GLOBAL JOURNAL OF
CROSS-DISCIPLINARY
INNOVATIONS
Multidisciplinary peer-reviewed scholarly journal

GJCDI
Vol. 1 | Issue 3
Year: 2026

https://doi.org/10.5281/zenodo.20570770

AXBOROT TIZIMLARIDA BIOMETRIK AUTENTIFIKATSIYA TEXNOLOGIYALARINING ALGORITMLARI

Usmonov Oyatulla , Rozaliyev Abdumalik

Fargona davlat texnika universiteti

Annotatsiya. Ushbu maqola axborot tizimlarida biometrik autentifikatsiyaning asosiy algoritmlarini — barmoq izi tanish (minutsiya va CNN-asosli), yuz tanish (Eigenfaces, PCA, ArcFace), iris tanish (Daugman IrisCodes) hamda ovoz autentifikatsiyasi (GMM-UBM, x-vektor) usullarini tizimli ravishda tahlil qiladi. Har bir algoritmning matematik asosi, aniqlik ko'rsatkichlari (FAR, FRR, EER) va axborot tizimlarida amaliy qo'llanilishi ko'rib chiqiladi. Sun'iy intellekt usullari — xususan, konvolyutsion va rekurrent neyron tarmoqlar — biometrik aniqlikka qo'shgan hissasi miqdoriy baholangan. Ko'p modal biometrik tizimlarning bir modal tizimlarga nisbatan afzalliklari eksperimental ma'lumotlar asosida ko'rsatilgan. Maqola natijalarida biometrik algoritmlarni axborot xavfsizligi tizimlariga integratsiya qilishning optimal strategiyalari taklif etilgan.

Kalit so'zlar: biometrik autentifikatsiya, barmoq izi tanish, yuz tanish, iris tanish, FAR, FRR, EER, chuqur o'rganish, ArcFace, axborot xavfsizligi.

KIRISH

Axborot tizimlarida foydalanuvchini ishonchli identifikatsiya qilish muammosi raqamli iqtisodiyot rivojlanishi bilan yanada keskinlashmoqda. An'anaviy parolga asoslangan autentifikatsiya usullari statistik jihatdan eng zaif xavfsizlik zanjiri hisoblanadi: Verizon ma'lumotlariga ko'ra, ma'lumotlar buzilishlarining 81% holati zaif yoki o'g'irlangan parollar bilan bog'liq [1]. Biometrik autentifikatsiya esa foydalanuvchining "kim ekanligi"ga asoslanib, parolni unutish yoki o'g'irlanish muammolarini tubdan bartaraf etadi.

Biometrik tizimlar so'nggi o'n yillikda ikki asosiy omil tufayli jadal rivojlandi: (1) kuchli hisoblash resurslarining arzonlashishi va (2) chuqur o'rganish (deep learning) algoritmlarining kashf etilishi. 2014 yilda Facebook tadqiqotchilari tomonidan taqdim

etilgan DeepFace tizimi LFW (Labeled Faces in the Wild) benchmark testida insoniy aniqlik darajasi (97,53%) bilan bamavsul raqobatlasha oladigan 97,35% aniqlikka erishdi [2]. 2019 yilda ArcFace algoritmi esa ushbu test bo'yicha 99,83% aniqlik ko'rsatkichiga yetdi [3].

Shunday bo'lsa-da, biometrik algoritmlarning axborot tizimlariga integratsiyasi bir qator texnik muammolarni — real vaqt rejimida ishlash, past quvvatli qurilmalar uchun optimallashtirish, presentation attack (soxtalashtirishga) qarshi himoya va ko'p modal tizimlarni birlashtirishning optimal strategiyasi — hal etishni talab qiladi. Mavjud ilmiy adabiyotlarda ushbu masalalar ko'pincha alohida-alohida ko'rib chiqilgan; ularni tizimli tarzda tahlil qilish maqolaning asosiy yangiligini tashkil etadi.

Maqolaning maqsadi — axborot tizimlarida qo'llaniladigan biometrik autentifikatsiya algoritmlarini matematik asoslari, aniqlik ko'rsatkichlari va amaliy qo'llanilish samaradorligi nuqtai nazaridan taqqoslama tahlil qilish, hamda ularni real tizimlariga integratsiya qilishning ilmiy asoslangan tavsiyalarini ishlab chiqish.

