Biometric Identification Integrated in IT System

Oliviu Mihai Musetoiu, Monica Leba and Andreea Cristina Ionica

Abstract**—** Biometric authentication, or simply biometrics, is to identify a person based on the physiological or behavioral characteristics such as fingerprint, face, iris, voice and signature. The existence of a paper-based data management system in various fields of activity has led to the need to replace it with a modern one. A possibility would be a biometrics-based information system that provides: fast access to information, data accuracy, simple and safe updating, database storage with security keys to ensure high data security and prevent loss or damage data. The paper proposes a biometrics-based information system with well-defined functionalities that will offer the advantages previously set out and where enrollment in the system is based on the data provided by the client on a voluntary basis. The design of the biometrics-based information system began with the design of the system architecture, a hardware prototype based on an Arduino platform and a test software application using the biometric identification library and a MongoDB unstructured database model. The results obtained are for the application of this computer system using fingerprint.

Keywords**—** fingerprint, authentication, database, sensor

I. Introduction

CONTINUED development of biometric technology has allowed its usage in different biometric applications with great advantages.

Biometrics has attracted extensive attention as a new authentication approach against traditional ones such as keys and passwords. Biometric traits are not stolen and forgotten compared with key, card and password. Therefore, biometrics techniques provide us better security and greater convenience than traditional person authentication techniques. Practical person authentication systems using fingerprint, face and iris have been commercially available and used in access control.

Both on national and international level, the biometric recognition system is developed on organizational level, building access and forensics.

These studies related to media processors, face recognition, fingerprint and iris recognition algorithms, etc.

Currently, the following biometric features have been developed.

Facial physiognomy is an automatic system based on the statistical analysis of available images, whose purpose consists in identifying a representative base against which any image can be expressed in the form of a linear vector combination of the base. The algorithm takes a spatial location and follow to decomposing faces into distinct components such as eyes, nose, mouth.

Papillary fingerprint is a new recognition method to identify more accurate the fingerprints with an optical tomography system, who takes a 3D image of finger.

Retina image: The system takes a picture of the retina and then collect data about the type of blood vessels in the portion of the eyeball, using a special video camera.

Iris images: Such as retina image process the camera takes 30 images/s about lines, dots, fibers, filaments, corneas, creases and blood vessels.

Facial thermo gram is the graphic representation of the heat emanations of the face. Before fluctuations of temperatures the pattern of the face remains unchanged.

Voice recognitions is the feature of a biometric authentication system who analysis the voice of the user, and if the voice pattern is the same the access is allowed. The audio and other sensors receive up to 7 levels of nose tones, neck, larynx vibrations, air pressure exerted by the voice. Most systems use similar equipment like phones.

Dynamic signatures are characterized by the speed of writing, the direction and pressure exerted on a writing instrument. These signatures are recorded through small sensors found inside the writing instrument or on the writing pad. They are required a number of 5 signatures to prevent counterfeiting and a good result.

DNA is probably the most reliable biometrics, because is unique and can`t be counterfeit. The process of DNA imprint requires a very long time to identify it because there are many chemical processes involved to detect the pattern stored in database.

Using a biometric system that has integral networking functionality, with a wireless protocol, the application can read the user’s information stored in a central database on a server. Biometric technology used in IT systems requires a collection of data representation, using a biometric sensor, of physiological characteristics unique for every individual person. This digital representation of biometric data is transformed using a dedicated algorithm in order to produce a unique template usually stored in smart card, in a central database on a server, or directly on the sensing device. These stored templates can be accessed when there is used the biometric sensor interface and the identification is achieved by comparing the real-time acquired template with the stored

O. M. Musetoiu is with the University of Petrosani, Doctoral School, Petrosani, Romania, 332006 (e-mail: musetoiuoliviu@hotmail.com).

M. Leba is with the University of Petrosani, Computer and Electrical Engineering Department, Petrosani, Romania, 332006 (corresponding author phone: 0040-736-980-865; e-mail: monicaleba@upet.ro).

