Mobile Multimodal Biometric System for Security

Waleed El Nahal, Ph.D
MSA University
6 October City

ABSTRACT
Among our huge life requirements, the most important requirement which has a vital role in our daily life is the security. Recently using biometrics in the security systems has a wide range of research interests since they provide systems have more efficient, reliable, and secure than the others.

In the present time researches for mobile biometric devices are provided with a fingerprint only which isn't sufficient for the areas where lawlessness and anarchy cases are existed recently due to the current political situation in some developing countries in Africa and Middle East where the rate of crime increased significantly involving a large number of people getting into the crime scene. Police departments are unable to identify robbers and criminals due to the presence of newly unrecorded ones with the lack of presence of a fixed database holding records of widely known criminals.

So in this paper we propose a mobile biometric authentication system (MOBAS) based on Zigbee technology and a multimodal biometric authentication system in which the primary biometric modalities adopted are the fingerprint and the face recognition.

The proposed system aims to provide a mobile, light, user friendly, reliable and secure biometric authentication system to the police departments, and that will help the officers anywhere to identify the criminals by taking a fingerprint or capturing an image or both for different scenarios, sending them wirelessly to the server at the appropriate police station and then waiting for a response concerning the person's criminal record sent wirelessly from the police station and displayed on a mobile biometric authentication device (MOBA). According to the sent criminal record, the police officers will take a suitable action towards this person.

Keywords
Biometric systems, Finger print, face recognition, Nomad Biometric Authentication (NOBA).

1. INTRODUCTION
Security may be applied for application, data, network, home and buildings. In this present day we have already several type of security systems like CCTV, barcode, identity card which are based on various type of technology and has tedious processing, which takes a long time for decision, highly expensive, less percentage of securing, chance of hacking and destroy or altered easily. Due to this dearth the present security system is unable to fulfill our best security and hence using biometrics in the recent security systems emerge [6].

Biometrics refers to the automatic identifications of a person based on his or her physiological or behavioral characteristics" [1]. Authorization process that depend on a database containing information about human physical or behavioral characteristics and trying to verify the identities by matching, the common need for high security measures lead to the interests from many organizations that gave constant support for leading the growth of biometrics technologies. Two main types of biometrics have been used mainly physical and behavioral. A physical biometrics is a part of a person's body; include fingerprints, hand geometry, retina scan, iris scan, facial location or recognition [2]. While a behavioral biometric is something that a person does; include voice recognition, signature, keystroke pattern and gait [2]. There are unusual biometrics which may be used in the future, including a person's unique smell, the shape of the ear or even the way they talk [2]. However, it has been claimed that "different applications require different biometrics as there is no supreme or best biometric technology" [3].

A biometric system is essentially a pattern-recognition system that makes a personal identification by determining the authenticity of a specific physiological or behavioral characteristics possessed by the user" [4]. The identification system starts to perform specific algorithms trying to extract and compare the features provided by the user, to come up with the answer of the question [4].

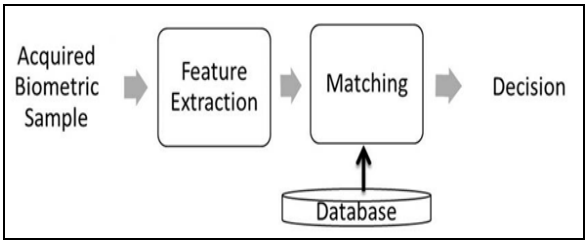

Fig.1. Typical biometric system

Fig.1. depicts the operation of a generic biometric system although some systems will differ in their particulars [5, 9]. The primary components for the purposes of this discussion are "capture," where the sensor collects biometric data from the subject to be recognized; the "reference database," where previously enrolled subjects' biometric data are held; the "matcher," which compares presented data to reference data in order to make a recognition decision; and "action," where the system recognition decision is revealed and actions are undertaken based on that decision. Biometric systems are quite similar in most of operations except at the captured data as the two basic operations performed by a general biometric system are the capture and storage of enrolment (reference) biometric samples and the capture of new biometric samples and their comparison with corresponding reference samples (matching) [5].

