AXBOROT TIZIMLARIDA BIOMETRIK AUTENTIFIKATSIYA ASOSIDA FOYDALANUVCHILAR XAVFSIZLIGINI OSHIRISH

Qo‘chqorova Durdona Sobir qizi
Mirzo Ulug‘bek nomidagi O‘zbekiston Milliy universiteti
qochqorovadurdona7@gmail.com

Annotatsiya. *Mazkur tadqiqotda axborot tizimlarida foydalanuvchilarni biometrik autentifikatsiyalash orqali xavfsizlik darajasini oshirish masalasi ko‘rib chiqilgan. Biometrik moslikni aniqlash, PAD (Presentation Attack Detection) va himoyalangan biometrik shablondan foydalanishni yagona autentifikatsiya jarayoniga birlashtiruvchi model taklif etilgan. Dasturiy prototipning nazoratli sinovida 100 ta autentifikatsiya urinishidan foydalanilib, FMR (False Match Rate), FNMR (False Non-Match Rate), APCER (Attack Presentation Classification Error Rate), BPCER (Bona Fide Presentation Classification Error Rate) va ACER (Average Classification Error Rate) ko‘rsatkichlari hisoblangan. Natijalar taklif etilgan modelning biometrik autentifikatsiya xavfsizligini kompleks baholash uchun qo‘llanish imkoniyatini ko‘rsatadi.*

Kalit so‘zlar: *Biometrik autentifikatsiya, axborot xavfsizligi, biometrik shablon, FMR (False Match Rate), FNMR (False Non-Match Rate), PAD (Presentation Attack Detection), autentifikatsiya.*

Аннотация. *В исследовании рассматривается повышение уровня безопасности информационных систем посредством биометрической аутентификации пользователей. Предложена модель, объединяющая проверку биометрического соответствия, обнаружение атак представления и защиту биометрического шаблона в едином процессе аутентификации. На контролируемом тестировании программного прототипа использовано 100 попыток аутентификации, по результатам которых рассчитаны показатели FMR (False Match Rate), FNMR (False Non-Match Rate), APCER (Attack Presentation Classification Error Rate), BPCER (Bona Fide Presentation Classification Error Rate) и ACER (Average Classification Error Rate). Полученные результаты показывают возможность применения предложенной модели для комплексной оценки безопасности биометрической аутентификации.*

Ключевые слова: *Биометрическая аутентификация, информационная безопасность, биометрический шаблон, FMR (False Match Rate), FNMR (False Non-Match Rate), PAD (Presentation Attack Detection), аутентификация.*

Abstract. *This study addresses the enhancement of information system security through biometric user authentication. A model integrating biometric matching, PAD (Presentation Attack Detection), and protected biometric templates into a unified authentication process is proposed. A controlled benchmark of the software prototype included 100 authentication attempts, and FMR (False Match Rate), FNMR (False Non-Match Rate), APCER (Attack Presentation Classification Error Rate), BPCER (Bona Fide Presentation Classification Error Rate), and ACER (Average Classification Error Rate) were calculated. The results demonstrate the applicability of the proposed model for comprehensive security evaluation of biometric authentication.*

Keywords: *Biometric authentication, information security, biometric template, FMR (False Match Rate), FNMR (False Non-Match Rate), PAD (Presentation Attack Detection), authentication.*

Kirish

Axborot tizimlarida foydalanuvchini ishonchli identifikatsiya va autentifikatsiya qilish axborot xavfsizligining muhim tarkibiy qismlaridan biridir. An’anaviy parol va PIN-kodlarga asoslangan autentifikatsiyada parolni o‘g‘irlash, taxmin qilish yoki boshqa shaxsga berish bilan bog‘liq xavflar mavjud. Shu sababli foydalanuvchining biologik va xulq-atvor xususiyatlariga asoslangan biometrik autentifikatsiya texnologiyalaridan foydalanish istiqbolli yo‘nalishlardan biri hisoblanadi. Biroq biometrik belgilar maxfiy “sir” emas va ularning markazlashgan holda saqlanishi qo‘shimcha maxfiylik hamda xavfsizlik muammolarini keltirib chiqarishi mumkin [1].

