Vulnerabilities and Performance Analysis over Fingerprint Biometric Authentication Network

Edward Guillen, Lina Alfonso, Karina Martinez and Marcela Mejia

***Abstract*—Fingerprint recognition system with optical sensors is one of the most efficient methods to identify people. This paper propose a method to evaluate vulnerabilities and performance in an identification fingerprint network with optical sensors, in order to establish the convenience of implementing this authentication technique, according to engineering parameters, such as security parameters, recognition time, database size and network architecture.**

***Index Terms*—Authentication, Biometrics, Fingerprint Recognition, Performance Analysis, Vulnerability.**

I. Introduction

BIOMETRIC authentication systems such as fingerprint, facial recognition, iris, gait, among others are increasingly used for people recognition, security procedures and access control by different corporations.

Some specific physical patterns or person's physical characteristics are identified by biometrics systems [1]. Fingerprint authentication systems are widely used thanks to characteristics such as simplicity on implementation, acceptable security level and high performance in fingerprint authentication [2] [3]. However, there are different kinds of sensors for fingerprint scanners including optical, capacitive and thermal sensors. [4]

The choice of hardware varies according to the corporation needs because the fingerprint scanner could be high security and/or high performance and enterprise implements fingerprint reader according to their own convenience. The optical sensors were evaluated in this investigation based on the high marketing of optical devices [5]. Vulnerability tests were done in the physical and electronic system. The data network performance were measured.

The aim of the investigation gives specific information and not only technical about how optical sensor works, the optical sensor performance in network must be analyzed to find the system delay for multiple fingerprint authentication actions. The potential final user will be able to know if the security and performance offered fit the system or if final users have to look for other sensors or biometric systems in order to fulfill user requirements.

The second part of this paper will lay emphasis on how the fingerprint biometric systems and the optical sensor work. In the third part, the vulnerabilities and performance will be identified and with this information a conclusion will be made about how this system works and the future research to do will be proposed.

A. Previous Research

In 2000, Putte and Keuning [6] evaluated many fingerprint sensors vulnerabilities with false fingerprints created a wafer-thin silicon dummy. Their work describe two different methods to create false fingerprints: the first method is with the cooperation of fingerprint owner and the second one is without the cooperation of the user. In the case the fingerprint owner cooperate to elaborate the fake fingerprint, the quality of the imitations is increased and the system is more likely to be deceived. Six sensors were evaluated and five of them such as optical and solid state sensor accepted the false fingerprint as valid. [6]

Moreover, in 2010, B. Ashwini et al from India carried out a comparison among 9 types of sensors; the researchers analyzed and compared the sensors' precision, tolerance, resolution, compatibility and limitations, in order to make known the specifications and properties of each of them for future engineering designs. [7]

Likewise, in 2011, inside the 'Institute for Informatics and Automation Problems', D. Kocharyan and H. Sarukhanyan proposed a high speed method for the recognition of fingerprints based on minutiae matching, the minutiae is an unique characteristics of each fingerprint. The high speed method takes into account region and line structures that exist between minutiae pairs, parameters that would allow them to get more structured information from the fingerprint. [8] The final method includes the following steps: 1)Binarization: the image is converted into a scale of grays and then into binary data; 2)Filter Block: the binarized image is diluted to reduce the thickness of the lines of the ridge to just one pixel; 3)Details Extraction: the details, bifurcations and ridges are defined through the algorithm of the crossed Number; 4)Details Coincidence: the characteristics previously obtained are compared with the database through a matrix and finally accepted or rejected. The authors finally develop a fingerprint recognition system based on the method proposed, a high speed method includes more details inside the image for more structured information and better minutiae precision.[8]

In 2010, K. Martinez et al identified the vulnerabilities of the fingerprint system through physical and electronic supplanting. [9]

This work was supported in part by the Military University Nueva Granada ING 831

E.Guillen is with Telecommunications Engineering Department, Military University Nueva Granada (e-mail: edward.guillen@unimilitar.edu.co), Bogota, Colombia.

L.Alfonso is with Telecommunications Engineering Department, Military University Nueva Granada (e-mail: u1400555@unimilitar.edu.co), Bogota, Colombia.

