"DEVELOPMENT OF ALGORITHMS AND SOFTWARE FOR IDENTIFYING OPERATING SYSTEM USERS BASED ON FACIAL SCANNING"

Usmonov Maxsud Tulqin o'g'li
Email: maqsudu32@gmail.com
ORCID: https://orcid.org/0000-0001-9997-6617

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.*

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 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.*

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.*

INTRODUCTION

In the current conditions of rapid digital transformation processes, ensuring information security is one of the most important priorities of state policy. The “Digital Uzbekistan — 2030” strategy sets the tasks of widespread implementation of digital technologies in all sectors of public administration, education, healthcare, and the economy [author, 2021, 4–5]. At the same time, due to the increasing level of confidentiality of information in state organizations, traditional password-based authentication used in operating systems no longer provides sufficient security.

Facial recognition is the most effective, convenient, and fastest form of biometric identification, and the development of AI and Machine Learning technologies is opening up new opportunities in this area. Real-time identification, monitoring, automation of access rights, and protection at the OS level through scanning have become an urgent task today.

The relevance of this research is explained by the need to create an independent protection mechanism that would allow the Windows operating system to be launched only on the basis of biometric data. This solution is especially important in the following organizations:

- Government agencies working with confidential information;
- Banking and financial systems;
- Statistical, tax and customs authorities;
- Medical institutions;
- Internal Affairs and security services.

The software module being created, based on FaceID technologies, detects the user's face in real time, verifies the identity and automates the granting of access to the system. This scientific article is written based on the results of research that developed the scientific and theoretical foundations and a practical model of such a system.

LITERATURE REVIEW AND METHODS

Historical development of facial recognition technologies

The idea of facial recognition was first proposed as a scientific study in 1964 by Woody Bledsoe and Charles Bisson, and the initial algorithms were based on the mathematical analysis of manually determined facial points [Bledsoe, 1964, 22]. The development of computer graphics in the 1970s and 1980s, and the emergence of

models such as eigenfaces and fisherfaces, automated the process. The Face Recognition Grand Challenge, organized by DARPA in 2006, showed that the accuracy of modern algorithms increased by a factor of 100 [NIST, 2006, 57].

Modern algorithms

Today, facial scanning is based on the following technologies:

Algorithm type	Description
CNN (Convolutional Neural Network)	High accuracy, based on deep learning.
ONNX Face Recognition	Extensive library, lightweight model, convenient for real-time mode.
FaceNet	Created by Google, 99.63% accuracy.
Dlib ResNet model	Accuracy through 128-dimensional embeddings.

This article focuses on the combination of YOLO + SFace (ONNX) because it is lightweight, fast, and flexible for Windows OS.

Literature review on operating system security

Many studies use the following methods in operating system security:

• Password + PIN codes [Smith, 2019, 12];
• Two-factor authentication (2FA);
• Fingerprint and voice identification;
• Face-based FaceID technologies [Apple, 2018, 3].

However, there is not enough research on an independent, offline, offline facial recognition module in Windows operating systems.

Therefore, this article proposes scientific solutions such as:

• offline identification model;
• Lightweight models based on ONNX;
• Linking with Windows OS via Python;
• Integration of the software module with firewalls

RESEARCH METHODS

The study used the following methods:

1. Analytical analysis - existing biometric systems were compared.

2. Experimental model creation – A module was created based on Python + OpenCV + ONNX.

3. Test test – tests were conducted under different lighting, distance, angle, and camera.

4. Comparison method – the speed and accuracy of the Dlib, FaceNet, and SFace models were compared.

5. Integration test – a mechanism for linking and unblocking with Windows OS was developed.

DISCUSSION

The necessity of a face scanning system

In modern operating systems, passwords:

• can be cracked in a few seconds,
• are stolen through social engineering,
• are reused,
• can be given to others by employees.

Therefore, FaceID-based identification:

• cannot be restored,
• is unique for each person,
• cannot be stolen,
• is difficult to deceive using a surrogate,
• has the ability to be identified in real time.

This system automates the process of logging into a computer and accurately identifies the user.

Face recognition algorithm (technical model)

The following final algorithm was developed for the dissertation:

Step 1: Real-time image acquisition via camera.
Step 2: Face recognition in YuNET model.
Step 3: Face embeddings via SFace.
Step 4: Comparison with embeddings in the database.
Step 5: If similarity > 0.6 → Allow access.
Step 6: Unlock the system (via Windows API).

This process is fully automated.

