

MAXKAMOV Anvarjon Abdujabborovich
O'zbekiston xalqaro islom akademiyasi
Zamonaviy axborot-kommunikatsiya
texnologiyalari kafedrası dotsenti, PhD

JUMAYEV Turdali Saminjonovich
O'zbekiston xalqaro islom akademiyasi
Zamonaviy axborot-kommunikatsiya
texnologiyalari kafedrası dotsenti, PhD

АХБОРОТ ХАВФСИЗЛИГИ ТА'МИНЛОВЧИ BIOMETRIK TIZIMLARNING QIYOSIY TAHLILI

СРАВНИТЕЛЬНЫЙ АНАЛИЗ БИОМЕТРИЧЕСКИХ СИСТЕМ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

COMPARATIVE ANALYSIS OF BIOMETRIC SYSTEMS ENSURING INFORMATION SECURITY

Annotatsiya. Ushbu maqolada biometrik tizimlar va ular ustida olib borilgan ilmiy yondashuvlar natijasida ularni axborot xavfsizligini ta'minlashdagi qiyosiy tahlillar ko'rib chiqilgan. Hozirga kelib biometrik texnologiyalar asosida yaratilgan tizimlar turli tijorat sohalari, davlat tashkilotlari xavfsizlik texnikaviy dasturlarida qo'llanilayotganligi sababli, qaysi biometrik texnologiyalar asosida yaratilgan tizimlar xavfsizlikni ta'minlashda eng samarali ekanligini aniqlash amalga oshirilgan. Biometrik texnologiyalarni axborot xavfsizligini ta'minlashdagi samarali tanib olish usullari, mezonlari, ma'lumotlarni soxtalashtirishga qarshilik darajasi, kuchli autentifikatsiya, tizimlarni biometrik xarakteristikalar, autentifikatsiya tezligi, moliyaviy darajalari bo'yicha taqqoslandi hamda O'zbekiston Respublikasida mavjudlari tahlil qilindi.

Kalit so'zlar: biometrik identifikatsiya, statik va dinamik identifikatsiya, soxtalashtirishga qarshilik ko'rsatish, kuchli autentifikatsiya, o'zgarmas biometrik xarakteristikalar; autentifikatsiya tezligi, xarajatlarni taqqoslash.

Аннотация. В данной статье рассмотрен сравнительный анализ биометрических систем и их информационной безопасности в результате проведенных к ним научных подходов. В связи с тем, что системы, созданные на основе биометрических

технологий, используются в технических программах безопасности различных коммерческих секторов и государственных организаций, определено, какие системы, созданные на основе биометрических технологий, являются наиболее эффективными в обеспечении безопасности. Сравнены и проанализированы доступные в Республике Узбекистан методы эффективного распознавания биометрических технологий в обеспечении информационной безопасности, критерии, уровень устойчивости к фальсификации данных, строгая аутентификация, биометрические характеристики систем, скорость аутентификации, финансовые уровни.

Ключевые слова: биометрическая идентификация, статические и динамические методы идентификации, устойчивость к подделке, строгая аутентификация, неизменные биометрические характеристики, скорость аутентификации, сравнение затрат.

Abstract. In this article, a comparative analysis of biometric systems and their information security as a result of the scientific approaches conducted on them is considered. Due to the fact that systems created on the basis of biometric technologies are used in security technical programs of various commercial sectors and state organizations, it was determined which systems created on the basis of biometric technologies are the most effective in ensuring security. Methods of effective recognition of biometric technologies in ensuring information security, criteria, level of resistance to falsification of data, strong authentication, biometric characteristics of systems, authentication speed, financial levels were compared and those available in the Republic of Uzbekistan were analyzed.

Keywords: biometric identification, static and dynamic identification methods, counterfeit resistance, strong authentication, invariable biometric characteristics, authentication speed, cost comparison.

KIRISH

Biometrik identifikatsiya bu foydalanuvchi tomonidan o'zining noyob biometrik parametrlarini taqdim etish va uni mavjud ma'lumotlarning butun ma'lumotlar bazasi bilan taqqoslash jarayoni hisoblanadi. Biometrik tanib olishni amalga oshirish uchun birinchi navbatda ma'lumotlar bazasi tashkil etiladi hamda yangi kiritilayotgan obyekt taqqoslash amalga oshiriladi. Biometrik ruxsatni boshqarish tizimlari foydalanuvchilar uchun qulay hisoblanadi. Chunki axborot tashuvchilar doimo ular bilan birga bo'lib, ularni yo'qotish yoki o'g'irlash mumkin emas.