A. C. Ionica is with the University of Petrosani, Management and Industrial Engineering Department, Petrosani, Romania, 332006 (e-mail: andreeaionica@upet.ro).

ones. If the matching templates is found then the user is recognized and counted as known by the system.

II. INFORMATION STORING USING BIOMETRIC SENSOR

Biometric technologies based on biometric sensor are basically pattern recognition systems that use data acquisition devices such as dedicated scanners in order to gather biometric characteristics which are distinctive between users. When the digital system identifies a proper fit, the characteristics are extracted and encoded into a biometric template that is a mathematical representation of a person biometric unique characteristic.

A. Purpose of Study

The IT systems that store personal record are useful tools that allow the tracking of users and identify problems or patterns that may help determine the course of health care, insurance, building access and any other application that involves a trustworthy and secure identification. Current procedures to identify individuals and information storage are based on two principles:

1. Classical one consisting on storage of information in paper files;
2. Computerized one consisting on storage of information in databases on dedicated servers.

These procedures do not allow a prompt, easy and secure identification of people who need this kind of services. Current procedures based on biometric information are used to identify people based on biometric features in order to increase the security of banking transactions, access to mobile devices (phone, tablet, laptop) and fixed devices (secured access interfaces).

B. Method advantages

The development of this biometrics system follows the well-known lifecycle, consisting in requirements capture, system design, development and implementation of the system (hardware and software), testing.

This system is based on a method that eliminates the classical methods insufficiencies by optimizing the time response, facilitating access and by ensuring an increased security regarding the primary personal information.

C. Flowchart of the Biometrical Storing Method

Fig. 1 describes the flowchart for personal information storage based on biometric identification regarding the basic biometric reader. Check the current status of biometric system in terms of hardware integrity and if the hardware self-test was successful when the biometric system with microcontroller will signal the current status; if after the hardware self-test the biometric system has any defects or does not match in terms of authenticity, the system will generate an error ID and will signal this current state appropriately, the system may be restarted only after the defect remedy compare the current supply voltage of the system with reliable running threshold imposed by the standards.

If the current value of the supply voltage is less than 20% of the rated value; if the supply voltage is above the threshold of 20% reliable function, the system will generate a unique identifier numeric specific to the equipment.

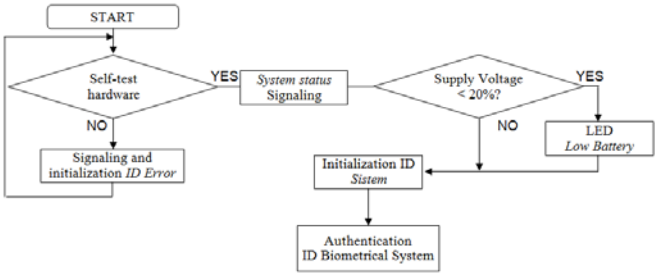


Figure 1. Basic biometric reader flowchart

Next it is described the unique identification number generation by the biometric system with microcontroller. If it is a valid ID, the biometric sensor belonging to the microcontroller system detects the biometric characteristics of the person whose personal data is to be stored; if the biometric sensor does not detect the biometric characteristic, the device allows successive attempts until achieved proper detection. Is checked the biometric data and the information about it is transmitted to the central database; if the person is recognized and it is already included in database, the system allows that authorized personal to add new personal information in the record; If the person is not recognized and therefore is not in database, then the system initiates the procedure for adding a new record through its validation; after this stage the biometrical system allows the user to create personal record and if it is desired to load everything into database, the system initiates an appropriate procedure.

If a template of the biometric data in database is not wanted, the system initiates a reset command that will allow a resuming of the entire procedure in order to store biometric data. If during this time there is a biometric system shutdown command or a fault occurs, the entire system will reset giving the user the chance to start all over again.

D. Flowchart of the Biometrical Storing Method

The processing flow for biometric template electronic submission contains basic biometric readers that submit the person biometric data to a central database via smart device. These submissions will originate from biometric sensors.

