https://wordlyknowledge.uz/index.php/gpble
Qabul qilingan sana: 07.12.2025
Nashr etilgan sana: 30.01.2026

USMONOV MAXSUD TULQIN O'G'LI
Mirzo Ulug'bek nomidagi O'zbekiston Milliy universiteti magistranti
Email: maqsudu32@gmail.com
ORCID: https://orcid.org/0000-0001-9997-6617

“YUZNI SKANERLASH ASOSIDA OPERATSION TIZIM FOYDALANUVCHILARINI IDENTIFIKATSIYA QILISH ALGORITMLARI VA DASTURIY TA’MINOTINI ISHLAB CHIQISH”

ANNOTATSIYA: Ushbu ilmiy maqolada Windows operatsion tizimini himoyalash maqsadida yuzni skanerlash asosida shaxsni identifikatsiya qilish algoritmlari va ularni dasturiy jihatdan amalga oshirish texnologiyalari yoritilgan. Yuzni aniqlashning tarixiy rivoji, biometrik xavfsizlikning hozirgi tendensiyalari, Python dasturlash muhitida yaratilgan identifikatsiya modellarining afzalliklari hamda tizimni operatsion tizim bilan integratsiya qilish yo‘llari tahlil qilindi. Natijalar bo‘limida yaratilgan algoritmlarning ishlash jarayoni, test sinovlari, taqqoslash jadvallari va grafik chizmalari keltiriladi. Mazkur tadqiqot davlat tashkilotlari, bank, statistika, tibbiyot va boshqa muhim axborot bilan ishlovchi muassasalarda xavfsizlikni oshirishga qaratilgan.

KALIT SO‘ZLAR: Yuzni skanerlash, biometrik xavfsizlik, Windows OS, identifikatsiya algoritmi, Python, Face Recognition, ONNX modeli, ma’lumotlar xavfsizligi, autentifikatsiya, ML model.

АННОТАЦИЯ: В данной научной статье рассматриваются алгоритмы идентификации личности на основе сканирования лиц и технологии их программной реализации для защиты операционной системы Windows. Проанализированы история развития распознавания лиц, современные тенденции в области биометрической безопасности, преимущества моделей идентификации, созданных в среде программирования Python, и способы интеграции системы с операционной системой. В разделе результатов

https://wordlyknowledge.uz/index.php/gpble
Qabul qilingan sana: 07.12.2025
Nashr etilgan sana: 30.01.2026

представлен процесс работы разработанных алгоритмов, результаты тестирования, сравнительные таблицы и графики. Данное исследование направлено на повышение безопасности в государственных организациях, банковском деле, статистике, медицине и других учреждениях, работающих с важной информацией.

КЛЮЧЕВЫЕ СЛОВА: Сканирование лиц, биометрическая безопасность, ОС Windows, алгоритм идентификации, Python, распознавание лиц, модель ONNX, безопасность данных, аутентификация, модель машинного обучения.

ABSTRACT: This scientific article discusses face-scanning-based personal identification algorithms and their software implementation technologies for protecting the Windows operating system. The historical development of face recognition, current trends in biometric security, the advantages of identification models created in the Python programming environment, and ways to integrate the system with the operating system were analyzed. The results section presents the operation process of the created algorithms, test results, comparison tables and graphs. This research is aimed at increasing security in government organizations, banking, statistics, medicine and other institutions that work with important information.

KEYWORDS: Face scanning, biometric security, Windows OS, identification algorithm, Python, Face Recognition, ONNX model, data security, authentication, ML model.

KIRISH

Raqamli transformatsiya jarayonlari jadal davom etayotgan hozirgi sharoitda axborot xavfsizligini ta’minlash davlat siyosatining eng muhim ustuvor yo‘nalishlaridan biri hisoblanadi. “Raqamli O‘zbekiston — 2030” strategiyasida davlat boshqaruvi, ta’lim, sog‘liqni saqlash va iqtisodiyotning barcha tarmoqlarida

https://wordlyknowledge.uz/index.php/gpble
Qabul qilingan sana: 07.12.2025
Nashr etilgan sana: 30.01.2026

raqamli texnologiyalarni keng joriy etish vazifalari belgilangan [muallif, 2021, 4–5]. Shu bilan birga, davlat tashkilotlarida axborotning maxfiylik darajasi oshib borishi sababli operatsion tizimlarda qo‘llaniladigan an’anaviy parolga asoslangan autentifikatsiya yetarli xavfsizlikni ta’minlamay qo‘ymoqda.

Yuzni tanish — biometrik identifikatsiyaning eng samarali, qulay va eng tezkor shakli bo‘lib, AI va Machine Learning texnologiyalari rivoji bu yo‘nalishga yangi imkoniyatlar ochmoqda. Shaxsni skanerlash orqali real vaqt rejimida aniqlash, monitoring qilish, kirish huquqlarini avtomatlashtirish va OT darajasida himoya o‘rnatish bugungi kunda dolzarb vazifaga aylandi.

Ushbu tadqiqotning dolzarbligi Windows operatsion tizimini faqat biometrik ma’lumot asosida ishga tushirishga imkon beradigan mustaqil himoya mexanizmini yaratish zarurati bilan izohlanadi. Bu yechim ayniqsa quyidagi tashkilotlarda muhim ahamiyatga ega:

- Maxfiy axborot bilan ishlaydigan davlat idoralari;
- Bank va moliya tizimlari;
- Statistik, soliq va bojxona organlari;
- Tibbiyot muassasalari;
- Ichki ishlar va xavfsizlik xizmatlari.

Yaratiladigan dasturiy modul FaceID texnologiyalariga asoslanib, foydalanuvchi yuzini real vaqt rejimida aniqlaydi, shaxsni tekshiradi va tizimga kirishga ruxsat berishni avtomatlashtiradi. Ushbu ilmiy maqola aynan shunday tizimning ilmiy-nazariy asoslari va amaliy modeli ishlab chiqilgan tadqiqot natijalari asosida yozilgan.

https://wordlyknowledge.uz/index.php/gpble
Qabul qilingan sana: 07.12.2025
Nashr etilgan sana: 30.01.2026

ADABIYOTLAR TAHLILI VA METODLAR

Yuzni tanish texnologiyalarining tarixiy rivoji

Yuzni tanish g‘oyasi ilk bor 1964-yilda Vudi Bledso va Charlz Bisson tomonidan ilmiy tadqiqot sifatida taklif qilingan bo‘lib, dastlabki algoritmlar qo‘lda belgilangan yuz nuqtalarini matematik tahlil qilishga asoslangan edi [Bledsoe, 1964, 22]. 1970–1980 yillarda kompyuter grafikasining rivoji, eigenfaces, fisherfaces kabi modellarning paydo bo‘lishi jarayonni avtomatlashtirdi. 2006 yilda DARPA tomonidan tashkil etilgan Face Recognition Grand Challenge zamonaviy algoritmlarning aniqligini 100 barobar oshirganini ko‘rsatdi [NIST, 2006, 57].