ASOSIY QISM

Biometrik identifikatsiyalash texnologiyalari. Biometrik identifikatsiya qilish usullarini ikki turga ya'ni statik va dinamik turga bo'linadi.

Statik – insonning butun hayoti davomida u bilan birga bo'lgan fiziologik xususiyatlariga asoslangan. Ularning ayrimlari haqida qisqacha ma'lumot berib o'tiladi:

- Barmoq izi;
- Yuz tasviri;
- Ko'zning rangdor pardasi;
- Qo'l geometriyasi;
- DNK identifikatsiyasi;
- Quloq chanog'i tasviri;

Dinamik – odamlarning xulq-atvor xususiyatlariga, ya'ni oddiy harakatni takrorlash jarayonida ongsiz harakatlarga asoslangan. Ular:

- Ovoz signallari;
- Qo'l yozuvi (kaft);
- Klaviatura qo'l yozuvi bo'yicha aniqlash va boshqalar.

Xulq-atvor biometrikasining ustuvor turlaridan biri bu klaviaturada yozish usulidir. U aniqlanganda, yozish tezligi, tugmachalarga bosim, tugmachani bosish davomiyligi va tugmachalarni bosish orasidagi vaqt oralig'i qayd etiladi. Alohida biometrik omil sichqonchani ishlatish usuli bo'lishi mumkin. Bundan tashqari, xulq-atvor biometrikasi kompyuter bilan bog'liq bo'lmagan ko'plab omillarni qamrab oladi.

Shuningdek, kirishni boshqarish tizimlarining ishonchliligi va xavfsizligi uchun eng qat'iy talablarni qondirish uchun bir nechta biometrik xususiyatlardan foydalanadigan birlashtirilgan identifikatsiya tizimlari mavjud.

Biometrik identifikatsiya mezonlari.

Biometrik identifikatsiyaga asoslangan kirishni boshqarish tizimining samaradorligini aniqlash uchun quyidagi ko'rsatkichlar qo'llaniladi:

- FAR – noto'g'ri o'tish tezligi;
- FMR - tizim kiritilgan namunani ma'lumotlar bazasidagi mos kelmaydigan tasvir bilan noto'g'ri solishtirish ehtimoli.
- FRR - noto'g'ri rad etish darajasi;
- FNMR - tizimning ma'lumotlar bazasidan kirish sxemasi va mos keladigan naqsh o'rtasidagi moslikni aniqlashda xato qilish ehtimoli;
- ROC syujeti - FAR va FRR ko'rsatkichlari o'rtasidagi kelishuvni vizualizatsiya qilish;

- Ro'yxatga olishni rad etish darajasi (FTE yoki FER) - kiritilgan ma'lumotlardan shablonni yaratishga muvaffaqiyatsiz urinishlar darajasi (ikkinchisining past sifati bilan);

- Erronous Retention Rate (FTR) - avtomatlashtirilgan tizim biometrik ma'lumotlarni to'g'ri taqdim etilganda aniqlay olmasligi ehtimoli;

- Shablon sig'imi - bu tizimda saqlanishi mumkin bo'lgan ma'lumotlar to'plamining maksimal soni.

Biometrik identifikatsiyaning asosiy usullarini qiyosiy tahlil qilish. Matematik statistika yordamida biometrik autentifikatsiya usullarini solishtirish (FAR va FRR) bilan tanishamiz. Har qanday biometrik tizimni baholashning asosiy parametrlari ikkita parametrdir:

- FAR (False Acceptance Rate) - noto'g'ri o'tish darajasi, ya'ni tizimda ro'yxatdan o'tmagan foydalanuvchiga kirishga ruxsat bergan holatlarning aniqlangan foizi.

- FRR (False Rejection Rate) - noto'g'ri rad etish darajasi, ya'ni tizimning haqiqiy foydalanuvchisiga kirishni rad etish.

Ikkala xususiyat ham matematik statistika usullariga asoslangan hisoblash yo'li bilan olinadi. Bu ko'rsatkichlar qanchalik past bo'lsa, ob'ektni aniqlash qanchalik aniq bo'ladi.

