UDK 004.056.5

Yakubov J.S.
magistrant
Muhammad al-Xorazmiy nomidagi Toshkent
axborot texnologiyalari universiteti
Toshkent, O‘zbekiston

BIOMETRIK TIZIMLARNING XAVFSIZLIGI

Annotatsiya: Ushbu maqolada odamlarni identifikatsiya qilish uchun odatda ishlatiladigan biometrik tizimlarning ishonchliligi tasvirlangan. Maqolada biometrik tizimlarning xavfsizligini buzish usullari tahlil qilinadi. Shuningdek, barmoq izi sensorlarining ishonchliligini tekshirish jarayoni ko’rib chiqildi.

Kalit so’zlar: Biometrik sensor, identifikatsiyalash texnologiyalari, aloqa interfeysi, funksiya, ma’lumotlar xavfsizligi, ishonchlilik.

Yakubov J.S.
student of master’s degree
Tashkent University of Information Technologies named
after Muhammad al-Khwarizmi
Tashkent, Uzbekistan

SECURITY OF BIOMETRIC SYSTEMS

Abstract: This article describes the reliability of biometric systems commonly used to identify people. The article analyzes the ways of hacking biometric systems. The process of verifying the reliability of fingerprint sensors was also discussed.

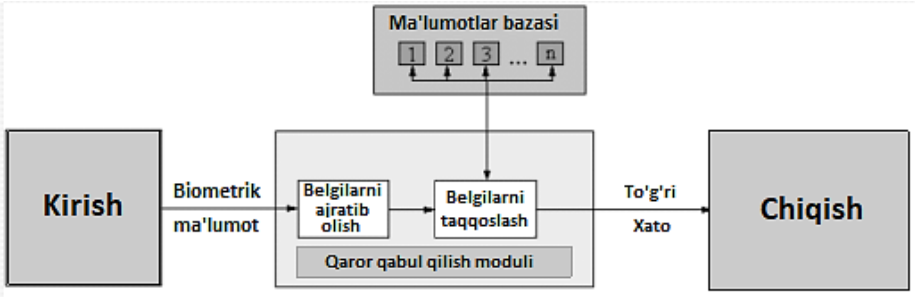
Keywords: Biometric sensor, identification technology, communication interface, function, data security, reliability.

Kirish. Biometrik sensor – bu odamning biometrik ma’lumotlarini elektr signaliga aylantiradigan o’zgartirgich. Biometrik ma’lumotlarga, asosan biometrik sensor tomonidan o‘qiladigan barmoq izlari, ko‘z qobig‘i, yuz, ovoz

va boshqalar kiradi. Hozirgi vaqtda nafaqat odamlar, ob’yektlar va ma’lumotlar xavfsizligini, balki shaxslarni identifikatsiyalashning ishonchliligini oshirishga bo‘lgan talab ortib bormoqda. Biometrik identifikatsiyalash shaxsiy identifikatsiyalashning ishonchliligini oshirishga yordam beradi.

Biometrik identifikatsiyalashning foydalanish sohalariga kriminalistika, turizm (bojxona rasmiylashtiruvi va pasport nazorati), odamlar harakatini nazorat qilish (antiterror tadbirlari, olomonni kuzatish), davomat va kirish tizimlari, ma’lumotlarni himoya qilish (shaxsiy kompyuter va boshqa ma’lumotlar manbalari), elektron bank xizmatlari, onlayn to‘lovlar va boshqa ko‘p sohalar kiradi [1].

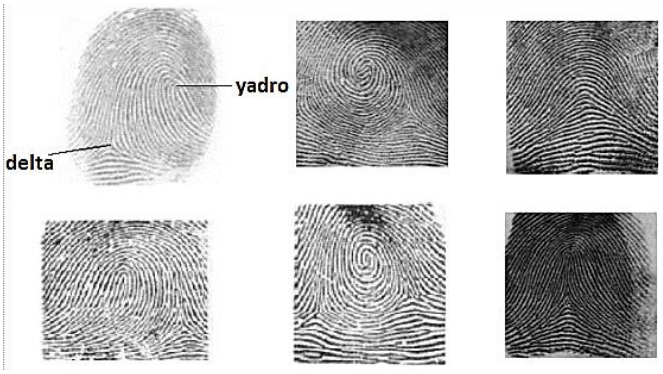
Biometrik identifikatsiya tizimining umumiy tuzilishi 1-rasmda keltirilgan.



