



<https://doi.org/10.5281/zenodo.20570569>

SHAXSNING BIOMETRIK IDENTIFIKATSIYA TEXNOLOGIYALARI ALGORITMLARI VA ULARNING QO'LLANILISH ISTIQBOLLARI

Melikuziev Hasanjon, Rozaliyev Abdumalik

Fargona davlat texnika universiteti

Annotatsiya: Ushbu maqolada shaxsni biometrik identifikatsiya qilishning asosiy texnologiyalari, algoritmlari va ularning zamonaviy amaliyotdagi o'rni tahlil qilingan. Barmoq izi, yuz, iris va ovoz tanish tizimlari ko'rib chiqilgan bo'lib, ularning ishlash tamoyillari, afzalliklari va kamchiliklari bayon etilgan. Shuningdek, sun'iy intellekt va chuqur o'rganish usullarining biometrik tizimlar samaradorligini oshirishdagi roli, hamda kelajakdagi qo'llanilish istiqbollari muhokama qilingan.

Kalit so'zlar: biometrik identifikatsiya, barmoq izi, yuz tanish, iris tanish, chuqur o'rganish, neyron tarmoq, autentifikatsiya.

KIRISH

Zamonaviy raqamli dunyoda shaxsni ishonchli identifikatsiya qilish masalasi tobora dolzarb ahamiyat kasb etmoqda. An'anaviy parol va PIN-kodlarga asoslangan autentifikatsiya usullari ko'pincha xavfsizlik jihatidan yetarli darajada ishonchli bo'lmasdan, foydalanuvchilarga ham noqulayliklar tug'diradi. Bu muammolarni hal etish maqsadida biometrik identifikatsiya texnologiyalari jadal rivojlanmoqda.

Biometrik identifikatsiya — bu shaxsning o'ziga xos biologik yoki xulq-atvor xususiyatlariga asoslanib uni tanib olish jarayonidir. Mazkur texnologiyalar barmoq izi, yuz tuzilishi, ko'zning iris qatlami, ovoz naqshi, qo'l geometriyasi kabi biometrik belgilardan foydalanadi. Har bir inson uchun noyob bo'lgan bu belgilar, raqamli muhitda ishonchli va qulay autentifikatsiya imkoniyatini beradi.

So'nggi yillarda sun'iy intellekt va kompyuter ko'rish sohasidagi yutuqlar biometrik tizimlarning aniqlik darajasini sezilarli oshirdi. Chuqur o'rganish (deep learning) algoritmlariga asoslangan zamonaviy yuz tanish tizimlari 99,8% gacha aniqlikka erishgan bo'lsa, barmoq izi tahlil qiluvchi tizimlar katta ma'lumotlar bazalarida

millionlab shaxslar ichidan aynan mos keladiganini bir necha soniya ichida topib bera oladi.

Maqolaning maqsadi biometrik identifikatsiya texnologiyalarining asosiy algoritmlarini tahlil qilish, ularning afzalliklari va cheklovlarini aniqlash hamda kelajakdagi rivojlanish yo'nalishlarini belgilashdan iborat.

Biometrik tizimlar odatda ikki asosiy kategoriyaga bo'linadi: fiziologik biometrika va xulq-atvor bimetikasi. Fiziologik biometrika anatomik xususiyatlarga — barmoq izi, yuz, ko'z, qo'l, DNK — asoslansa, xulq-atvor bimetikasi dinamik belgilar — yurish, imzo, klaviatura bosish uslubi — ni o'rganadi.

Barmoq izi tanish algoritmlari. Barmoq izi tanish — eng keng tarqalgan va yaxshi o'rganilgan biometrik texnologiya hisoblanadi. Zamonaviy algoritmlar uchta asosiy yondashuvga tayanadi: minutsiya asosidagi usullar (minutiae-based), naqsh asosidagi usullar (pattern-based) va gibrid usullar. Minutsiya usulida barmoq izining tayanch nuqtalari — soqov uchlari (ridge endings) va bifurkatsiyalar (bifurcations) — aniqlanadi hamda ularning koordinatalari, yo'nalishlari va o'zaro nisbatlari taqqoslanadi. ISO/IEC 19794-2 standartiga muvofiq ishlaydi va NIST BOZORTH3 kabi klassik algoritmlar bunga misol bo'ladi. Chuqur o'rganishga asoslangan zamonaviy yondashuv sifatida VeriFinger 12 va Innovatrics kabi SDK-lardan foydalanib, konvolyutsion neyron tarmoqlar (CNN) barmoq izi tasviri xususiyatlarini avtomatik ajratadi.