2. PREVIOUS WORK AND LIMITATIONS

Generally the previous security systems use the manual based security system like CCTV (closed circuit television camera), alarm, security lighting, security card, security code and security guard. These manual methods are more expensive and can be easily altered or manipulated. In the case of security code and card it can be forgotten, hacked and altered by another person.

On the other hand most biometric security systems deployed in real-world applications are unimodal [9], which is a system, has several drawbacks like noisy sensor data, non-universality or lack of distinctiveness of the biometric trait, unacceptable error rates, and spoof attacks [11]. For efficient practical utilization, biometric authentication systems should be user friendly, fast and reliable. In practice however, many prove to be intrusive and cumbersome with varying levels of reliability. Iris recognition, for example, is potentially the highest performing solution, but it typically relies on high resolution, near infrared, images captured under very controlled conditions. Moreover, these systems require the biometric data of individuals to be stored on servers, which may conflict with the protection policies for personal data [12].

One solution is to use multimodal biometrics which refers to the combination of two or more biometric modalities in a single identification. Most biometric verification systems are done based on knowledge base and token based identification these are prone to fraud. Biometric authentication employs unique combinations of measurable physical characteristics; fingerprint, facial features, iris of the eye, voice print and so on- that cannot be readily imitated or forged by others.

Therefore, multimodal biometric systems will be more effective as it improves the accuracy of the biometric identification or verification, provide a certain degree of flexibility for some unusable biometric traits and provide strong protection against spoof attacks due to the difficulty in spoofing multiple biometric sources.

3. PROPOSED SYSTEM (MOBAS) OVERVIEW

The MOBAS targets the ability of deployment and improvement of biometric technologies to achieve higher level of security based on a flexible capturing the human physical characteristics or the biometric information, targeting the collection of maximum amount of data acquirement. Accordingly, the choice of a multimodal biometric system is presented to combine two different aspects of biometric measurements [7, 8] to reach out for high accuracy and reliability.

The created MOBAS is able to recognize any person based on the fingerprint sensor combined with the facial camera sensor and the extracted data is successfully sent over a wireless channel to the PC workstation to be processed by comparing and matching the extracted data with the database available.

The proposed system in Fig.2 provides an unconstrained mobile device (MOBA) that creates an efficient authentication by acquiring and fusing biometric data to generate robust and reliable authentication in unconstrained scenarios where many factors may impede the acquisition of ideal samples. Also it will overcome the traditional systems dearth and identify the human identity more accurately.

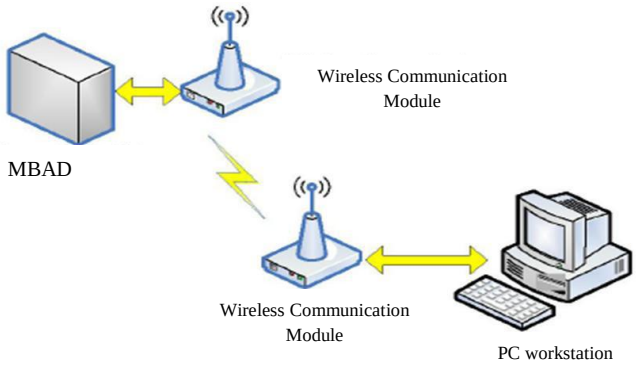

Fig.2. Proposed MOBAS

4. PROPOSED SYSTEM (MOBAS) DESIGN

The MOBAS system consists of two main parts the MOBA and the PC workstation. The MOBA is responsible for capturing necessary personal attributes for human identification from the fingerprint and camera (face recognition) sensors. The PC workstation containing database of users templates happen to do all the processing of matching captured samples and saved templates using various techniques (Hamming distance) and give a feedback response to the MBD.

