

SHAXSNI TANIB OLUVCHI BIOMETRIK TIZIMLAR

Temirov Zavqiddin Xusen o'g'li¹, Olimova Mahzuna Mirzoxurshid qizi¹

¹Alfraganus University

KALIT SO'ZLAR

ANNOTATSIYA

Biometriya, verifikasiya, identifikasiya, autentifikatsiya.

Ushbu maqolada shaxsni identifikatsiyalovchi biometrik tizimlarda ko'p faktorli biometrik tizimning tadbiri taklif qilingan. Xavfsizlik – har kuni biz to'qnashadigan hayotimizning jihati eshikni qulflaymiz, qimmatbaho narsalarni begona ko'zlardan berkitamiz va hamyonni

duch kelgan joyda qoldirmaymiz. Bu "raqamli dunyoga" ham rasm bo'lishi shart, chunki har bir foydalanuvchining kompyuteri qaroqchi hujumi ob'ekti bo'lishi mumkin. Hozirgi kunda butun dunyo mamlakatlarida axborotni muhofaza qilish davlat tizimining tashkiliy asoslari va vazifalarini o'rganish, axborot xavfsizligi va ma'lumotlarni muhofaza qilish sohasidagi xalqaro tajriba, axborot xavfsizligini ta'minlashning usul va vositalari hamda ma'lumotlarni muhofaza qilishning kompleks tizimlarini yaratish, shaxs, jamiyat va davlatning axborot xavfsizligi, davlat organlarining axborot xavfsizligini ta'minlash sohasidagi asosiy faoliyat yo'nalishlari, axborot xavfsizligining obyektlari, tahdidlar va ularning manbalari, axborotlarni kriptografik va texnik himoyalash asoslari, axborotlarni muhofaza qilishning tashkiliy chora-tadbirlarini ishlab chiqish keng yo'lga qo'yilgan va buni takomillashtirish bo'yicha qator ishlar qilinmoqda. Taklif etilgan ko'p faktorli biometrik texnologiyalarni tasniflashda, ishlatiluvchi biometrik alomatlar turi bo'yicha, biometrik tizimlar ikki guruhga ajratilib olindi. Biometrik parametrlardan ko'plab sohalarda xavfsizlikni ta'minlash maqsadida foydalanilib kelinmoqda. Mobil qurilmalarda turli biometrik parametrlardan autentifikatsiyalash jarayonida foydalanilishi, ulardan mobayl bankingda autentifikatsiyalashda ham foydalanish imkoniyati keltirib chiqardi. Shaxsni aniqlashning yuqori ishonchligini ta'minlovchi biometrik texnologiyalarining xarakteristikallari ko'rib chiqilgan.

I.Kirish.

Axborot xavfsizligi sohasiga muvofiq biometriya (ingl. biometrics) deganda inson shaxsiyatini, uning fiziologik va xatti harakat xarakteristikallari bo'yicha, avtomatik tarzda identifikatsiyalash va tasdiqlash usulini ifodalovchi bilim sohasi tushuniladi. Oldingi asrning 90-yillarida biometrik tizimlardan asosan harbiy ob'ektlarni va ayniqsa muhim tijoriy axborotni himoyalashda foydalanilgan bo'lsa, hozirda ayroportlar, yirik savdo markazlari, ko'pgina kompaniya ofislari foydalanishning biometrik tizimlari bilan jihozlangan. Extiyojning ortishi ushbu sohadagi tadqiqotlarni rag'batlantirib, yangi texnologiyalar va qurilmalarning paydo bo'lishiga olib keldi.

Foydalanuvchilarni identifikatsiya va autentifikatsiyadan o'tkazish asosan tizimdan foydalanishga ruxsat berish uchun amalga

oshiriladi. Ma'lumotlarni uzatish kanallarida himoyalashda sub'ektlarning o'zaro autentifikatsiyasi, ya'ni aloqa kanallari orqali bog'lanadigan sub'ektlar haqiqiyligining o'zaro tasdig'i bajarilishi shart.

Xavfsizlik nuqtai nazaridan yuqorida keltirilganlarning har biri o'ziga xos masalalarni yechishga imkon beradi. Shu sababli autentifikatsiya jarayonlari va protokollari amalda faol ishlatiladi. Shu bilan bir qatorda ta'kidlash lozimki, nullik bilim bilan isbotlash xususiyatiga ega bo'lgan autentifikatsiyaga qiziqish amaliy xarakterga nisbatan ko'proq nazariy xarakterga ega. Balkim, yaqin kelajakda ulardan axborot almashinuvini himoyalashda faol foydalanishlari mumkin. Autentifikatsiya protokollariga bo'ladigan asosiy hujumlar quyidagilar: - maskarad (impersonation). Foydalanuvchi o'zini boshqa shaxs deb ko'rsatishga urinib, u shaxs

tarafidan xarakatlarning imkoniyatlariga va imtiyozlariga ega bo'lishni mo'ljallaydi; autentifikatsiya almashinuvi tarafini almashtirib qo'yish (interleaving attack). Niyati buzuvchi odam ushbu hujum mobaynida ikki taraf orasidagi autentifikatsion almashinish jarayonida trafikni modifikatsiyalash niyatida qatnashadi. Almashtirib qo'yishning quyidagi xili mavjud: ikkita foydalanuvchi o'rtasidagi autentifikatsiya muvaffaqiyatli o'tib, ulanish o'rnatilganidan so'ng buzuvchi foydalanuvchilardan birini chiqarib tashlab, uning nomidan ishni davom ettiradi;