K.Martinez is with Telecommunications Engineering Department, Military University Nueva Granada (e-mail: securityinvgroup@unimilitar.edu.co), Bogota, Colombia.

M.Mejia is with Telecommunications Engineering Department, Military University Nueva Granada (e-mail: angela.mejia@unimilitar.edu.co), Bogota, Colombia.

II. Fingerprint and Sensor Authentication System

Fingerprint authentication systems have four basic parts as shown in Fig 1 [10]. After these processes, a verification decision is made with the results of similarity obtained from the matching step.

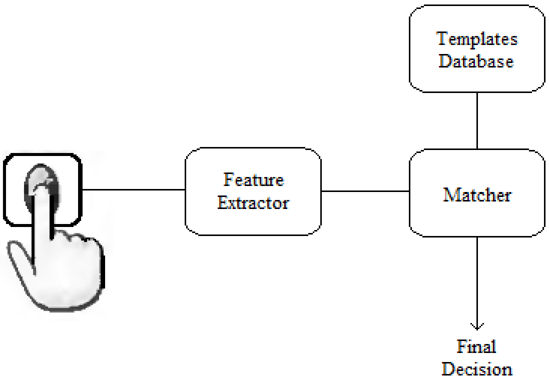

Fig. 1. Block of Fingerprint Authentication System [9] with an optical scanner, feature extraction, matcher and database sever.

Live-scan images are acquired with optical sensor, some points or minutiae different for each individual are identified in the image; image is processed by the characteristics extractor to create a model or template of the fingerprint. In the comparison process, template is used in order to determine the user's identity. Finally the biometric system accepts the user or a warning message indicate that the user was not found in the database.

A. Fingerprint

A protruding portion of the skin known as ridges usually appears as a series of black lines in fingerprint image, while the valleys appear as a white space and they are the lowest parts as shown in Figure 2 [10]. Fingerprint identification is based mainly in the minutiae, or the location and direction of the ridge endings and bifurcations along a ridge path. [11] [12]

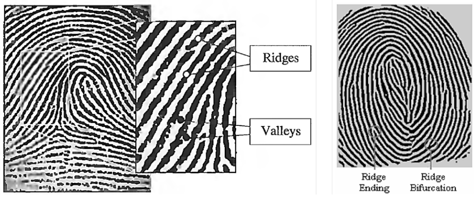

Fig. 2. Minutiae of a Fingerprint [11] [13]. The most evident characteristics of a fingerprint.

B. Fingerprint Acquisition Sensors

There are two ways to acquire a fingerprint; the first one is through an inked impression and the other one is on-line through a scanner [10]. The most important part of a fingerprint scanner is the sensor because the fingerprint reader scan the fingerprint image. Most of the existing sensors belong to one of these three families: optical, solid state and ultrasound. Due to the cost and applicability of them, the investigation works and study the first type of sensor.

Figure 3 shows Frustrated Total Internal Reflection -FTIR-, the livescan acquisition technique for an optical sensor. When the finger surface contact with the crystal or sensor surface, a change is produced in the internal reflection of the light; the ridges and valleys [14] modify the angles and directions of the incident light beam, this change makes a clear image of the finger surface and the ridges can be discriminated from the valleys. [15]

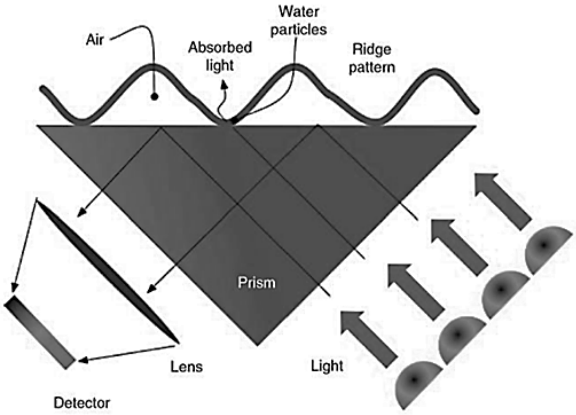

Fig. 3. Optical Scanner System [16]. The right side of the prism is illuminated through a diffused light, in the left side the lens onto a CMOS image sensor receives the light rays.

