Trends in Life Sciences
An International Peer-reviewed Journal

www.sciencejournal.in

DAMA INTERNATIONAL

DATA SECURITY ASSESSMENT USING INTELLIGENT BIOMETRICS AND COMPARING ITS PERFORMANCE WITH NANO-SENSORS

Nejati Jahromi , Mansour[1] and Afshin Bazargani[2]
[1]Department of Electrical Engineering, Aeronautical College and Islamic Azad University Tehran South Branch, Tehran, Iran,
Email: m_nejati@azad.ac.ir
[2]MS student of Islamic Azad University, South Tehran branch
Email: bazarganafshin@yahoo.com

ABSTRACT

The point of the present study is the examination of protection control systems based on intelligent biometrics. One of the most significant applications of these systems is being used as a protection-security system. This research aims to prove the reliability of biometric methods. It is stated that each individual (in case of being identified) is the one who has claimed he/she is, and another individual cannot impersonate him/her easily. Thus, it helps the users utilizes this system with a higher degree of ease. The reasons to be mentioned are the implications of simplicity of applying biometrics instead of current common tool; moreover, applying biometric technologies will accelerate the user's access to the desired resources. Also, the maintenance cost of systems and relevant security issues will be reduced. The most notable point is that along with the development of security systems, the biometric systems should be enhanced, which can be realized nowadays with the aid of various types of sensors and Nano-sensors.

KEYWORDS: biometrics; fingerprint; adaptive algorithm; Nano-sensor; identification

INTRODUCTION

The necessity of applying biometric systems has been under the focus of security system designers since long ago. Therefore, the designers decided to implement their desired design. But the emergence of adaptive algorithms such as IBA and MBA, fingerprint sensors and other types of sensors has enhanced the designers' ability in applying them. In fact, biometrics is a new technology for identifying people's identity automatically and is a more reliable method for improving the security of information societies in comparison with other identification methods such as pin code, password, or magnetic cards. The applied methods in biometrics are broad and are developing day by day. The other remarkable advantages of biometrics compared to other traditional methods are the lack of need for password or Identity Card, decrease of people's unnecessary access to information, and reduction of impersonation cases.

Different types and application of biometrics

Biometrics consists of two essential and important branches which are dependent on behavioral and physical attributes. Each of the used methods is a subset of the aforementioned branches: for example, body odor, fingerprint, face and vinous, palm print and DNA are included in the arena of physical biometrics, and the speech and signature are classified in the field of behavioral biometrics. Each of the aforementioned methods has their own unique application, but they are mostly useful in security-related cases such as criminal identification, Electronic driving license, smartphones, and economic usages like indirect teaching, running financial affairs. These methods are also a great help in identifying the missing people (Panahi et al., 2005).

Architecture and performance of biometric system

The majority of biometric systems have the same structure: data request-signal processing-adaptation-decision making-storage space-data transfer environment and data request subsystem are all included in this set. Its operational signal processing subsystem is as follows:

1. Receiving raw data from data collection subsystem
2. Feature extraction
3. Filtering operation for noise elimination
4. Data correction

Converting the received data to the required form (pattern production) for adaptation subsystem (Eriki and Magbeli, 2012; Lee *et al.*, 2010).

Security in biometric systems

Information security is defined as "protection of information and information system from individuals' unauthorized access". These unauthorized activities include abusing, reading, copying, distorting and manipulating the security-related computer words, and reliable and trusted information which are sometimes used instead of each other mistakenly. Protecting these systems is one of the tasks assigned to biometrics systems. These systems are constantly under malicious attacks such as attack to system input ports, attack to database, and attacks to identification system by forged biometrics and the fraudulent people apply different techniques to deceive these systems (Eriki and Magbeli , 2012).

Nano-sensors

The emergence and advance of Nanotechnology has influenced all scientific contexts and fields such as medicine, national security, electronics, energy, etc., so that the researchers predict a bright future for this field of science and expect numerous investments on the field. To say the least important influence of Nanotechnology, we can name the possibility of information storage with minimal scale and with a space thousand times of ordinary space. These special features of Nano as well as its flexibility in different situations and locations have made Nanostructures to be used as a proper tool in fields of electronics, such as development of sensors. Cooperation between Nanotechnology and Biotechnology and advances in this field will lead to producing smaller sensors with higher rate of sensitivity, better capability of processing and higher information transfer speed (Husseini and Jamaloo, 2005).