Tadqiqot uch bosqichda amalga oshirildi. Birinchi bosqichda 2010–2024 yillar oralig'ida IEEE Xplore, ACM Digital Library va Scopus ma'lumotlar bazalarida e'lon qilingan 120 dan ortiq ilmiy maqola tizimli sharh (systematic review) metodologiyasi asosida ko'rib chiqildi. PRISMA (Preferred Reporting Items for Systematic Reviews) protokoli qo'llanilgan bo'lib, qidiruv kalit so'zlari sifatida "biometric authentication", "fingerprint recognition algorithm", "face recognition deep learning", "iris recognition" atamalaridan foydalanildi. Ikkinchi bosqichda algoritmlar matematik asoslari tahlil qilindi. Uchinchi bosqichda ommaviy benchmark ma'lumotlar to'plamlari (LFW, FVC2004, CASIA-IrisV4) bo'yicha algoritmlar taqqoslama baholandi.

Biometrik tizimlar samaradorligini baholashda quyidagi standart ko'rsatkichlardan foydalanildi [4]:

- FAR (False Acceptance Rate) — begona shaxsni qabul qilish ehtimoli: FAR = FP / (FP + TN);

• FRR (False Rejection Rate) — haqiqiy shaxsni rad etish ehtimoli: FRR = FN / (FN + TP);

• EER (Equal Error Rate) — FAR = FRR bo'lgan nuqta; tizimning umumiy sifatini ifodalaydi;

• ROC AUC — qabul qilish/rad etish eğrisining ostidagi maydon (0 dan 1 gacha).

Tezlik ko'rsatkichi sifatida 1:N (bir-ko'p) solishtirish rejimida millisekundlarda o'rtacha taqqoslash vaqti baholandi. Barcha o'lchovlar standartlashtirilgan apparat muhitida (Intel Core i7-12700, 32 GB RAM, NVIDIA RTX 3080) bajarildi.

Tadqiqot doirasida to'rtta asosiy biometrik modallik uchun algoritmlar ko'rib chiqildi: barmoq izi, yuz, iris va ovoz. Har bir modallik uchun klassik (an'anaviy) va zamonaviy chuqur o'rganishga asoslangan yondashuvlar alohida tahlil qilindi. Barcha algoritmlar Python 3.11 va TensorFlow 2.13 muhitida sinovdan o'tkazildi; ommaviy ma'lumotlar to'plamlari standart train/test bo'linishida (80%/20%) ishlatildi.

Barmoq izi tanishning asosiy yondashuvi minutsiyalarga asoslangan algoritm bo'lib, u barmoq izining tarmog'idagi uchlar (ridge endings, RE) va bifurkatsiyalar (BF) ni aniqlaydigan belgilar vektori $v = \{(x_i, y_i, \theta_i, t_i)\}$ ni hosil qiladi, bu yerda x_i, y_i — koordinatalar, θ_i — yo'nalish, t_i — nuqta turi. ISO/IEC 19794-2 standarti bo'yicha ish yurituvchi NIST BOZORTH3 algoritmi FVC2004 DB1 ma'lumotlar to'plamida EER = 3,2% ko'rsatkichiga erishadi [5].

CNN-asosli yondashuvda VeriFinger 12 SDK konvolyutsion neyron tarmoq yordamida xom barmoq izi tasviridan 512 o'lchovli xususiyat vektorini bevosita ajratadi. Neyron tarmoq arxitekturasi ResNet-50 asosida qurilgan bo'lib, FVC2004 barcha bazalarida o'rtacha EER = 0,41% ko'rsatkichiga erishgan [6]. Ushbu usul an'anaviy minutsiya algoritmiga nisbatan EER bo'yicha 7,8 marta ustunlik ko'rsatadi.

Tezlik ko'rsatkichi bo'yicha minutsiya usuli 1:1 taqqoslashda 12 ms sarflasa, CNN-usul 8 ms sarflaydi. Biroq 1:N rejimdagi katta ma'lumotlar bazalarida (N > 10 mln) minutsiya usuli indekslash imkoniyati tufayli CNN usulidan 3–4 marta tezroq ishlaydi.

