DEVELOPMENT OF SCIENCE

ISNN 3030-3907

2026 AUGUST

ISSUE - 8
VOLUME -1

DEVELOPMENT OF SCIENCE

D E V O S

РАЗВИТИЕ НАУКИ

ILM-FAN TARAQQIYOTI

Development of science

Scientific journal
Ilmiy jurnal
Научный журнал

AUGUST 2026
Issue - 8, VOLUME - 1

ISSN 3030 -3907

The scientific journal ***«Development of Science»*** *was registered by the State on April 15, 2024 with certificate number №256445.*

«Ilm fan tarqqiyoti» *ilmiy jurnali 2024 yil 15 aprel kuni №256445 sonli guvohnoma bilan Davlat ro'yxatidan o'tgan.*

Научный журнал ***«Развитие науки»*** *был зарегистрирован государством 15 апреля 2024 года под номером свидетельства № 256445.*

The proceedings will be provided to the authors in electronic form (PDF format). The authors bear full responsibility for the content of the articles included in the proceedings, the accuracy and reliability of the statistical data and regulatory documents cited therein, as well as for any opinions and judgments expressed in their articles. Articles that do not meet the established requirements will not be included in the proceedings. The Organizing Committee reserves the right to shorten the text of an article, make minor editorial corrections, and assign submissions to the appropriate sections.

To'plam elektron ko'rinishda (pdf formatida) mualliflarga taqdim etiladi. To'plamga kiritiladigan maqolalarning mazmuni, ulardagi statistik ma'lumotlar va me'yoriy hujjatlarning to'g'riligiga hamda har qanday fikr - mulohazalarga mualliflarning o'zlari mas'ul hisoblanadilar.Talablarga javob bermaydigan maqolalar to'plamga kiritilmaydi. Tashkiliy qo'mita maqola matnini qisqartirish, qisman tuzatish kiritish, seksiyalarga joylashtirish huquqiga ega.

Сборник предоставляется авторам в электронном виде (в формате PDF). Авторы несут полную ответственность за содержание статей, включённых в сборник, достоверность приведённых в них статистических данных и нормативных документов, а также за изложенные мнения и суждения. Статьи, не соответствующие установленным требованиям, в сборник не включаются. Организационный комитет оставляет за собой право сокращать текст статьи, вносить отдельные редакционные исправления и распределять материалы по соответствующим секциям.

EDITOR-IN-CHIEF:
Temirov Alisher Hashim oglu - Doctor of Philosophy (PhD) in Technical Sciences, Associate Professor.
CHAIRMAN OF THE EDITORIAL BOARD:
Fozilov Sadriddin Fayzullayevich - Doctor of Technical Sciences, Professor
MEMBERS OF THE EDITORIAL BOARD:

Faheem Uddin
Professor,Iqra university, Pakistan
Siddikova Sadokat Gafforovna
DSc, Rector of Bukhara State Technical University, Uzbekistan
Dr. Amit Rawal
Professor, Department of Textile and Fibre Engineering Indian Institute of Technology Delhi, India
Alexander Vitalievich Dudan
Associate Professor, Euphrosyne Polotskaya State University of Polotsk, Republic of Belarus
Bozorov Gayrat Rashidovich
Professor Bukhara State Technical University, Uzbekistan
Vladimir Mikhailovich Kapustin
Professor,Gubkin Russian State University of Oil and Gas (National Research University),Russian Federation
Shaoliang Chen
Ph. D., Engineer,Cement Science and New Building Materials Research Institute, China
Tukhtayeva Zebo Sharifovna
Bukhara State Technical University, Professor.
Kodirov Abduakhad Abdurakhimovich
Karshi State University, Professor
Turemuratov Sharibay Naurizbaevich
General Scientific Secretary of the Karakalpakstan Branch of the Academy of Sciences of the Republic of Uzbekistan, Professor
Tursunov Kakhor Shonazarovich
Karshi State University, Professor
Sharipov Muzaffar Samandarovich
Bukhara State University, Professor.
Alikulov Rustam Valiyevich
Termez State University, Professor
Makhmudov Mukhtar Jamolovich
Bukhara State Technical University, Professor.
Oral Kurganbekovich Beyseynbayev
Professor,M. Auezov South Kazakhstan University,Republic of Kazakhstan
Tropov Khamza Tursunovich
Samarkand State University, Professor
Nizamov Aslitdin Badreddinovich
Bukhara State Technical University, Professor.
Saidakhmedova Nodira Ilkhomovna
Tashkent State University of Economics, Professor

ORGANIZATIONAL STRUCTURE:

