УДК 004.422.833

СИСТЕМА БИОМЕТРИЧЕСКОЙ АУТЕНТИФИКАЦИИ KIRTapp

Романов Д. А., Колбанов Г.П.,

Учащиеся УО «Национальный детский технопарк»
г. Минск, Республика Беларусь

Научный руководитель: Белоусова Е.С. – канд. техн. наук, доцент кафедры защиты информации

Аннотация. В данной работе рассматривается система биометрической аутентификации KIRTapp, предназначенная для регистрации и контроля доступа с использованием распознавания лиц. Проведён анализ различных алгоритмов, на основе которого был выбран оптимальный метод идентификации Face Recognition. Система KIRTapp обеспечивает постоянный мониторинг пользователя и автоматическое реагирование на изменения в процессе аутентификации, снижая риск несанкционированного доступа. В перспективе планируется интеграция нейросетей и анти-спуфинг технологий для повышения безопасности.

Ключевые слова. Face Recognition; OpenCV; биометрическая аутентификация; машинное обучение, нейронные сети; распознавание лиц.

В современном мире аутентификация играет ключевую роль в обеспечении безопасности данных и ограничении доступа к системам [1]. Традиционно для идентификации пользователей применялись пароли и PIN-коды, но эти методы имеют ряд недостатков: они могут быть забыты, украдены или скомпрометированы.

Биометрическая аутентификация предлагает более надёжную альтернативу, используя уникальные физиологические характеристики человека, такие как отпечатки пальцев, радужка глаза и лицо. Одним из наиболее популярных и удобных методов является распознавание лиц [2].

В статье проведен сравнительный анализ распространенных моделей распознавания лиц, на основе которого обоснован выбор, внедрение и тестирование модели Face Recognition в операционной системе Secux Linux для контроля пользователей корпоративных сетей.

Для выбора модели для системы биометрической аутентификации изучено исследование разных моделей распознавания лиц [3]:

1 RetinaFace – это высокоточный детектор лиц, представленный в 2019 году. Он использует одностадийный метод обнаружения лиц с дополнительными возможностями предсказания ключевых точек (глаз, носа, рта).

2 DBFace – это компактная, одностадийная нейросеть для детекции лиц, разработанная для высокой скорости работы.

3 Facenet-pytorch – это высокоуровневый интерфейс для FaceNet, модели, представленной Google в 2015 году.
4 Face Recognition – это популярная библиотека для Python, основанная на dlib. Она предоставляет удобный API для детекции, кодирования и сравнения лиц.
5 Ultra-Light-Fast-Generic-Face-Detector-1MB – это ультралегковесная модель для детекции лиц, предназначенная для мобильных устройств и встроенных систем.
Автором исследования [3] был создан собственный датасет, проведен процесс его разметки и осуществлено тестирование ранее перечисленных моделей.
Для проведения анализа результатов тестирования и определения наиболее подходящей модели использовались следующие метрики: Precision, Recall и Intersection over Union (IoU). Эти метрики позволят нам оценить производительность моделей в контексте точности распознавания лиц, полноты детекции и качества локализации объектов.
Precision (Точность) – метрика измеряет долю правильно предсказанных положительных примеров (истинных положительных) среди всех предсказанных положительных примеров и вычисляется по формуле:

$$Precision = \frac{TP}{TP + FP} \quad (1)$$

где TP – количество истинных положительных предсказаний (правильно распознанных лиц); FP –количество ложных положительных предсказаний (ошибочно распознанных лиц).
Precision важен, когда необходимо минимизировать количество ложных срабатываний (когда модель ошибочно распознает лицо, где его нет).
Recall (Полнота) – метрика для измерения способности модели обнаружить все реальные положительные примеры среди всех истинных положительных. Она отражает, сколько из всех объектов были корректно обнаружены моделью. Формула для расчета Recall:

$$Recall = \frac{TP}{TP + FN} \quad (2)$$

где TP – количество истинных положительных предсказаний; FN – количество ложных отрицательных предсказаний (когда модель не распознает лицо, которое есть на изображении).
Recall критичен в задачах, где важно н пропустить ни одного лица, даже если это приводит к большему числу ложных срабатываний.
Intersection over Union (IoU) – метрика IoU измеряет степень совпадения между предсказанной областью (например, bounding box) и реальной областью, охватывающей объект. Эта метрика особенно важна для задач детекции объектов, так как она позволяет оценить точность локализации. Формула для расчета IoU:

$$IoU = \frac{\text{Area of Intersection}}{\text{Area of Union}}$$

$$IoU = \frac{Area\ of\ Intersection}{Area\ of\ Union} \quad (3)$$

где Area of Intersection – площадь пересечения предсказанного прямоугольника и истинного прямоугольника, ограничивающего лицо; Area of Union – площадь объединения этих двух прямоугольников.