1-rasm. Biometrik identifikatsiyalash tizimining tuzilishi [2].

Barmoq izlaridan foydalanib kirishni boshqarish tizimlari. Barmoq izlaridan foydalanib kirishni boshqarish tizimidan barmoq izlarini o‘qiydigan, foydalanishiga ruxsat berishni istagan har bir kishiga kirishga ruxsatni amalga oshirish uchun foydalaniladi. Keyin, ular barmoq izlarini o‘qiydigan sensorga, eshik oldida o‘z barmog‘ini tekkizganda, bu barmoq belgilari ma’lumotlar bazasida saqlangan shablon bilan taqqoslanadi. Agar mos keladigan bo‘lsa, ularga kirish huquqi beriladi. Barmoq izlarini olish eng mashhur biometrik identifikatsiyalash usullaridan biridir. Odatda kriminologiyada qo’llaniladigan barmoq izlari bugungi kunda tijorat xavfsizligida keng qo‘llaniladi. Ushbu usul barmoqlar chiziqlarining yo‘nalishli chizmalarini aniqlashga asoslangan

(papillyar chiziqlar). Papillyar chiziqlarini tasniflash uchun uchta asosiy sxema mavjud, ular 2-rasmda keltirilgan.



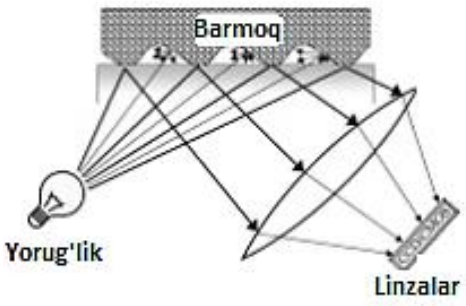
2-rasm. Asosiy ko‘rinishlar (chap halqasimon, spiralsimon, yoysimon) [2].

1. Halqasimon - papillyar chiziqlar halqa shaklida. Barmoq izlarining taxminan 65 foizini halqa tashkil qiladi.

2. Spiralsimon - papillyar chiziqlar aylana, oval, yadroli spiral shakllarida. Spiral shakllari barcha barmoq izlarining taxminan 25% ni tashkil qiladi.

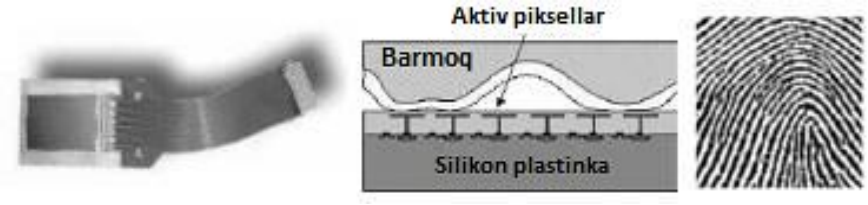
3. Yoysimon - papillyar chiziqlar oddiy yoy shaklida. Bu ko‘rinish minimal hisoblanib, barmoq izlarining taxminan 5-10 foizlarida uchratish mumkin.

Barmoq izi datchiklarining turlari va ishlash prinsipi. Optik barmoq izlari sensori. Optik barmoq izlari sensorlari akslantirish yoki yorug’lik o’tkazuvchanligiga asoslangan. Ushbu sensorlar liniya chiziqlaridan yorug‘likning turli xil akslarini va shu chiziqlar orasidagi bo‘shliqni ishlatadi. Akslangan yorug‘lik CCD (Charge-Coupled Device) yoki CMOS (Complementary Metal Oxide Semiconductor) sensori yordamida baholanadi.



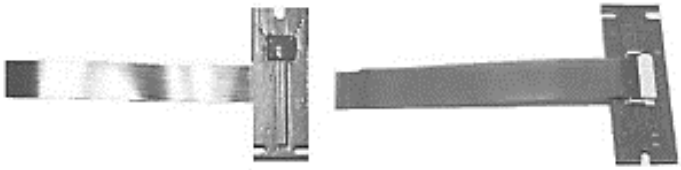
3-rasm. Akslanish prinsipiga asoslangan optik sensor [2].

Sig’imli barmoq izlari sensori. Ushbu sensorning ishlash prinsipi sensor plastinkasi va barmoq o’rtasidagi sig’imning farqini o’lchashga asoslangan. Sensor zonasi barmoq ichidagi balandlik va chuqurliklar orasida sig’imdagi farqni baholash uchun juda ko‘p sonli mikroelektrodlar bilan jihozlangan.



