BIOMETRIK TIZIMLARDA FAR VA FRR KO‘RSATKICHLARINING TAHLILI – ANIQLIK VA ISHONCHLILIKNI OSHIRISH YO‘LLARI

Xolmuratov Jamshidbek Xayrulla o'g'li

E-mail: Jamshidbekxolmuratov.02@gmail.com

Qabul qilindi: 08.10.2025
Ko‘rib chiqildi: 09.10.2025
Tasdiqlandi: 10.10.2025

Kalit so‘zlar:
Biometrik tizimlar, FAR, FRR, autentifikatsiya, aniqlik, ishonchlilik, xavfsizlik, sun’iy intellekt

Annotatsiya. Ushbu tezisda biometrik tizimlarda FAR (False Acceptance Rate) va FRR (False Rejection Rate) ko‘rsatkichlarini tahlil qilish, shuningdek, tizimning aniqlik va ishonchliligini oshirish yo‘llari o‘rganiladi. Biometrik autentifikatsiya barmoq izi, yuzni aniqlash, ko‘z qorachig‘i skanerlari va ovoz tanish kabi noyob fiziologik yoki xulq-atvor belgilariga asoslanadi. Tadqiqotda FAR va FRR darajalari tizim xavfsizligi va foydalanuvchi qulayligiga ta’siri, shuningdek, ko‘p faktorli autentifikatsiya, algoritmik optimallashtirish va sun’iy intellekt orqali ularni kamaytirish usullari tahlil qilinadi. Natijalar shuni ko‘rsatadiki, FAR pasaytirilishi xavfsizlikni oshiradi, FRR kamaytirilishi esa foydalanuvchi qulayligini ta’minlaydi.

Key words:
Biometric systems, FAR, FRR, authentication, accuracy, reliability, security, artificial intelligence.

Annotation. This thesis analyzes FAR (False Acceptance Rate) and FRR (False Rejection Rate) in biometric systems and explores methods to enhance system accuracy and reliability. Biometric authentication relies

on unique physiological or behavioral traits such as fingerprints, facial recognition, iris scanning, and voice identification. The study examines how FAR and FRR affect system security and user convenience, and evaluates strategies like multi-factor authentication, algorithmic optimization, and AI-based improvement to reduce error rates. Results indicate that reducing FAR increases security, while lowering FRR enhances user experience.

Ключевые слова:
Биометрические системы, FAR, FRR, аутентификация, точность, надежность, безопасность, искусственный интеллект.

Аннотация. В данном тезисе проводится анализ показателей FAR (False Acceptance Rate) и FRR (False Rejection Rate) в биометрических системах, а также рассматриваются методы повышения точности и надежности этих систем. Биометрическая аутентификация основана на уникальных физиологических или поведенческих характеристиках, таких как отпечатки пальцев, распознавание лица, сканирование радужки глаза и идентификация по голосу. Исследование оценивает влияние FAR и FRR на безопасность системы и удобство пользователя, а также рассматривает методы снижения ошибок, включая многофакторную аутентификацию,

алгоритмическую оптимизацию и искусственный интеллект. Результаты показывают, что снижение FAR повышает безопасность, а уменьшение FRR улучшает пользовательский опыт.

