ADVANCES in NATURAL and APPLIED SCIENCES

ISSN: 1995-0772
EISSN: 1998-1090
2016November10(16):pages 129-137

Published BY**AENSI Publication**
http://www.aensiweb.com/ANAS
Open Access Journal

Design and Implementation of a security system composite biometric equipment, sensors and digital radios Hytera for Security Company

Jesus Ortiz, Jorge Portilla, Oscar Gualdron

Department EEST, University of Pamplona, Pamplona, Colombia

Received 23 August 2016; Accepted 21 November 2016; Published 30 November 2016

Address For Correspondence:
Jorge Portilla, Department EEST, University of Pamplona, Pamplona, Colombia.

Copyright © 2016 by authors and American-Eurasian Network for Scientific Information (AENSI Publication).
This work is licensed under the Creative Commons Attribution International License (CC BY).http://creativecommons.org/licenses/by/4.0/

Open Access

ABSTRACT

Background: This project seeks to be a new proposal in the area of electronic security and telecommunications, **Objective:** The design an integrated security consisting of a biometric access control fingerprint sensors, fire and temperature telemetry digital wireless system supported Smart Dispatch platform. Fire sensors and temperature will be selected by their characteristics and have a treatment stage to perform conversions to electrical units managed by Hytera radios. **Results:** The information through the DMR protocol that uses digital radios Hytera is transmitted. Performing telemetry supported digital radios and the Smart Dispatch station, where you can view remotely on any computer with internet access state of the variables controlled by sensors. **Conclusion:** In addition, the platform allows Smart Dispatch should be more controlled by biometrics and GPS location in Google Maps locating objects. This design will be made with high-quality tools and industrial.

KEYWORDS: Electronic Security, Telemetry, Smart Dispatch, GPS

INTRODUCTION

Technological growth worldwide do not stop, more and more electronic mechanisms that are designed for industrial, medical, security, military, and consumer appliances. Modern day life of human being is dependent on using computations based on computer automation. [1]In the world of digital technology, accurate and reliable system of authentication is very important for human computer interaction.[2]In the field of electronic security these devices are used for disaster prevention, theft, monitoring of physical variables, alarms, risks, installation and maintenance of structured cabling. They are also highly employed in access to places, personal identification based on unique biometric features in each individual. The widely used authentication system used to control access to security locations are passwords, personal identification number (PIN) but those can be stolen or cracked. Thus biometrics has become strong alternative to the traditional methods. [3] For this at national and international level have taken steps in the development of electronic devices to improve safety, this project stems from the need for the company SETRONICS S.A.S to merge its two development areas (Electronic Security and Telecommunications) to offer new products innovative and viable in its construction. The basic component of a biometric identification system is a sensing module that ensure scanning of biometric

ToCite ThisArticle: Jesus Ortiz, Jorge Portilla, Oscar Gualdron., Design and Implementation of a security system composite biometric equipment, sensors and digital radios Hytera for Security Company. **Advances in Natural and Applied Sciences**. 10(16);Pages: 129-137

characters. The major part is the decision-making module that compare the biometric features defined in the database. [4]

In this project, biometric and sensor systems with a communications system be integrated to transmit information, variables and states. To be monitored from a remote station anywhere in the world with internet access and the Smart Dispatch software installed on the computer as unique requirements.

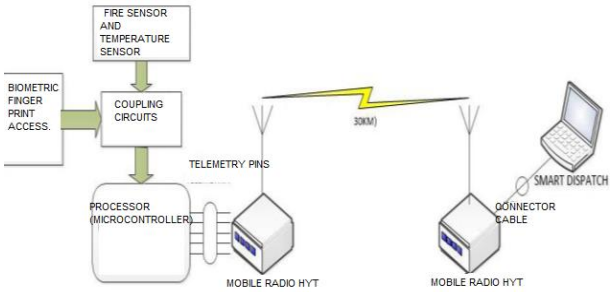

Fig. 1: Project Scheme

Security System:

An electronic monitoring device that alerts about potential hazards and emergencies.[5] [6]It takes parameters associated to be a robust, and have efficient operation. Then the design methodology described.

A. Control Module:

Given the characteristics of signals from smoke detectors, biometric sensor, temperature sensor, electric lock and magnetic contact as inputs to the module and outputs the 6-pin GPIO to base radio MD786G UHF a control module that manages inputs are designed signal, process and make the link with digital radios.

