СТАТЬИ

УДК 004.89

ИСПОЛЬЗОВАНИЕ БИОМЕТРИЧЕСКИХ ДАННЫХ В СИСТЕМАХ РАСПОЗНАВАНИЯ ЛИЦ

Амеличев Г.Э., Панина В.С., Белов Ю.С.

Московский государственный технический университет имени Н.Э. Баумана, Калужский филиал, Калуга, e-mail: amelichev.g2020@mail.ru

Поскольку биологические данные являются огромным источником информации, из которого необходимо извлекать полезные знания, распознавание образов становится все более важным. Биометрические данные – это измерения и расчеты, связанные с характеристиками человека. Эти данные состоят из так называемых биометрических идентификаторов – отдельных измеримых характеристик, используемых для идентификации и описания людей. В настоящее время использование биометрических данных зачастую связано с идентификацией личности и контролем доступа. Практически каждая современная модель смартфонов снабжена системой распознавания лиц или сканером отпечатков пальцев для аутентификации пользователя. Однако биометрическая идентификация заставила многих с осторожностью относиться к ее использованию в качестве автономной аутентификации. При этом нельзя отрицать, что биометрические технологии предлагают привлекательные решения для обеспечения безопасности. И, несмотря на риски, данные системы удобны и их сложно дублировать. Кроме того, эти системы продолжают постоянно развиваться и совершенствоваться. Данная статья посвящена вопросу использования биометрических данных в современном мире. Рассмотрены наиболее популярные типы биометрии. Выявлены основные этапы для разработки систем распознавания лиц. Обозначены различные методы, включая локальный, целостный и гибридный подходы, которые обеспечивают распознавание изображения лица, используя физические или поведенческие черты (одну и более).

Ключевые слова: биометрические данные, детектор, детектор Виолы – Джонса, распознавание образов, этапы распознавания лиц, классификация методов распознавания лиц

USING BIOMETRIC DATA IN FACIAL RECOGNITION SYSTEMS

Amelichev G.E., Panina V.S., Belov Yu.S.

Bauman Moscow State Technical University, Kaluga branch, Kaluga, e-mail: amelichev.g2020@mail.ru

Since biological data is a huge source of information from which useful knowledge must be extracted, pattern recognition becomes more and more important. Biometric data are measurements and calculations related to a person's characteristics. This data consists of so-called biometric identifiers – individual measurable characteristics used to identify and describe people. Today, the use of biometric data is often associated with personal identification and access control. Almost every modern smartphone model is equipped with a face recognition system or a fingerprint scanner for user authentication. However, biometric identification has led many to be wary of using it as an offline authentication. That being said, it cannot be denied that biometric technologies offer attractive security solutions. And, despite the risks, these systems are convenient and difficult to duplicate. In addition, these systems continue to evolve and improve continuously. This article focuses on the use of biometric data in the modern world. The most popular types of biometrics are considered. The main stages for the development of face recognition systems are identified. Various techniques are outlined, including local, holistic, and hybrid approaches that provide facial recognition using one or more physical or behavioral traits.

Keywords: biometric data, detector, Viola-Jones detector, pattern recognition, stages of face recognition, classification of face recognition methods

Все физические и биологические особенности человека позволяют идентифицировать личность. Наиболее популярными способами цифровой идентификации личности являются распознавание отпечатков пальцев, структуры радужной оболочки глаза, сетчатки глаза, аутентификация на основе динамики рукописной подписи и голоса. Основной сферой внедрения биометрических данных являются места, где необходимо обеспечить безопасность доступа к информации или материальным объектам. Биометрия предоставляет уникальный доступ к данным, который нельзя потерять и практически невозможно подделать [1].

Биометрия, как правило, более удобна, чем другие методы аутентификации личности. Выходя из номера отеля, вы можете забыть свой ключ, но все равно сможете использовать биометрические устройства для аутентификации личности. Достаточно просто приложить палец к сканеру или посмотреть в камеру [2].

Популярность биометрических данных растет с каждым годом. Они стали одним из главных символов нашего времени, и их распространение вошло не только в систему защиты данных, но и на путь развлечений. Биометрия все еще находится на ранних стадиях развития, но конкретные приложения уже существуют.