Safarov J.A.-*editor*
Panoyev N.Sh. -*editor*
Buranov N.G. -*assistant editor*
Shodiyev D.X.- *layout editor*
Izzatov D.X. - *layout editor*
Urinov J.B. - *layout editor*
Temirov A.T. - *graphic designer*
Temirov I.G. – *layout designer*

Changes to the composition of the Editorial Board, including the appointment of new members or the removal of existing members, shall be made by the Editor-in-Chief.

www.devos.uz

ISSN 3030-3907

YUZ, HARAKAT VA VAQTGA BOG‘LIQ MODELLAR ASOSIDA KO‘P MODALLI BIOMETRIK UZLUKSIZ AUTENTIFIKATSIYA TIZIMI: MUAMMOLAR VA YECHIMLAR

Alayev Ruhillo Habibovich
Mirzo Ulug‘bek nomidagi O‘zbekiston Milliy universiteti dotsenti, PhD.
E-mail: alayev_r@nuu.uz
Nurmatov Abduraxim Shaxriyor o‘g‘li
Mirzo Ulug‘bek nomidagi O‘zbekiston Milliy universiteti magistr talabasi
E-mail: codergq@gmail.com

Annotatsiya. Ushbu tezisda web-kamera video oqimi asosida foydalanuvchini sessiya davomida uzluksiz autentifikatsiya qilish masalasi bo‘yicha olib borilgan so‘nggi ilmiy ishlar tahlil qilinadi. Uzluksiz autentifikatsiya odatiy bir martalik autentifikatsiyadan farqli ravishda, foydalanuvchini seans davomida haqiqiy yoki haqiqiy emasligini passiv va uzluksiz tekshiruvchi yondashuv bo‘lib, u biometrik, xulqiy va kontekstga oid sensor belgilariga tayangani sababli xavfsizlik bilan birga maxfiylik muammolarini ham keltirib chiqaradi [1]. Tahlil doirasida yuz biometrikasi (CNN/embedding), harakat signallari (bosh holati, kichik harakatlar kabi) hamda vaqtga bog‘liq modellar (LSTM/GRU va Transformer) asosida ko‘p modalli (multimodal) autentifikatsiya arxitekturasi qanday shakllanishi, qaysi bosqichlarda xatoliklar yuzaga kelishi va ularni kamaytirish yechimlari yoritiladi. Ko‘p modalli yondashuvning motivatsiyasi — yakka modal tizimlardagi samaradorlik pastligi va taqdimot hujumlari (presentation attacks) xavfi — ham nazariy, ham amaliy manbalar orqali asoslanadi [2]. Shuningdek, spoofing/replay va deepfake tahdidlariga qarshi PAD/tiriklikni aniqlash standart metrikalari, real vaqt sharoitida resurs cheklovlari [3] va tasvir sifati masalalari bo‘yicha xulosalar beriladi.

Kalit so‘zlar: uzluksiz autentifikatsiya, ko‘p modalli biometrika, yuzni tanish, vaqtga bog‘liq modellar, Transformer, LSTM/GRU, tiriklikni aniqlash, taqdimot hujumlarini aniqlash.

Аннотация. В данной тезисной работе представлен анализ последних научных исследований в области непрерывной аутентификации пользователя на основе видеопотока веб-камеры в течение сессии. В отличие от традиционной одноразовой аутентификации, непрерывная аутентификация представляет собой пассивный и непрерывный подход к проверке подлинности пользователя на протяжении всей сессии. Поскольку данный подход основывается на биометрических, поведенческих и контекстных сенсорных признаках, наряду с повышением уровня безопасности он также приводит к возникновению проблем конфиденциальности [1]. В рамках анализа рассматривается формирование

ISSN 3030-3907

мультимодальной архитектуры аутентификации на основе лицевой биометрии (CNN/embedding), сигналов движения (положение головы и небольшие движения), а также временных моделей (LSTM/GRU и Transformer). Освещаются этапы возникновения ошибок и подходы к их снижению. Мотивация использования мультимодального подхода, обусловленная более низкой эффективностью одномодальных систем и риском атак представления (presentation attacks), обосновывается на основе теоретических и практических источников [2]. Также представлены выводы относительно стандартных метрик PAD/обнаружения живости для противодействия угрозам spoofing/replay и deepfake, ограничений вычислительных ресурсов в условиях реального времени [3], а также проблем качества изображений.

Ключевые слова: непрерывная аутентификация, мультимодальная биометрия, распознавание лица, временные модели, Transformer, LSTM/GRU, обнаружение живости, обнаружение атак представления.

