on a copper board (See Figure 7). Finally, liquid gelatin is spread on etched copper pattern. After drying and removing gelatin from the surface of board, a fake fingerprint is ready to use [21].

Method C & D

These methods are used to create artificial fingers to fool the touch less fingerprint scanners. In method C, the finger is made from glycerin supersedes gelatin which is illustrated in figure 7[24],[20].

Matsumoto[21] showed that 11 types of fingerprint sensors accepted gelatin/gummy fingers, which were easy to make with cheap, easily obtainable tools and materials. The images produced by these fake fingers can be accepted and processed by sensors as a real finger as shown in figure 8.



(a) (b) (c)

Fig 8. a) Live Finger b) Silicon Finger c) Gummy Finger [21]

There are many other possibilities to use fingerprints to get illegal access to the AFIS are discussed in the following section.

Residual fingerprint

Using the residual fingerprint on the sensor surface by dusting graphite powder and then pressing an adhesive film on the sensor's surface to make a fake fingerprint is one of many other techniques [25] . By adding preservative to gelatin based artificial finger, the fake finger can last even more than a week. Also high-resolution camera can be used to photograph the residual fingerprints and that can be used to make fake fingerprints.

The registered finger

Separating the finger from the legitimate user's body, stealing fingerprint of user by making mold or pressing fingerprint sensors by either force or sleeping drug to push the legitimate user [26].

The unregistered (illegitimate) finger

Impostor can use their own finger to try to log in as another user. The probability of this fraud is based either on the high FAR of the system or in case of categorized system such as "loops," "whorls," "arches," by presenting the similar unregistered pattern as registered finger [19].

A genetic clone of the registered finger

Generally, identical twins do not have the same fingerprint, and neither would clones. This can deceive the system if fingerprints are not entirely genetically determined or rather determined in part by its pattern of nerve growth into the skin [2, 19].

Advances in image processing and material technologies have made ways to copy and regenerate perfect patterns of fingertip (e.g valleys, ridges and bifurcation). It is now much easier to make artificial fingers than before. In the last ten years, a lot of

commercially implemented AFIS have revealed their weaknesses in detecting fake finger [20, 22, 25-28].

B. PROCESSING LEVEL ISSUES

Denial of service (DoS)

DoS is a common attack in network based systems. In many applications, AFIS are implemented in a networked environment. A hacker can use DoS to control a system when a legitimate user can no longer access the system [29,30].

Privacy and Subversive

Get access to the system and change a registered user to unauthorized. In that case he/she may not get access to the AFIS or to manipulate the system and use the data for criminal activities [31][30].

Collusion

To get Access to the system by way of colluding between the administrator (super-users) and other users to overrule the decision made by the system[29].

Coercion

Coercion means forcing the legitimate user to identify themselves to the system and access to the system as genuine user [32].

Disclaiming

By using this way, denial of having accesses to the system by authorized user to obtain double personal benefit [31].

C. TEMPLATE DATBASE ISSUES

Another security concern with AFIS is that once the fingerprint data is compromised, the effect will be forever. In fact, many researchers have proven that fingerprint information stored in a database may leak features which can be used to reconstruct a fingerprint image [33]. Some examples are explained here

- A minutiae template can provide three levels of fingerprint information: orientation, class or type and friction ridge structure [34]
- Reconstruct a fingerprint image based on a standard template[35]
- Reconstruct the gray scale image through the phase image. It is also possible to produce the whole fingerprint with few spurious minutiae [36]
- Reconstructing a full fingerprint from partial fingerprint [34]

V. PROPSED CONTERMEASURES FOR AFIS

This section summarizes various protection scheme to find optimum solution to improve the security in AFIS as shown in Table 2.

TABLE.2 COUNTERMEASURES PROPOSED FOR AFIS

Option	Sensor Level	Processing Level	Template Database level
A	The best countermeasure against this attack is liveness detection or combining fingerprint with password or ID card [32]	Deployment of appropriate firewalls, routers, antiviral and anti-spam methods will help to reduce the impact of a system breach by a hacker [30].	A cancelable template is a potential solution in addressing the template security[34-36]
B	Use of method, that works under duress or two-person control or where the system requires fingerprints from two different persons, which are not capable and feasible in every situation [38] .		Diffusion and digital watermarking techniques can be used to improve the security and secrecy of the fingerprint templates database[26, 37].
C	To minimize this kind of attempts, the FAR of system should be reduced and in case of categorized system, not only the evaluation of categories is necessary but fingers within each category as well [39]		
D	Fingerprints are different in identical twins, but only slightly different, this similarity can be tried to deceive fingerprint systems. Therefore, it raises the demand of close watch on such possibility with genetic engineering in fingerprint identification system [40] .		

