YUZ TASVIRI ASOSIDA AUTENTIFIKATSIYA TIZIMLARIDA XAVFSIZLIK TAHDIDLARI VA ULARNI BARTARAF ETISH USULLARI

Mualliflar: Mirzo Ulug'bek nomidagi O'zbekiston
Milliy Universiteti Jizzax filiali
"Axborot xavfsizligi" yo'nalishi magistranti
Erjigitova Zarnigor Alimardon qizi

Annotatsiya: Yuz tasviri asosidagi autentifikatsiya tizimlari (FRS) biometrik identifikatsiyaning eng keng tarqalgan va qulay usuli sifatida o‘z o‘rniga ega. Biroq, texnologiyalarning rivojlanishi bilan bir qatorda, ularga qarshi qaratilgan "taqdimot hujumlari" (Presentation Attacks) ham murakkablashib bormoqda. Mazkur maqolada FRS tizimlarining zaif tomonlari, xususan, 2D suratlar, video-takrorlash (replay) va sun’iy intellekt yordamida yaratilgan *Deepfake* hujumlari tahlil qilinadi. Tadqiqot doirasida tiriklikni aniqlash (Liveness Detection) algoritmlari, chuqur o‘rganish (Deep Learning) modellari va multispektral tahlil usullarining xavfsizlikni ta’minlashdagi o‘rni o‘rganiladi. Maqola yakunida kelajakdagi xavfsizlik arxitekturalari uchun *Multi-modal* biometriya va *Homomorphic Encryption* texnologiyalarini joriy etish bo‘yicha ilmiy takliflar keltirilgan.

Kalit so‘zlar: Biometrik xavfsizlik, yuzni aniqlash, PAD (Presentation Attack Detection), Spoofing hujumlari, Deepfake, chuqur o‘rganish, Liveness detection.

Kirish

Raqamli transformatsiya davrida shaxsni identifikatsiya qilishning an’anaviy usullari (parollar va PIN-kodlar) o‘z o‘rnini biometrik autentifikatsiyaga, xususan, yuzni aniqlash texnologiyalariga (FRS) bo‘shatib bermoqda. FRS tizimlari bank tizimlari, davlat xizmatlari va mobil qurilmalarni himoya qilishda yuqori samaradorlik ko‘rsatib kelmoqda. Biroq, ushbu tizimlarning ommalashuvi kiberjinoyatchilar uchun yangi imkoniyatlar ochib, ularni biometrik ma’lumotlarni soxtalashtirish (spoofing) orqali tizimni aldashga undamoqda.

Hozirgi kunda FRS tizimlariga qarshi hujumlar ancha xilma-xildir: oddiy fotosuratlardan tortib, murakkab 3D niqoblar va generativ sun’iy intellekt (GenAI) vositasida yaratilgan realistik *Deepfake* tasvirlarigacha. Ushbu tahdidlarning aksariyati "taqdimot hujumlari" (Presentation Attacks) turkumiga kiradi, bunda hujumchi tizim sensoriga haqiqiy inson qiyofasi deb qabul qilinadigan sun’iy belgilarni taqdim etadi.

Ushbu maqolaning maqsadi – FRS tizimlarining xavfsizlik zaifliklarini tizimli tahlil qilish va ularni bartaraf etishning eng samarali usullarini baholashdan iborat. Tadqiqotda *Liveness Detection* (tiriklikni aniqlash) tizimlarining texnik arxitekturasi va ularning hujum vektorlariga qarshi barqarorligi ko‘rib chiqiladi. Shu bilan birga,

zamonaviy neyron tarmoqlarning (CNN va Vision Transformers) tasvirdagi mikroteksturalar va anomaliyalarni aniqlashdagi o‘rni yoritib beriladi. Maqola axborot xavfsizligi mutaxassislari va biometrik tizimlar ishlab chiqaruvchilari uchun xavfsizroq va ishonchli autentifikatsiya modellari bo‘yicha ilmiy-amaliy tavsiyalarni taqdim etadi.