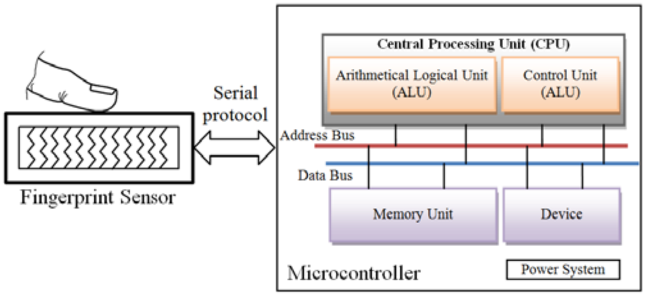


Figure 2. Basic biometric readers. The case of fingerprint

Fig. 2 describes the block diagram basic biometric readers that ensure the biometric scanning of persons. The identification is made using a biometric digital interface, which takes over information regarding the biometric data using a biometric sensor and transmit them to the microprocessor, via a serial protocol. Biometric system identification is powered from an accumulator and is switched on/off using button, and its current status is signaling by LED block.

Fig. 3 describes the block diagram of the storing information using biometric sensor.

Loading persons data is made using a classical PC or laptop (2), connected to the digital biometric system (1), via a USB cable, either using wireless or Bluetooth protocol. Data transmission to the central system, for storing data in the central database, located on the server (3), is done through the internet protocol.

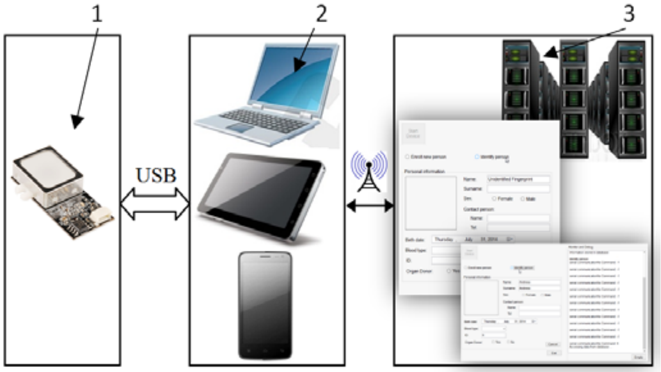


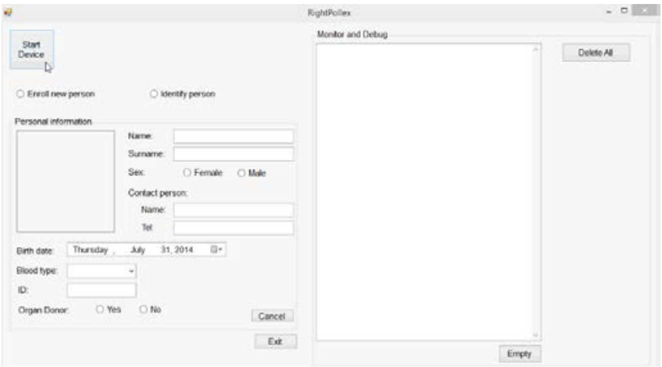
Figure 3. Architecture of storing data

Storing templates in a central database on a server means that users authenticating from multiple locations and the access to the encryption keys will have only authorized personnel.

The biometric system is used for verification, enroll and identification of persons. In verification process, a user that has a certain identity will use a biometric sensor, and the biometric system performs a comparison between the offered biometric and the biometric reference information stored in the central database.

Person biometric data enrollment is a process that is responsible for registering individuals in the central database. During the enrollment process, the biometric characteristic of a subject is first captured by a biometric scanner to produce a sample. A quality check is often performed to ensure that the acquired sample can be reliably processed by successive stages. A feature extraction module is then used to produce a feature set. The template creation module uses the feature set to produce an enrollment template.

In order to identify, a comparison is performed between the offered biometric template and all available reference information stored in database to reveal the identity of a patient.



Birth date: Thursday , July 31, 2014

Figure 4. Developed database interface

Fig. 4 describes a simplified version of the developed database. Through the graphical interface the user can view the current status of basic biometric reader, can choose between enroll new person and identify new person types. Database provides information regarding the user's picture, name and surname, birth date and other relevant data.