Abstract. This thesis presents an analysis of recent scientific research on continuous user authentication based on webcam video streams throughout a session. Unlike conventional one-time authentication, continuous authentication is a passive and ongoing approach to verifying the authenticity of a user throughout the session. Since this approach relies on biometric, behavioral, and contextual sensor features, it not only enhances security but also introduces privacy concerns [1]. The analysis focuses on the development of multimodal authentication architectures based on facial biometrics (CNN/embedding), motion-related signals (head pose and subtle movements), and temporal models (LSTM/GRU and Transformer). The stages at which errors may occur and approaches to reducing such errors are also discussed. The motivation for adopting a multimodal approach, driven by the lower effectiveness of unimodal systems and the risk of presentation attacks, is substantiated through both theoretical and practical sources [2]. The thesis also provides conclusions regarding standard PAD/liveness detection metrics for countering spoofing/replay and deepfake threats, computational resource constraints in real-time environments [3], and image quality issues.

Keywords: continuous authentication, multimodal biometrics, face recognition, temporal models, Transformer, LSTM/GRU, liveness detection, presentation attack detection.

KIRISH.

Ko‘plab amaliy tizimlarda autentifikatsiya kirishda tekshirish (parol/2FA/biometrika) bilan cheklanadi; ammo sessiya davomida qurilma yoki xizmatdan foydalanayotgan shaxs almashib qolishi (masalan, ish joyida kompyuterni tark etish, masofaviy imtihonda o‘rin almashish, uy sharoitida umumiy qurilmadan foydalanish) ehtimoli doimo mavjud. Shu ehtiyoj fonida uzluksiz autentifikatsiya (continuous authentication) konsepsiyasi taklif qilinadi: u foydalanuvchini seans davomida passiv va uzluksiz tarzda tekshiradi, biometrik, xulq hamda kontekstga oid belgilarni birlashtirishi mumkin [1].

Biroq uzluksiz autentifikatsiyaning amaliy joriy etilishi bir vaqtning o‘zida bir nechta sinf muammolarni keltirib chiqaradi. Birinchidan, uzluksiz autentifikatsiya ko‘pincha shaxsga oid ma’lumotlar bilan ishlaydi va bu maxfiylik xavotirlarini kuchaytiradi [1]. Ikkinchidan, uzluksiz tekshiruv real-vaqt hisoblashini, past kechikishni va resurs tejamkorligini talab qiladi; buning ustiga tadqiqotlarda uzluksiz autentifikatsiya usullari qalbakilashtirish orqali aldash (spoofing) va qayta foydalanish (replay) hujumlari kabi amaliy xavflar qayd etiladi [3]. Uchinchidan, yuzga asoslangan autentifikatsiya web-kamera real hayotda maska, yorug‘lik, kamera sifati, rakurs, qisman to‘silish kabi omillarga sezgir bo‘lib, xato qabul/xato inkor (false accept/false reject) balansini buzishi mumkin; shu bois real tizimlar ko‘pincha sifat nazorati va namunani tanlash kabi yordamchi bosqichlarni talab qiladi [4].

Shu maqsadda *ko‘p modalli biometrika* muhim yozndashuv sifatida foydalaniladi: *yagona modal* identifikatsiya cheklovlarini yumshatish va ishonchlilikni oshirish uchun bir nechta signal manbalarini (masalan, yuz + harakat + vaqt bo‘yicha o‘zgarish) birlashtirish tavsiya etiladi. Ko‘p modalli yondashuv yagona modal tizimlarning cheklovlarini bartaraf etish zarurati, uning qo‘llanish motivatsiyasi va ustunliklari, shuningdek xususiyatlar, ballar, qaror va reyting darajasidagi birlashtirish strategiyalarini batafsil tahlil qiluvchi ilmiy maqolalar bilan asoslanadi [4]. Mazkur tezisda aynan web-kamera video oqimi kontekstida “yuz + harakat + vaqtga bog‘liq model” kombinatsiyasining ilmiy-texnik muammolari va ularni bartaraf etish yechimlari umumlashtiriladi.