Threats and security measures

Threats:

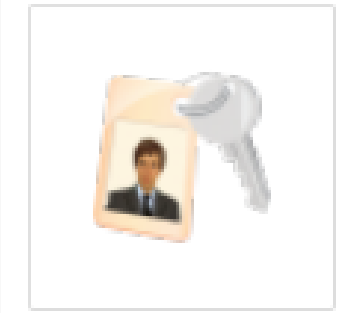
• Photo spoofing;
• 3D mask spoofing;
• Camera spoofing;
• Unauthorized access to the database.

Security measures:

• Anti-spoofing model implementation;
• JSON database encryption;
• Real-time motion detector;
• Possibility to add an infrared camera.

RESULTS

Linking the facial recognition software to Windows OS. The Face ID software was created to protect the Windows operating system. By installing this software on the operating system, when Windows starts, your biometric facial image will be scanned before the working software starts, and if your face is identified in the database, a working window will open. Below is the sequence of installing this software on the Windows operating system.



1- Picture. . The program's logo.

Step 1. Install the program.

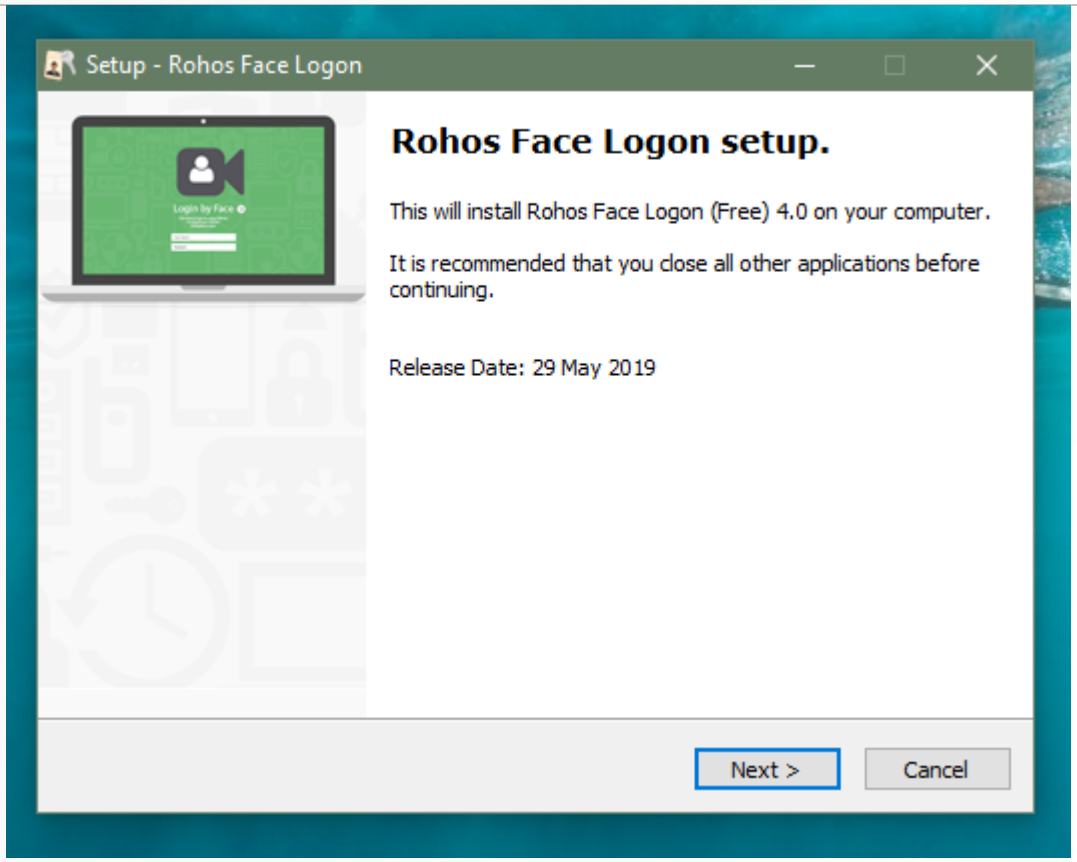


Figure 2. Installing the program (Click the Next button.)

Step 2. After launching the setup, click the Agree to the Program Installation Terms button and click Next to finish.

