ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 11, November 2015

Advanced User Authentication System on Mobile for Signing Digital Transactions

Shagupta M. Mulla[1], Prof. Dr. Vijay R. Ghorpade[2], Mr. Javed J. Mulani[3]

[1]Assistant Professor, BVCOE, Shivaji University, Kolhapur, India

[2] Professor, D.Y.Patil College of Engineering, Kolhapur, India

[3]Assistant Professor, AMGOI, Wathar, India

ABSTRACT: Biometrics are expected to add a new level of security to applications, as a person attempting access must prove who he or she really is by presenting a biometric to the system. Such systems may also have the convenience, from the user's perspective, of not requiring the user to remember a password.All these vulnerabilitiesare minimized by using proposed systemarchitecture for mobile biometric system. This architecture provides an extensible, open, andsecure framework in which different groups can interact to give users a biometric solution that works on multiple operating systems and hardware platforms. It binds user's biometric data with digital signature to generate signed reply to proceed securely for signing digital transactions.

KEYWORDS:Biometric; Digital signature.

I. INTRODUCTION

Identification and authentication requirements are steadily increasing in both the online and off-line worlds. There is a great need on the part of both public and private sector entities to "know" who they are dealing with. The current security model is used mainly for the verification of identity, protection of information, and authorization to access premises or services. It is based on using a token to either authenticate identity or allow access to information, premises or services. This token may be a password or shared secret (something you know), an identity card (something you have), or a biometric (something you are). In all of these cases, the details of the token are held by a third party whose function is to authorize and, at times, allow the transaction to proceed if the details of an individual's token match with those stored in a database. The biometric is increasingly viewed as the ultimate form of authentication or identification, supplying the third and final element of proof of identity. Accordingly, it is being rolled out in many security applications [1].

This system discusses privacy-enhanced uses of biometrics, with a particular focus on the privacy and security advantages of DigitalSignature over other uses of biometrics.

II. RELATED WORK

Authors in [2] have given the detail descriptionof biometrics. Biometrics refers to methods for uniquely identifying and verifying an individual identity based upon one or more intrinsic physical or behavioural traits. In information technology, in particular, biometrics is used as a form of identity access management and access control. It is also used to identify individuals in groups that are under surveillance. The main biometric technologies include face recognition, fingerprint, hand geometry, iris and voice.These systems are based on the following steps: a biometric sample is taken from an individual, for instance a fingerprint or iris scan. This physical characteristic may be presented by an image. Often data are extracted from that sample. These extracted data constitute a **biometric template**. The biometric data, either the image or the template or both, are then stored on a storage medium. The medium could be a database or a distributed environment, such as smart cards. These preparatory phases together constitute the process of **enrolment.** The person whose data are thus stored is called the enrolee. Authors in [3-4] presented the drawbacks of Basic Biometric Systems. The typical biometric system consists of a huge biometric database and one sensor per application or access.The most obvious is compromising the database itself. To overcome this problem, the system designer should encrypt the templates on the database.Unfortunately, doing so can deteriorate the system's quality.Another issue is that

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 11, November 2015

if no active control exists for the system's sensors, attackers can manipulate them or replace them with fakes to steal users' personal data (such as with false ATMs used in banking, or credit-card skimmers). Such data travels over communication lines to accomplish matching.System designers must take extreme care to protect that data from sniffing or spoofing.

Authors in [5-6] have discussed the technique to overcome problems inherent to unique biometric databases. The biometrics industry has proposed architectures such as *match-on-token* or *template-on-token* as shown in figure 1.In these architectures, all users hold a token with their biometric data that never leaves them. Although this solves problems related to database and communication security, the same sensor vulnerabilities still exist. Authors in [7-8] have developed an evolved version of the match-on-token architecture, called the *sensor-on-token* or *fingerprint card*, in which the user has a smart card with a fingerprint sensor.This solution also has its problems. The user must trust that the card is secure because almost no information exists about what algorithms are at work in it or their quality.