Исторически приложения, использующие биометрию, используются властями для контроля доступа военных, идентификации преступников или гражданских лиц в рамках жестко регулируемой правовой и технической базы.

Сегодня секторы, включая банковское дело, розничную торговлю и мобильную коммерцию, демонстрируют реальный интерес к преимуществам биометрии.

За последние семь лет осведомленность и признание биометрии повысилось, поскольку миллионы пользователей смартфонов разблокируют свои телефоны с помощью лица или отпечатка пальца.

Цель исследования: рассмотреть современные типы биометрии. Выявить основные этапы для разработки систем распознавания лиц. Привести описание различных методов, включая локальный, целостный и гибридный подходы, которые обеспечивают распознавание изображения лица, используя физические или поведенческие черты (одну и более).

Типы биометрии. Поскольку основной задачей биометрии является идентификация личности, выделяют следующие типы характеристик: физиологические (статистические) и поведенческие (динамические). Физиологические характеристики основываются на строении человеческого тела, которые являются неизменными. К ним можно отнести отпечаток пальцев. Поведенческие характеристики завязываются на поведении человека, к ним можно отнести, скорость написания текста. Некоторые исследователи ввели термин «бихевиометрия» для описания последнего класса биометрии.

Наиболее распространенными типами биометрии являются:

1. Идентификация по отпечатку пальца. В последние годы сканеры отпечатков пальцев стали повсеместными благодаря их широкому распространению на смартфонах. Любое устройство, к которому можно прикоснуться, например экран телефона или сенсорная панель, может стать простым и удобным сканером отпечатков пальцев. Согласно Spiceworks, сканирование отпечатков пальцев является наиболее распространенным типом биометрической аутентификации [3].

2. Распознавание на основе фото и видео. Если устройство оснащено камерой, его можно легко использовать для аутентификации. Распознавание лиц и идентификация по радужной оболочке глаза являются двумя общими подходами [4].

3. Идентификация по лицу. Распознавание лиц является третьим наиболее распространенным типом аутентификации. Другие методы аутентификации на основе изображений включают распознавание геометрии рук, считывание радужной оболочки или сетчатки глаза.

4. Идентификация с помощью человеческого голоса. С другой стороны, идентификация – это задача определения личности неизвестного говорящего. В некотором смысле верификация представляет собой поиск совпадений 1:1, где голос одного говорящего сопоставляется с определенным шаблоном, тогда как идентификация говорящего – это совпадение 1:N, где голос сравнивается с несколькими шаблонами. Цифровые помощники на основе голоса и порталы телефонного сервиса уже используют распознавание речи для идентификации пользователей и аутентификации клиентов.

5. Идентификация по рукописному почерку. Аутентификация с помощью подписи часто используется в тех сферах деятельности, где речь заходит об оформлении документов. Проверка подлинности подписи не подойдет, если стоит задача получения доступа к помещению, так как это будет очень долгий процесс. А подпись документа будет быстрой и нетрудной.

6. Идентификация по ДНК. Сегодня ДНК-тесты используются главным образом в правоохранительных органах для выявления подозреваемых. На практике секвенирование ДНК было очень долгим процессом, но сейчас технологии меняются. Существует возможность провести ДНК-тест за считанные минуты.

Основные этапы систем распознавания лиц. Создание системы распознавания лиц включает три основных этапа: получение изображения лица, извлечение основных признаков и распознавание личности [5]. На первом этапе системе необходимо получить изображение, в которое попало человеческое лицо. На этапе извлечения признаков происходит создание вектора признаков для конкретного человеческого лица, обнаруженного на предыдущем этапе. В завершение необходимо сравнить полученный вектор признаков с другими лицами, имеющимися в базе данных. В случае успешного нахождения пользователя можно сказать, что идентификация прошла успешно.

– Получение изображения лица. Система распознавания лиц начинается с локализации человеческих лиц на имеющемся изображении. Основная задача – определить, присутствует на данном изображении человеческое лицо или нет. Внешние факторы могут отразиться на корректности распознавания. К внешним факторам можно отнести освещенность помещения, в котором

делалось изображение. Предварительная обработка поможет сделать процесс распознавания человека более легким. Существует множество методов для обнаружения и определения местоположения человеческого лица на изображении, например детектор Виолы – Джонса, представленный на рис. 1, гистограмма ориентированного градиента (HOG) и анализ главных компонентов (PCA) [6–8].

