

СИСТЕМА БИОМЕТРИЧЕСКОЙ АУТЕНТИФИКАЦИИ KIRTap

Д.А. Романов, Г.П. Колбанов, Е.С. Белоусова

Учреждение образования «Национальный детский технопарк», Минск, Беларусь

Аннотация. В работе представлена биометрическая система аутентификации (KIRTap), интегрированной в операционную систему Secux. Система поддерживает два режима регистрации: локальный и корпоративный. В локальном режиме администратор регистрирует пользователя через графический интерфейс, после чего проводится сканирование лица с использованием библиотек алгоритмов компьютерного зрения OpenCV и face_recognition. В корпоративном режиме реализована автоматизированная настройка базы данных PostgreSQL с использованием Docker. Биометрическая аутентификация основана на сравнении эмбедингов лиц, полученных при регистрации, с текущими изображениями, используя встроенные функции face_recognition и евклидову метрику. Система также включает механизм фоновой проверки, анализируя соответствие пользователя сохраненным биометрическим данным. В перспективе планируется внедрение нейросетевых методов для повышения точности распознавания, а также разработка анти-спуфинг модели для защиты от кибератак с поддельными изображениями.

Ключевые слова: face_recognition; OpenCV; PostgreSQL; биометрическая аутентификация; нейронные сети; распознавание лиц.

KIRTap BIOMETRIC AUTHENTICATION SYSTEM

D.A. Romanov, Kolbanov G.P., E.S. Belousova

Educational Institution "National Children's Technopark", Minsk, Belarus

Abstract. The paper presents a biometric authentication system (KIRTap) integrated into the Secux operating system. The system supports two registration modes: local and corporate. In local mode, the administrator registers the user through the graphical interface, after which a face scan is performed using the libraries of OpenCV and face_recognition computer vision algorithms. In the corporate mode, automated configuration of the PostgreSQL database using Docker is implemented. Biometric authentication is based on comparing the embeddings of the faces obtained during registration with the current images using the built-in face_recognition functions and the Euclidean metric. The system also includes a background monitoring mechanism, analyzing the user's compliance with the stored biometric data. In the future, it is planned to introduce neural network methods to improve recognition accuracy, as well as develop an anti-spoofing model to protect against cyber attacks with fake images.

Keywords: face_recognition; OpenCV; PostgreSQL; biometric authentication; neural networks; face recognition.

Введение

Современные информационные системы требуют от разработчиков постоянного повышения уровня безопасности доступа. В условиях растущих угроз несанкционированного доступа традиционные методы аутентификации все чаще дополняются биометрическими решениями. Биометрическая аутентификация с использованием распознавания лиц демонстрирует высокую точность и удобство для конечных пользователей. В данной работе представлена разработка системы регистрации и контроля доступа KIRTapр, основанной на анализе изображений с веб-камеры для защищенной операционной системы Secux.

Целью данной работы была разработка системы регистрации и контроля доступа KIRTapр с биометрической аутентификацией.

Дополнительно, в работе представлено обоснование выбора гиперпараметров, активационных функций и описан процесс обучения модели, лежащей в основе алгоритмов распознавания лиц. Несмотря на то, что в работе демонстрируется готовое решение, детальный анализ этих аспектов позволяет обосновать отказ от самостоятельного обучения нейросети с точки зрения вычислительных ресурсов и надежности проверенных моделей.

Основная часть

В системе регистрации и контроля доступа KIRTapр используются два режима работы: локальный и корпоративный.

В локальном режиме администратор с помощью графического интерфейса (на основе библиотеки customtkinter) регистрирует пользователя (рис. 1, *a*), после чего выполняется сканирование лица с использованием OpenCV и библиотеки face_recognition (рис. 1, *b*). В основе работы системы лежит алгоритм распознавания лиц, использующий эмбединги – 128-мерные векторы, описывающие ключевые характеристики лица. Для сравнения эмбедингов применяются два метода: встроенные функции библиотеки face_recognition и прямой расчет евклидовой дистанции между векторами.