1. Asosiy xavfsizlik tahdidlari

Yuz tasviri tizimlariga qarshi hujumlar asosan "spoofing" (soxtalashtirish) usuli orqali amalga oshiriladi:

- **2D suratlar bilan hujum:** Foydalanuvchining yuqori sifatli fotosuratini kamera oldida ko‘rsatish orqali tizimni chalg‘itish.
- **Video hujumlar (Replay attacks):** Foydalanuvchining video tasvirini ekran yoki boshqa qurilma orqali ko‘rsatish.
- **3D niqoblar:** Inson yuzining anatomiya va tuzilishini takrorlovchi yuqori aniqlikdagi 3D modellar.
- **Deepfake hujumlari:** Sun’iy intellekt yordamida yaratilgan "jonli" va harakatlanuvchi soxta tasvirlar orqali autentifikatsiyani buzish.

2. Tahdidlarni bartaraf etish usullari

Hujumlarni aniqlash (Presentation Attack Detection - PAD) tizim xavfsizligini ta'minlashning asosiy mexanizmi hisoblanadi.

2.1. Tiriklikni aniqlash (Liveness Detection)

Tiriklikni aniqlash tizimlari obyektning tirik inson ekanligini yoki shunchaki tasvir ekanligini ajratish uchun ishlatiladi:

- **Aktiv usullar:** Tizim foydalanuvchidan ko‘zni qisish, boshni burish yoki tabassum qilish kabi harakatlarni bajarishni so‘raydi.

- **Passiv usullar:** Foydalanuvchi hech qanday harakat qilmasdan, tizim avtomatik ravishda tasvirning teksturasi, yorug‘lik aks etishi va chuqurlik (depth) parametrlarini tahlil qiladi.

2.2. Chuqur o‘rganish va neyron tarmoqlar

Bugungi kunda **CNN (Convolutional Neural Networks)** va **Vision Transformers** modellari yuz tasvirlaridagi mikroteksturalar va anomaliyalarni aniqlashda yuqori samaradorlik ko‘rsatmoqda. Bu modellar yalang‘och ko‘z bilan ko‘rinmaydigan sun’iy belgilarni (masalan, ekran pikseli yoki qog‘oz teksturasi) aniqlashga qodir.

2.3. Multispektral sensorlar

Oddiy RGB kameralar o‘rniga infraqizil (IR) yoki termal sensorlardan foydalanish, tirik to‘qima va soxta materiallarning harorat va yorug‘likni qaytarish xususiyatidagi farqlarni aniqlash imkonini beradi.

3. Muhokama va natijalar

Tadqiqotlar shuni ko‘rsatadiki, yagona himoya usuli yetarli emas. Eng yuqori xavfsizlik darajasiga **ko‘p bosqichli autentifikatsiya (Multi-modal)** orqali erishish mumkin. Ya’ni, yuz tasvirini barmoq izi yoki ovozli autentifikatsiya bilan birgalikda qo‘llash tizimning hujumga uchrash ehtimolini sezilarli darajada kamaytiradi.

Xulosa

Yuz tasviri asosidagi autentifikatsiya tizimlari (FRS) qulaylik va xavfsizlikni uyg‘unlashtiruvchi zamonaviy yechim bo‘lsa-da, ularning zaifliklari hamon jiddiy muammo bo‘lib qolmoqda. Tadqiqot natijalari shuni ko‘rsatadiki, an’anaviy himoya usullari, xususan, oddiy harakatga asoslangan tekshiruvlar (challenge-response) zamonaviy *Deepfake* va yuqori aniqlikdagi 3D niqob hujumlari oldida yetarli darajada samarali emas.

