SHAXSNI YUZ TASVIRI BO‘YICHA BIOMETRIK IDENTIFIKATSIYA QILISHGA ASOSLANGAN KIRISHNI NAZORAT QILISH VA BOSHQARISH TIZIMLARI

Ataxanov M.X.
O‘zbekiston Respublikasi Fanlar Akademiyasi Botanika instituti
Xusainov N.O.
“Temurbeklar maktabi” harbiy akademik liseyi
Jo‘rayev Sh.U.
Namangan davlat universiteti
Abdullayeva B.M.
Namangan davlat universiteti

Annotatsiya. Maqolada shaxsni yuz tasviri bo‘yicha biometrik identifikatsiyaga qilishga asoslangan kirishni nazorat qilish va boshqarish zamonaviy tizimlari tahlil qilingan. Unda bunday tizimlarning ishlash tamoyillari, tanib olish algoritmlari, neyron tarmoqlar arxitekturasi hamda ularning korporativ va ijtimoiy infratuzilmaga integratsiyalashuvi masalalari ko‘rib chiqilgan. Ayniqsa, tijoriy va ochiq manbali yechimlarning qiyosiy tahliliga, mavjud muammolarga, axloqiy jihatlarga hamda xavfsizlik va raqamli identifikatsiya sohasidagi rivojlanish istiqbollariga alohida e’tibor qaratilgan.

Kalit so‘zlar: biometrika, kirishni boshqarish tizimlari, neyron tarmoqlar, identifikatsiya.

Abstract. This article presents an overview of modern access control systems based on biometric identification using facial images. It explores the principles of operation, recognition algorithms, neural network architectures, and integration challenges of such systems within corporate and public infrastructures. Special attention is given to a comparative analysis of commercial and open-source solutions, current issues, ethical concerns, and future development prospects in the fields of security and digital identity.

Keywords: biometrics, access control systems, neural networks, identification.

Kirish.

Zamonaviy xavfsizlik texnologiyalarida biometrik identifikatsiya usullari tobora keng qo‘llanilmoqda, ularning orasida esa yuzni tanib olish alohida o‘rin egallaydi. Shaxsni yuz tasviri bo‘yicha biometrik identifikatsiyaga qilishga asoslangan kirishni nazorat qilish va boshqarish tizimlari (KNQBT) turli sohalarda – ofislar va sanoat korxonalaridan tortib aeroportlar va davlat muassasalarigacha – keng tatbiq etilmoqda. Ushbu maqolada mazkur yo‘nalishdagi asosiy yondashuvlar, arxitektura yechimlari hamda rivojlanish tendensiyalarining tahliliy sharhi keltirilgan.

ISSN 3030-3907

I. Yuz orqali biometrik identifikatsiya ishlash prinsiplari. Yuz tasviri asosida biometrik identifikatsiya qiluvchi tizimlar tasvirni olish, belgilarni ajratish va ularni etalon shablonlar bilan solishtirish jarayonlariga tayanadi. Bu jarayonda mashinaviy o‘qitish va kompyuter ko‘rish usullari, jumladan, konvolyutsion neyron tarmoqlar (CNN), tasvirlarni normallashtirish usullari, shuningdek, ma’lumotlarni dastlabki va keyingi qayta ishlash algoritmlari qo‘llaniladi [1, 2].

Yuz tasviri asosida biometrik identifikatsiya jarayoni shartli ravishda bir necha asosiy bosqichlarga bo‘linadi.

Tasvirni olish bosqichida foydalanuvchining yuzini qayd etuvchi videokameralar qo‘llaniladi. Tasvir sifati keyingi qayta ishlash jarayonlarida hal qiluvchi ahamiyat kasb etadi. Shuningdek, real vaqt rejimida tasvir olish tizimlari bilan integratsiya qilish hamda tasvirni ko‘rish burchagi, aniqligi va yoritilganlik darajasi bo‘yicha dastlabki filtratsiyani amalga oshirish imkoniyati mavjud.