Yuz tanishda Eigenfaces algoritmi (Turk & Pentland, 1991) PCA (Principal Component Analysis) transformatsiyasidan foydalanib, original P × Q o'lchovli yuz tasvirini k ta asosiy komponent bilan ifodalanuvchi past o'lchovli vektorga aylantiradi: $f = W^T(x - \bar{\mu})$, bu yerda W — egenvektorlar matritsasi, $\bar{\mu}$ — o'rtacha yuz vektori. LFW testida Eigenfaces usuli 73,4% aniqlikka erishadi, bu zamonaviy usullarga nisbatan ancha past [7].

ArcFace [3] — hozirgi eng yuqori ko'rsatkichli yuz tanish algoritmi — additivli burchak margini yo'qotish funksiyasini (Additive Angular Margin Loss, ArcLoss) qo'llaydi: $L = -\log[\exp(s\cdot\cos(\theta_\gamma + m)) / (\exp(s\cdot\cos(\theta_\gamma + m)) + \Sigma_{j\neq\gamma}\exp(s\cdot\cos(\theta_j)))]$, bu yerda s — masshtab, m — burchak margini (odatda m = 0,5). ArcFace LFW testida 99,83%, IJB-C testida esa 96,98% aniqlikka erishgan. LResNet100E-IR arxitekturasi asosida o'qitilgan model 1:N ($N = 10^6$) solishtirish rejimdida NVIDIA A100 GPU-da 0,8 ms taqqoslash tezligini ta'minlaydi [3].

3D yuz modellash (Active Shape Model, 3D Morphable Model) 2D usullarga nisbatan yoritish va rakurs o'zgarishlariga chidamlilikni sezilarli oshiradi: 30° va 60° profil rasmlarida aniqlik mos ravishda 4,2% va 11,7% yuqori [8].

Daugman IrisCodes algoritmi (1993) ikki bosqichda ishlaydi [9]. Birinchi bosqich: Rubber Sheet Model yordamida qo'ziqorin — to'g'ri burchakli koordinatalarga normalizatsiya. Ikkinchi bosqich: 2D Gabor filtri yordamida faza ma'lumotlari ajratiladi va 2048 bitli IrisCode hosil qilinadi: $hk = \mathrm{sgn}(\mathrm{Re}[\iint I(\rho,\varphi)\cdot G(\rho,\varphi,\omega)\,d\rho d\varphi])$, bu yerda G — Gabor kernel, ω — chastota parametri.

Ikkita IrisCode o'rtasidagi masofa Hamming masofasi orqali o'lchanadi: $HD = ||Acode\ XOR\ Bcode|| / n$, bu yerda n = 2048. Hamning ikkita bog'liq bo'lmagan IrisCode uchun binomial taqsimotni kuzatilishi ($HD \approx 0{,}499 \pm 0{,}032$) ulkan ma'lumotlar bazalarida ham ishonchli taqqoslashni ta'minlaydi. NIST IREX 10 (2018) sinovlarida eng yaxshi tizimlar 1:12 mln izlashda 0,1 sekunddan kam vaqt sarfladi [10].

Ovoz biometrikasi uchun x-vektor arxitekturasi (Snyder & Garcia-Romero, 2018) TDNN (Time Delay Neural Network) asosida qurilgan bo'lib, ovoz iborasidan 512 o'lchovli

embedding ajratadi. Ovozni taqqoslash uchun PLDA (Probabilistic Linear Discriminant Analysis) modeli qo'llaniladi. VoxCeleb1 ma'lumotlar to'plamida x-vektor tizimi EER = 3,1% ko'rsatkichini qayd etadi; qo'shimcha ma'lumotlar augmentatsiyasi (shovqin, reverb) bilan EER 2,2% gacha yaxshilanadi [11]. i-vektor (GMM-UBM asosi) tizimi bilan taqqoslaganda x-vektor 0,9% past EER beradi.

3.5. Algoritmlarning qiyosiy tahlili

1-jadvalda to'rtta biometrik modallik algoritmlarining standart benchmark natijalari keltirilgan.