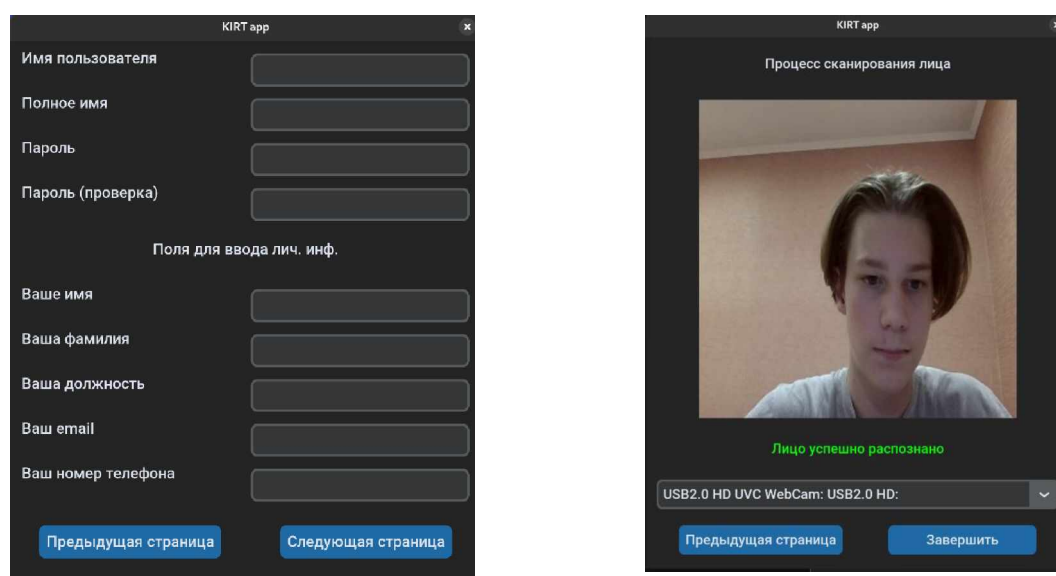


Рис. 1. Локальный режим KIRTapр: *a* – регистрация пользователя; *b* – процесс сканирования лица
Fig. 1. KIRTapр Local Mode: *a* – user registration; *b* – the face scanning process

Для работы KIRTApp в корпоративном режиме реализована автоматизированная развертка базы данных PostgreSQL в Docker-контейнере (рис. 2), что упрощает процесс подключения и обеспечивает высокий уровень безопасности данных. С помощью консольного приложения администратор вводит необходимые параметры (db_name, user_name, user_password, port), после чего посредством Docker автоматически разворачивается контейнер с PostgreSQL. Настройки подключения формируются с использованием SQLAlchemy, а тест доступности базы данных производится через вызов функции socket.create_connection с заданным IP-адресом и портом.

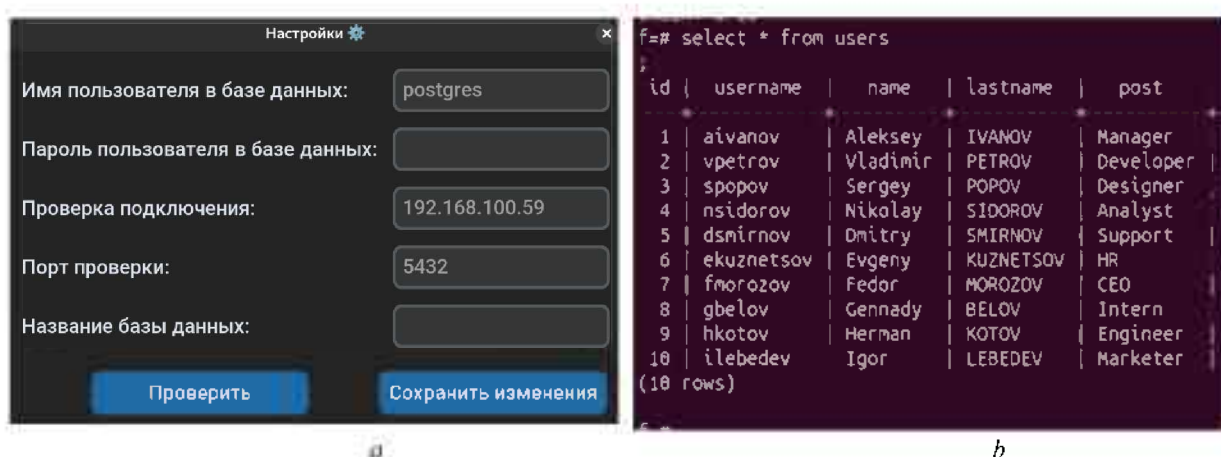


Рис. 2. Пример работы корпоративного режима KIRTApp: а – проверка подключения к базе данных; б – примерное содержание базы данных

Fig. 2. An example of the KIRTApp corporate mode: a – checking the connection to the database; b – approximate database contents

Системы регистрации и контроля доступа KIRTApp с биометрической аутентификацией внедрена в операционную система Secux, в которой выполняет следующие задачи:

1 Регистрация пользователя, для которой разработан графический интерфейс с использованием customtkinter, предназначенный для ввода данных пользователя (фамилия, имя, username, password) администратором. После ввода регистрационных данных пользователь проходит процедуру сканирования лица, осуществляемую посредством веб-камеры и обработку изображения с помощью OpenCV и face_recognition.

