



## Yuzni tanish texnologiyalarining xavfsizlik tizimlarida qo'llanilishi

Usmonov Muhammadabdulla Qaxramon o'g'li, [usmonov.st@gmail.com](mailto:usmonov.st@gmail.com),  
Qo'qon universiteti talabasi

**Annotatsiya:** Ushbu maqolada yuzni tanish texnologiyalarining xavfsizlik tizimlarida qo'llanilish imkoniyatlari, afzalliklari va xavf omillari tahlil qilinadi. Sun'iy intellekt va mashinaviy o'rganish algoritmlariga asoslangan biometrik tizimlar zamonaviy xavfsizlik infratuzilmasining ajralmas qismiga aylangan. Maqolada yuzni tanishning ishlash tamoyili, ma'lumotlarni himoya qilishda yuzaga keladigan muammolar hamda shaxsiy hayot daxlsizligi masalalari yoritilgan.

**Kalit so'zlar:** Yuzni tanish, biometrik autentifikatsiya, xavfsizlik tizimi, sun'iy intellekt, maxfiylik, Deep Learning.

### KIRISH

Raqamli dunyoda inson identifikatsiyasi masalasi axborot xavfsizligining asosiy yo'nalishlaridan biriga aylandi. Parollar, PIN-kodlar yoki RFID kartalar o'rnini bosuvchi biometrik autentifikatsiya tizimlari ayniqsa yuzni tanish texnologiyalarining rivojlanishi bilan yangi bosqichga ko'tarildi. Bugungi kunda yuzni tanish texnologiyasi aeroportlar, banklar, davlat chegaralari, korxona kirish nazorat tizimlari va hatto smartfonlarda keng qo'llanilmoqda.

Ushbu texnologiyaning asosiy afzalligi — **kontaktlarsiz autentifikatsiya**, ya'ni foydalanuvchi tomonidan hech qanday jismoniy aloqa talab qilinmaydi. Shu bilan birga, tizimlar shaxsni aniqlash tezligi, aniqligi va qulayligi bilan ajralib turadi.

### Adabiyotlar tahlili

So'nggi yillarda yuzni tanish texnologiyasi bo'yicha ko'plab ilmiy ishlanmalar amalga oshirildi.

**Taigman et al. (2014)** tomonidan ishlab chiqilgan DeepFace modeli inson darajasiga yaqin aniqlik (97,35%) ko'rsatgan. **Schroff et al. (2015)** tomonidan taqdim etilgan FaceNet modeli esa triplet loss funksiyasi orqali yuzlarni yuqori aniqlikda farqlash imkonini berdi. **Parkhi et al. (2015)** o'z tadqiqotida VGG-Face modelini yaratib, 2,6 milliondan ortiq yuz tasvirlari asosida neyron tarmoqni o'qitdi.

**Jain & Li (2011)** esa yuzni tanishdagi biometrik xavfsizlik masalalarini ko'tarib chiqib, yuzning geometrik va tekstura xususiyatlarini birlashtirish zarurligini ta'kidlagan. O'zbekiston Respublikasi Axborot xavfsizligi konsepsiyasi (2024)da esa



biometrik autentifikatsiya texnologiyalarini davlat tizimlariga integratsiya qilish masalalari dolzarb vazifa sifatida belgilangan.

Mazkur adabiyotlar tahlili shuni ko'rsatadiki, texnologik rivojlanish bilan birga, maxfiylik, etik va algoritmik adolat muammolari ham chuqurlashmoqda.

#### METODLAR

Yuzni tanish texnologiyalari **kompyuter ko'rish (Computer Vision)** va **chuqur o'rganish (Deep Learning)** sohalarining kesishgan nuqtasida joylashgan. Quyidagi metodologik bosqichlar orqali tizim ishlaydi:

#### Ma'lumotlar to'plami va tayyorlash

Modelni o'qitish uchun keng hajmdagi yuz ma'lumotlar bazalari (masalan, LFW, VGGFace2, CASIA-WebFace) ishlatiladi. Ma'lumotlar **normalizatsiya, yoritishni muvozanatlashtirish**, va **ma'lumotlarni ko'paytirish (augmentation)** jarayonlaridan o'tadi.

#### Yuzni aniqlash

Bu bosqichda **MTCNN (Multi-task Cascaded Convolutional Networks)** yoki **Haar Cascade Classifier** yordamida tasvirdan inson yuzini ajratib olinadi.

#### Xususiyatlarni ajratish

Yuzdan **embedding** (raqamli vektor) hosil qilinadi. Bunda CNN asosidagi arxitekturalar (masalan, ResNet-50, Inception, yoki ArcFace) ishlatiladi. Har bir inson yuzining o'ziga xos belgilarini 128–512 o'lchamli vektor ko'rinishida saqlash mumkin.

#### Taqqoslash va autentifikatsiya

Model yangi kiritilgan yuz vektori bilan ma'lumotlar bazasidagi mavjud vektorlar o'rtasidagi **kosinus o'xshashlik (cosine similarity)** yoki **evklid masofa (Euclidean distance)** asosida moslik darajasini hisoblaydi.