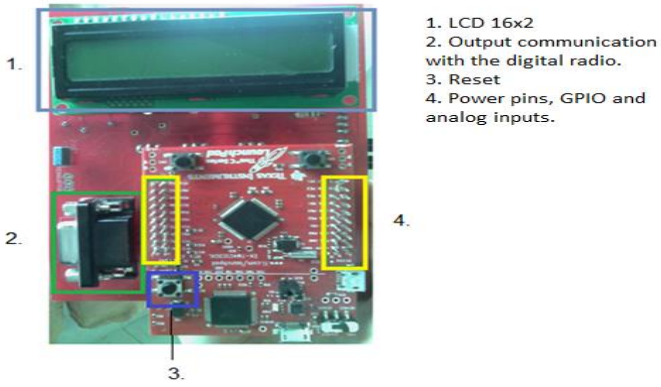

Fig. 2: Control Module

The main function of this module is to make the link between reading sensors, information processing by the microcontroller high-end TIVA-C TM4C123 and transmission to digital radios through its pin communication general purpose (GPIO) connected to the outputs of the control module to send the events of sensors.[7]

Voltage regulators used are described to communicate the biometric sensor and smoke sensor with the control module. 16X2 LCD display that handles the sensor status (open, closed and the temperature value) is added.

B. Telemetry radios Hytera:

Each type has a radio programming software given by the manufacturer and cable programming, software MD786G radio VHF and UHF PD786G is DMR_SW_CPS_V6.05.05.019.SA6 (Each radio has a label on the back with the name of the programming software) and cable programming is PC47 (USB CONNECTOR). In Figure 3 the connector pins shown GPIO telemetry.

Fig. 3: Text messages with sensors state.

The voltage levels of the mobile radios are TTL, TTL 3.6-5V low level and high level 0 - 2.4V.

- GPIO input pin: 0 - 1.2V (Low) y 2 - 5V (High)
- GPIO input pin : 0 - 0.8V (Low) y 2.4 - 5V (High)

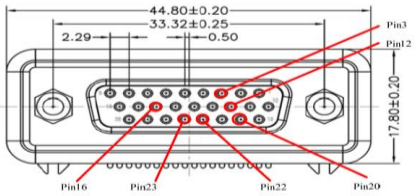

Fig. 4: Telemetry Pins [16]

No.	Feature	Description	Action	Pulse Time[ms]	Digital Call	Target VIO	Quick Text
1	Telemetry Button1	Button1	None	200	None	None	None
2	Telemetry Button2	Button2	None	200	None	None	None
3	Telemetry Button3	Button3	None	200	None	None	None
4	Telemetry VIO1	TelemetryVIO1	Send Status w/ Text Command	200	PaP General	None	Biometrico
5	Telemetry VIO2	TelemetryVIO2	Send Status w/ Text Command	200	OSCAR PRUEBA 102	None	Sensor Puerta abierta
6	Telemetry VIO3	TelemetryVIO3	Send Status w/ Text Command	200	PaP General	None	Temperatura Alta
7	Telemetry VIO4	TelemetryVIO4	Send Status w/ Text Command	200	PaP General	None	Sensor de Incendio Activado
8	Telemetry VIO5	TelemetryVIO5	Send Status w/ Text Command	200	OSCAR PRUEBA 102	None	Sin energia electrica
9	Telemetry VIO6	TelemetryVIO6	Send Status w/ Text Command	200	PaP General	None	Alarma

Fig. 5: Telemetry configuration messages.

You can see the pins telemetry, of which 6 will use, which are general purpose GPIO pins. Instead, the other pins are radio buttons that they are more limited for their applications because they do not allow to receive external signals but only press the switch and would be more for such emergency applications to generate a call.

C. Smart Dispatch Software:

This software is an integrated office system fundamentals client / server technology. It provides features such as GPS location, radio communications and text messages which makes it a very complete and highly efficient system.

The software consists of a gateway, server, repeater (optional), sent station and receiver radio.

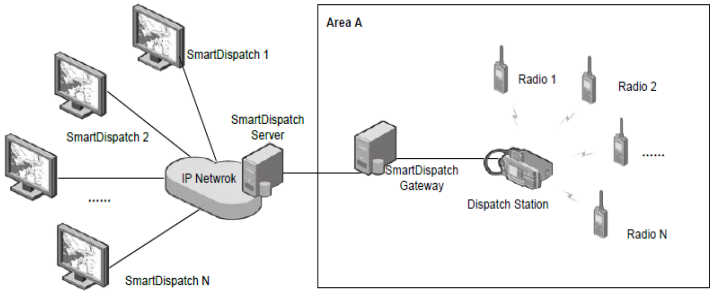

Fig. 6: Smart Software Dispatch scheme

This system is thinking in design to monitor, manage and warn of potential natural disasters and public safety emergencies so that in these cases is a reliable and effective system. This system was developed by the company Hytera according to ETSI DMR standard as wireless communications solution.

