Информационные системы. Информатика. Проблемы информационной безопасности

Information systems. Computer sciences. Issues of information security

УДК: 004.932
https://doi.org/10.32362/2500-316X-2021-9-3-7-14

НАУЧНАЯ СТАТЬЯ

Применение биометрических систем в технологиях идентификации лиц

А.А. Куликов @

МИРЭА – Российский технологический университет, Москва, 119454 Россия
@ *Автор для переписки, e-mail: tibult41@gmail.com*

Резюме. В работе приведен аналитический обзор применения биометрических систем распознавания применительно к технологиям идентификации лицевых изображений. Представлена классификация биометрических систем. Рассмотрены тенденции технологического прогресса в области биометрии и возможностей распознавания лиц. Определено, что в 2020 году наблюдается тенденция перехода от использования биометрических технологий распознавания в традиционных системах государственной безопасности в сферу коммерческого и пользовательского применения. Приведен процесс «связывания» ключей шифрования и паролей с биометрическими параметрами субъекта данных. Предложено под биометрическим признаком и параметром биометрии подразумевать некоторую величину, обладающую физическим смыслом, характеризующим сам субъект. Также представлена возможность использования в биометрии круговой окрестности и билинейной интерполяции значений интенсивностей пикселей, что даст возможность выстраивания локального бинарного шаблона. Для того чтобы решить проблему идентификации лиц, целесообразно исследовать суть биометрических систем в технологиях идентификации лиц, их виды, определив недостатки каждого из них, на основании чего представить направления устранения и поиска наиболее надежных технологий. Суть применения биометрических систем в технологиях идентификации лиц состоит, например, в том, что пользователь может предоставить банку или другому контрагенту доказательства того, что именно он хочет воспользоваться услугами по своим счетам. При этом спрос увеличился именно на бесконтактные биометрические решения. Данные технологии внедряются с целью проведения дополнительной биометрической проверки пользователей, которая позволяет минимизировать возможное мошенничество или нарушение внутренних правил сервиса, например, передачу аккаунтов одних зарегистрированных пользователей другим.

Ключевые слова: биометрия, параметры, признаки, преобразователь «биометрия – код», ключ, распознавание

• **Поступила:** 04.12.2020 • **Доработана:** 21.03.2021 • **Принята к опубликованию:** 01.04.2021

Для цитирования: Куликов А.А. Применение биометрических систем в технологиях идентификации лиц. *Российский технологический журнал*. 2021;9(3):7–14. https://doi.org/10.32362/2500-316X-2021-9-3-7-14

Прозрачность финансовой деятельности: Автор не имеет финансовой заинтересованности в представленных материалах или методах.

Автор заявляет об отсутствии конфликта интересов.

RESEARCH ARTICLE

Application of biometric systems in face identification technologies

Alexander A. Kulikov [@]

MIREA – Russian Technological University, Moscow, 119454 Russia
[@] *Corresponding author, e-mail: tibult41@gmail.com*

Abstract. The paper presents an analytical review of the application of biometric recognition systems in relation to facial image identification technologies. The classification of biometric systems is presented. The trends of technological progress in the field of biometrics and facial recognition capabilities are considered. It is determined that in 2020 there is a trend of transition from the use of biometric recognition technologies in traditional state security systems to the sphere of commercial and user applications. The process of «linking» encryption keys and passwords with the biometric parameters of the data subject is described. It is proposed that a biometric feature and a biometrics parameter mean a certain value that has a physical meaning that characterizes the subject itself. The possibility of using circular neighborhood and bilinear interpolation of pixel intensity values in biometrics is also presented. This will make it possible to build a local binary template. In order to solve the problem of identification of persons, it is advisable to investigate the essence of biometric systems in the technologies of identification of persons, their types, identifying the shortcomings of each of them, on the basis of which to present the directions of elimination and search for the most reliable technologies. The essence of the use of biometric systems in the technologies of identification of persons is, for example, that the user can provide the bank or other counterparty with evidence that it is he who wants to use the services on his accounts. At the same time, the demand has increased for contactless biometric solutions. These technologies are implemented in order to conduct additional biometric verification of users. This allows to minimize possible fraud or violation of the internal rules of the service, for example, the transfer of accounts of some registered users to others.