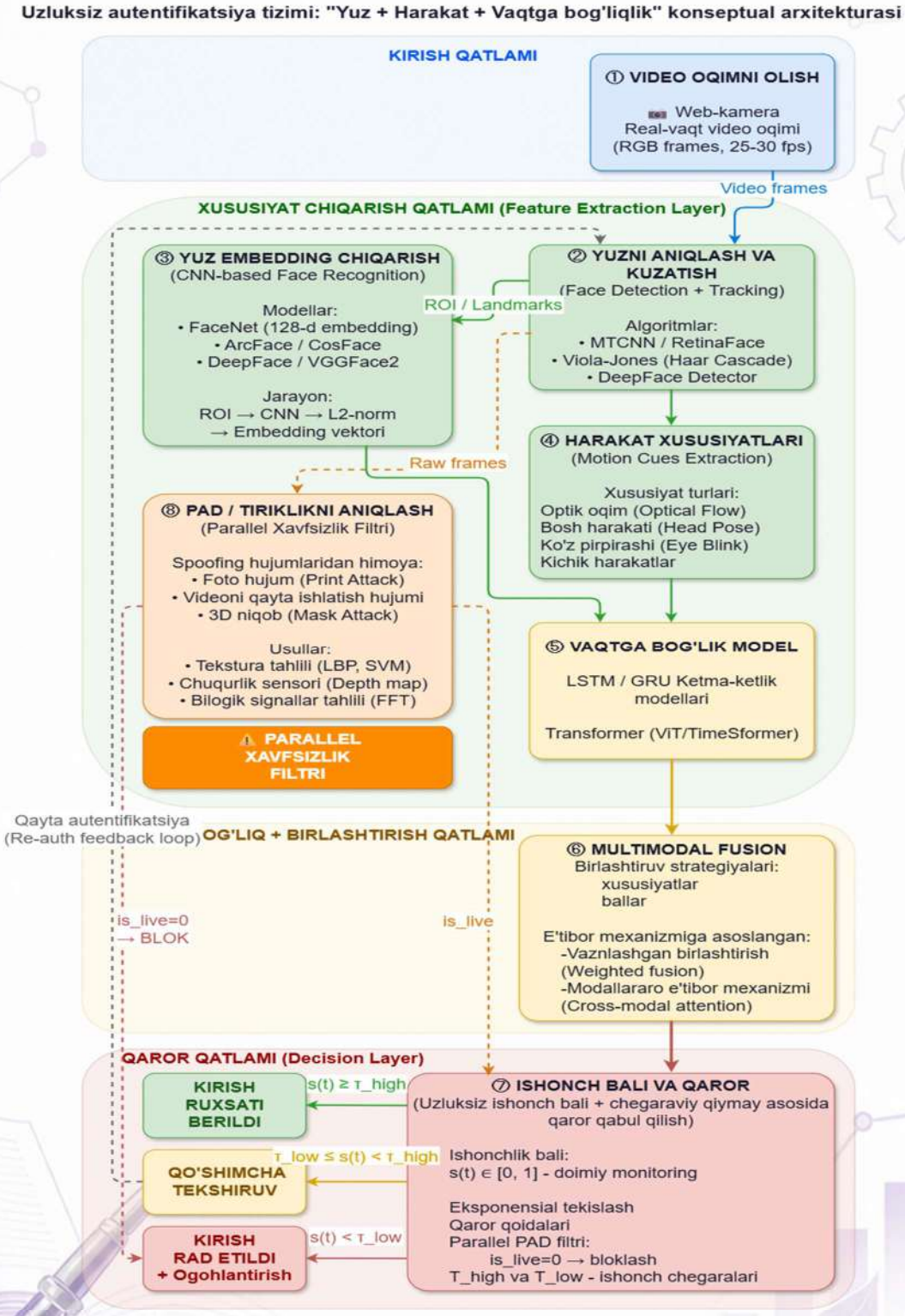
METODOLOGIYA

Ushbu ish mavjud ilmiy manbalardagi yondashuvlarni tizimlashtirish, muammolarni sinflarga ajratish va real vaqt web-kamera uzluksiz autentifikatsiya uchun amaliy tavsiyalarni berishni maqsad qilgan. Manbalar tanlashda uch mezon asos bo‘ldi: (1) uzluksiz autentifikatsiya konsepti va amaliy muammolar (xavfsizlik/maxfiylik/resurs), (2) multimodal fusion strategiyalari va vaqtga bog‘liq modellar, (3) taqdimot hujumlari (spoofing/replay/deepfake) va taqdimot

ISSN 3030-3907

hujumlarini aniqlash (Presentation Attack Detection, PAD)/tiriklikni aniqlashning standart metrikalari [4].

Tahlil natijasida “yuz + harakat + vaqtga bog‘liqlik” asosidagi uzluksiz autentifikatsiya tizimini quyidagi konseptual pipeline sifatida ifodalash mumkin (1-rasm).



1-rasm. Uzluksiz autentifikatsiya tizimi konseptual arxitekturasi. Ma’lumot oqimi va asosiy qatlamlar

ISSN 3030-3907

Yuz embedding (CNN/Face Recognition). Amaliy tizimlar odatda yuzni to‘g‘ridan-to‘g‘ri identifikatsiya qilishdan ko‘ra, avval yuzni kompakt fazoda vektorga aylantirib, keyin masofa/yaqinlik orqali tekshiradi. Masalan, FaceNet yondashuvi yuz tasvirlarini kompakt Evklid fazosiga o‘tkazib, masofani “o‘xshashlik” o‘lchoviga aylantiradi; o‘qitish jarayonida *triplet loss* ishlatilib, bir shaxs ichidagi masofa kichraytiriladi va turli shaxslar orasidagi masofa oshiriladi [5]. FaceNet’da 128 o‘lchamli embedding (kvantlash orqali ixcham saqlash) yondashuvi ham amalda ko‘p uchraydi [5]. Yangi avlod *yuzni chuqur tanish (deep face recognition)* tadqiqotlarida esa diskriminativlikni oshirish uchun *chegaraviy farqqa asoslangan yo‘qotish funksiyalari (margin-based loss)* qo‘llaniladi; *ArcFace additive angular margin* orqali *Gipersfera* geometriyasida sinflar ajraluvchanligini kuchaytirishni taklif qiladi [6].

