UDC 621.3.05

Volodymyr Kazymyr, Doctor of Technical Sciences
Andrii Mokrohuz, PhD student
Chernihiv National Technological University, Chernihiv, Ukraine

INFORMATION TECHNOLOGIES OF BIOMETRIC SECURITY FOR MOBILE DEVICES

В.В. Казимир, д-р техн. наук
А.О. Мокрогуз, аспірант
Чернігівській національний технологічний університет, м. Чернігів, Україна

ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ БІОМЕТРИЧНОГО ЗАХИСТУ ДЛЯ МОБІЛЬНИХ ПРИСТРОЇВ

В.В. Казимир, д-р техн. наук
А.А. Мокрогуз, аспирант
Черниговский национальный технологический университет, г. Чернигов, Украина

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ БИОМЕТРИЧЕСКОЙ ЗАЩИТЫ ДЛЯ МОБИЛЬНЫХ УСТРОЙСТВ

This article provides an overview of biometric security for mobile devices. Biometric security systems that use the retina, voice, facial geometry, fingerprints, signature and others have been considered. Analysis of the advantages and disadvantages of biometric security systems is carried out in terms of integration with mobile devices. Improvement of biometric security for mobile devices using the existing systems of biometric security is proposed.

***Key words**: biometric security, biometrics, mobile device, recognition systems.*

Представлено огляд біометричної безпеки для мобільних пристроїв. Розглянуто системи біометричного захисту, які використовують сітківку ока, голос, геометрію обличчя, відбитки пальців, підпис та інші. Аналіз переваг і недоліків біометричних систем безпеки здійснюється з погляду інтеграції з мобільними пристроями. Запропоновано варіант удосконалення біометричної безпеки для мобільних пристроїв, використовуючи наявні системи біометричного захисту.

***Ключові слова**: біометрична безпека, біометрія, мобільний пристрій, системи розпізнавання.*

Представлен обзор биометрической безопасности для мобильных устройств. Рассмотрены системы биометрической защиты, использующие сетчатку глаза, голос, геометрию лица, отпечатки пальцев, подпись и другие. Анализ преимуществ и недостатков биометрических систем безопасности осуществляется с точки зрения интеграции с мобильными устройствами. Предложен вариант усовершенствования биометрической безопасности для мобильных устройств, используя существующие системы биометрической защиты.

***Ключевые слова**: биометрическая безопасность, биометрия, мобильное устройство, системы распознавания.*

Introduction. Before consideration of using biometric security with the mobile devices in the future it is useful to look back and pay attention to the main events in the history of the biometrics and the biometric security development.

The term ‘biometrics’ consists of two Greek words ‘bio’ (life) and ‘metrics’ (to measure). The origin of biometric technology is much older than suggested by their futuristic image. The creators of the Great Pyramids in ancient Egypt recognized the benefits of working on the identification of pre-recorded personal characteristics. Egyptians are clearly ahead of their time, as for the next four thousand years in this area practically nothing new happened. Only in the late 19th century began to emerge systems using fingerprints and other physical characteristics to identify people. For example, in 1880, Henry Faulds, a Scottish physician, who lived in Japan, published his reflections on the diversity and uniqueness of fingerprints, and suggested that they may be used to identify criminals. In 1900 Galton-Henry published a significant work about a system of fingerprint classification. Every 3-5 years after 1930 some significant researches had been made in the field of the biometrics before nowadays. The development of the biometrics became faster with the improvement of computer systems in 20th century [1]. Meaning of the ‘biometrics’ is changed due to the rapid development of the computer systems. There is a quite good definition of the biometrics which is “the process by which a person's unique physical and other traits are detected and recorded by an electronic device or system as a means of confirming identity: Scanning of the human iris is a reliable

form of biometrics" [2]. And another definition is "the analysis of biological data using mathematical and statistical methods the practice of digitally scanning and the physiological or behavioral characteristics of individuals as a means of identification" [2].