Bugungi kunda eng mashhur biometrik identifikatsiya usullari uchun o'rtacha FAR va FRR qiymatlari quyidagicha:

Biometrik ACS quyidagi-lardan foydalanadi:	FAR	FRR
Barmoq izi	0,001%	0,6%
2D yuzni aniqlash	0,1%	2,5%
3D yuzni aniqlash	0,0005%	0,1%
Iris	0,00001%	0,016%
Retina	0,0001%	0,4%
Tomirlarni chizish	0,0008%	0,01%

Ammo mukammal FAR va FRR ko'rsatkichlari kirishni boshqarishning samarali tizimini yaratish uchun yetarli emas. Masalan, DNK tahliliga asoslangan ACSni tasavvur qilish qiyin, garchi ushbu autentifikatsiya usuli bilan ko'rsatilgan koeffitsientlar nolga teng bo'lgan holda ham. Ammo identifikatsiya vaqti o'sib bormoqda, inson omilining ta'siri kuchaymoqda, tizimning narxi asossiz ravishda oshib bormoqda.

Ma'lumotlarni soxtalashtirishga qarshilik ko'rsatishning biometrik usullarini taqqoslash.

Biometrik ma'lumotlarni soxtalashtirish har qanday holatda ham juda murakkab jarayon bo'lib, ko'pincha maxsus tayyorgarlik va texnik yordamni talab qiladi. Ammo agar siz uyda barmoq izini soxtalashtirishingiz mumkin bo'lsa, unda Irisni muvaffaqiyatli soxtalashtirish haqida hali ma'lum emas. Biometrik retinal autentifikatsiya tizimlari uchun soxtasini yaratish mumkin emas.

Biometrik ACS quyidagilardan foydalanadi:	Soxtalashtirish
Barmoq izi	Mumkin
2D yuzni aniqlash	Mumkin
3D yuzni aniqlash	Muammoli
Iris	Muvaffaqiyatsiz
Retina	Mumkin emas
Tomirlarni chizish	Mumkin emas

Kuchli autentifikatsiya qilish imkoniyati uchun biometrik usullarni taqqoslash. Biometrik kirishni boshqarish tizimining xavfsizlik darajasini oshirish, qoida tariqasida, dasturiy va apparat usullari bilan erishiladi. Masalan, tazyiqlar uchun "jonli barmoq" texnologiyalari, ko'zlar uchun beihitoyor titroqlarni tahlil qilish. Xavfsizlik darajasini oshirish uchun biometrik usul ko'p faktorli autentifikatsiya tizimining tarkibiy qismlaridan biri bo'lishi mumkin.

Dasturiy ta'minot va apparat majmuasiga qo'shimcha himoya vositalarini kiritish odatda uning narhini sezilarli darajada oshiradi. Biroq, ba'zi usullar uchun standart komponentlar asosida kuchli autentifikatsiya qilish mumkin: foydalanuvchi identifikatsiyasi uchun bir nechta shablonlardan foydalanishi mumkin (masalan, bir nechta barmoq izlari).

Biometrik ACS quyidagilar-dan foydalanadi:	Kuchli autentifikatsiya (bir omil)
Barmoq izi	Mumkin
2D yuzni aniqlash	Yo'q
3D yuzni aniqlash	Yo'q
Iris	Mumkin
Retina	Mumkin
Tomirlarni chizish	Mumkin

O'zgaras biometrik xarakteristikalar uchun autentifikatsiya usullarini solishtirish. Vaqt o'tishi bilan biometrik xarakteristikaning o'zgarasligi ham shartli tushunchadir: barcha biometrik parametrlar tibbiy operatsiya yoki

shikastlanish natijasida o'zgarishi mumkin. Ammo agar foydalanuvchini barmoq izi bilan tekshirishni qiyinlashtiradigan oddiy uy kesish odatiy hol bo'lsa, unda ko'zning rangdor pardasini o'zgartiradigan operatsiya kamdan-kam uchraydi.

Biometrik ACS quyidagilardan foydalanadi:	Xususiyatning o'zgarasligi
Barmoq izi	Past
2D yuzni aniqlash	Past
3D yuzni aniqlash	Yuqori
Iris	Yuqori
Retina	O'rtacha
Tomirlarni chizish	O'rtacha

Tashqi omillarga sezuvchanlikni solishtirish. Atrof-muhit parametrlarining ACS samaradorligiga ta'siri uskunalar ishlab chiqaruvchisi tomonidan amalga oshirilgan algoritmlar va operatsion texnologiyalarga bog'liq va hatto bitta biometrik usul doirasida ham sezilarli darajada farq qilishi mumkin. Bunday farqlarning yorqin misoli, odatda, tashqi omillarga nisbatan sezgir bo'lgan barmoq izlarini o'qish qurilmalaridir.

