Y. Y. Bilynskyy, Dr. Sc. (Eng.) Prof.; M. Y. Yukysh, Cand. Sc. (Eng.); O. A. Pavlyuk

FINGERPRINT SCANNERS

The paper analyses the main methods of fingerprint scanning and presents the structures of main scanner types describing their advantages and disadvantages. There had been outlined the main problem of fingerprint scanning and ways for its solution.

Keywords: *fingerprint scanner, fingerprint, biometrics.*

Introduction

Biometric technologies are widely used to determine a person's identity, for example, voice recognition, facial recognition, iris recognition, fingerprint sensing, palm scanning, DNA analysis, etc. Biometric methods are frequently applied in the systems of access management, working time and visitor registration, electronic payments and voting systems. These very systems mostly contribute the biometrics market [1-3].

Rapid development of biometric technologies was caused by the events on September 11, 2001. At that time such companies as LG, Sanyo, Polaroid, NEC, Panasonic have started the development of biometric equipment.

Finger scanners are the devices for conversion of ridge pattern into a digital image. As early as in the 19^{th} century it was determined that a ridge pattern is unique for every person (even twins have different ridge patterns). For more than 100-year history of using ridge pattern in crime detection practice there were not discovered any two people with identical patterns [1,2,4,5]. Now you can find the finger scanners in the banks, custom offices, public institutions, laptops, mobile phones and other places and devices. By estimation of Frost & Sullivan agency, the use of finger scanners will grow by 25% every year because of mass creation of biometric passports in the USA and European Union. India has started the Unique Identification Authority program with the purpose of issuing a biometric identity card for each of its 1.2 billion citizens.

Problem definition

Scanners' reliability and security are mostly achieved by using special software. But scanner technology leaves some uncertainty and probability in making a wrong decision in the result of possible ill-posed intervention. For example, in Germany the hackers have got a finger print of Wolfgang Scheuble, the Head of German Ministry of Home Affairs, stuck his fingerprints on their own and were identified by optical scanners [6]. That is why it is important to develop more secure technologies, as in many European countries one can pay in supermarkets by a fingerprint using no credit card.

In future the use of fingerprints in other spheres of human life will only increase. A weak point of the scanners, as it was mentioned above, is a poor ability to distinguish the artificial copy of a finger from a real one. That is why it is necessary to use the parameters of a natural human finger for identification. Such parameters include temperature, electrical impulses from heart, variations of blood pressure (pulse), electrical charge of surface skin cells from blood flow [7]. It will be more difficult to interfere with the scanner security for checking one or several parameters mentioned above when scanning a fingerprint.

That is why the purpose of this work is to review modern automated methods of fingerprint scanning, which provide high level of fraud security.

Main part

Today there are many known types of fingerprint scanners. They can be divided into 3 main categories: optical, ultrasonic and semiconductor (fig. 1) [8].

