BIOMETRIK AUTENTIFIKATSIYA TIZIMINING AFZALLIKLARI VA KAMCHILIKLARI

[1] Abdullayev Axrorbek Anvarjon o‘g‘li,
[2] Qurbonova Durdona G‘olibjon qizi
[1,2] Namangan davlat universiteti o‘qituvchilari.

Annotatsiya: *Ushbu maqolada biometrik autentifikatsiya va identifikatsiyalash tizimlari, afzalliklari va kamchiliklari, o‘ziga xoslik darajasi haqida tahliliy fikrlar ko‘rsatib o‘tilgan.*

Kalit so‘zlar: *biometrik autentifikatsiya, biometrik identifikatsiya, False Access Rejection, False Access Grant.*

ПРЕИМУЩЕСТВА И НЕДОСТАТКИ БИОМЕТРИЧЕСКОЙ СИСТЕМЫ АУТЕНТИФИКАЦИИ

[1]Абдуллаева Ахрорбека Анваржон Огли,
[2]Курбанова Дурдона
[1,2]Преподаватели Наманганского государственного университета.

Аннотация: *В данной статье представлены аналитические мнения о биометрических системах аутентификации и идентификации, их достоинствах и недостатках, уровне уникальности.*

Ключевые слова: *биометрическая аутентификация, биометрическая идентификация, ложный отказ в доступе, ложное предоставление доступа.*

ADVANTAGES AND DISADVANTAGES OF A BIOMETRIC AUTHENTICATION SYSTEM

[1]Abdullayev Akhrorbek, [2]Kurbanova Durdona
[1,2] Teachers of Namangan State University.

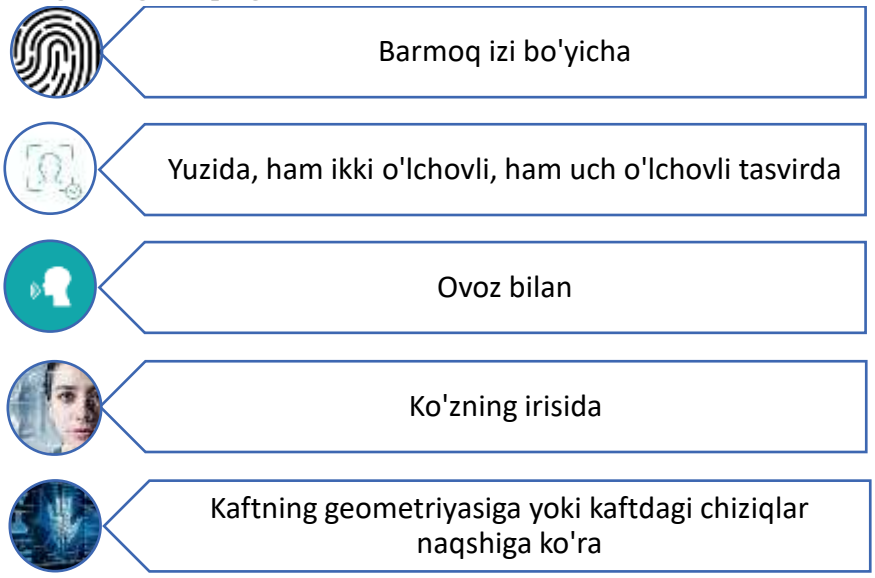
Annotation*: This article presents analytical opinions about biometric authentication and identification systems, their advantages and disadvantages, and the level of uniqueness.*

Key words*: biometric authentication, biometric identification, False Access Rejection, False Access Grant.*

Biometrik identifikatsiya/autentifikatsiya har yili ommalashib bormoqda. Bunday texnologiyalar butun dunyo bo‘ylab turli sohalarga faol integratsiya qilinmoqda va deyarli har bir insonning hayotiga mustahkam kirdi. Biometrik ko‘plab zamonaviy mobil qurilmalarda qo‘llaniladi. Biz viza olganimizda, masalan, Shengen vizasi, bizdan biometrik ma’lumotlarni (barmoq izlari) taqdim etishimiz talab qilinadi. 2012 yildan boshlab O‘zbekistonda biometrik xorijiy pasportlar berila boshlandi[1,4]. Yuqori ehtimollik bilan oddiy umumiy pasport yoki uning analogi ham yaqin kelajakda biometrik bo‘ladi.

Yirik kompaniyalarda biometrik autentifikatsiya kirishni tashkil qilishda korporativ tarmoqda tobora ko‘proq foydalanilmoqda. ATM modellari paydo bo‘ldi, ularga kirish biometrik tekshiruvdan so‘ng amalga oshiriladi. Eng yirik biometrik identifikatsiya loyihalari davlat darajasida amalga oshirilmoqda. Dunyodagi eng yirik biometrik identifikatsiya tizimi Hindistonda joriy qilingan. 2018-yil boshida unda 1 milliarddan ortiq kishi ro‘yxatga olingan. Ayni paytda mamlakatimizda fuqarolarning bankka bormasdan turib bank xizmatlaridan foydalanishi uchun yuzma-yuz va ovozli aloqa orqali masofaviy biometrik autentifikatsiya qilish davlat loyihasi va boshqa qator xizmatlar amalga oshirilmoqda[1,4].