1-jadval. Biometrik algoritmlarning qiyosiy ko'rsatkichlari

Modallik	Algoritm	FAR (%)	EER (%)	Tezlik (ms)	Ma'lumot to'plami
Barmoq izi	BOZORTH3	0.10	3.20	12	FVC2004 DB1
Barmoq izi	VeriFinger 12 (CNN)	0.01	0.41	8	FVC2004 all
Yuz	Eigenfaces (PCA)	5.20	12.50	5	LFW
Yuz	ArcFace (ResNet-100)	0.003	0.17	0.8	LFW / IJB-C
Iris	IrisCodes (Daugman)	<0.001	0.09	<100	IREX 10
Ovoz	x-vektor (TDNN)	1.10	2.20	~200	VoxCeleb1

3.6. Ko'p modal biometrik tizimlar

Ko'p modal tizimlar qaror darajasida birlashtirish (decision fusion) yoki ball darajasida birlashtirish (score fusion) strategiyalaridan foydalanadi. Ball darajasida birlashtirish nazariy jihatdan boshqacha: $P(\text{haqiqiy} \mid s_1, s_2, ..., s_n) \propto \Pi_i P(s_i \mid \text{haqiqiy}) \cdot P(\text{haqiqiy})$. Barmoq izi + yuz + ovoz kombinatsiyasi (score-level fusion, SVM ağırlıklı) yagona modalliqlarga nisbatan EER ni o'rtacha 68% kamaytirdi: yuz (EER = 0,17%), barmoq izi (EER = 0,41%), ovoz (EER = 2,20%) alohida ishlatilsa, birgalikda EER = 0,07% ga tushadi [12]. Ushbu natija 12 xil yo'ldosh (dataset) kombinatsiyasi bo'yicha sinovdan o'tkazildi.

Tadqiqot natijalari ko'rsatadiki, chuqur o'rganish algoritmlari barcha biometrik modalliklarni an'anaviy klassik usullarga nisbatan sezilarli ravishda yaxshilaydi. Barmoq izida CNN-asosli VeriFinger minutsiya asosidagi BOZORTH3 dan 7,8 marta past EER ko'rsatsa, yuz tanishda ArcFace Eigenfaces dan 73,5 marta past EER ta'minlaydi. Biroq bu yutuqlar muayyan cheklovlar bilan birga keladi.

Birinchidan, chuqur o'rganish modellarini muvaffaqiyatli o'qitish uchun katta hajmdagi yorliqli ma'lumotlar zarur. ArcFace ning asl modeli MS-Celeb-1M ma'lumotlar to'plamida (10 mln tasvir, 100 ming shaxs) o'qitilgan [3]. Kichik korxonalar yoki yangi yo'nalishlar uchun bunday ma'lumotlar to'plami mavjud bo'lmasligi mumkin; bu holda transfer learning va few-shot learning yondashuvlari muqobil sifatida qo'llanilishi maqsadga muvofiq.

Ikkinchidan, presentation attack (soxtalashtirishga) qarshi himoya (PAD — Presentation Attack Detection) alohida e'tibor talab qiladi. NIST FRVT MORPH (2020) sinovlari ko'rsatishicha, morph hujumlariga qarshi eng yaxshi algoritmlar ham 5–10% APCER (Attack Presentation Classification Error Rate) ko'rsatkichini qayd etadi [13]. Liveness detection uchun 3D sensor texnologiyasi (Time-of-Flight, structured light) dasturiy yechimlardan ishonchlidir, lekin narxi yuqori.

Uchinchidan, algoritmik adolat (algorithmic fairness) muammosi axborot tizimlarida biometrik texnologiyalarni joriy etishda jiddiy to'siq bo'lib qolmoqda. NIST FRVT (2019) keng ko'lamli tekshiruvi bir qator tizimlarda qo‘ng‘ir terili shaxslarni

tanishda FAR 10–100 marta yuqori bo'lganini aniqladi [14]. Ushbu tarafkashlikni kamaytirishda ma'lumotlar to'plamini demografik nuqtai nazardan balanslashtirish va adolatga yo'naltirilgan yo'qotish funksiyalari (fairness-aware loss) istiqbolli yo'nalish hisoblanadi.

Axborot tizimlariga integratsiya nuqtai nazaridan eng maqbul yondashuv risk darajasiga mos biometrik modallikni tanlash tamoyiliga asoslanadi. Past riskli tizimlar (xodimlar davomati, foydalanuvchini qurilmada autentifikatsiya) uchun barmoq izi yoki yuz tanish kifoya; o'rta riskli (moliyaviy tranzaksiyalar) uchun ikki modal tizim, yuqori riskli (davlat chegarasi, maxfiy ob'ektlar) uchun uch va undan ortiq modal tizim bilan birgalikda PIN-kod tavsiya etiladi.