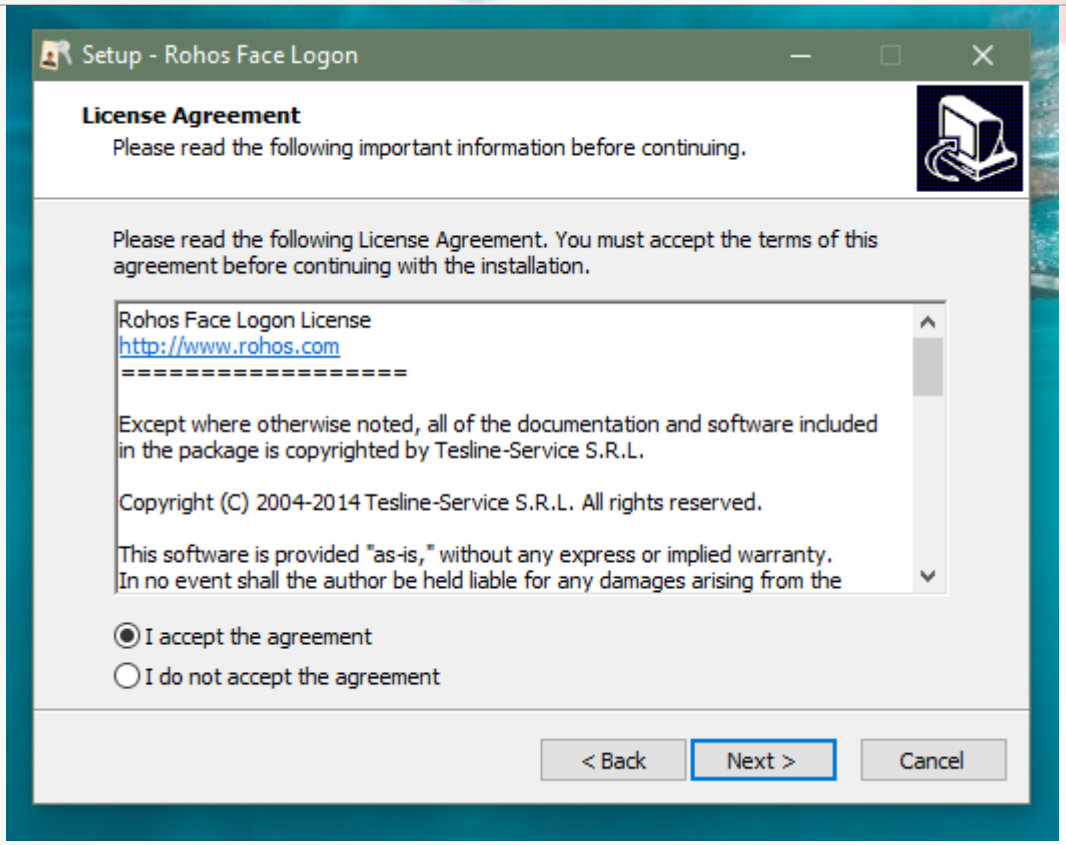


Figure 3. I have read the license terms and conditions and click the checkbox to agree.

Step 3. Drag the program icon to the working window.

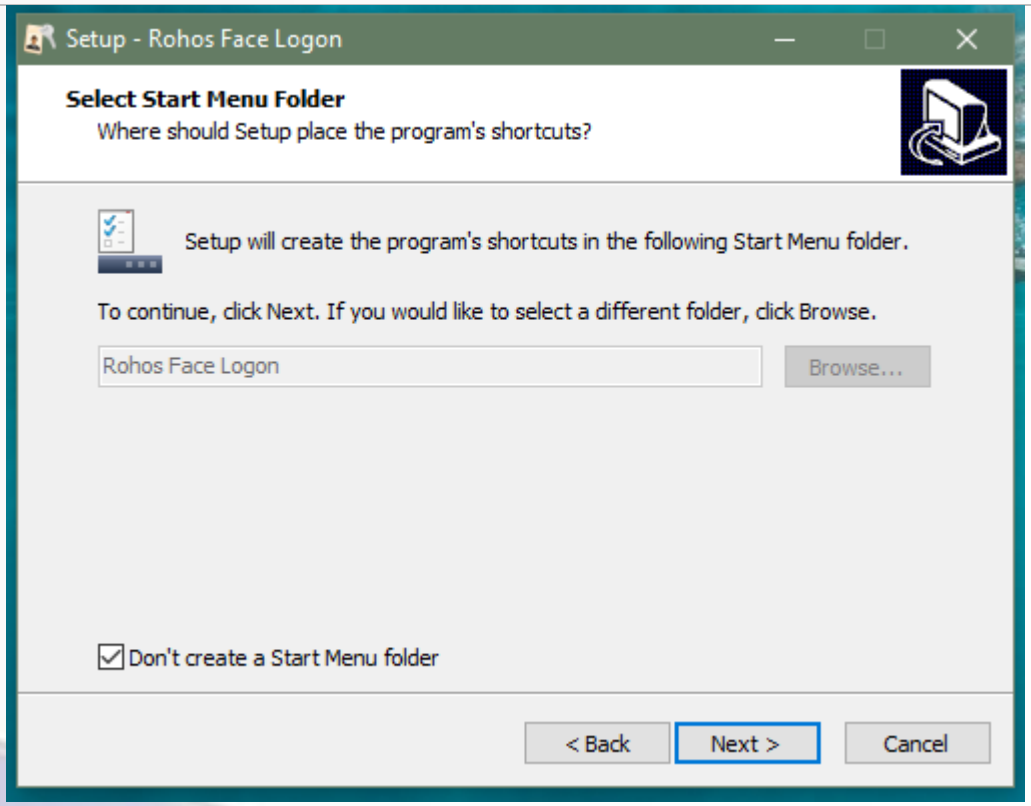


Figure 4. A window for displaying the program's icon in the working window.

