УДК 004.9:005.9;004.89

АВТОМАТИЗАЦИЯ КОНТРОЛЯ И УПРАВЛЕНИЯ ДОСТУПОМ НА ОСНОВЕ БИОМЕТРИЧЕСКОЙ ВЕРИФИКАЦИИ ПО ЛИЦУ

Дудкина Е.А., Парамонов А.И.
Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь
E-mail: a.paramonov@bsuir.by

Аннотация:

Дудкина Е.А., Парамонов А.И. Автоматизация контроля и управления доступом на основе биометрической верификации по лицу. *В работе рассматриваются вопросы разработки современной автоматизированной системы контроля и управления доступом. Предлагается комплексное решение с использованием двухфакторной аутентификации, сочетающее идентификацию по QR-коду и обработку биометрических данных (верификацию по лицу) с интеграцией человека в контур принятия решений (Human-in-the-Loop). Описана архитектура гибридной системы, построенной по клиент-серверной модели с использованием облачной платформы Firebase, Android-приложения для пользователя и Kotlin-приложения для сотрудника охраны. Биометрическая верификация реализована на основе глубоких свёрточных нейронных сетей с вычислением косинусного расстояния между эмбеддингами лиц. Приведён механизм адаптивного обучения системы за счёт накопления подтверждённых охранником вариаций лица, что позволяет повышать точность автоматического распознавания в реальных условиях эксплуатации*

Annotation:

Dudkina E.A., Paramonov A.I. Automation of Access Control and Management Based on Facial Biometric Verification. *The problem of automating access control and management based on facial biometric verification is addressed. A comprehensive solution combining QR code identification and facial biometric verification with a Human-in-the-Loop decision-making framework is proposed. The architecture of a hybrid system built on a client-server model using the Firebase cloud platform, an Android application for the user, and a Kotlin application for the security officer is described. Facial biometric verification is implemented using deep convolutional neural networks with cosine distance computation between face embeddings. An adaptive learning mechanism is presented, where face variations confirmed by the security officer are accumulated, improving automatic recognition accuracy under real-world operating conditions.*

Ключевые слова: *верификация по лицу, Human-in-the-Loop, контроль и управление доступом, QR-код, машинное обучение (ML).*

Keywords: *Face Verification, Human-in-the-Loop, Access Control and Management, QR code, Machine Learning (ML).*

Общая постановка проблемы

Современные организации, включая образовательные учреждения, сталкиваются с возрастающими требованиями к обеспечению безопасности и эффективности процессов управления доступом. Одной из ключевых проблем в данной области является использование устаревших методов контроля, таких как бумажные журналы посещений или ручная идентификация, что сопряжено с низкой скоростью обработки данных, высокой вероятностью ошибок и недостаточной защитой персональной информации. Эти методы

создают серьезные неудобства для пользователей и сотрудников, увеличивают временные затраты и снижают общую безопасность.

В эпоху цифровой трансформации остро стоит вопрос о необходимости автоматизации процессов управления доступом с целью их усовершенствования. Автоматизация позволяет исключить человеческий фактор, минимизировать количество ошибок, повысить удобство и безопасность для пользователей. Глобально проблема автоматизации управления доступом связана с необходимостью разработки универсальных алгоритмов и средств, способных адаптироваться к различным условиям использования, обеспечивать надежность и безопасность, учитывать специфику организации, масштабируемость системы, а также возможность интеграции с другими информационными платформами.

Внедрение современных средств и технологий обеспечивает быструю обработку и передачу данных в рамках информационной системы контроля и управления доступом, что исключает проблемы ручного ввода и минимизирует риски утраты или подделки информации.

В работе предлагается комплексное решение для идентификации и контроля прохода, в основе которого система с применением QR-кодов и с интегрированным модулем анализа биометрических данных (на примере верификация по лицу).