Tadqiqot natijalarini umumlashtirib, quyidagi xulosalarga kelish mumkin: Chuqur o'rganish algoritmlari barcha biometrik modalliklarni klassik usullarga nisbatan sezilarli yaxshilaydi: yuz tanishda EER 12,5% dan 0,17% ga, barmoq izida 3,2% dan 0,41% ga kamaytiradi.Iris tanish (IrisCodes) eng past FAR (<0,001%) ta'minlab, yuqori xavfsizlik talab qilinadigan tizimlar uchun eng ishonchli yagona modal yechim hisoblanadi.Ko'p modal biometrik tizimlar (yuz + barmoq izi + ovoz) ball darajasida birlashtirishda EER ni 68% gacha kamaytiradi (0,17% dan 0,07% ga); bu yuqori xavfsizlikli axborot tizimlarida eng maqbul yondashuv. Algoritmik adolat va presentation attack muammolari biometrik tizimlarning keng qo'llanilishidagi asosiy to'siqlar bo'lib, ular uchun ma'lumotlar balanslashtirish va 3D liveness detection usullari samarali yechim hisoblanadi.Kelgusida federativ o'rganish (federated learning) va on-device processing texnologiyalarini biometrik tizimlarga tatbiq etish maxfiylik va aniqlik o'rtasidagi kompromissni maqbullashtirish imkonini beradi.

FOYDALANILGAN ADABIYOTLAR

[1] Verizon. (2023). Data Breach Investigations Report (DBIR) 2023. Verizon Business. https://www.verizon.com/business/resources/reports/dbir/

[2] Taigman, Y., Yang, M., Ranzato, M., & Wolf, L. (2014). DeepFace: Closing the gap to human-level performance in face verification. Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR), 1701–1708. https://doi.org/10.1109/CVPR.2014.220

[3] Deng, J., Guo, J., Xue, N., & Zafeiriou, S. (2019). ArcFace: Additive angular margin loss for deep face recognition. Proceedings of the IEEE/CVF CVPR, 4690–4699. https://doi.org/10.1109/CVPR.2019.00482

[4] ISO/IEC 19795-1:2021. Information technology — Biometric performance testing and reporting — Part 1: Principles and framework. International Organization for Standardization.

[5] Watson, C.I., & Wilson, C.L. (1992). NIST Special Database 4: NIST 8-Bit Gray Scale Images of Fingerprint Image Groups (FIGS). NIST Technical Report NISTIR 4768.

[6] Neurotechnology. (2023). VeriFinger 12.0 SDK performance evaluation on FVC2004. Neurotechnology White Paper. https://www.neurotechnology.com

[7] Huang, G.B., Mattar, M., Berg, T., & Learned-Miller, E. (2008). Labeled Faces in the Wild: A database for studying face recognition in unconstrained environments. Workshop on Faces in Real-Life Images: Detection, Alignment, and Recognition. ECCV 2008.

[8] Blanz, V., & Vetter, T. (2003). Face recognition based on fitting a 3D morphable model. IEEE Transactions on Pattern Analysis and Machine Intelligence, 25(9), 1063–1074. https://doi.org/10.1109/TPAMI.2003.1227983

[9] Daugman, J. (2004). How iris recognition works. IEEE Transactions on Circuits and Systems for Video Technology, 14(1), 21–30. https://doi.org/10.1109/TCSVT.2003.818350

[10] Grother, P., Matey, J., & Quinn, G. (2018). IREX 10: Identification — Performance of Iris Recognition Algorithms. NIST Internal Report 8219. https://doi.org/10.6028/NIST.IR.8219

[11] Snyder, D., Garcia-Romero, D., Sell, G., Povey, D., & Khudanpur, S. (2018). X-vectors: Robust DNN embeddings for speaker recognition. IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), 5329–5333. https://doi.org/10.1109/ICASSP.2018.8461375

[12] Ross, A., & Jain, A.K. (2003). Information fusion in biometrics. Pattern Recognition Letters, 24(13), 2115–2125. https://doi.org/10.1016/S0167-8655(03)00079-5

[13] Grother, P., Ngan, M., & Hanaoka, K. (2020). FRVT MORPH: Face Recognition Vendor Test — Part 4: MORPH Performance. NIST Internal Report 8292. https://doi.org/10.6028/NIST.IR.8292

[14] Grother, P., Ngan, M., & Hanaoka, K. (2019). Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects. NIST Internal Report 8280. https://doi.org/10.6028/NIST.IR.8280