Yuz tanish algoritmlari. Yuz tanish texnologiyasi so'nggi o'n yillikda inqilobiy rivojlanishni boshdan kechirdi. Dastlabki algoritmlar — Eigenfaces (1991, Turk va Pentland), Fisherfaces (1997), Local Binary Patterns (LBP) — piksel qiymatlariga asoslangan matematik transformatsiyalardan foydalangan bo'lsa, hozirgi zamonaviy tizimlar chuqur neyron tarmoqlarga tayanadi. DeepFace (Facebook, 2014) va FaceNet (Google, 2015) tizimlari ommaviy ma'lumotlar to'plamlarida insoniy aniqlik darajasiga (97,35%) erishdi. ArcFace (2019) algoritmi esa additivli burchak margini yo'qotish funksiyasidan (additive angular margin loss) foydalanib, LFW benchmark testida 99,83% aniqlikni ta'minladi. Zamonaviy yuz tanish tizimlari 3D yuz modellashtirishni

ham qo'llaydi — bu soyalar, yoritish o'zgarishlari va yuz ifodalariga chidamlilikni oshiradi.

Iris tanish algoritmlari. Ko'z irisi insonning eng noyob biometrik belgisi hisoblanadi — ikki xil ko'zning iris naqshi bir-biriga mos kelish ehtimoli 10^{-78} ga teng. IrisCodes algoritmi (John Daugman, 1993) iris naqshidan 2048 bitli raqamli kod hosil qilish uchun Gabor wavelet transformatsiyasidan foydalanadi. Hamming masofasi orqali taqqoslash milliardlab ma'lumotlar bazasida bir necha millisekund ichida bajariladi. Tirik ko'z aniqlash (liveness detection) muammosi hal etilgandan so'ng — pupilning yorug'likka munosabatini, ko'z yumish dinamikasini kuzatish orqali — iris tizimlarining ishonchliligi yanada oshdi.

Ovoz tanish algoritmlari. Ovoz biometrikasi diapazoni 20 Hz — 20 kHz oralig'idagi akustik xususiyatlarni tahlil qiladi. Asosiy algoritmlar Gaussian Mixture Models (GMM), i-vektor va x-vektor yondashuvlariga tayanadi. Zamonaviy Deep Speaker va SpeakerNet tizimlari Res-Net arxitekturasidan foydalanib, shovqinli sharoitlarda ham yuqori aniqlikni ta'minlaydi. EER (Equal Error Rate) ko'rsatkichi eng yaxshi tizimlarda 0,5% dan past bo'lib, bu texnologiya telefon bankingida va aqlli qurilmalarda keng qo'llanilmoqda.

Har qanday biometrik identifikatsiya tizimi quyidagi asosiy komponentlardan iborat: sensor yoki tasvirga olish qurilmasi, xususiyat ajratuvchi modul (feature extractor), taqqoslov mexanizmi (matcher) va qaror qabul qilish bloki. Ro'yxatga olish (enrollment) bosqichida foydalanuvchining biometrik namunasi olinadi, xususiyatlar ajratiladi va shablon (template) ma'lumotlar bazasiga saqlanadi. Identifikatsiya bosqichida yangi namuna shablonlar bilan taqqoslanib, o'xshashlik ballari hisoblanadi.

Tizimning sifatini baholashda asosiy ko'rsatkichlar sifatida FAR (False Acceptance Rate — yolg'onchi qabul qilish darajasi) va FRR (False Rejection Rate — yolg'on rad etish darajasi) ishlatiladi. Bu ikki ko'rsatkich o'rtasidagi kompromiss ROC-egri chizig'i orqali ifodalanadi. EER nuqtasi — FAR va FRR teng bo'lgan holat —

tizimning umumiy sifatini baholashda standart mezon hisoblanadi. Yuqori xavfsizlik talab qilinadigan tizimlarda FAR 0,001% darajasida ushlab turiladi.