III. Evaluation Methodology

The evaluation process for fingerprint recognition system is analyzed in two parts. In the first part, the analysis identifies the current vulnerabilities in the system. In the second part, system performance includes a database server, the application developed, the fingerprint scanner and the network in general. Network delay was analyzed during the evaluation process.

In [17] and [5], the attacks to the biometric identification systems are classified in two big groups: the first group are direct attacks, the physical devices are directly attacked, as is mentioned in [6], [15], [18]. False Fingerprint and Damage to the Sensor are direct attacks; the second group are indirect attacks, the authentication systems are infringed by illegally accessing the communication channels to extract or modify the information in the database as is mentioned in [19],[20],[21]. Sniffing, Hill Climbing, Trojans, Inverse Engineering and Snooping are indirect attacks.

Once the vulnerabilities that affect the system have been detected, a test evaluates a series of parameters that identify the risk of the fingerprint system, and the results allows to the final user to make a decision about the biometric system to implemented.

A. Number of Vulnerabilities

This variable defines the amount of vulnerabilities that can occur in both a physical system and an electronic system.

B. Ease of Attack -EA-

Ease of attack defines the grade of complexity required to perform some existing attacks in the fingerprint verification systems having in consideration some support parameters. EA was measured in a scale from 1 up to 4, where 1 means the attack is unlikely to occur because it is very difficult to carry it out and 4 means the attack is very easy to occur because of its easiness. [9]

To be able to determine the ease of attack, four fundamental parameters must be taken into account such as:

1) Attack Probability -AP-: AP determines the frequency wherewith the attack can occur.

2) Attack Speed -AS-: AS specifies how fast in terms of time an attack can be performed; this point is explained in Table I.

TABLE I
EASE OF ATTACK

Time Concept	**Time-hour-**	**Score**
High	more than 24	1
Moderate	11-24	2
Significant	5-10	3
Little Significant	less than 5	4

3) Quality of Information -QuI-: This parameter shows how detailed is the information found in order to perform an attack. Table II specify the scoring of this parameter.

TABLE II
QUALITY OF INFORMATION

Quality of Information	**Definition**	**Score**
Very Little Explanatory	Indicates where to find information	1
Little Explanatory	Mentions the process	2
Explanatory	Explains the process	3
Very Explanatory	Details the process	4

4) Quantity of Information -QI-: How much information can be found about an attack; Table III explains each parameter used to evaluated QI.

TABLE III
QUANTITY OF INFORMATION

Quantity	**QI -videos, books, articles-**	**Score**
Very Little Information	less than 2	1
Little Information	2-5	2
Enough Information	6-10	3
Much Information	more than 10	4

Once all the attributes that determined the ease of attack are explained, equation 1 represents the final score of EA:

$$EA = 0.3 * AP + 0.3 * AS + 0.2 * QuI + 0.2 * QI \quad (1)$$

If AP, AS, QuI and QI tend to the lowest score, then EA is 1; 1 indicates the attack is very difficult to execute, but if on the contrary AP, AS, QuI and QI tend to get a score of 4, 4 indicates that there is a high probability for the attack occurs.

C. Attack Impact -AI-

AI shows the impact or consequence that some vulnerabilities can produce in the verification system. Just as the previous parameter, attack impact is also scored from 1 to 4 as shown in Table IV.

TABLE IV
ATTACK IMPACT

Consequence	**Risk**	**Score**
Attack against the communication channel	Low risk	1
Attack to the sensor	Potential risk	2
Repetitive Attack with software against the system	Significant risk	3
Attacker replaces an entity of the system	High risk	4

D. Risk Level -RL-

RL measures the risk level during an attack taking into account the variables ease of attack and the impact of system vulnerabilities. The values for risk level goes from 1 up to 16 and equation 2 shows how the score is calculated.

$$RL = EA * AI \quad (2)$$

If the result obtained by RL is between 1 and 5, the vulnerability has low risk and values higher than 5 are considered of medium high level and they must be analyzed carefully in order to try to eliminate these attacks or control them.