Hozirgi vaqtda biometrik identifikatsiya/autentifikatsiyaning quyidagi 1-rasmdagi turlari eng keng tarqalgan[1,4]:



1-rasm (identifikatsiya/autentifikatsiyaning turlari)

Biometrik identifikatsiya (BI) autentifikatsiyadan (BA) farq qiladi, chunki identifikatsiyalash paytida foydalanuvchi o‘zining biometrik ma’lumotlarini tizimda mavjud bo‘lgan barcha ma’lumotlar bilan solishtirish yo‘li bilan aniqlanadi. Biometrik autentifikatsiya yordamida foydalanuvchi tizimga kimligini aytadi (masalan, unikal login kiritadi), tizim ushbu login yordamida ma’lumotlar bazasidan o‘zining biometrik

ma’lumotlarini o‘qiydi va keyin ularni foydalanuvchi tomonidan taqdim etilganlar bilan tekshiradi.

Biometrik barmoq izini autentifikatsiya qilish hozirda dunyoda eng keng tarqalgan bo‘lishiga qaramay, boshqa texnologiyalar faol rivojlanmoqda va yangilari paydo bo‘lmoqda. Hozirgi vaqtda eng istiqbollilari kaftdagi chiziqlar naqshiga asoslangan va irisga asoslangan biometrik autentifikatsiya texnologiyalari bo‘lib ko‘rinadi (Samsung flagman smartfonlarida joriy etilgan). Tez orada ushbu texnologiya boshqa ishlab chiqaruvchilarning qurilmalarida paydo bo‘lishini kutish mumkin.

Nega biometrik ma’lumotlar shunchalik jozibali?

Javob oddiy ko‘rinadi: bu insonning ajralmas qismi bo‘lib, vaqt o‘tishi bilan o‘zgarmaydi va uni o‘ziga xos tarzda belgilaydi. Aslida bu haqiqat emas. Turli xil biometrik autentifikatsiya texnologiyalari uchun bu da’volar turli darajadagi ishonchlilikka ega. Barmoq izi yoki iris biometric identifikatsiya uchun uchta bayonot ham juda to‘g‘ri. Ovoz yoki yuz autentifikatsiyasi uchun endi bunday emas. Bu ko‘rsatkichlar fiziologik o‘zgarishlar tufayli inson hayoti davomida sezilarli darajada o‘zgaradi. Yuzni autentifikatsiya qilishga kelsak, bu erda odamning o‘zi qisqa vaqt ichida o‘z qiyofasini tubdan o‘zgartirishi mumkin[2,3].

Agar zamonaviy plastik jarrohlik imkoniyatlarini hisobga oladigan bo‘lsak, unda identifikatorning (yuzning) uzoq vaqt davomida o‘zgarmasligi haqidagi bayonot odatda ishonchliligini yo‘qotadi. Xuddi shu narsa ovozga ham tegishli. U nafaqat hayot davomida o‘zgaribgina qolmay, balki turli kasalliklarda, ayniqsa, sovuqlarda jiddiy o‘zgarishlarga duchor bo‘ladi, insonning vaqtincha ovozini yo‘qotishi mumkinligi haqida gapirmaslik kerak, ya’ni aslida aniqlash vositalarini yo‘qotadi.

Identifikatsiyaning o‘ziga xoslik darajasi ham nisbiy tushunchadir. Bularning barchasi tizimda sozlangan identifikatsiya/autentifikatsiya jiddiyligi darajasiga bog‘liq. Tashkilotimizda biometrik barmoq izlari autentifikatsiyasini joriy qilganimizda, deyarli har qanday odam turli xil barmoqlarni turli pozitsiyalarda qo‘llash bilan 10-15 daqiqa davomida tajriba o‘tkazgandan so‘ng, boshqa foydalanuvchi hisobi ostida autentifikatsiya qilishiga duch keldik. Bu qanday, deb so‘raysiz, chunki odamning barmoq izi noyobdir? Gap shundaki, biometrik autentifikatsiya tizimlari ikki barmoq izini to‘g‘ridan-to‘g‘ri solishtirmaydi. Dastlab, tizimda ro‘yxatdan o‘tishda odam barmog‘ini qo‘yadi, uni skanerlaydi va taxminan aytganda, papiller naqshning ma’lum nuqtalarida ma’lum bir matematik model (konvolyutsiya) hosil bo‘ladi. Keyingi autentifikatsiya vaqtida barmoq namunasi skanerlanadi va matematik konvolyutsiya qayta hisoblab chiqiladi. Aynan u standart bilan taqqoslanadi. Ko‘rinib turibdiki, odam har safar barmog‘ini biroz boshqacha

qo‘yganda, skanerlash maydoni boshqacha bo‘ladi, shuning uchun tizim izlarning mos kelishining jiddiyligini belgilaydi.