Ключевые вопросы биометрической верификации по лицу

Распознавание лиц является одним из наиболее изученных направлений биометрии. Современные подходы основаны на использовании глубоких свёрточных нейронных сетей (CNN), которые преобразуют исходное изображение в компактный вектор признаков – эмбеддинг. Этот вектор представляет собой числовое описание лица, устойчивое к изменениям освещения, поворотам головы и мимическим выражениям. В отличие от классических методов (PCA, LBP, HOG), глубокие сети обучаются на миллионных наборах данных и способны выделять иерархические признаки высокого уровня, что обеспечивает высокую точность даже в сложных условиях [1–3].

Сравнение двух лиц в современных биометрических системах сводится к вычислению расстояния между их эмбеддингами – компактными числовыми векторами, полученными из изображений с помощью глубоких нейронных сетей. Чем ближе векторы в пространстве признаков, тем выше вероятность того, что лица принадлежат одному человеку. Наиболее часто для оценки схожести используются косинусное расстояние и евклидово расстояние.

Косинусное расстояние (вычисляемое как 1 – косинус угла между векторами) обладает рядом преимуществ: его значения лежат в диапазоне [0, 2], оно не зависит от масштаба вектора (длины) и хорошо работает с нормализованными эмбеддингами. В отличие от него, евклидово расстояние чувствительно к модулю векторов, поэтому требует предварительной нормализации, но в некоторых реализациях также даёт стабильные результаты.

Для принятия бинарного решения – принадлежат ли два лица одному человеку – вводится пороговое значение. Если вычисленное расстояние меньше порога, лица считаются идентичными, в противном случае – разными. Выбор порога непосредственно влияет на две ключевые метрики: частоту ложного принятия (FAR – False Acceptance Rate) и частоту ложного отказа (FRR – False Rejection Rate). При снижении порога уменьшается FAR (меньше шансов пропустить чужого), но растёт FRR (чаще отказывается доступ своему пользователю). На практике невозможно одновременно минимизировать обе ошибки, поэтому выбирается компромисс, соответствующий требованиям конкретного приложения [4].

В системах контроля доступа приоритетом обычно является безопасность, а не абсолютное удобство. Поэтому выбирают относительно низкий порог, что даёт низкий FAR (минимизирует риск пропуска постороннего) даже ценой увеличения FRR (возможных

ложных отказов). Однако высокий FRR приводит к задержкам на проходной и недовольству пользователей. Именно здесь механизм Human-in-the-Loop оказывается особенно полезным: для случаев, когда автоматическое сравнение даёт результат, близкий к порогу, решение передаётся сотруднику охраны. Это позволяет установить более строгий порог для автоматического пропуска (повышая безопасность), а ручное подтверждение компенсирует возможные ложные отказы.

Выбор конкретного числового порога для разработанной системы производился экспериментально на основе тестового набора данных, включающего эталонные и текущие изображения, собранные в реальных условиях. Была построена ROC-кривая (зависимость FRR от FAR), и порог выбран в точке, обеспечивающей FAR ≤ 0,01 при приемлемом FRR, который в начальный момент эксплуатации компенсировался участием охранника. В дальнейшем, по мере накопления вариаций лица, точность автоматического распознавания повышается, что позволяет либо оставить порог неизменным (снизив долю ручных проверок), либо ужесточить его для дополнительного повышения безопасности. Такой адаптивный подход описан в работах по непрерывному обучению биометрических систем [5, 6].

Реальные условия эксплуатации систем распознавания лиц вносят множество факторов, значительно усложняющих задачу идентификации. К таким факторам относятся изменения внешности человека: смена причёски, появление или исчезновение бороды и усов, ношение очков с разными диоптриями или без них, использование головных уборов, макияж, а также естественные возрастные изменения. Кроме того, значительное влияние оказывают условия съёмки: освещение может быть ярким или тусклым, направленным сверху, сбоку или снизу, создавая глубокие тени на лице; угол поворота головы варьируется от анфаса до профиля; выражение лица может меняться от нейтрального до улыбки или нахмуренности. Даже самые высококачественные модели глубокого обучения, обученные на многомиллионных датасетах, могут давать сбои, если эталонное фото сделано в идеальных условиях студии, а текущий кадр получен в полумраке вестибюля или когда человек повёрнут вполоборота.