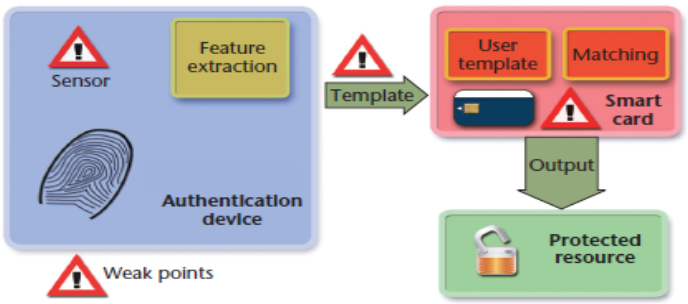


Figure 1. The match-on-token architecture [5-6].

In paper [9] author has given strengths of biometric technology.Biometric systems are widely used for Border Security Control, Crime and Fraud Prevention, Detection, and Forensics, Attendance Recording, Payment Systems, Access Control.

III. PROPOSED SYSTEM

Through the innovative use of biometrics technology, this proposed system will provide a strong authentication approach without sacrificing end-user convenience. When integrated into mobile PCs and PC peripherals, a user's fingerprint can be used as an additional authentication factor to secure access to devices, networks and web-based applications and portals.

- **System Architecture**

Architecture shown in figure 2 is proposed to build on a hardware platform with light requirements. It doesn't need a high-end PDA or computer to use it and some software packages. It can work on any hardware platform with sensing capabilities and one or more communication interfaces.System comprises three modules.

1) **System Core-** The *system core* is the main module controlling the whole system. It handles requests from the outside world and interacts with the user and other system modules.
2) **Certification module-** The *certification module* handles the user's private and public keys and the public-key chain. It's critical to the system and requires anti-tampering protection.
3) **Biometrics module-**Finally, the *biometrics module* senses and extracts features and authenticates the user using the personal characteristics in the device (such as fingerprint minutiae). It has a common API, and users can select from among different modules depending on their security requirements or handicaps, or the biometric modality selected (for example, fingerprints, voice recognition, or iris scanning).

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 11, November 2015

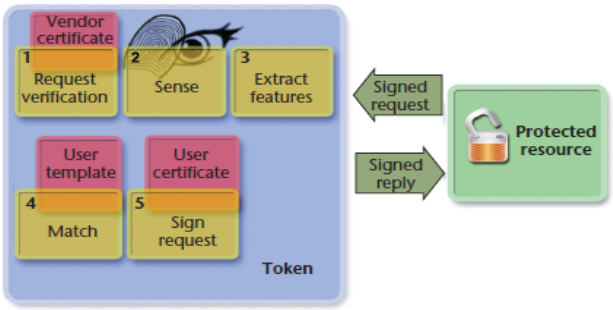


Figure 2. System Architecture.

IV. METHODOLOGIES

The biometric module is used for data collection. The Mobile Biometric System consists of a mobile (token) the user carries that can accomplish all the tasks required of a biometric system:

• sense biometric parameters,
• extract features, and
• match extracted features with the original features, delivering a yes/no answer.

In addition to conducting functionalities common to any biometric system, the token should be able to communicate with the outside world in a secured, authenticated way and provide the user with straightforward information about what he or she is accepting. A transaction's output is just a signed reply without biometric information. The token can be any device with sensing, processing (as with fingerprint sensors or cameras), and communication capabilities (such as the Global System for Mobile Communications).

A. Fingerprint Acquisition

System is using Futronic FSS88 FIPS 201/PIV Fingerprint Scanner mentioned in [10] that scans the finger print and gives out a high quality image while maintaining sub-pixel geometric accuracy. This image will then be stored and processed to extract the critical pixel information (minutiae).

B. Minutiae Detection

Traditionally, two fingerprints have been compared using discrete features called minutiae. These features include points in a finger's friction skin where ridges end (called a *ridge ending*) or split (called a ridge *bifurcation*). Typically, there are on the order of 100 minutiae on a tenprint. In order to search and match fingerprints, the coordinate location and the orientation of the ridge at each minutia point are recorded. Figure 3 shows an example of the two types of minutiae. The minutiae are marked in the right image, and the tails on the markers point in the direction of the minutia's orientation [11].

