BIOMETRIK IDENTIFIKATSIYA TIZIMLARIDA SOXTALASHTIRISH HUJUMLARINI ANIQLASHNING MASHINALI O‘QITISHGA ASOSLANGAN USULLARI VA ALGORITMLARI

Muhammad al-Xorazmiy nomidagi Toshkent
Axborot Texnologiyalari Universiteti katta o‘qituvchisi
Irmuxamedova Navruza Abdullajonovna
Muhammad al-Xorazmiy nomidagi Toshkent
Axborot Texnologiyalari Universiteti 1-kurs magistranti
Ishonqulova Shaxlo Abdugapir qizi

Annotatsiya. *Mazkur maqolada biometrik identifikatsiya tizimlarida soxtalashtirish hujumlarini aniqlash masalasi va bunda mashinali o‘qitish algoritmlaridan foydalanish imkoniyatlari tahlil qilinadi. Tadqiqot yuz tasviri asosidagi tekshiruvni misol qilib oladi: bosma fotosurat yoki elektron ekranda ko‘rsatilgan tasvir orqali tizimni chalg‘itishga urinishlar biometrik taqdimot hujumlariga misol bo‘la oladi. Ushbu ishda “taqdimot hujumi” atamasi biometrik sensor oldiga haqiqiy foydalanuvchining biometrik xususiyatini soxtalashtiruvchi namuna taqdim etish holatini anglatadi; “soxtalashtirish hujumi” iborasi shu mazmunda qo‘llanadi. Mavjud ilmiy ishlar va xalqaro standartga tayangan holda, bunday hujumlarni aniqlash jarayonining asosiy bosqichlari, klassik tasniflagichlar va chuqur o‘qitish yondashuvlari ko‘rib chiqiladi. Tayanch vektorlar mashinasi (SVM), Random Forest hamda konvolyutsion neyron tarmoq (CNN) algoritmlarini bir xil ma’lumotlar va baholash mezonlari asosida taqqoslash taklif etiladi. Tezisda hali bajarilmagan tajriba natijalari keltirilmaydi; aniqlik (accuracy), precision, recall, F1-mezon va ROC-AUC kabi ko‘rsatkichlar hamda APCER, BPCER va ACER kabi PAD metrikalarini keyingi tajribada qo‘llash uchun tavsiya etiladi.*

Kalit so‘zlar: *biometrik identifikatsiya, biometrik taqdimot hujumi, soxtalashtirish hujumini aniqlash, mashinali o‘qitish, SVM, Random Forest, CNN, yuz tasviri, biometrik xavfsizlik, APCER, BPCER, ACER.*

Biometrik identifikatsiya shaxsni uning fiziologik yoki xulq-atvor belgilariga qarab tanib olishga asoslanadi. Axborot tizimlarida identifikatsiya va autentifikatsiya foydalanuvchining kimligini tekshirish jarayonining muhim qismlari hisoblanadi[1]. Biroq biometrik belgi mavjudligi tizimni avtomatik ravishda hujumlardan himoyalanganligini avtomatik ravishda kafolatlamaydi. Tizimga haqiqiy foydalanuvchining biometrik belgisini taqlid qiluvchi material taqdim etilishi mumkin.

Yuzni tanish tizimlariga qarshi keng o‘rganilgan misollardan biri bosma fotosurat yoki elektron ekran orqali tasvirni ko‘rsatishdir. Chingovska, Anjos va Marcel tadqiqotida Local Binary Patterns (LBP) kabi tekstura xususiyatlari bosma fotosuratlar hamda ekranlarda ko‘rsatilgan foto va videolarni farqlash uchun tekshirilgan; mualliflar keng turdagi hujumlar sharoitida natija mukammal emasligini qayd etgan [2]. Bu holat bitta xususiyat yoki bitta

sinov ssenariysiga tayanish o‘rniga, bir nechta hujum turini qamrab oluvchi baholash zarurligini ko‘rsatadi.