Keywords: biometrics, parameters, features, biometrics-code converter, key, recognition

• **Submitted:** 04.12.2020 • **Revised:** 21.03.2021 • **Accepted:** 01.04.2021

For citation: Kulikov A.A. Application of biometric systems in face identification technologies. *Rossiiskii tekhnologicheskii zhurnal = Russian Technological Journal*. 2021;9(3):7–14 (in Russ.). https://doi.org/10.32362/2500-316X-2021-9-3-7-14

Financial disclosure: Author has no a financial or property interest in any material or method mentioned.

The author declares no conflicts of interest.

ВВЕДЕНИЕ

Технология распознавания лиц в условиях цифровой революции стала актуальной для множества отраслей и сфер жизнедеятельности. В связи с этим в последние годы многими российскими разработчиками и учеными из других стран проводились эксперименты в части использования биометрических технологий. Ряд из них можно назвать удачными, другие провалились. Однако все большую популярность получают технологии, строящиеся на использовании биометрических данных человека. В тоже время стоит отметить непроработанность ряда таких технологий, что влечет за собой снижение эффективности идентификации лиц и сбои в выполнении функций, возложенных на соответствующее оборудование.

Для того, чтобы решить указанную проблему, целесообразно провести исследование биометрических систем в технологиях идентификации лиц, их видов, определив недостатки каждого из них, на основании чего представить направления решения проблем и поиска наиболее надежных технологий.

БИОМЕТРИЧЕСКИЕ СИСТЕМЫ В ТЕХНОЛОГИЯХ ИДЕНТИФИКАЦИИ ЛИЦ

На текущий момент аутентификация по биометрическим данным является настоящим прорывом в технологиях. Суть применения биометрических

систем в технологиях идентификации лиц состоит в том, что пользователь, например, может предоставить банку или другому контрагенту доказательства того, что именно он хочет воспользоваться услугами по своим счетам; биометрические системы служат для поиска преступников, применяются для доступа к служебным объектам (пример: доступ на военную базу). При этом значительно увеличился спрос на бесконтактные биометрические решения [1].

Каждая такая технология, по сути, является независимой, выполняющей задачи биометрической идентификации (распознавания лица или образа) на локальном уровне. Специфика любого подобного решения состоит в том, что они интегрируются в системы безопасности предприятий. Однако зачастую при применении подобного решения, возникает ряд сложностей. Примером может послужить невозможность передачи запроса на получение статистики из аппаратного биометрического решения [2].

Данные технологии внедряются с целью проведения дополнительной биометрической проверки пользователей, которая позволяет минимизировать возможное мошенничество или нарушение внутренних правил сервиса, например, передачу аккаунтов одних зарегистрированных пользователей системы другим лицам (злоумышленникам). Идентификация может применяться для ретроспективного поиска в архиве видеозаписей, например, при расследовании инцидентов или при обнаружении VIP-персон/постоянных клиентов на объектах ритейла [3].

Помимо верификации при физическом контроле доступа, распознавание лиц успешно заменяет пароли и ПИН-коды в задачах подтверждения платежных операций или при входе в аккаунт.

Изучение рынка таких систем позволяет сделать вывод о том, что все подобные технологии разделяются на две группы:

1. Работающие на базе одной системы;
2. Мультимодульные решения.

Распознавание лиц можно комбинировать с распознаванием отпечатков пальцев или любой другой биометрической технологией, но такое решение будет стоить дороже и не всегда оправданно.

Обобщенная классификация биометрических систем представлена на рис. 1.

Рис. 1 показывает, что в биометрии могут быть задействованы фактически все функциональные особенности человека. Большая часть современных биометрических моделей строится на использовании модальных технологий, совмещающих в себе несколько приведенных выше типов. Примером является использование «слепка» лица с разных ракурсов и отпечатков пальцев. В то же время наиболее популярными на современном этапе видом биометрической аутентификации являются технологии на основе распознавания голоса [4]. Спрос на биометрию в системе распознавания лиц повышается все более активно, поскольку усиливается потребность в безопасных механизмах идентификации. Это прослеживается фактически во всех отраслях экономики, что связано с нарастанием возможностей распознавания лиц.