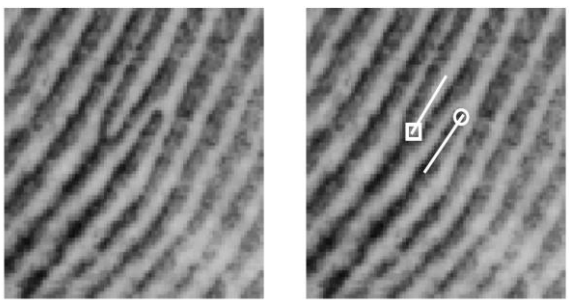


Figure 3. Minutiae: bifurcation (square marker) and ridge ending (circle marker) [11].

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 11, November 2015

C. **MINDTCT Algorithm**

The algorithms used in MINDTCT were inspired by the Home Office's Automatic Fingerprint Recognition System; specifically the suite of algorithms commonly referred to as "HO39"[11]. The NIST software is an entirely original implementation exceeding the capabilities of HO39. It incorporates new algorithms, a modular design, dynamic allocation, and flexible parameter control, which provide a framework for supporting future enhancement and adaptation of the technology. It should be noted that the algorithms and software parameters have been designed and set to optimally process images scanned at 19.69 pixels per millimeter (ppmm) (500 pixels per inch) and quantized to 256 levels of grey [11].

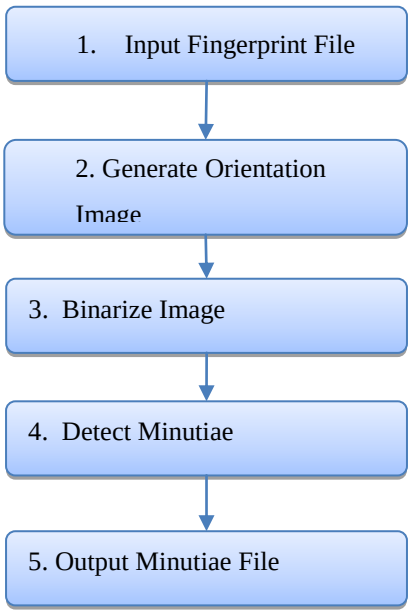


Figure 4. Minutiae detection process.

This process methodically scans the binary image of a fingerprint, identifying localized pixel patterns that indicate the ending or splitting of a ridge.

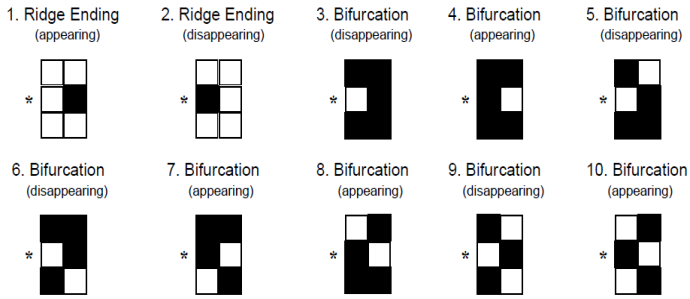


Figure 5. Pixel patterns used to detect minutiae [11].

Candidate ridge endings are detected in the binary image by scanning consecutive pairs of pixels in the image looking for sequences that match this pattern. Pattern scanning is conducted both vertically and horizontally. The pattern as illustrated is configured for vertical scanning as the pixel pairs are stacked on top of each other. To conduct the horizontal scan, the pixel pairs are unstacked, rotated 90°clockwise, and placed back in sequence left to right. Using the representation above, a series of minutiae patterns are used to detect candidate minutia points in the binary fingerprint image. These patterns are illustrated in Figure 5. There are two patterns representing candidate ridge

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 11, November 2015

endings, the rest represent various ridge bifurcations. A secondary attribute of appearing/disappearing is assigned to each pattern. This designates the direction from which a ridge or valley is protruding into the pattern. All pixel pair sequences matching these patterns, as the image is scanned both vertically and horizontally, form a list of candidate minutia points.Figure 6 displays the detected minutiae for the example fingerprint [11].

