BIOMETRIK AUTENTIFIKATSIYA VA IDENTIFIKATSIYA TIZIMLARINI ISHLAB CHIQISH HAMDA BIOMETRIK IDENTIFIKATSIYA MEZONLARI

Xusenov Murodjon Zoxirovich *(Buxoro davlat universiteti, e-mail: m.z.xusenov@buxdu.uz, ORCID: 0000-0002-1533-3102)*

Annotatsiya: Maqolada kirishni boshqarish va nazorat qilish tizimlarida biometrik autentifikatsiya texnologiyalarini yaratish va qo‘llash usullari hamda maqsadlari muhokama qilingan. Shaxsning statik va dinamik, fiziologik xususiyatlariga asoslangan zamonaviy biometrik autentifikatsiya vositalarining tasnifi, shuningdek, ularni amalga oshirishning fizik tamoyillari va ularni qo‘llash samaradorligini statistik baholash keltirilgan.

Kalit so‘zlar: biometriya, identifikatsiya, autentifikatsiya, biometrik usullar, kirishni boshqarish va nazorat qilish tizimi, ko‘zning shox pardasi, to‘r pardasi, termal yuz tasviri, barmoq izlari, qo‘l geometriyasi, DNK, yozuv va imzo dinamikasi, ovoz va nutq xususiyatlari, klaviaturada ishlash ritmi.

Kirish: Biometrika — bu insonning jismoniy yoki xulq-atvor xususiyatlarini tavsiflovchi texnik atama. Biometrik autentifikatsiya ma’lumotlar xavfsizligi tushunchasidir. Biometrik autentifikatsiya yechimlari shaxsni ifodalovchi ma’lumotlarga asoslangan modelni yaratadi. Ushbu model va biometrik ma’lumotlar bilan xavfsizlik tizimlari ilovalar va boshqa tarmoq resurslariga kirishni autentifikatsiya qilishi mumkin. Biometrik autentifikatsiya tez sur’atlar bilan ko‘r faktorli autentifikatsiya strategiyalarining mashhur komponentiga aylanmoqda, chunki u kuchli autentifikatsiya muammosini foydalanuvchilarga qulay foydalanuvchi interfeysi bilan birlashtiradi.

Asosiy qism: Biometrik autentifikatsiya — bu o‘z shaxsini tasdiqlovchi shaxs haqiqatan ham o‘zini kim ekanligini tasdiqlash jarayonidir. Bu foydalanuvchi tomonidan taqdim etilgan biometrik ma’lumotlarni tizimda allaqachon saqlangan ma’lumotlar bilan taqqoslash orqali sodir bo‘ladi. Agar ma’lumotlar bir xil bo‘lsa, u holda shaxs autentifikatsiya qilinadi.

Biometrik identifikatsiya — bu barmoq izlari, ko‘z qorachig‘i, ovoz, yuz, yurak urish tezligi va boshqalar kabi noyob biometrik xususiyatlariga asoslanib, shaxsning kimligini aniqlash jarayoni hisoblanadi.

Shunday qilib, biometrik identifikatsiya shaxsni aniqlaydi va biometrik autentifikatsiya tasdiqlangan shaxsning haqiqiyligini tekshiradi. Ushbu ikkala texnologiya turli sohalarda, jumladan, kompyuter va binolarga kirish, kirishni boshqarish, bank, davlat xizmatlari va boshqalarda qo‘llaniladi.

Avtomatlashtirilgan biometrik autentifikatsiya tizimlari autentifikatsiya qilish uchun foydalanadigan biometrik xususiyat turiga va biometrik zondlash va tanib olish uchun ishlatiladigan texnologiyaga qarab tasniflanishi mumkin. Bu yerda bir nechta umumiy toifalar:

1. Barmoq izini aniqlash tizimlari: Barmoq izini aniqlash tizimlari biometrik texnologiyaning bir turi bo‘lib, odamlarni noyob barmoq izlari asosida identifikatsiya qiladi. Ushbu tizimlar rasmni olish yoki odamning barmoq izlarini skanerlash, so‘ngra bu tasvirni shaxsni aniqlash uchun ma’lum barmoq izlari bazasi bilan solishtirish orqali ishlaydi. Barmoq izini aniqlash tizimlari odatda smartfonlar qulfini ochish, xavfsiz binolarga kirish va huquqni muhofaza qilish maqsadlarida shaxslarni aniqlash kabi xavfsizlik maqsadlarida qo‘llaniladi. Ular biometrik identifikatsiyaning ishonchli va aniq shakli hisoblanadi va dunyo bo‘ylab turli ilovalarda keng qo‘llaniladi.