Ilmiy muammo va ilmiy bo‘shliq

Biometrik autentifikatsiya bo‘yicha tadqiqotlarda yuz, barmoq izi, ko‘z qorachig‘i va boshqa biometrik belgilar asosida foydalanuvchini tanib olish aniqligi, xatolik ko‘rsatkichlari hamda biometrik shablonlarni himoyalash masalalari keng o‘rganilgan. FMR va FNMR kabi ko‘rsatkichlar biometrik tizimning moslik samaradorligini baholashda qo‘llanadi, PAD esa sensor oldida taqdim etiladigan qalbakilashtirilgan biometrik namunalarni aniqlashga qaratilgan [1; 2]. ISO/IEC 30107-3:2023 PAD mexanizmlarini baholash, test natijalarini hisobot qilish va hujum turlarini tasniflash tamoyillarini belgilaydi [2]. ISO/IEC 24745:2022 esa

biometrik ma’lumotlarni saqlash va uzatishda maxfiylik, qayta tiklanmaslik va yangilanish kabi talablar bilan bog‘liq biometrik shablon himoyasini tavsiflaydi [3].

Tadqiqot maqsadi

Axborot tizimlarida foydalanuvchilarni biometrik autentifikatsiyalash jarayonining xavfsizlik darajasini oshirishga xizmat qiluvchi ko‘p bosqichli himoya modelini ishlab chiqish va uning dasturiy prototipini shakllantirish.

Tadqiqot metodlari

Tadqiqotda tizimli tahlil, taqqoslash, modellashtirish, biometrik moslikni baholash va xavfsizlik ko‘rsatkichlarini statistik hisoblash usullaridan foydalanildi. Dasturiy prototipda biometrik namunani vektor ko‘rinishida ifodalash, kosinus o‘xshashligi orqali moslikni hisoblash va belgilangan threshold asosida autentifikatsiya qarorini qabul qilish mexanizmi qo‘llanildi. Test protokolida 50 ta genuine va 50 ta impostor urinish, shuningdek 20 ta presentation attack va 20 ta bona-fide PAD urinishlari ko‘rib chiqildi. Eslatma: ushbu benchmark sintetik feature vectorlar asosida o‘tkazilgan bo‘lib, real inson biometrik namunalariga asoslanmagan.

Tadqiqot obyekti va predmeti

Tadqiqot obyekti – axborot tizimlarida foydalanuvchilarni biometrik autentifikatsiyalash jarayoni.

Tadqiqot predmeti – biometrik autentifikatsiya jarayonida biometrik moslikni aniqlash, qalbakilashtirilgan namunalarni aniqlash va biometrik shablonni himoyalash orqali autentifikatsiya qarorini shakllantirish usullari.

Taklif etilayotgan model va ilmiy yangilik

Tadqiqotning ilmiy yangiligi sifatida biometrik autentifikatsiya xavfsizligini uchta o‘zaro bog‘liq bosqich orqali baholovchi model taklif etildi. Birinchi bosqichda foydalanuvchidan olingan biometrik namuna ro‘yxatdan o‘tkazilgan shablon bilan taqqoslanib, moslik koeffitsiyenti aniqlanadi. Ikkinchi bosqichda presentation attack detection yordamida biometrik namunaning qalbakilashtirilmaganligi baholanadi. Uchinchi bosqichda asl biometrik tasvir o‘rniga himoyalangan biometrik shablon bilan ishlash tamoyili qo‘llanadi.

Modelda yakuniy xavfsizlik ko‘rsatkichi konseptual ravishda $R = \alpha S + \beta P + \gamma T$ ko‘rinishida ifodalanadi. Bu yerda S – biometrik moslik darajasi, P – PAD orqali aniqlangan hujum xavfi bo‘yicha ko‘rsatkich, T – biometrik shablonning himoyalanganlik darajasi, α, β va γ esa tizim talablariga mos vazn koeffitsiyentlaridir.