- takroriy uzatish (replay attack). Foydalanuvchilarning biri tomonidan autentifikatsiya ma'lumotlari takroran uzatiladi;

- uzatishni qaytarish (reflection attack). Oldingi hujum variantlaridan biri bo'lib, hujum mobaynida niyati buzuvchi odam protokolning ushbu sessiya doirasida ushlab qolingani axborotni orqaga qaytaradi.

- majburiy kechikish (forced delay). Niyati buzuvchi odam qandaydir ma'lumotni ushlab qolib, biror vaqtdan so'ng uzatadi. autentifikatsiya trafiginu ushlab qolib, uzoq muddatli kriptografik kalitlar xususidagi axborotni olishga urinadi. Yuqorida keltirilgan hujumlarni bartaraf qilish uchun autentifikatsiya protokollarini qurishda quyidagi usullardan foydalaniladi: -"so'rov-javob", vaqt belgilari, tasodifiy sonlar, indentifikatorlar, raqamli imzolar kabi mexanizmlardan foydalanish;

- autentifikatsiya natijasini foydalanuvchilarning tizim doirasidagi keyingi harakatlariga bog'lash. Bunday misol yondashishga tariqasida autentifikatsiya jarayonida foydalanuvchilarning keyingi o'zaro aloqalarida ishlatiluvchi maxfiy seans kalitlarini almashishni ko'rsatish mumkin;

- aloqaning o'rnatilgan seansi doirasida autentifikatsiya muolajasini vaqti-vaqti bilan bajarib turish va h. Autentifikatsiya protokollarini taqqoslashda va tanlashda quyidagi xarakteristikalarini hisobga olish zarur:

- o'zaro autentifikatsiyaning mavjudligi. Ushbu xususiyat autentifikatsion almashinuv taraflari o'rtasida ikki yoqlama autentifikatsiyaning zarurligini aks ettiradi;

- hisoblash samaradorligi. Protokolni bajarishda zarur bo'lgan amallar soni;

- kommunikatsion samaradorlik. Ushbu xususiyat autentifikatsiyani bajarish uchun zarur bo'lgan xabar soni va uzunligini aks ettiradi;

- uchinchi tarafning mavjudligi. Uchinchi tarafga misol tariqasida simmetrik kalitlarni taqsimlovchi ishonchli serverni yoki ochiq kalitlarni taqsimlash uchun sertifikatlar daraxtini amalga oshiruvchi serverni ko'rsatish mumkin;

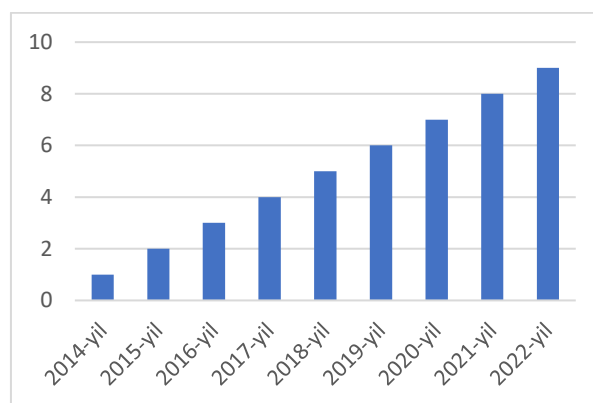
- xavfsizlik kafolati asosi. Misol sifatida nullik bilim bilan isbotlash xususiyatiga ega bo'lgan protokollarni ko'rsatish mumkin;

- sirni saqlash. Jiddiy kalitli axborotni saqlash usuli ko'zda tutiladi.

Autentifikatsiya jarayoni quyidagi xizmatlar uchun qo'llaniladi:

II. Asosiy qism.

Biometrik parametrlarga asoslangan autentifikatsiyalash usuli foydalanishga qulay bo'lib, unda esdan chiqarish yoki har doim birga olib yurish kabi muammolar mavjud emasligi sababli, hozirda keng foydalanilib kelinmoqda. Xususan, mobil qurilmalarda biometrik xususiyatlardan foydalanish orqali olinadigan daromadning yillar bo'yicha o'sishi quyidagi 1 - rasmda keltirilgan [5].