Harakat modali. Web-kamera oqimida harakat signallari yuzning statik ko‘rinishidagi o‘zgaruvchanlikni qisman kompensatsiya qiladi: boshning burilishi / boshni oldinga-orqaga egilish(pitch) / chapga–o‘ngga burilish(yaw), mikromimika, ko‘z qimirlashi va boshqa kichik harakatlar tiriklik belgilariga ham, shaxsga xos xulq belgilarga ham ishora qilishi mumkin. Bunday signallar ko‘pincha ketma-ket freymlarda barqarorroq ko‘rinadi; shu bois ularni vaqtga bog‘liq model bilan bog‘lash mantiqan asosli [4].

Vaqtga bog‘liq modellar (LSTM/GRU va Transformer). Uzluksiz autentifikatsiyada qaror bitta kadr asosida emas, balki “*sliding window*” ketma-ketligi asosida qabul qilinadi. Bu yondashuv shovqin, qisqa muddatli qisman yopilish holati yoki yoritish o‘zgarishini yumshatadi va “ishtirokchi bir zumga kameraga qaramadi” kabi holatlarni “*yolg‘on bekor*”-ga aylantirib yubormaslikka yordam beradi [3]. Adabiyotlarda vaqt bog‘liq modellashtirish uchun RNN oilasidagi LSTM/GRU chuqur neyron tarmoqlari hamda uzun bog‘liqliklarni ushlashda *o‘zaro e’tibor (self-attention)* mexanizmiga tayanuvchi Transformer arxitekturalari qo‘llanishi haqida bayon qilingan.

Multimodal birlashtirish strategiyalari. Multimodal identifikatsiyada eng kritik arxitektura qarori – qaysi bosqichda birlashtirish. Ilmiy taqdqiqotlar sharhida multimodal identifikatsiyada xususiyatlar, moslik ballari, qaror va reyting darajalarida birlashtirish kabi bir necha birlashtirish strategiyalarini tizimlashtiradi. Bu ish doirasida web-kamera uzluksiz autentifikatsiya uchun ikki amaliy yo‘l ajratildi:

- Xususiyatlar darajasida birlashtirish: yuz embedding + harakat vektorlari vaqtga bog‘liq blokka kirishdan oldin birlashtiriladi; afzalligi – model o‘rganishda boyroq signal ko‘radi, kamchiligi – normalizatsiya, o‘lcham moslash va domen siljishi (domain shift)ga sezgirlik.

ISSN 3030-3907

•Moslik ballar darajasida birlashtirish: har bir modal alohida ballga aylantirilib (masalan, yuz o‘xshashligi + harakat mosligi + tiriklik bali), yakuniy “ishonch bali”ga yig‘iladi; afzalligi – modul/komponentlarni mustaqil sozlash, kamchiligi – optimal og‘irliklarni tanlash va kalibrlash muammosi.

PAD / tiriklikni aniqlash va metrikalar. Spoofing/replay/deepfake kabi hujumlar web-kamera biometrikasining eng kuchsiz nuqtalaridan biri bo‘lib, ularni alohida filtrlash kerak [1]. PAD bo‘yicha ISO standartlari sinash va hisobot tayyorlash tamoyillarini belgilaydi: ISO/IEC 30107-3:2017 PAD mexanizmlarining samaradorlikni baholash prinsiplari, test natijalari hisobotini tayyorlash va ma’lum hujum turlarini tasniflashni ko‘zda tutadi; shu bilan birga, u aniq anti-spoofing algoritmlarini standartlashtirishni o‘z ichiga olmaydi [10]. Standart metrikalar amaliy muhokamada juda muhim: masalan, APCER (attack presentation classification error rate) – hujum namunalarining haqiqiy (bona fide) sifatida noto‘g‘ri tasniflanish ulushi; BPCER (bona fide presentation classification error rate) – haqiqiy (bona fide) namunalarning hujum sifatida noto‘g‘ri rad etilish ulushi [11].

NATIJALAR VA MUHOKAMA.