There are a lot of different types of systems which use the biometric security for person recognition and providing access to some information. These systems are based on fingerprints recognition, face recognition, iris recognition, voice recognition and others. Biometric security systems are used in different fields of human life, for instance, healthcare industry, government agencies, customer market, etc. The mobile devices protection could be implemented using biometrics, but there are still some problems dealing with technology of biometric security. There are many types of biometrics can be measured and used for protection in the mobile device. It is required to choose the most appropriate variant and consider the main advantages, disadvantages, potential risks, and benefits of the technology. Ethical problem is also one of the most important, because many people will not use biometric security on their mobile device and this problem requires consideration as well.

So this work considers biometric security technologies with short overview of each one including drawbacks, benefits, risk, etc. Some choices of biometrics recognition systems that can be used with mobile devices in the future are presented in the paper.

It is also required to determine the meaning of the 'mobile device' in terms of this article. People usually associate term 'mobile device' with smartphone, tablet or laptop, but many different and unusual mobile devices will appear in the future and this can change the concept of 'mobile device'. For instance, Google glass is a good example of entirely new mobile device which was produced only in 2012 [3]. Mobile robots [4] which can perform some actions are another example of mobile device of the future.

Overview of biometric security for mobile devices. Many biometrics solutions exist nowadays. Some of them are used for biometric security systems and are able to provide appropriate level of protection. A survey of the biometric security systems [5] provides information about existing biometric security systems and their effect on people's life in the future. Author of the article presents such solutions as facial recognition detector, fingerprint reader, voice recognition, iris scanner and recognition, veins recognition, DNA biometrics and 2D barcode scanner [5]. It is possible to add hand geometry and signature recognition solutions to this list [6]. As it was mentioned above, these approaches are able to provide security. Author of the article [6] gives some advantages of the biometric security. For instance, the biometric security is much preferable than traditional password-based authentication schemes, because they are more reliable then password-based system as biometric traits cannot be lost or forgotten. It is very hard to copy, distribute or share biometrics traits. Another significant advantage of biometrics is that they require person to be present at the time and the point of authentication. Thus, biometrics is more powerful than standard password-based systems, but it can be enhanced with password as well [6].

Two types of protection can be provided by the biometric security systems. They are physical access control and logical access control. Physical access control can be used for access devices which are applied at doors or computers. Logical access is a process of accessing data or computer programs [5]. Mobile devices can be used for different purposes in the future, so it will be possible, using biometric security, to provide both logical access and physical access. Using biometric security for logical access is an obvious and straight forward task, but how mobile device protected with biometric security can be used for physical access presents source [7], where smartphone with special application installed on it plays role of e-key. This application replaces houses keys and allows using smartphone as digital key, as seen in Fig. 1.

Fig. 1. Smartphone is a digital key [7]

Another variant of using mobile devices is presented in the source [8]; Google wallet application is presented in this article and it replaces credit cards with smartphone. Mobile device will be able to perform a lot of actions in the future and some of them definitely require high level of security which can be provided by using biometrics. These two examples demonstrate very important role of the mobile device.

- **Fingerprint recognition**

The biometrics undoubtedly has advantage over standard schemes of security and authentication. Therefore, the most appropriate approaches should be chosen for mobile device security. One of them is fingerprint recognition. This approach is based on uniqueness of the different patterns of ridges which are the upper layer of skin [5]. This solution has a lot of advantages. For instance, it has very high accuracy, it is the most economic and widely spread solutions for PC, it is the oldest [1] and the most developed biometrics, it is standardized. Moreover, mobile devices with fingerprint recognition systems are available now. It is very popular solutions, but it has some disadvantages and social problems as well. One of the significant drawbacks is possibility to bypass fingerprint scanner using some technics. These technics were demonstrated in one of the episodes of 'Mythbusters' [9]. This episode demonstrates possibility of bypassing fingerprint recognition security system using finger pads which were made from different materials such as ballistic gel, silicon, etc. However, there are a lot more disadvantages for this approach. Dirty or dryness of the finger's skin can be a reason of fingerprint scanner mistakes. It is impossible to use scanner for children, because the size of their fingerprint changes very quickly. There is also one big ethical problem dealing with this solution. Some people will never use the fingerprint security system on their mobile devices, because it is still related to the criminal identification [10]. So, using the fingerprint security system with mobile devices may not be possible without some modifications in the future.