Таблица 1 – Сравнительный анализ моделей биометрической аутентификации

Метрика	RetinaFace	DBFace	Facenet-pytorch	Face Recognition	Ultra-Light-Fast-Generic-Face-Detector-1MB
Precision	0,99	1	0,95	1	0,74
Recall	0,8	0,8	0,71	0,38	0,75
IoU	0,75	0,74	0,72	0,67	0,59
Время обработки, с	91	13	14	11	3

Анализ результатов показал, что модель RetinaFace продемонстрировала наилучшие показатели точности, однако её время выполнения составило 91 секунду, что является неприемлемым для системы биометрической аутентификации. DBFace также показала хорошие результаты, но не предоставляет встроенного механизма сравнения лиц, что потребовало бы дополнительной реализации, например, с использованием евклидова расстояния. В связи с этим Face Recognition является наиболее подходящим выбором: несмотря на не самое высокое значение Recall, полное распознавание всех лиц не является приоритетом для разрабатываемой системы биометрической аутентификации, так как она анализирует только единственного пользователя, работающего за устройством.

Таким образом, для разработки системы биометрической аутентификации KIRTapp была выбрана модель Face Recognition. Принцип работы KIRTapp основан на регистрации пользователей администратором, и в последующем автоматическим сканированием пользователей каждые N минут, где N – число, настраиваемое администратором.

Алгоритм работы фоновой службы автоматического сканирования пользователей представлен на рисунке 1.

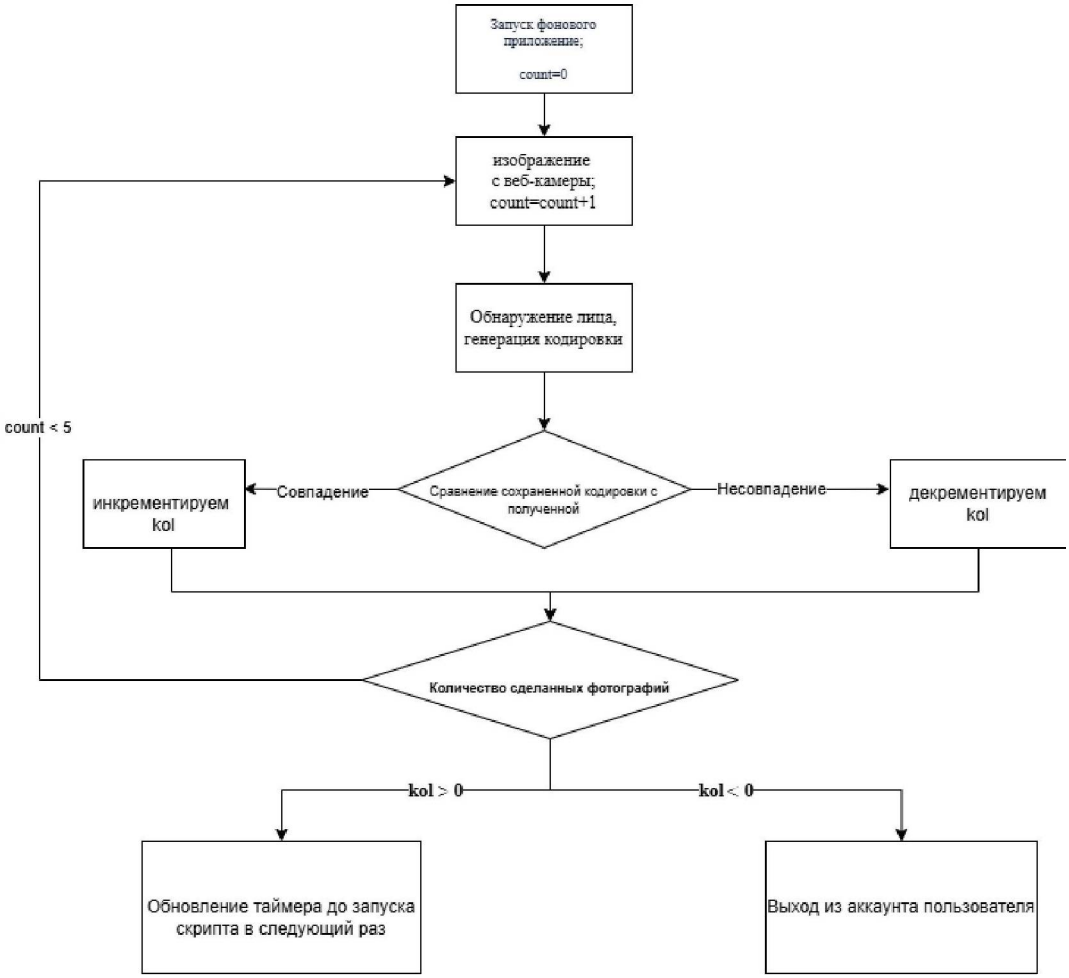

Рисунок 1. Алгоритм работы фоновой службы автоматического сканирования пользователей

На следующем этапе алгоритм, основанный на библиотеке face_recognition, выполняет детекцию лица на полученном изображении. Обнаруженное лицо преобразуется в вектор признаков, называемый кодировкой (face_encoding). Этот вектор представляет собой компактное числовое описание уникальных характеристик лица пользователя, вычисленное с помощью сверточной нейронной сети.