Its main features are that you can perform remote monitoring of portable or mobile units, support for multiple online mapping systems like Google maps, Open Street Map, along with the ability to do online monitoring units radios.

For its operation software requires the installation of SQL Server data base where all information management software as calls, duration, GPS position, telemetry and messages will be stored.

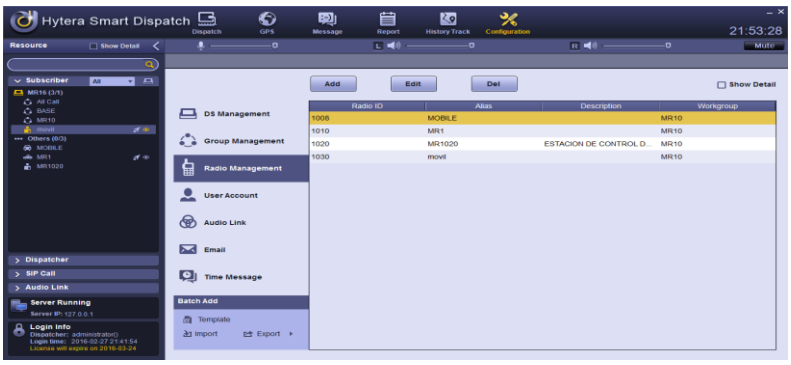

Fig. 7: Setting radios in the Software.

Figure 7 shows the configuration option where each radio IDs are added to be identified, the software can also create groups shown. Finally telemetry is configured, the arrival option is selected address data and if the driving voltage for high or low state voltage. The other configuration of telemetry is already set in the programming of radios.

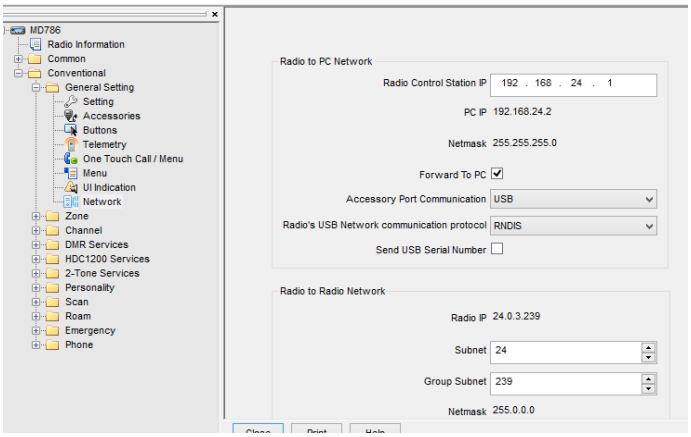

Fig. 8: Connection Dispacth station

Communication software to Smart Dispatch is via a connected computer where all the radio receives data unit's transmitted radio.

D. Programming and Development:

One of the most significant parties was to ensure that the control module could interpret, process and efficiently transmit each signal. The result is expected in the design, a very good performance, with user-friendly design restructuring in configuration pin input, output and converters. As for the design, opens the door to use almost any type of electrical sensor, mechanical electronic as through electronic instrumentation can make the coupling to the microcontroller.

E. Communication Channels Digital Radio:

Each of the radios used employed the same frequency and channel configuration described below. By accessing the channel characteristics found among which are important channel name and color code. The code color should be the same in all radios programmed to identify different encoding if this value cannot communicate.

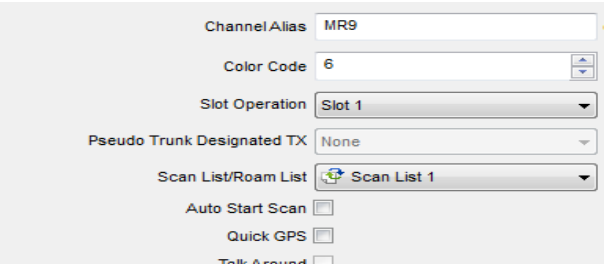

Fig. 9: Path to the cannel.