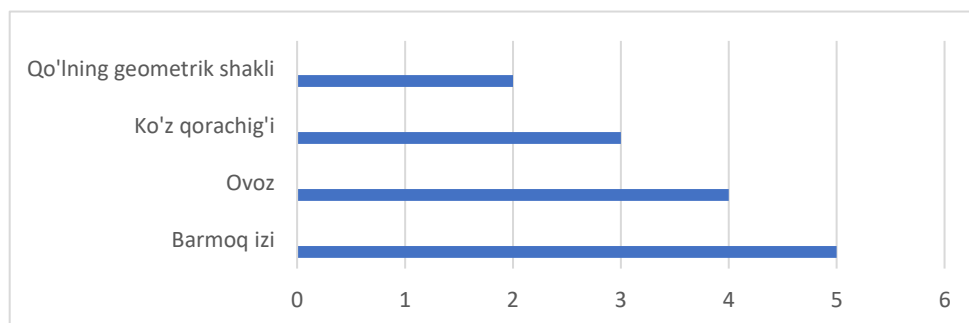


1 - rasm. Mobil qurilmalarda biometrik texnologiyalar foydasidan olinadigan daromadning yillar bo'yicha o'zgarishi

Ushbu statistik ma'lumotlardan ko'rish mumkinki biometrik parametrlarga asoslangan autentifikatsiyalash usullariga asoslangan vositalar miqdorining keyingi yillarda ortishi kuzatilmoqda. Biometrik parametrlardan ko'plab sohalarida xavfsizlikni ta'minlash maqsadida foydalanilib kelinmoqda. Mobil qurilmalarda turli biometrik parametrlardan autentifikatsiyalash jarayonida foydalanilishi, ulardan mobil bankingda

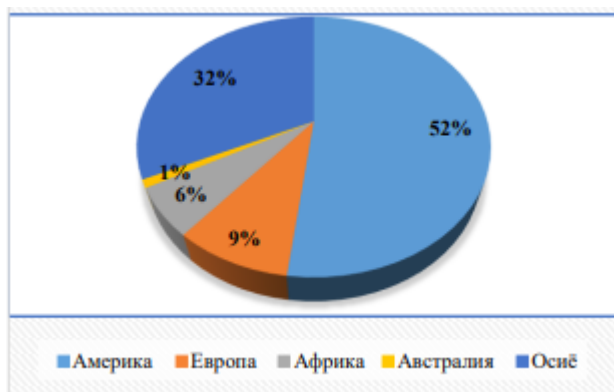
autentifikatsiyalashda ham foydalanish imkoniyati keltirib chiqardi. Bu soha hozirda jadallik bilan rivojlanayotgan bo'lib, bu sohadan tushayotgan daromadlarning ortishini 1 – rasmdan ham bilish

mumkin. Quyidagi 2 – rasmda bank sohasida foydalanilgan biometrik autentifikatsiyalash usullarining 2016 – yildagi ko'rsatkichlari keltirilgan [5].



2 – rasm. 2022 – yilda bank sektorlarida biometriklardan foydalanish ko'rsatkichi

Biometrik autentifikatsiyalash usullaridan bank sohasida foydalanishda asosan Osiyo va Amerika qit'asida joylashgan davlatlar yetakchilik qilib kelmoqda ularning ko'rsatkichlarini quyidagi 3 – rasmdan ham ko'rish mumkin [6].



3– rasm. Turli mintaqalardagi banklarda biometriklardan foydalanish ko'rsatkichlari

Yuqorida keltirilgan tahlil natijalari asosida biometrik autentifikatsiyalash sohasi Osiyo va Amerika davlatlarida keng tarqalganligini, biometrik autentifikatsiyalash usullaridan asosan moliya sohasida va mobil qurilmalarda foydalanilayotganligini ko'rish mumkin.

Odatda, biometrik texnologiyalarni tasniflashda, ishlatiluvchi biometrik alomatlar turi buyicha, biometrik tizimlar ikki guruhga ajratiladi.

Tizimlarning birinchi guruhi inson tug'ilishida orttirilgan va vaqt o'tishi bilan o'zgaraydigan statik biometrik alomatlardan foydalaniladi. Bunday alomatlarga quyidagilar taalluqli:

- barmoq izlari;
- ko'z yoyi va to'r pardasining naqshi;
- yuzning shakli va o'lchamlari;
- qo'l panjasining geometrik shakli;
- DNK va h

Tizimlarning ikkinchi guruhi vaqt bo'yicha o'zgarishlarga duchor bo'luvchi va har bir insonning shaxsiy xususiyatlarini ifodalovchi dinamik biometrik alomatlardan foydalaniladi. Bunday alomatlarga quyidagilar taalluqli;

- imzo (dastxat);
- ovoz;
- klaviaturada ishlash uslubi va h.