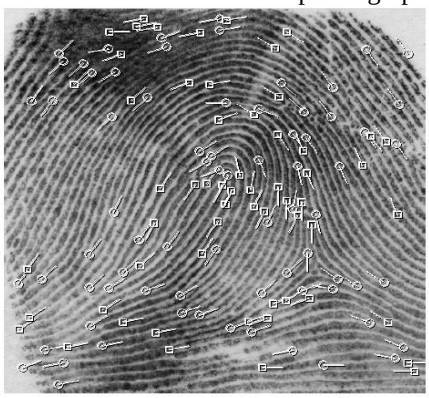


Figure 6. Minutiae results [11].

D. **Certificate Generation**

Today, people can conduct much official business remotely thanks to digital certificates. An official organization issues an RSA certificate that lets the user sign digital transactions anywhere in the world with a computer. In many countries, this digital signature has the same legal validity as a physical one.In this concept, the certificate is generated by examining appropriate biometric information. The certificate is based on the X.509 standard, but an own format of the certificate structure can also be used. The main idea is that the certificate should be generated only by that user who possesses the key pair of the certification authority. This guarantees that the whole process of key generation and storage of relevant information to the certificate will be successful and trustful.This certificate is used by user to proceed further to sign in digital transaction [12].

V. SIMULATION RESULTS

A. **User Interfaces on Windows Phone**

The Interface design is achieved to enhance the system performance. It establishes the layout and interaction mechanism for human -machine interaction.

- **Fingerprint Enrollment and Minutiae Extraction**

The first phase of mobile biometric system is fingerprint enrollment. In this phase, system provides the sample website application to perform online transaction. This application is provided on the Windows Phone 7.5 Mobile Device shown in figure 7(a-c). Figure 7 shows whole procedure of new user registration and login. Also it saves user's fingerprint template into the database. Figure 8(a-c)shows stepwise process of minutiae extraction i. e. generation of grey scale image, binarize image, minutiae detection and finally visual matching of two fingerprints(live and database template). MobileBiometric Systemis using WCF service for sending personal information of user and its fingerprint image template from Windows Phone application to SQL database for storage purpose. While verifying the user, again this data is retrieved from database through WCF service in Windows Phone Application. After successful verification of biometric templates, security certificate is generated to proceed for online transaction by using same WCF service. Mainly WCF service is used in this system to perform fingerprint image processing tasks and database operations. The most challenging task is to convert fingerprint image into byte array and then store this template into the database.

On Windows Phone 7.5 first one sample online book shopping website application is displayed. When user makes request to buy a book and try to perform online transaction, app will ask to verify user. Then login window is displayed as shown in figure 7-a. There are two options for login- admin and user. When mobile owner click on admin login (Fig. 7-b), his username and password will be checked as a first step of authentication. Then after successful login he can enrol new user with his live biometric template (Fig. 7-c).

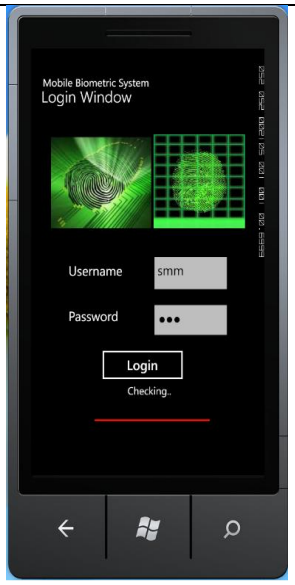
ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

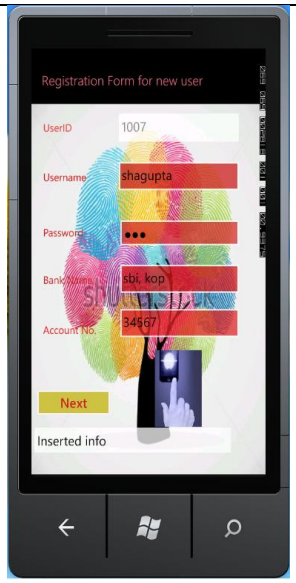
(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 11, November 2015

a. Login page for Admin and User



b. Admin login process



c. New user enrolment

Figure 7. Application on Windows Phone 7.5-User Enrolment.

a. Generation of grey scale image

b. Minutiae extraction result on live fingerprint image

c. Visual matching of the fingerprints

Figure 8. Application on Windows Phone 7.5-Minutiae Extraction.