General design of adaptive algorithms

The majority of fingerprint recognition systems are structured on minutia (the end of the knob and bifurcation of the knob). These systems comprise three steps for recognition: pre-processing, obtaining minutia, and adapting minutia. The first step is performed for enhancing image quality. It should be noticed that there are different methods for adaptation, including adaptation of set of points, graph adaptation, and uniformity of two sub-graphs. Adaptation step requires complex calculations in case of the following items:

- Low quality of fingerprint
- Magnitude of fingerprints databank

The images with a structural defect need robust algorithms to be adapted properly. In order to adapt the produced image in biometrics to the existent images in the memory, adaptive algorithms such as PBA or IBA (Print-based Algorithm and Image-based Algorithm) and a more complicated algorithm called "Minutia-Based-Algorithm". In PBA algorithm, the design of fingerprint such as curvatures and circles are compared with the memory samples and the algorithm consist of type, size and direction of designs within the fingerprint balanced design, while in MBA algorithm, several points of fingerprint in the memory such as the ridge ending in the fingerprint, line bifurcation and short ridges between the lines are compared with the input fingerprint. This method needs a balanced image of fingerprint. The only different item in this method is the application of a reference frame instead of adapting the centers. Each point of fingerprint section is stored as a vector in the fingerprint image.

Fingerprint sensors of MBA and IBA contain capacitor bits which are made in the form of standard CMOS technology. The majority of fingerprint sensors in the aforementioned algorithms cover a long range, from MEMS to Nano-technology. The pixels are constructed from a metal electrode which operates as a capacitor plate. Touch of finger with the sensor surface produces the capacitor. Passivation layer on the fragment surface makes a dielectric layer between the finger and the pixels, causing the chemical resistance in the finger friction. Fingerprint is produced by calculating the capacitor space of each pixel and conversion of data to a black and white image. Currently, various types of fingerprint scanners are available with difference in their sensor types (optical sensor, capacitance sensor, sensors with sensitivity to heat or pressure, and ultrasound wave sensors.

Center simulation using biometrics

For perceiving all types of technologies- applied and environmental purposes, a systematic method is required. This is known as applied and environmental classification. In addition, biometric application for relevant environments can be changeable according to the supervision or lack of supervision on the internal or external environment, or the presence of trained or amateur people in the environment. Fingerprint recognition systems are developed to protect the security of governmental and military systems. This system controls the authorized access to information by conducting the process operation which is a combination of complex image processing algorithms and checks the fingerprint of individuals who intend to access the information. Typically, a biometric system tries to extract the features from the individual's behavior or structure with the aid of pattern recognition, and then stores these features in a database (for identification and verification). The systems which perform based on physiologic signs are much more reliable than behavior-based systems.

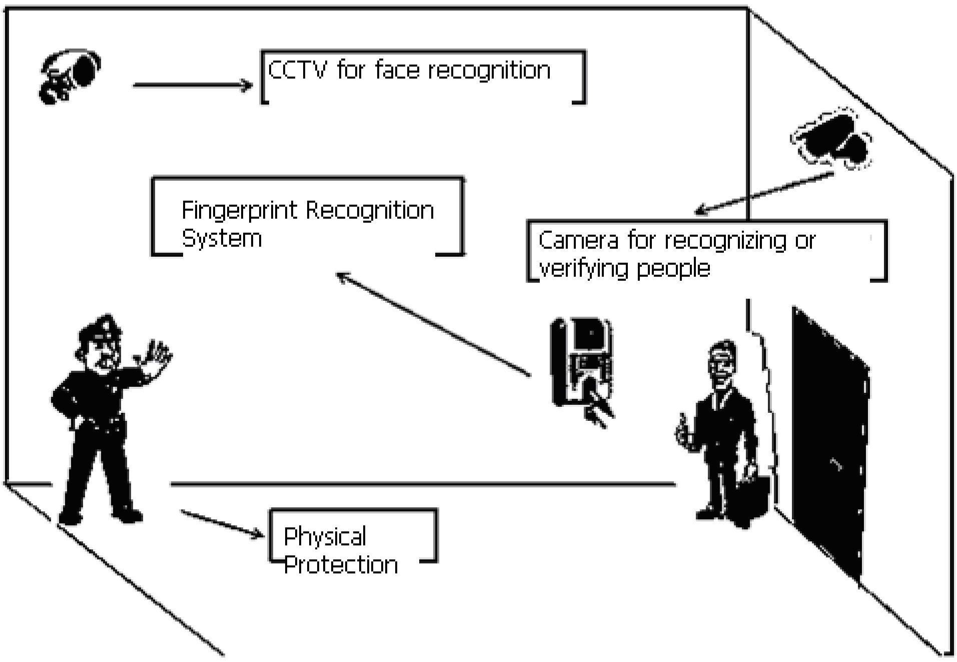
CCTV for face recognition
Fingerprint Recognition System
Camera for recognizing or verifying people
Physical Protection