E. Average Connection Time -ACT-

ACT measures the application connection time with the database server on network independent from the number of records stored.

F. Average Inscription Time -AIT-

AIT evaluates the performance of both the algorithm and the network during the storage of data from a user. Besides, AIT shows the time in seconds that the whole network takes to do this process.

G. Average Comparison Time -AComT-

AComT evaluates the network performance in the comparison and identification of a fingerprint. The response time and latency in seconds is measured from the database towards the application.

IV. PERFORMANCE ANALYSIS

The algorithm by Griaule Biometrics was used to develop the identification application since it was the winner of FVC -Fingerprint Verification Competition- [22], the competition evaluated multiple algorithms and sensors, besides different security and speed parameters.

To carry out the analysis of the system performance, first an application was developed, the application allow to store 3 fingerprints from each finger in a total of 30 fingerprints records per person into a database server on network and besides the application verifies and identify person's identity through his fingerprint.

Some devices has an internal database but system storage capacity is limited to a small number of records by the local database. For that reason this investigation implemented a network system, the database server could measure the real time performance of an access control system and this network system could also respond the needs of any user.

The network shown in Figure 4 helps to measure the scanner performance, the connection time of the database and the recognition time of a fingerprint.

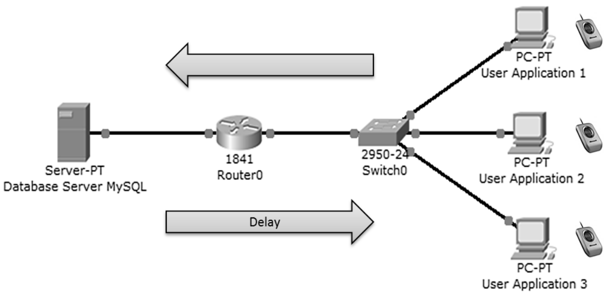

Fig. 4. Network System Implemented. The system allows the connection of more than 1 simultaneous users to the same database

The network characteristics includes a database server by MySQL with a 256GB hard drive and 4GB RAM, link speed of 100Mbps and an optical sensor reader by Microsoft. First, performance tests was carried out with a database of 50 records or fingerprints stored; then, stored records was increased to 100, 150 and 200 fingerprints, finally the test was done with a sample of 390 fingerprints stored.

V. Vulnerabilities Results

The results obtained by the study are shown in the following items.

A. *Number of Vulnerabilities*

Some false fingerprints were created by 3 different methods as is mentioned in [15], [23], [24] and the fake fingerprints were analyzed over an optical sensor in order to prove if they can be identified as false fingerprints or not.

The first method includes collaboration of the user where user's fingerprint is captured with ink on a piece of paper; in the second method, a latent fingerprint was gotten from a transparent surface, just a few of carbon powder was applied to make the fingerprint more visible and fake fingerprint on tape was also used, the optical sensor was proved to know if the device could receive the fake fingerprint as a real user; and in the third test was used molding plasticine or some soft surface like plaster in order to recreate person's fingerprint to falsify.

The first two methods did not leave favorable results to infringe the sensor, since 2 fingerprints were made, one from the index finger and the other from the thumb. The system was tested 10 times with each fingerprint made but the system was not able to read them since the fingerprint was in 2D and the scanners can not handle because FTIR technology only reads elements in 3D; however, when the third method used 3D fingerprints, the optical sensor was infringed more than 60 %; the final result allows to conclude that the better the fingerprint is made and the less the rotation obtained while the fingerprint is on the sensor, the success percentage will be higher for the attacker.

TABLE V
Test of False 3D Fingerprint on an Optical Sensor

False Fingerprint	Attack Attempts	Attacks Accepted	Attacks Rejected
Index Finger	10	6	4
Thumb Finger	10	3	7

B. *Ease of Attack*

Taking into account the vulnerabilities described previously and applying the equation 1 to them, Figure 5 shows the final results of all the vulnerabilities analyzed.