При этом стоит отметить, что с одновременным развитием цифровых и бесконтактных систем имеет место и развитие биометрических технологий. Особенно ярко это проявилось в 2020 году, когда биометрические технологии распознавания, применяемые в большей степени в системах государственной безопасности, постепенно стали интегрироваться в сферу коммерческого и пользовательского применения. Ключевыми сегментами коммерческого использования биометрических технологий стали сферы финансов, туризма, медицины и др. Более подробная информация по отраслям, использующим биометрию в обеспечении безопасности своих бизнес-процессов, приведена в таблице 1.

Таблица 1. Ключевые отрасли, использовавшие биометрию в обеспечении безопасности своих бизнес-процессов в 2020 году

Сектор	Сфера, где используются	Примеры решений
Государственный сектор	Регистрация электронных данных населения в документах. Документы, содержащие биометрические данные	Электронные паспорта, электронные водительские удостоверения, бесконтактное получение государственных услуг через личный кабинет в «Госуслуги»
Туризм, перелеты и миграция	Предоставление иностранных виз с помощью дистанционных технологий, приобретение билетов на авиа- и ж/д транспорт	Все биометрические системы, используемые на объектах транспортной инфраструктуры и в иммиграционном контроле
Банки и кредитно-финансовые организации	Работа платежных систем и страхование, идентификация лиц для получения финансовых услуг	Работа с онлайн-банками
Здравоохранение	Государственный и частный сектор (государственные и частные больницы)	Электронные медицинские карты, электронные больничные листы
Ритейл	Системы мониторинга покупателей	Оценка лица покупателя при выходе из магазина (удовлетворен покупками или нет)