Yuzni belgilash va normallashtirish bosqichida tizim kadrda yuz mavjudligini aniqlash uchun unga mos algoritmlaridan, masalan, MTCNN (Multi-task Cascaded CNN) [3] dan foydalanadi. Keyin esa boshning egilishi, burilishi yoki mimika tufayli yuzaga keladigan farqlarni bartaraf etish maqsadida asosiy nuqtalar — ko‘zlar, burun va og‘iz koordinatalari bo‘yicha tasvirni to‘g‘irlash amalga oshiriladi.

Belgilarn ajratib olish chuqur o‘qitilgan konvolyutsion neyron tarmoqlar yordamida amalga oshiriladi, masalan: FaceNet [4], ArcFace [5] va DeepFace [6]. Ushbu tarmoqlar bir xil shaxsga tegishli belgilar orasidagi masofani minimallashtiradi hamda turli shaxslarga oid belgilar o‘rtasidagi farqni maksimal darajada oshiradi.

Etalon shablonlar bilan solishtirish jarayoni o‘xshashlik metrikalari (kosinus masofasi yoki Yevklid masofasi) ni hisoblash orqali amalga oshiriladi [1].

Ma’lumotlarning xavfsizligini ta’minlash uchun shifrlash usullari va soxtalashtirishga qarshi himoya tizimi texnologiyalari qo‘llaniladi. Bular tarkibiga terining teksturasini tahlil qilish hamda yuzning 3D hajmga ega ekanligini tekshirish kabi usullar kiradi [7].

Yangi foydalanuvchi tizimga qo‘shilganda, uning yuz tasvirlari turli rakurslardan olingan holda tahlil qilinadi va bu tasvirlar asosida shakllantirilgan bir yoki bir nechta belgi vektorlari maxsus himoyalangan ma’lumotlar bazasida saqlanadi.

Bundan tashqari, tizim xavfsizlik va ma’lumotlarning maxfiyligini ta’minlaydi – barcha biometrik ma’lumotlar shifrlangan shaklda saqlanishi lozim. Yuz tasviri orqali amalga oshiriladigan soxtalashtirish hujumlardan himoyalanish uchun teri teksturasini tahlil qilish, yuzning 3D hajmini aniqlash, shuningdek ko‘z va bosh harakatlarini tekshirish kabi himoya usullari qo‘llaniladi.

ISSN 3030-3907

II. Zamonaviy arxitekturalar va algoritmlar tahlili. Bugungi kunda yuzni aniqlash sohasida eng samarali hisoblangan arxitekturalar qatoriga VGG-Face [8], FaceNet [4], ArcFace [5], DeepFace [6] va ularning turli modifikatsiyalari kiradi. Ushbu modellar chuqur konvolyutsion neyron tarmoqlar va optimallashtirilgan yo‘qotish funksiyalaridan (Additive Angular Margin Loss) foydalanish orqali identifikatsiya aniqligining yuqori darajasini ta’minlaydi. Barcha modellar ish tezligi, hisoblash resurslariga bo‘lgan talab hamda sabablarning o‘zgarishga (yoritilganlik, rakurs yoki yoshdagi o‘zgarishlar) nisbatan barqarorlik jihatidan bir-biridan farq qiladi.

Yuzni tanish uchun mo‘ljallangan zamonaviy neyron tarmoq arxitekturalari chuqur konvolyutsion neyron tarmoqlar asosida quriladi. Ularda e’tibor mexanizmlari, qoldiq bog‘lanishlar hamda maxsus yo‘qotish funksiyalari qo‘llaniladi. Quyida ushbu sohada eng muhim hisoblangan model va usullar keltirilgan.