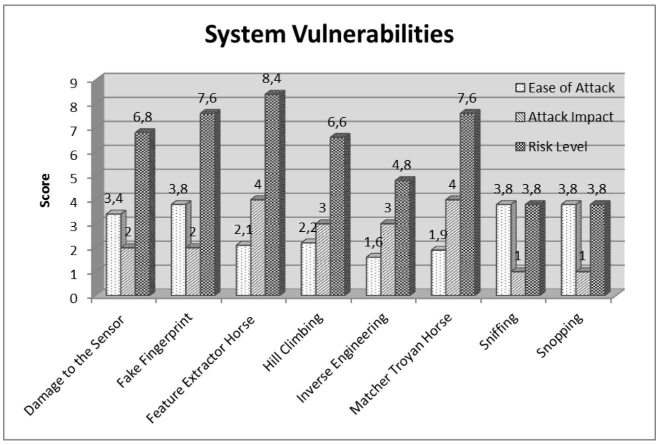

Fig. 5. Test results of attacks, impact and risk level of the system

Figure 5 shows the system vulnerabilities, the results determinate that four of the vulnerabilities such as false fingerprints, damages to the sensor, snooping and sniffing obtained scores above 3 points; this result allow to conclude that these vulnerabilities were the easiest to carry out and hence they are the most frequent and used when attackers try to infringe the system. However, even though the other vulnerabilities did not get high scores due to its complexity, these vulnerabilities must not be ignored because these attacks could infringe the system if the attacker has enough knowledge about it.

C. *Attack Impact*

Attacks who got scores equal or higher than 3 could replace an electronic unit or through repetitive attacks could create images achieving the access of non-authorized users; Feature Extractor Horse, Hill Climbing, Inverse Engineering and Matcher Troyan Horse were previously consulted and special interest must be given to them in order to avoid these attacks while the rest of the attacks must be taken in consideration.

D. *Risk Level*

The risk level is obtained through the multiplication of the parameter Ease of Attack by Vulnerability Impact, leaving the results in Figure 5.

From Figure 5, the attacks with scores higher than 6 such as Hill Climbing [25], Service Negation Attack, Fake Fingerprint and Trojans could affect the system in a considerable way even by accepting non-registered users; hence, a series of pertinent measures must be taken in case the system must be secure. Those attacks with lower scores than 6 must not be ruled out even though they are unlikely to happen.

VI. Performance Result

A. Database Connection

The first test establishes the application connection time with the database, this time has not relationship with the number of records stored and the type of sensor but this time is part of the latency of the system.

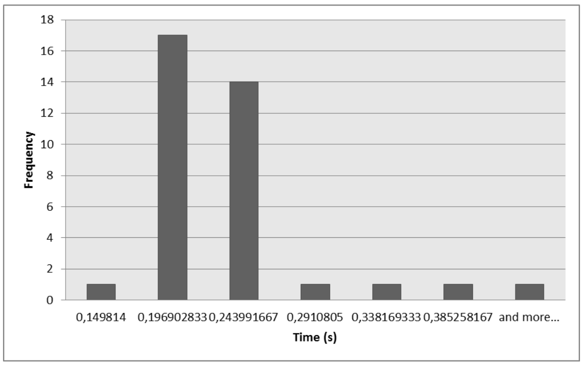

Fig. 6. Connection Time Histogram.

Figure 6 shows the application connection time behavior with the database. To establish the connection time the average was found of different successful connection attempts, then the standard deviation was found in order to identify and establish which periods has the highest frequency.

$$GeometricMean = 0.2076s \tag{3}$$

$$StandardDeviation = 0.0584s \tag{4}$$

The geometric mean is according to the Figure 6, between 0.1969s and 0.2439s is the most average time. These results are efficient because whatever the amount of information contained in the database, these times are not affected and therefore the application can have fast access to database.

B. Inscription Time

The application was developed in such a way that all records were first saved into a vector and when all the templates was taken from all the user's fingers, all data of the vector is sent to the database. This step allows to reduce the inscription time of a person instead of recognizing and sending the information 32 times -number of columns per line-, the information is exported only once.

This process though efficient is not very secure because the data do not travel encrypted and therefore the information could be seen by somebody interested in steeling and/or supplant this information.