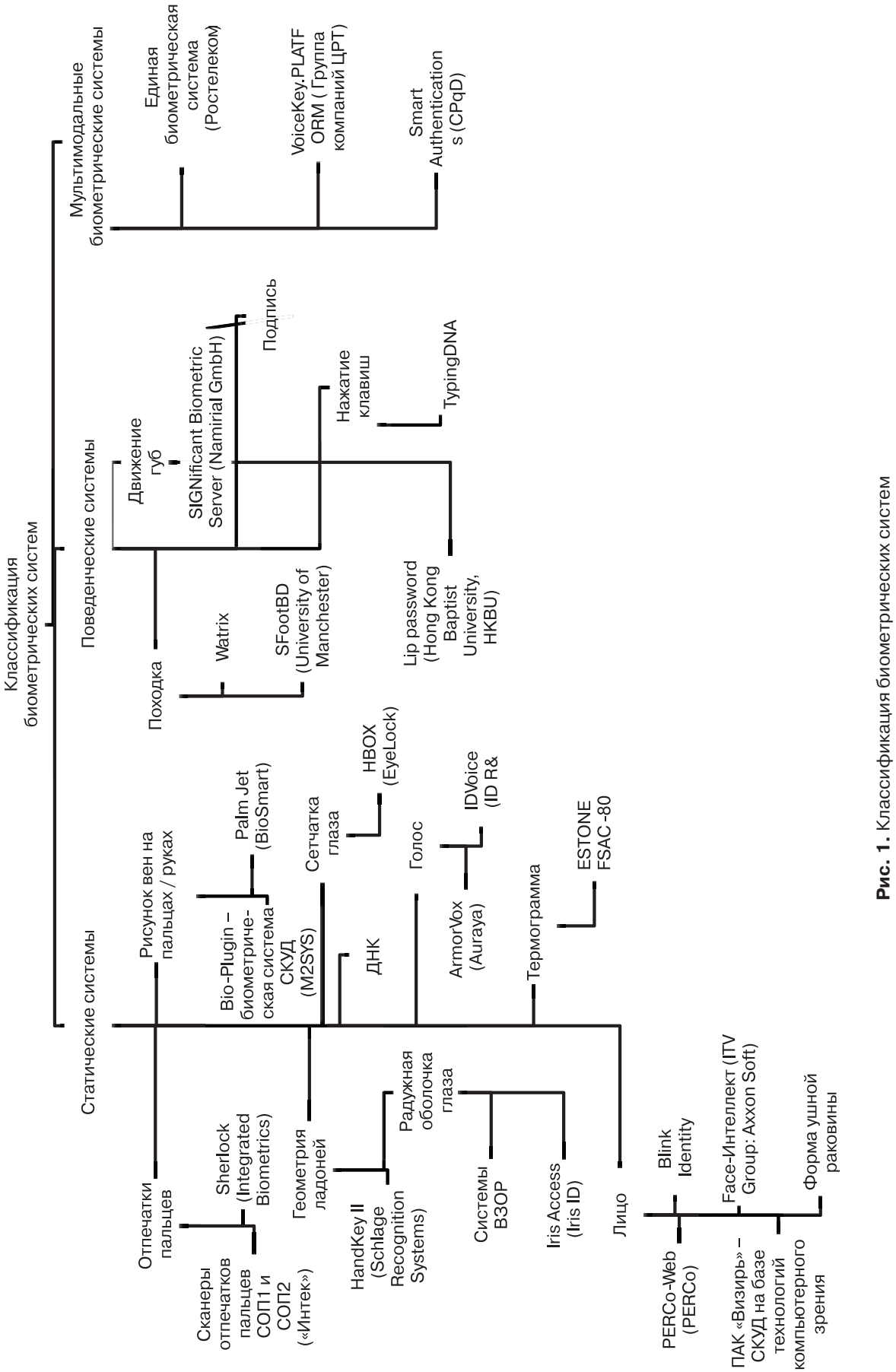

Рис. 1. Классификация биометрических систем

В целом можно сделать вывод, что биометрические системы используются практически во всех отраслях и сферах современного государства. Это доказывает и график (рис. 2), где приведены данные по динамике объема рынка биометрических технологий и его сегментов.

Биометрические технологии проникают практически во все сегменты рынка, постепенно наращивая свое участие в каждом из них. Так, если биометрические системы в банкоматах в 2016 году вообще не использовались, то в 2019 году они уже начали активно применяться в данном сегменте, а в 2021 году прогнозируется увеличение объема данных технологий до 1.5 млн долл. [5]. В 2020 году биометрические технологии преобладали в аутентификации в корпоративных ИТ-системах и государственной сфере.

Развитие спроса на биометрические технологии повлияло на рост числа их разработчиков. Крупнейшей в мире системой биометрической идентификации к концу 2019 года стала запущенная в Индии система «Aadhaar», в которой было зарегистрировано более 1.19 млрд человек [6].

Основными требованиями к таким системам у пользователей является их надежность, скорость работы и возможность быстрой интеграции аппаратной и программной частей в общую платформу. Для того чтобы понимать, какая именно система подходит пользователю, проводится их детальный анализ. Здесь стоит пояснить, что в основе системы находится преобразователь «биометрия – код» (ПБК), являющийся ключевым понятием, относящимся к «связыванию» ключей шифрования и паролей с биометрическими параметрами субъекта данных и нацеленный на преобразование вектора нечетких, неоднозначных биометрических параметров «свой» в четкий однозначный код ключа (пароля).

В России введена серия стандартов ГОСТ Р 52633, которые определяют требования к проведению процедур обработки биометрической информации и нечетких биометрических образов субъекта данных. В соответствии с этим ГОСТ, получаемая информация в области биометрии человека преобразуется в его длинный пароль либо ключ, используемый в дальнейшей аутентификации пользователя [7].