2. Yuzni tanish tizimlari: Yuzni tanish tizimlari biometrik texnologiya turi bo‘lib, odamlarni yuz xususiyatlariga qarab identifikatsiya qiladi. Ushbu tizimlar odamning yuzi tasvirini yoki videosini olish va ko‘zlar orasidagi masofa, burun shakli va yuz konturi kabi turli xil ma’lumotlarni tahlil qilish orqali ishlaydi. Keyin tizim ushbu ma’lumotni shaxsni aniqlash uchun ma’lum yuzlar bazasi bilan taqqoslaydi. Yuzni tanib olish tizimlari odatda jamoat joylarida tahdidlarni kuzatish, jinoiy tergovda gumonlanuvchilarni aniqlash va xavfsiz joylarga kirishni boshqarish kabi xavfsizlik maqsadlarida qo‘llaniladi. Ular biometrik identifikatsiyaning ishonchli va aniq shakli hisoblanadi, biroq maxfiylik va texnologiyadan noto‘g‘ri foydalanish borasida xavotirlar mavjud.

3. Ko‘z qorachig‘i aniqlash tizimlari: Bu tizimlar aniqlash tizimlari biometrik texnologiya turi bo‘lib, odamlarni aniqlash uchun ko‘z qorachig‘ini aniqlashdan foydalanadi. Ushbu texnologiya kamera yordamida odamning ko‘z qorachig‘idagi noyob naqshlarning tasvirini olish uchun ishlatiladi, keyinchalik ular tahlil qilinadi va ma’lum bo‘lgan ko‘z qorachig‘i naqshlarining ma’lumotlar bazasi bilan taqqoslanadi. Ko‘z qorachig‘ini aniqlash tizimlari huquqni muhofaza qilish, chegara nazorati va xavfsiz obyektlarga kirishni nazorat qilish kabi xavfsizlik dasturlari uchun tobora ommalashib bormoqda. Ular, shuningdek, autentifikatsiya qilish maqsadida smartfonlar kabi ba’zi iste’molchi qurilmalarida ham foydalanilmoqda.

4. Ovozni aniqlash tizimlari: bu inson nutqini tanib olish va transkripsiya qilish uchun mashinani o‘rganish algoritmlaridan foydalanadigan dasturiy ilovalar. Bu tizimlar akustik modellar va neyron tarmoqlardan inson ovozining tovush to‘lqinlarini tahlil qilish va ularni matnga aylantirish uchun foydalanadi. Ovozni aniqlash tizimlarida Siri va Alisa kabi virtual yordamchilar, avtomatlashtirilgan telefon tizimlari va transkripsiya uchun nutqdan matnga dasturiy ta’minot kabi keng ko‘lamli ilovalar mavjud. Ular ko‘pincha nogironligi bo‘lgan odamlarning foydalanish imkoniyatini yaxshilash yoki turli xil sozlamalarda qo‘llarsiz ishlashni ta’minlash uchun ishlatiladi.

Ovozni aniqlash texnologiyasi doimo rivojlanib bormoqda va u kelajakda yanada rivojlangan va keng tarqalish potensialiga ega.