Shaxsning psixofizik holatiga nisbatan mustaqilligi, aniqlash algoritmlarini amalga oshirishdagi sarf-harajatning kamligi va natijada, insonlarning katta guruhini biometrik identifikatsiyalashni tashkil etish imkoniyati statik biometrik alomatlardan foydalanishning afzalligi hisoblanadi.

Aynan birinchi guruhga taalluqli yuqorida keltirilgan 3 ta alomatlardan (barmoq izlari, ko'z yoyi va to'r pardasining naqshi, yuzning shakli va o'lchamlari) foydalanishga asoslangan biometrik usullarning amalda eng ko'p tarqalganligi bejiz emas. Statik biometriyaning kamchiligi sifatida ishlatiluvchi biometrik alomatlarining statikligini (o'zgarasligini) va natijada ularni soxtalashtirish (almashtirish) imkoniyati paydo bo'lishini hamda maxsus o'quvchi qurilmaning mavjudligi talabini ko'rsatish mumkin.

Birinchi guruhga tegishli usullardan farqli o'laroq, dinamik biometrik usullar ko'p variantlikni ta'minlaydi (masalan, dastxatni va parol iborasini osongina yangilash mumkin). Ushbu muolaja kompyuterning standart tashqi qurilmalaridan foydalanib, dasturiy yo'l bilan osongina amalga oshiriladi. Ushbu holat masofadan foydalanishda shaxsni identifikasiyalashda va autentifikasiyalashda dinamik biometriyaning afzalligini yanada yaqqol ko'rsatadi. Dinamik biometriyaning asosiy kamchiligi sifatida shaxsning psixofizik xolatining (toliqqanliq, qo'rquv va dori –darmonlar tasiri) biometrik tizim ishlashiga ta'sirini ko'rsatish mumkin.

Ta'kidlash lozimki, hozirda barcha davlatlarda yangi avlod pasport-viza hujjatlari (biometrik pasportlar) uchun aynan yuzning raqamli tasviri majburligi e'tirof etilgan. Boshqa ikkita parametrlar –barmoq izlari, ko'z yoyi va to'r pardasining naqshi qo'shimcha hisoblanadi hamda ularni har bir davlat o'z ixtiyoriga ko'ra biometrik pasportga qo'shishi mumkin.

Biometriya sohasidagi halqaro standartga (ISO/JEC 19794-5) tuzatish kiritilib, unga binoan saqlashga, almashishga mo'ljallangan va shaxsni avtomatik aniqlashda ishlatiluvchi ma'lumotlar formatiga oddiy ikki o'lchamli fotosurat bilan bir qatorda, yuzninig uch o'lchamli raqamli tasviri kiritildi. A4 Vision kompaniyasi tomonidan taqdim etilgan uch o'lchamli (3D) fotosurat 5 Kbayt xotirani egallaydi, uni osonlik bilan biometrik pasportga yozish mumkin. Uch o'lchamli fotosurat shaxsni identifikasiyalash aniqligini va hujjatlarni avtomatik taqqoslash ishonchligini oshiradi. Ekspertlarning ta'kidlashicha uch o'lchamli fotosuratning aniqlash darajasi 90% dan oshadi, ikki o'lchamli tasvirda esa bu ko'rsatkich kamdan – kam 50% dan yuqori bo'ladi [1].

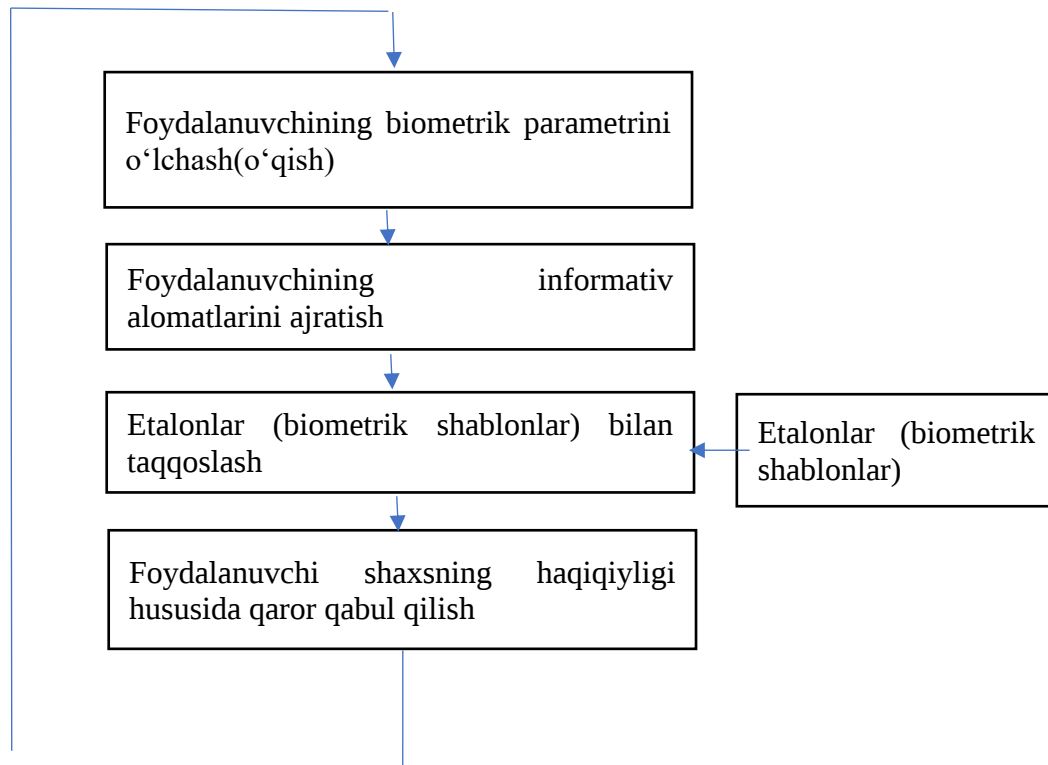
Har qanday biometrik tizim ishlashi asosida quyidagi harajatlar zanjiri yotadi (4-rasm):