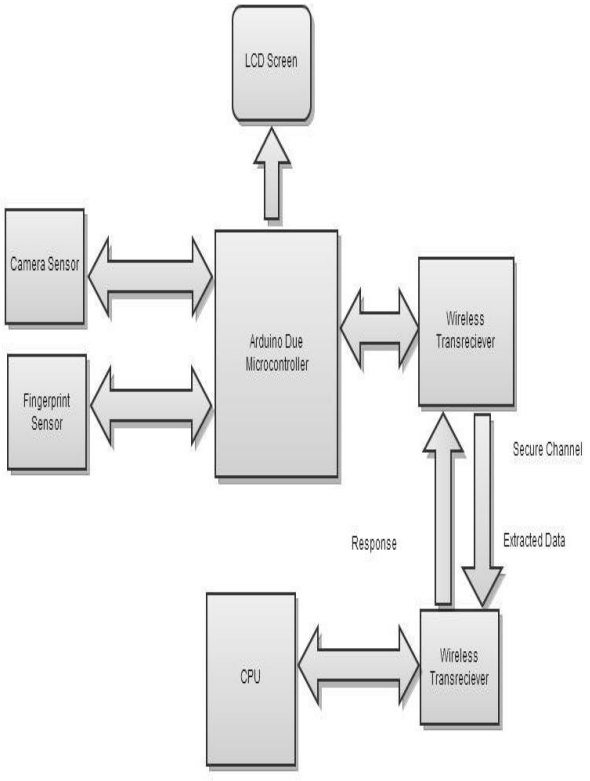

Fig.3. MOBAS basic functional block diagram

The MOBAS system depends on multimodal biometric system represented by the fingerprint sensor and camera sensor modules. In the MOBA, the fingerprint module and the camera sensor capture the target sample from the user and send it to the CPU which stores it in the database created. The camera is used in facial capturing and sending the data to the

microcontroller. A microcontroller is used to provide an interface between the sensors and the transmitting module. Microcontroller manages acquiring data from the sensors on the user permission and passes it to the transmitter.

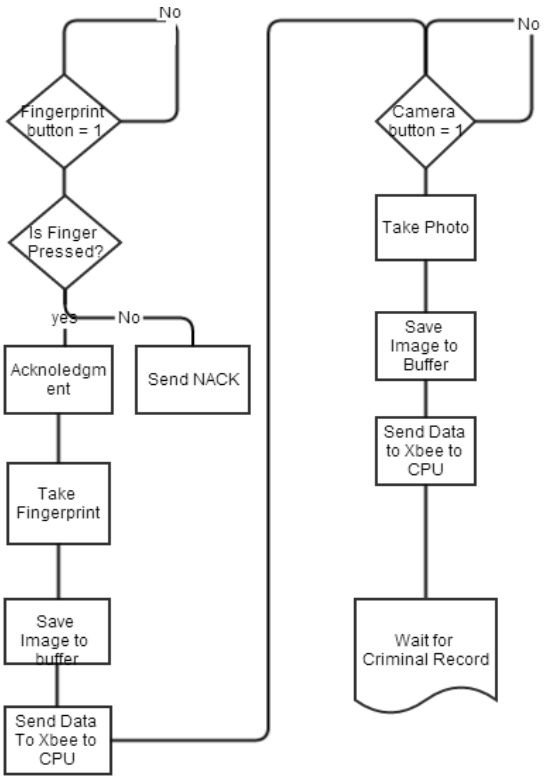

Fig.4. MOBA operation flowchart.

At the receiving end, the PC workstation does all the work concerning the algorithm used by the adaptive system to compare and match the captured data with the database. The CPU follows specific restrictions defined in the False Acceptance rate (FAR) and False Reject rate (FRR). The Graphical User Interface (GUI) created automatically triggers all these actions, and show us a simple window with the fingerprint picture, the face picture, the person score after combining the results, and send the reply back over the wireless channel to be displayed on the LCD.