Facebook AI tomonidan ishlab chiqilgan DeepFace modeli – LFW (Labeled Faces in the Wild) ma’lumotlar bazasida 97% aniqlikka erishgan dastlabki modellaridan biridir [6]. Google tomonidan taklif etilgan FaceNet modeli esa triplet loss (uchlik yo‘qotish) funksiyasidan foydalanadi hamda ishlab chiqarish tizimlarida keng qo‘llanuvchi kompakt belgi vektorlarini shakllantirish imkonini beradi [4].

Oxford VGG tadqiqotchilari tomonidan taklif etilgan VGG-Face modeli VGG-16 arxitekturasi asosida qurilgan bo‘lib, juda katta hajmdagi yuz tasvirlari to‘plamida o‘qitilgan [8]. ArcFace esa belgilarni yanada aniqroq ajratish imkonini beruvchi va tasvir sharoitlaridagi o‘zgarishlarga nisbatan barqarorlikni oshiruvchi “Additive Angular Margin Loss” (yo‘qotish funksiyasi) deb ataluvchi o‘zgartirilgan matematik modelni qo‘llaydi [5].

CosFace va SphereFace modellarida sinflar o‘rtasidagi burchak masofalarini optimallashtirish yondashuvi yanada rivojlantirilgan [2]. Mobil va edge-qurilmalar uchun esa yengillashtirilgan neyron tarmoqlar – MobileFaceNets va EfficientFace ishlab chiqilgan bo‘lib, ular aniqlikni saqlagan holda energiya sarfini kamaytirish imkonini beradi [9]. Shuningdek, tasvirlarni dastlabki qayta ishlash jarayonida MTCNN algoritmi keng qo‘llaniladi; u yuzni aniqlash va tekislashni bir vaqtning o‘zida amalga oshiradi [3].

III. Biometrik tizimlarni kirishni nazorat qilish va boshqarish tizimlariga integratsiyalash. Biometrik tizimlarni korxona infratuzilmasiga integratsiyalash tegishli dasturiy-apparat yechimlarini talab qiladi. Yuqori aniqlikdagi kameralar, edge-hisoblash qurilmalari, shuningdek biometrik ma’lumotlarni saqlash va qayta ishlash serverlari qo‘llaniladi. Xavfsizlik va shifrlash protokollari, shuningdek shaxsiy ma’lumotlar to‘g‘risidagi qonunchilik

ISSN 3030-3907

talablariga rioya etish ham bunday tizimlarni joriy etishning ajralmas jihatlaridan biridir. Alohida e'tibor shifrlash protokollariga va ISO/IEC 19794-5:2011 kabi xalqaro standartlarga rioya etishga qaratiladi [7].

Integratsiya jarayoni o'z ichiga bir necha bosqichni oladi:

– talablarni yig'ish: bino arxitekturasini, foydalanish ssenariylarini, foydalanuvchilar sonini va xavfsizlik darajasini tahlil qilish;

– uskunani tanlash: biometrik modullar bilan mos kameralar, kirish terminallari, kontrollerlar, serverlar va dasturiy ta'minot (DT)ni tanlash;

– mavjud KNQBT bilan integratsiya: biometrik modullarni korporativ KNQBT, ERP tizimlari va videokuzatuv tizimlariga ulash;

– DTni joylashtirish va modellarga o'qitish: tanish tizimi dasturiy ta'minotini sozlash, foydalanuvchilarning etalon ma'lumotlarini yuklash, modellarni o'qitish yoki qayta o'qitish;

– sinovdan o'tkazish va optimallashtirish: tanib olish aniqligini, ishlash tezligini hamda tashqi omillarga barqarorlikni tekshirish;

– me'yorlarga rioya etish: shifrlash, jurnalga olish, audit mexanizmlarini joriy etish hamda foydalanuvchilarning biometrik ma'lumotlarni qayta ishlashga roziligini ta'minlash.