Стоит отметить, что термины «биометрический» или «биометрический образ», определенные ГОСТ Р 52633, соответственно, означают какой-то единичный образец биометрических данных и их совокупность. Однако понятие биометрического параметра зачастую путается с понятием признака, являющегося идентичным с позиции байесовской классификации. Поэтому на наш взгляд под биометрическим признаком и параметром биометрии стоит подразумевать некоторую величину, которая характеризует сам субъект. При этом, если генерируется ключ, который в той или иной степени отличается от составленного для субъекта, имеет место ошибка 1-го рода, а ошибка 2-го рода может возникнуть, если ключ, полученный из биометрических данных субъекта, в метрике расстояний по параметрам оценивания близок к ключу другого субъекта настолько, что может быть принят за чужой ключ. Здесь, по нашему мнению, более правильно использовать расширенный оператор локального бинарного шаблона (ЛБШ). Использование круговой окрестности и билинейной интерполяции значений интенсивностей пикселей (pixel – наименьший логический элемент двумерного цифрового изображения) дает возможность построить локальный бинарный шаблон с произвольным набором точек P и радиусом R. Примеры такого изображения (двумерного) представлены на рис. 3.

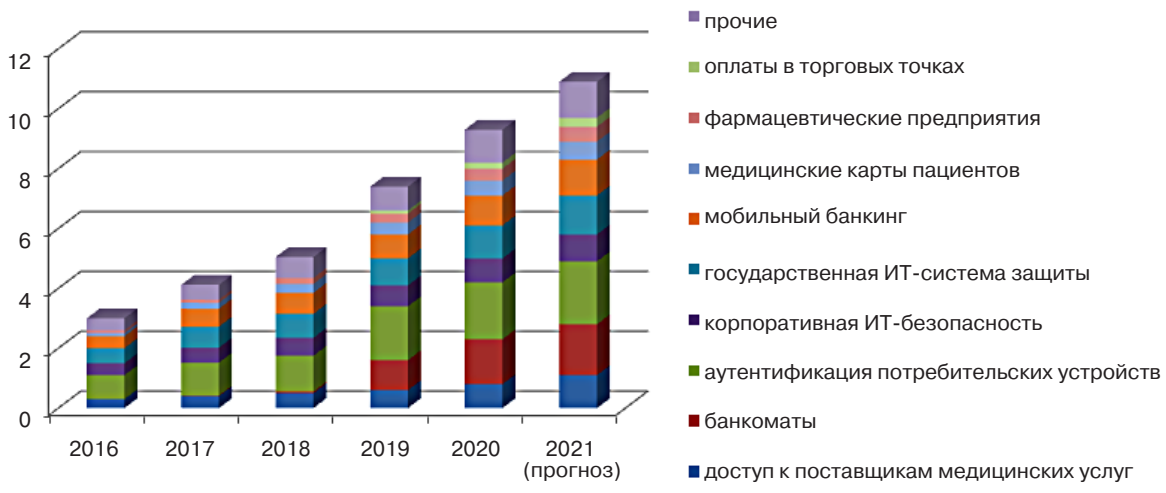

Рис. 2. Динамика объема рынка биометрических технологий и его сегментов, млн долл. [4]

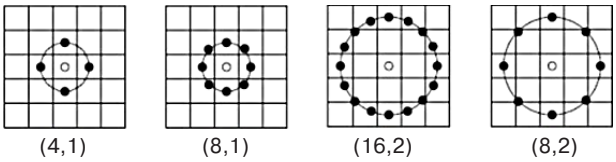

Рис. 3. Расширенное описание набора точек *P* и радиус *R*

Необходимо учитывать, что в классификации важную роль играет равномерность ЛБШ. В их состав целесообразно включать шаблоны, содержащие не более трех серий «0» и «1», которые представлены в таблице 3. Величины «0» и «1» представлены в виде единиц измерения (битов).

Таблица 3. Пример равномерных и неравномерных ЛБШ

ЛБШ	Количество серий	Равномерный
11111111	1	Да
00001111	2	Да
01110000	3	Да
11001110	4	Нет
11001001	5	Нет

Поскольку показанные ЛБШ кодируют концы линий, углы, пятна и другие особенности цифрового изображения в целом, они позволяют довольно ощутимо экономить память, т.к. хранят информацию в виде последовательностей «0» и «1».