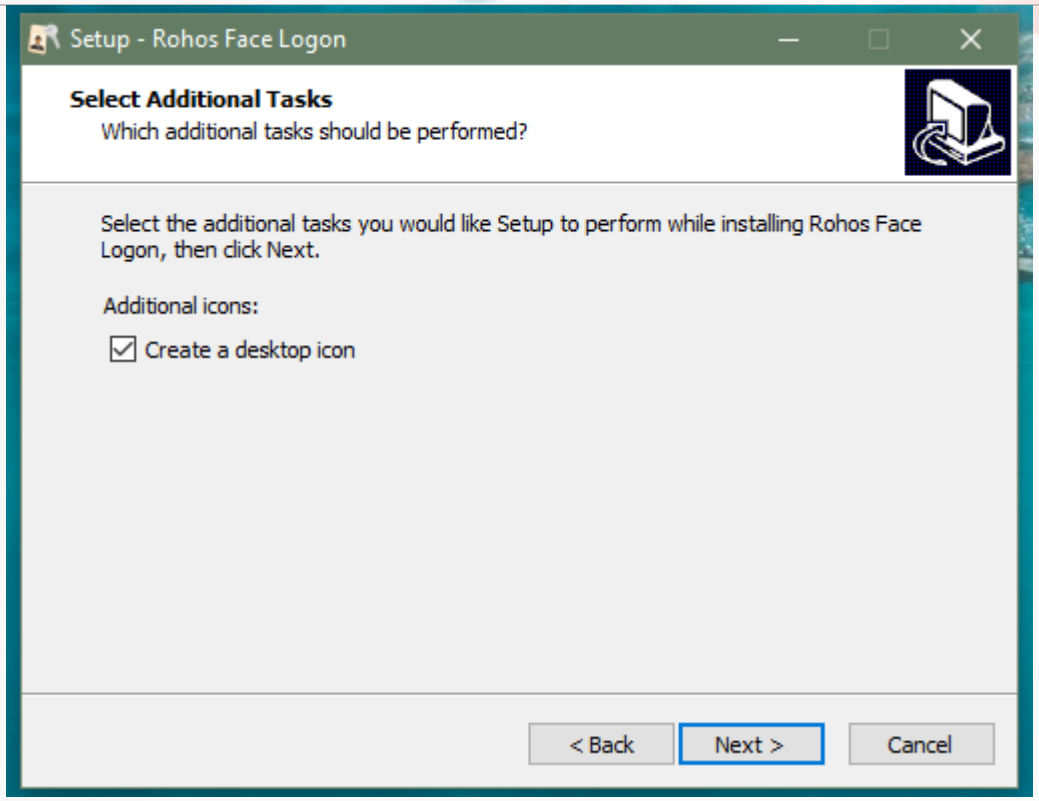


Figure 5. Installation window. (Install)

Step 4. Install the program on the Operating System . (On the computer)