Bundan tashqari, zamonaviy tizimlar o'z ichiga ish vaqtini hisobga olish modullari, prediktiv tahlil (predictive analytics) moduli, shuningdek ko'p modalli biometrikani (masalan, ovoz va ko'z qorachig'i asosidagi identifikatsiya) qo'llab-quvvatlash hamda mobil ilovalar bilan integratsiyani o'z ichiga olishi mumkin.

IV. Mavjud yechimlarning taqqoslama tahlili. Bozor ham tayyor tijoriy mahsulotlarni, ham open-source (ochiq kodli) yechimlarni taklif etadi. Muayyan yechimni tanlashda identifikatsiya aniqligi, unumdorlik, narx, integratsiya qulayligi va texnik qo'llab-quvvatlash kabi omillar hisobga olinadi.

KNQBT asoslarini ularning afzallik va kamchiliklarini ko'rsatgan holda ko'rib chiqamiz.

NEC NeoFace. Ushbu tizim videokuzatuv, CRM va hisob tizimlari bilan integratsiyalashish imkoniyatiga ega, oson masshtablanadi hamda ko'p tilli interfeysga ega. Jahon bozoridagi real vaqt rejimida ishlovchi eng aniqligi yuqori bo'lgan yuzni aniqlash tizimlaridan biri sifatida, u ishonchli texnik qo'llab-quvvatlash bilan ta'minlangan va yirik infratuzilmaviy obyektlarda qo'llash uchun mosdir. Biroq, ushbu tizim KNQBT litsenziyalash va joriy etish xarajatlarining yuqoriligi, shuningdek, yopiq arxitekturaga ega ekani bilan ajralib turadi.

VisionLabs LUNA Platform – bu tizim oqimda (real vaqt rejimida) yuzni aniqlash, kuzatish (tracking), foto va video asosida identifikatsiya qilish imkoniyatiga ega. U modul asosida tuzilgan arxitekturaga, API interfeyslarga ega bo'lib, edge va server yechimlarini qo'llab-quvvatlaydi. Tizim MDH mamlakatlari

ISSN 3030-3907

uchun yaxshi moslashtirilgan (lokalizatsiyalangan) bo‘lib, haqiqiy ish sharoitlarida yuqori aniqlikka ega. Kamchiliklari sifatida – mintaqadan tashqarida kamroq tanilganligi va bulutli (cloud) muhitda masshtablashdagi qiyinchiliklar ko‘rsatiladi.

SenseTime Face++ – bu bulutli API asosida ishlovchi tizim bo‘lib, yuzni tanish, his-tuyg‘ularni tahlil qilish, jins va yoshni aniqlash imkoniyatiga ega. Shuningdek, IoT va “aqlli shahar” yechimlari bilan chuqur integratsiya qilishni qo‘llab-quvvatlaydi hamda multimodal imkoniyatlarga ega. Shu bilan birga, tizimning xalqaro bozorda mavjudligi va hujjatlashtirilganlik darajasi cheklangan.

OpenFace [10] – bu open-source (ochiq kodli), yengil model bo‘lib, biometrik yechimlarni ishlab chiqish va sinovdan o‘tkazish uchun mo‘ljallangan. U asosiy dasturlash tillarini (Python, C++) qo‘llab-quvvatlaydi, hamda, ilmiy tadqiqotlar va KBNQT prototiplarini ishlab chiqish uchun qulaydir. Biroq, zamonaviy arxitekturalar bilan solishtirilganda, ushbu model biroz eskirgan bo‘lib, u asosida yaratilgan tizimlar murakkab sharoitlarda yuzni aniqlashda past aniqlikka ega.