- **Face recognition**

Every mobile device has a camera which can be used as a face recognition scanner nowadays. The face is one of the easiest characteristic which can be used for security purposes. In the future it will not be difficult to install high definition camera special for this purpose in every mobile device. The obvious advantages of the face recognition systems are:

1. does not require special hardware for face recognition, because it uses only camera;
2. it is cheap technology;
3. it is non-intrusive, because users of mobile devices do not need perform any additional actions to get access to their device [10].

This approach is not unique as other biometrics recognition systems such as retinal, iris and DNA (Deoxyribonucleic acid) recognition. Camera can provide only 2D recognition, so quality of recognition can be affected by changes in lighting, the person's hair, age and if person wear glasses [10]. This solution can be used in the future, but 2D recognition should be replaced by 3D recognition. This will help reduce errors and mistakes in recognition system and provide higher level of security. 3D scanners are available nowadays. However, their size may not compatible with some mobile devices and this restricts using of the face recognition systems. Therefore, reducing the size of the 3D scanners is one of the priority tasks to make them appropriate for mobile device.

- **Iris recognition**

This approach is focused on specific traits of human eye and uses characteristics of the iris. There is a definition of the iris "The iris is the annular region of the eye bounded by the pupil and the sclera (white of the eye) on either side. The visual texture of the iris is formed during fetal development and stabilizes during the first two years of life. The complex iris texture carries very distinctive information useful for personal recognition" [6]. So, it is possible to use iris traits in biometric security systems. The iris recognition has very high accuracy. FMR (False match rate) and FNMR (False non-match rate) of iris recognition gives result 0,99 % and 0,94 % [6]. This fact makes iris recognition systems is the most reliable in comparison with other approaches. Moreover, scanning of the iris takes about 5 seconds, so it is very fast approach as well. It is impossible to use eye of the dead person to bypass this system, because iris of the dead person deteriorates very fast to be useful [10].

Taking into account all advantages of the iris recognition system it seems very promising, but some drawbacks exist for this solution. These systems are very expensive nowadays, but in future this problem may be solved. There is an ethical problem which can delay introduction mobile device with iris recognition system to people. The iris recognition system is very intrusive, because user has to keep his eye too close to the iris scanner and this can be annoying for some people [10]. Therefore, it is required to concentrate efforts on overcoming of this problem. Nevertheless, this solution can be used for protection of mobile devices.

- **Hand geometry and veins recognition**

Hand of the human being is very unique and traits of the hand can be used in biometric security systems as well. Hand geometry recognition systems are based on measurements taken from the human hand. For instance, these measurements can be size and shape of palm, height and width of fingers [6]. Another measurement that can be taken from the human hand is veins topology. Every person's vein has unique physical traits that can be useful for recognition systems. Recognition system is able to capture image pattern of the veins, as seen in Fig. 2 [5].

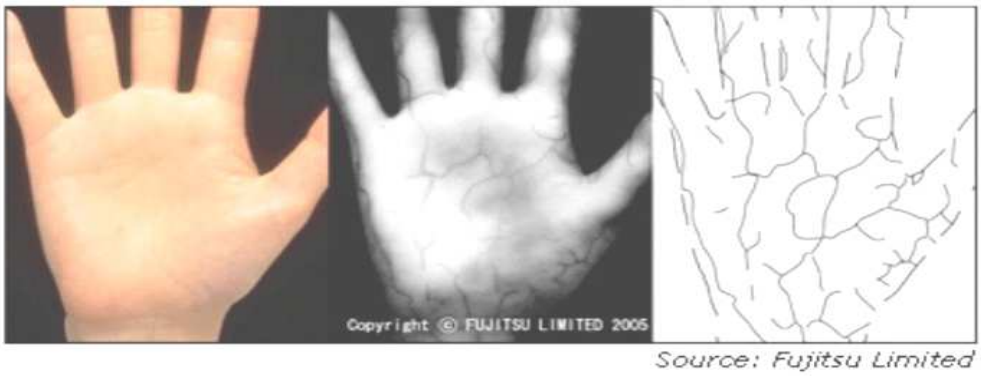

Fig. 2. Example of vein scanning [5]

These two approaches can be used together to increase quality of recognition and provide better level of security. The advantages of vein and hand geometry systems are very impressive:

1. very high level of accuracy;
2. only 1/2 sec is required to verify person;
3. does not have negative attitude of society [10].