Ilmiy ishlar sharhi natijalari web-kamera asosidagi “yuz + harakat + vaqtga bog‘liq” uzluksiz autentifikatsiya tizimida muammolarni 5 ta asosiy blokka ajratish mumkinligini ko‘rsatadi: (1) tasvir sifati va real muhitning beqarorligi, (2) spoofing/replay/deepfake, (3) vaqt bo‘yicha barqarorlik va chegaraviy qiymat asosida qaror qabul qilish, (4) real vaqt resurs cheklovlari, (5) maxfiylik.

Tasvir sifati va real muhit beqarorligi. Web-kamera oqimida yuzni aniqlash va embedding chiqarish sifati tasvir sifatiga kuchli bog‘liq. NIST-ning FRVT Quality Assessment konseptual hujjatlarida qayd etilishicha, yuz tasvirlarini almashinuvi va tasvirga olish talablariga oid standartlar mavjud bo‘lishiga qaramay, yuz tasviri sifatini avtomatik baholash hamda ushbu algoritmlarning samaradorligini obyektiv mezonlar asosida baholash bo‘yicha yetuk standartlar yetarli darajada ishlab chiqilmagan. Mazkur muammoni hal etish maqsadida NIST tasvir sifatini skalyar ko‘rsatkich (scalar quality score) ko‘rinishida qaytaruvchi yondashuvlarni ishlab chiqish va ularni standartlashtirilgan baholash metodologiyalari asosida tahlil qilishni ilgari suradi [4].

Amaliy usullar. Tadqiqotlar tahlili shuni ko‘rsatadiki, web-kamera uzluksiz autentifikatsiyada quyidagi amaliy usullar yuqori baholanadi:

•*Quality-aware sample selection*: har bir kadrni tekshirish o‘rniga, sifat bahosi yuqori bo‘lgan freymlarni (yaxshi fokus, mos yaw/pitch, yetarli rezolyutsiya) tanlab olish; bu *yolg‘on bekor qilishni* kamaytirishi va resurs sarfini tushirishi mumkin.

ISSN 3030-3907

•*Face tracking + "best-shot" tanlash*: qisqa vaqt oynasida (masalan 1–3 soniya) bir nechta kadrdan eng yaxshi/eng barqarorini olish – embedding shovqinini kamaytiradi, vaqtga bog‘liq modelga kiruvchi signalni silliqlashtiradi.

•*Margin-based embeddinglar*: FaceNet (triplet-loss asosida) va ArcFace (margin-based loss asosida) kabi embedding yondashuvlari amaliyotda yuqori darajadagi diskriminativ xususiyatlarni shakllantirishga xizmat qiladi. Bu esa uzluksiz autentifikatsiya tizimlarida yuz signali sifatini oshirish va identifikatsiya aniqligini yaxshilash uchun muhim omil hisoblanadi.

Spoofing, replay va deepfake. Uzluksiz autentifikatsiyada tahdid modeli odatda tasodifiy emas: hujumchi foto ko‘rsatishi, ekran orqali videoni qayta qo‘yishi yoki deepfake orqali real vaqtga yaqin manipulyatsiya qilishi mumkin; shuning uchun tiriklik/PAD blokini alohida qatlam sifatida qo‘shish talab etiladi.

Standart metrikalar va hisobot tayyorlash. PAD baholashda APCER/BPCER kabi metrikalar tizimning xavfsizlik-qulaylik kompromissini aniq ko‘rsatadi: APCER past bo‘lsa – hujumni o‘tkazib yuborish kamayadi, BPCER past bo‘lsa – real foydalanuvchini noto‘g‘ri rad etish kamayadi [11]. ISO/IEC 30107-3 esa PAD mexanizmlarini baholash va hisobot tayyorlash uchun metodik qo‘llanma beradi [10].

Deepfake texnologiyalarining umumlashtirish muammosi. Zamonaviy multimedia forensika tadqiqotlarida deepfake aniqlash usullari uchun cross-dataset baholash muhim metodologik bosqich sifatida qaraladi. Bunga sabab, real sharoitda o‘qitish ma’lumotlaridan farq qiluvchi yangi hujum turlarining doimiy ravishda yuzaga kelishi va "statik distribusiya" farazining buzilishidir. Ushbu holat modelning ilgari ko‘rilmagan hujumlarga nisbatan umumlashtirish qobiliyatining pasayishiga olib keladi. Eng xavfli ssenariya – uzluksiz autentifikatsiya tizimida yuz signali "ishonchli" ko‘ringani holda, hujumchi deepfake/replay bilan tizimni aldashi. Shu bois PAD nafaqat bir martalik kirish bosqichida, balki sessiya davomida ham (masalan, davriy yoki trigger asosida) ishlashi maqsadga muvofiq [12].

