DOI: 10.18137/RNU.V9187.24.02.P.123 УДК 004.75:004.27

З.У. Меджидов, З.Х. Ахмедова

ИСПОЛЬЗОВАНИЕ ТЕХНОЛОГИИ СИСТЕМЫ РАСПОЗНАВАНИЯ ЛИЦ В ОБЕСПЕЧЕНИИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ

Аннотация. Статья посвящена изучению теоретической и эмпирической базы исследования, а также проектированию будущей системы распознавания лиц. Цель работы – раскрыть особенности систем распознавания лиц в части определения их преимуществ и недостатков с позиции информационной безопасности, а также выполнить программную реализацию системы распознавания лиц на базе технологии нейронных сетей. К результатам работы следует отнести систематизацию сведений в части применения систем распознавания лиц в различных видах деятельности (здравоохранение, розничная торговля, образование, банковский и финансовый секторы). Обобщены основные преимущества систем распознавания лиц: идентификация преступников, отслеживание посещаемости в образовательных учреждениях, транспортная безопасность, а также их недостатки: угроза частной жизни личности и общества, возможности для мошенничества и других преступлений. Предложена схема процедуры моделирования лица, а также логическая модель данных разрабатываемого программного продукта. Следует отметить, что системы распознавания лиц несовершенны и требуют дальнейшей доработки, в том числе устранения законодательных пробелов при их эксплуатации.

Ключевые слова: информационная безопасность, система распознавания лиц, идентификация, нейронные сети.

Z.U. Medzhidov, Z.H. Akhmedova

FACE RECOGNITION SYSTEM AS A MODERN WAY TO ENSURING INFORMATION SECURITY

Abstract. The article focuses on the theoretical and empirical basis of the study, as well as the design of a future face recognition system. The purpose of the work is to reveal the features of face recognition systems in terms of determining their advantages and disadvantages from the position of information security, as well as to perform a software implementation of a face recognition system based on neural network technology. The results of the work include the systematization of information regarding the use of facial recognition systems in various types of activities (health care, retail trade, education, banking and financial sectors). The article summarizes the main advantages of facial recognition systems (identification of criminals, tracking attendance in educational institutions, transport security), as well as their disadvantages (threat to the privacy of individual and society, opportunities for fraud and other crimes. The article proposes a diagram of the facial modeling procedure, as well as a logical data model of the software product under development. It should be noted that facial recognition systems are not perfect and require further improvement, including eliminating legislative gaps in their operation.

Keywords: information security, face recognition system, identification, neural networks.

Введение

Системы распознавания лиц развивались с 60-х годов XX века. Неоднократно осуществлялись попытки автоматически идентифицировать человека по фотографии, базе данных, видео- или цифровому изображению. Большинство из них имели недостатки и

Меджидов Заур Уруджалиевич
кандидат экономических наук, доцент кафедры информационных технологий и информационной безопасности. Дагестанский государственный университет народного хозяйства, город Махачкала. Сфера научных интересов: информационная безопасность, защита информации, кибербезопасность, киберугрозы. Автор более 80 опубликованных научных работ. SPIN-код: 3038-3448, AuthorID: 776269.
Электронный адрес: zaur-medzhidov@mail.ru

Ахмедова Зухра Халипаевна
кандидат физико-математических наук, доцент, заведующий кафедрой информационных технологий и безопасности компьютерных систем. Дагестанский государственный университет, город Махачкала. Сфера научных интересов: информационная безопасность, защита информации, кибербезопасность, киберугрозы. Автор более 40 опубликованных научных работ. SPIN-код: 4305-3419, AuthorID: 264733.
Электронный адрес: zuhra2473@mail.ru

могли оказаться неэффективными, если полный обзор лица был отклонен на 20 градусов, или при других обстоятельствах. Сегодня распознавание лиц как система безопасности перешло в идентификацию в режиме реального времени, которой не мешают условия освещения, угол наклона лица или движения тела.

Значение термина «распознавание лиц» интуитивно понятно. Технология использует алгоритмы компьютерного зрения для отображения, анализа и подтверждения личности лица на фотографии или видео. Хотя решения для распознавания лиц, которые часто основываются на собственных алгоритмах, работают по-разному, процесс распознавания лиц можно разделить на три этапа.