Finally, the time of five inscriptions was taken and the geometric mean was determined for the storage time per line or user with the database on a network.

$$AIT = 0.0727s \tag{5}$$

C. Fingerprint Identification

Having a total of 390 fingerprints stored in the MySQL Database Server, an analysis was carried out on different points of it. Tests were done with some records at the beginning, the middle and at the end of the database, and the processing time was analyzed in these points. Now Figure 7 shows the behavior of the geometric mean identification time of the database according to the fingerprint to be recognized.

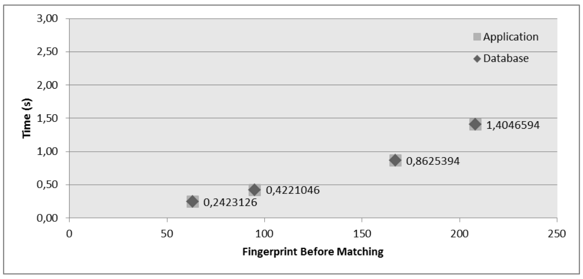

Fig. 7. Fingerprint Recognition Time. It shows the trend of time when the number of records stored are increasing

According to Figure 7, a trend of future results could be determined according to the number of records stored in the database. If there is a tendency of the points found, a potential equation could be:

$$\mathbf{AComT} = 0.0008 * \mathbf{X}^{1.3832} \tag{6}$$

Where **AComT** is the geometric mean identification time in seconds and **X** is the number of records stored in database before the matcher find a match.

As **AComT** increases, the identification time also, so it is recommended if the corporation will work on a database with more than 1000 records, this corporation should work with two parallel database, reducing the time about the half. Table VI shows an approximation of future identification time according to the number of records stored.

TABLE VI
TEST OF FALSE 3D FINGERPRINT ON AN OPTICAL SENSOR

Number of Records Stored Before Find a Match	Identification Time in Seconds
10	0.0192
100	0.4629
1000	11.1350
10000	267.849

Times were measured both in the application as well as in the database in order to get the latency time. Another method to find it is:

$$L = AIT - DIT \tag{7}$$

Where L = Latency
AIT = Application Identification Time
DIT = Database Identification Time

$$L = 0.7565s - 0.7557s = 0.0008s \tag{8}$$

Since this value is very slow, latency can be assumed as a worthless variable into the fingerprint recognition time.

VII. Conclusions and Future Researching

Using an optical sensor during the vulnerability and performance analysis was concluded that the offer quality of service is good enough for access control systems. The developed software allows using more than one server being a scalable system, optical sensors is recommended in systems where quick and efficient processing is required but no a high security level. If higher security is needed, another type of sensor is suggested to implement with life detection in order to avoid infiltration with fake fingerprints.

A recognition system with a network database reduce implementation costs to corporation, because devices with local database do not allow to store a high volume of person's fingerprint and corporation would have to buy a big number of optical sensors, making it not profitable or scalable in medium or long term future.

Therefore, by beginning from the analysis performed in this article, the same procedure with capacitive and thermal sensors is planned to carry out in order to create a choice model among the multiple options found in the market. The best system can be chosen according to the level of security and/or speed required.

Acknowledgment

We would like to thank Security and Communication System Research Group, this research is supported by Military University Nueva Granada, ING 831 "Vulnerabilities and Performance Analysis over Biometric Authentication System Based on Optical, Capacitive and Electric Field Sensors".

References

[1] S. Alotaibi and D. Argles, "FingerID: A new security model based on fingerprint recognition for distributed systems" Congress on Internet Security (WorldCIS), 2011.

[2] A. Bossen, R. Lehmann and C. Meier, "Internal fingerprint identification with optical coherence tomography", IEEE photonics technology letters, vol. 22, no. 7, 2010.

[3] A. Jain, A. Ross and K. Nandakumar, "High resolution ultrasonic method for 3D fingerprint representation in biometrics", Department of Computer Science and Engineering, Michigan State University, East Lansing, Michigan, USA, Introduction to biometrics, Fingerprint Recognition, Springer US. 2011.