Vaqt bo‘yicha barqarorlik va chegaraviy qiymat asosida qaror qabul qilish. Uzluksiz autentifikatsiya qarori odatda bitta embedding mosligiga emas, vaqt bo‘yicha yig‘ilgan dalillarga tayanadi. Bu yondashuvning kuchli tomoni – "bir kadrdagi shovqin"ni kamaytirish, lekin zaif tomoni – *chegaraviy qiymat* va *oynaning uzunligini* noto‘g‘ri tanlashda tizim kechikishi yoki *yolg‘on ogohlantirish* ko‘payishi.

Tadqiqotlar tahlili asosida tavsiyalar:

•*Sliding window + silliqlashtirish*: ballarni (yuz o‘xshashligi darajasi, harakatning izchilligi, tiriklik ko‘rsatkichi) vaqt bo‘yicha silliqlashtirish va qarorni

ISSN 3030-3907

bir nechta ketma-ket *oynalarda* mustahkamlash – uzluksiz autentifikatsiyada keng qo‘llaniladigan holat sifatida qaraladi.

•*Moslashuvchan chegaraviy qiymat asosida qaror qabul qilish*: yorug‘lik sharoitlarining o‘zgarishi, kameraga masofaning ortishi yoki yuzning qisman yopilishi kabi omillar ta’sirida qaror chegarasini dinamik tarzda moslashtirish, shuningdek past sifatli tasvirlar uchun qayta namuna olish mexanizmlarini qo‘llash yolg‘on rad etish darajasini kamaytirishga xizmat qiladi. Mazkur yondashuvni samarali tashkil etishda tasvir sifati bahosi konseptlari asosiy metodologik omil hisoblanadi [4].

Real vaqt hisoblash va resurs cheklovlari

Web-kamera asosidagi uzluksiz autentifikatsiya tizimlarining amaliy qo‘llanishi hisoblash resurslari cheklovlari bilan chambarchas bog‘liq. Uzluksiz video oqimini qayta ishlash yuqori darajadagi CPU/GPU yuklanishini keltirib chiqaradi, energiya sarfini oshiradi va natijada tizimning foydalanuvchi tajribasiga (user experience) salbiy ta’sir ko‘rsatishi mumkin [4]. Resurs cheklangan qurilmalarda uzluksiz autentifikatsiya yondashuvlari “kam tekshiruv bilan yetarli ishonch” tamoyiliga intiladi: masalan, ayrim ishlar yuzni embeddingga aylantirib, atrof-muhit triggerlari (yorug‘lik yoki shovqin o‘zgarishi) bo‘lganda qayta tekshiruvni amalga oshirish orqali ortiqcha tekshiruvlarni kamaytirishni ko‘rsatadi [3]. Ushbu konsepsiya web-kamera asosidagi uzluksiz autentifikatsiya tizimlariga tatbiq etilishi mumkin. Doimiy ravishda har bir kadr uchun *inference* bajarish o‘rniga, adaptiv monitoring strategiyasini qo‘llash tavsiya etiladi: (a) bosh holati, fokus yoki tasvir sifati o‘zgarishida, (b) foydalanuvchining ekran bilan o‘zaro masofasi o‘zgarganda, (c) liveness bo‘yicha shubhali signallar aniqlanganda tekshiruv jarayoni kuchaytiriladi.

1-jadval ilmiy ishlar tahlili asosida “yuz, harakat, vaqtga bog‘liq model va PAD” komponentlaridan tashkil topgan tizimda uchraydigan muammolar hamda ularga mos yechim yo‘nalishlarini tizimli ravishda umumlashtiradi.

1-jadval.

Multimodal uzluksiz autentifikatsiya tizimining (yuz, harakat, temporal model va PAD) komponentlari bo‘yicha muammo va yechimlar tahlili

Komponent	Tipik signal yoki algoritm	Tipik muammo	Review asosidagi yechim yo‘nalishi (misollar)
Yuz embedding (CNN)	Yuz embedding, kosinius yoki Evklid masofasi	Rakurs, yorug‘lik va qisman yopilish sabab	Sifatga asoslangan kadr tanlash; kuzatish; diskriminativ yo‘qotish