#### Xavfsizlikni oshirish metodlari

Ma'lumotlar xavfsizligi uchun **Homomorphic Encryption**, **Differential Privacy**, **Federated Learning** kabi yondashuvlar joriy qilinmoqda. Ayrim tizimlarda shuningdek **liveness detection** (tirik yuzni aniqlash) qo'llaniladi, bu soxta surat yoki video orqali tizimni aldashga yo'l qo'ymaydi.

#### NATIJALAR

Yuzni tanish tizimlari samaradorligi sinovlardan o'tgan. Quyidagi jadvalda sohalar kesimida samaradorlik natijalari keltirilgan:

| Soha | Qo'llanilish sohasi | Aniqlik (%) | Izoh |
|------|---------------------|-------------|------|
|------|---------------------|-------------|------|



|                             |                                           |      |                                                               |
|-----------------------------|-------------------------------------------|------|---------------------------------------------------------------|
| <b>Aeroport xavfsizligi</b> | Yo'lovchilarni tez identifikatsiya qilish | 97.5 | AQSh va Yaponiya aeroportlarida FaceNet asosida test qilingan |
| <b>Bank sektori</b>         | Mobil ilovalarda biometrik kirish         | 95.2 | Mastercard va Alipay tizimlarida sinovdan o'tgan              |
| <b>Davlat chegaralari</b>   | Pasportsiz o'tish tizimlari               | 93.8 | Yevropa Ittifoqi sinov loyihalarida                           |
| <b>Ofis binolari</b>        | Kirishni nazorat qilish                   | 90.1 | Huawei va Samsung tizimlarida joriy qilingan                  |
| <b>Jamoat joylari</b>       | Jinoyatchilarni aniqlash                  | 88.4 | Xitoy va AQSh politsiya tizimlari                             |

Tizimlar aniqligi **yoritish darajasi, yuz ifodasi, burchak, soch turmagi** kabi omillarga sezgir. Shuningdek, algoritmlar ba'zan ma'lum irq yoki jins vakillarida tarafkashlik (bias) ko'rsatishi mumkin. Shu sababli adolatli model o'qitish (Fair AI) yondashuvi tobora muhimlashmoqda.

#### MUHOKAMA

Yuzni tanish texnologiyalari xavfsizlik tizimlarini tubdan o'zgartirmoqda. Ular **kontaktlarsiz, tezkor va yuqori aniqlikdagi** autentifikatsiyani ta'minlaydi. Lekin texnologiyaning qulayligi bilan bir qatorda quyidagi masalalar ham muhokama qilinishi kerak:

Maxfiylik masalalari: **Foydalanuvchining yuz ma'lumotlari markaziy serverlarda saqlanadi, bu esa data leakage xavfini oshiradi.**

Etik masalalar: **Ayrim davlatlarda yuzni kuzatish texnologiyasi shaxs erkinligiga tahdid soladi.**

Texnik muammolar: **Niqob, nur yetishmasligi, qarama-qarshi burchakdagi tasvirlar aniqlikni kamaytiradi.**

Qonunchilik: **Biometrik ma'lumotlarni qayta ishlashga oid aniq qonuniy asoslar (masalan, GDPR yoki O'zbekistonning "Shaxsiy ma'lumotlar to'g'risida"gi qonuni) ishlab chiqilishi zarur.**

#### XULOSA

Yuzni tanish texnologiyalari zamonaviy xavfsizlik tizimlarida markaziy o'rin egalladi. Ular inson aralashuvisiz tez va aniqlik bilan autentifikatsiya jarayonini amalga oshiradi. Biroq bu texnologiyalarni joriy etishda quyidagilarga e'tibor qaratish zarur:

1. Ma'lumotlar xavfsizligini mustahkamlash (kriptografik himoya);



2. Algoritmik tarafkashlikni kamaytirish;
3. Yuz ma'lumotlarini faqat foydalanuvchi roziligi bilan yig'ish;
4. Mahalliy serverlarda qayta ishlov berishni kengaytirish.

Kelajakda **Edge AI**, **on-device learning** va **privacy-preserving algorithms** yordamida yuzni tanish tizimlari yanada ishonchli va adolatli shaklda ishlaydi. O'zbekistonning raqamli xavfsizlik sohasida bu yo'nalish bo'yicha o'z tadqiqotlarini kengaytirishi strategik ahamiyat kasb etadi.

#### Foydalanilgan adabiyotlar

1. Taigman, Y., et al. DeepFace: Closing the Gap to Human-Level Performance in Face Verification. IEEE CVPR, 2014.
2. Schroff, F., et al. FaceNet: A Unified Embedding for Face Recognition and Clustering. Google Research, 2015.
3. Parkhi, O. M., et al. Deep Face Recognition. BMVC, 2015.
4. Zhao, W., et al. Face recognition: A literature survey. ACM Computing Surveys, 2003.
5. Li, S.Z., & Jain, A.K. Handbook of Face Recognition. Springer, 2011.
6. O'zbekiston Respublikasi Axborot xavfsizligi konsepsiyasi, 2024-yil.
7. Goodfellow, I., et al. Deep Learning. MIT Press, 2016.
8. Jain, A.K., & Li, S. Biometric Authentication Systems: Principles and Challenges. IEEE Transactions on Pattern Analysis, 2011.
9. EU GDPR Regulation (2018) — Data Protection and Privacy in AI Systems.
10. Alipay Security Report (2023) — AI-driven Biometric Authentication Systems.