[4] N. Ratha and R. Bolle, "Automatic Fingerprint Recognition Systems", Editorial Springer, 2004.

[5] J. Galbally, F. Fernandez, J. Alonso and J. Ortega, "A high performance fingerprint liveness detection method based on quality related features", Future Generation Computer Systems, 2010.

[6] PUTTE, Ton var den; KEUNING, Jeroen, "Biometrical Fingerprint Recognition Don't Get Your Fingers Burned", Septiembre de 2000, 17 ps. [Online]. Available: http://cryptome.org/fake-prints.htm

[7] B. Ashwini, Ladhay, S. Digambarrao and S.P Patil, "Performance Analysis of Finger Print Sensors", IEEE Library, 2010.

[8] D. Kocharyan and H. Sarukhanyan, "High Speed Fingerprint Recognition Method", IEEE Library, 2011.

[9] E. Guillen, D. Padilla and K. Martinez, "Vulnerabilities and Performance Analysis over Fingerprint Recognition Systems", Worldcomp 2010 The World Congress in Computer Science SAM 10, 2010.

[10] D. Maltoni, D. Maio, A. Jain and S. Prabhakar, "Handbook of Fingerprint Recognition", Springer-Verlag New York Inc., 2009.

[11] National Science and Technology Council (NSTC) Subcommittee on Biometrics, 2006. Available: http://www.biometrics.gov

[12] S. Chae, J. Kim, S. Lim, S. Pan, D. Moon and Y. Chung, "Ridge-based fingerprint verification for enhanced security", Conference on consumer electronics, 2009, ICCE '09.

[13] D. Maltoni and R. Cappelli, "Advances in fingerprint modeling", Image and Vision Computing Volume 27, Pages 258-268, 2009.

[14] S. Prabhakar, A. Ivanisov and A.K. Jain, "Biometric Recognition: Sensor Characteristics and Image Quality", Instrumentation and Measurement Magazine, IEEE. ISSN: 1094-6969, 2011.

[15] T. Matsumoto, H. Matsumoto, K. Yamada and S. Hoshino, "Impact of Artificial 'Gummy' Fingers on Fingerprint Systems" SPIE, 2002.

[16] S. Z. Li and A. K. Jain, "Encyclopedia of Biometrics", Editorial Springer, 2009.

[17] J. Galbally, J. Fierrez, F. Alonso and M. Martinez, "Evaluation of direct attacks to fingerprint verification systems", Journal Telecommunication Systems, Springer Netherlands, 2011.

[18] X. Keping and S. Chenxi, "The Research of Optical Non-contact Fingerprint Sample Method", International Conference on Control, Automation and Systems Engineering (CASE), 2011.

[19] O. Martinsen, S. Clausen, J. Nysther and S. Grimnes, "Utilizing Characteristic Electrical Properties of the Epidermal Skin Layers to Detect Fake Fingers in Biometric Fingerprint Systems-A Pilot Study", IEEE Transactions on Biomedical Engineering, 2007.

[20] C.J.Hill, "Risk of Masquerade Arising from the Storage of Biometrics", B.S Thesis, 2001.

[21] N.K Ratha, S.Chikkerur, J.H. Connel and R.M Bolle, "Generating Cancelable Fingerprint Template", IEEE Transactions on Pattern Analysis and Machine Intelligence, Vol 29, pp.561-572, April 2007.

[22] Figerprint Verification Competition. Available: http://bias.csr.unibo.it/fvc2006/default.asp

[23] J. Galbally, J. Fierrez, J. Rodriguez, F. Alonso, J. Ortega, and M. Tapiador, "On the Vulnerability of Fingerprint Verification Systems to Fake Fingerprints Attacks", Proceedings 40th Annual IEEE International Carnahan Conferences Security Technology, 2006.

[24] S. Palk, B.A. Hamilton and H. Wechsler, "Fingerprint Readers: Vulnerabilities to Front- and Back- end Attacks" In Proc, IEEE Biometrics: Theory, Applications, and Systems, 2007. BTAS 2007.

[25] U. Uludag and A. K. Jain, "Attacks on biometricsystems: a case study in fingerprints," in Proc. SPIE, 2004.