InsightFace [9] – bu open-source tizim bo‘lib, zamonaviy arxitekturalarni (ArcFace, CurricularFace), hamda MXNet, PyTorch kabi ramkalarni qo‘llab-quvvatlaydi. Tizimning afzalliklariga yuqori aniqlik va tezlik, faol hamjamiyat, muntazam yangilanishlar hamda to‘liq hujjatlashtirish kiradi. Ushbu tizim ilmiy tadqiqotlar va tijoriy maqsadlarda qo‘llash uchun ham mosdir. Ammo tizimni to‘g‘ri integratsiya qilish uchun DevOps/ML ko‘nikmalari talab etiladi, shuningdek, rasmiy texnik qo‘llab-quvvatlash yo‘q (barchasi GitHub yoki hamjamiyat orqali amalga oshiriladi).

V. Biometrik kirishni nazorat qilish va boshqarish tizimlarini tanlash bo‘yicha tavsiyalar. Biometrik nazorat tizimining samaradorligi tashkilot miqyosi, xavfsizlik talablarining darajasi, foydalanish sharoitlari va ajratilgan byudjetga bog‘liq. Quyida turli xil tashkilotlar uchun mos yechimlarni tanlash bo‘yicha tavsiyalar keltirilgan.

Tashkilot turlari	Tavsiya etiladigan yechimlar	Tanlash sabablari	Xususiyatlari
1. Yirik korporatsiyalar va sanoat korxonalari	NEC NeoFace, VisionLabs LUNA, SenseTime	• foydalanuvchilar oqimi katta bo‘lgan sharoitda yuqori aniqlikdagi identifikatsiya; • taqsimlangan arxitektura va markazlashtirilgan	mavjud IT-infratuzilmaga (ERP, HRM, videokuzatuv tizimlari) integratsiyalash imkoniyatiga

ISSN 3030-3907

		boshqaruvni qo‘llab-quvvatlash; • korporativ xavfsizlik va qonunchilik talablariga muvofiqlik.	ega bo‘lgan masshtablanadigan tizim zarur.
2. O‘rta va kichik korxonalar	VisionLabs LUNA (local versiya), InsightFace (on-premise), OpenFace (prototiplar uchun)	• o‘tkazuvchanlik (bandwidth) bo‘yicha o‘rtacha talablar; • narx va funksionallik o‘rtasidagi muvozanatni saqlash zarurati.	ustuvorlik ochiq APIga ega, bulutga ulanmasdan lokal tarzda joylashtirilishi mumkin bo‘lgan yechimlarga beriladi.
3. Davlat muassasalari va xavfsizlik idoralari	NEC NeoFace, SenseTime, muallif tomonidan ishlab chiqilgan yechimlar.	• ishtirok etayotgan tizimlardan yuqori darajada ishonchlilik, maxfiylik va nosozliklarga bardoshlilik talab etiladi; • normativ-huquqiy hujjatlar talablariga to‘liq muvofiqlik zarur.	majburiy tarzda jurnal yuritish, shifrlash va ma’lumotlarni mantiqiy ajratish tizimining mavjudligi
4. Ta’lim muassasalari	InsightFace, OpenFace	• mavjudligi va IT bo‘limi kuchi bilan mustaqil joriy etish imkoniyati; • kirish nazoratini, davomatni hisobga olishni va xavfsizlikni oshirishni ta’minlash uchun mos.	sozlashning soddaligi va kirish darajalarini moslashuvchan tarzda belgilash imkoniyati muhim ahamiyatga ega
5. Chakana savdo, sport va fitnes sohalari	SenseTime, VisionLabs, InsightFace	• tezkor identifikatsiya, CRM va marketing tizimlari bilan integratsiya; • yosh, jins va emotsiyalarni aniqlash imkonini beruvchi tahlil funksiyalarini qo‘llab-quvvatlash.	ish tezligi, vizual integratsiya va foydalanuvchi qulayligi muhim ahamiyatga ega

ISSN 3030-3907

VI. Muammolar va chaqiriqlar. Yutuqlarga qaramay, hali ham bir qator hal etilmagan masalalar mavjud: tashqi ko‘rinishdagi o‘zgarishlar sababli aniqlikning pasayishi, etika va maxfiylik bilan bog‘liq muammolar, shuningdek, tasvirlar yoki 3D niqoblar yordamida amalga oshiriladigan hujumlar ehtimoli. Shuningdek, ko‘p foydalanuvchilar oqimi sharoitida yuz beruvchi ommaviy xatolarga qarshi tizimning barqarorligi ham muhim ahamiyatga ega bo‘ladi.