VI. CONCLUSION

In general, AFIS have been successfully implemented in many applications with the use of a single or multiple fingerprints. In addition, it has many advantages among other biometrics in terms of cost, reliability, robustness, and efficiency. Most importantly, it is cheap compared to other biometrics and user friendly. The possibility of defeating

AFIS lies in its inability to detect liveness at sensing level. The fake fingerprint stamps can make AFIS vulnerable to various possible attacks. From this study, it can be concluded that more work need to be done to include liveness detection and facilitate unsupervised identification in order to make the AFRS more appropriate in modern-world high security applications.

It is therefore necessary to make AFIS more sophisticated by developing new fingerprint sensors with integrated liveness detection capability and high resolution image capturing with improvements in False Acceptance Rate (FAR) and False Rejection Rate (FRR). In addition, more research is required in securing communication channels in particular wireless channels when biometric data is transmitted. Secure database technologies and communication protocols can deter imposters and hackers from attacking AFIS.

REFERENCES

[1] AK Jain, A Ross and S Pankanti, "Biometrics: a tool for information security," IEEE Transactions on Information Forensics and Security, vol. 1, June 2006, 2006.

[2] Anonymous "Reliability, availability and maintainability of biometrics," Biometric Technology Today, vol. 16, pp. 8-10, 3, 2008.

[3] G. Wei and D. Li, "Biometrics: Applications, Challenges and the Future," Privacy and Technologies of Identity, pp. 135-149, 2006.

[4] A. K. Jain and A. Kumar, "Biometrics of Next Generation: An Overview," Second Generation Biometrics, 2010.

[5] A. Juels, "Biometrics in electronic travel documents," in Proceedings of the 12th ACM Workshop on Multimedia and Security, 2010, pp. 1-2.

[6] Cyril H. Wecht, John T. Rago, Forensic Science and Law. CRC Press, 2006.

[7] Maltoni, D., Maio, D., Jain, A.K., Prabhakar, S. (2009, Handbook of Fingerprint Recognition.

[8] International Biometric Group (2008, October 2008). Biometrics revenues by technology 2009. 2009 (/0315), pp. 1.

[9] Nalini Kanta Ratha, Ruud Bolle. (2004, Automatic Figerprint Recognition System.

[10] A. K. Jain, P. J. Flynn and A. A. Ross, Handbook of Biometrics. Springer, 2008.

[11] Anil K. Jain, "Biometric recognition," NATURE, vol. 449, pp. 38-40, September 2007, 2007.

[12] W. S. Coats, "The practitioner's guide to biometrics," in 2007, .

[13] Anil K. Jain, Yi Chen and Meltem Demirkus. (2007, Pores and ridges: High-resolution fingerprint matching using level 3 features. IEEE Transactions on Pattern Analysis and Machine Intelligence 29(1), pp. 15-27.

[14] S. Memon, M. Sepasian and W. Balachandran, "Review of finger print sensing technologies," in Multitopic Conference, 2008. INMIC 2008. IEEE International, 2008, pp. 226-231.

[15] R. Bolle, Guide to Biometrics. Springer verlag, 2004.

[16] A. K. Jain, S. Pankanti, S. Prabhakar, L. Hong and A. Ross, "Biometrics: A grand challenge," in Proc. of IC PR, 2004, pp. 935-942.

[17] A. Moore, "Biometric technologies — an introduction," Biometric Technology Today, vol. 15, pp. 6-7, 1, 2007.

[18] N. K. Ratha and V. Govindaraju, Advances in Biometrics: Sensors, Algorithms and Systems. Springer-Verlag New York Inc, 2008.

[19] V. Lee, "Biometrics and identity fraud," Biometric Technology Today, vol. 16, pp. 7-11, 2, 2008.