Agar biometrik identifikatsiyaning boshqa usullarini solishtiradigan bo'lsak, 2D yuzni aniqlash eng sezgir bo'ladi: ko'zoynak, shlyapa, yangi soch turmugi yoki o'sgan soqolning mavjudligi juda muhim bo'lishi mumkin. Retinal autentifikatsiya usulidan foydalanadigan tizimlar skanerga nisbatan ancha qattiq ko'z holatini, foydalanuvchining harakatsizligini va ko'zning o'ziga qaratilishini talab qiladi.

Tomirlar va ko'zning irisini naqshiga asoslangan foydalanuvchini identifikatsiyalash usullari, agar siz ularni ekstremal ish sharoitida ishlatishga harakat qilmasangiz nisbatan barqaror ishlaydi.

Uch o'lchovli yuzni aniqlash tashqi omillar ta'siriga nisbatan eng kam sezgir bo'ladi. Bunday ACS ning ishlashiga ta'sir qilishi mumkin bo'lgan yagona parametr - bu haddan tashqari yorug'lik.

Biometrik ACS quyidagilar-dan foydalanadi:	Tashqi omillarga sezgirlik
Barmoq izi	Yuqori
2D yuzni aniqlash	Yuqori
3D yuzni aniqlash	Past
Iris	O'rtacha
Retina	Yuqori
Tomirlarni chizish	O'rtacha

Autentifikatsiya tezligini taqqoslash.

Autentifikatsiya tezligi ma'lumotlarni yig'ish vaqtiga, shablonning o'lchamiga va uni qayta ishlash uchun ajratilgan resurslar miqdoriga va ma'lum bir biometrik usulni amalga oshirish uchun ishlatiladigan asosiy dasturiy ta'minot algoritmlariga bog'liq bo'ladi.

Biometrik ACS quyidagilardan foydalanadi:	Autentifikatsiya tezligi
Barmoq izi	Yuqori
2D yuzni aniqlash	O'rtacha
3D yuzni aniqlash	Past
Iris	Yuqori
Retina	Past
Tomirlarni chizish	Yuqori

Foydalanuvchining psixologik qulayligi uchun biometrik usullarni taqqoslash. Axborot xavfsizlik tizimini tanlashda foydalanuvchilarning psixologik qulayligi ham juda mos ko'rsatkichdir. Agar ikki o'lchovli yuz yoki iris tanib olish holatida u sezilmaydigan tarzda sodir bo'lsa, ko'zning rangdor to'r pardasini skanerlash juda yoqimsiz jarayondir. Barmoq izini autentifikatsiya qilish, garchi yoqimsiz bo'lsa ham, sud-tibbiyot usullari bilan salbiy bog'lanishga olib kelishi mumkin.

Biometrik ACS quyidagilardan foydalanadi:	Foydalanuvchining qulayligi
Barmoq izi	O'rtacha
2D yuzni aniqlash	Yuqori
3D yuzni aniqlash	O'rtacha
Iris	Yuqori
Retina	Qisqa
Tomirlarni chizish	O'rtacha

ACSda biometrik usullarni joriy qilish xarajatlarini taqqoslash. Amaldagi biometrik autentifikatsiyalash usullariga qarab kirishni nazorat qilish va hisobga olish tizimlarining narxi bir-biridan juda farq qiladi. Shu bilan birga, farq tizimning maqsadi, ishlab chiqarish texnologiyalari, ruxsatsiz kirishdan himoyani oshirish usullari va boshqalarga qarab bitta usulda aniq bo'lishi mumkin.

Biometrik ACS quyidagilardan foydalanadi:	Narxi
Barmoq izi	Past
2D yuzni aniqlash	O'rtacha
3D yuzni aniqlash	Yuqori
Iris	Yuqori
Retina	Yuqori
Tomirlarni chizish	O'rtacha

O'zbekiston Respublikasida biometrik autentifikatsiyalash usullarining mavjudligini taqqoslash. U yoki bu biometrik autentifikatsiya usulidan foydalangan holda kirishni boshqarish tizimlarining mavjudligi ularning umumiy tarqalishiga bog'liq bo'ladi. O'zbekiston bozorining o'ziga xosligi o'z cheklovlarini qo'yadi. Qiyin iqtisodiy muhitni hisobga olgan holda, narx birinchi o'ringa chiqadi. Bundan tashqari, O'zbekiston uchun nafaqat turli usullarini qo'llash xarajatlarini qiyosiy baholash, balki biometrik autentifikatsiya qilish uchun ko'rsatilgan usullardan foydalanadigan mahalliy ishlab chiqarilgan uskunalarning mavjudligi ham rol o'ynaydi. Avvalo, o'zi ishlab chiqaruvchilarimizning kattalik buyurtmasi bo'yicha mavjudligi uskunaning narxini pasaytiradi.