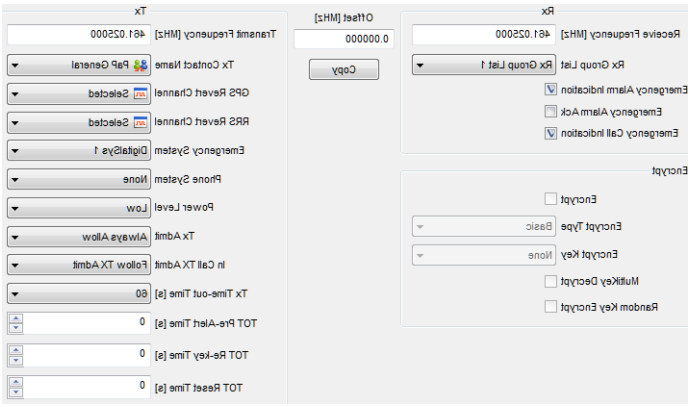

Fig. 10: Channel frequencies

In Figure 10, shows the reception operation frequencies 461,025 MHz and the same value observed for transmission, will only be different when a UHF signal repeater RD986 or RD626 UHF is added

B. Design implemented:

This is the outline of the overall operation of the safety system consists of the following elements:

- Biometric Access Control F08 connectivity RS232, RS485, USB and TCP / IP.
- Electric lock 12VDC.
- LM335Z sensor.
- Smoke sensor fotoeléctric12VDC.
- Magnetic contact.
- Radio UHF based MD786G
- 3 mobile radios PD786G UHF.

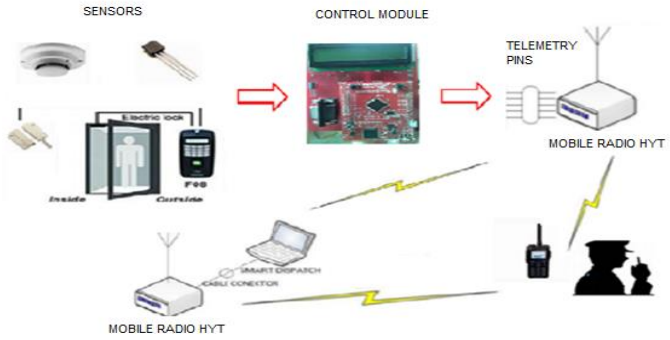

Fig. 11: System.

In the picture above we can see the whole system with its attached components. This whole system provides security for a specific place remote monitoring of the status of sensors in the control station located 3 km away from the place or in case of using repeater signal reaches 50Km distance communication. Any event in the sensors will be communicated via text message also to the 3 mobile radios carried by the security people also have communication real-time voice between units and also with the monitoring station.

Results:

A. Operation smart dispatch software:

The proposed design leaves an effective system for remote measurement and transmission of the sensor. In Figure 12 the display of incoming calls, duration, communication channel shown

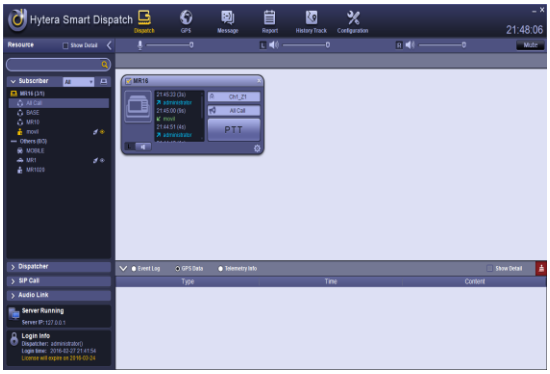

Fig. 12: Dispatch

GPS positioning was something added to the project as a monitoring station will perform better if you can identify the exact position of a radius associated with a guard.

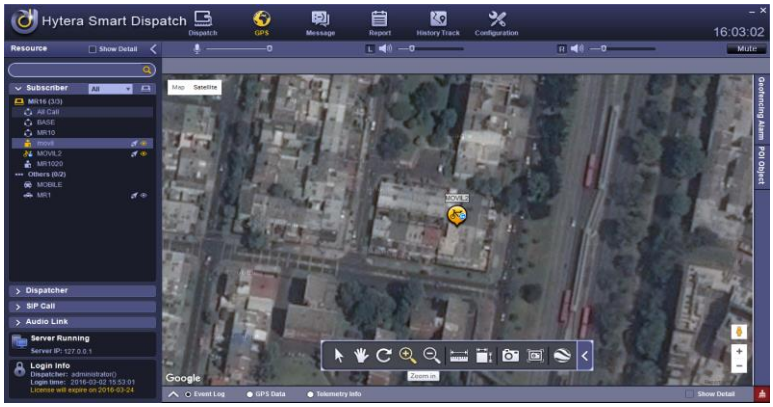

Fig. 12: Position GPS.