The basic biometric reader hardware used in our research contains of a fingerprint sensor connected to the microprocessor, via a serial protocol. This biometric assembly work together with the PC (developed database) trough USB cable (Fig.5).

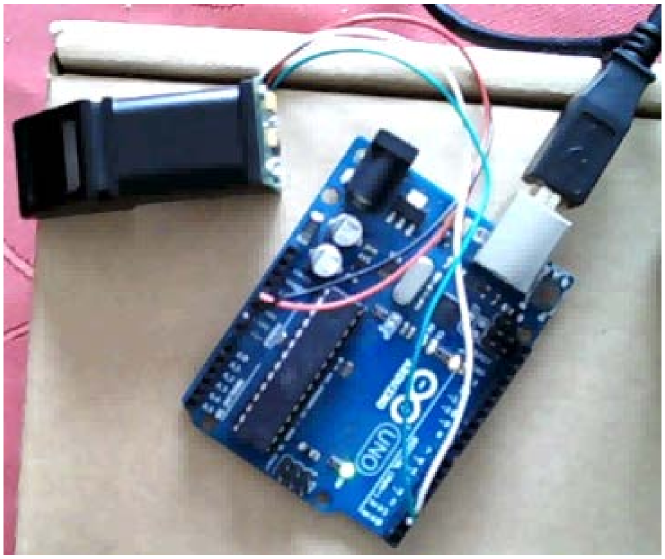
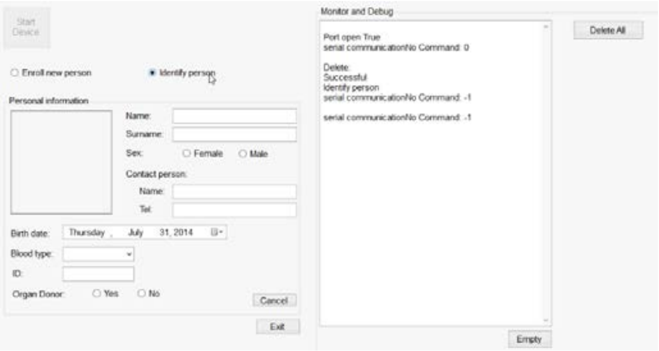


Figure 5. Basic fingerprint reader hardware

For this project was used optical fingerprint readers because are the most common at present. They are based on reflection changes at the spots where the finger lines touch the readers surface. All the optical fingerprint readers comprise of the source of light, the light sensor and a special reflection surface that changes the reflection according to the pressure. Some of the readers are fitted out with the processing and memory chips as well.

The fingerprint technology can be used for identification even within large databases. Fig. 6 presents database graphical interface, in which we tried to identify a new person which does not have the fingerprint template stored in database.



```
Port open True
serial communicationNo Command: 0

Delete
Successful
Identify person
serial communicationNo Command: -1

serial communicationNo Command: -1
```