Barmoq izini aniqlashda hozirda davlatimiz miqyosida hech qanday muammo yo'q va ilmiy yondashuv natijasida quyidagicha xulosaga kelindi:

- import qilingan va milliy jihozlarning keng assortimenti iste'molchiga taqdim etiladi.
- arzonroq, mijozlar va montajchilar orasida mashhurdir.
- ko'p faktorli autentifikatsiya tizimlarini amalga oshirish uchun qulay.

Ikki o'lchovli yuzni autentifikatsiya qilish tizimini yaratish uchun etarli darajada samarali emas. Aksincha, bu usul video-tahlil vazifalari uchun yoki ko'p faktorli autentifikatsiya tizimlarining tarkibiy qismlaridan biri sifatida ishlatiladi. 3D autentifikatsiya qilish qimmat, hatto biometrik autentifikatsiyalash usullarini oddiy taqqoslaganda ham.

Irisni autentifikatsiyalash usuli ko'p yillar davomida eng istiqbolli va samarali usullardan biri hisoblanadi va uning jahon bozoridagi ulushi, albatta, ortib bormoqda. Shu bilan birga, yuqori narx va texnologiya patentlari bilan bog'liq qiyin vaziyat ham jahon sahnasida cheklovchi omillardir.

Biometrik ACS quyidagi-lardan foydalanadi:	O'zbekiston bozorida mavjudligi
Barmoq izi	Yuqori
2D yuzni aniqlash	O'rtacha
3D yuzni aniqlash	O'rtacha
Iris	Past
Tomirlarni chizish	Past
Quloq chanog'i	Past

Xulosa

Hozirgi kunda har bir tashkilot va korhonalarga kirish tizimlarini nazorat qilishda biometrik tanib olish usullaridan foydalangan holda tanib olish amalga oshiriladi. Ammo tanib olish biometrik tanib olishning turli hillarida tanib olishni amalga oshirish ko'p rivojlanmagan. Masalan, shaxsni quloq chanog'i asosida tanib olish unchalik rivojlanmagan. Bularni rivojlantirilsa biometrik tanib olish tizimlari ko'paytirilsa maqsadga muvofiq bo'lar edi.

FOYDALANILGAN ADABIYOTLAR

1. Anil k. Jain, fellow, IEEE, Arun Ross, member, IEEE, "Biometrics: A Tool for information security" IEEE Transactions on information forensics and security. VOL.1.No.2.June 2006.
2. AES Encryption Information. <http://www.bitzipper.com/aes-encryption.html>.
3. Advanced encryption standard. http://en.wikipedia.org/wiki/Advanced_encryption_standerd
4. Biometrics and Biostatistics. <http://www.omicsonline.org/jbmbshome.php>
5. Biometrics for network security Paul Reid, 2004 by pearson education.
6. Alfredo c.lopez, Ricardo R. lobez "fingerprint rscognition".
7. Jammi Ashok, vaka shivashankar, "An overview of biometrics".(IJCSE)International journal an computer science and Engineering.VOL.02.no.07 ,2010.
8. Ramen V.Ramen, V.yampoolskiy, biometrics: a survey and classification. Int. J. Biometrics, vol.1.1, no.1,2008.
9. Chitresh Saraswat, An efficient automatic Attendance System using Fingerprint Verification Technique, IJCSE, Vol.02.No. 02, 2010, 264-269.
10. Anil k.Jain, Arun Ross, "An introduction to biometrics recognition", IEEE transactions Vol.14, Issue 1, Jan 2004.
11. L.O'Gorman, "Overview of fingerprint verification technologies," Elsevier Information security technical Report, Vol.3, No.1.,1998.
12. "Guide to fingerprint recognition" <http://www.digitalpersona.com>
13. Hand book fingerprint recognition, D. Maltoni, A.K.Jain, Springer 2009. <http://bias.csr.unibo.it/maltoni/handbook/>
14. W. Stallings, cryptography and network security: principles, 3rd ed.
15. Klein D.V. Foiling the cracker: a survey of, and improvements to password security // 2nd USENIX Workshop security, 1990.
16. Fingerprint Database (FVC2002). <http://bias.csr.unibo.it>.