1. Обнаружение относится к процессу определения местоположения лица на входном изображении. Таким образом, каждое лицо помещается в ограничивающую рамку. Для завершения этого этапа алгоритмы распознавания лиц сначала обучаются узнавать, как выглядит лицо, из различных вводимых данных.

2. Анализ заключается в отображении черт каждого лица. Это делается путем измерения расстояния между глазами, носом и ртом, а также путем определения формы подбородка.

3. Затем эти расстояния объединяются и преобразуются в уникальный набор чисел – так называемый отпечаток лица.

Системе распознавания лиц как современному способу обеспечения информационной безопасности посвящены исследования [1–8].

Распознавание относится к фактическому определению личности человека по вводимой фотографии. В некоторых приложениях этот этап заменен категоризацией. В таких случаях алгоритмы не подтверждают личность человека, а помечают его как принадлежащего к одной из определенных групп, например, по полу или возрасту.

Применение систем распознавания в секторе здравоохранения

Рассмотрим применение систем распознавания лиц на примере здравоохранения.

Идентификация пациентов. При включении в систему видеонаблюдения больницы распознавание лиц может упростить регистрацию пациентов, освобождая работников

больницы и пациентов от бумажной волокиты и предотвращая человеческие ошибки. «Глядя» на пациента, система распознавания лиц может подтвердить его личность и данные страховки, тем самым ускоряя процесс госпитализации, закладывая основу для персонализированного обслуживания и предотвращая мошенничество [9; 10].

Биометрические технологии, включая распознавание лиц, также могут использоваться для проверки личности хирургических пациентов, идентификации пациентов, находящихся без сопровождения медицинского работника, и отслеживания людей, входящих и выходящих из помещений, для предотвращения угроз безопасности.

Диагностика генетических нарушений. Распознавание лиц может помочь диагностировать редкие генетические нарушения, особенно с легкими симптомами.

Приложение сканирует фотографию пациента, сопоставляя его лицо со 130 ориентирами, и использует машинное обучение для сопоставления обнаруженных характеристик лица с характеристиками редких генетических заболеваний. В результате приложение генерирует список потенциальных диагнозов, каждому из которых присваивается оценка вероятности [11–13].

Применение систем распознавания в секторе образования

Безопасность кампуса. Система распознавания лиц анализирует лица людей, входящих в кампус или перемещающихся по нему, и сравнивает их с базой данных авторизованных лиц, включая учащихся, текущий персонал школы и родителей, для установления их личности. Если человек отсутствует в базе данных или совпадает с личностью нежелательного лица, например, отчисленного студента или бывшего сотрудника, система немедленно оповещает службу безопасности и автоматически отказывает посетителю во входе на территорию кампуса. Современные решения для распознавания лиц могут иметь дополнительные функции, такие как распознавание объектов, позволяющие идентифицировать объекты в форме пистолета.

Мониторинг посещаемости. Отслеживание посещаемости раньше было длительным и утомительным процессом, который, несмотря на значительное количество времени, затрачиваемого в начале каждого занятия, приводит к неизбежным пробелам и пропускам при проведении вручную. Чтобы исправить это, преподаватели обращаются к образовательным решениям на базе искусственного интеллекта [14]. Эти приложения для распознавания лиц предлагают более быстрый и не вызывающий сбоев способ отслеживания посещаемости.

Применение систем распознавания в банковском и финансовом секторе

Верификация клиента. Поскольку финансовые услуги становятся цифровыми, вполне естественно следовать процедурам верификации клиентов. Опираясь на eKYC – цифровую версию стандарта «знай своего клиента», который регулирует проверку и аутентификацию данных клиента, финансовые учреждения могут полностью перевести процесс адаптации клиентов в онлайн-режим, особенно с учетом исследований, показывающих, что трое из четырех клиентов банка принимают биометрическую аутентификацию [15].

Операции в банкоматах без использования карт. Сегодня преступники регулярно используют скимминговые устройства для взлома банкоматов. Распознавание лиц потенциально может заменить пластиковые карты и PIN-коды в качестве более безопасного способа предотвращения мошенничества.