Процесс повторяется 5 раз с интервалом в 2 секунды между итерациями. На каждом этапе фиксируется результат: идентифицирован ли пользователь как владелец устройства или нет. Если по итогам пяти попыток количество положительных идентификаций превышает количество отрицательных, система подтверждает присутствие владельца и продолжает работу. В противном случае система выполняет блокировку: текущий сеанс завершает свою работу, предотвращая несанкционированный доступ.

Такой подход, основанный на многократной проверке, позволяет повысить надёжность алгоритма, минимизируя вероятность ошибок распознавания, вызванных внешними факторами, такими как изменения освещения или случайные искажения изображения.

Система биометрической аутентификации KIRTapp была внедрена в операционную систему Secux Linux. На рисунке 2 показан процесс работы KIRTapp. При успешном распознавании пользователя выводится "good", а при несовпадении или отсутствии распознавания – "bad" в журнале сервиса. Вся информация также сохраняется в файл logs в папке с программой (рисунок 3).

```
мар 14 20:46:16 kirttest systemd[1]: Starting Run KIRTapp...
мар 14 20:46:18 kirttest python3[3698]: [ WARN:0@1.321] global cap_gstreamer.cpp:1777 open OpenCV
мар 14 20:46:30 kirttest python3[3698]: good
мар 14 20:46:30 kirttest python3[3698]: kol - 1
мар 14 20:46:30 kirttest python3[3698]: count - 1
мар 14 20:46:30 kirttest python3[3698]: good
мар 14 20:46:30 kirttest python3[3698]: kol - 2
мар 14 20:46:30 kirttest python3[3698]: count - 2
мар 14 20:46:30 kirttest python3[3698]: good
мар 14 20:46:30 kirttest python3[3698]: kol - 3
мар 14 20:46:30 kirttest python3[3698]: count - 3
мар 14 20:46:30 kirttest python3[3698]: good
мар 14 20:46:30 kirttest python3[3698]: kol - 4
мар 14 20:46:30 kirttest python3[3698]: count - 4
мар 14 20:46:30 kirttest python3[3698]: good
мар 14 20:46:30 kirttest python3[3698]: kol - 5
мар 14 20:46:30 kirttest python3[3698]: count - 5
```

Рисунок 2 – Журнал сервиса KIRTapp

```
 GNU nano 8.3
2025-03-14 20:46:30 - INFO - The checking was successful
2025-03-14 20:51:43 - INFO - The checking was successful
2025-03-14 20:57:03 - INFO - The checking was failed
2025-03-14 21:02:33 - INFO - The checking was failed
2025-03-14 21:07:40 - INFO - The checking was failed
2025-03-14 21:13:03 - INFO - The checking was failed
2025-03-17 19:09:46 - INFO - The checking was successful
```

Рисунок 3 – Файл с логами

Таким образом, на основе проведенного тестирования показано, что система KIRTapp обеспечивает надёжный контроль доступа и мониторинга пользователей, минимизируя риск несанкционированного входа. В будущем планируется внедрение нейросетей и анти-спуфинг технологий для повышения точности распознавания и защиты от попыток обхода системы.

Список использованных источников:

1. Вержбицкий, С. В. Биометрические системы и технологии: основы, методы, средства. – М.: Горячая линия – Телеком, 2019 г. – 304 с.
2. Исследование эффективности библиотек распознавания лиц [Электронный ресурс]. – Режим доступа: https://libeldoc.bsuir.by/bitstream/123456789/51893/1/Petrov_Issledovanie.pdf.
3. Сравнение алгоритмов детекции лиц [Электронный ресурс]. – Режим доступа: https://habr.com/ru/articles/661671/.

UDC 004.422.833

KIRTAPP BIOMETRIC AUTHENTICATION SYSTEM

Romanov D.A., Kolbanov G. P.
students of the educational institution "National Children's Technopark",
Minsk, Republic of Belarus
Belousova E.S. – PhD (Tech.), Ass. Prof. of Department of IP

Annotation. In this paper, we consider the KIRTapp system, designed for registration and access control using facial recognition. The analysis of various algorithms was carried out, on the basis of which the optimal identification method of Face Recognition was chosen. The KIRTapp system provides continuous monitoring of the user and automatic response to changes in the authentication process, reducing the risk of unauthorized access. In the future, it is planned to integrate neural networks and anti-spoofing technologies to increase security.

Keywords. Face Recognition; OpenCV; biometric authentication; machine learning, neural networks; face recognition.