národní
úložiště
šedé
literatury

Data Security in Biomedicine

Horňáková, Anna
2011

Data Security in Biomedicine

Post-Graduate Student:
ING. ANNA HORŇÁKOVÁ

Department of Medical Informatics
Instutite of Computer Science of the ASCR, v. v. i.
Pod Vodárenskou věží 2
182 07 Prague 8, CZ

hornakova@euromise.cz

Supervisor:
ING. MILAN ŠÁREK, CSC.

CESNET, z.s.p.o.
Zikova 4
160 00 Prague 6, CZ

ms@cesnet.cz

Field of Study:
Biomedical Informatics

This work has been supported by the Ministry of Education of the Czech Republic under the project 1M06014 (The Centre of Biomedical Informatics - CBI).

Abstract

This thesis analyzes current state of use of biometrics in computer security. It provides an overview of the most commonly used anatomical-physiological and behavioral biometric identification methods. The result of the work will be a new set of methods, which allows reliable identification of the user in the most comfortable way. These new principles of data security will be used to enhance the protection of specialized health record. This will contribute to expansion of generally conceived EHR MUDR concept to other application areas.

1. Introduction

Biometrics, biometric identification and verification have been investigated since the early 80's of the last century. At the end of the 20th century first applications began to emerge, especially in forensic practice where biometrics was represented by automated processing of fingerprints and palm prints found at a crime scene. Nowadays, biometric methods are irreplaceable both in the forensic sciences and in commercially available applications.

In this paper we analyze current state of use of biometrics in computer security, especially the possibilities of identification based on biometric data. Biometric characteristics can be divided into anatomical-physiological and behavioral.

2. Anatomical-physiological biometric characteristics

The most frequently used anatomical-physiological biometric characteristics in common practice are fingerprints, palm prints, geometry of hand shape and scanning of bloodstream patterns of the palm or the back of one's hand.

2.1. Fingerprints and palm prints

Fingerprints and palm prints are based on the uniqueness of ridge patterns. Miniaturization of sensors and processors allows the fingerprint-based biometric identification for large commercial use.

In practice, fingerprints are often used for authentication of persons accessing to computers or communication devices, for enhancement of protection of identification or credit cards, for authorization to access buildings and for protection of precious or dangerous devices from unauthorized use.

Interactive fingerprinting, which is now often implemented in a variety of technical equipment, is done by means of sensors. These sensors may be contact or contactless and their functions can be based on different physical principles [2].

2.1.1 Contact fingerprint sensors: Contact sensors include optical, electronic, optoelectronic, capacitive, pressure and temperature sensors. Some of these sensor types will be described in detail below. Main advantages and disadvantages of each method are clearly shown in Table 1.

Sensor	Advantages	Disadvantages
Optical contact sensors	very quick user-friendly	not resistant to dirt not hygienic don't recognize living tissue
Electronic contact sensors	resistant to dirt very quick user-friendly	not hygienic don't recognize living tissue
Capacitive contact sensors	very quick	not resistant to dirt don't recognize living tissue not hygienic
Temperature contact sensors	recognize living tissue very quick	not hygienic
Optical non-contact sensors	resistant to dirt hygienic very quick	don't recognize living tissue
Ultrasonic non-contact sensors	resistant to dirt hygienic very quick	don't recognize living tissue

Table 1: Comparison of contact and non-contact fingerprint sensors.

Optical contact sensors: Optical sensors are based on FTIR technology (Frustrated Total Internal Reflection). This means that a laser beam illuminates the bottom surface of a finger that touches a transparent sensor plate. Reflected light flux is then captured by a CCD (Charge-Coupled Device) element. The amount of reflected light depends on the depth of papillary lines and furrows. Papillary lines reflect more light than furrows.

Other optical sensors use a thick bundle of optical fibers that are perpendicular to the plane of the sensor. Here again, the method of exposure and reflection of light flow is applied. Another type of sensors uses CMOS technology (Complementary Metal-Oxide-Semiconductor).

Electronic contact sensors: Electronic sensors operate on the principle of electric field between two parallel, conductive and electrically charged plates (see Figure 1). If the shape of the originally flat plate on top changes to wavy (papillary lines and furrows), the shape of the electric field changes too. The upper plate of the sensor is represented by surface of the skin that is connected to the source reference electrical signal.

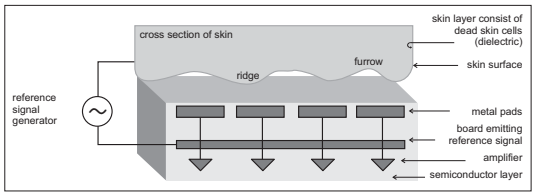

Figure 1: Simplified diagram of the electronic sensors (according to [8]).