– Извлечение признаков: после этапа получения изображения человеческого лица необходимо извлечь особенности черт его лица. Данная функция представляет все признаки в виде набора векторных признаков. Под векторными признаками принято понимать такие элементы лица, как глаза, нос, рот и их геометрическое распределение [9]. Человеческое лицо представляет собой сложную структуру. У каждого человека свои размеры головы, разрез глаз, форма носа – этот набор признаков помогает идентифицировать человека. В основном методы основываются на выделении рта, глаз или носа для проверки личности по размеру и расстоянию. Для извлечения черт лица широко используются следующие методы: HOG, масштабно-инвариантное преобразование признаков (SIFT), вейвлеты Хаара, фильтр Габора, преобразования Фурье и методы локальной двоичной структуры (LBP) Eigenface, линейный дискриминантный анализ (LDA), локальное квантование фазы (LPQ), независимый компонентный анализ (ICA) [10].

– Распознавание лиц: все признаки, извлеченные на прошлом этапе, сравниваются с заполненной ранее базой данных. Набор признаков сравнивается с признаками из базы данных и на основе имеющихся данных выдает результат распознавания. Существует два основных способа распознавания лиц: один называется идентификацией, а другой – верификацией. На этапе идентификации лицо человека сравнивается с известным лицом в базе данных, чтобы принять решение, совпадает ли лицо с имеющимся в базе данных. Корреляционные фильтры (CF) [10], сверточная нейронная сеть (CNN), а также k-ближайший сосед (K-NN), как известно, эффективно решают эту задачу.

На рис. 2 представлена схема этапов распознавания лица.

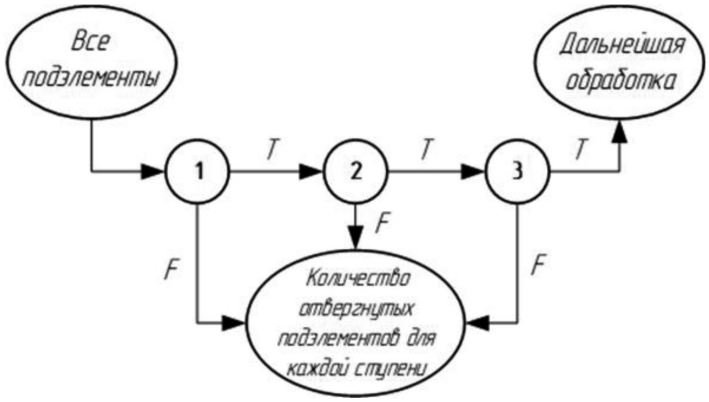

Рис. 1. Детектор Виолы – Джонса

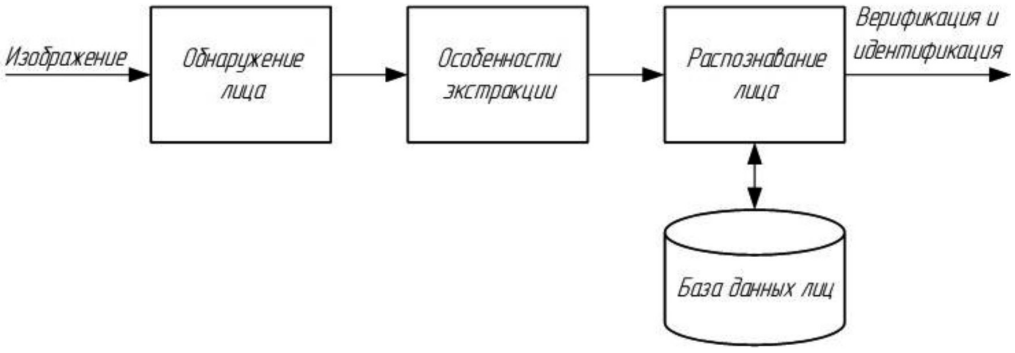

Рис. 2. Этап распознавания лиц

Классификация систем распознавания лиц. Системы распознавания лиц являются не самыми эффективными и надежными методами по сравнению с другими биометрическими системами, такими как распознавание сетчатки, радужной оболочки или отпечатков пальцев. Кроме того, несмотря на все вышеперечисленные преимущества, эта биометрическая система имеет множество ограничений. Распознавание лиц в контролируемых условиях является очень всеобъемлющим.