Преимущества системы распознавания лиц с позиции информационной безопасности

Решение для распознавания лиц является одним из основных компонентов в области информационной безопасности. Наиболее перспективными направлениями применения систем распознавания лиц являются:

- идентификация преступников;
- видеонаблюдение;
- деятельность правоохранительных органов;
- отслеживание посещаемости в учебных заведениях;
- оборонные услуги;
- банковские услуги;
- онлайн-платежи;
- обслуживание в аэропортах.

Минусы системы распознавания лиц

Как и у любой технологии, у использования функции распознавания лиц есть недостатки, представленные ниже.

Создает большую угрозу частной жизни личности и общества. Угроза технологического вторжения в права человека на неприкосновенность частной жизни, пожалуй, является самой большой угрозой, создаваемой широким использованием технологии распознавания лиц. При массовом использовании распознавания лиц потенциальной угрозе подвергается не только личная неприкосновенность – простой акт записи или сканирования с помощью технологии может отбить у людей охоту свободно передвигаться по своему району или городу.

Создает уязвимости в данных. Распознавание лиц также создает проблемы с защитой данных и кибербезопасностью. Собираемый и хранимый большой объем личной информации является привлекательной мишенью для киберпреступников, и уже есть примеры того, как хакеры получали доступ к таким системам [16].

Открывает возможности для мошенничества и других преступлений. Нарушители закона могут использовать технологию распознавания лиц и для совершения преступлений против невинных жертв. Они могут собирать личную информацию людей, включая изображения и видео, полученные при сканировании лиц и сохраненные в базах данных, для совершения мошенничества с личными данными.

Технология несовершенна, ее можно обмануть. Технология распознавания лиц далека от совершенства, и на нее нельзя полагаться при получении точных результатов вместо суждений человека.

Невиновным людям могут быть предъявлены обвинения. Из-за несовершенства системы распознавания лиц ложноположительные результаты сопряжены с неизбежной опасностью. Программное обеспечение для распознавания лиц может неверно идентифицировать кого-либо как преступника, что приведет к его аресту или иным образом нанесет ущерб его репутации, если его включат, например, в список магазинных воров.

Реализация системы распознавания лиц на базе технологии нейронных сетей

Распознавание лиц идентифицирует людей на изображениях лиц или видеокадрах. То есть система распознавания лиц извлекает особенности из входного изображения лица и сравнивает их с особенностями помеченных лиц в базе данных. Сравнение основано на метрике сходства объектов, а метка наиболее похожей записи в базе данных используется для

обозначения входного изображения. Если значение сходства ниже определенного порога, входное изображение помечается как неизвестное. Сравнение двух изображений лиц, чтобы определить, изображен ли на них один и тот же человек, называется проверкой лица.

Основной задачей алгоритма моделирования портрета человека с помощью нейронной сети является применение нейронной сети. Рассмотрим в связи с этим процедуру моделирования лица. Блок-схема представлена на Рисунке 1.

Рисунок 1. Блок-схема процедуры моделирования лица
Источник: схема составлена авторами.

Следующим этапом будет постановка задачи разработки логической модели будущего программного продукта. На Рисунке 2 представлена логическая модель разрабатываемой программы.