Figure 6. Database interface – identify person routine

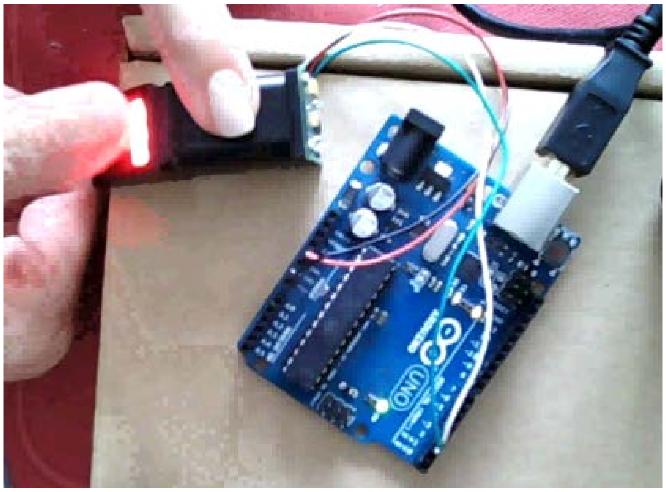
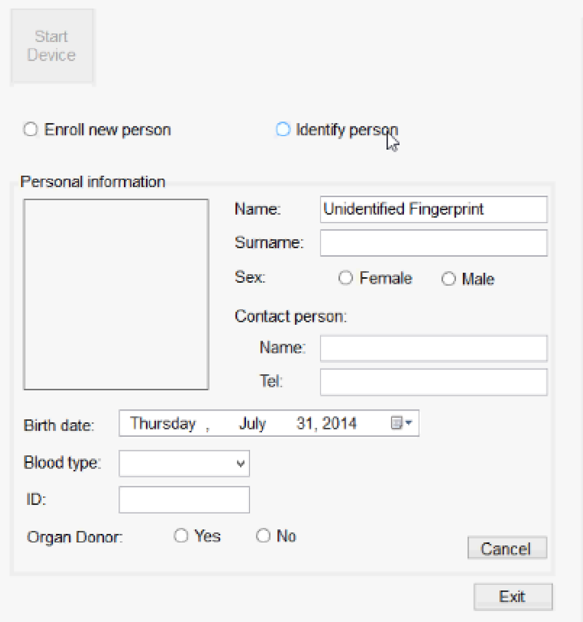


Figure 7. Basic fingerprint reader hardware – fingerprint processing



Name: Unidentified Fingerprint

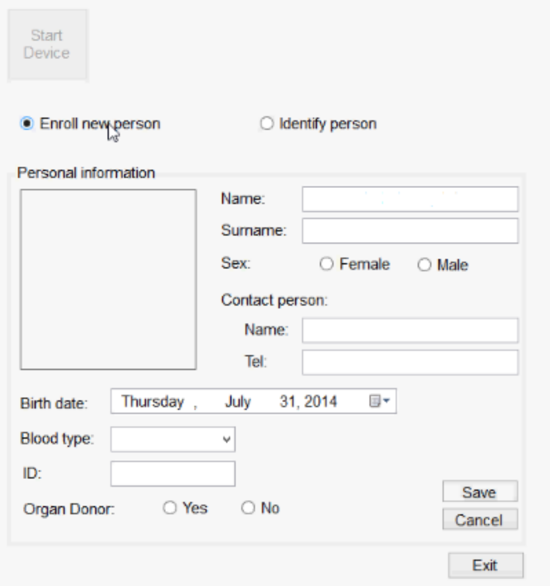
Birth date: Thursday , July 31, 2014

Figure 8. Developed database interface

Fingerprint device used do all the processing by the hardware. Connect to any microcontroller or system with TTL serial, and send packets of data to take photos, detect prints, hash and search. This basic fingerprint reader also enrolls new fingers directly - up to 162 finger prints can be stored in the onboard FLASH memory. There's a red LED in the lens that lights up during a photo when working.

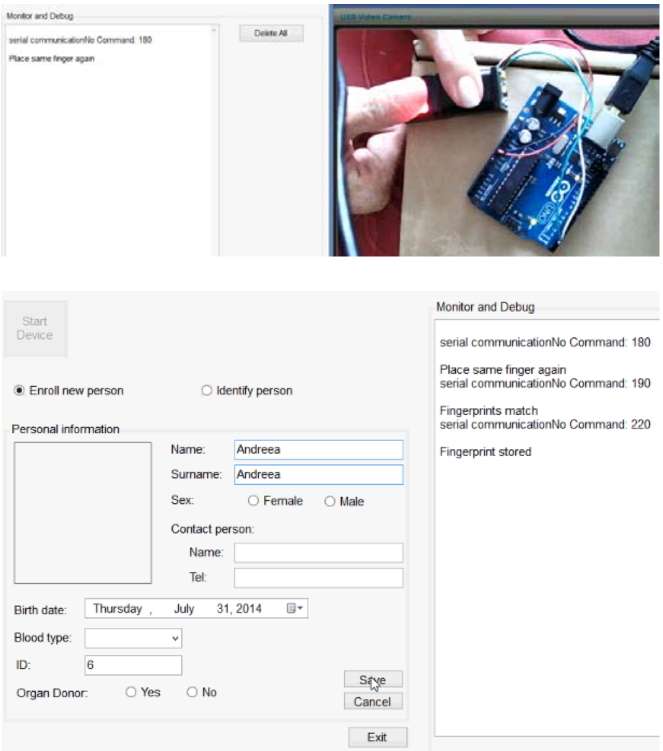
In this case, when the person fingerprint was not stored in database, right after the sensor detect the finger, database displays “Unidentified Fingerprint” (Fig.8). So, if the fingerprints is not enroll, that means no assigning ID's to each print they can’t query them later. Using optical fingerprint sensor and the developed database will make adding fingerprint detection and verification simple.