Fig. 13: Digital radios usedMD786G UHF and PD786G UHF

Within the platform monitoring and control events recorded by the sensors are received.

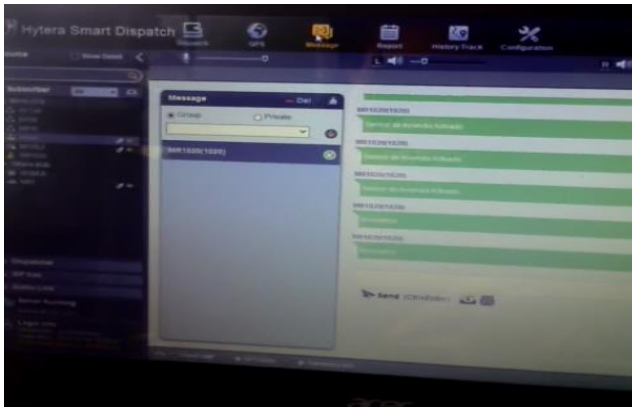

Fig. 14: Telemetry messages.

A. Setting Biometric Access Control F08:

Access control allows you to record 4,000 fingerprints each with an identification code since management software can be assigned a name to each ID. The software is called "Attendance Management" and comes with access control F08, with it you can do monitoring from a computer using TCP / IP, RS232 and RS485 / RS232 communication. Within the software registered with their personal data and their time of entry and exit observation site users are observed.

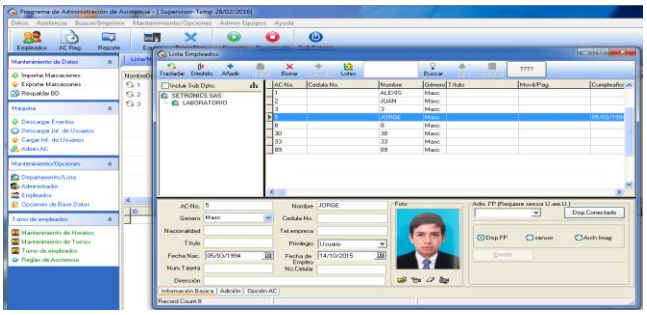

Fig. 15: Software Attendance Management

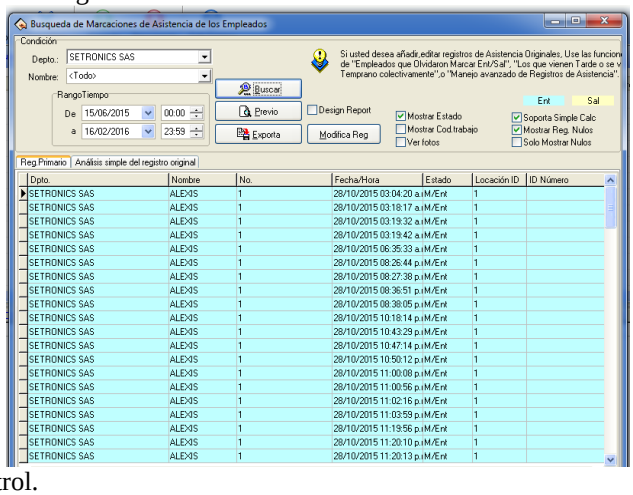

Fig. 16: Registry access control.

Having radio equipment gives us a great advantage if the data is limited in terms of variables here that a system GPRS, Wi-Fi, Bluetooth or ZIG BEE. The advantage is the great distance that can be obtained from communication between radios and 3KM with repeater between 30-50 KM added this method of radio communication works in any place under almost any situation remains very robust

B. *Security System Settings:*

Hostile environments, this configuration is named because it was devised in order to get all the information access to a certain place and control through sensors without relying on internet. The control module SE-

BIOHYT processes all the information from the sensors in place and sends the information to a radius located elsewhere if you must have internet connection for the proper functioning of software Smart Dispatch, if you want to have a complete report on the state of the satellite position of digital radios.Based on this system it has the following characteristics:

• UHF 1 Radio PD786G.
• UHF 2 Radio PD786G Watchers place where they will receive status messages from the sensors, called by the dispatcher software, emergency button and calls between guards.
• Biometric Access Control F08 with data download via USB.
• Smoke sensors, temperature, open door and electric lock.
• 1 MD786 UHF with 6-pin telemetry to transmit to the Smart Dispatch station.