- yozish - foydalanuvchining biometrik ma'lumotlari skaner yordamida o'qiladi;
- ajratish - taqdim etilgan biometrik ma'lumotlardan noyob axborot tanlab olinadi va bu axborot muayyan shaxsning biometrik “obrazi” hisoblanadi;
- taqqoslash - taqdim etilgan biometrik obrazni tizim ma'lumotlar bazasida saqlanuvchi bitta yoki ko'p sonli etalonlar (shablonlar) bilan taqqoslash amalga oshiriladi;

Qaror qabul qilish - tizim biometrik obrazlar mosligini yoki mos emasligini hal etib identifikasiya muolajasining tugallanganligi, uni takrorlash yoki o'tkazish shartlarini o'zgartirish xususida qaror qabul qiladi. Biometrik ma'lumotlarni ajratish va taqqoslash bosqichlarida biometrik shablonlardan foydalaniladi. Biometrik shablonlar, odatda tarkibida mos biometrik obrazlar xususida kodlangan (zichlangan) ko'rinishdagi axborot bo'lgan berk, binar formatdagi ma'lumotlar naboridan iborat. Biometrik ma'lumotlarni taqdim etishning yagona formatini o'rnatuvchi xalqaro standart CBEFF (Common Biometris Exchange File Format) mavjud.

Biometrik tizim ishlashining ikkita rejimi farqlanadi – verifikasiya (bittani bitta bilan taqqoslash) va identifikasiya (bittani ko'p bilan taqqoslash). Verifikasiya rejimida foydalanuvchi tizimga o'zining biometrik ma'lumotlarini (biometrikasini) taqdim etadi, ya'ni, tizimga o'zining kim ekanligini ma'lum qiladi. Ushbu holda tizimning vazifasi olingan axborotning “haqiqiyligini” tekshirish, ya'ni, olingan biometrik ma'lumotlarni shaxs bildirgan, oldindan yozilgan shablon (etalon) bilan taqqoslash hisoblanadi.

Ilmiy Axborotlar



4-rasm. Biometrik identifikasiya muolajasi

1-jadval

Biometrik texnologiyalarining xarakteristikalar

Kriteriyalar Texnologiyalar	O'lchanuvchanlik	Atrof muhitga barqarorlik	Qalbakilashtirishga barqarorlik	Aniqlash aniqligi
Yuz ra'siri bo'yicha: -2D-fotosurat: -3D-Fotosurat	O' O'	P O'	P Y	P P
Barmoq izlari bo'yicha	P	P	P	O'
Ko'z yoyi va to'r pardasining naqshi bo'yicha	P	O'	P	O'
Ovoz bo'yicha	P	P	Y	Y
P-past; O' – o'rtacha; Y- yuqori				

Identifikasiya rejimida ham foydalanuvchi tizimga o'zining biometrikasini taqdim etadi. Ammo, tizim vazifasi o'zgaradi, u foydalanuvchining tizimga ma'lum shaxslar sirasiga taalluqligi xususida qaror qabul qilishi lozim bo'ladi. Agar taalluqli bo'lsa – u kim? Bunda o'lchangan biometrik ma'lumotlar tizimga “ma'lum” shaxslarning oldindan yozilgan

shablonlarining ma'lumotlar bazasi bilan taqqoslanadi.