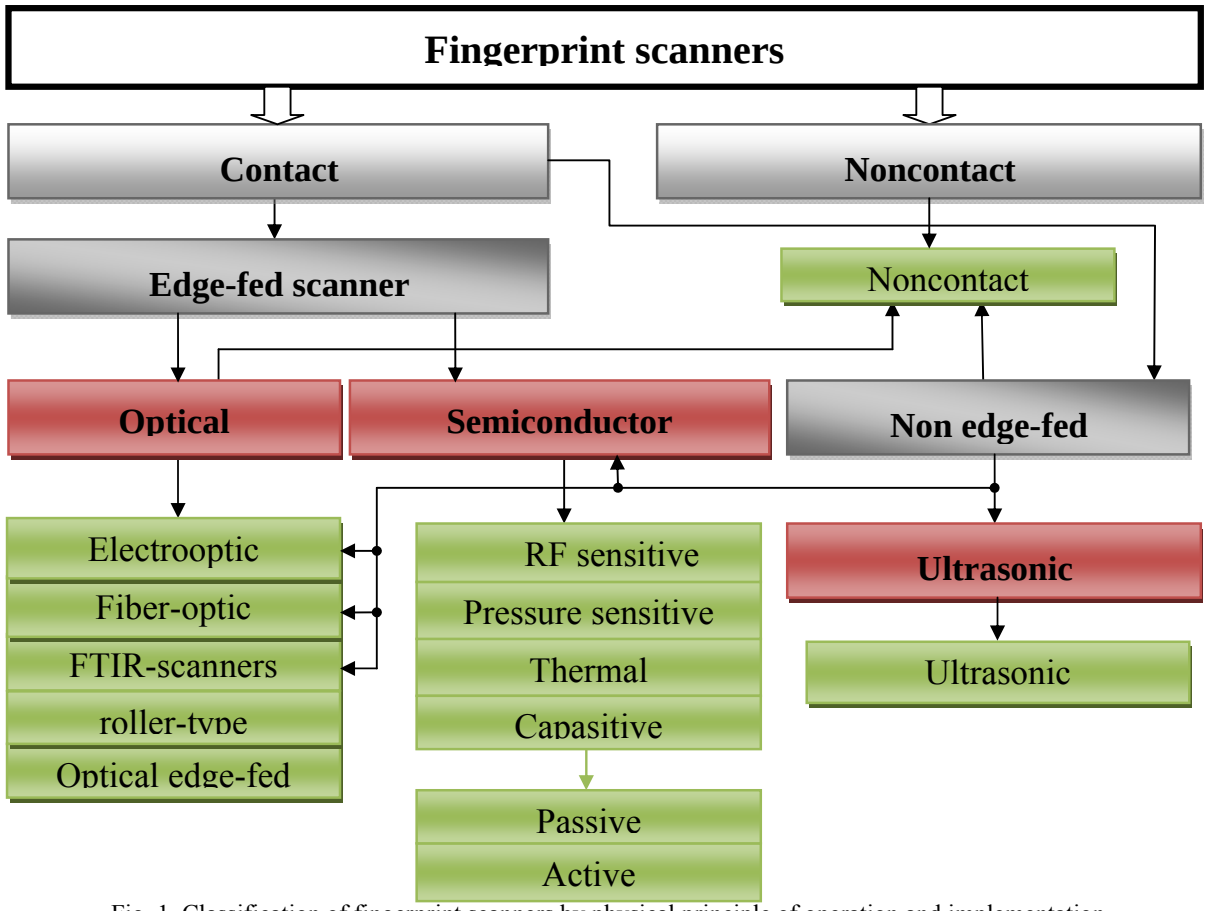

Fig. 1. Classification of fingerprint scanners by physical principle of operation and implementation

The main scanner parameters include resolution, speed of scanning, wear resistance etc. Table 1 presents the main scanner parameters basing on print sources of domestic and foreign authors [9-17].

Table 1

Main parameters of fingerprint scanners.

Parameter	Scanner type		
	Optical	Ultrasonic	Semiconductor
Resolution (dpi)	500-3000	500	508
Speed of scanning (frame/s)	50-2130	-	20-30
Durability (bill. touches)	1-4	-	1-10
Dimensions (mm)	45 * 63 * 26	87*150*82	27*20,4* 3,5
Price $	130-200		20-50
Probability of wrong authorization	10^{-9}	-	10^{-9}
Sensitivity to skin impurities	high	low	low

The main manufactures of optical scanners are BioLink, Digital Persona, Identix. The semiconductor scanners are produced by Infineon, ST-Microelectronics, Veridicom, IDEX, Atmel and the ultrasonic ones are produced by Ultra-Scan Corporation.

The optical scanners are based on optical methods of imaging. These scanners are used most widely. Today there are the following technologies of optical scanners implementation: FTIR ((Frustrated Total Internal Reflection), fiber-optical, electro optic, edge-fed, roller-type and noncontact scanners [8,18-20].

The FTIR scanners are based on the total internal reflectance. The finger should contact the glass with the light source and a camera under it, which are placed in different sides. The light reflects from the glass and falls on the camera. The camera detects less light in the region without total internal reflectance i.e. where ridges contact the glass. Thus the camera detects and digitizes a dark ridge pattern [8, 20].

The fiber-optic scanners consist of a set of arranged optical fibers, which, in turn, compose the matrix to which a finger should be applied. A finger is illuminated by a light source located over it and shines the finger through. Each optical fiber ends with a light detector. When a ridge contacts an optical fiber, a light detector detects the light passed through the finger. If there is no ridge in the region then the detector detects no light. Further the light detectors generate a digital ridge image [8, 18].

The electrooptic scanners use a special electrooptic polymer containing light emitting layer. When a finger contacts the scanner, the heterogeneity of the electric field on its surface (the voltage difference between ridges and hollows) influences this layer in such a way that it luminescences the fingerprint. Then the light detector array converts this luminescence into the digital image.

The optical edge-fed scanners are similar to FTIR devices. Their peculiarity is that the finger should not be simply applied to the scanner but passed over a narrow type-reader. When a finger moves on the scanner surface, a number of snap-shots are captured. And the neighboring picture areas are captured with overlapping of one another to form an exact image. Such a design allows to reduce dimensions of both the prism used and the scanner.

The roller-type scanners consist of a transparent cylindrical roller with a static light source, lens and a tiny camera inside. A finger is scanned rolling the roller. When a finger moves on the roller surface, a number of snap-shots of fingerprint pattern is captured. The fingerprint image is captured after the whole finger had been processed [8].