Основная проблема компьютерного зрения – большая контрастность зрительных образов. На изображение могут повлиять внешние факторы. К таким факторам можно отнести освещение помещения, цвет изображения, угол обзора [11]. Количество факторов, которые могут повлиять, сложно предугадать. К примеру, это могут быть цвет и яркость отдельных пикселей изображения.

Обычно к этим факторам относят:

1) количество и расположение источников света;

2) цвет и интенсивность излучения;

3) тени или отражения окружающих предметов.

Большие объемы данных могут затруднить поиск объектов. Поскольку изображения могут содержать тысячи пикселей, каждый пиксель имеет смысл. Чтобы в полной мере воспользоваться информацией, содержащейся в изображении, необходимо проанализировать каждый пиксель объекта или фона и рассмотреть возможную изменчивость объекта. Из-за большой памяти и производительности компьютера этот анализ может быть дорогостоящим.

Для решения этой задачи необходимо правильно подобрать описание объекта и систему распознавания обнаружения. Описание объекта должно быть достаточно репрезентативным, чтобы отличить его от остальной окружающей сцены.

При построении системы обнаружения и распознавания необходимо учитывать:

1) выбор между 2D и 3D представлением сцены: алгоритмы, использующие двумерные представления, проще, но требуют большого количества различных описаний, которые соответствуют представлению объекта в различных условиях наблюдения;

2) выбор между описанием объекта в целом или как системы, состоящей из набора взаимосвязанных элементов;

3) выбор между системой признаков на основе геометрических характеристик или характеристик, описывающих особенности объекта.

Были реализованы несколько систем для идентификации человеческого лица в 2D или 3D изображениях [12]. Эти системы на основе метода их обнаружения и распознавания, как показано на рис. 3, можно классифицировать на три подхода:

1) локальный подход;

2) целостный подход;

3) гибридный подход.

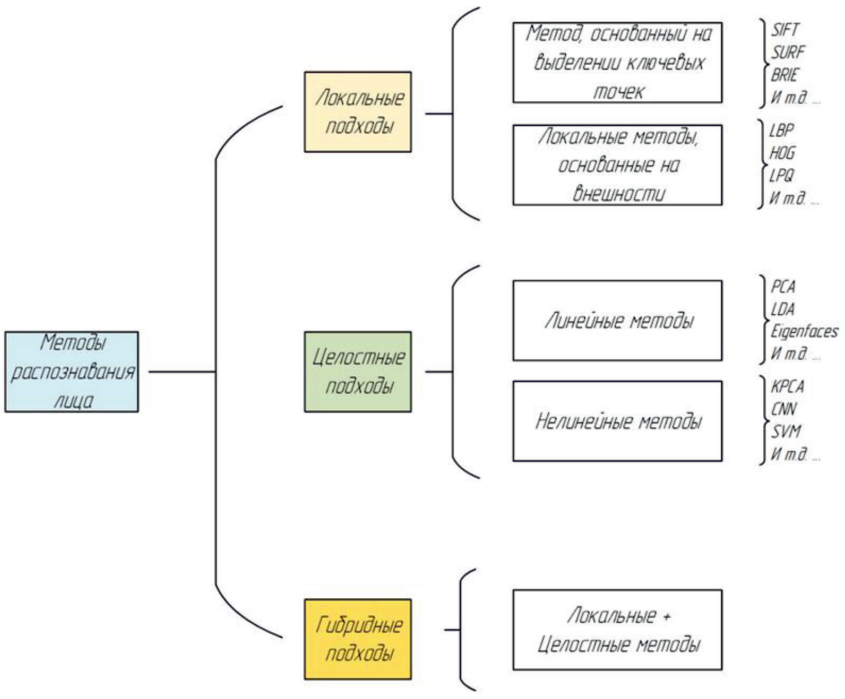

Рис. 3. Классификация методов распознавания лица

Первый подход основан на рассмотрении отдельных черт лица, не рассматривает полностью лицо. Второй подход использует полностью грань, как входной параметр, а после проецирует в небольшое подпространство или в корреляционную плоскость. Третий подход использует локальные и глобальные особенности для повышения точности распознавания лиц.