5. Multimodal biometrik tizimlar: bu shaxslarni aniqlash uchun biometrik ma’lumotlarning bir nechta shakllaridan foydalanadigan xavfsizlik tizimlari. Ushbu tizimlar identifikatsiyaning aniqligi va ishonchliligini oshirish uchun yuzni aniqlash, barmoq izini skanerlash, ovozni aniqlash va ìrísíni aniqlash kabi turli xil biometrik autentifikatsiya usullarini birlashtiradi. Ma’lumotlarning bir nechta shakllaridan foydalangan holda, multimodal biometrik tizimlar individual biometrik usullarning cheklovlarini yengib o‘tishlari mumkin. Ular chegara nazorati, moliyaviy tizimlar va milliy identifikatsiya dasturlari kabi yuqori darajadagi xavfsizlik dasturlarida tobora ommalashib bormoqda. Multimodal biometrik tizimlar autentifikatsiyaning yanada xavfsiz va qulay shakllarini ta’minlash uchun smartfonlar kabi iste’molchi qurilmalarida ham qo‘llanilmoqda.

6. Xulq-atvor biometrik tizimlar: bu shaxsning xatti-harakatlaridagi noyob naqshlarni tahlil qilish va aniqlash uchun mashinani o‘rganish algoritmlaridan foydalanadigan xavfsizlik tizimining bir turi. Bu tizimlar har bir foydalanuvchi uchun o‘ziga xos “xulq-atvor imzosi”ni o‘rnatish uchun klavishlar bosish dinamikasi, sichqoncha harakati va boshqa xatti-harakatlar namunalari kabi ma’lumotlardan foydalanadi. Keyinchalik bu foydalanuvchining identifikatorini tekshirish uchun ishlatilishi mumkin. Xulq-atvor biometrik tizimlar, ayniqsa, an’anaviy biometrik tizimlar amaliy bo‘lmasligi mumkin bo‘lgan holatlarda, masalan, shaxsning jismoniy biometrik ma’lumotlarining namunasini olish qiyin yoki amaliy bo‘lmagan holatlarda foydalidir. Xulq-atvor biometrik tizimlarining ba’zi ilovalari firibgarlikni aniqlash, kirishni boshqarish va foydalanuvchi autentifikatsiyasini o‘z ichiga oladi. Xulq-atvor biometrik tizimlar ortidagi texnologiya doimo rivojlanib bormoqda va kelajakda yanada aniqroq va keng qo‘llanilishi mumkin.

Biometrik identifikatsiya va autentifikatsiyaning afzalliklari sifatida quyidagilarni ta’kidlash mumkin:

Yuqori darajadagi xavfsizlik: Biometrik ma’lumotlar har bir shaxs uchun unikal hisoblanadi, ushbu usul biometrik identifikatsiya va autentifikatsiyani parol yoki kalitlarga qaraganda xavfsizroq qiladi.

Foydalanish qulayligi: unutilishi yoki yo‘qolishi mumkin bo‘lgan parollardan farqli o‘laroq, biometrik xususiyatlar har doim siz bilan bo‘ladi va qo‘shimcha esda saqlashni talab qilmaydi.

Firibgarlik xavfini kamaytiring: Yuqori darajadagi aniqlik va ishonchlilik bilan biometrik autentifikatsiya firibgarlik va ruxsatsiz kirishning oldini olishga yordam beradi.

Avtomatlashtirish qobiliyati: Biometrik tizimlar turli tizimlar va jarayonlarga integratsiya qilinishi mumkin. Bu esa ish samaradorligini oshirib foydalanuvchilarga qulayliklar yaratib beradi.

Shaxsiy identifikatsiyaning shaffofligi: biometrik ma'lumotlardan foydalanish ma'lum bir shaxsni aniqlashga imkon beradi, bu xavfsizlik va tartibni ta'minlash nuqtayi nazaridan muhim bo'lishi mumkin.

Biometrik identifikatsiya va autentifikatsiyaning afzalliklariga ega bo'lib qolmay balkim kamchiliklarga ham egadir:

Maxfiylik va ma'lumotlar xavfsizligi: Biometrik ma'lumotlarni to'plash va saqlash maxfiylik va shaxsiy ma'lumotlarni himoyasi bilan bog'liq muammolarni keltirib chiqarishi mumkin.