Для преодоления этой проблемы применяются методы адаптации, при которых система обновляет представление о пользователе на основе новых успешных проходов, накапливая информацию о вариативности его внешности в реальных условиях эксплуатации. Наиболее простой и распространённый подход заключается в сохранении нескольких вариантов эмбеддингов для одного пользователя, соответствующих различным ракурсам, освещению и мимике. При верификации сравнение проводится не только с единственным эталонным эмбеддингом, но и со всем набором накопленных вариантов, и за результат принимается минимальное расстояние (или максимальное сходство) среди них. Альтернативой является использование усреднённого (среднего арифметического) эмбеддинга, полученного из всех сохранённых образцов, что позволяет получить более устойчивое представление о лице, сглаживающее случайные отклонения.

Более сложный, но потенциально более точный подход – дообучение (fine tuning) самой нейросетевой модели на собранных в процессе эксплуатации данных. Это требует существенных вычислительных ресурсов (мощного графического процессора), специализированного программного обеспечения для обучения, а также организации периодических сеансов переобучения модели с последующим обновлением её в клиентских приложениях. Такой метод позволяет модели адаптироваться к специфическим условиям конкретного объекта (освещению, углам обзора камер) и к особенностям внешности контингента. Однако из-за сложности реализации и высоких требований к ресурсам, для систем контроля доступа на ограниченной территории чаще выбирают первый вариант – накопление вариантов эмбеддингов, который легко реализуется с помощью облачных баз данных и не требует переобучения сети [5, 6].

Подход на основе концепции Human-in-the-Loop

Концепция Human in the Loop (HITL), или «человек в цикле», предполагает интеграцию человека в контур принятия решений автоматизированной системы, особенно на начальных этапах эксплуатации или при обработке сложных, неоднозначных случаев. Применительно к задаче биометрической верификации по лицу это означает, что система на первом этапе выполняет автоматическую оценку сходства между текущим изображением и эталонными образцами, вычисляя, например, косинусное расстояние между эмбеддингами. Однако окончательное решение – разрешить или запретить проход – принимает сотрудник охраны. Такой подход позволяет сочетать скорость автоматической обработки с надёжностью, обеспечиваемой человеческим опытом и способностью учитывать контекст, который не всегда поддаётся формализации.

Каждое решение охранника служит ценным маркированным примером для системы. Если охранник подтверждает личность, несмотря на то что автоматическое сравнение дало результат, близкий к порогу (например, из-за нестандартного освещения или ракурса), система фиксирует этот кадр как дополнительный образец лица данного пользователя. В простейшем случае такой образец просто добавляется в базу эталонных вариантов, расширяя набор эмбеддингов, с которыми будут сравниваться будущие попытки прохода. Это позволяет системе постепенно «узнавать» внешность человека в разных условиях, повышая точность автоматического распознавания. В более сложной реализации подтверждённые примеры могут использоваться для корректировки порогов принятия решений (например, снижения порога для конкретного пользователя, если он часто сталкивается с ложными отказами) или даже для периодического дообучения (fine tuning) самой нейросетевой модели на накопленных данных, что требует больших вычислительных ресурсов, но даёт максимальное повышение точности [7].

Преимущество подхода HITL заключается в том, что он позволяет организовать постепенный переход от полностью ручного контроля к автоматическому без снижения уровня безопасности. На начальном этапе, когда система ещё не накопила достаточного количества вариаций лиц, охранник может принимать решения практически по каждому проходу, а система лишь отображает степень сходства. По мере накопления подтверждённых образцов доля автоматически пропускаемых проходов растёт, а нагрузка на охранника снижается. В итоге система выходит на режим, при котором лишь единичные, действительно сложные случаи требуют человеческого вмешательства. Такой подход соответствует современным требованиям к адаптивным системам контроля доступа, где безопасность и удобство не противопоставляются, а достигаются в результате совместной работы человека и алгоритмов [7].