Зная значения ЛБШ для каждого пикселя изображения, можно разработать гистограмму, в которой каждому равномерному шаблону будет соответствовать столбец, а также дополнительный столбец, который содержит информацию по всем неравномерным шаблонам.

Для более эффективного описания изображения лица его можно разбить на области и далее для каждой построить гистограмму. Принимая во внимание, что изображение может состоять из *m* регионов, гистограмму надо определить для каждого региона. Пример изображения для общего количества регионов 7 × 7 (можно разбить изображение на большее количество частей) приведен на рис. 4.

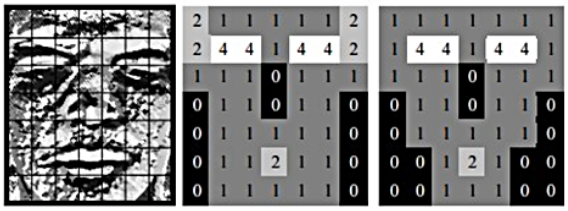

Рис. 4. Пример изображения лица и веса его регионов

Затем полученные гистограммы объединяются в одну, что позволит получить информацию не только о наличии тех или иных локальных особенностей, но и о месте их расположения на изображении.

В результате получим вектор размерностью 2891 (всего 7 × 7 регионов и для каждого вычислена гистограмма 59 bin), который и будет описывать ключевые особенности изображение лица (рис. 5).

Рис. 5. Пример изображения лица с вычисленными шаблонами

Таким образом, при интеграции расширенного оператора локального бинарного шаблона логика будет частично изменена. Если в базе зарегистрирована одна персона, то вероятность ее идентификации достигает максимального значения при приемлемом значении вероятности ложноположительной идентификации (ВЛПИ). В режиме верификации распознавание выполняется с большей точностью. В таблице 4 приведены количественные характеристики точности алгоритма распознавания лиц.

Таблица 4. Точность распознавания при разных значениях ВЛПИ и объема базы зарегистрированных лиц *N*

ВЛПИ	*N* = 1 (верификация)	*N* = 15 (идентификация)
0	80%	82%
0.02	99%	82%

Из приведенных значений следует, что режим верификации выполняет распознавание с большей точностью, чем режим идентификации, т.к. проверяется истинность значений, а не само изображение.

ЗАКЛЮЧЕНИЕ

Таким образом, применение биометрических систем распознавания в технологии идентификации лиц позволит предоставить санкционированный доступ к различным служебным, секретным объектам, осуществлять поиск преступных лиц в общественных местах и т.д.

Проведение дополнительных исследований, направленных на выявление более совершенных методов компенсации изменения освещенности в полученных изображениях лиц, а также методов классификации, позволит повысить надежность алгоритма и применять программные решения на его основе в более широкой области.