4.1 Hardware Architecture

The hardware design consists of camera sensor, fingerprint sensor module, Zigbee antenna with Shield, microcontroller, LCD.

4.1.1. MOBA Camera Sensor

The camera sensor shown in Fig.5 captures a facial image biometric sample by using a set of commands sent from the microcontroller of the MOBA to capture and send the images. Camera is chosen to be small size to fit our design.

4.1.2. MOBA Fingerprint Sensor Module

The fingerprint sensor shown in Fig.6 is used to capture a fingerprint biometric sample by using a set of commands sent from the microcontroller of the MOBA and then extract fingerprint biometric data necessary for the authentication process. Fingerprint is chosen to be reliable as it combines 3 or more samples and small size to fit our design.

Fig.5. Camera sensor module.

Fig.6. Fingerprint sensor module.

4.1.3. MOBA Microcontroller Unit

It is used to provide interface between the camera sensor, the fingerprint sensor, the wireless transceiver and the LCD screen. It is used to send instruction commands to the LCD screen to display the criminal record comes from the police station to the policeman in the street, and also it permits the camera and fingerprint sensor modules to capture the extracted data by using specific commands sent to these modules through the interfaced wireless transceiver. We can summarize the functions of the MOBA microcontroller as the following; GUI design, fingerprint recognition, face recognition, score match level decision and hexadecimal binary data to image conversion.

4.2 Software Architecture

MOBAS system must provide the user with a reliable and user friendly interface to be able to deal with feature data and execute the process of comparing and matching. MOBAS system will be provided with a Visual Basic based interface, Visual Basic allows the programming of GUI, which is more reliable and convenient. Visual Basic was the ideal choice due to its compatibility with Windows Operating System which is widely used, which will be reflected on the capability of our software. The authentication software provided with the MOBAS system based on a multimodal biometric authentication technique with a matching score-level fusion [5, 6] which provides the ability to search, enroll, compare and match results.

4.2.1.Visual Studio

Microsoft Visual Studio is an integrated development environment (IDE) from Microsoft, that is used to develop graphical user interface applications. The proposed system uses Visual Studio to create our database, to convert sensor outputs from hex to image, to make face recognition software by using OpenCV, to make fingerprint detection, to create our GUI, and to integrate everything into the GUI.

4.2.2. Database

The database consists of tables that stores records implemented in Microsoft SQL Server database, which is fast and easy, it can store a very large record and requires little configuration.

4.2.3. OpenCV for Face Recognition

Open Computer Vision Library (OpenCV) is available for Windows and Linux. It is distributed under Intel's license for both commercial and non-commercial (research and teaching) purposes [15]. The library includes over 300 image analysis and processing methods from morphology, geometry, image treatment, etc., up to the recently added methods for computing face recognition or 3D tracking. The proposed system uses library "Iscross-platform" that focuses mainly on real-time image processing. If this library finds Intel's integrated performance primitives on the system, it will use these proprietary optimized routines for acceleration.

A facial recognition system is a computer application for automatically identifying or verifying a person from a digital image or a video frame from a video source. One of the ways to do this is by comparing selected facial features from the image and a facial database. We choose "OpenCV" because it has a readymade library for face recognition.

4.2.4.GRfinger for Fingerprint Recognition

GRfinger Fingerprint SDK is fingerprint recognition Software Development Kit (SDK) that allows you to integrate biometrics in a wide variety of applications. It is supported by dozens of programming languages, richness of code samples, its thorough documentation and also reliable application developing in a matter of hours. We chose GRfinger as it has a readymade library that can be used by various programming languages, reliable, and it supports multiple readers.

5. RESULTS AND SIMULATIONS

This system has been verified to observe the 200 authorized and 10 unauthorized people for entry into the parliament. In case of authorized, 199 identification have been identified successfully and only one identification didn't recognize due to their wrong manner of giving fingerprint and in case of unauthorized person all person have been successfully denied. Accuracy in both situations is shown below (Table. 1&2).