Архитектурное решение системы контроля и управления доступом

Система построена по клиент-серверной модели и состоит из двух независимых клиентских приложений, взаимодействующих с общей облачной платформой Firebase. Такой подход позволяет разделить функциональные зоны: пользователь работает с мобильным приложением для управления своим профилем и генерации QR-кодов, а сотрудник охраны – со стационарным приложением для верификации и контроля доступа.

Android-приложение (личный кабинет) выполняет следующие задачи:

– аутентификация и управление пользователями – регистрация, вход, редактирование профиля;

– генерация QR-кодов – создание персонального QR-кода, содержащего идентификатор пользователя;

– загрузка эталонного фото – выбор изображения из галереи или камеры, отправка в Firebase Storage и сохранение ссылки в Realtime Database;

– просмотр личных данных – отображение имени, статуса, загруженного фото.

Kotlin-приложение (рабочее место охраны) предоставляет следующие функциональные возможности:

– сканирование QR-кода – считывание кода с мобильного устройства посетителя через камеру;

– получение эталонных данных – по идентификатору из QR-кода загрузка из Firebase эталонного фото и накопленных биометрических шаблонов пользователя;

– захват текущего изображения – использование камеры для получения фотографии лица в момент прохода;

– сравнение лиц (ML Kit) – извлечение эмбеддингов лица из текущего кадра и сравнение с эталоном, а также с накопленными вариациями;

– интерфейс охранника – отображение результатов автоматического сравнения, предоставление возможности ручного подтверждения или отклонения прохода;

– обучение (Human-in-the-Loop) – при подтверждении охранником сохранение текущего кадра в Firebase Storage как новой вариации лица.

Дополнительно развернутая *облачная инфраструктура (Firebase)* позволяет эффективно выполнить следующие задачи:

– управление учётными записями пользователей (Firebase Authentication);

– хранение структурированных данных (например, профили пользователей, ссылки на фото, журнал событий) (Firebase Realtime Database);

– хранение файлов изображений (например, эталонные фото, обучающие снимки) (Firebase Storage).

Выбор технологического стека системы определялся архитектурным решением, каждая часть которого решает свой круг задач.

Для Android-приложения, реализующего личный кабинет пользователя, базовым языком разработки выбран Java. Взаимодействие с Firebase в Android-приложении осуществляется через стандартные SDK, предоставляемые Google.

Kotlin-приложение с использованием фреймворка Ktor для построения серверной части. Выбор Kotlin обусловлен его современными возможностями, лаконичностью и полной совместимостью с Java-экосистемой, что упрощает интеграцию с Firebase SDK, написанными на Java. Ktor выбран благодаря своей лёгкости, асинхронной модели на корутинах и встроенной поддержке работы с multipart-запросами, необходимыми для приёма изображений с камеры. В качестве библиотеки для работы с камерой использован CameraX – официальное решение от Google, предоставляющее высокоуровневый API для предпросмотра, захвата изображений и анализа видеопотока [10]. CameraX автоматически адаптируется к аппаратным возможностям устройства, что критически важно для стабильной работы на различных компьютерах, которые могут быть установлены на посту охраны.

Биометрическая верификация реализована с помощью Google ML Kit (Face Detection). Выбор ML Kit обоснован тем, что библиотека работает полностью на устройстве (on device), что исключает задержки, связанные с передачей данных на внешний сервер, и позволяет системе функционировать даже при временном отсутствии интернет-соединения. ML Kit предоставляет готовые модели для обнаружения лиц и извлечения эмбеддингов – компактных векторов признаков, которые затем сравниваются между собой с помощью косинусного расстояния. Использование готового решения позволило сосредоточиться на логике адаптивного обучения (Human in the Loop), не затрачивая ресурсы на разработку и обучение собственной нейросети.