This solution is one of the most appropriate, but for mobile device it is almost unacceptable. Firstly scanners of the hand are too large [6] to be used with mobile device. Person has to put palm on scanner to be verified, but arthritic person cannot do this properly, so errors in recognition are possible. Therefore, it is required to change principle of scanning of the person's hand in the future. For instance, it may be some kind of 3D scanner that can be applied for face recognition as well. Children cannot use hand geometry and veins recognition systems, because their hand is changing fast during the growth period [6].

Mobile device with hand geometry and veins recognition security systems can be used in the future, but it is required to solve problems dealing with method of scanning and size of scanners.

- **DNA recognition**

This solution is the most reliable and accurate. It is based on DNA biometrics which is impossible to fake, because each person's DNA is unique. The author of the source [5] states that "each cell in the human body contains a copy of this DNA. DNA profiling will decide the amount of VNTR (variable number tandem repeat) which repeats at a number of distinctive loci. These amounts of VNTR will make up an individual's DNA profile" [5]. DNA recognition systems use unique characteristics which are standardized, so the probability of mistakes is very low. Nevertheless, DNA recognition systems do not widespread as other systems and there are reasons for this. One of the most significant drawbacks of the DNA recognition systems is need to get physical samples such as hair or blood to collect DNA data. This process is not convenient for person and many people will not use this solution on their mobile devices [5]. Moreover, these systems are very expensive and require a lot of time to identify person. So, security systems with DNA recognition could be used in the future, but it is required to make DNA recognition less intrusive and decrease time of recognition. And even after all these improvements many people refuse using DNA recognition security system.

- **Voice recognition**

Human's voice has unique traits such as voice tract and voice accent [5]. These two features of the voice make it useful for biometric identification of a person. Biometric security systems which use voice recognition systems can be a good solution for mobile devices, because vice recognition has high social acceptability, it is not intrusive, verification time is about 5 seconds and it is very cheap technology [10]. Term 'mobile device' implies that this device is used everywhere. People may use it in crowded places, in the street, at home etc. The voice recognition systems are very sensitive to the background noise. Nevertheless, it is not all drawbacks for these systems. Another significant disadvantage is that voice can change due to the age, medical conditions, weather or emotional state [6]. Thus, improvements of the voice recognition are required in the future. Mobile devices with voice recognition systems will not require additional hardware and this will make them more compact and comfortable to use.

Only the most appropriate biometrics technologies were considered for mobile devices of the future, but there a lot more biometrics that can be measured and used for security purposes in the future. Table 1 shows some comparison of biometric technologies.

Only visible biometrics of the human body was considered in this paper, but 'hidden' biometrics exists and can be used for security purposes. Source [12] gives examples of hidden biometrics such as using MRI and X-RAY images to measure human body hidden biometrics [12], but this approach does not suitable for mobile devices even in the future, so consideration of these technologies is beyond the scope of this paper.

Table 1

Comparison of various biometric technologies [6]

Factors → / Biometric identifier ↓	Universality	Distinctiveness	Permanence	Collectable	Performance	Acceptability	Circumvention
Face	H	H	M	H	L	H	H
Fingerprint	M	H	H	M	H	M	M
Hand geometry	M	M	M	H	M	M	M
Iris	H	H	H	M	H	L	L
Keystroke	L	L	L	M	L	M	M
Signature	L	L	L	H	L	H	H
Voice	M	L	L	M	L	H	H

Appropriate types of biometric security for mobile devices. Mobile device performs some vital actions in the future. So, a very high level of security is required to restrict unauthorized access. It is assumed that mobile devices play role of a wallet, a key, a passport, etc. They store private and maybe secret information. As it was mentioned above biometrics security has advantage over standard authentication and authorization systems which are used nowadays. Nevertheless, every biometric recognition technology together with benefits has significant drawbacks. Thus, using only one biometric security system on the mobile device will not provide an appropriate security level. Several security systems may need to be installed in mobile devices. These biometric security systems should not be intrusive and collect biometrics data insensibly for user.