Normal environments, this configuration was designed to provide solutions to many everyday events of some companies with security systems where you have access to a network where you can monitor online access to a certain place through the biometric sensor.

• UHF 1 Radio PD786G.
• 2 UHF Radio PD786G Watchers place where they will receive status messages from the sensors, called by the dispatcher software, emergency button and calls between guards.
• F08 Biometric Access Control with TCP / IP connection and online monitoring through software provided by the manufacturer.
• Sensors and electric lock door open.
• 1 MD786 UHF with 6-pin telemetry to transmit to the Smart Dispatch station.

Conclusions:

The prototype security system designed reveals the usefulness of joining two such important areas as electronic security and telecommunications, obtaining a new product that allows monitoring of a number of sensors via digital radio transmission means of reliable, powerful and effective information. Each data transmission medium has its own advantages and disadvantages according to the need of each design. Unlike other media such as Bluetooth, GSM / GPRS, WIFI or X bee among many other radio communications they are effective for their great coverage in the transmission.

The biometric fingerprint sensor F08 for its part has an internal memory that stores user records, data inputs and outputs with exact time, also it has the option to set the electric lock and door sensor open which were processed by the high-end microcontroller and sent to the telemetry pin. When telemetry logic states as I mentioned previously was impossible to transmit that user was entering or leaving the place secure, and know that the biometric sensor was activated and allowed the entry of a person this for configuring hostile environments, but all income information, movements and schedules can be up to the control module via USB and downloading files and displayed on the device software. In the closed configuration environment to have TCP / IP connectivity it is possible to identify who enters the system in real time.

The purpose of the project was to develop a telemetry system iS measuring physical variables and transmit information. He managed to unify the system that receives information from the sensors and sends it through the media for their alertness and monitoring. The developed project leaves the option not only transmit the information that there is a fire, the temperature is very high or agreed violently at the door entering without authorization, if not the possibility of adding a control mechanism of these events as activating protections buildings as automated ventilation and opening water valves in case of fire while the necessary measures are taken in the response time of the control station. The distance monitoring of this system without repeater reaches 3 km maximum depending on an ideal location of antenna height, transmit power and gain, if a repeater between the control module and the station is added Smart Dispatch could be obtained distances up to 50Km.

Knowledge:

The project is a success because it allowed merging the two areas meet development of the company to generate a new product, besides these first results will be the basis for future projects. Cost-benefit analysis reflects how costly it is selling the project as compared to other conventional alarm systems are very economical, to make this project feasible is necessary to locate customers who need this system in sectors such as mining and public safety. This system is not equal to conventional alarm as it has voice communications between users, GPS tracking, monitoring station and notifications via text message to state of the sensors. The two configurations designed, hostile environments and normal environments, for enterprise SAS were Setronics were successfully validated in operation, and the possibility of developing specific projects of the company using this method opens.

REFERENCES

1. Yanes-Estévez, V., A.M. García-Pérez and J.R. Oreja-Rodríguez, 2013. "La importancia de las redes de comunicación con clientes o proveedores en función de la incertidumbre percibida del entorno," *Rev. Eur. Dir. y Econ. la Empres.*, 22(1): 39-52.
2. Selwal, A., S.K. Gupta and Surender, 2016. "Fuzzy Analytic Hierarchy Process based Template Data Analysis of Multimodal Biometric Conceptual Designs," *Procedia Comput. Sci.*, 85: 899-905.
3. Athale, S.S., D. Patil, P. Deshpande and Y.H. Dandawate, 2015. "Hardware Implementation of Palm Vein Biometric Modality for Access Control in Multilayered Security System," *Procedia Comput. Sci.*, 58: 492-498.
4. Ad??mek, M., M. Mat??sek and P. Neumann, 2015. "Security of biometric systems," *Energy Procedia*, 100: 169-176.
5. Thanki, R. and K. Borisagar, 2015. "ScienceDirect Sparse Watermarking Technique for Improving Security of Biometric System," *Procedia - Procedia Comput. Sci.*, 70: 251-258.
6. Singh, A.K. and C. Bhatnagar, 2015. "Biometric security system for watchlist surveillance," *Procedia Comput. Sci.*, 46: 596-603.
7. Gualdron, O., C. Duran, J. Ortiz and J. Araque, 2014. "Implementation of a neural model in a hardware device(FPGA) for the classification of chemical compounds in a multisensory (E-nose)," *Rev. Colomb. Tecnol. Av.*, 2(24): 127-133.