4-rasm. Sig’imli sensorning ishlash prinsipi [3].

Haroratli barmoq izlari sensori. Haroratli barmoq izlari sensorlarida issiqlik sensori sifatida kichik pirodetektor ishlatiladi. Ushbu texnologiyaning ishlash prinsipi barmoq ustidagi papillyar chiziqlar balandligi va pastligi o‘rtasidagi harorat farqini o‘lchashga asoslangan.



5-rasm. Haroratli barmoq izlari sensorining ko‘rinishi [4].

Barmoq izi sensorining ishonchliligini tekshirish. Barmoq izi sensorlarining ishonchliligini tekshirish uchun ikkita asosiy funksiya mavjud. FAR (False Accepted Reads) deb nomlangan birinchi funksiya – yolg‘on qabul qilingan o’qishlar soni. Ushbu funksiyani quyidagicha aniqlash mumkin:

$$FAR = \frac{N_{FR}}{N_{EIA(EVA)}} \cdot 100\ [\%] \qquad (1)$$

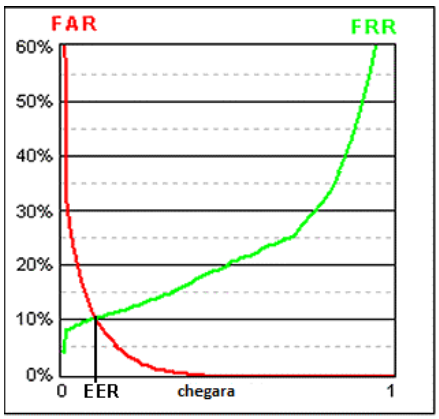
bu yerda, N_{FR} – yolg‘on rad etishlar soni; N_{EIA} – belgilarni aniqlashga urinishlar soni; N_{EVA} – barcha tekshiruv urinishlaridan foydalanganlar soni.

Ikkinchi FRR (False Rejected Reads) funksiyasi – yolg‘on rad etilgan o’qishlar soni. Ushbu funksiyani quyidagicha aniqlash mumkin:

$$FRR = \frac{N_{FA}}{N_{IIA(IVA)}} \cdot 100\ [\%] \qquad (2)$$

bu yerda, N_{FA} – ruxsatsiz qabul qilishlar soni; N_{IIA} – ruxsatsiz shaxslarni aniqlashga urinishlari soni; N_{IVA} – ruxsatsiz shaxslar tomonidan tekshirishga urinishlar soni.

FAR va FFR funksiyalari o'rtasidagi munosabatlar quyidagi rasmda keltirilgan. EER (Equal Error Rate) nuqtasi - teng xato darajasi - bu FAR va FRR bir xil qiymatga ega bo'lgan nuqta. Ushbu o'tish biometrik qurilmalarning umumiy ko'rsatkichlarining yaxshi ko'rsatkichidir. O'tish kamroq bo'lishi, biometrik qurilmaning EER ko'rsatkichlari yaxshilanishini anglatadi [5].



7-rasm. FAR va FFR funksiyalari o'rtasidagi munosabatlar [3].

Xulosa. Shunday qilib, xulosa qilishimiz mumkinki, biometrik texnologiyalarni joriy etish, umuman, tizimni boshqarishni, uning xavfsizlik tizimini rivojlantirishga yordam beradi. Maxfiy ma'lumotlarga yoki ob'yektga kirishda shaxsiy identifikatsiyalash muammosi ham doim dolzarb bo'lib kelgan.

Foydalanilgan adabiyotlar:

[1] O. Bitto, Encryption and biometrics: or arcane bits and touches.: Computer Media, 2005. ISBN 80-86686-48-5.

[2] R. Rak, Biometrics and identity of people: the forensic and commercial applications, BEN, Prague, 2008. ISBN 978-80-247-2365-5.

[3] Fingerprint structure imaging based on an ultrasound camera [online]. 2012 [cit. 2012-06-23]. <http://www.optel.pl/article/english/article.htm>.

[4] T. Coufal, What is FingerChip [online]. 2007 [cit. 2012-04-29]. <http://hw.cz/teorie-praxe/art2020-co-je-fingerchip.html>.

[5] M.Adamek, M.Matysek, P.Neumann. Security of Biometric Systems. 25th DAAAM International Symposium on Intelligent Manufacturing and Automation, DAAAM, 2014. Available online at <www.sciencedirect.com>.