Ravshanki, real sharoitda biometrik tizimlardan foydalanishda qator muommolarga duch kelinadi. Ulardan biri - shaxsni aniqlashning yuqori ishonchligini ta'minlash zaruriyati bo'lib, ushbu muammoni echish murakkabligi quyidagilar bilan izohlanadi:

- o'lganuvchi biometrik ma'lumotlar katta sonli noaniqlik omillariga yo'liqqani bois, biometrik identifikatsiya/ autentifikatsiya muolajasi ehtimollik xarakterga ega bo'ladi va natijada "o'zinikini tan olmaslik" va "begonani o'ziniki deb hisoblash" ehtimolliqi saqlanadi:

- biometrik tizim atayin qilingan aldovaldan himoyalanihi lozim, ya'ni, biometrik skanerlash ob'ektini almashtirib qo'yish imkoniyati;

- yig'ilgan biometrik axborotning yaxlit saqlanishi masalasini dolzarblashi (so'z nafaqat uning buzilishi va h. xususida boradi, balki, har qanday biokod masalan, ko'z yoyi va to'r pardasining naqshi yoki barmoq izlari o'zida muayyan shaxs sog'lig'i xususida ko'pgina axborotni eltadi va h. Bu noqonuniy maqsadlarda ishlatilishi mumkin).

Turli biometrik texnologiyalarni qiyosiy baholash 1 – jadvalda keltirilgan [2]. Jadvalning ustunlarida biometrik texnologiyalarning u yoki bu darajada javob berishi lozim bo'lgan asosiy kriteriyalar hamda ushbu kriteriyalarning turli texnologiyalar uchun sifatii mazmuni keltirilgan (faqat yuz tasviri bo'yicha aniqlash - ikki o'lgamli (2D) va uch o'lgamli (3D) fotosurat barmoq izi hamda ko'z yoyi va to'r pardasining naqshi hamda ovoz buyicha aniqlash texnologiyalari ko'rilgan). Yuqorida keltirilgan kriteriyalar quyida batafsil tavsiflangan:

1. O'lganuvchanlik. Biometrik alomat (parametr) osongina o'lganishi lozim. O'lganuvchanlikni miqdoriy ravishda 1-FER tenglik bilan baholash mumkin. Bu erda, FER (Failure to Enroll) - ro'yxatdan o'ta olmagan shaxslar ulushi (tizim biometrik shablonni shakllantirmaganligi sababli) va aniqlashning o'rtacha vaqti kattalıkları (Recognition Time). Aniqlash vaqti deganda tizim ishlashi rejimiga mos holda verifikatsiya vaqti yoki identifikatsiya vaqti tushuniladi.

Ko'z yoyi va to'r pardasining naqshi buyicha aniqlash ko'zning skanerlovchi qurilmaga nisbatan aniq joylashtirish lozimligi bilan bog'liq ma'lum qiyinchiliklarga olib keladi.

Barmoq izlari bo'yicha aniqlash esa insonlarning ko'pgina guruhi, (ayniqsa, fizik mehnat bilan shug'ullanuvchi xodimlar, terisi nuqsonli insonlar, terisi quruq keksalar), qiyin hisoblanadi.

Yuz tasviri bo'yicha aniqlash usullari kontaktsiz va shu sababli biometrik alomatların yuqori o'lganuvchanligiga ega.

2. Atrof muhitga barqarorligi. Biometrik texnologiya atrof muhit o'zgarishiga barqaror bo'lishi lozim. Turli texnologiyalarning eksplutatsiya sifati ko'p holatlarda atrof-muhit sharoitiga bog'liq va bu sharoitlar o'zgarganida barqarorlik yo'qolishi mumkin.

Masalan, barmoq izlari skanerlarining tez kirlanishi ish sifatining pasayishiga olib keladi. Ikki o'lgamli fotosurat bo'yicha yuzni aniqlashda esa tashqi yoritilganlikning taqsimlanishi muhim ahamiyatga ega. Bunday texnologiyalarni ishlab chiquvchi kompaniyalar barmoq izlarini olishda turli, xususan elektrik, elektromagnit va boshqa usullarni amalga oshiruvchi vositalardan foydalanadilar. Skanerlardan biri barmoq izi tasvirini shakllantirish maqsadida teri qismlarining sig'im qarshiligini o'lgaydi. Masalan, Veridicom kompaniyasining daktiloskopik qurilmasi yarimo'tkazgichli datchik yordamida sig'im qarshiligini aniqlash orqali axborotni yig'adi. Sensor ishlashining prinsipi quyidagicha: Ushbu asbobga qo'yilgan barmoq kondensator plastinalarining biri vazifasini o'taydi. Sensor sirtida joylashgan ikkinchi plastina kondensatorning 90000 sezgir plastinkali kremniy mikrosxemasidan iborat. Sezgir sig'im datchiklari barmoq sirti do'ngliklari va pastliklari orasidagi elektrik maydon kuchining o'zgarishini o'lgaydi. Natijada do'ngliklar va pastliklarga bo'lgan masofa aniqlanib, barmoq izi tasviri olinadi. Integral sxema asosidagi sensorli tekshirishda.