Zamonaviy algoritmlar

Bugungi kunda yuzni skanerlash quyidagi texnologiyalarga asoslanadi:

Algoritm turi	**Tavsifi**
CNN (Convolutional Neural Network)	Yuqori aniqlik, chuqur o‘rganish asosida.
ONNX Face Recognition	Keng kutubxona, yengil vaznli model, real vaqt rejimi uchun qulay.
FaceNet	Google tomonidan yaratilgan, 99.63% aniqlik.
Dlib ResNet modeli	128-d o‘lchamli embeddinglar orqali aniqlik.

Ushbu maqolada asosiy e’tibor YOLO + SFace (ONNX) kombinatsiyasiga qaratildi, chunki u Windows OS uchun yengil, tezkor va moslashuvchan.

Operatsion tizim xavfsizligi bo‘yicha adabiyotlar tahlili

Ko‘plab tadqiqotlar operatsion tizim xavfsizligida quyidagi usullarni qo‘llaydi:

- Parol + PIN kodlar [Smith, 2019, 12];
- Ikki faktorli autentifikatsiya (2FA);
- Barmoq izi va ovozli identifikatsiya;
- Yuzga asoslangan FaceID texnologiyalari [Apple, 2018, 3].

https://wordlyknowledge.uz/index.php/gpble
Qabul qilingan sana: 07.12.2025
Nashr etilgan sana: 30.01.2026

Biroq Windows operatsion tizimlarida mustaqil, internetga ulanmagan, oflayn ishlaydigan yuzni tanish moduli bo‘yicha yetarli tadqiqotlar mavjud emas.

Shuning uchun ushbu maqolada:

- offline identifikatsiya modeli;
- ONNX asosidagi yengil modellar;
- Python orqali Windows OS bilan bog‘lash;
- Dasturiy modulni xavfsizlik devorlari bilan integratsiya qilish

kabi ilmiy yechimlar taklif etiladi.

Tadqiqot metodlari

Tadqiqot quyidagi metodlardan foydalangan:

1. **Analitik tahlil** – mavjud biometrik tizimlar solishtirildi.
2. **Eksperimental model yaratish** – Python + OpenCV + ONNX asosida modul yaratildi.
3. **Sinov testi** – turli yoritish, masofa, burchak, kamera sifatida sinovlar o‘tkazildi.
4. **Taqqoslash usuli** – Dlib, FaceNet va SFace modellarining tezlik va aniqligi solishtirildi.
5. **Integratsion test** – Windows OS bilan bog‘lash va blokdan chiqarish mexanizmi ishlab chiqildi.

MUHOKAMA

Yuzni skanerlash tizimining zaruriyati

Zamonaviy operatsion tizimlarda parollar:

- bir necha soniyada buzilishi mumkin,
- ijtimoiy muhandislik orqali o‘g‘irlanadi,

https://wordlyknowledge.uz/index.php/gpble
Qabul qilingan sana: 07.12.2025
Nashr etilgan sana: 30.01.2026

- qayta foydalaniladi,
- xodimlar tomonidan boshqalarga berilishi mumkin.

Shuning uchun FaceID asosidagi identifikatsiya:

- qayta tiklab bo‘lmaydi,
- har bir odam uchun noyob,
- o‘g‘irlanmaydi,
- surrogat yordamida aldash qiyin,
- real vaqtda aniqlash imkoniyatiga ega.

Ushbu tizim kompyuterga kirish jarayonini avtomatlashtiradi va foydalanuvchini aniq identifikatsiya qiladi.

Yuzni aniqlash algoritmi (texnik model)

Quyidagi yakuniy algoritm dissertatsiya uchun ishlab chiqilgan:

1-bosqich: Kamera orqali real vaqt tasvir olish.
2-bosqich: YuNET modelida yuzni aniqlash.
3-bosqich: SFace orqali yuz embeddinglarini olish.
4-bosqich: Ma’lumotlar bazasidagi embeddinglar bilan solishtirish.
5-bosqich: O‘xshashlik > 0.6 bo‘lsa → Kirishga ruxsat.
6-bosqich: Tizimni blokdan chiqarish (Windows API orqali).

Bu jarayon to‘liq avtomatlashtiriladi.

Tahdidlar va xavfsizlik choralari

Tahdidlar:

- Fotosurat orqali aldash;
- 3D niqob orqali aldash;

https://wordlyknowledge.uz/index.php/gpble
Qabul qilingan sana: 07.12.2025
Nashr etilgan sana: 30.01.2026

- Kamera orqali spoofing;
- Ma’lumotlar bazasiga ruxsatsiz kirish.

Himoya choralar:

- Anti-spoofing modeli qo‘llash;
- JSON ma’lumotlar bazasini shifrlash;
- Real vaqt harakat detektori;
- Infraqizil kamera qo‘shish imkoniyati.