Выбор именно Firebase обусловлен также наличием бесплатного начального тарифа, что особенно важно на этапе прототипирования, и возможностью масштабирования при переходе к промышленной эксплуатации. Все сервисы Firebase предоставляют готовые SDK для Java/Kotlin и Android, что обеспечивает бесшовную интеграцию с обоими клиентскими приложениями [8, 9]. Таким образом, предложенный технологический стек позволяет

эффективно реализовать заявленную функциональность, обеспечивая высокую производительность, безопасность данных и возможность дальнейшего развития системы.

Выводы

В статье описан один из подходов к разработке гибридной системы контроля доступа, сочетающей идентификацию по QR-коду и биометрическую верификацию по лицу с возможностью непрерывного дообучения по накопленным материалам в ходе эксплуатации. Предложенное решение позволяет модернизировать существующий прототип, добавляя важный уровень безопасности и адаптации к изменяющимся условиям. Использование предложенных современных технологических решений открывает возможности для дальнейшего совершенствования системы в процессе эксплуатации. Система находится на этапе опытной эксплуатации и компьютерных экспериментов, что позволит накопить материалы для анализа выдвинутых гипотез по ее устойчивости, надежности и безопасности.

Литература

8. Schroff, F. FaceNet: A Unified Embedding for Face Recognition and Clustering / F. Schroff, D. Kalenichenko, J. Philbin // Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR). – Boston, 2015. – P. 815–823.

9. Deng, J. ArcFace: Additive Angular Margin Loss for Deep Face Recognition / J. Deng, J. Guo, N. Xue, S. Zafeiriou // Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR). – Long Beach, 2019. – P. 4690–4699.

10. Wang, M. Deep Face Recognition: A Survey [Электронный ресурс] / M. Wang, W. Deng // arXiv. – 2020. – arXiv:1804.06655v9. – Режим доступа: https://arxiv.org/abs/1804.06655. – Дата доступа: 20.03.2025.

11. Lerworatham, A. Enhancing Facial Recognition Accuracy in eKYC Systems: A Comparative Evaluation of Euclidean Distance, Cosine Similarity, and SSIM Under Real-World Challenges [Электронный ресурс] / A. Lerworatham, E. Smajli, G. Feldman, M. Ghonem, H. Mahmoud, N. Elmitwally // The 4th International Conference of Advanced Computing and Informatics. – Birmingham, 2024. – Режим доступа: https://www.open-access.bcu.ac.uk/16135/. – Дата доступа: 21.03.2025.

12. Ul Haq, M. A Comprehensive Review of Face Detection/Recognition Algorithms and Competitive Datasets to Optimize Machine Vision / M. Ul Haq, M. A. J. Sethi, S. Ahmad, N. Ahmad, M. S. Anwar, A. Kutlimuratov // Computers, Materials & Continua. – 2025. – Vol. 84, No 1. – P. 1–24. – DOI: 10.32604/cmc.2025.063341.

13. Kiran, M. Incremental Template Learning for Occlusion-Aware Visual Object Tracking [Электронный ресурс] / M. Kiran, L. T. Nguyen-Meidine, R. Menelau-cruz, E. Granger // SSRN. – 2025. – DOI: 10.2139/ssrn.5218069. – Режим доступа: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5218069. – Дата доступа: 21.03.2025.

14. Wu, X. A Survey of Human-in-the-loop for Machine Learning [Электронный ресурс] / X. Wu, L. Xiao, Y. Sun, J. Zhang, T. Ma, L. He // arXiv. – 2021. – arXiv:2108.00941. – Режим доступа: https://arxiv.org/abs/2108.00941. – Дата доступа: 21.03.2025.

15. Google Developers. Firebase Documentation [Электронный ресурс] / Google Developers. – Режим доступа: https://firebase.google.com/docs. – Дата доступа: 22.03.2025.

16. Google Developers. ML Kit for Android: Face Detection [Электронный ресурс] / Google Developers. – Режим доступа: https://developers.google.com/ml-kit/vision/face-detection. – Дата доступа: 24.03.2025.

17. Android Developers. CameraX Overview [Электронный ресурс] / Android Developers. – Режим доступа: https://developer.android.com/training/camerax. – Дата доступа: 24.03.2025.