Global Journal of
Computer Sciences

Volume 05, Issue 1, (2015) 13-18

www.awer-center/gjcs

Biometric Identification – between Necessity and Innovation

Monica Leba *, Computer and Electrical Engineering Department, University of Petrosani, Romania.
Andreea Ionica, Management Department, University of Petrosani, Romania.
Remus Dobra, Computer and Electrical Engineering Department, University of Petrosani, Romania.

Suggested Citation:
Leba, M., Lonica, A., & Dobra, R. (2015). Biometric Identification – between Necessity and Innovation. *Global Journal of Computer Sciences*. *5*(1), 13-18.

Received 28 December, 2014; revised 28 February, 2015; accepted 26 March, 2015.
Selection and peer review under responsibility of. Prof. Dr. Doğan İbrahim, Near East University, Cyprus.

Abstract

The procedures for individual's identification and medical information storage must ensure prompt, easy and safe identification of those who need emergency medical services. This requires a means to identify people based on a cheap technology, using easy matching analysis that does not require complex electronic devices. This is possible by means of fingerprint scanning. The paper proposes a method of storing relevant medical information based on biometric identification and for this reason we have developed an optimal system that allows the person identification based on fingerprint, the storage/access to information in a centralized database and the delivery of reports containing relevant personal and medical data. The developed biometric system provides a method for storing relevant primary health information based on biometric identification that lead to a prompt, easy and secure determination of the identity of people who require medical emergency intervention and their relevant medical information. This solution provides the possibility of taking the right decisions and immediate actions by authorized medical staff due to the access to personal information (name, ID, address, phone number, picture, contact person) and relevant medical information (blood type, RH, allergies, chronic diseases, organ donor option, resuscitation option) stored in a central database.

Keywords: Biometric Identification, medical information storage, database.

*ADDRESS FOR CORRESPONDENCE: **Monica Leba,** Computer and Electrical Engineering Department, University of Petrosani, Romania. *E-mail address:* monicaleba@yahoo.com / Tel.: +4-073-698-0865

1. Introduction

Continued development of biometric technology has allowed its usage in different biometric applications with great advantages [4]. An important application refers to the identification methods of those who need emergency medical services. The goal of emergency medical services is to provide treatment to those patients in need of urgent medical care, or preparing for fast movement of the patient to the next medical facility, but in order to do make the right decisions in this amount of time they need to know with whom they are dealing with. Using a biometric system that has integral networking functionality, with a wireless protocol, the medical personnel can read the patient medical information stored in a central database on a server.

Biometric technology used in emergency medicine requires a collection of data representation using a fingerprint 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 [3]. These stored templates can be accessed when the finger is presented to the biometric sensor interface and the identification is achieved by comparing the finger template with the stored ones. If the matching templates is found then the patient is recognized and counted as known by the system.

2. Medical information storing based on biometric fingerprint sensor

Biometric technologies based on fingerprint 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 [1]. When the digital system identifies a proper fit the fingerprints are extracted and encoded into a biometric template that is a mathematical representation of a person biometric unique characteristic.

2.1. Purpose of Study

The paper proposes a method of storing relevant medical information based on biometric identification. The medical record is a useful tool that allows the emergency medical personal to track the patient medical history and identify problems or patterns that may help determine the course of health care [2]. Current procedures to identify individuals and medical information storage are based on two principles:

- classical one consisting on storage of information in paper files
- computerized one consisting on storage of information in databases on dedicated servers

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

2.2. Method advantages

The development of this innovative product follows the well-known lifecycle, consisting in requirements capture, system design, development and implementation of the system (hardware and software), testing. The research methodology was based on the collaboration between specialists from different fields, like computer engineering, electronics, quality management and medicine, and led to the objective achievement, the biometric identification system for emergency medical situations. This developed product 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 medical information for emergency situations. A new approach is developed for storage the primary healthcare information based on biometric identification by means of fingerprint sensor.

2.3. Method description

Primary care is crucial for the health status being the most accessible and less expensive and it is the responsibility of family doctors. The primary healthcare provider must use modern techniques based on medical decision support systems and this is a must because the communication between family doctors and emergency services doctors is deficient, because there is no real coordination between preventive services and emergency services.