O'tkazilmasligi va o'zgarmasligi: Agar biometrik ma'lumotlar yo'qolsa yoki shikastlansa, tiklash jarayoni qiyin yoki imkonsiz bo'lishi mumkin.

Texnik muammolar: Ba'zi biometrik tizimlar noto'g'ri ishlab ketishi yoki noto'g'ri tanib olish kabi muammolarga duch kelishi mumkin, bu esa qoniqarsiz foydalanuvchi tajribasiga olib kelishi mumkin.

Amalga oshirish xarajatlari: Biometrik tizimlarni joriy etish apparat, dasturiy ta'minot va xodimlarni o'qitishga katta sarmoya talab qiladi.

Hujumlarga nisbatan zaiflik: Yuqori darajadagi himoyaga qaramay, ba'zi biometrik tizimlar barmoq izlarini buzish yoki fiziologik sensorlarni buzish kabi hujumlarga qarshi himoyasiz bo'lishi mumkin.

Biometrik identifikatsiya mezonlari

Biometrik identifikatsiya asosida ACS (**kirishni boshqarish tizimlari**) samaradorligini aniqlash uchun quyidagi ko'rsatkichlar qo'llaniladi:

- FAR— noto'g'ri o'tish tezligi;
- FMR — tizim kiritilgan namunani ma'lumotlar bazasidagi mos bo'lmagan shablon bilan noto'g'ri taqqoslash ehtimoli;
- FRR— noto'g'ri rad yetish darajasi;
- FNMR — tizim kiritilgan namuna va ma'lumotlar bazasidan mos keladigan shablon o'rtasidagi moslikni aniqlashda xato qilish ehtimoli;
- ROC syujeti — FAR va FRR xususiyatlari o'rtasidagi o'zaro kelishuvni vizualizatsiya qilish;
- Ro'yxatga olishning muvaffaqiyatsizligi darajasi (FTE yoki FER) — kiritilgan ma'lumotlardan shablonni yaratishga muvaffaqiyatsiz urinishlar darajasi (ikkinchisining past sifati bilan);
- Noto'g'ri saqlash darajasi (FTC) — avtomatlashtirilgan tizim biometrik ma'lumotlar to'g'ri taqdim yetilganda ularni aniqlay olmasligi ehtimoli;
- Shablon sig'imi — tizimda saqlanishi mumkin bo'lgan ma'lumotlar to'rlarining maksimal soni.

Biometrik identifikatsiyaning asosiy usullarini qiyosiy tahlil qilish

Matematik statistika **(FAR va FRR)** yordamida biometrik autentifikatsiya usullarini taqqoslash

Har qanday biometrik tizimni baholashning asosiy parametrlari ikkita parametrdir:

FAR (False Accyertancye Rate) - noto‘g‘ri o‘tish darajasi, ya’ni. tizim tizimda ro‘yxatdan o‘tmagan foydalanuvchiga kirishga ruxsat beradigan holatlar foizi.

FRR (False Rejection Rate)— noto‘g‘ri rad yetish darajasi, ya’ni. tizimning haqiqiy foydalanuvchisiga kirishni rad yetish.

Ikkala xususiyat ham matematik statistika usullari asosida hisoblash yo‘li bilan olinadi. Ushbu ko‘rsatkichlar qanchalik past bo‘lsa, obyektni tanib olish qanchalik aniq bo‘ladi.

Bugungi kunda yeng mashhur biometrik identifikatsiya usullari uchun o‘rtacha FAR va FRR

Biometrik ACS quyidagilardan foydalanadi:	**FAR**	**FRR**
Barmoq izi	0,001%	0,6%
2D yuzni aniqlash	0,1%	2,5%
3D yuzni aniqlash	0,0005%	0,1%
Irs	0,00001%	0,016%
Retina	0,0001%	0,4%
Tomirlar namunasi	0,0008%	0,01%

qiymatlari quyidagicha:

.