Yuzni aniqlash asosidagi biometrik KNQBT texnologik jihatdan yetuk va keng qo‘llanilish imkoniyatiga ega bo‘lsa-da, ularning samaradorligi, ishonchliligi va jamoatchilik tomonidan qabul qilinishini cheklovchi bir qator muammolar mavjud:

– aniqlik va ishonchlilik muammosi. KNQBT tizimining ishonchliligiga tashqi ko‘rinishdagi o‘zgarishlar (soqol, bo‘yanish, ko‘zoynak, yosh o‘zgarishi, jarohatlar), suratga olish sharoitining yomonligi (yomon yoritish, keskin soyalar, yon tomondan rakurs, harakatlanish), shuningdek, niqob va turli aksessuarlarning ishlatilishi ta’sir qiladi. COVID-19 pandemiyasi yuzning yopiq qismlariga nisbatan tizimlarning zaifligini yaqqol ko‘rsatdi;

– xavfsizlikka hujumlar. KNQBT tizimlari spoofing-hujumlar (foto, video yoki 3D-niqoblar yordamida soxtalashtirish)ga, shuningdek, tarmoq infratuzilmasini buzish, shablonlarni qalbakilashtirish va autentifikatsiyani aylanib o‘tish kabi harakatlarga nisbatan zaif hisoblanadi;

– maxfiylik muammolari. Bunga shaxsiy ma’lumotlarni qayta ishlash (biometrik ma’lumotlar – qonun bilan himoyalangan sezgir ma’lumotlar), foydalanuvchining roziligining yo‘qligi (ko‘p hollarda foydalanuvchilar ma’lumot to‘plash hajmi va maqsadidan bexabar), hamda ma’lumotlar bazasining buzilishi tufayli yuzaga keluvchi oqibatlar kiradi;

– huquqiy va axloqiy to‘siqlar. Ayrim mamlakatlarda biometrik ma’lumotlar bilan ishlash bo‘yicha aniq me’yorlar mavjud emas. Shuningdek, ayrim algoritmlar aniqlikda etnik, jinsiy yoki yoshga oid farqlarni namoyon qilishi mumkin;

– infratuzilmaviy cheklovlar. Bunga joriy etish xarajatlari (uskunalar, serverlar, dasturiy ta’minot, integratsiya va texnik xizmat ko‘rsatish xarajatlari), eski tizimlar bilan moslashuv muammolari (to‘liq modernizatsiyani talab qilishi), shuningdek, masshtablashdagi murakkabliklar kiradi. Tajriba loyihasidan sanoat darajasidagi tizimga o‘tganda unumdorlik va boshqaruv bilan bog‘liq muammolar paydo bo‘ladi.

VII. Rivojlanish istiqbollari. Biometrik KNQBT tizimlarining kelajagi modellarni tashqi omillarga nisbatan barqarorligini oshirish, gibrid identifikatsiya usullarini (masalan, yuz va ovoz) qo‘llash, edge AI texnologiyalaridan foydalanish, shuningdek, kontaktsiz va noinvaziv kirish usullariga qiziqishning ortishi bilan chambarchas bog‘liq.