Ko'p modal biometrik tizimlar (multimodal biometrics) bir nechta biometrik modalliklarni birlashtirish orqali yagona tizimlarning kamchiliklarini bartaraf etadi. Misol uchun, barmoq izi va yuz tanishni birgalikda qo'llash tizimning umumiy aniqligini oshiradi hamda aldashga qarshiligini kuchaytiradi. Yig'ish darajasiga ko'ra sensor darajasida, xususiyat darajasida yoki qaror darajasida birlashtirishning turli strategiyalari qo'llaniladi.

Biometrik texnologiyalar hozirda quyidagi asosiy yo'nalishlarda faol qo'llanilmoqda: davlat chegaralari nazorati va milliy identifikatsiya tizimlari; moliyaviy xizmatlar va internet-banking; qurilmalarga kirish va korporativ xavfsizlik; sog'liqni saqlash tizimlari; qonunni muhofaza qilish organlari.

Hindistonning Aadhaar biometrik dasturi dunyodagi eng yirik biometrik tizim bo'lib, 1,3 milliarddan ziyod fuqaroning barmoq izi, iris va yuz ma'lumotlarini o'z ichiga oladi. Bu tizim ijtimoiy nafaqalar taqsimoti, bank xizmatlari va hukumat elektron xizmatlarida qo'llanilmoqda. AQSHning IDENT/NGI tizimi FBI tomonidan boshqarilib, 200 milliondan ortiq shaxsning biometrik ma'lumotlarini saqlaydi. O'zbekistonda ham 2021 yildan boshlab fuqarolarning biometrik ma'lumotlari yagona milliy registrga kiritilmoqda.

Smartfon ishlab chiqaruvchilari biometrik autentifikatsiyani qurilmalarga integratsiya qilishda peshqadamlik qilmoqda. Apple Face ID tizimi 30,000 infraqizil nuqta yordamida 3D yuz xaritasini tuzib, 1:1 000 000 qiymat aldashga qarshilik ko'effitsientiga ega. Qualcomm ultratovushli barmoq izi sensori esa displey ostida ishlash imkoniyatiga ega bo'lib, suyuq va quruq barmoq izilarini ham ishonchli tahlil qila oladi.

Biometrik identifikatsiya sohasining kelajagi bir nechta asosiy yo'nalishlar bo'yicha rivojlanadi. Birinchidan, masofaviy va aloqasiz identifikatsiya — COVID-19 pandemiyasidan so'ng uzoq masofadan yuz va iris tanish tizimlari talab sezilari oshdi.

Gait biometrikasi (yurish tahlili) videokuzatuv kameralaridan insonni masofadan identifikatsiya qilish uchun qo'llanilmoqda.

Ikkinchidan, chuqur soxtalashtirishga (deepfake) qarshi kurash. Generativ raqobatdosh tarmoqlar (GAN) tomonidan yaratilgan sintetik biometrik ma'lumotlar an'anaviy tizimlar uchun jiddiy muammo tug'dirmoqda. Bunga javoban liveness detection va presentation attack detection (PAD) algoritmlarini takomillashtirish bo'yicha faol tadqiqotlar olib borilmoqda. ISO/IEC 30107-3 standarti bu yo'nalishda xalqaro me'yoriy baza vazifasini o'taydi.

Uchinchidan, maxfiylik va ma'lumotlar muhofazasi. GDPR (Yevropa) va boshqa milliy qonunchiliklar biometrik ma'lumotlarni shaxsiy ma'lumotlarning alohida toifasi sifatida ko'rib, ularni qayta ishlashga qattiq talablar qo'ymoqda. Mahalliy qurilmada qayta ishlash (on-device processing) — biometrik shablonlarni markaziy serverga yubormasdan qurilmada saqlash — maxfiylikni ta'minlashning istiqbolli yechimi sifatida ko'rilmoqda. Homomorphic encryption va federated learning usullari biometrik ma'lumotlarni markazlashtirmagan holda tizimlarni o'qitish imkoniyatini beradi.