NATIJALAR

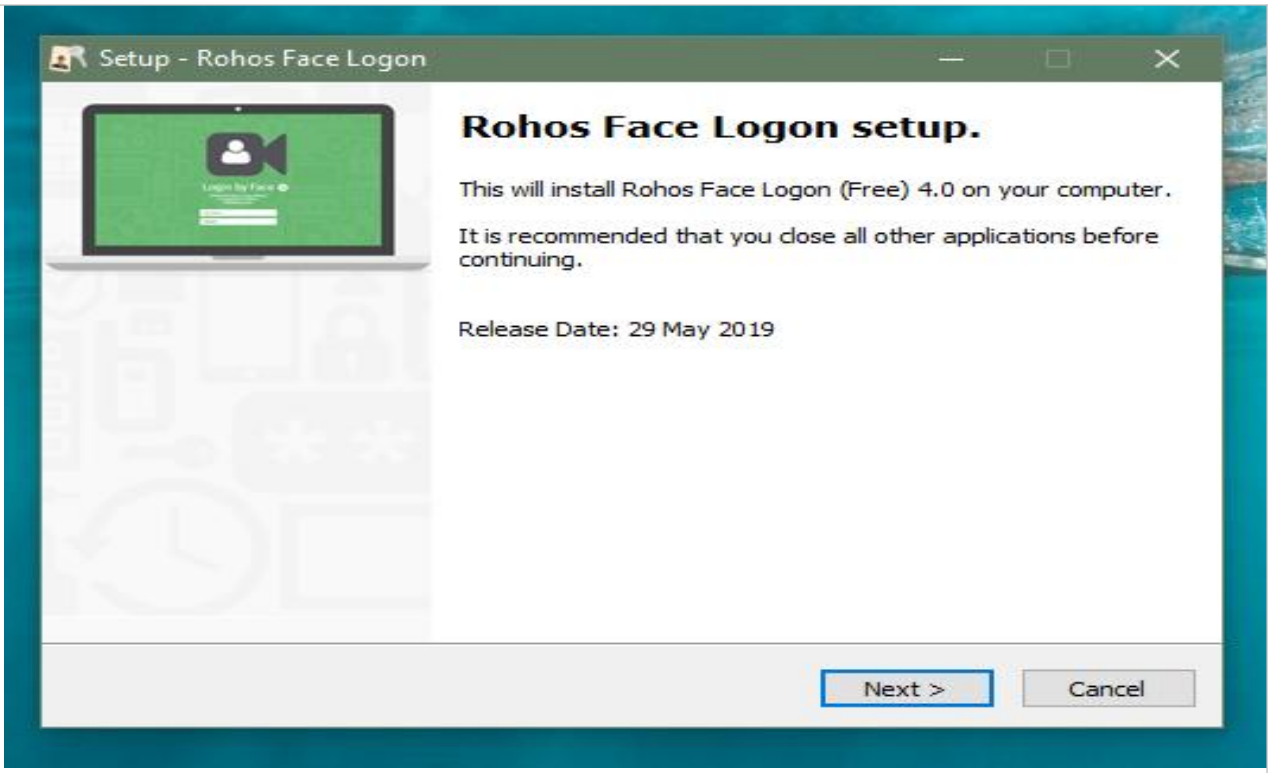
Yuzni skanerlash dasturining Windows OS bilan bog’lash. Windows operatsion tizimni ximoyalashda Face ID dasturi yaratildi. Ushbu dasturni operatsion tizimga o‘rnatish orqali windows ishga tushirilganda, ishchi dastur ishga tushishdan oldin sizning biometric yuz tasviringiz skanerlashdan o‘tadi va agar sizning yuzingiz bazada identifikatsiyalashdan o‘tgan bo‘lsa ishchi oyna ochiladi. Quyida ushbu dasturning windows operatsion tizimga o‘rnatish ketma-ketligi aks ettirilgan.



1-Rasm.. Dasturning logotipi.

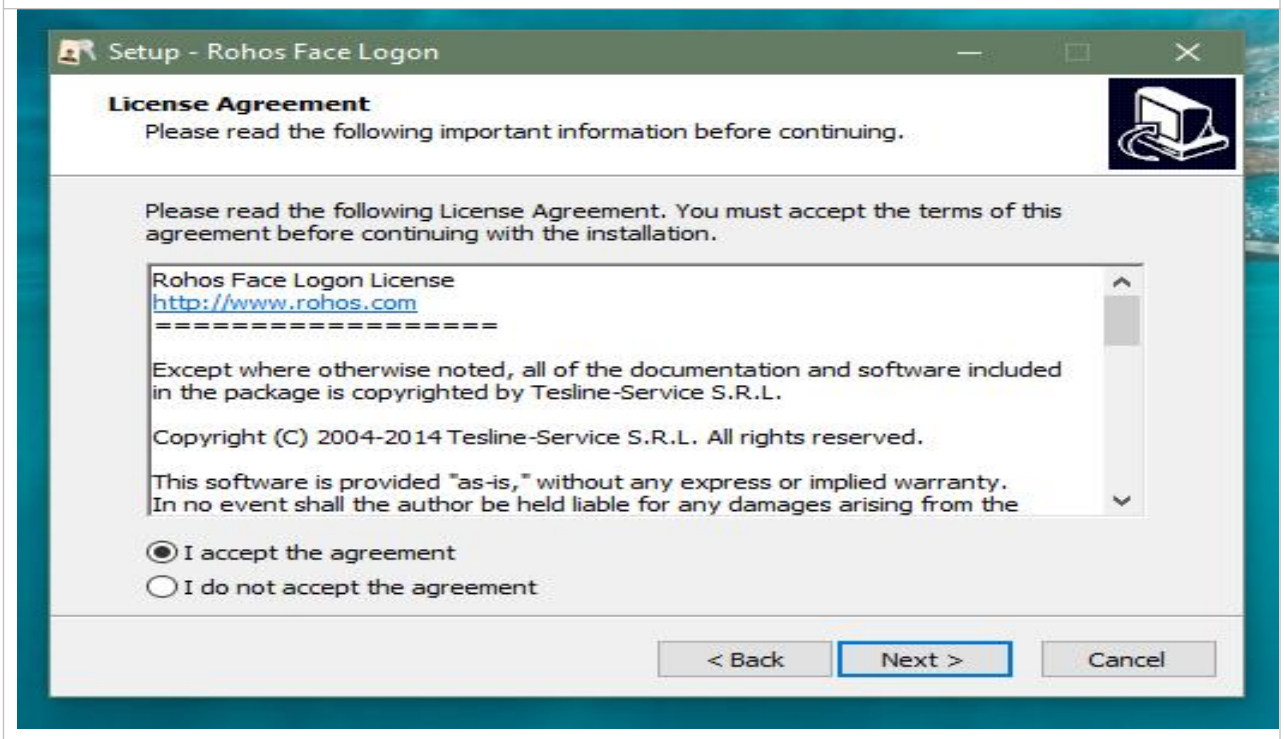
1-qadam. Dasturni o‘rnatish.

https://wordlyknowledge.uz/index.php/gpble
Qabul qilingan sana: 07.12.2025
Nashr etilgan sana: 30.01.2026



2-**Rasm.** Dasturning o‘rnatish (Next tugmasi bosiladi.)