Enrollment of each fingerprint (3 samples) + face photos takes around 30 seconds. Identification takes around 20 seconds which makes the proposed system (MOBAS) efficient and reliable for a policeman to take a decision.

5.1. For Authorized Person

Table 1: Authorized person

Persons No.	Successful Identification	Unsuccessful Identification	Accuracy
200	199	1	99.5%

5.2. For Unauthorized Person

Table 2: Unauthorized people

Persons No.	Successful Identification as Denied	Unsuccessful Identification	Accuracy
10	10	0	100%

The window obtained after taking the fingerprint and the face detection of a person from MOBA is shown in Fig.10. It appears on the PC workstation screen in the front of the police officer. The window shows the fingerprint, the face detection, the match status, the person name and the person criminal record. According to the match status, the police officer will send to the appropriate MOBA the person criminal record as shown in Table 3 if the match status is perfect or to take the facial imprint or fingerprint again if the match status is not perfect. During the simulations the proposed system provides a perfect match status.

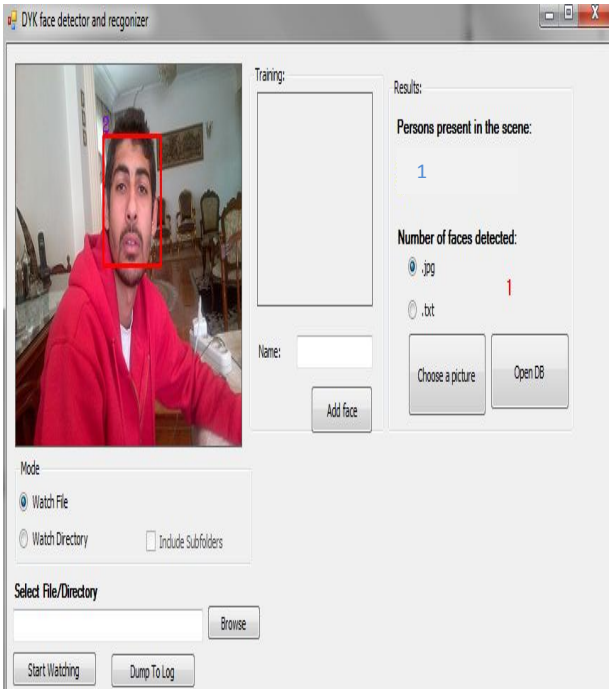

Fig.7. Face recognition

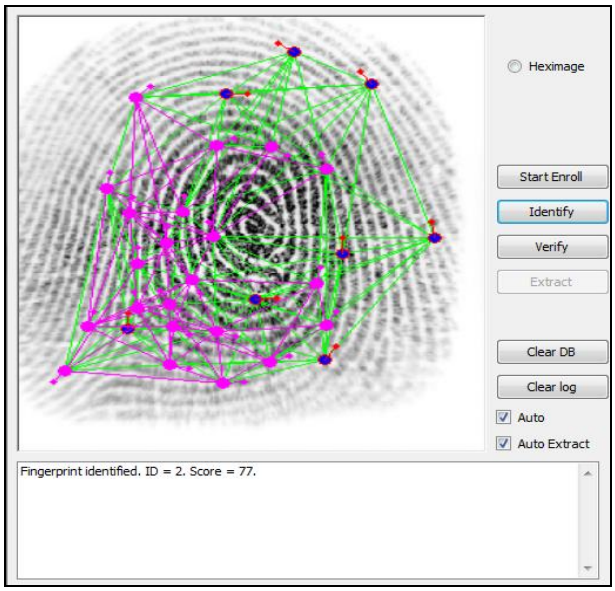

Fig.8. Fingerprint recognition

6. CONCLUSION

The proposal system (MOBAS) is based on providing user mobility and friendly, cost effective in large-scale production and processing. Captured data from sensors is sent to the PC workstation over a channel within a wireless network between the transmitter and receiver in order to provide a secure channel for the data exchange. Some changes may occur depending on the environment of implementation and accordingly minor specifications change may exist.