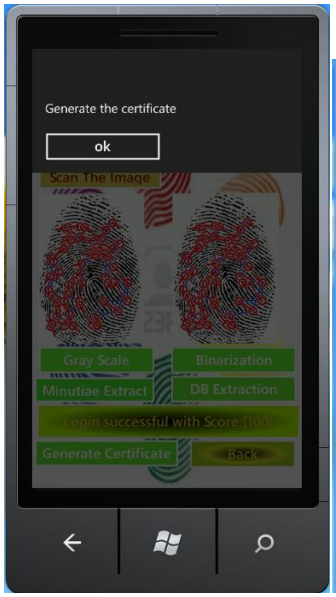
New enrolled user have to perform login using biometric features before performing online transaction as shown in figure 8-a. In the same figure generation of grey scale image and binarization process is shown. In figure 8-b, extracted minutiae points of live fingerprint image are shown. In figure 8-c, visual matching of live fingerprint template and database template is shown and matching score is displayed. If it is greater than 75 % then user is allowed for further process.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 11, November 2015



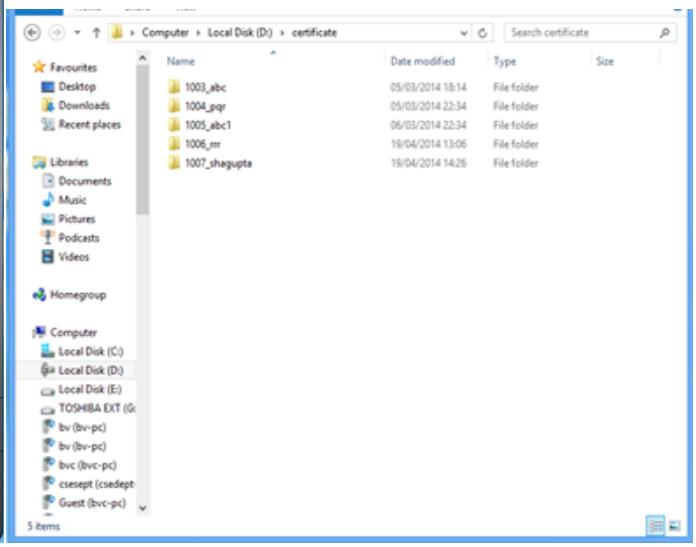


Figure 9-a. Certificate generation process.

Figure 9-b. Certificates generated.

In figure 9-a, after successful matching of fingerprints, button is shown to generate the certificate. Click on ok button (Fig. 9-b) will generate the certificate and store it in specified directory to sign in for online transaction.

B. **Result Analysis**

Chart 1 shows the time required in milliseconds per user for minutiae detection process and Chart 2 shows the time required in milliseconds per user for certificate generation process.