СПИСОК ЛИТЕРАТУРЫ

1. Гришина Е.А. Биометрические технологии в российских банках: мечты или реальность. *Наука и общество*. 2015;3:17–21.
2. Ворона В.А., Костенко В.О. Биометрические технологии идентификации в системах контроля и управления доступом. *Computational nanotechnology*. 2016;3:224–241.
3. Глобальное исследование «Доверие к цифровым технологиям». 2021. URL: https://www.pwc.ru/ru/publications/dti-2021/e-version-digital-trust-insights-2021-in-russian.pdf
4. Tractica: Объем рынка биометрии к 2025 году достигнет $15 млрд. URL: https://iot.ru/promyshlennost/tractica-obem-rynka-biometrii-k-2025-godu-dostignet-15-mlrd
5. Обзор международного рынка биометрических технологий и их применение в финансовом секторе. 2018, январь, Москва. URL: https://cbr.ru/Content/Document/File/36012/rev_bio.pdf
6. Куприяновский В.П., Сотников А.Е., Соловьев А.И., Дрожжинов В.И., Намиот Д.Е., Мамаев В.Ю., Куприяновский П.В. Aadhaar – идентификация человека в цифровой экономике. *International Journal of Open Information Technologies*. 2017;5(2):34–45.
7. Куликов А.А. Разработка системы автоматической идентификации изображения лица персоны по видеоизображению. *Глобальный научный потенциал*. 2013;3(24):75–79.
8. Куликов А.А. Модель репринта объекта на изображении. *Российский технологический журнал.* 2020;8(3):7–13. https://doi.org/10.32362/2500-316X-2020-8-3-7-13
9. *Защита информации. Техника защиты информации. Требования к средствам высоконадежной биометрической аутентификации.* ГОСТ Р 52633.0-2006. М.: Стандартинформ; 2007.
10. Alghaili M., Li Z., Ali H.A.R. Facefilter: face identification with deep learning and filter algorithm. *Scientific Programming*. 2020;2020: Article ID 7846264. https://doi.org/10.1155/2020/7846264
11. Чесалин А.Н., Гродзенский С.Я., Нилов М.Ю., Агафонов А.Н. Модификация алгоритма WaldBoost для повышения эффективности решения задач распознавания образов в реальном времени. *Российский технологический журнал*. 2019;7(5):20–29. https://doi.org/10.32362/2500-316X-2019-7-5-20-29
12. Кононыхин И.А., Ежов Ф.В., Мартынюк Р.А., Мищенко А.Д., Можайский Г.В. Реализация системы распознавания и отслеживания лиц. *Молодой ученый*. 2020;28(318):8–12.
13. Балдин А.В., Елисеев Д.В. Алгебра многомерных матриц для обработки адаптируемой модели данных. *Наука и образование*. 2010;7:1–11. URL: http://technomag.edu.ru/doc/199561.html
14. Самаль Д.И., Фролов И.И. Алгоритм подготовки обучающей выборки с использованием 3d-моделирования лиц. *Системный анализ и прикладная информатика*. 2016;4:17–23.
15. Романенко А.О., Юфряков А.В. Оценка размытия изображения для биометрической идентификации. *Наука и образование сегодня*. 2018;7(30):16–19.

REFERENCES

1. Grishina E.A. Biometric technologies in Russian banks: dreams or reality. *Nauka i obshchestvo*. 2015;3:17–21 (in Russ.).
2. Vorona V.A., Kostenko V.O. Biometric identification technologies in access control and management systems. *Computational Nanotechnologies*. 2016;3:224–241 (in Russ.).
3. Global'noe issledovanie «Doverie k tsifrovym tekhnologiyam» (Global research «Trust in Digital Technologies»). 2021. Available from URL: https://www.pwc.ru/ru/publications/dti-2021/e-version-digital-trust-insights-2021-in-russian.pdf
4. Tractica: Ob''em rynka biometrii k 2025 godu dostignet $15 mlrd. (Tractica: The biometrics market will reach $ 15 billion by 2025). Available from URL: https://iot.ru/promyshlennost/tractica-obem-rynka-biometrii-k-2025-godu-dostignet-15-mlrd
5. Obzor mezhdunarodnogo rynka biometricheskikh tekhnologii i ikh primenenie v finansovom sektore. 2018, yanvar', Moskva. (Review of the international market of biometric technologies and their application in the financial sector. January 2018. Moscow. Available from URL: https://cbr.ru/Content/Document/File/36012/rev_bio.pdf
6. Kupriyanovskii V.P., Sotnikov A.E., Solov'ev A.I., Drozhzhinov V.I., Namiot D.E., Mamaev V.Yu., Kupriyanovskii P.V. Aadhaar – identification of a person in the digital economy. *International Journal of Open Information Technologies*. 2017;5(2):34–45 (in Russ.).
7. Kulikov A.A. Development of a system for automatic identification of the image of a person's face by video image. *Global'nyi nauchnyi potentsial = Global Scientific Potential.* 2013;3(24):75–79 (in Russ.).
8. Kulikov A.A. The model is a reprint of an object in the image. *Rossiiskii tekhnologicheskii zhurnal = Russian Technological Journal*. 2020;8(3):7–13 (in Russ.). https://doi.org/10.32362/2500-316X-2020-8-3-7-13
9. *Zashchita informatsii. Tekhnika zashchity informatsii. Trebovaniya k sredstvam vysokonadezhnoi biometricheskoi autentifikatsii. GOST R* 52633.0-2006. (*Information Security. Information security techniques. Requirements for highly reliable biometric authentication tools. GOST R* 52633.0-2006). (in Russ.).
10. Alghaili M., Li Z., Ali H.A.R. Facefilter: face identification with deep learning and filter algorithm. *Scientific Programming*. 2020;2020: Article ID 7846264. https://doi.org/10.1155/2020/7846264
11. Chesalin A.N., Grodzenskiy S.Y., Nilov M.Yu., Agafonov A.N. Modification of the WaldBoost algorithm to improve the efficiency of solving pattern recognition problems in real-time. *Rossiiskii tekhnologicheskii zhurnal = Russian Technological Journal*. 2019;7(5):20–29 (in Russ.). https://doi.org/10.32362/2500-316X-2019-7-5-20-29
12. Kononykhin I.A., Ezhov F.V., Martynyuk R.A., Mishchenko A.D., Mozhaiskii G.V. *Molodoi uchenyi = Young Scientist*. 2020;28(318):8–12 (in Russ.).
13. Baldin A.V., Eliseev D.V. Algebra of multidimensional matrices for processing an adaptable data model. *Nauka i obrazovanie = Science and Education of Bauman MSTU*. 2010;7:1–11 (in Russ.). Available from URL: http://technomag.edu.ru/doc/199561.html