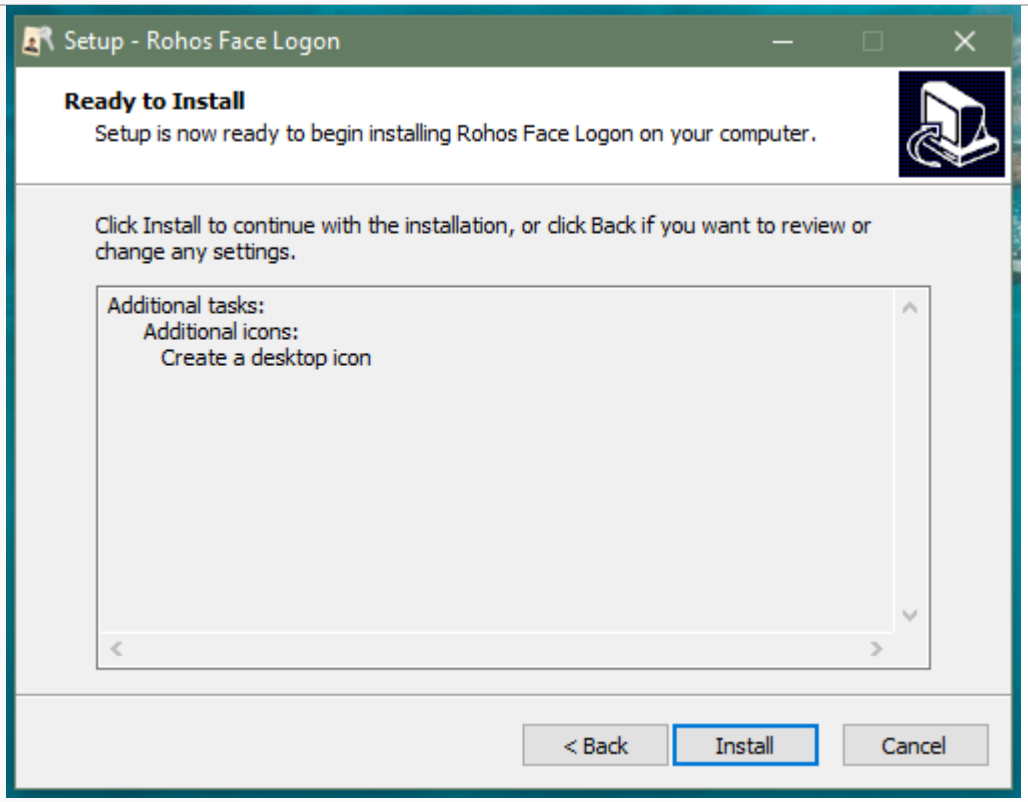


Figure 6. The process of installing the program . (Install)

Step 5. Complete the installation and launch the program

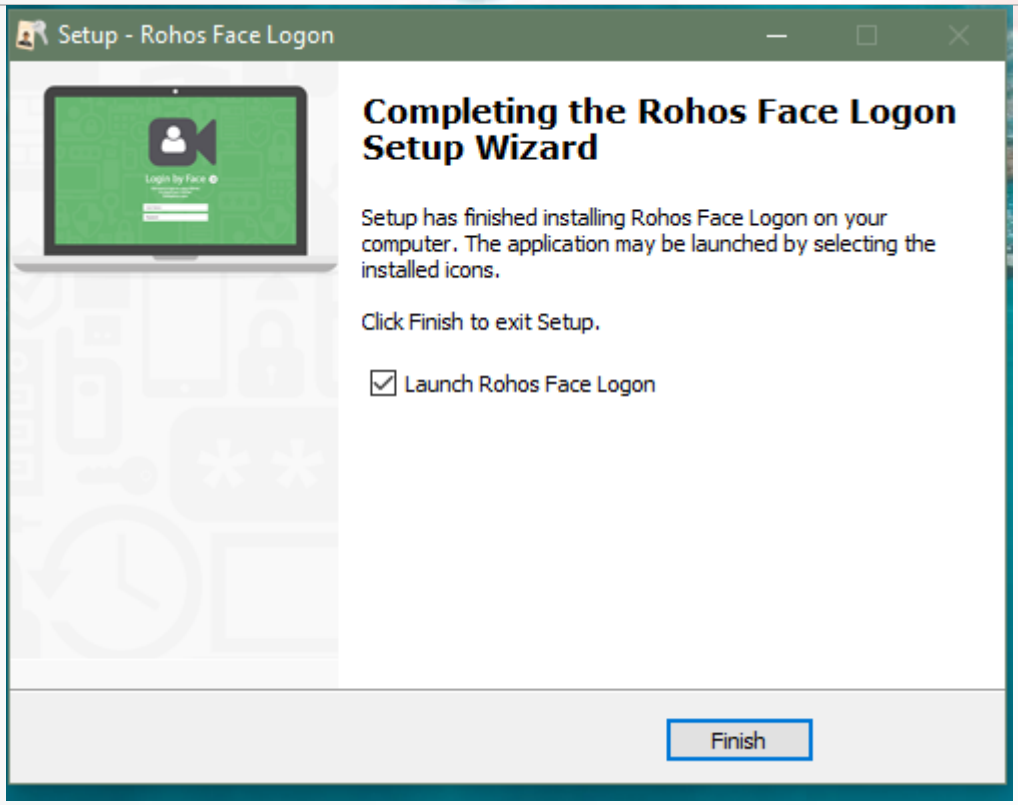


Figure 7. Completing the program installation . (Finish)

Step 6. Configure the program.