ISO/IEC 30107-3:2023 standarti biometrik taqdimot hujumlarini aniqlash mexanizmlarini baholash va sinov natijalarini hisobot qilish tamoyillarini belgilaydi [3]. Shu sababli modelni faqat o‘qitish natijasi bilan baholash yetarli emas: test ma’lumotlari, hujum turlari va baholash sharoitlari aniq ko‘rsatilishi lozim.

Tadqiqotning maqsadi — biometrik identifikatsiya tizimlarida soxtalashtirish hujumlarini aniqlash uchun mashinali o‘qitishga asoslangan usullarni o‘rganish va ularni qiyosiy baholashga mo‘ljallangan metodikani ishlab chiqish.

Tadqiqot vazifalari:

- biometrik taqdimot hujumlari va ularni aniqlash bo‘yicha ilmiy adabiyotlarni tahlil qilish;
- tadqiqot chegarasini belgilash va yuz tasviri misolida ko‘rib chiqiladigan hujum turlarini aniqlash;
- SVM, Random Forest va CNN algoritmlarining qo‘llanish imkoniyatlari hamda cheklovlarini taqqoslash;
- ma’lumotlarni tayyorlash, o‘qitish, validatsiya va mustaqil sinov jarayonlari uchun metodikani belgilash;
- natijalarni bir nechta metrika orqali baholash va dalillarga tayangan tavsiyalar ishlab chiqish.

Klassik mashinali o‘qitish yondashuvida dastlab tasvir yoki signaldan xususiyatlar ajratiladi, so‘ng tasniflagich namunani haqiqiy yoki soxta sinfiga kiritadi. LBP kabi tekstura tavsiflagichlari tasvirdagi mahalliy naqshlarni ifodalash uchun ishlatilishi mumkin [2]. SVM xususiyatlar fazosida sinflarni ajratishga asoslanadi [4], Random Forest esa bir nechta qaror daraxtlari natijalarini birlashtiradi [5]. CNN tasvirdan xususiyatlarni avtomatik o‘rganishi mumkin [6], lekin uning natijasi ma’lumotlar sifati, model tuzilishi va o‘qitish sharoitiga bog‘liq. Shuning uchun ushbu algoritmlardan birini oldindan eng yaxshi deb e’lon qilish emas, balki bir xil sharoitda tekshirish ilmiy jihatdan to‘g‘riroqdir.

Tajriba uchun haqiqiy va soxta namunalarni o‘z ichiga olgan, foydalanish shartlari aniq bo‘lgan ma’lumotlar to‘plami tanlanishi kerak. Bunday to‘plamlarga Replay-Attack [2], CASIA-FASD va OULU-NPU misol bo‘la oladi. Ma’lumotlar o‘qitish, validatsiya va test qismlariga ajratiladi. Bir shaxsga tegishli yoki deyarli bir xil kadrlarning turli qismlarga tushib qolishi natijani sun’iy ravishda oshirishi mumkin; shu bois ajratish tartibi ma’lumotlarning tuzilishiga mos tanlanadi. Test qismi modelni sozlash uchun ishlatilmasligi kerak.

Biometrik xavfsizlikda soxta namunani xato tarzda qabul qilish xavfi alohida muhim, shu sababli faqat aniq ko‘rsatkichiga tayanish yetarli emas. ISO/IEC 30107-3:2023 standartida biometrik taqdimot hujumlarini aniqlashni baholashda APCER (Attack Presentation Classification Error Rate — hujum taqdimotlarini tasniflashdagi xatolik darajasi) va BPCER (Bona Fide Presentation Classification Error Rate — haqiqiy taqdimotlarni tasniflashdagi xatolik darajasi) kabi ko‘rsatkichlar muhim o‘rin tutadi; ACER ushbu ikki

ko‘rsatkichning o‘rtacha qiymati sifatida qo‘llanishi mumkin [3]. Keyingi tajribada precision, recall, F1-mezon va ROC-AUC kabi qo‘shimcha metrikalarni ham hisoblash tavsiya etiladi.