The proposed MOBAS offers a new feature which is a mobile multi-modal biometric device "face detection and fingerprint) by which the policeman can capture the personal face in some cases where he can't take a fingerprint especially in lawlessness case or anarchy case that is recently existed in some development countries in the present time. If we apply the proposed system (MOBAS) on the areas where the rate of crime increased significantly such as Egypt, Iraq and Libya in this present day, the rate of crime will be decreased and also we could stop the criminal cases that happened in the previous periods such as "Port Said Stadium Incident" in Egypt.

Also MOBAS provides other features such as easy GUI for the user, low cost, sufficient results (using low cost sensors), fast and reliable transmission (identification takes around 20 seconds).

Table 3

Criminal Record	Meaning	Conclusion
A	Many previous crimes	Dangerous Record
B	On tuck a criminal case	Dangerous Record
C	No previous crimes	Not Dangerous

7. ACKNOWLEDGMENTS

The author is thankful to Yahiya, Adel and Kareem for giving him the opportunity to present this research work.

8. REFERENCES

[1] M. Lourde R, D. Khosla, "Fingerprint Identification in Biometric Security Systems" International Journal of Computer and Electrical Engineering, Vol. 2, No. 5, October, 2010.

[2] International Journal of Engineeringand Advanced Technology (IJEAT), "Wireless Fingerprint Based College Attendence System using Zigbee Technology", 201. ISSN: 2249 – 8958, Volume-2, Issue 3, February 2013.

[3] Liu S. and Silverman M. "A practical guide to biometric security technology", pp 27-32. 2001.

[4] A. K. Jain, and et al., "Biometric Template Selection: A Case Study in Fingerprints", Proc. 4th Int'l Conf. on Audio- and Video-Based Biometric Person Authentication (AVBPA), pp. 335-342, Guildford, UK, June 9-11, 2003.

[5] Joseph N. Pato and Lynette I. Millett, "Biometric Recognition: Challenges and Opportunities", National Research Council of the United States, 2004.

[6] Keith A Rhodes, and et al. "Challenges in Using Biometrics", U.S. General Accounting Office, Technology Assessment: Using Biometrics for Border Security, GAO-03-1137T, September 2003.

[7] Nanavati, S., and et al. "Biometrics: Identity Verification in a Networked World", Toronto: John Wiley & Sons. 2002.

[8] L. Ravi Kumar, and et al. "Fingerprint Minutia Match Using Bifurcation Technique", International Journal of Computer Science & Communication Networks, Vol. 2(4), 478-486.

[9] Anil K.Jain, Ajay Kumar, "Biometrics of Next Generation: An Overview", SPRINGER 2010. (1), pp 1-36.

[10] De Vel, and et al. "Line-based face recognition under varying pose", Pattern Analysis and Machine Intelligence, IEEE Transactions on. 1999. Pp.1081 - 1088.

[11] P.H.Zope and Poonam Mote, "Multimodal Biometric system using Gabor Filter", International Journal of Advanced Trends in Computer Science and Engineering, Volume 1, No.2, May – June 2012.

[12] Saeed Meshgini, and et al. "Face Recognition Using Gabor Filter Bank, Kernel Principle Component Analysis and Support Vector Machine", International Journal of Computer Theory and Engineering, Vol. 4, No. 5, October 2012.

[13] P. D. Garje, and et al. "Multibiometric Identification System Based On Score Level", IOSR Journal of Electronics and Communication Engineering (IOSRJECE), Issue 6, Volume 2, pp. 07-11, Sep-Oct 2012.

[14] Smita Kulkarni, "Improving Biometric Identification through Score Level Face Fingerprint Fusion", International Journal of Scientific & Engineering Research, Issue 6, Volume 3, June-2012.

Fig.9. Match and ID acquired