Figure1. Simulation of the Center

In the above design, the individual's information is obtained in various methods once he/she enters the center. First, the person is identified by fingerprinting biometric system and the accuracy of information in the center is processed. Multi camera networks are seen as the common solution for supervision applications. Having a network of cameras with the capability of providing several images from people's faces will enhance the process of describing the faces with more robust methods. In this situation, recording the image of a given person from the front view is more probable and can be used in the simulation. So, the first step in face recognition process is to take an image from the face; this is usually possible with a camera. Such face recognition system is highly expected to use high-quality images, that is, the image taken under the desired circumstances.

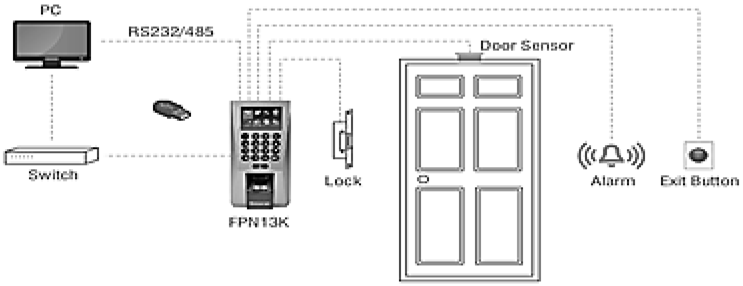

Figure2. Input biometrics of the center

CONCLUSION

The present paper introduced two adaptive algorithms: IBA and MBA. The capabilities of both algorithms in protecting the information were explained. Then, a comparison was drawn between the algorithms and Nano-sensors. Biometric methods ensure that a given identified person is the one he/she has claimed he/she is and another individual cannot impersonate him/her easily. Table 1 displays the features of various biometric sensors, showing the efficiency of each one.

Sensor type	Frequency of Use	Efficiency	Advantages	Deficits	Errors
Capacitiv	High	High	High speed	is turned on in each time of request transmit	**Little**
MBF200	High	High	High accuracy and good speed	Complex construction technology with higher price	**Little**
Ultrasoun	Moderate	High	The frequencies of this sensor are able to pass through inanimate cells	Experiences some complications in volatile climate	**Little**
Sound	Moderate	Low	Can be used in high-frequency waves	Improper efficiency when facing with humidity, diagonal fingerprint	**Moderate**
Optimal	Moderate	High	Resistant against scratch	Moderate speed	**Little**
Thermal	Moderate	Moderate	Simple manufacturing technology, resistant against scratch	Undesired outcome when finger surface is thermally misinformed or misled	**Little**
Nano-sensors	**Moderate**	**High**	**Lowe price-smaller and more sensitive**	**Inaccessibility to all features and facilities**	**low**

As it is observed, biometrics can play a major role in the field of information security and among the current algorithms and sensors, MBF200 sensor is one of the best tools of fingerprint recognition sensor with appropriate accuracy and speed

REFERENCES

Eriki D. and Magbeli T. (2012). Penetrability index of biometric system with the use of neural networks. International Conference of Artificial Intelligence and Image Processing. UAE, Dubai. October 2012

Husseini T. and Jamaloo F. (2005). Intelligent systems and Nano-sensors. 8th Conference of Electrical Engineering. Department of Electrical Engineering and Electronics.

Lee E.C., Jung H. and Kim D. (2010). Infrared Imaging Based Finger Recognition Method. Proceedings of International Conference on Convergence and Hybrid Information Technology , Daejeon, Korea, August 2010; pp. 228–230 .

Miura N., Nagasaka A. and Miyatake T. (2007). Extraction of Finger -Vein Patterns Using Maximum Curvature Points in Image Profiles. IEICE Trans Inform Syst 2007, E90-D, 1185–1194.

Panahi H., Gharebalagh M. and Razmi H. (2005). A review on neural networks applications in biometrics. 8th Conference of Electrical Engineering- Department of Electrical Engineering and Computer, University of Tabriz, 2005