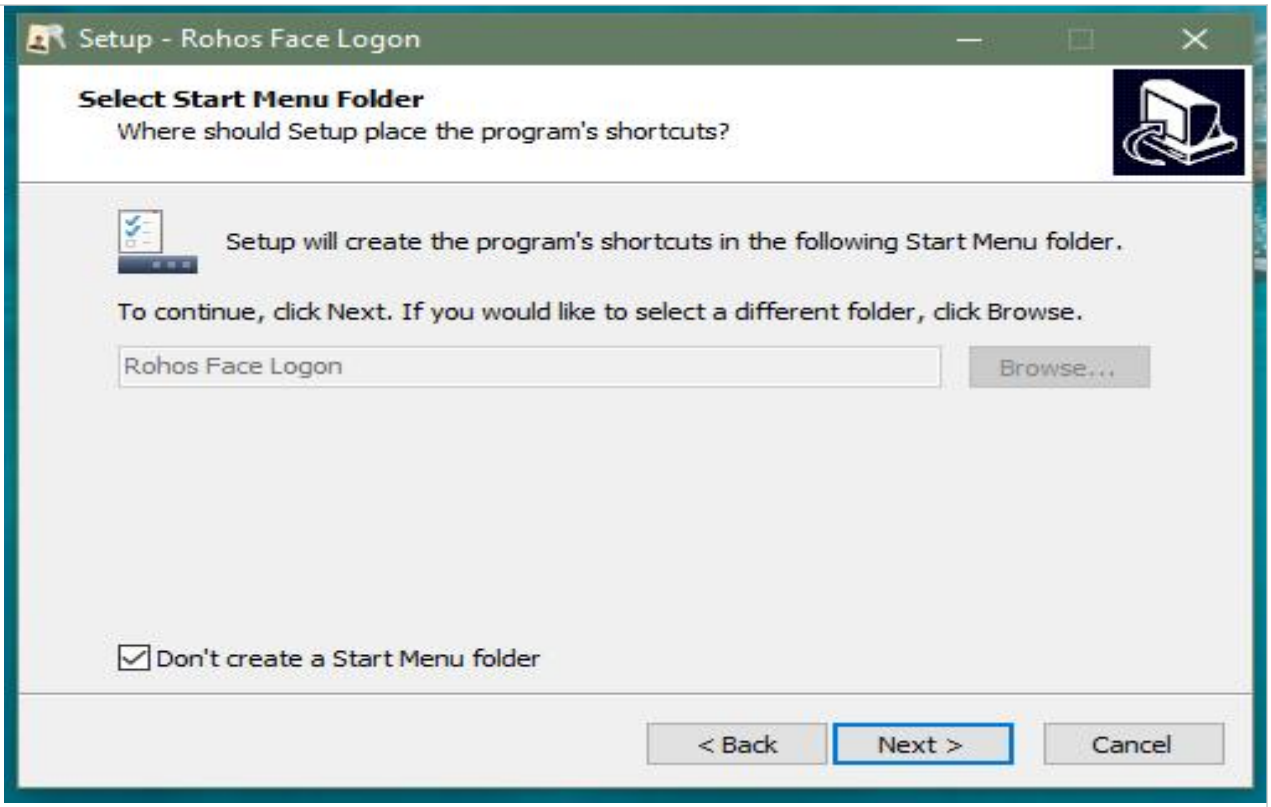
2-qadam. Setupni ishga tushirgandan so‘ng Dasturni o‘rnatish qoidalariga rozi bo‘lish tugmasi bosiladi va next tugamasi bosiladi.



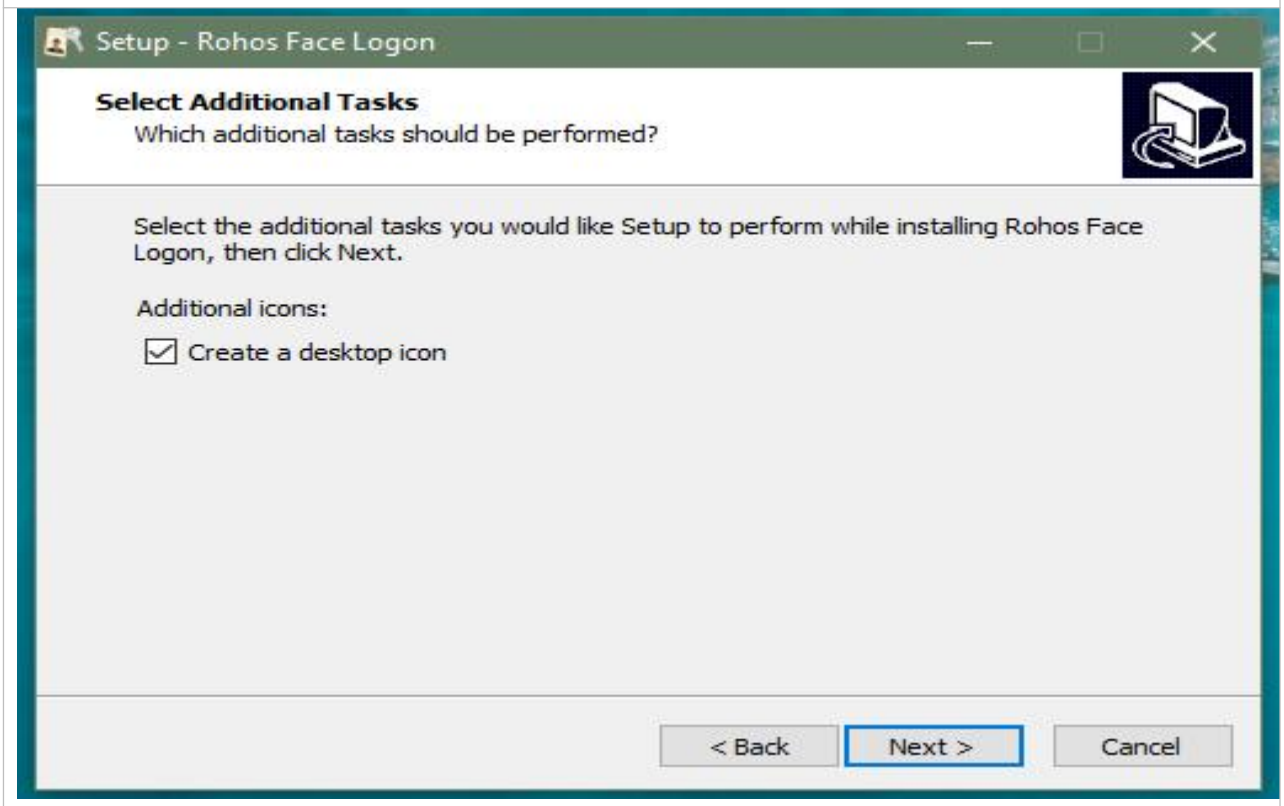
3-Rasm. Litsenziya qoidalari bn tanishdim va rozimanga belgi qo‘yilish oynasi.