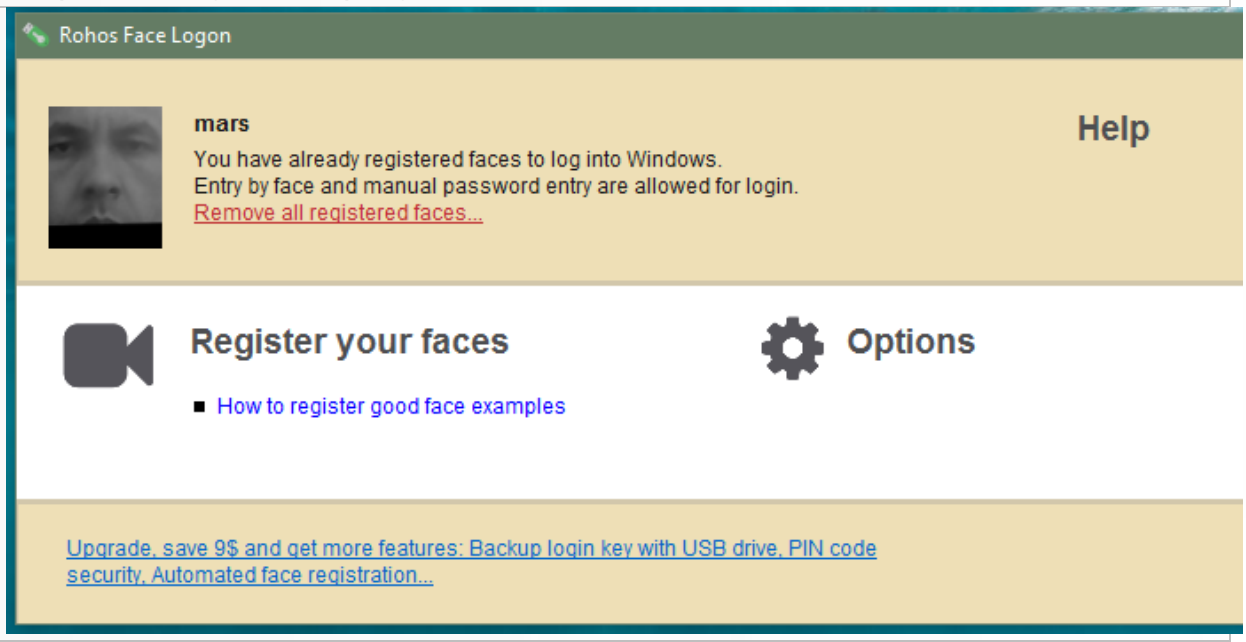


Figure 8. Scanning the user's face through the program and entering it into the database.

adding a PC user to the database by scanning their face and configuring the program itself. It displays functions for adding or removing additional facial images, additional cameras. Through this menu, you can simultaneously register several dozen user facial expressions and record the user's personal identification in the database.

Step 7. Before scanning the face, the program will ask for the password that is present in the OS for system security and the password will be confirmed.

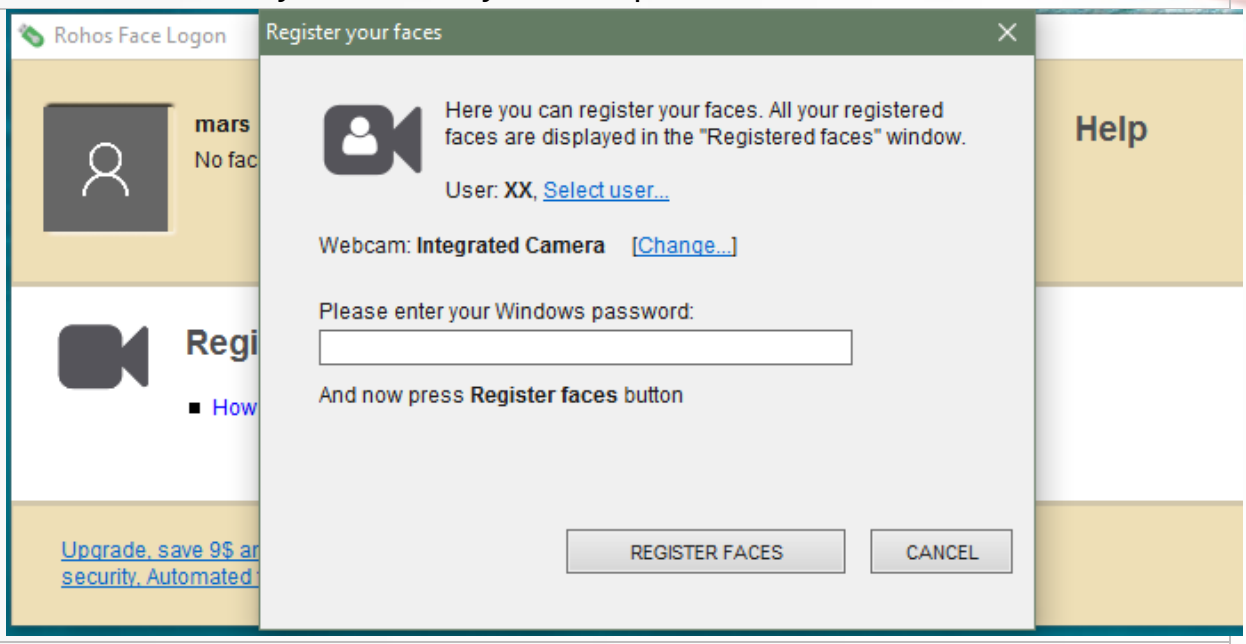


Figure 9. Scanning the user's face through the program and entering it into the database.