The medical information storing, presented in figure 1, begins in the family doctors cabinets which gather information for operational administration of personal data contained in a medical record specific to each person. Data loading is possible by means of biometric fingerprint sensor that is based on an optical or capacitive transmitting image captured by the microcontroller, every patient signature will be loaded in to a data base and a medical record will be created also. This medical record will contain relevant information about the patient like, the name, NPC, address, blood type, allergies, chronic diseases, organ donor or resuscitation option, and so on.

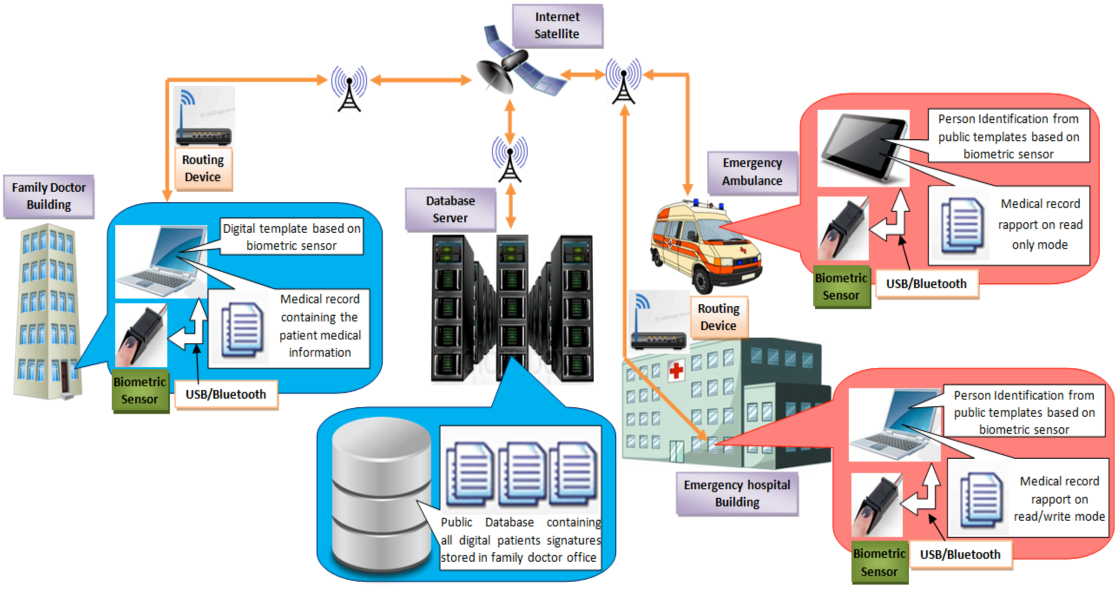

Internet Satellite
Routing Device
Family Doctor Building
Digital template based on biometric sensor
Medical record containing the patient medical information
Biometric Sensor
USB/Bluetooth
Database Server
Public Database containing all digital patients signatures stored in family doctor office
Emergency Ambulance
Person Identification from public templates based on biometric sensor
Medical record rapport on read only mode
Biometric Sensor
USB/Bluetooth
Routing Device
Emergency hospital Building
Person Identification from public templates based on biometric sensor
Medical record rapport on read/write mode
Biometric Sensor
USB/Bluetooth

Figure 1. Biometric system schematic diagram

All data loaded in the family doctor cabinets will be stored in a central database which will contain the digital patient's signatures together with their relevant medical data. Using passwords or PINs to control access to programs and computer files is a pretty good method, but can be quite easily hijacked and for that reason we have used a biometric method able to make permanent identify of the user. This system should not allow access to the data until the time the operator is identified as an authorized user.

When an emergency comes along the victim is taken by the emergency ambulances which will be equipped with biometric identifications systems. The victim finger is placed on the biometric sensor and using an USB cable or a Bluetooth protocol the microcontroller system will connect with a mobile device (laptop or tablet). After the fingerprint identification on the tablet will be displayed in the shortest time a medical report regarding the victim.

If the victim shows up at the emergency hospital building the procedure will be similar with that described above, because a biometric system will be used in this case also and the person will be quickly identified both in terms of its identity as well as her health status.