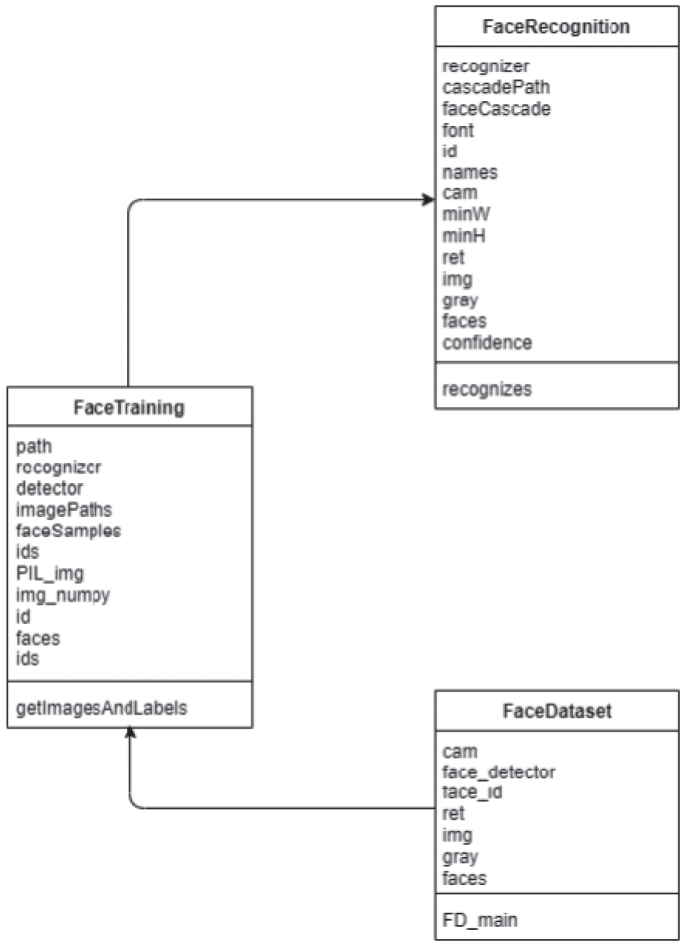

Рисунок 2. Логическая модель данных разрабатываемого программного продукта
Источник: модель составлена авторами.

Заключение

Независимо от того, к какой сфере деятельности мы относимся, на рынке присутствуют интересные приложения для распознавания лиц, которые могли бы быть апробированы в индивидуальном порядке. Несмотря на то, что технология развивается и становится все более доступной, законодательные пробелы по-прежнему ограничивают ее многообещающий потенциал.

Дальнейшее развитие исследования видится как переход к выбору алгоритмов, которые будут использоваться при разработке программного продукта. За основу разрабатываемого алгоритма моделирования портрета человека будет взят OpenCV, метод Хаара и API face_recognition – самый популярный на данный момент API с открытым исходным кодом.

Признаки Хаара – это признаки цифрового изображения, которые используются в распознавании различных образов, например, образов человеческого тела или человеческого лица.

Предполагается реализация программного продукта с использованием языка программирования Python в качестве средства для разработки.