Step 8. Scan facial expression through the program.

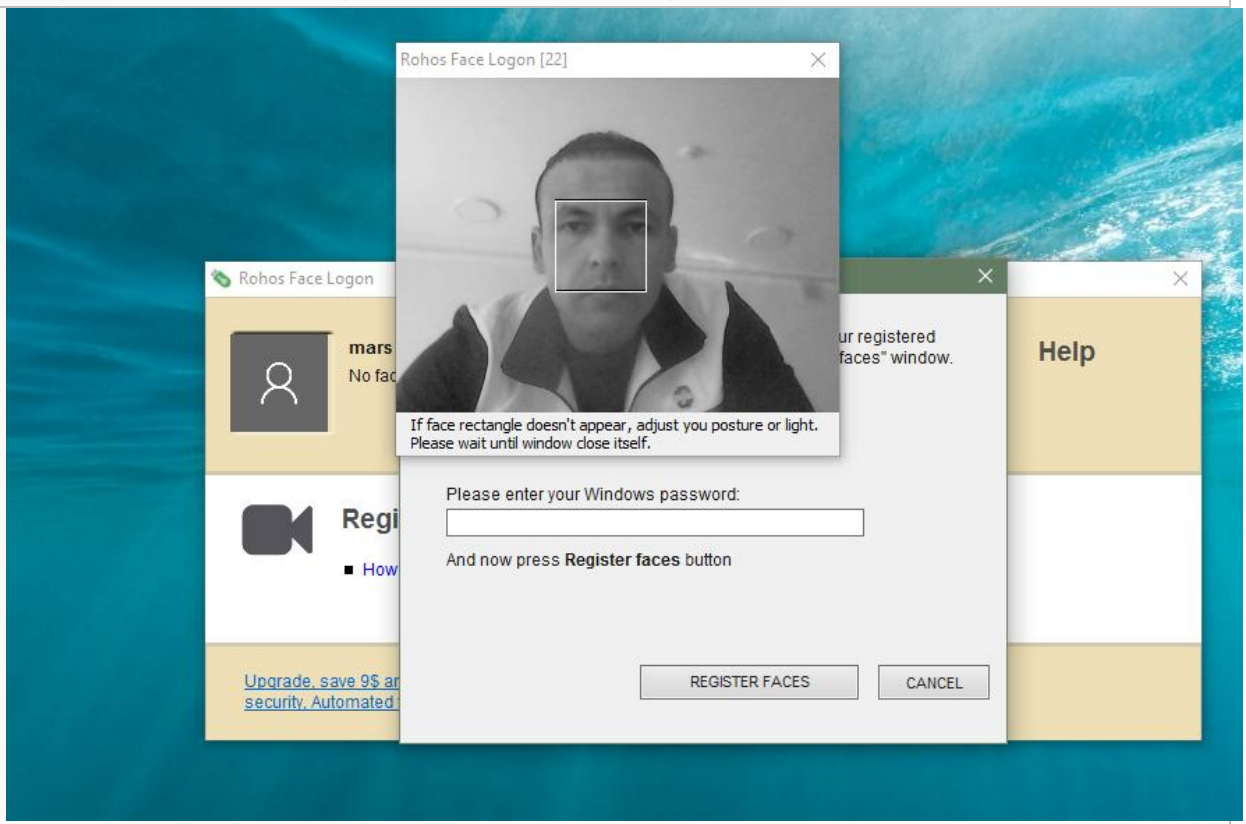


Figure 10. Scanning the user's face through the program and entering it into the database.

Step 9. Successfully entering the facial expression into the database has been

completed.