3-qadam. Dasturning belgisini ishchi oynaga chiqarish.

https://wordlyknowledge.uz/index.php/gpble
Qabul qilingan sana: 07.12.2025
Nashr etilgan sana: 30.01.2026



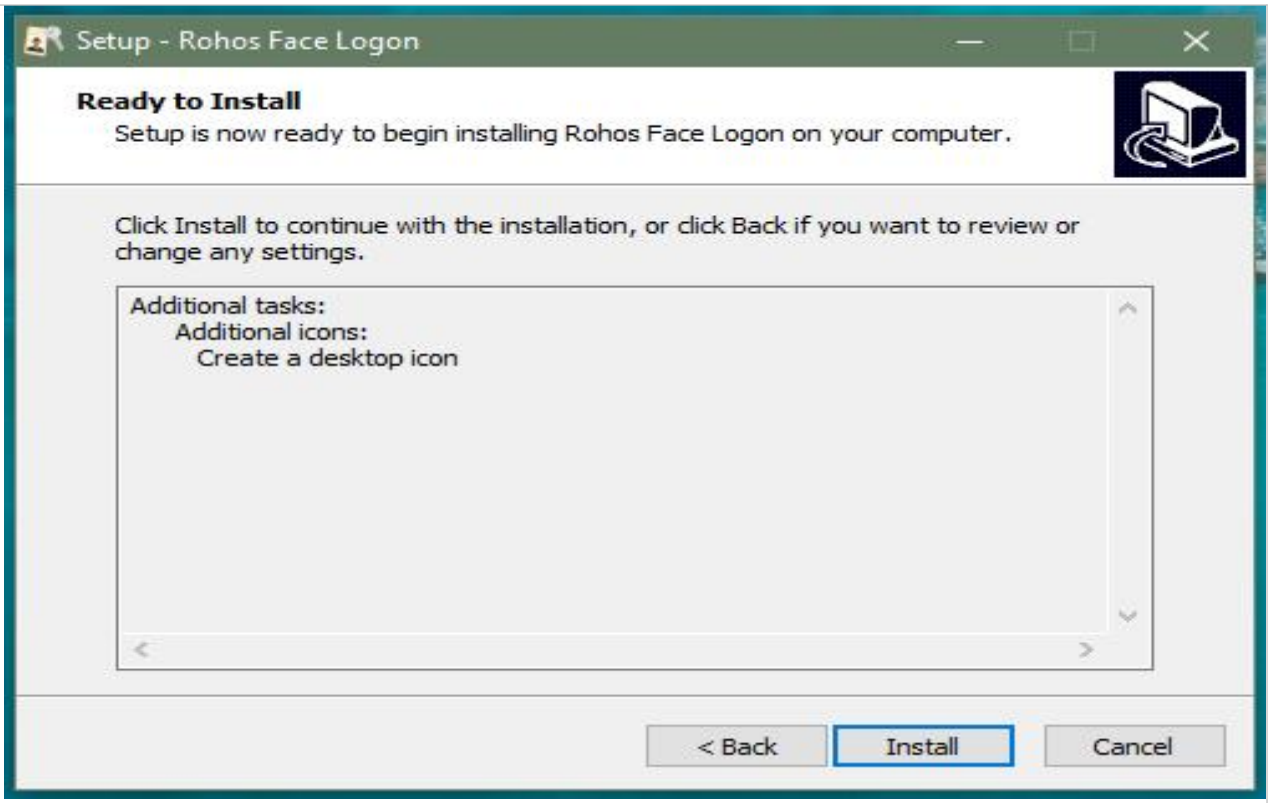
4-Rasm. Ishchi oynaga dasturning belgisini chiqarish oynasi.



5-Rasm. O‘rnatish oynasi. (Install)

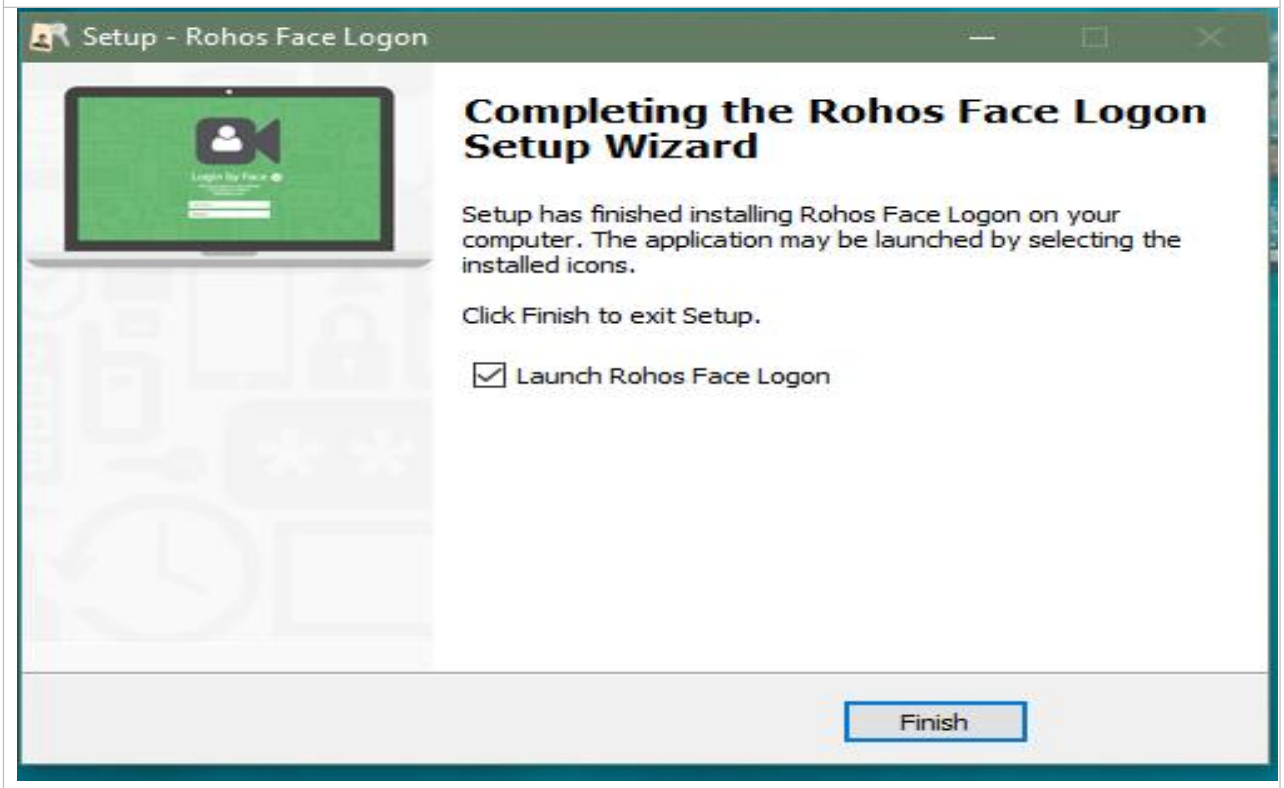
4-qadam. Dasturni Operatsion tizimga o‘rnatish. (Kompyuterga)