Kirish. So‘nggi yillarda biometrik autentifikatsiya tizimlari raqamli xavfsizlikning ajralmas qismiga aylangan bo‘lib, an’anaviy parolga asoslangan tizimlarga nisbatan ishonchli va foydalanuvchi qulayligini oshiruvchi usullarni taklif qiladi. Ushbu tizimlar shaxsni aniqlash uchun noyob fiziologik yoki xulq-atvor xususiyatlariga — barmoq izi, yuz tuzilmasi, ko‘z qorachig‘i naqshi, ovoz tanish kabi — asoslanadi. Shu bilan birga, biometrik tizimlarning ishlash samaradorligi False Acceptance Rate (FAR) va False Rejection Rate (FRR) ko‘rsatkichlari bilan o‘lchanadi. FAR tizimga ruxsatsiz shaxs kirish ehtimolini, FRR esa haqiqiy foydalanuvchining rad etilish ehtimolini bildiradi. FAR va FRR o‘rtasidagi muvozanat muhim ahamiyatga ega: FAR kamaytirilsa, tizim xavfsizligi oshadi, FRR kamaytirilsa, foydalanuvchi qulayligi yaxshilanadi. Ammo bitta ko‘rsatkichni yaxshilash ko‘pincha ikkinchisiga salbiy ta’sir ko‘rsatadi, shu sababli optimal muvozanatni ta’minlash muhimdir. Hozirgi kunda sun’iy intellekt, algoritmik optimizatsiya va ko‘p faktorli autentifikatsiya kabi texnologiyalar FAR va FRRni optimallashtirish va tizim aniqligi hamda ishonchliligini oshirish imkoniyatini beradi. Ushbu tadqiqotning maqsadi — biometrik tizimlarda FAR va FRR ko‘rsatkichlarini tahlil qilish, ularga ta’sir etuvchi omillarni aniqlash va tizim aniqligi hamda ishonchliligini oshirish usullarini o‘rganishdir. Tadqiqot natijalari biometrik autentifikatsiya tizimlarini raqamli xavfsizlik kontekstida samarali va ishonchli ishlashini ta’minlashga qaratilgan. Biometrik autentifikatsiya tizimlari nafaqat raqamli qurilmalar va

onlayn xizmatlar xavfsizligini ta’minlash, balki bank, sog‘liqni saqlash, davlat idoralari va sanoat korxonalarida ham keng qo‘llanilmoqda. An’anaviy parol va PIN-kodlar bilan solishtirganda, biometrik tizimlar foydalanuvchini noyob fiziologik yoki xulq-atvor xususiyatlari orqali aniqlaydi, bu esa shaxsiy ma’lumotlarni himoya qilish va ruxsatsiz kirishning oldini olishda muhim rol o‘ynaydi. Shuningdek, zamonaviy biometrik tizimlar sun’iy intellekt va mashina o‘rganish algoritmlari bilan jihozlangan bo‘lib, ular foydalanuvchi harakatlarini o‘rganish va xatoliklarni aniqlash imkoniyatini oshiradi.

Materiallar va usullar. Ushbu tadqiqotda biometrik tizimlarda FAR (False Acceptance Rate) va FRR (False Rejection Rate) ko‘rsatkichlarini tahlil qilish uchun eksperimental va analitik usullar birlashtirildi. Tadqiqot uch asosiy komponentga qaratildi: barmoq izi, yuzni aniqlash, va ovoz tanish tizimlari. Birinchi bosqichda adabiyotlar tahlili va mavjud standartlar, jumladan ISO/IEC biometrik xavfsizlik mezonlari o‘rganildi. Bu orqali FAR va FRRga ta’sir etuvchi omillar aniqlanib, har bir biometrik usulning afzallik va kamchiliklari tahlil qilindi. Ikkinchi bosqichda tajriba o‘tkazildi. Open-source va tijorat biometrik autentifikatsiya tizimlari yordamida FAR va FRR qiymatlari turli sharoitlarda sinovdan o‘tkazildi. Misol uchun, barmoq izi tizimlarida turli sensorlar va foydalanuvchi sharoitlari (quruq, nam teri) ta’siri o‘lchandi, yuzni aniqlashda yorug‘lik va burchak farqlari, ovoz tanishda esa fon shovqini va ovoz tembrining farqlari tekshirildi. Olingan natijalar statistik tahlil yordamida, xususan standart og‘ish va korrelyatsiya ko‘rsatkichlari asosida baholandi. Uchinchi bosqichda foydalanuvchi tajribasi va xatti-harakatlarini o‘rganish uchun 100 nafar ishtirokchi orasida so‘rovnoma o‘tkazildi. So‘rovnoma foydalanuvchilarning tizim qulayligi, rad etilish holatlari va umumiy xavfsizlikni qabul qilish darajasini aniqlashga qaratildi. Tadqiqotda olingan barcha ma’lumotlar FAR va FRR ko‘rsatkichlarini optimallashtirish, biometrik tizimlar aniqligi va ishonchliligini oshirishga xizmat qiladigan tavsiyalar ishlab chiqishda ishlatilgan. Bu yondashuv

eksperimental, statistik va foydalanuvchi xatti-harakatlari tahlilini birlashtirgan holda tizim samaradorligini yanada oshirish imkonini beradi.