- **Minutiae Extraction:**

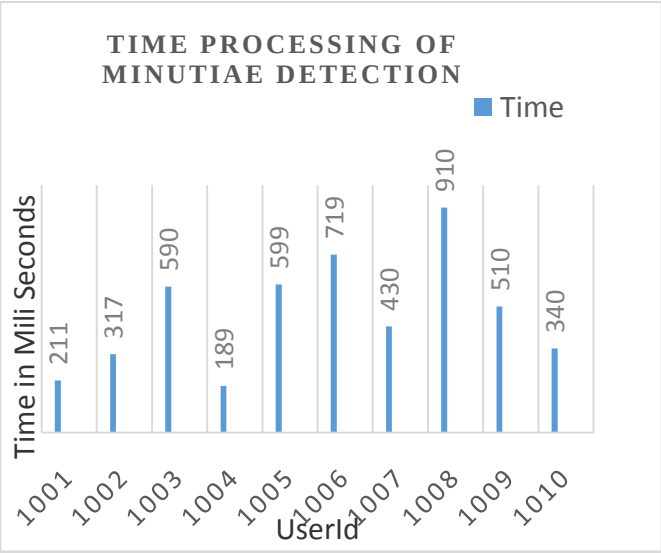


Chart 1: Time Taken To Extract the Minutiae Points

- **Certificate Generation:**

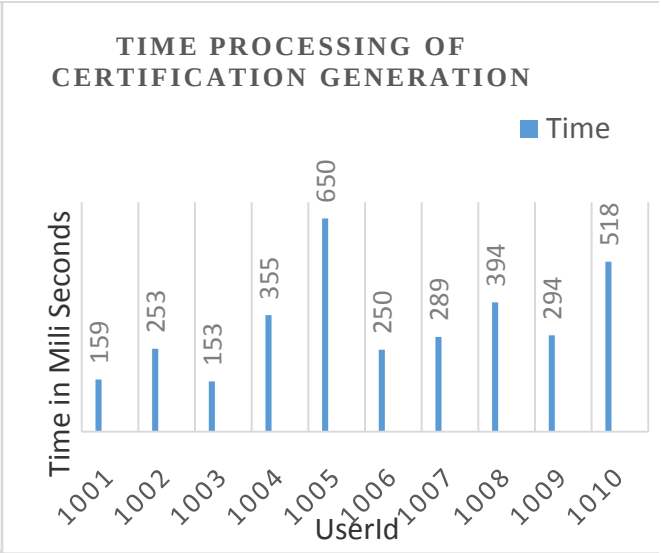


Chart 2: Time Taken For Certificate Generation

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 11, November 2015

VI. CONCLUSION AND FUTURE WORK

Biometrics, the use of a physiological or behavioural aspect of the human body for identification and verification, is a rapidly growing industry. Biometric technology is being used successfully by airports, law enforcements agencies, retail, banking, and the health care industry. Because of its ease of use, accuracy, reliability, and flexibility, it is quickly establishing itself as the premier authentication technology. Biometric technology is still susceptible to vulnerability issues such as system circumvention, verification fraud, enrollment fraud, and Man in the Middle attacks. Additionally, there are serious concerns that the information gathered by biometric systems can be misused to invade or violate personal privacy.

The Systemarchitecture provides a solid alternative for credit cards and an easy way to harden electronic transactions' security via biometrics. In the future, we would like to see the system ported to more platforms, improving its universality. Biometric systems providers will implement more biometric modules, giving the system even more security.

REFERENCES

1. A. Jain, A. Ross, S. Pankanti, "Biometrics: A tool for information security," *IEEE Trans. Information Forensics and Security*, vol. 1, pp. 125–143, 2006
2. Ann Cavoukian, Alex Stoianov**, "**Biometric Encryption: A Positive-Sum Technology That Achieves Strong Authentication, Security, and Privacy" , Mar.2007
3. A.K. Jain, K. Nandakumar, and A. Nagar, "Biometric Template Security," EURASIP J. Advances in Signal Processing, special issue on pattern recognition methods for biometrics, vol. 2008, 2008, pp. 1–17.
4. A. Adler, "Vulnerabilities in Biometric Encryption Systems," Proc. IAPR Audio and Video-Based Biometric Person Authentication (AVBPA 05), LNCS 3546, Springer, 2005, pp. 469–472.
5. D. Moon et al., "Implementation of the USB Token System for Fingerprint Verification," Proc. 13th Scandinavian Conf. (SCIA 03), LNCS 2749, Springer, 2003, pp. 998–1005.
6. Y. Lin, X. Maozhi, and Z. Zhiming, "Digital Signature Systems Based on Smart Card and Fingerprint Feature," J. Systems Eng. and Electronics, vol. 18, no. 4, 2007, pp. 825–834.
7. Ellise T. Eskridge, "Biometric Technology", Bowie State University, Maryland in Europe May 2009
8. N. K Rathaet al., "Generating cancelable fingerprint templates", IEEE Trans. Pattern Anal. Machine Intell. 29 (4), pp. 561–572, 2007.
9. Drahanský, M. "Biometric Security Systems", Brno University of Technology, 2005
10. Futronic FSS88 FIPS 201/PIV Fingerprint Scanner Specifications by Bayometric, 2013.
11. Garris, M.D., Watson, C.I., McCabe, R.M., Wilson, C.L. "*NIST Fingerprint Image Software (NFIS)"*, NISTIR 6813, National Institute of Standards and Technology, 2001.
12. Santesson, S., Nystrom, M., Polk, T. "Internet X.509 Public Key Infrastructure – Qualified Certificates Profile", Microsoft & RSA Security & NIST, 2004.