Non-contact scanners do not need a finger contact on the scanning surface. A finger should be put on the hole in the scanner where several light sources illuminate it from different sides. There is a lens in the center of the scanner which projects data to the CMOS camera to convert them into the fingerprint image [8, 19, 20].

Another variant of a non-contact scanner is a scanner which uses light polarization. It works as follows. A hand and a fingerprint are illuminated by a polarized light. Then the image is captured after passing the reflected light through a polarization filter. After capturing the first image, the electric motor turns the filter to 90^0 and another image is captured again. The comparison of two images allow to significantly increase the fingerprint contrast and receive the image of tissues under the skin. The advantages of this scanner are: no scanner dirtying, biological security (from hygienic point of view), protection of the scanner by the armored glass. The scanner disadvantages are complicated design and relatively high price [21].

The advantages of optical scanners are relative cheapness and compact size. The disadvantages are that they need constant maintenance. Besides dust, mud and scratches may significantly decrease the image quality. These scanners are also sensitive to the skin's surface condition. Dry, oil or damaged skin may result in image blur.

But the biggest drawback is that these scanners do not identify the plaster casts and other types of fraud [8, 18 – 20].

An ultrasonic scanning means a fingerprint surface scanning with ultrasonic waves. Then the distance between the wave source and the ridges and cavities can be measured by the returned waves.

The advantages of such scanners are: the captured image is 10 times better than in optical ones; this method almost completely secured from plaster casts and enables not only fingerprint imaging but measuring other parameters (for example, pulse inside the finger). The disadvantages are high price and big dimensions [8] in comparison with other scanners.

The semiconductor scanners are based on using semiconductor properties for fingerprint imaging. The semiconductor behavior changes in the points where the ridges of fingerprint pattern contact the scanner surface. For the present time there are several implementations of the semiconductor scanners: thermal, pressure-sensitive, capacitive and radiofrequency scanners [8, 18 – 20].

The thermal scanners use sensors which consist of the pyroelectric elements. These elements can register the temperature differences and convert it into the voltage. When a finger contacts the sensor, it builds the finger's surface temperature map by the temperature of ridges contacting the pyroelectric elements and the air temperature in the cavities with further converting this map into the digital image [8, 18, 19]

The pressure-sensitive scanners are based on arrays of piezoelectric cells. When a finger contacts the scanning surface, the fingerprint ridges push some cells on the surface and the cavities make no pressure, respectively. The voltage array received from piezoelectric cells is further converted into the fingerprint image.

The RF-scanners use sensor arrays. Every sensor operates as a tiny antenna. A weak radio signal is projected to the finger surface being scanned. Every sensor in the array receives the signal reflected from the fingerprint pattern. The voltage inducted in each antenna depends on the presence or absence of fingerprint ridge above it. The received voltage array is then converted into the digital image [8, 18, 20].

The capacitive scanners are produced on the silicon plate with microcapacitors region. There are two types of such scanners: passive where every cell has only one disk, and active where a capacitive cell has two disks. The advantages of the active method are the ability to use additional functions of fingerprint image processing, higher resistance to external influences and higher noise-to-signal ratio. The short-range interaction of the finger surface with silicon plate enables registering the heartbeat electrical impulses. This feature allows to recognize plaster casts [8, 19, 20, 22].

All the semiconductor scanners listed above have the edge-fed variants that make them smaller and cheaper. The advantages of semiconductor scanners are small dimensions, high image accuracy independent on the skin state, and the possibility to receive the high-quality image even of the dirty finger.

The disadvantages are fast sensor wearing because one should put a finger directly on the scanning surface (any intermediate layer influences the scanning results); high sensitivity to strong external electrical fields; sensitivity to vibrations and strokes [8, 18 – 20].

Conclusions

The paper considers the methods of fingerprint scanning and the main types of scanners, their advantages and drawbacks. There had been determined the main problem which appeared during the wide use of fingerprint scanners - poor security from plaster casts. That is why the most promising direction in further developments are scanners with registration of biological characteristics of the living organisms. The semiconductor thermal and capacitive scanners are among such scanners.