Biometrik autentifikatsiya tizimlarining ikki xil xatosi[1,3]:

1. False Access Rejection (FR) - resursdan foydalanish huquqiga ega bo‘lgan vakolatli shaxsga kirishni rad etish;

2. False Access Grant (FA) - ob’ektga kirish huquqiga ega bo‘lmagan yoki undan mahrum bo‘lgan shaxslarni resursga qabul qilish.

Birinchi holda, identifikatorni noto‘g‘ri ishlatish yoki biometrik xususiyatlarni noto‘g‘ri kiritish tufayli xato (FR) paydo bo‘ladi.

Xato (FA) odatda dastlabki ma’lumotlarni noto‘g‘ri ro‘yxatdan o‘tkazish yoki oldingi foydalanuvchilardan qolgan uchinchi tomon yozuvlari mavjudligi bilan bog‘liq.

Bundan tashqari, menejerlar ko‘pincha qurilmalarning o‘zlari bilan taqqoslash uchun ishonch chegarasini ortiqcha baholaydilar yoki kam baholaydilar. Ushbu chegarani oshirish ruxsatsiz shaxslarning ob’ektga kirish imkoniyatini minimallashtiradi, ammo bu holda ruxsat berilgan foydalanuvchilarga ko‘proq kirish taqiqlanadi.

Biometrik tizimning afzalliklari:

- Autentifikatsiyaning ishonchliligi va tezligi: barmoq izi yoki iris namunasi asosida elektron tahliliy qurilmalar bir yoki ikki soniya ichida shaxsni aniqlaydi;
- Xavfsizlikning yuqori darajasi: shaxsning biometrik xususiyatlari noyobdir, bu identifikatsiyalashda xatolar sonini kamaytiradi;
- Biometrik ma’lumotlarni yo‘qotish yoki unutish mumkin emas;
- Biometrik autentifikatsiya qurilmalaridan foydalanish oson va tejamkorlik bilan ishlaydi.

Biometrik tizimning kamchiliklari:

- Joriy ma’lumotlar bazasida biometrik xususiyatlarni o‘zgartirish mumkin emas - parollardan farqli o‘laroq, ular hayoti davomida ma’lum bir shaxs bilan bog‘lanadi;
- Yoshga bog‘liq o‘zgarishlar, jarohatlar, amputatsiyalar va boshqa narsalar tufayli elektron hisoblash qurilmalari xotirasiga kiritilgan mos yozuvlar taqqoslash modellarini doimiy ravishda yangilab turish talab etiladi;
- Biometrik namunalarni yaratish uchun maxsus o‘quvchilar talab qilinadi;
- Biometrik ma’lumotlarni sir saqlash mumkin emas, shuning uchun malakali hujumchilar barmoq izlari yoki qo‘l izlari namunalarini soxtalashtirishi mumkin.

Hozirgi vaqtda biometrik ma’lumotlarni o‘qish uchun eng ko‘p qirrali qurilma bu mobil telefondir. Ehtimol, ushbu qurilmalarda yangi biometrik identifikatsiya

texnologiyalari joriy etiladi. Mobil telefonlar ko‘p faktorli biometrik skanerlarga aylanadi. Mutaxassislarning fikriga ko‘ra, elektronika davriga qadam qo‘yayotganimizni va tibbiy telemetriya sakrash va chegaralar bilan oldinga siljishini hisobga olsak, yaqin kelajakda o‘ziga xos kamchiliklardan xoli yangi biometrik identifikatsiya texnologiyalari paydo bo‘lishi mumkin[2,4].

FOYDALANILGAN ADABIYOTLAR

1. https://lex.uz/docs/-1729272?ONDATE=01.06.2018 - O‘zbekiston Respublikasida pasport tizimini takomillashtirishga doir qo‘shimcha chora-tadbirlar to‘g‘risida. O‘zbekiston Respublikasi Prezidentining Farmoni, Toshkent sh., 2011-yil 5-yanvar, PF-4262-son

2. https://securitymedia.org/info/biometriya-dostoinstva-i-nedostatki.html - Биометрия: достоинства и недостатки.

3. Abdullaev A. (2023). MAKTABDA INFORMATIKA FANINI SUN’IU INTELLEKT BILAN INTEGRASHGAN USULDA O‘QITISh. Talqin Va tadqiqotlar, 1 (31).https://talqinvatadqiqotlar.uz/index.php/tvt/article/view/1276.

4. H.E. Holmirzayev. Yuz biometriyasi va dasturiy mahsulotni tanlash mezonlari. 3-8 betlar, NamDU maxsus son 2020 yil.