Bu usul bo'yicha asosiy skaner sifatida Identix kompaniyasining TouchSafe II skanerlarini keltirish mumkin. Bu skaner kontrolleri kompyuterga ISA shinasini orqali ulanadi. Qator ishlab chiqaruvchilar biometrik tizimlarni smart-kartalar va karta – kalitlar bilan kombinatsiyalaydilar. Integral sxemalar asosidagi barmoq izlari datchiklarining kichik o'lgamlari va yuqori bo'lmagan narxi ularni himoya tizimi uchun ideal interfeysga aylantiradi. Ularni kalitlar uchun breloklarga o'rnatish mumkin. Natijada foydalanuvchi kompyuterdan boshlab to kirish yo'li, avtomobillar va bankomatlar eshiklaridan himoyali foydalanishni ta'minlaydigan universal kalitga ega bo'ladi. **AuthenTeck** kompaniyasida

ishlatiluvchi usul aniqlikni yana ham oshirishga imkon beradi.

3. Qalbakilashtirishga barqarorlik. Biometrik tizim turli qalbakilashtirish usullariga (ruxsatsiz foydalanishga) barqaror bo'lishi lozim. Yuzning ikki o'lchamli tasviri bo'yicha aniqlash tizimini, unga ro'yxatdan o'tgan biror shaxs fotosuratini taqdim etib, osongina aldash mumkin. Begona ko'z pardasini o'g'irlash yuz fotosuratini o'g'irlashga qaraganda murakkabroq. Ammo, ko'z pardasi o'g'irlangan taqdirda, tizimni "talab etilgan" ko'zning fotografik tasviri orqali aldash mumkin.

Barmoq izlari bo'yicha ruxsatsiz foydalanish huquqini qo'lga kiritishni ixtiyoriy sirtida qoldirilgan "kerakli" shaxsning barmoq izlarini olib, raqamlashtirib, olingan tasvirni kompyuterda ishlov berib, so'ngra "soxta" barmoqni yasash orqali amalga oshirish mumkin.

Yuzning uch o'lchamli tasviri bo'yicha aniqlash texnologiyasi qalbakilashtirishga eng barqaror hisoblanadi. Bunday tizimni aldash uchun yuz geometriyasining barcha detallarini aniq akslantiruvchi maskani yaratish talab etiladi. Amalda buning imkoni yo'q. Ovoz xususiyatlari bo'yicha shaxsni identifikatsiyalashning bir qancha o'ziga xos tomonlari mavjud. Birinchidan, rivojlangan telefon tarmog'ining mavjudligi. Ikkinchidan, ovoz kartalari zamonaviy shaxsiy kompyuterlarning standart uskunasiga aylanib ulgurdi. Bundan tashqari, ovoz bo'yicha identifikatsiya insonlar uchun an'anaviy hisoblanadi va psixologik noqulaylikni keltirib chiqarmaydi. Bu tizimlar arzonligi tufayli eng foydalanuvchan hisoblanadilar, chunki aksariyat zamonaviy kompyuterlar video va audio vositalariga ega. Bu biometrik tizimlari telekommunikatsiya tarmoqlarida masofadagi foydalanuvchi subyektni identifikatsiyalash uchun ishlatiladi. Yuz tuzilishini skanerlash texnologiyasi boshqa biometrik texnologiyalar yaroqsiz bo'lgan ilovalar uchun to'g'ri keladi. Bu holda shaxsni identifikatsiyalash va verifikatsiyalash uchun ko'z, burun va lab xususiyatlari ishlatiladi. Yuz tuzilishini aniqlovchi qurilmalarni ishlab chiqaruvchilar foydalanuvchini identifikatsiyalashda xususiy matematik algoritmlardan foydalanadilar. Ta'kidlash lozimki, yuz tuzilishini aniqlash texnologiyasi yanada takomillashtirishni talab

etadi. Yuz tuzilishini aniqlovchi aksariyat algoritmlar quyosh yorug'ligi jadalligining kun bo'yicha tebranishi natijasidagi yorug'lik o'zgarishiga ta'sirchan bo'ladilar. Yuz holatining o'zgarishi ham aniqlash natijasiga ta'sir etadi. Yuz holatining 90° ga o'zgarishi aniqlashni samarasiz bo'lishiga olib keladi.

4. Aniqlash aniqligi. Biometrik tizimning ishlash aniqligini baholaganda quyidagi ko'rsatkichlardan foydalaniladi:

- FAR (False Acceptance Rate) - tizim ruxsatga ega bo'lmagan foydalanuvchini haqiqiy deb topgandagi yolg'ondan aniqlash ehtimolligi; - FRR (False Rejection Rate) – foydalanish ruxsatini yolg'ondan rad etish ehtimolligi bo'lib, tizim haqiqiy foydalanuvchini o'zida mavjud bo'lmagan sifatida qaraydi.