1- Jadval: Barmoq izi tizimlarida FAR va FRR qiymatlari

Foydalanuvchi guruhi	FAR (%)	FRR (%)
Guruh 1	0.5	2.1
Guruh 2	0.7	1.8
Guruh 3	0.6	2.0

Birinchi jadvalda barmoq izi tizimlarida FAR (False Acceptance Rate) va FRR (False Rejection Rate) ko‘rsatkichlari turli foydalanuvchi guruhlari bo‘yicha taqdim etilgan. Jadvaldan ko‘rinib turibdiki, FAR qiymatlari 0,5–0,7% oralig‘ida, FRR esa 1,8–2,1% oralig‘ida o‘zgaradi. Bu natijalar shuni ko‘rsatadiki, barmoq izi tizimlari nisbatan yuqori aniqlik va ishonchlilik darajasiga ega, chunki ruxsatsiz shaxsning tizimga kirish ehtimoli juda past (FAR), va haqiqiy foydalanuvchining rad etilishi ham minimal darajada (FRR) saqlanadi. Shu bilan birga, foydalanuvchi guruhi farqlari ko‘rsatkichlarga sezilarli ta’sir ko‘rsatmaydi, bu tizimning turli foydalanuvchilar uchun barqaror ishlashini tasdiqlaydi. Barmoq izi tizimlarida FAR va FRRni yanada kamaytirish uchun sensor sifati, algoritmik optimizatsiya, adaptiv thresholdlar va multi-factor autentifikatsiya qo‘llanishi tavsiya etiladi.

Tadqiqot muhokamasi. Tadqiqot natijalari shuni ko‘rsatadiki, biometrik autentifikatsiya tizimlarida FAR (False Acceptance Rate) va FRR (False Rejection Rate) ko‘rsatkichlari tizim samaradorligi va foydalanuvchi qulayligini belgilashda asosiy omil hisoblanadi. Eksperimentlar va adabiyotlar tahliliga ko‘ra, FAR pasaytirilsa, tizim xavfsizligi oshadi, ya’ni ruxsatsiz shaxslar tizimga kira olmasligi kafolatlanadi. Shu bilan birga, FRR darajasini kamaytirish foydalanuvchining haqiqiy autentifikatsiyasini rad etilish ehtimolini kamaytiradi, bu esa qulaylikni oshiradi. Barmoq izi tizimlari yuqori aniqlik va tezkorlikni

ta’minlasa-da, sensor sifati, teri holati va atrof-muhit sharoitlariga sezgir. Yuzni aniqlash tizimlari qulay va kontakt bo‘lmagan autentifikatsiya imkonini beradi, ammo yorug‘lik, yuz burchagi va yoshga bog‘liq o‘zgarishlar FRRni oshiradi. Ovoz tanish tizimlari esa fon shovqiniga va ovoz imitatsiyasiga sezgir, ko‘z qorachig‘i skanerlari esa yuqori xavfsizlik ta’minlasa-da, maxsus uskuna va intruziv jarayon talab qiladi. Tadqiqot shuni ko‘rsatadiki, FAR va FRRni optimallashtirishda algoritmik filtrlar, sun’iy intellekt va ko‘p faktorli autentifikatsiya samarali vositalar hisoblanadi. Multi-modulli biometrik tizimlar va adaptiv thresholdlar FAR va FRR o‘rtasida optimal muvozanatni yaratishga yordam beradi. Shuningdek, foydalanuvchi xatti-harakatini o‘rganish, xususan, tizimga kirishda qulaylik va xavfsizlikni baholash, tizim ishonchliligini oshiradi. Natijalar shuni ko‘rsatadiki, FAR va FRR ko‘rsatkichlarini integratsiyalashgan yondashuv yordamida optimallashtirish biometrik tizimlarni xavfsiz, ishonchli va foydalanuvchi qulay qilish imkonini beradi. Shu bilan birga, tizim dizayni va algoritmik yechimlar foydalanuvchi ehtiyojlari bilan uyg‘un bo‘lishi zarur. Bu esa kelajakda biometrik autentifikatsiya tizimlarini raqamli xavfsizlikning muhim qismi sifatida samarali ishlatishga imkon beradi. Ushbu tadqiqot natijalari shuni ko‘rsatdiki, biometrik autentifikatsiya tizimlarida FAR (False Acceptance Rate) va FRR (False Rejection Rate) ko‘rsatkichlarini tahlil qilish tizim samaradorligini baholashda asosiy ahamiyatga ega. Eksperimentlar va adabiyotlar tahliliga ko‘ra, FAR darajasini kamaytirish tizim xavfsizligini oshiradi va ruxsatsiz kirish ehtimolini minimal darajaga tushiradi, FRR darajasini kamaytirish esa haqiqiy foydalanuvchilarni rad etish ehtimolini kamaytirib, foydalanuvchi qulayligini oshiradi. Barmoq izi tizimlarida FAR va FRR qiymatlari past bo‘lib, tizimning yuqori aniqlik va barqaror ishlashini ko‘rsatadi. Yuzni aniqlash tizimlarida yorug‘lik sharoiti, burchak va yuz ifodalarining o‘zgarishi FRRga ta’sir qiladi, ovoz tanish tizimlarida fon shovqini va ovoz imitatsiyasi FAR va FRRni oshirishi mumkin. Iris skanerlari esa yuqori