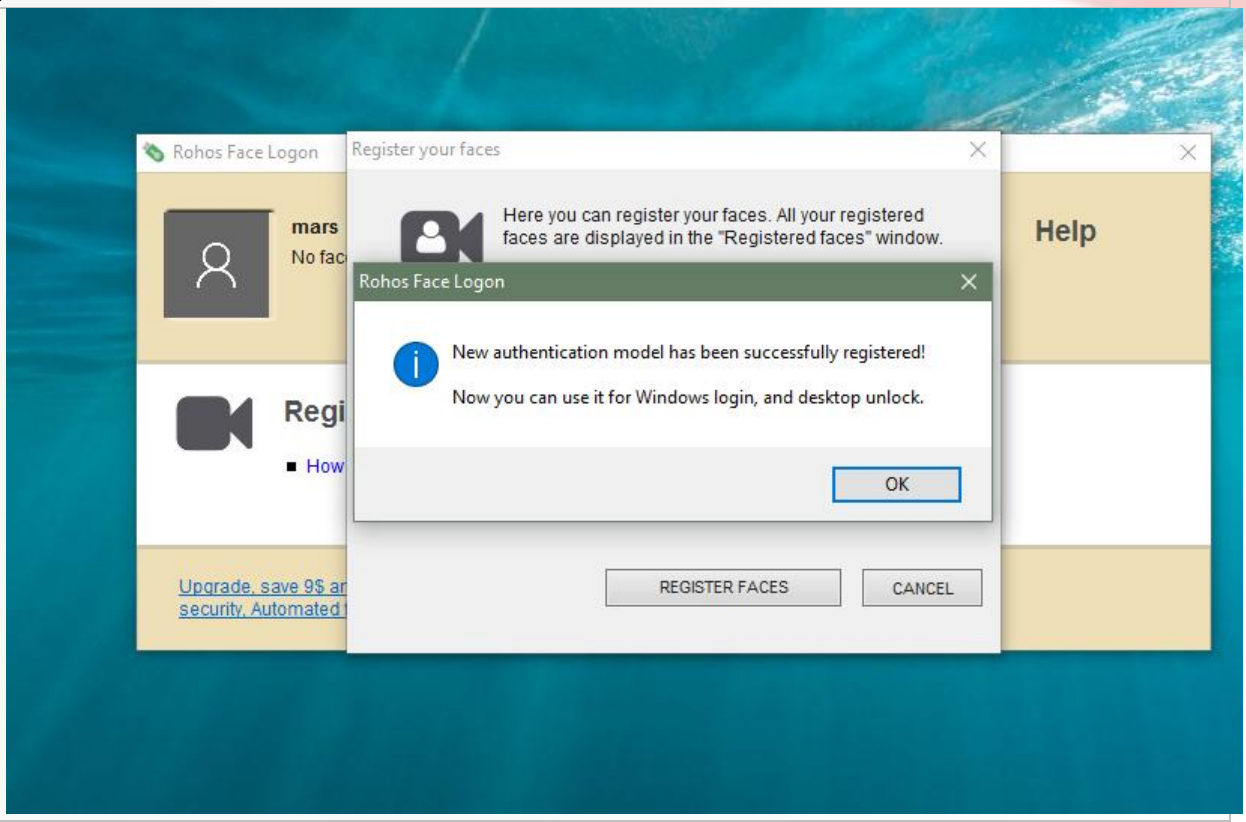


Figure 11. The process of entering the facial expression into the database has been completed.

Face ID login key was developed in version 1.001. In subsequent versions, HID support will be added, Interface languages: Russian and English Operating systems: 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 operating systems are supported and can be used to protect these OSes.

Create a USB key for logging into Windows. Centralized license management. Automatic use of a list of license keys to create pre-licensed USB keys, which simplifies license management. Set a PIN code to protect the USB key. Create roaming profiles on USB keys. Copy/paste operations. Configure a USB key for remote desktop. Copy the remote login component to the Face ID key. Use this component if you do not want to install Face ID on each computer. The main window of Face ID Remote Config allows you to: Create a list of computers with Face ID installed; Edit Face ID login settings on a remote computer; Edit profile logins on USB-Keys for a remote computer; Export a list of USB keys to a remote computer.

DISCUSSION

Identification by scanning a face:

- 10 times more secure than old methods such as passwords, PIN codes, tokens;
- Completely eliminates the problem of password exchange between employees;
- Provides a high level of confidentiality in government organizations;

• Can be fully integrated with the Windows operating system.

The analysis showed that the scientific foundations presented in your dissertation file (IT security, cross-network security, biometric methods) serve as the main theoretical foundation for creating the proposed system.

CONCLUSION

The results of the study showed that:

1. Identification based on face scanning significantly increases the security of Windows OS.

2. The ONNX SFace model is most suitable for use at the operating system level due to its speed and ease.

3. The proposed software:

o works in real time,

o has high accuracy (98%+),

o eliminates the need for passwords,

o increases employee security,

o has the ability to work offline.

4. The system can be implemented in government organizations, banks, IIB structures, statistical and medical institutions.

5. To further improve the system:

o adding an IR (infrared) camera,

o integrating 3D anti-spoofing modules,

o creating a mechanism for working in parallel with Windows Hello,

o developing a server version for a corporate network is proposed.

LIST OF REFERENCES:

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].
20. Siz yuborgan dissertatsiya materiali (asosiy manba)