Natijalar

Dasturiy prototipning nazoratli benchmark sinovida 100 ta autentifikatsiya urinishidan foydalanildi: 50 tasi genuine, 50 tasi impostor urinishlardan iborat bo‘ldi. PAD qismi uchun qo‘shimcha ravishda 20 ta attack va 20 ta bona-fide sinov o'tkazildi. Threshold mustaqil development to‘plamidan hisoblangan va test namunalariga keyinchalik qo‘llangan.

1-jadval. Dasturiy prototip sinovlarining umumiy natijalari.

Ko‘rsatkich	Sinovlar soni	Natija	Foiz
Genuine	50	50/50 qabul qilindi	100%
Impostor	50	0/50 noto‘g‘ri qabul qilindi	0%
PAD attack	20	18/20 aniqlangan	90%
PAD bona-fide	20	20/20 to‘g‘ri bona-fide	100%

2-jadval. Dasturiy prototipning hisoblangan xavfsizlik ko‘rsatkichlari.

Ko‘rsatkich	Qiymat	Mazmuni
FMR	0.00%	Impostor urinishlarining noto‘g‘ri qabul qilinishi
FNMR	0.00%	Genuine urinishlarning noto‘g‘ri rad etilishi
APCER	10.00%	Presentation attacklarning noto‘g‘ri bona-fide sifatida qabul qilinishi
BPCER	0.00%	Bona-fide namunalarining noto‘g‘ri attack sifatida tasniflanishi
ACER	5.00%	APCER va BPCER o‘rtacha qiymati

Sinov natijalariga ko‘ra, genuine va impostor urinishlar bo‘yicha mos ravishda 0,00% FNMR va 0,00% FMR qayd etildi. PAD sinovlarida 20 ta attack urinishining 18 tasi aniqlangan, 2 tasi esa biometrik moslik chegarasidan o‘tgan; natijada APCER 10,00% ni tashkil etdi. Bona-fide sinovlarining barchasi to‘g‘ri tasniflanganligi sababli BPCER 0,00%, ACER esa 5,00% bo‘ldi. ISO/IEC 30107-3:2023 PAD mexanizmlarining ishlashini baholash va test natijalarini hisobot qilish uchun metodik asos beradi [2].

Olingan natijalar prototipning nazoratli, sintetik benchmarkdagi xususiyatini aks ettiradi. Shu sababli ularni real foydalanuvchilar populyatsiyasiga umumlashtirish mumkin emas. NIST biometrik tizimlar uchun FMR va FNMRni

standartlashtirilgan sharoitlarda baholashni hamda PADni qo‘llashni tavsiya qiladi [1].

Xulosa

Tadqiqotda axborot tizimlarida biometrik autentifikatsiya xavfsizligini oshirishga qaratilgan uch bosqichli model taklif etildi. Model biometrik moslikni tekshirish, presentation attack detection va himoyalangan biometrik shablondan foydalanishni yagona jarayonda birlashtiradi. Dasturiy prototipning 100 ta autentifikatsiya urinishidan iborat sintetik benchmarkida FMR va FNMR 0,00%, PAD bo‘yicha APCER 10,00%, BPCER 0,00% va ACER 5,00% natijalar qayd etildi. Ushbu natijalar metodik prototipni ko‘rsatadi; real biometrik ma’lumotlar asosidagi kengaytirilgan test keyingi tadqiqot bosqichi sifatida belgilandi.

Foydalanilgan adabiyotlar

1. National Institute of Standards and Technology. Digital Identity Guidelines: Authentication and Authenticator Management. NIST Special Publication 800-63B-4. Gaithersburg: NIST, 2025.

2. ISO/IEC 30107-3:2023. Information technology — Biometric presentation attack detection — Part 3: Testing and reporting. Geneva: International Organization for Standardization, 2023.

3. ISO/IEC 24745:2022. Information security, cybersecurity and privacy protection — Biometric information protection. Geneva: International Organization for Standardization, 2022.

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

5. ISO/IEC 2382-37:2022. Information technology — Vocabulary — Part 37: Biometrics. Geneva: International Organization for Standardization, 2022.