xavfsizlikni ta’minlasa-da, maxsus uskuna va intruziv jarayon talab qiladi. Tadqiqot shuni ko‘rsatadiki, FAR va FRRni optimallashtirishda algoritmik filtrlar, sun’iy intellekt, multi-modulli tizimlar va ko‘p faktorli autentifikatsiya samarali vositalardir. Shu yondashuv FAR va FRR o‘rtasidagi optimal muvozanatni yaratishga yordam beradi va tizimni xavfsiz, ishonchli va foydalanuvchi qulay qiladi. Shuningdek, foydalanuvchi xatti-harakatlarini o‘rganish va tizim dizaynini foydalanuvchi ehtiyojlariga moslashtirish FAR va FRRni yanada yaxshilashga imkon beradi. Natijalar shuni ko‘rsatadiki, biometrik autentifikatsiya tizimlarini optimallashtirish raqamli xavfsizlikni mustahkamlash va foydalanuvchi ishonchini oshirishda muhim ahamiyatga ega. Tadqiqot davomida olingan natijalar shuni ko‘rsatdiki, biometrik tizimlarda FAR va FRR ko‘rsatkichlari nafaqat tizim xavfsizligi, balki foydalanuvchi qulayligini ham belgilaydi.

Xulosa. Ushbu tadqiqot shuni ko‘rsatdiki, biometrik autentifikatsiya tizimlarida FAR (False Acceptance Rate) va FRR (False Rejection Rate) ko‘rsatkichlarini optimallashtirish tizimning aniqligi, ishonchliligi va foydalanuvchi qulayligini oshirishda muhim ahamiyatga ega. FAR darajasini kamaytirish tizim xavfsizligini oshiradi va ruxsatsiz kirishning oldini oladi, FRR darajasini kamaytirish esa haqiqiy foydalanuvchining rad etilish ehtimolini kamaytirib, tizim qulayligini yaxshilaydi. Tadqiqot natijalari shuni ko‘rsatadiki, algoritmik optimizatsiya, ko‘p faktorli autentifikatsiya va sun’iy intellekt asosidagi yondashuvlar FAR va FRR ko‘rsatkichlarini muvozanatlashda samarali vosita hisoblanadi.

Foydalanilgan adabiyotlar ro`yxati.

1. Jain, A. K., Ross, A., & Nandakumar, K. (2021). Introduction to Biometrics. Springer.

2. ISO/IEC 30107-3:2017. Information Technology — Biometric Presentation Attack Detection — Part 3: Testing and Reporting. International Organization for Standardization.
3. ISO/IEC 24745:2011. Information Technology — Security Techniques — Biometric Information Protection. International Organization for Standardization.
4. Maltoni, D., Maio, D., Jain, A. K., & Prabhakar, S. (2018). Handbook of Fingerprint Recognition. Springer.
5. Ross, A., & Jain, A. K. (2020). “Multimodal Biometrics: An Overview.” Proceedings of the IEEE, 85(9), 1347–1368.
6. Kim, H., & Lee, S. (2023). “Advancements in Personal Data Protection Using Biometric Encryption.” IEEE Access, 11, 45879–45892.