The main advantage of this sensor is that it does not scan only the surface of the skin but it scans deeper skin layers too. This means that this type of sensor is resistant to dirt and possible damage of the skin surface.

Optoelectronic contact sensors: Optoelectronic sensors consist of two layers. The upper layer is in contact with the skin and it is able to emit light. This light is captured in the second glass layer in which photodiodes are sealed. These photodiodes convert the light into an electrical impulse.

Capacitive contact sensors: Capacitive sensors capture fingerprint by measuring electrical capacity (see Figure 2). Scanning sensor is composed of a large number of scanning surfaces that are isolated from each other. By touching the sensor, papillary lines bridge the conductive pads while furrows act as isolators. The shape of papillary drawing, therefore, modulates voltage and capacitance drops between the conductive pads. These drops are measured and they form a digitalized picture of papillary drawing.

These sensors are highly nonresistant to various types of dirt that may significantly alter conductivity of the skin.

Pressure contact sensors: Pressure sensors respond to a pressure of papillary lines on the surface of sensor.

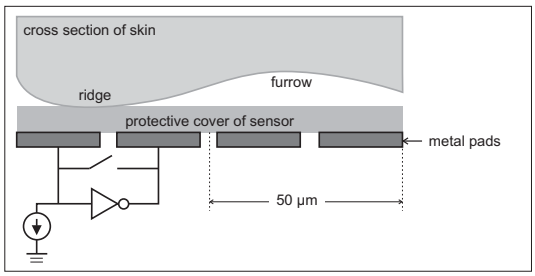

Figure 2: Simplified diagram of the capacitive sensors (according to [8]).

The sensor surface is made of an elastic piezoelectric material that transforms the pressure into an electrical signal and thus creates a picture of fingerprint.

Temperature contact sensors: Temperature sensors react to temperature differences between papillary lines and furrows. A great advantage of this sensor is that temperature is an important factor that can tell whether the scanned fingerprint belongs to a living person.

2.1.2 Contactless sensors for fingerprint: The best-known groups of non-contact sensors include optical and ultrasound sensors. The main advantages and disadvantages of these sensors are also included in Table 1.

Optical non-contact sensors: The principle of optical non-contact sensors is similar to the optical contact sensors described above with only one difference. The beam of light allows scanning from a distance of 3-5 cm.

The greatest advantage of this sensor is that it prevents contamination caused by contact with dirty fingers.

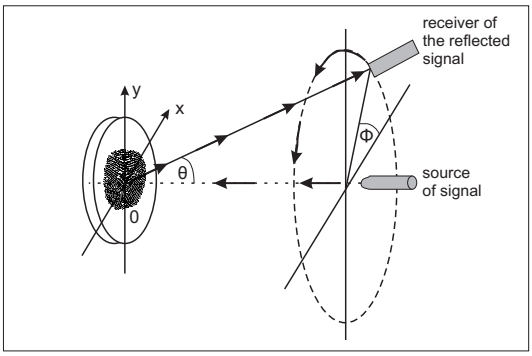

Figure 3: Simplified diagram of the ultrasonic sensors (according to [8]).

Ultrasonic non-contact sensors: Ultrasonic sensors are also based on a similar principle as the optical ones but instead of a light beam a beam of short mechanical waves (ultrasound) is being reflected from the skin surface (see Figure 3). This type of sensor eliminates all the disadvantages of previous types of sensors explained above [1].

2.2. Geometry of hand shape

Another frequently used method is the geometry of hand shape, the essence of which is measurement of lengths and widths of fingers, bones or joints of the hand (see Figure 4). The hand touches a horizontal scanner that has special fixation pins. These ensure that the hand is always in the same position. The scanner captures one image from the top (perpendicularly to the sensor board) and one image from the side. This generates two monochrome images of 'hand silhouette'.

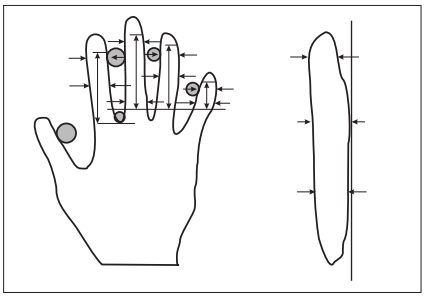

Figure 4: The basic principle of hand geometry (according to [8]).

At first, a user requiring evidence of his identity enters his or her identification number (PIN) via keyboard or he or she touches a magnetic stripe, a chip or a card to a reader. Then the user puts his or her hand to a specified position according to visual instructions that are on keyboard on the scanner [5]. Hand geometry scanners are now common in many areas including healthcare.