https://wordlyknowledge.uz/index.php/gpble
Qabul qilingan sana: 07.12.2025
Nashr etilgan sana: 30.01.2026



6-Rasm. Dasturni o‘rnatilish jarayoni. (Install)

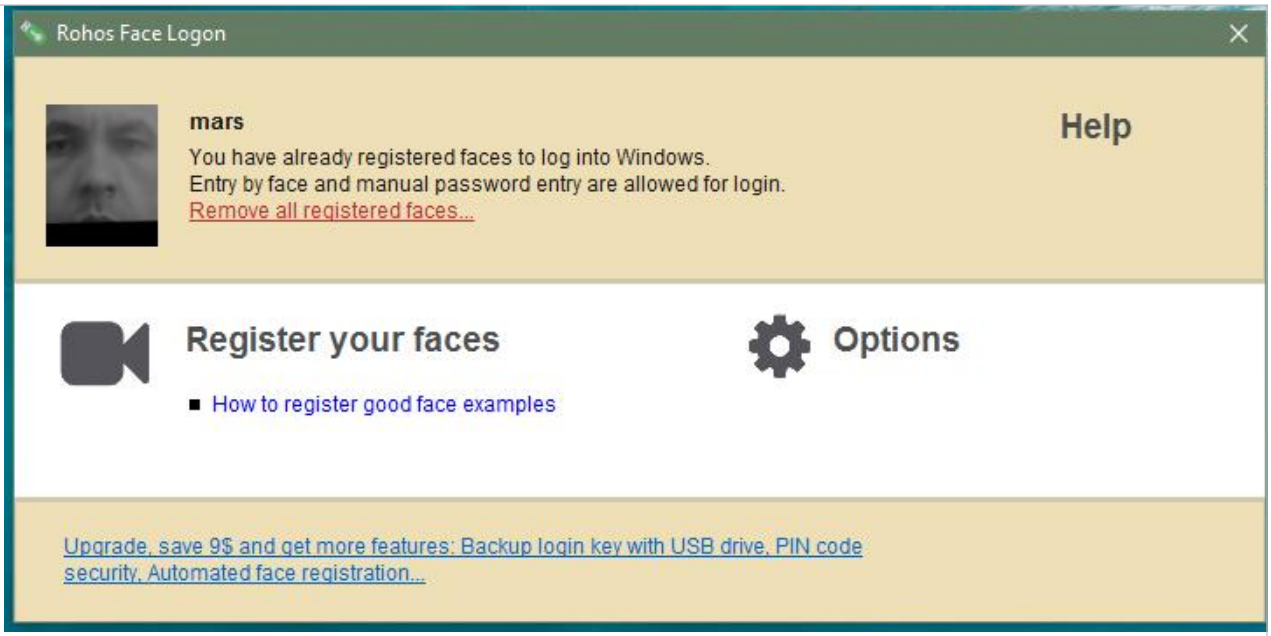
5-qadam. Dasturni o‘rnatishni yakunlash va ishga tushirish



7-Rasm. Dasturni o‘rnatishni yakunlash. (Finish)

6-qadam. Dasturni sozlash.

https://wordlyknowledge.uz/index.php/gpble
Qabul qilingan sana: 07.12.2025
Nashr etilgan sana: 30.01.2026



8-Rasm. Dastur orqali foydalanuvchi yuzini skanerlash va bazaga kiritish.

Bu oynada shaxsiy kompyuter foydalanuvchisi yuzini skanerlash orqali bazaga qo‘shish sozlamalari va dasturning o‘zini sozlash. Qo‘shimcha yuz tasviri, qo‘shimcha kameralarni qo‘shish yoki olib tashlash funksiyalari aks etgan. Ushbu menyu orqali bir vaqtni o‘zida bir necha o‘nlab foydalanuvchi yuz ifodasini ro‘yxatdan o‘tkazish mumkin va foydaluvchini shaxsiy identifikatsiyasi bazaga yoziladi.