Fig.9 describes enrolling situation, which means assigning ID to the corresponding fingerprint template.



Birth date: Thursday , July 31, 2014

Figure 9. Developed database interface – enroll new person



```
serial communicationNo Command: 180
Place same finger again
```

Name: Andreea

Surname: Andreea

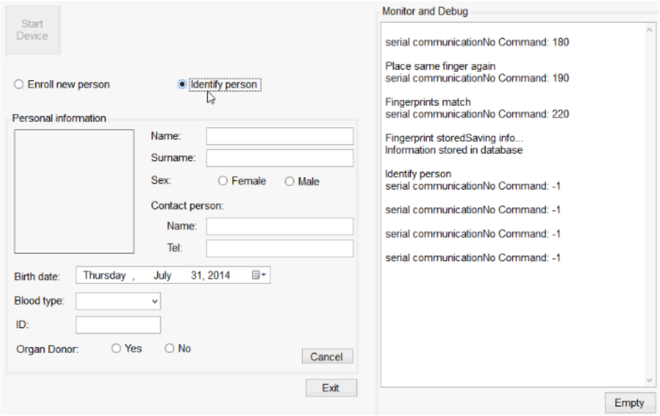
Birth date: Thursday , July 31, 2014

ID: 6

```
serial communicationNo Command: 180

Place same finger again
serial communicationNo Command: 190

Fingerprints match
serial communicationNo Command: 220

Fingerprint stored
```

Figure 10. Developed database interface – fingerprint stored

Fig. 10 show the enroll routine when the developed database ask person to place the same finger again. After this step the fingerprint template is stored and some fields can be filled, also a person photo can be uploaded.



○ Enroll new person ● Identify person

Personal information

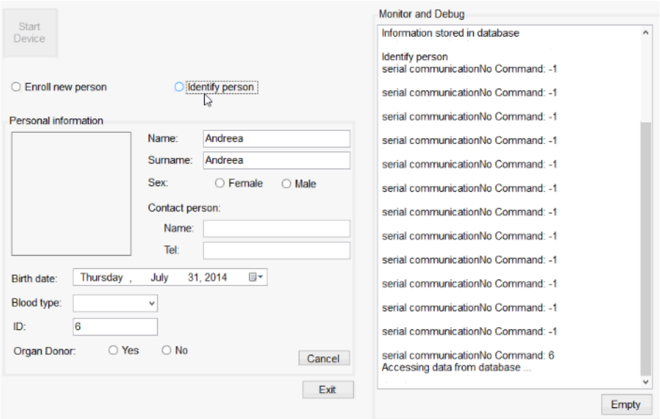
Name:
Surname:
Sex: ○ Female ○ Male
Contact person:
Name:
Tel:
Birth date: Thursday , July 31, 2014
Blood type:
ID:
Organ Donor: ○ Yes ○ No

```
serial communicationNo Command: 180

Place same finger again
serial communicationNo Command: 190

Fingerprints match
serial communicationNo Command: 220

Fingerprint storedSaving info...
Information stored in database

Identify person
serial communicationNo Command: -1

serial communicationNo Command: -1

serial communicationNo Command: -1

serial communicationNo Command: -1
```

Figure 11. Developed database interface – identify person

Fig. 11, 12 describe routine when the developed database query all stored fingerprints in order to find the one corresponding to the queried person. As shown accessing data from database displays a medical repot about the person and also his corresponding fingerprint ID.