Development of the biometric security systems will allow realization of this concept, but development of the bypass technologies will progress in the future as well. So, even several security systems on the mobile device will not be enough. Thus, it is required to provide some algorithm that will prevent bypass cases or will make bypass inefficient. For instance, mobile device has four biometric recognition (security) systems installed on it. They are a face recognition security system, an iris recognition system, a voice recognition system and a hand recognition system. These systems work in turn and collect data randomly. It is possible that only two systems work at one moment of time, but the user does not know which system is verifying him at that moment, because systems collect data insensibly for user. If user is able to provide biometrics data, for instance, for face recognition security system and for iris recognition system he gets an access to the data on the mobile device. This should prevent bypass, because even if someone has all required artificial biometric traits, it is impossible to guess which biometrics traits are required at that moment to get access to the device because of randomly collecting of the biometric data.

It is assumed that this approach will prevent illegal access to the mobile device for unauthorized persons. Nevertheless, there are some problems dealing with this concept of the mobile device with several biometric security systems. Firstly, mobile device has to have a very powerful hardware to provide resources for several security systems. Secondly, all biometric scanners have some level of intrusiveness; hence it is impossible to make scanning insensible for users. Therefore, these problems should be solved in the future.

Summary. Using information presented above it was defined, that not all biometric security system can be used with mobile devices. There are two main reasons for this: technical restrictions of mobile device and ethical considerations. Some of the systems require improvement. Time and technologies are also required to adjust some security systems for mobile devices.

The most appropriate biometric security systems have been chosen for mobile devices and the method of improvement of security has been presented for mobile devices in this article.

References

1. *Biometrics* history (2006, August 6) [Online]. Available : http://www.biometrics.gov/documents/biohistory.pdf.

2. *Dictionary* [Online]. Viewed May 5, 2013. Available : http://dictionary.reference.com/browse/biometrics.

3. *Google* glass [Online]. Viewed May 3, 2013. Available : http://www.google.com/glass/start/what-it-does/.

4. *Song-Hiang Chia*; Jr-Hung Guo; Yi-Lin Liao; Kuo-Lan Su, "Implementation of the Multiple Tasks Allocation Problem for Mobile Robots," Digital Manufacturing and Automation (ICDMA), 2011 Second International Conference on , vol., no., pp. 618, 623, 5-7 Aug. 2011.

5. *Chien Le*. A survey of biometrics security systems. (November 28, 2011) [Online]. Available : http://www.cs.wustl.edu/~jain/cse571-11/ftp/biomet.pdf.

6. *Jain, A.K.;* Ross, A.; Pankanti, S., "Biometrics: a tool for information security" Volume: 1 Issue: 2, Issue Date: June 2006, page(s): 125–143.

7. *ShareKey* smartphone app replaces your house keys [Online]. Viewed May 4, 2013. Available : http://www.gizmag.com/sharekey-smartphone-nfc-house-keys/25653/.

8. *Tap-to-pay* Google Wallet launched [Online]. Viewed 7 May, 2013. Available : http://www.gizmag.com/google-wallet-launched-today/19881/.

9. *MythBusters* Fingerprints Busted HD! [Online]. Viewed May 7, 2013. Available : http://www.youtube.com/watch?v=3Hji3kp_i9k.

10. *Advantages* and disadvantages of technologies [Online]. Viewed May 5, 2013. Available : http://biometrics.pbworks.com/w/page/14811349/Advantages%20and%20disadvantages%20of%20technologies.

11. *Boehnen, C.*; Flynn, P., "Accuracy of 3D scanning technologies in a face scanning scenario," 3-D Digital Imaging and Modeling, 2005. 3DIM 2005. Fifth International Conference on , vol., no., pp. 310, 317, 13-16 June 2005.

12. *Nait-Ali, A.* "Beyond classical biometrics: When using hidden biometrics to identify individuals," Visual Information Processing (EUVIP), 2011 3rd European Workshop on, vol., no., pp. 241, 246, 4-6 July 2011.