To'rtinchidan, kvant hisoblash va kriptografik xavfsizlik. Kvant kompyuterlarining rivojlanishi hozirgi RSA va ECC asosidagi kriptografik himoyani zaiflashtirgani uchun post-kvant kriptografiyaga o'tish zarurati biometrik tizimlar uchun ham dolzarb bo'lib qolmoqda. NIST 2024 yilda post-kvant kriptografiya standartlarini tasdiqlagan bo'lib, biometrik tizim ishlab chiqaruvchilari ularni joriy etish jarayonida.

Beshinchidan, etik va ijtimoiy muammolar. Yuz tanish texnologiyasining ommaviy kuzatuvda qo'llanilishi, ba'zi algoritmlarda aniqlangan irqiy va jinsiy tarafkashlik (NIST FRVT tekshiruvda qo'ng'ir terili afrikaliklarni tanishda FAR 10-100 marta yuqori bo'lgani aniqlangan) kabi muammolar texnologiyaning ommaviy joriy etilishida jiddiy to'siqlarni vujudga keltirmoqda. Bu yo'nalishdagi algoritmik adolat tadqiqotlari alohida ilmiy soha sifatida rivojlanmoqda.

Biometrik identifikatsiya texnologiyalari zamonaviy axborot xavfsizligi tizimlarining ajralmas qismiga aylangan. Chuqur o'rganish algoritmlarining tadbir

etilishi tizimlar aniqligini keskin oshirib, ommaviy foydalanishga yo'l ochdi. Barmoq izi, yuz, iris va ovoz tanish modalliklari o'z qo'llanilish sohalarida yetuklik darajasiga erishgan bo'lsa-da, har birining o'ziga xos cheklovlari mavjud.

Kelajak tadqiqotlarining asosiy yo'nalishlari: masofaviy identifikatsiyaning aniqligini oshirish; deepfake hujumlariga qarshi bardoshlilikni ta'minlash; maxfiylikni saqlagan holda ishlash (privacy-preserving biometrics); turli etnik va demografik guruhlar uchun bir xil aniqlikni ta'minlaydigan adolatli algoritmlarni ishlab chiqish.

O'zbekistonda biometrik texnologiyalarni rivojlantirish davlat va xususiy sektorda raqamli transformatsiya dasturlari bilan uzviy bog'liq bo'lib, milliy mutaxassislar tayyorlash, tadqiqot markazlari tashkil etish va xalqaro hamkorliklarni kengaytirish orqali bu sohadagi imkoniyatlardan to'la foydalanish mumkin.

FOYDALANILGAN ADABIYOTLAR

1. Jain, A.K., Ross, A., Prabhakar, S. (2004). An Introduction to Biometric Recognition. *IEEE Transactions on Circuits and Systems for Video Technology*, 14(1), 4–20.
2. Daugman, J. (2004). How iris recognition works. *IEEE Transactions on Circuits and Systems for Video Technology*, 14(1), 21–30.
3. Taigman, Y., Yang, M., Ranzato, M., Wolf, L. (2014). DeepFace: Closing the Gap to Human-Level Performance in Face Verification. *CVPR 2014*.
4. Schroff, F., Kalenichenko, D., Philbin, J. (2015). FaceNet: A Unified Embedding for Face Recognition and Clustering. *CVPR 2015*, 815–823.
5. Deng, J., Guo, J., Xue, N., Zafeiriou, S. (2019). ArcFace: Additive Angular Margin Loss for Deep Face Recognition. *CVPR 2019*, 4690–4699.
6. Maltoni, D., Maio, D., Jain, A.K., Prabhakar, S. (2009). *Handbook of Fingerprint Recognition* (2nd ed.). Springer.
7. NIST. (2022). *Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects*. NISTIR 8280.
8. O'zbekiston Respublikasi Prezidentining «Raqamli O'zbekiston — 2030» strategiyasi to'g'risidagi Farmoni. PF-6079, 2020 yil 5 oktyabr.



9. Ross, A., Jain, A.K. (2003). Information fusion in biometrics. *Pattern Recognition Letters*, 24(13), 2115–2125.
10. ISO/IEC 19794-2:2011. Information technology — Biometric data interchange formats — Part 2: Finger minutiae data.