Основным отличием при использовании гибридных подходов можно назвать избавление или сведение к минимуму недостатков каждого метода распознавания по отдельности.

Заключение

Таким образом, система биометрической верификации – это новая тенденция, меняющая наш образ жизни. Она внедрена почти во все отрасли и секторы для обеспечения конфиденциальности и безопасности как отдельных лиц, так и организаций. В ближайшем будущем мы увидим более широкое внедрение технологии распознавания лиц для доступа к личным устройствам для реорганизации и аутентификации. Это, несомненно, внесет изменения в наши судебные и правоохранительные органы, предоставив им возможность обеспечить безопасность данных с помощью систем биометрической проверки и обеспечить безопасность записей преступников и материалов дела. Благодаря этой технологии мы сможем обмениваться файлами и данными из одной системы в другую и передавать их без какой-либо угрозы кражи. Она обеспечит безопасность с комфортом и простым в использовании решением, которое, несомненно, сделает нашу жизнь простой, легкой и безопасной.

Список литературы

1. Biometrics Institute. «Biometrics Institute Privacy Code». [Electronic resource]. URL: http://www.biometricsinstitute.org/displaycommon.cfm?an=1&subarticlenbr=8 (date of access: 11.09.2021).

2. Mordini E., Massari S. Body, Biometrics and Identity. Bioethics. 2008. Vol. 22. Issue 9. P. 488–498.

3. Duarte T. Biometric access control systems: A review on tecnolodies to improve their efficiency. power Electronics and Motion Control Conference (PEMC). 2016. P. 2–5.

4. Funk W., Arnold M., Busch C., Munde A. Evaluation of image compression algorithms for fingerprint and face recognition systems. In: Systems, Man and Cybernetics (SMC) Information Assurance Workshop. Proceedings from the Sixth Annual IEEE. West Point, NY, USA: IEEE Computer Society, 2005. P. 72–78.

5. Napoléon T., Alfalou A. Pose invariant face recognition: 3D model from single photo. Opt. Lasers Eng. 2017. No. 89. P. 150–161.

6. Viola P., Jones M. Rapid object detection using a boosted cascade of simple features. In Proceedings of the 2001 IEEE Computer Society Conference on Computer Vision and Pattern Recognition, Kauai, HI, USA, P. 3–6, 8–14 December 2001.

7. Ouerhani Y., Alfalou A., Brosseau C. Optics and Photonics for Information Processing XI. Volume 10395. SPIE; Bellingham, WA, USA: 2017. Road mark recognition using HOG-SVM and correlation; P. 2–5. International Society for Optics and Photonics.

8. Shah J.H., Sharif M., Raza M., Azeem A. A Survey: Linear and Nonlinear PCA Based Face Recognition Techniques. Int. Arab J. Inf. Technol. 2013. No. 10. P. 536–545.

9. Smach F., Miteran J. Atri M., Dubois J., Abid M., Gauthier J.P. An FPGA-based accelerator for Fourier Descriptors computing for color object recognition using SVM. J. Real-Time Image Process. 2007. No. 2. 249–258.

10. Berg T. and Belhumeur P. POOF: Part-based one-vs-one features for fine-grained categorization, face verification, and attribute estimation. In Proc. CVPR. 2013. P. 4–7.

11. Редько А.В., Молчанов А.Н., Белов Ю.С. Использование алгоритмов определения ключевых точек изображения в задаче реконструкции трехмерных сцен // Электронный журнал: наука, техника и образование. 2016. № 1 (5). С. 94–101.

12. Кузнецов Г.С., Белов Ю.С. Обзор метода 3D распознавания лиц без преобразования лицевой поверхности // Электронный журнал: наука, техника и образование. 2016. № 2 (6). С. 104–110.