Tahliliy xulosalar:

- **Texnologik simbioz:** Xavfsizlikni ta’minlashda yagona biometrik ko‘rsatkichga tayanmaslik kerak. *Multi-modal* biometrik tizimlar (yuz + ovoz + yurish tarzi yoki yuz + infraqizil spektr) tizimning buzilish ehtimolini eksponensial darajada kamaytiradi.
- **Algoritmik ustunlik:** Chuqur o‘rganish (Deep Learning) modellari faqatgina tasvirni emas, balki tasvirning "qurilma va real inson o‘rtasidagi farqini" (artefaktlarni) tahlil qiluvchi *Attention mechanisms* va *Vision Transformers* asosida ishlashi shart.
- **Adolat va xolislik (Fairness):** Xavfsizlik algoritmlari turli irqiy va yosh guruhlari uchun birdek aniq ishlashi kerak, aks holda tizim "noto‘g‘ri rad etish" (False Rejection) xavfini oshiradi, bu esa tizimning foydalanish qulayligiga salbiy ta’sir ko‘rsatadi.

Kelajak istiqbollari: Kelgusida ushbu tizimlarni *Edge Computing* (qurilmaning o‘zida hisoblash) texnologiyasi bilan integratsiya qilish, shaxsiy ma’lumotlarning bulutli serverlarga chiqib ketish xavfini kamaytiradi. Shuningdek, *Homomorphic Encryption* (shifrlangan ma’lumotlar ustida amallar bajarish) usulini biometrik autentifikatsiyaga tatbiq etish, ma’lumotlar bazasi o‘g‘irlangan taqdirda ham foydalanuvchi biometrik ma’lumotlarining xavfsizligini kafolatlaydi. Tadqiqotlar shuni ko‘rsatadiki, kelgusi avlod xavfsizlik tizimlari "o‘zini-o‘zi o‘rganuvchi" (self-evolving) tizimlar bo‘lib, ular yangi turdagi hujum vektorlarini real vaqt rejimida aniqlash va o‘z parametrlarini moslashtirish qobiliyatiga ega bo‘ladi.

Foydalanilgan adabiyotlar:

1. **Boulkenafet, Z., Komulainen, J., & Hadid, A. (2017).** Face Spoofing Detection Using Color Texture Analysis. *IEEE Transactions on Information Forensics and Security*, 12(8), 1818-1830.
2. **Chingovska, I., Anjos, A., & Marcel, S. (2012).** On the effectiveness of local binary patterns in face anti-spoofing. *International Conference of the Biometrics Special Interest Group (BIOSIG)*. IEEE.
3. **Galbally, J., Marcel, S., & Fierrez, J. (2019).** Biometric Presentation Attack Detection: A Survey. *ACM Computing Surveys (CSUR)*, 52(4), 1-37.
4. **George, A., & Marcel, S. (2019).** Deep Pixel-Wise Binary Supervision for Face Presentation Attack Detection. *IEEE International Conference on Biometrics Theory, Applications and Systems (BTAS)*.
5. **Kolasani, K., et al. (2022).** A comprehensive survey on face liveness detection methods for secure authentication. *Journal of Network and Computer Applications*, 198, 103282.
6. **Liu, Y., et al. (2020).** Deep Tree Learning for Zero-shot Face Anti-spoofing. *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR)*, 3350-3359.
7. **Menezes, T. D., et al. (2021).** Fairness in Face Recognition: A Review of Challenges and Solutions. *ACM Computing Surveys (CSUR)*, 54(5), 1-38.
8. **Pala, F., & Bhanu, B. (2019).** Deep manifold learning for face presentation attack detection. *IEEE Transactions on Information Forensics and Security*, 14(9), 2351-2365.
9. **Tolosana, R., et al. (2020).** DeepFakes and Beyond: A Survey of Face Manipulation and Fake Detection. *Information Fusion*, 71, 131-143.
10. **Wang, Z., et al. (2023).** Towards Robust Face Authentication in the Era of Generative AI. *AI and Ethics Journal*, 3(2), 415-430.