2.3. Scanning of the bloodstream of the palm or the back of hand

Another method suitable for use in computer security is scanning of the bloodstream of the palm or the back of one's hand. A CCD camera, which is most commonly used in this case, takes a picture of the hand and a specific pattern of blood vessel distribution captured in the image is then used to identify the person.

An unquestionable advantage of this method is that it also verifies whether the tested object is alive. The scanning runs in infrared band which is sensitive to temperature. This method takes advantage of the fact that blood

vessels in the body are warmer than their surroundings. The scanned image is further processed in a similar way as fingerprint (with the shape of vessels being compared).

Another advantage in comparison to scanning of hand geometry is that it is not necessary to place a hand in the scanner in the same position every time.

Other options for this method are to scan the bloodstream of the palm or to perform non-contact scanning of both the palm and the back of hand, which provides a high level of hygiene unlike hand geometry scanning or fingerprints [5].

2.4. Scanning of face and its parts

Instead of hands a face or a part of the face can be used to identify a person as well. There are computer programs that can recognize human faces like human brain does. Face recognition is now typical especially in criminology and there are many different methods and algorithms used for these purposes.

This method can also be easily used to secure common computing and telecommunication systems. Any standard video camera, which can be already found integrated in many screens, is sufficient to take the image of the face. The face scan can replace traditional password entry. A great advantage of this method is that there is absolutely no need for direct contact between the user and the sensor [10].

However, face recognition can be further improved in many ways. As an example, we can register signs of emotions.

An interesting application of this method in IT security suggests itself. Continuous face scanning during the work with computer would make it possible to evaluate whether it is still the same person accessing sensitive data. Not only that this method secures the system at the time of login, it can even protect the data later on, when the authorized user, for example, leaves the unlocked terminal for a period of time.

2.5. Scanning of iris or retina

Recently, thanks to its simple implementation using only conventional video systems, scanning of iris or retina is becoming a more widespread method of identification. Iris recognition is possible regardless of size, location and orientation but it requires a complicated algorithm. This method is, therefore, usually used only to ensure a high level of security [5].

A light beam is used to map the bloodstream in the retina. A part of the beam is absorbed by the retina while the other part is reflected. Special camera, that is required for the scanning, is expensive and the scanning process itself is not very user-friendly (many people are afraid of the technology) [5].

3. Behavioral biometric characteristics

Keystroke dynamics could be an interesting behavioral biometric characteristic for use in computer security not being widely used so far.

3.1. Keystroke dynamics

Keystroke dynamics allows so-called continuous (dynamic) verification, which is based on the use of keyboard as a medium of continuous interaction between user and computer. This offers a possibility of continuous control over the whole time the computer is being used. This method is useful in situations when there is a risk of leaving a computer without control for a while [3].

The most common characteristic is the time of pressing individual keys or the duration of the keypress. Another possibility is to measure typing speed, frequency of errors, style of writing capital letters or a force used to press the keys. This latter type requires a special keyboard that allows the force of the push to be measured. All other methods can be evaluated by a special program without any modification of hardware [4, 6].

4. Comparison of the methods

Most of current data security systems verify user's authorization to access the system only at the time of login. In the case that the question of user identification is solved only on the basis of biometric data, only one biometric component (or just a few of them) is used for verification in most cases.

A solution should preferentially include the methods mentioned in the introduction and emphasize those of them, which will prove themselves long-time stable or the least disturbing for staff. The method must be fast enough for the user. Hardware requirements and required processing power will also be considered.

Table 1 shows the main advantages and disadvantages of different types of contact and contactless sensors for fingerprinting. All sensors for fingerprinting are relatively quick and easy in comparison to other biometric methods.

Sensor	Advantages	Disadvantages
Geometry of hand shape	resistant to dirt	don't recognize living tissue require scanning in the same position not hygienic
Contactless scanning of bloodstream	don't require scanning in the same position recognize living tissue hygienic resistant to dirt	no possibility of continuous control
Scanning of the face	resistant to dirt recognize living tissue don't require scanning in the same position possibility of continuous control	time-consuming
Scanning of iris	resistant to dirt don't require scanning in the same position user-friendly	
Scanning of retina	resistant to dirt don't require scanning in the same position	not user-friendly time-consuming
Keystroke dynamics	user-friendly possibility of continuous control hardware-efficient	

Table 2: Comparison of anatomical-physiological and behavioral biometric characteristics.

The main differences are in resistance to dirt, which is important for the following two reasons. The first one is that the sensor should be able to work even when there is dirt on its surface or on the surface of the finger that is being scanned. The second reason is, of course, the hygienic aspect.

The greatest benefit is sensor's ability to distinguish living tissue from dead or synthetic material. Then it becomes very resistant to possible abuse.