16. Завалов Р.А., Гараев Р.А. Реализация алгоритма Виолы–Джонса на микроконтроллере с ограниченными ресурсами. *Наука и образование сегодня*. 2018;6(29):20–26.
17. Korotkov A. Database index for approximate string matching. In: *Proceedings of the 4th Spring/Summer Young Researchers' Colloquium on Software Engineering. SYRCoSE*'10. 2010. p. 136–140. https://doi.org/10.15514/SYRCOSE-2010-4-27
18. Etemad K., Chellappa R. Discriminant analysis for recognition of human face images. *Journal of the Optical Society of America A*. 1997;14(8):1724–1733. https://doi.org/10.1364/JOSAA.14.001724

14. Samal' D.I., Frolov I.I. Algorithm of training sample preparation using 3D face modeling. *Sistemnyi analiz i prikladnaya informatika = System analysis and applied informatics*. 2016;4:17–23 (in Russ.).
15. Romanenko A.O., Yufryakov A.V. Evaluation of image blurring for biometric identification. *Nauka i obrazovanie segodnya*. 2018;7(30):16–19 (in Russ.).
16. Zavalov R.A., Garaev R.A. Implementation of the Viola–Jones algorithm on a microcontroller with limited resources. *Nauka i obrazovanie segodnya*. 2018;6(29):20–26 (in Russ.).
17. Korotkov A. Database index for approximate string matching. In: *Proceedings of the 4th Spring/Summer Young Researchers' Colloquium on Software Engineering. SYRCoSE*'10. 2010. p. 136–140. https://doi.org/10.15514/SYRCOSE-2010-4-27
18. Etemad K., Chellappa R. Discriminant analysis for recognition of human face images. *Journal of the optical society of America A*. 1997;14(8):1724–1733. https://doi.org/10.1364/JOSAA.14.001724

Об авторе

Куликов Александр Анатольевич, к.т.н., доцент, доцент кафедры инструментального и прикладного программного обеспечения Института информационных технологий ФГБОУ ВО «МИРЭА – Российский технологический университет» (119454, Россия, Москва, пр-т Вернадского, д. 78). E-mail: tibult41@gmail.com. https://orcid.org/0000-0002-8443-3684

About the author

Alexander A. Kulikov, Cand. Sci. (Eng.), Associate Professor, Department of Instrumental and Applied Software, Institute of Information Technologies, MIREA – Russian Technological University (78, Vernadskogo pr., Moscow, 119454 Russia). E-mail: tibult41@gmail.com. https://orcid.org/0000-0002-8443-3684