Tadqiqot yakunida soxtalashtirish hujumlarini aniqlashning umumiy jarayon sxemasi, algoritmlarni taqqoslash metodikasi va natijalarni baholash mezonlari ishlab chiqilishi kutiladi. Klassik algoritmlar xususiyatlari oldindan ajratilgan ma’lumotlar uchun boshlang‘ich taqqoslash modeli bo‘lishi mumkin [4], [5]; CNN esa tasvirdan xususiyatlarni avtomatik o‘rganish imkoniyati sababli ko‘rib chiqiladi [6]. Qaysi usul maqsadga muvofiq ekanligi sinov natijalari, hujum turlarining xilma-xilligi va hisoblash resurslariga qarab belgilanadi. Amaliy jihatdan ishlab chiqiladigan tavsiyalar biometrik tizimni tanlash yoki sinashda xatolik turlarini ko‘rish, turli hujumlar bo‘yicha alohida test o‘tkazish va real muhitga o‘tishdan oldin mustaqil tekshiruvni rejalashtirishga yordam berishi mumkin. Laboratoriya natijalari real hayotdagi barcha hujumlarga chidamlilikni kafolatlamaydi; kamera, yoritish, tasvir sifati va hujum vositalarining o‘zgarishi alohida sinovlarni talab qiladi.

Xulosa. Adabiyotlar tahliliga ko‘ra, mashinali o‘qitish algoritmlari biometrik taqdimot hujumlarini aniqlashda haqiqiy va soxta namunalarni farqlashga yordam berishi mumkin. SVM, Random Forest va CNN algoritmlarini bir xil ma’lumotlar hamda sinov sharoitlarida taqqoslash, aniqlik (accuracy), precision, recall, F1-mezon va ROC-AUC bilan bir qatorda ISO/IEC 30107-3:2023 standartida ko‘rsatilgan APCER, BPCER va ACER metrikalarini ham hisobga olish maqsadga muvofiq. Mazkur tezisda tajriba natijalari keltirilmagan; shu sababli qaysi algoritm samaraliroq ekani faqat keyingi sinovlar asosida aniqlanishi mumkin. Taklif etilgan metodika biometrik tizimlar xavfsizligini baholash va amaliy tavsiyalar ishlab chiqish uchun asos bo‘lib xizmat qilishi mumkin.

FOYDALANILGAN ADABIYOTLAR:

1. G‘aniyev S.K., Karimov M.M., Tashev K.A. Axborot xavfsizligi: darslik / S.K. G‘aniyev tahriri ostida. — Toshkent: Fan va texnologiya, 2016. — 372 b. (Foydalanilgan bo‘lim: VI bob “Identifikatsiya va autentifikatsiya”, 144–184-b.; xususan 6.5-bo‘lim “Foydalanuvchilarni biometrik identifikatsiyalash va autentifikatsiyalash”, 178-b.).
2. Chingovska I., Anjos A., Marcel S. On the Effectiveness of Local Binary Patterns in Face Anti-spoofing // Proceedings of the 11th International Conference of the Biometrics Special Interest Group (BIOSIG). — 2012. — P. 1–7.
3. ISO/IEC 30107-3:2023. Information technology — Biometric presentation attack detection — Part 3: Testing and reporting. — 2nd ed. — Geneva: ISO/IEC, 2023. — 39 p. (Qo‘llanilgan mavzular: atamalar va metrikalar, 2–5-b.; PAD baholash yondashuvi, 7–10-b.).
4. Cortes C., Vapnik V. Support-Vector Networks // Machine Learning. — 1995. — Vol. 20. — P. 273–297.
5. Breiman L. Random Forests // Machine Learning. — 2001. — Vol. 45. — P. 5–32.
6. Goodfellow I., Bengio Y., Courville A. Deep Learning. — Cambridge, MA: MIT Press, 2016.