Table 2 displays main advantages and disadvantages of other anatomical-physiological and behavioral characteristics. Besides the aspects mentioned above, we compared also the possibility of continuous authentication, the need for scanning in the same position and difficulty/ease of use.

Table 3 compares selected methods in terms of stability of biometric characteristics and time-consumption. Data in the table are not accurate readings but empirical estimates. The table shows that there is no method that would be "ideal", i.e. would offer high stability of biometric characteristics and low time consumption. Iris scanning, which is currently not used in everyday practice, is close to this ideal.

5. Application of selected methods in electronic health record security

The aim of this work is to propose a multifactor system that will verify a number of biometric features simultaneously, thus ensuring greater reliability of identification. This will protect access to patient data in electronic record personal identification ERPI, which is conceptually based on the proposal of Universal Electronic Health Record MUDR, see [7].

Security of patient data is one of the key issues in telemedicine. It may appear that this is a standard solution using the principles of electronic record EHR MUDR. But unlike our task, the concept of EHR MUDR record is designed with respect to ordinary patient data, accessed during everyday hospital operation.

Contrastingly, in the case of the electronic record of personal identification ERPI, there will be much more sensitive data related to the identification of individuals from different perspectives. For this reason there is also

Method	Stability of biometric characteristics	Time-consuming
	high = more than 80 %, medium = more than 60 %, low = less than 60 %	high = more than 3 sec, medium = less than 3 sec, low = less than 1 sec
Fingerprint	medium	low
Geometry of hand shape	medium	medium
Scanning of bloodstream	medium	medium
Scanning of the face	low	high
Scanning of iris	high	medium
Scanning of retina	high	high
Keystroke dynamics	low	low

Table 3: Comparison of methods in terms of stability of biometric characteristics in and time-consuming.

a demand for higher level of identification of persons accessing the data.

With regard to the nature of such data it appears necessary to use some set of DLP (Data Loss Prevention) allowing identification of the risks associated with the loss of sensitive data and possible dynamic reduction of these risks. Moreover, with regard to the type of sensitive identification data it is useful to have a resource that will allow consecutive audit of the data.

Commercial solutions such as RSA or Websense are available. These sets are designed to reduce the impact of potential risks, irrespective of whether the data are stored in the datacenter, transmitted over the network (network DLP) or processed in user terminal equipment (DLP endpoint). This solution is particularly interesting because in Czech Republic there has not yet been a deployment of DLP published in similar context [9].

6. Conclusion

The result should be a complex of new biometric identification methods that would allow reliable identification of users in the most comfortable form. Final application of these new principles of security will increase the level of protection of specialized health record. Furthermore, the EHR MUDR concept will expand to other application areas.

References

[1] W. Bicz, et al., "Fingerprint structure imaging based on an ultrasound camera", http://www.optel.com.pl /article /english /article.htm, 2005.

[2] N. Cravotta, "Looking under the surface of fingerprint scanners", *EDN*, http://www.edn.com /article /507025-Looking _under _the _surface _of _finger _print _scanners.php, 2000.

[3] D. Gunetti and C. Pikardi, "Keystroke analysis of free text." In *ACM Transactions on Information and System Security*, Vol. 8, No. 3, str. 312-347, 2005.

[4] J. Ilonen, "Keystroke Dynamics." In *Advanced Topics in Information Processing*, Lappeenranta University of Technology, 2003, http://www2.it.lut.fi /kurssit/03-04/010970000/seminars/Ilonen.pdf

[5] A. Jain, R. Bolle, and S. Pankarti, "Biometrics: personal identification in networked society", Kluwer Academic Publisher, Norwell, Massachusetts, USA, 1999.

[6] F. Monrose and D. Rubin, "Keystroke dynamics as a biometric for authentication". In *Future Generation Computer Systems*, Vol. 16, No. 4, str. 351-359, 2002.

[7] M. Nagy, et al., "Applied Information Technologies for Development of Continuous Shared Health Care." In *CESNET Conference 08*, CESNET, z.s.p.o., Prague, 2008, http://www.ces.net /events /2008 /conference /cesnet08-proceedings.pdf

[8] R. Rak, V. Matyáš, and Z. Říha, "Biometrie a identita člověka: ve forenzních a komerčních aplikacích", Grada, Praha, 2008.

[9] RSA, The Security Division of EMC: Security Solutions for Business Acceleration [online]. 2010 [cit. 2011-07-19]. RSA Data Loss Prevention (DLP) Suite. http://www.rsa.com /node.aspx ?id =3426.

[10] D. Zhang, "Automated biometrics: technologies and systems", Kluwer Academic Publisher, Boston, 2000.