ISSN 3030-3907

		o‘xshashlik pasayishi	funksiyalari (FaceNet, ArcFace oilasi) [5,6]
Harakat	Bosh holati (pitch/yaw), kichik harakatlar, vaqt bo‘yicha izchillik	Statik rasm yoki replay hujumlarini ajratish qiyinligi	Harakatni tiriklik signali sifatida qo‘shish; Vaqt bo‘yicha izchillikni tekshirish [4]
Vaqtga bog‘liq model	LSTM/GRU, Transformer	Vaqt oynasi parametrlari va chegaraviy qiymat noto‘g‘ri tanlanganda kechikish yoki yolg‘on ogohlantirish	*Sliding window* asosida silliqlashtirish; moslashuvchan chegaraviy qiymat; sifat bahosi asosida tanlab olish [3]
Birlashtirish	Xususiyatlar darajasi yoki moslik ballari darajasida birlashtirish	Kalibrlash muammolari, modal signallar siljishi, domen siljishi	Birlashtirish strategiyalarini tizimli tanlash (feature/score/decision); modullarni kalibrlash [4]
PAD / tiriklikni aniqlash	APCER/BPCER metrikalari asosida baholash	Deepfake va yangi turdagi hujumlarda umumlashtirish muammosi	ISO/IEC 30107-3 asosida testlash; cross-dataset baholash; davriy PAD [10-11]

XULOSA.

Ilmiy tadqiqotlar tahlili shuni ko‘rsatadiki, web-kamera asosida uzluksiz autentifikatsiya qilishda faqat *yuzni tanishga* tayanish ko‘pincha yetarli emas: real muhitdagi tasvir sifati, qisman yopilish va yoritish o‘zgarishi, shuningdek spoofing/replay/deepfake tahdidlari bitta modalni zaiflashtiradi. Shu bois multimodal yonfashuv – yuz embedding + harakat signallari + vaqtga bog‘liq modellashtirish + PAD/tiriklikni aniqlash – amaliy barqarorlikni oshiruvchi asosiy yo‘nalish sifatida ajralib chiqadi. Multimodal birlashtirish strategiyalari (feature/score/decision) bo‘yicha ilmiy tadqiqotlar bunday tizimlarni konseptual asoslash va arxitektura tanlovlarini tartibga solish uchun nazariy asos beradi.

Multimodal yondashuvlar barcha muammolarni avtomatik ravishda hal etmaydi. Birinchidan, real vaqtli hisoblash resurslari cheklovlari sharoitida *inference* chastotasini optimallashtirish, xususan trigger asosida va sifat

ISSN 3030-3907

ko‘rsatkichiga asosida tanlab olish mexanizmlarini joriy etish zarur. Ikkinchidan, PAD tizimlarini ISO/IEC 30107-3 standartiga muvofiq APCER va BPCER metrikalari asosida baholash hamda natijalarni standartlashtirilgan shaklda hisobot ko‘rinishida taqdim etish talab etiladi. Uchinchidan, deepfake texnologiyalarining jadal rivojlanishi fonida cross-dataset umumlashtirish muammosi dolzarbligicha qolmoqda. To‘rtinchidan, maxfiylik masalalari tizim arxitekturasining markazida turishi zarur, chunki demografik farqlar va ma’lumotlar maxfiyligi bilan bog‘liq xavflar uzluksiz autentifikatsiya tizimlarining amaliy qo‘llanishiga bevosita ta’sir ko‘rsatadi.

FOYDALANILGAN ADABIYOTLAR

1. Baig, A.F., Eskeland, S. (2021). Security, Privacy, and Usability in Continuous Authentication: A Survey. Sensors, 21(17), 5967.
2. Ammour, N., Bazi, Y., Alajlan, N. (2023). Multimodal Approach for Enhancing Biometric Authentication. Journal of Imaging, 9(9), 168.
3. Zeeshan, N., Moradpoor, N., La Spada, L. (2025). Continuous Authentication in Resource-Constrained Devices via Biometric and Environmental Fusion. Sensors, 25(18), 5711.
4. Qin, Z., Zhao, P., Zhuang, T., Deng, F., Ding, Y., Chen, D. (2023). A survey of identity recognition via data fusion and feature learning. Information Fusion, 91, 694–712.
5. Schroff, F., Kalenichenko, D., Philbin, J. (2015). FaceNet: A Unified Embedding for Face Recognition and Clustering.
6. Deng, J., Guo, J., Yang, J., et al. (2019). ArcFace: Additive Angular Margin Loss for Deep Face Recognition.
7. Grother, P., Ngan, M., Hanaoka, K. (2019). FRVT Ongoing: Face Recognition Quality Assessment—Concept and Goals.
8. NIST. Face Recognition Vendor Test (FRVT): Program Overview and Reports.
9. Grother, P. (2022). Face Recognition Vendor Test (FRVT) Part 8: Summarizing Demographic Differentials (NIST IR 8429).
10. ISO/IEC 30107-3:2017. Biometric presentation attack detection — Testing and reporting.
11. Busch, C. The ISO/IEC 30107-3 standard for testing of Presentation Attack Detection (PAD).
12. Amerini, I., et al. (2025). Deepfake Media Forensics: Status and Future Challenges.

ISSN 3030-3907