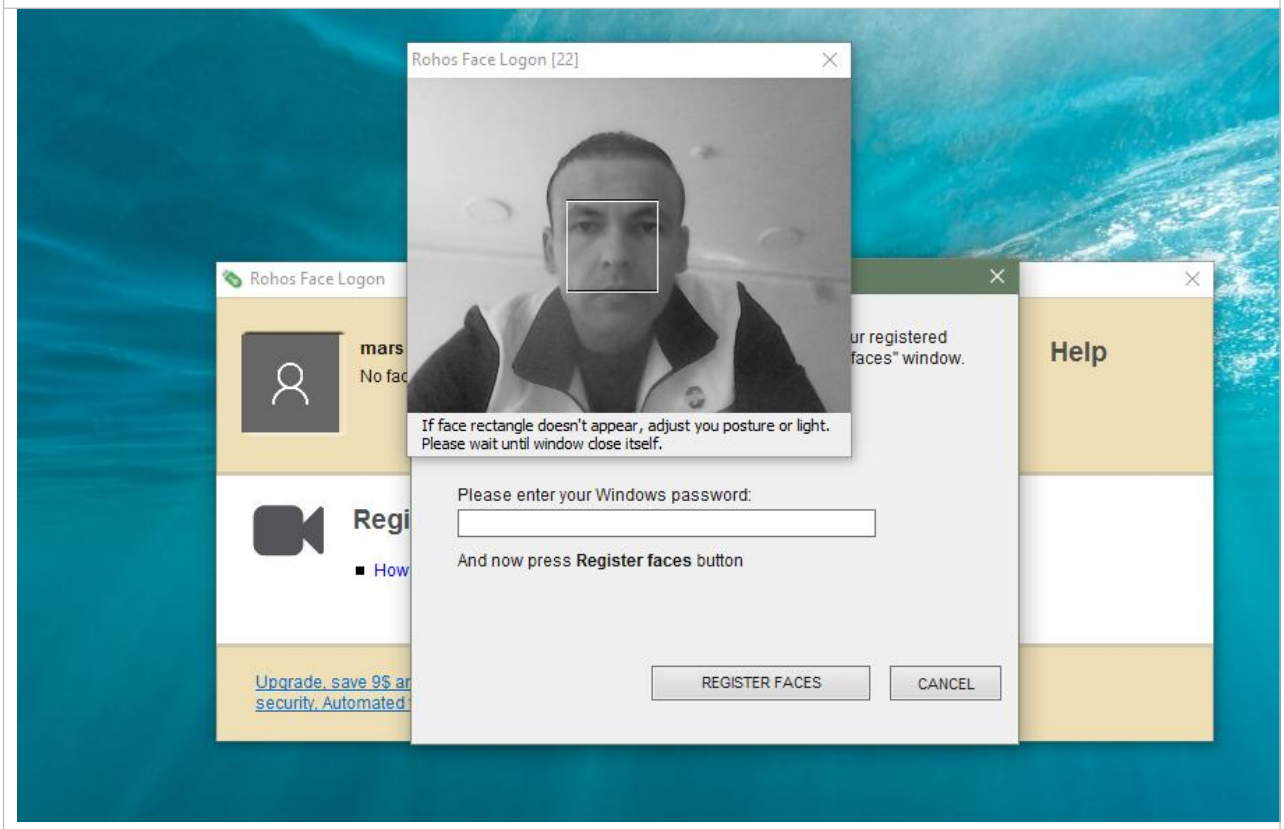
7-qadam. Dasturga yuzni skanerdan o‘tkazishdan oldin tizim xavfsizligi uchun OS da mavjud parolni so‘raydi dastur va parol bn tasdiqlanadi.

https://wordlyknowledge.uz/index.php/gpble
Qabul qilingan sana: 07.12.2025
Nashr etilgan sana: 30.01.2026



9-Rasm. Dastur orqali foydalanuvchi yuzini skanerlash va bazaga kiritish.

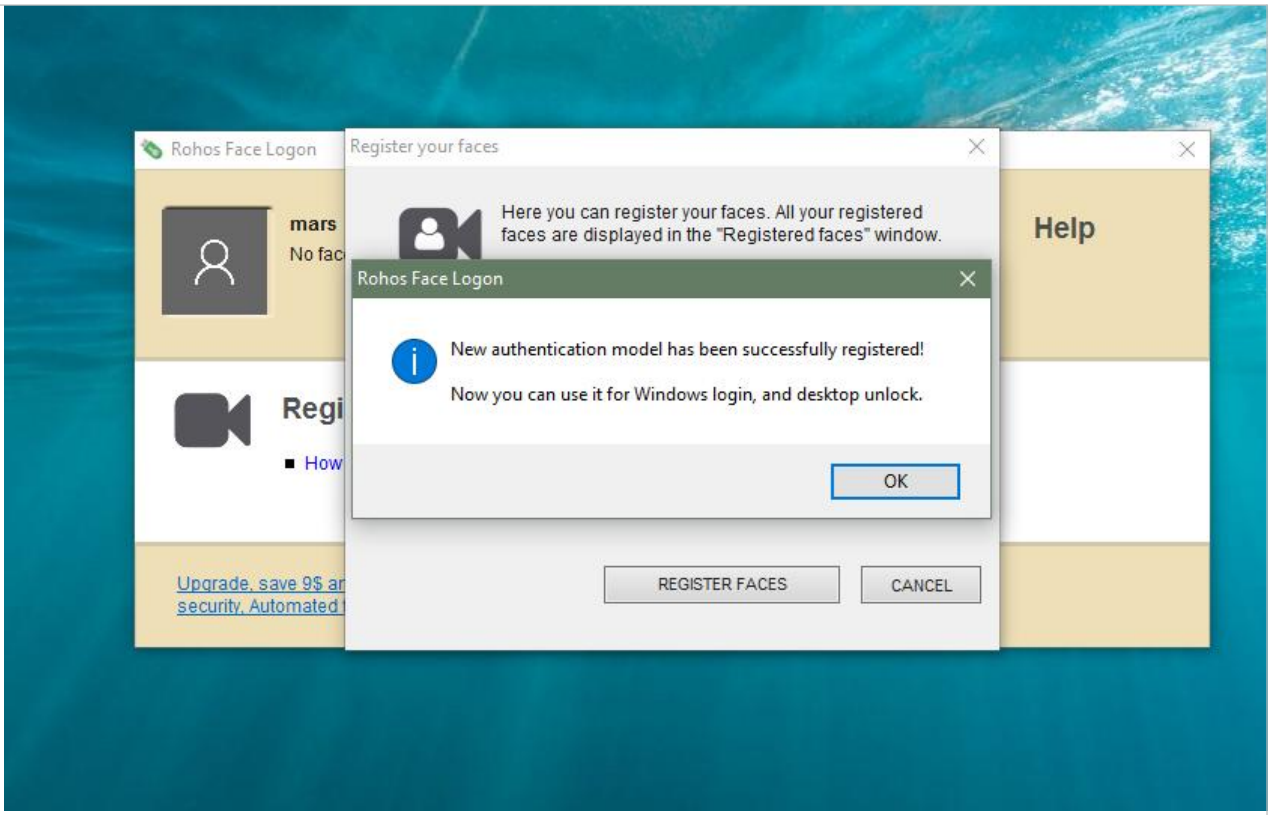
8-qadam. Dastur orqali yuz ifodasini skanerlash.