REFERENCES

1. Общая характеристика биометрических технологий. Основные группы биометрических идентификаторов и технологий [Електронний ресурс] // ООО Биолинк Солюшенс, 2007. Режим доступу: http://www.biolink.ru/technology/biometric.php

2. Рынок биометрии будет каждый год расти на четверть [Електронний ресурс] // Security News : Информационно-аналитическое издание по техническим средствам и системам безопасности. Режим доступу: http://www.secnews.ru/foreign/15660.htm

3. Обзор биометрических технологий [Електронний ресурс]: Прогноз финансовых рисков 2000 – 2009. /

В. Задорожный // Режим доступу: http://www.bre.ru/security/20234.html

4. Идентификация по отпечаткам пальцев. Часть 2 [Електронний ресурс]: Прогноз финансовых рисков 2000 – 2009. / В. Задорожный // PC Magazine/Russian Edition №2, 2004. Режим доступу: http://www.bre.ru/security/21052.html

5. Биометрия: итоги и ожидания [Електронний ресурс]: ООО Биолинк Солюшенс, 2007 – 2010. / А. Арсентьев // Режим доступу: http://www.biolink.ru/technology/newss/4124/

6. Немецкие хакеры грозят «пальцем» [Електронний ресурс]: Франкфурт-на-Майне. / К. Куц // Режим доступу: http://vz.ru/society/2008/4/2/156615.html.

7. Система физической идентификации по отпечаткам пальцев Sagnier [Електронний ресурс]: Nicsaworld S.A. 2005. // Режим доступу: http://www.nicsaworld.com/pdf/FIngrus.pdf

8. Идентификация по отпечаткам пальцев. Часть 1 [Електронний ресурс]: Прогноз финансовых рисков 2000 – 2009. / В. Задорожный // PC Magazine / Russian Edition №2, 2004. Режим доступу http://www.bre.ru/security/20994.html.

9. Биометрическая идентификация по отпечаткам пальцев. Технология Finger Chip [Електронний ресурс] / О. Гуреева // Компоненты и технологии №4, 2007. Режим доступу: http://www.kit-e.ru/articles/rfid/2007_4_176.php

10. AES1711 is AuthenTec's slide sensor [Електронний ресурс] // Виробник Authentec. Режим доступу: http://www.authentec.com/products-wireless-aes1711.cfm

11. Сканер отпечатков пальцев BioLink U-Match 3.5 [Електронний ресурс] // Виробник BioLink. Режим доступу: http://biolink.ru/products/scanners/

12. Lock LH9-3 [Електронний ресурс] // Виробник ADEL. Режим доступу: http://www.adellock.com/en/product_show.asp?id=66

13. The world's thinnest fingerprint sensor, SmartFinger® Film, is a finalist in the Sesames Awards competition [Електронний ресурс] // Виробник IDEX. Режим доступу: www.idex.no

14. Fingerprint Sensor FPC1011F [Електронний ресурс] // Fingerprint. Режим доступу: http://www.fingerprint.se/en/Products/All%20products%20overview.aspx?sc_lang=en.

15. Product Specifications TCS5 TouchStrip® Fingerprint Sensor (TCEEA4 (TCS4C+TCD50A)) [Електронний ресурс] // Upek. Режим доступу: http://www.upek.com/solutions/productfinder/

16. AuthenTec Fingerprint Sensors AES2660 [Електронний ресурс] // Authentec. Режим доступу: http://www.authentec.com/products-pcsandperipherals.cfm.

17. Сканер отпечатков пальцев Model [Електронний ресурс] // Виробник Ultra-scan. Режим доступу: http://www.ultra-scan.com/Default.aspx?tabid=496.

18. Введение в биометрию [Електронний ресурс] // ООО «н-Тегрити». Режим доступу: http://www.n-trance.ru/?area=5&block=5.

19. Биометрические технологии [Електронний ресурс] / М. Давлетханов // Р Контроль системи безопасности. Режим доступу: http://www.r-control.ru/articles/8/

20. Аппаратная реализация методов идентификации по отпечаткам пальцев [Електронний ресурс] / О. Никулин // Специальная Техника. – 1999 г. – №3. Режим доступу: http://ess.ru/publications/articles/nikulin/nikulin.htm.

21. Патент 67772 України МПК 7G06K9/20, A61B5 / 117. Спосіб та пристрій для ідентифікації особи шляхом безконтактного розпізнавання ліній руки і пальців / Хауке Рудольф, DE, Айнігхаммер Хайнс Й., DE, Айнігхаммер Йєнс, DE., заявник і патентовласник – ТСТ-ТАЧЛЕСС СЕНСОР ТЕКНОЛОДЖИ СЕЙЛЗ ЕНД МАРКЕТІНГ АГ, CH – опубл. 15.07.2004, Бюл. №7, 2004 р.

22. Современные технологии идентификации личности по отпечатку пальца с использованием емкостных датчиков [Електронний ресурс] / Г. Рябов // Radioradar. Режим доступу: http://www.radioradar.net/articles/scientific_technical/identif_otpech.html.

Bilinsky Yosif – Dr. Sc. (Eng), Prof., head of department of electronics.

Yukish Maryna – Cand. Sc. (Eng), Department of theoretical electric engineering and electric measurements .

Pavliuk Oleksandr – Student.
Vinnytsya National Technical University.