[20] C. Barral and A. Tria, "Fake Fingers in Fingerprint Recognition: Glycerin Supersedes Gelatin," Formal to Practical Security, pp. 57-69, 2009.

[21] T. Matsumoto, H. Matsumoto, K. Yamada and S. Hoshino, "Impact of artificial fingers on fingerprint systems," in San Jose, CA, USA, 2002, pp. 275-289.

[22] H. Kang, B. Lee, H. Kim, D. Shin and J. Kim, "A Study on Performance Evaluation of the Liveness Detection for Various Fingerprint Sensor Modules," Knowledge-Based Intelligent Information and Engineering Systems, pp. 1245-1253, 2003.

[23] [23] M. Tistarelli, S. Z. Li and R. Chellappa, "Handbook of Remote Biometrics: for Surveillance and Security," Advances in Pattern Recognition, pp. 382, 2009.

[24] [24] X. Boyen, Y. Dodis, J. Katz, R. Ostrovsky and A. Smith, "Secure remote authentication using biometric data," Advances in Cryptology–EUROCRYPT 2005, pp. 147-163, 2005.

[25] [25] Qinghan Xiao, "Security issues in biometric authentication," in Information Assurance Workshop, 2005. IAW '05. Proceedings from the Sixth Annual IEEE SMC, 2005, pp. 8-13.

[26] U. Uludag and A. K. Jain, "Attacks on biometric systems: A case study in fingerprints," in Proc. SPIE-EI 2004, Security, Seganography and Watermarking of Multimedia Contents VI, 2004, pp. 622-633.

[27] W. David , L. Mike. (2010, Six biometric devices point the finger at security. [Online]. 2010(03/05), pp. 2. Available: http://www.networkcomputing.com/910/910r1.html.

[28] Y. Flink. (2009, 08-01-2009). Million dollar border security machines fooled with ten cent tape. Find Biometrics-Global Identity Management [Online]. 2010(03/13), Available: http://www.findbiometrics.com/articles/i/6090/.

[29] N. Ratha, "Privacy Protection in High Security Biometrics Applications," Ethics and Policy of Biometrics, pp. 62-69, 2010.

[30] K. Saini and M. Dewal, "Designing of a Virtual System with Fingerprint Security by considering many Security threats," International Journal of Computer Applications IJCA, vol. 3, pp. 25-31, 2010.

[31] V. Matyáš, "Security of Biometric Authentication Systems–Extended Version," 2010.

[32] J. Galbally, R. Cappelli, A. Lumini, G. Gonzalez-de-Rivera, D. Maltoni, J. Fierrez, J. Ortega-Garcia and D. Maio, "An evaluation of direct attacks using fake fingers generated from ISO templates," Pattern Recog. Lett., vol. 31, pp. 725-732, 2010.

[33] K. Takahashi and S. Hirata, "Cancelable Biometrics with Provable Security and Its Application to Fingerprint Verification," IEICE Trans. Fund. Electron. Commun. Comput. Sci., vol. 94, pp. 233-244, 2011.

[34] A. T. B. Jin and L. M. Hui, "Cancelable biometrics," Scholarpedia, vol. 5, pp. 9201, 2010.

[35] A. M. P. Canuto, F. Pintro, A. F. Neto and M. C. Fairhurst, "Enhancing performance of cancellable fingerprint biometrics using classifier ensembles," in 2010 Eleventh Brazilian Symposium on Neural Networks, 2010, pp. 55-60.

[36] M. Kaur, S. Sofat and D. Saraswat, "Template and database security in Biometrics systems: A challenging task," International Journal of Computer Applications IJCA, vol. 4, pp. 1-5, 2010.

[37] G. Bhatnagar, Q. Jonathan Wu and B. Raman, "Biometric Template Security based on Watermarking," Procedia Computer Science, vol. 2, pp. 227-235, 2010.

[38] N. Ratha, "Privacy Protection in High Security Biometrics Applications," Ethics and Policy of Biometrics, pp. 62-69, 2010.

[39] F. Sabena, A. Dehghantanha and A. P. Seddon, "A review of vulnerabilities in identity management using biometrics," in 2010 Second International Conference on Future Networks, 2010, pp. 42-49.

[40] J. Fulton, "Fingerprint the point of sale," Biometric Technology Today, vol. 2011, pp. 7-9, 2011.