2 Контроль пользователя в фоновом режиме. После перезагрузки операционной системы и аутентификации пользователя автоматически запускается фоновый процесс, который каждые 2 с делает снимок с веб-камеры, и анализирует соответствие текущего лица сохраненному образцу. Для принятия решения анализируется серия из пяти изображений. Если количество совпадений превышает число ошибок распознавания, система регистрирует событие и откладывает повторный запуск фонового приложения на заданное время (по умолчанию 5 минут). При несоответствии система блокирует доступ пользователя, требует повторного ввода пароля и регистрирует событие в системе. В корпоративном режиме время последнего входа пользователя заносится в базу данных.

Для обеспечения безопасности доступа ключевую роль играет алгоритм распознавания лиц. В основе метода лежит получение эмбеддингов – это процесс преобразования каких-либо данных в набор чисел, векторы, которые машина может не только хранить, но и с которыми она может работать, и последующее сравнение этих векторов с сохраненными шаблонами.

Чаще всего сравнение фотографий лиц, преобразованных в эмбединги происходит с помощью одного из двух алгоритмов: алгоритма расчета евклидова расстояния, алгоритма расчета манхэттенского расстояния. В системе регистрации и контроля доступа KIRТарр был реализован алгоритм расчета евклидова расстояния, в соответствии с которым геометрическое расстояние в многомерном пространстве рассчитывается по формуле:

$$d(a, b) = \sqrt{\sum_{i=1}^n (a_i - b_i)^2}, \quad (1)$$

где a, b – две точки в n -мерном евклидовом пространстве; a_i, b_i – векторы, ведущие из начала координат евклидова пространства.

В соответствии с алгоритмом расчета манхэттенского расстояния используется формула:

$$d(a, b) = |a_i - b_i|, \quad (2)$$

В результате сравнения двух алгоритмов был выбран алгоритм расчета евклидова расстояния для реализации в системе регистрации и контроля доступа KIRТарр, так как он больше подходит для измерения абсолютных различий.

Сходство между векторами измеряет $S(a, b)$ (степень «похожести»). В эмбедингах это используется для определения степени семантической или контекстной близости между элементами. Один из наиболее популярных способов – это косинусное сходство. Косинусное сходство измеряет косинус угла между двумя векторами. Если угол между векторами мал, косинус приближается к 1, что указывает на высокое сходство. Математически оно выражается как:

$$S(a, b) = \frac{a \cdot b}{|a||b|}, \quad (3)$$

где a $|a|$ и b $|b|$ – их нормы скалярного произведения векторов.

Заключение

Разработка системы регистрации и контроля доступа KIRТарр представляет собой актуальное и востребованное решение для повышения контроля работы сотрудников и доступа к устройствам области информационной безопасности. В данной работе были рассмотрены основные компоненты системы, включая графическое приложение регистрации, фоновый процесс контроля доступа и корпоративный режим автоматизированного развертывания базы данных.

Система обеспечивает непрерывный мониторинг пользователя с помощью периодических проверок и автоматического реагирования на изменения в состоянии аутентификации, что минимизирует риск несанкционированного доступа. Корпоративный режим позволяет быстро и надежно развернуть базу данных, обеспечивая гибкость и масштабируемость решения.

В перспективе возможно внедрение обучения собственных нейросетей для распознавания лиц, что позволит более гибко адаптировать систему к различным условиям эксплуатации. Дополнительно планируется интеграция анти-спуфинг модели, способной определять попытки обмана системы с использованием фотографий, видео или масок. Это повысит уровень безопасности и сделает систему более устойчивой к потенциальным кибератакам.

Список использованных источников

1. Вержбицкий, С. В. Биометрические системы и технологии: основы, методы, средства. – М.: Горячая линия – Телеком, 2019 г. – 304 с.
2. Журавлев, Ю. И., Панкратова, Н. Д., Петров, В. С. Идентификация личности по биометрическим признакам. – М.: Физматлит, 2021. – 248 с.

References

1. Verzhbitsky, S. V. Biometric systems and technologies: fundamentals, methods, tools. – Moscow: Hotline – Telecom, 2019. 304 p.
2. Zhuravlev, Yu. I., Pankratova, N. D., Petrov, V. S. Identification of personality by biometric signs. Moscow: Fizmatlit, 2021. 248 p.

Сведения об авторах

Романов Д.А., учащийся учреждение образования «Национальный детский технопарк». dinromgomell@gmail.com
Колбанов Г.П., учащийся, учреждение образования «Национальный детский технопарк». grigoriy.kolbanov@gmail.com
Белусова Е.С., канд. техн. наук, доц., доцент кафедры защиты информации, учреждение образования «Белорусский государственный университет информатики и радиоэлектроники». belousova@bsuir.by.

Information about the authors

Romanov D.A., Student. Educational Institution "National Children's Technopark". dinromgomell@gmail.com
Kolbanov G.P., Student. Educational Institution "National Children's Technopark". grigoriy.kolbanov@gmail.com
Belousova E.S., PhD. Associate Professor. Information Security Department, Educational Institution "Belarusian State University of Informatics and Radioelectronics". belousova@bsuir.by.