FRR va FAR statistik echimlar nazariyasida, mos holda 1-va 2-xildagi xatoliklar deb yuritiladi

Har qanday biometrik tizimni "sergakligi"ning turli darajasiga, ya'ni, yolg'ondan aniqlash (FAR)ning turli qiymatiga sozlash mumkin. Ammo, FAR-ning kamayishi doimo tizim sezuvchanligini pasayishiga va yolg'on rad etish FRR ehtimolligining oshishiga olib keladi. Shunday qilib, tizim "begonalarni" o'tkazmaslikka qanchalik "sergak" sozlangan bo'lsa, u shunchalik kam sezuvchanlikka ega, ya'ni, "o'zinikilarni" yomonroq o'tkazadi. Zamonaviy tizimlarda FAR qiymati foizning ulushini tashkil etsa, FAR-ning qiymati 2-5% ga teng

Tadqiqotlar ko'rsatadiki, tizim aniqligining muayyan ko'rsatkichlari ishlab chiqaruvchilarga va testlash usuliga bog'liq holda o'zgaradi. Ammo, yuzning uch o'lchamli tasviri, barmoq izlari va ko'z yoyi va to'r pardasining naqshi bo'yicha aniqlash texnologiyalari taqqoslab bo'ladigan aniqlikka ega. Yuzning ikki o'lchamli tasviri bo'yicha aniqlash texnologiyasining aniqligi sanab o'tilgan texnologiyalar aniqligiga nisbatan ancha past. Ammo, ikki o'lchamli tasvir operator tomonidan ko'z bilan taqqoslashda qulay hisoblanadi.

Identifikatsiya rejimda aniqlash aniqligini oshirishda bir nechta biometrik texnologiyalardan birligida foydalanish maqsadga muvofiq

hisoblanadi. Biometrik tizimlardagi ushbu istiqbolli yo'nalish identifikasiyaning ko'p faktorli biometrik (multibiometrik) tizimni (AMIS, Automated Multimodal Biometric Identification Systems) qurish konsepsiyasiga asoslanib, [3] manbada qo'riqlash sohasida quyidagi texnologiyalarni integrasiyalash taklif etilgan:

- barmoq izlari bo'yicha;
- yuz tasviri bo'yicha;
- ovoz bo'yicha;
- imzo (dastxat) bo'yicha.

Ushbu biometrik texnologiyalarni integrasiyalash ikkita jihatni ko'zda tutadi: texnik va algoritmik. Texnik integrasiyaga binoan bir necha dasturiy apparat komplekslari yagona interfeys orqali birlashtiriladi. Ushbu masala standartlash yo'li bilan yetarli darajada hal etiladi. Algoritmik nuqtai nazaridan biometrik texnologiyalarining integrasiyasi biometrik obrazlar naborlarining bir xilligi xususida qaror qabul qilishning yetarlicha murakkab tadbiqiy matematik masalasi xisoblanadi.

III.Xulosa

Xulosa sifatida aytish lozimki, ko'p faktorli biometrik tizimning tadbiqi shaxsni aniqlash jarayonining sifatini oshirishga imkon beradi. Shuningdek biror bir korxona tashkilot binosiga xodimlarning kirish vaqtida yoki muayyan ma'lumotlardan foydalanishga ruxsat olishda biometrik azolardan foydalanish ma'lumotlar xavfsizligini ta'minlashda juda katta yordam beradi. Biometrik tizimlar hozirgi kunda eng ko'p foydalaniladigan tizimlar qatoriga kiradi. Ko'p faktorli biometrik tizimni yaratishda biometrik integratsiyaning o'zi yetarlicha katta hisoblash muolajasi ekanligini ko'zda tutish lozim. Demak,

mazkur holatda dasturiy apparat kompleksi tarkibiga yuqori unumdorlikka ega serverni kiritish talab etiladi, Boshqacha aytganda, ko'p faktorli biometrik tizim klient-server ilova sifatida yaratiladi.

IV.Adabiyotlar.

1. Sovremennie biometricheskie sistemi bezopasnosti [Elektronniy rusurs]. - Rejim dostupa: http://www/npo_inform/com/press/sovribio.
2. Vakulenk A. Biometricheskie metodi identifikatsii lichnosti:obosnovanniy vibor i vnedrenie /A.Vakulenk, A.Yuxin //PC Week/RE/ - 2019/-№ 29. –S. 15-16,31
3. Umashev O. Realizatsiya konsepsii mnogofaktornoy biometricheskoy identifikatsii: materialy konf. /VI Mejdunarodniy biometricheskaya konf. BIOMETRICS AIA 2020 LEGS "Pasportnie i pravooxranitel'nie sistemi 2018.
4. P.Stavroulakis, M.Shtam «Spravochnik po inforsionnoy i kommunikatsionnoy bezopasnosti» Springer Science &Business Media, 2021
5. Biometrics: the Future of Mobile Payments. U.S. Economic Watch. Nathaniel Karp. 20 July 2021.
6. Review banking on biometric in the world's banks and introducing a biometric model for Iran's banking system. Seyyede Samine Hosseini. <https://www.researchgate.net/publication/237862021>. September, 2021.