ISSN 3030-3907

Zamonaviy rivojlanish tendensiyalari biometrik KNQBT tizimlarining aniqlik, ishonchlilik va moslashuvchanlik darajasini oshirishga, shuningdek, ularni korporativ raqamli ekotizimlar va “aqlli shaharlar” infratuzilmasi bilan chuqur integratsiyalashishga yo‘naltirilgan. Ushbu tizimlarning evolyutsiyasidagi asosiy yo‘nalish – yuzni aniqlash algoritmlarini takomillashtirishdir. So‘nggi yillarda turli neyron arxitekturalarning afzalliklarini birlashtiruvchi ko‘p modelli yondashuvlarni qo‘llash kengaymoqda. Shuningdek, mashg‘ulot (train) jarayonida multimodal ma’lumotlardan – tasvir, ovoz va xulq-atvor xususiyatlarini birlashtirgan hamda sintetik ma’lumotlar to‘plamlaridan foydalanish orqali o‘qitish materialining xilma-xilligini kengaytirish va haqiqiy namunalar bog‘liqligini kamaytirish imkonini bermoqda. Muhim yo‘nalishlardan yana biri – diqqat mexanizmlari va o‘z-o‘zini nazorat qilish orqali o‘rganish yondashuvlarini joriy etish bo‘lib, ular yangi ish sharoitlariga moslashishni va belgilarni samaraliroq ajratishni ta’minlaydi.

Yana bir muhim yo‘nalish – gibrid va ko‘pmodalli identifikatsiya tizimlarini rivojlantirishdir. Bunda ishonchlilikni oshirish maqsadida turli biometrik belgilar – yuz, ko‘z qorachig‘i, barmoq izi, ovoz va boshqa parametrlar birgalikda qo‘llaniladi. Bu yondashuv tizimning soxtalashtirishga qarshi barqarorligini oshiradi hamda shaxsni aniqlashda ko‘p bosqichli himoya va yuqori aniqlikni ta’minlaydi.

Zamonaviy KNQBT arxitekturasiga sezilarli ta’sir ko‘rsatayotgan yo‘nalishlardan yana biri – periferik hisoblash (edge computing) texnologiyalarini joriy etishdir. Biometrik ma’lumotlarni markaziy serverlardan lokal qurilmalarga – kameralar, terminallar yoki kirish nazorati kontrollerlariga ko‘chirish tizimning kechikishlarini kamaytiradi, javob tezligini oshiradi va shaxsiy ma’lumotlarni himoya qilishni kuchaytiradi. Bu nafaqat infratuzilma yuklamasini kamaytiradi, balki maxfiy ma’lumotlarning sizib chiqish xavfini ham pasaytiradi.

Muhim rivojlanish yo‘nalishlaridan yana biri biometrik kirishni nazorat qilish va boshqarish tizimlarini “aqlli qurilmalar tarmog‘i” hamda “aqlli binolar” infratuzilmasi bilan integratsiya qilishdir. Bunday muhitda kirishni nazorat qilish tizimi videokuzatuv, yoritish, iqlim nazorati, ogohlantirish va energiya iste’molini boshqarish kabi boshqa tizimlar bilan uzviy bog‘lanadi. Natijada, foydalanuvchining xatti-harakatlari va odatlariga mos ravishda avtomatik tarzda sozlanadigan kontekstual autentifikatsiya imkoniyati yuzaga keladi.

Texnologik taraqqiyot jarayonida biometrik ma’lumotlardan foydalanishning huquqiy, axloqiy va texnik asoslari ham izchil shakllanib bormoqda. Biometrik ma’lumotlarni saqlash, qayta ishlash va uzatish tartibini belgilovchi xalqaro standartlar hamda protokollar yaratilmoqda. Shu bilan birga, yuz, barmoq izi yoki ovoz kabi biometrik belgilarni tahlil qiluvchi algoritmlarda

ISSN 3030-3907

xatolik yoki adolatsizlikka olib keluvchi omillarni kamaytirish maqsadida, ochiq va ishonchli ma’lumotlar bazalarini yaratishga alohida e’tibor qaratilmoqda. Shuningdek, foydalanuvchilar va mutaxassislar uchun biometrik tizimlarning ishlash tamoyillarini tushunarli shaklda izohlab bera oladigan “izohli sun’iy intellekt” texnologiyalarini ishlab chiqish ham dolzarb yo‘nalishlardan biri hisoblanadi. Ushbu yondashuv biometrik tizimlarning shaffofligi va ishonchliligini oshirishga xizmat qiladi.