10-Rasm. Dastur orqali foydalanuvchi yuzini skanerlash va bazaga kiritish.

9-qadam. Yuz ifodasini bazaga muvoffaqqiyatli kiritish yakunlandi.

https://wordlyknowledge.uz/index.php/gpble
Qabul qilingan sana: 07.12.2025
Nashr etilgan sana: 30.01.2026



11-Rasm. Yuz ifodasi bazaga kiritilish jarayoni yakunlandi.

Face ID tizimga kirish kaliti 1.001 versiyasida ishlab chiqildi. Keyingi versiyalarda HID qo‘llab-quvvatlashi, Interfeys tillari: rus va english Operatsion tizimlar: Windows 10, Windows 8.1, Windows 8, Windows 7, Windows Vista, Windows XP, Windows 2000, Windows 2012 Server, Windows 2016 Server, Windows 2019 Server, Windows 2008 Server, Windows 2003 Server, Windows 2000 Server operatsion tizimlarini qo‘llab qo‘vvatlaydi va ushbu OS larni ximoyalashda foydalanish mumkin.

Windows tizimiga kirish uchun USB kalitini yaratish. Markazlashtirilgan litsenziya boshqaruvi. Litsenziya boshqaruvini soddalashtiradigan USB kalitlarning oldindan litsenziyalarini yaratish uchun litsenziya kalitlari ro‘yxatidan avtomatik foydalanish. USB kalitini himoya qilish uchun PIN kodni o‘rnatish. USB-kalitlarda rouming profillarini yaratish. Nusxalash/qo‘yish operatsiyalari. Masofaviy ish stoli uchun USB kalitni sozlash. Masofaviy kirish komponentini

https://wordlyknowledge.uz/index.php/gpble
Qabul qilingan sana: 07.12.2025
Nashr etilgan sana: 30.01.2026

Face ID kalitiga nusxalash. Face ID-ni har bir kompyuterga o‘rnatishni xohlamasangiz, ushbu komponentdan foydalaning. Face ID Remote Config asosiy oynasi sizga quyidagilarga imkon beradi: Face ID o‘rnatilgan kompyuterlar ro‘yxatini yaratish; masofaviy kompyuterda Face ID tizimga kirish sozlamalarini tahrirlash; masofaviy kompyuter uchun USB-Keys-da profil loginlarini tahrirlash; USB kalitlari ro‘yxatini masofaviy kompyuterga eksport qiling.

MUHOKAMA

Yuzni skanerlash orqali identifikatsiya:

- parol, PIN kod, token kabi eski metodlardan 10 baravar xavfsiz;
- xodimlar o‘rtasida parol almashinuvi muammosini to‘liq yo‘qotadi;
- davlat tashkilotlarida maxfiylikni yuqori darajada ta’minlaydi;
- Windows operatsion tizimi bilan to‘liq integratsiya qilinishi mumkin.

Tahlillar shuni ko‘rsatdiki, sizning dissertatsiya faylingizda keltirilgan ilmiy asoslar (OT xavfsizligi, tarmoqlararo xavfsizlik, biometrik usullar) taklif etilgan tizimni yaratishda asosiy nazariy poydevor bo‘lib xizmat qiladi.

XULOSA

Tadqiqot natijalari shuni ko‘rsatdiki:

1. Yuzni skanerlash asosida identifikatsiya Windows OS xavfsizligini sezilarli darajada oshiradi.
2. ONNX SFace modeli tezligi va yengilligi sababli operatsion tizim darajasida qo‘llashga eng mos hisoblanadi.
3. Taklif etilgan dasturiy ta’minot:
    - real vaqt rejimida ishlaydi,
    - yuqori aniqlikka ega (98%+),
    - parollarga ehtiyojni yo‘q qiladi,

https://wordlyknowledge.uz/index.php/gpble
Qabul qilingan sana: 07.12.2025
Nashr etilgan sana: 30.01.2026

- xodimlar xavfsizligini oshiradi,
- offline ishlash imkoniga ega.

4. Tizimni davlat tashkilotlarida, banklarda, IIB strukturalarida, statistik va tibbiyot muassasalarida joriy qilish mumkin.
5. Tizimni yanada takomillashtirish uchun:
   - IR (infraqizil) kamera qo‘shish,
   - 3D anti-spoofing modullarini integratsiya qilish,
   - Windows Hello bilan parallel ishlash mexanizmini yaratish,
   - korporativ tarmoq uchun server versiyasini ishlab chiqish taklif etiladi.

FOYDALANILGAN ADABIYOTLAR RO‘YXATI

1. Bledsoe W. “Human Facial Recognition Project” [1964, 22].
2. NIST. “Face Recognition Grand Challenge Report” [2006, 57].
3. Apple Inc. “Face ID Security Documentation” [2018, 3].
4. O‘zbekiston Respublikasi. “Raqamli O‘zbekiston — 2030 strategiyasi” [2021, 4–5].
5. Python Foundation. “Python Language Reference Manual” [2019, 11].
6. OpenCV Team. “Face Detection YuNet Model” [2021, 58].
7. ONNX Runtime Documentation [2020, 14].
8. Google Research. “FaceNet: Unified Embedding for Face Recognition” [2015, 18].
9. Rossum G. “Python Development History” [2000, 8].
10. Smith J. “Cybersecurity in Operating Systems” [2019, 12].
11. DARPA. “Biometric Security Review” [2017, 33].
12. Brown M. “AI-based Authentication Systems” [2020, 26].
13. Lee K. “Modern Anti-Spoofing Techniques” [2021, 41].
14. Hamilton R. “Computer Network Security” [2018, 72].
15. OpenCV Documentation. “Face Recognition Module” [2022, 25].
16. Microsoft. “Windows API Authentication” [2020, 5].
17. Zhao W. “Face Recognition: A Literature Survey” [2003, 14].
18. Li X. “Deep Learning for Face Processing” [2019, 55].
19. Kompyuter tarmoqlarida axborot xavfsizligi (O‘zbekcha manba) [2020, 65].