The identification system recognizes an individual by searching the entire enrollment template database for a match. It conducts to comparisons to establish if the individual is present in database and if so, returns the identifier of the enrollment reference that matched. In an identification system, the system establishes a subject's identity without the subject having to claim an identity. The template may be stored in internal storage devices like the basic fingerprint reader internal memory or external internal storage like the developed database.



○ Enroll new person ○ Identify person

Personal information

Name: Andreea
Surname: Andreea
Sex: ○ Female ○ Male
Contact person:
Name:
Tel:
Birth date: Thursday , July 31, 2014
Blood type:
ID: 6
Organ Donor: ○ Yes ○ No

```
Information stored in database

Identify person
serial communicationNo Command: -1

serial communicationNo Command: -1

serial communicationNo Command: -1

serial communicationNo Command: -1

serial communicationNo Command: -1

serial communicationNo Command: -1

serial communicationNo Command: -1

serial communicationNo Command: -1

serial communicationNo Command: -1

serial communicationNo Command: -1

serial communicationNo Command: -1

serial communicationNo Command: -1

serial communicationNo Command: 6
Accessing data from database ...
```

Figure 12. Developed database interface – accessing data

III. CONCLUSIONS

The procedures for individuals' identification and relevant information storage must ensure prompt, easy and safe identification of those who need secure information. This requires a means to identify people based on a cheap technology, using easy matching analysis that does not require complex electronic devices and this is possible by means of biometric scanning.

The research results, through the biometric identification system for the case of fingerprint scanning, allow the response time optimization, easy access and enhanced security ensuring the personal information. This paper presents a new approach to personal information storage based on biometric identification, using a fingerprint sensor. More specifically, in case of an emergency situation, the system allows the identification of the person based on fingerprint scanning which represents the key to access the relevant information, previously stored in database.

REFERENCES

[1] M.S. Antony Vigil, P.S. Meena Kumari, U. Soumiya, J. Abinaya, P. Bhargav Akash, A Robust Approach for Iris and Fingerprint Authentication, Journal of Advanced Research in Dynamical & Control Systems, 11-Special Issue, July 2017, ISSN 1943-023X, pp. 194-204.

[2] Sanchez-Reillo Raul, Carmen Sanchez-Avila, Ana Gonzalez-Marcos. "Biometric identification through hand geometry measurements." Pattern Analysis and Machine Intelligence, IEEE Transactions on 22.10, 2000, pp. 1168-1171.

[3] Ribaric Slobodan, Ivan Fratric. "A biometric identification system based on eigenpalm and eigenfinger features." Pattern Analysis and Machine Intelligence, IEEE Transactions on 27.11, 2005, pp. 1698-1709.

[4] Im Sang-Kyun, et al. "An biometric identification system by extracting hand vein patterns." JOURNAL-KOREAN PHYSICAL SOCIETY 38.3, 2000, pp. 268-272.

[5] De Luis -García Rodrigo , et al. "Biometric identification systems." Signal Processing 83.12, 2003, pp. 2539-2557.

[6] Kwapisz Jennifer R., Gary M. Weiss, Samuel A. Moore. "Cell phone-based biometric identification."Biometrics: Theory Applications and Systems (BTAS), 2010 Fourth IEEE International Conference on. IEEE, 2010, pp. 1-7.

[7] M. Leba, R. Dobra, A. Ionica, Method of Storing Relevant Medical Information Based on Biometric Identification, O.S.I.M. Romanian Patent Application, 2014

[8] Van der Putte, Ton, Jeroen Keuning. "Biometrical fingerprint recognition: don't get your fingers burned." Smart Card Research and Advanced Applications. Springer US, 2000, pp. 289-303.

[9] B. Shah and G. Panchal, "Comparative analysis on different Region of Interest (RoI) extraction mechanisms for fingerprint," 2017 International Conference on Intelligent Sustainable Systems (ICISS), Palladam, India, 2017, pp. 690-694. doi: 10.1109/ISS1.2017.8389261