Nihoyat, foydalanuvchi qulayligi va jismoniy aloqasiz ishlash imkoniyati masalalari ham alohida ahamiyat kasb etmoqda. Zamonaviy foydalanuvchilar biometrik tizimlardan nafaqat yuqori aniqlik, balki tezkor va qulay foydalanish imkonini ham kutishadi. Shu sababli, ustuvorlik foydalanuvchidan bevosita tegishni talab qilmaydigan, tabiiy va tez ishlaydigan identifikatsiya usullariga berilmoqda. Ayniqsa, ommaviy kirish tizimlari yoki gigiyena talablari yuqori bo‘lgan muhitlarda, bunday kontaktsiz va intuitiv interfeyslar foydalanuvchi tajribasining yangi standarti sifatida shakllanmoqda.

Xulosa. Yuz tasviri orqali shaxsni biometrik identifikatsiya qiluvchi kirishni nazorat qilish tizimlari xavfsizlikni ta’minlash hamda foydalanuvchilar uchun qulaylik yaratishda yuqori samaradorlik ko‘rsatmoqda. Ular biznes va ijtimoiy institutlarning raqamli transformatsiyasining ajralmas qismiga aylanmoqda.

Biroq, bunday tizimlarni muvaffaqiyatli va axloqiy jihatdan to‘g‘ri joriy etish uchun texnologik cheklovlar, huquqiy me’yorlar va ijtimoiy omillarni e’tiborga olish zarur.

Kelgusida ushbu tizimlarning rivojlanishi ularning ishonchliligi, moslashuvchanligi va aqlli muhitning kompleks platformalariga integratsiyalashuvini yanada oshirish bilan bog‘liq bo‘ladi.

FOYDALANILGAN ADABIYOTLAR RO‘YXATI

1. Jain, A. K., Ross, A., Nandakumar, K. *Introduction to Biometrics*. – London: Springer, 2011. – 312 p.
2. Li, S. Z., Jain, A. K. (Eds.). *Handbook of Face Recognition*. – 2nd ed. – London: Springer, 2011. – 655 p.
3. Zhang, K., Zhang, Z., Li, Z., Qiao, Y. Joint Face Detection and Alignment using Multi-task Cascaded Convolutional Networks // *IEEE Signal Processing Letters*. – 2016. – Vol. 23, No. 10. – P. 1499–1503.
4. Schroff, F., Kalenichenko, D., Philbin, J. FaceNet: A unified embedding for face recognition and clustering // *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition*. – 2015. – P. 815–823.
5. Deng, J., Guo, J., Xue, N., Zafeiriou, S. ArcFace: Additive Angular Margin Loss for Deep Face Recognition // *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition*. – 2019. – P. 4690–4699.

ISSN 3030-3907

6. Taigman, Y., Yang, M., Ranzato, M. A., Wolf, L. DeepFace: Closing the gap to human-level performance in face verification // *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition*. – 2014. – P. 1701–1708.
7. ISO/IEC 19794-5:2011. Information technology – Biometric data interchange formats – Part 5: Face image data. – Geneva: ISO, 2011. – 54 p.
8. Parkhi, O. M., Vedaldi, A., Zisserman, A. Deep face recognition // *British Machine Vision Conference*. – 2015. – P. 1–12.
9. InsightFace: 2D and 3D Face Analysis Project [Электронный ресурс]. – Режим доступа: https://github.com/deepinsight/insightface (дата обращения: 20.10.2025).
10. OpenFace: Free and open-source face recognition with deep neural networks [Электронный ресурс]. – Режим доступа: https://cmusatyalab.github.io/openface/ (дата обращения: 20.10.2025).

ISSN 3030-3907