3. Flowchart of the biometrical storing method

In figure 2 is presented the flowchart for relevant medical information storage based on biometric identification and sequentially through the following steps:

- 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 signaling 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

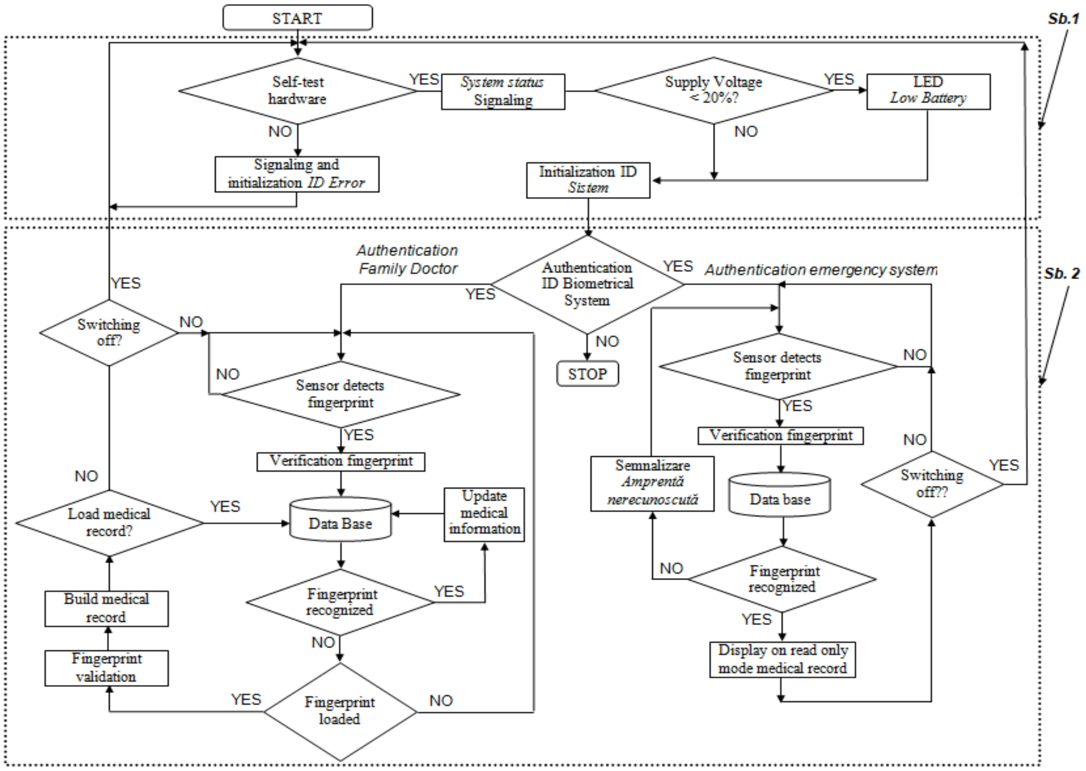


Figure 2. Biometric system algorithm flowchart

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;

- Check the unique identification number generated by the biometric system with microcontroller:
    - if it is a valid ID and corresponds *to the cabinets of family doctors*, the biometric sensor belonging to the microcontroller system detects the fingerprint of the person whose personal data is to be stored; if the biometric sensor does not detect the fingerprint or the finger was not properly placed, the device allows successive attempts until achieved fingerprint detection. Is checked the fingerprint and the information about it is transmitted to the central database; if the person fingerprint is recognized and it is already included in the database, the system allows that authorized personal from family doctor cabinet can add new personal or medical information in the patient medical record; If the fingerprint is not recognized and therefore is not in the database, then the system initiates the procedure for adding a new fingerprint through its validation; after this stage the biometrical system allows the user to create patient medical record and if it is desired to load everything it into the database, the system initiates an appropriate procedure; if a load of the fingerprints in the 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.
    - if it is valid ID and corresponds *to emergency services* or legal medicine, then the biometric sensor corresponding to the numerical system with microcontroller detects the person fingerprint for data reading; if the biometric sensor does not detect the fingerprint or the finger was not properly placed, the device allows successive attempts until fingerprint detection will be achieved; Is checked the fingerprint and the information about it is transmitted to the central database; if the person fingerprint is recognized and it is already included in the database, the system displays in the shortest time a patient summary medical report containing its relevant personal information; If the fingerprint is not recognized and therefore is not in the database, system indicates that in the database is no template related to the concerned patient (victim). 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.

4. Fingerprint reader system and medial data storage

In figure 3 is presented the block diagram of the storing medical information using biometrical fingerprint sensor that ensure the identification of persons in need of emergency services.