ACS nima va u qanday ishlaydi? Tekshirish moslamasi o‘quvchilardan ma’lumotlarni oladi va olingan ma’lumotlarga, shuningdek belgilangan kirish sozlamalariga asoslanib, blokirovka qiluvchi qurilmalarni boshqaradi. Har bir kirish, chiqish va o‘tishga urinish hodisasi nazoratchi tomonidan qayd yetiladi. Kirish taqiqlanganda, boshqaruvchi o‘g‘ri signalini yoqishi mumkin. Barcha qayd yetilgan hodisalar yagona ACS ma’lumotlar bazasiga o‘tkazilishi mumkin. Favqulodda vaziyatlarda, masalan, yong‘in sodir bo‘lganda, boshqaruvchi yong‘in signalizatsiyasidan signal olishi va o‘tish joylarini ochishi mumkin. Nazoratchilar ham avtonom ishlaydi, ham umumiy tarmoqqa birlashtirilishi mumkin.

1-rasm Identifikatordan ma’lumotlarni o‘qiydigan va uni boshqaruvchiga uzatuvchi qurilmalar.

Talabalar boshqariladigan o‘tish joylari yaqinida ko‘zga tashlanadigan joylarda joylashgan yoki turniket kabi blokirovka qiluvchi qurilmalarga o‘rnatilgan.

Biometrik avtorizatsiya qurilmalari:S

- bosish tugmasi
- identifikatorlardan o‘quvchilar (kartalar, kalit foblar, shtrixli chiptalar)
- biometrik (barmoq izlari, kaft tomirlari, to‘r pardasi, yuz shakli, ovoz)

2-ra fi ri

Egasini aniqlash va uning vakolatlari doirasini belgilash imkonini beruvchi noyob kodga ega qurilmalar. Shaxsiy identifikatsiyalash vositasi sifatida quyidagilar qo‘llaniladi:

- Kontaktli va kontaktsiz kartalar
- Kalit halqalar "tabletkalar"
- Shtrixli chiptalar va kartalar

Identifikatorlar doimiy egasi uchun ham, vaqtinchalik tashrif buyuruvchilar uchun ham amal qilish muddati yoki ruxsatnomalar soni bo‘yicha cheklov bilan berilishi mumkin.

Foydalanilgan adabiyotlar:

1. Biometrics Researcher Asks: Is That Eyeball Dead or Alive? [Электронный ресурс] / IEEE Spectrum: Technology, Engineering, and Science News. — Электрон.дан.,URL:http://spectrum.ieee.org/thehumanos/biomedical/imaging/ biometric-researcher asks-is-that-eyeball-alive-or-dead, свободный. – Яз. англ
2. Биометрические методы компьютерной безопасности [Электронный ресурс] / BYTE; ред. Шаров В. — Электрон. дан., URL: https://www.bytemag.ru/articles/detail.php?ID=6719. свободный. – Яз. рус.
3. Идентификация по отпечаткам пальцев. Часть 2. [Электронный ресурс] / Институт экономической безопасности — Электрон. дан., ред. В. Задорожный. URL:http://www.bre.ru/security/20994.html. свободный. – Яз. рус.
4. Биометрические технологии — алтернатива персоналним идентификационним номерам и паролям // к2капитал.com Аналитические обзори 8 мая 2000.
5. Завгородний В.И. Комплексная зашита информации в компютерних системах // Учебное пособие. — М.: Мир, 2001. — 264 с.
6. M.Z.Xusenov, L.O.Sharipova, Oliy ta’lim muassasalarida masofaviy ta’limni joriy qilish, “Pedagogik mahorat” ilmiy-nazariy va metodik jurnal. 2022, № 2 B: 94-96
7. M.Z.Xusenov, L.O.Sharipova, Kimyo fanini o‘qitishda VR texnologiyasini qo‘llash, Pedagogik mahorat Ilmiy-nazariy va metodik jurnal maxsus son (2021-yil, dekabr) 164-166
8. M.Z.Khusenov, L.O.Sharipova, Statistical analysis of network problems and their impact on the practice of social computing in Uzbekistan, E3S Web of Conferences Volume 389, 09017 (2023) Ural Environmental Science Forum “Sustainable Development of Industrial Region-31 May 2023