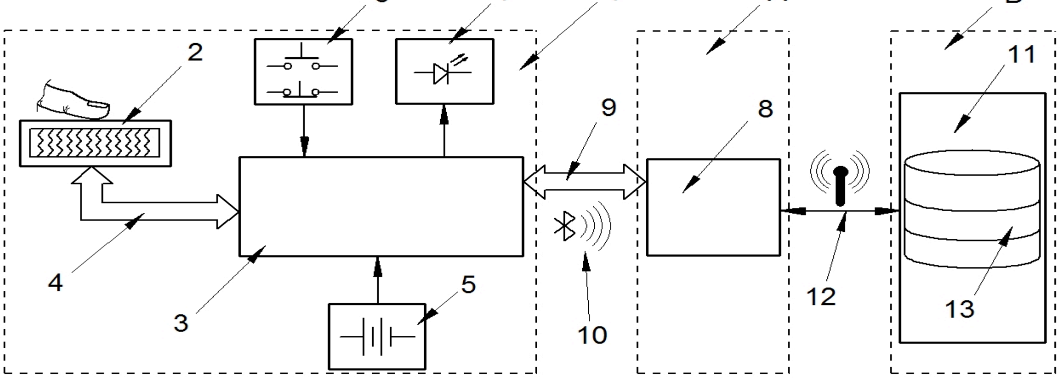
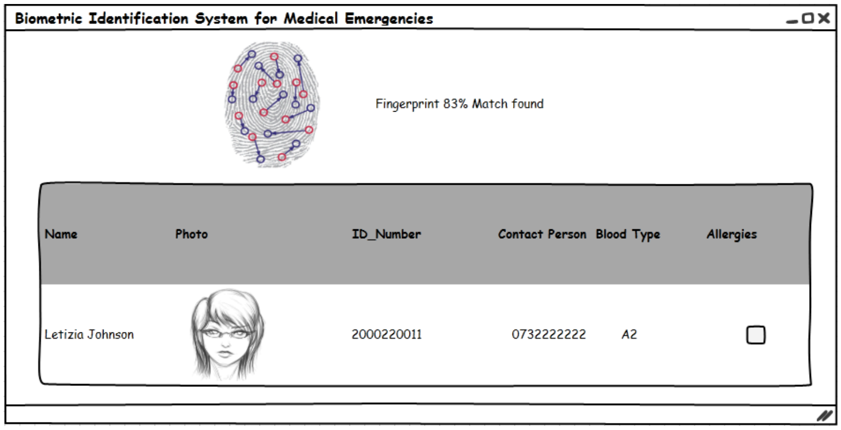


Figure 3. Biometric system block diagram

The identification is made using a digital interface biometric (1), which takes over information regarding the fingerprint using a biometric sensor (2) and transmit them to the microprocessor (3), via a serial protocol (4). Biometric system identification is powered from an accumulator (5) and is switched on/off using button (6), and its current status is signaling by LED block (7). Loading persons data is made in family doctors' offices and the reading part take place in the emergency services (A), using a classical PC or laptop (8), connected to the digital biometric (1) via a USB cable (9), either using wireless or Bluetooth protocol (10). Data transmission to the central system, (B) for storing data in the central database (11), located on the server (12), is done through the internet protocol (13).

This medical record will contain relevant information about the patient like, the name, NPC, address, blood type, like is presented in figure 4.



Biometric Identification System for Medical Emergencies

Fingerprint 83% Match found

Name	Photo	ID_Number	Contact Person	Blood Type	Allergies
Letizia Johnson		2000220011	0732222222	A2	□

Figure 4. Biometric system user interface design

All data loaded in the family doctor cabinets will be stored in a central database which will contain the digital patient's signatures together with their relevant medical data.

5. Conclusions

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

References

[1] Dessimoz, D., Champod, C., Richiardi, J., & Drygajlo, A., (2006). MBIoD Multimodal Biometrics for Identity Documents, Research Report PFS 341-0805 (Version 2.0), 9-15

[2] Leba, M., Dobra, R., & Ionica AC. (2014). Procedure for Relevant Medical Information Storage based on Biometric Identification, Romanian Patent, OSIM Registration Number A/00167/27.02.2014.

[3] Liu, Y. (2008). Identifying Legal Concerns in the Biometric Context, *Journal of the International Commercial Law and Technology, 3*(1), 45-54

[4] Midori, A. (2011). Biometric –Unique and Diverse Applications in Nature, Science and Technology, Published by Intech, 2011, Received from: www.intechopen.com.