Литература

1. *Марьенков А.Н., Кузнецова В.Ю., Гелагаев Т.М.* Применение технологий распознавания лиц в системах контроля и управления доступом // Прикаспийский журнал: управление и высокие технологии. 2021. № 1 (53). С. 83–90. EDN MOEMFG. DOI: 10.21672/2074-1707.2021.53.1.083-090
2. *Горлов А.П., Лысов Д.А., Лысова К.М., Пестракова К.А.* Применение технологии распознавания лиц через камеру при аутентификации в системах контроля и управления доступом // Новые горизонты : Материалы VI Международной научно-практической конференции, посвященной 90-летию БГТУ. Брянск, 21 марта 2019 г. Брянск : Брянский государственный технический университет, 2019. С. 898–902. EDN SMWQJU.
3. *Кряжев А.С.* Исследование возможностей реализации модуля распознавания лиц для систем контроля и управления доступом // Фундаментальные и прикладные исследования молодых учёных : Сборник материалов IV Международной научно-практической конференции студентов, аспирантов и молодых учёных. Омск, 06–07 февраля 2020 г. Омск : Сибирский государственный автомобильно-дорожный университет, 2020. С. 356–360. EDN ANPTAW.
4. *Voronov V.I., Zharov I.A., Bykov A.D., Trunov A.S., Voronova L.I.* Designing a neural network identification subsystem in the hardware-software complex of face recognition // T-Comm. 2020. Vol. 14. No. 5. С. 69–76. EDN NUBENK. DOI: 10.36724/2072-8735-2020-14-5-69-76
5. *Антипова С.А.* Разработка системы контроля доступа на основе распознавания лиц // Программные продукты и системы. 2021. № 2. С. 245–256. EDN ATZEPM. DOI: 10.15827/0236-235X.134.245-256
6. *Сорокин Л.Е.* Информационно-аналитическая поддержка управления безопасностью в местах массового пребывания людей: автореф. дис. ... канд. техн. наук: 05.13.10. М., 2017. 21 с.
7. *Дорофеев К.А.* Сравнительный анализ уязвимостей биометрических систем распознавания лиц // Вестник УрФО. Безопасность в информационной сфере. 2022. № 3 (45). С. 34–46. EDN CSSKEK. DOI: 10.14529/secur220304
8. *Исхаков А.Ю.* Методическое и программно-алгоритмическое обеспечение процесса идентификации посетителей в местах массового пребывания людей : автореф. дис. ... канд. техн. наук : 05.13.19. Томск, 2016. 22 с.
9. *The PLOS ONE Staff (2021)* Correction: A survey of U.S. public perspectives on facial recognition technology and facial imaging data practices in health and research contexts. PLoS ONE. Vol. 16. No. 12. Art. ID e0261738. DOI: https://doi.org/10.1371/journal.pone.0261738 (дата обращения: 22.04.2024).
10. Facial Recognition in Healthcare: Unlocking Potential Medical Applications // Alchera. 2023. August 14. DOI: https://alchera.ai/en/meet-alchera/blog/facial-recognition-in-healthcare-unlocking-potential-medical-applications (дата обращения: 22.04.2024).
11. *Dolgin E.* AI face-scanning app spots signs of rare genetic disorders // Nature. 2019. January 07. DOI: https://doi.org/10.1038/d41586-019-00027-x
12. *Lavrentyeva E.* The big promise AI holds for mental health // Itrex Group. 2022. December 13. URL: https://itrexgroup.com/blog/ai-mental-health-examples-trends/ (дата обращения: 20.04.2024)
13. Machine learning solution for checkout-free shopping // Itrex. URL: https://itrexgroup.com/case-studies/machine-learning-solution-for-checkout-free-stores/#info (дата обращения: 24.04.2024).

14. AI solutions for education and corporate training // Itrex. URL: https://itrexgroup.com/services/ai-for-education/#header (дата обращения: 21.04.2024).
15. *Borak M.* Nearly 3 in 4 bank customers comfortable with biometric authentication: Entrust survey // Biometric update.com. 2023. November 10. URL: https://www.biometricupdate.com/202311/nearly-3-in-4-bank-customers-comfortable-with-biometric-authentication-entrust-survey (дата обращения: 23.04.2024).
16. *Hellard B.* Clearview AI client list hacked // ITPro. 2020. February 27. URL: https://www.itpro.com/security/data-breaches/354866/clearview-ai-client-list-hacked (дата обращения: 21.04.2024).

References

1. Maryenkov A.N., KuznetsovaV.Yu., Gelagaev T.M. (2021) Application of facial recognition technologies in access control and management systems. *Caspian Journal: Management and high technologies*. No. 1 (53). Pp. 83–90. (In Russian).
2. Gorlov A.P., Lysov D.A., Lysova K.M., Pestrakova K.A. (2019) Application of face recognition technology through a camera for authentication in access control and management systems. In: Golembiovskaya O.M. (Ed) *Novye gorizonty* [New Horizons] : Proceedings of the VI International Scientific and Practical Conference dedicated to the 90th anniversary of BSTU. Bryansk, March 21, 2019. Bryansk : Bryansk State Technical University Publ. Pp 898–902. (In Russian).
3. Kryazhev A.S. (2020) Research on the possibilities of implementing a face recognition module for access control and management systems. In: Zhigadlo A.P., Korchagin P.A. (Eds) *Fundamental'nye i prikladnye issledovaniya molodykh uchenykh* [Fundamental and applied research of young scientists] : Proceedings the IV International Scientific and Practical Conference of Students, Postgraduate Students and Young Scientists. Omsk, February 06-07, 2020. Omsk : Siberian State Automobile and Road University Publ. Pp. 356–360. (In Russian).
4. Voronov V.I., Zharov I.A., Bykov A.D., Trunov A.S., Voronova L.I. (2020) Designing a neural network identification subsystem in the hardware-software complex of face recognition. *T-Comm*. Vol. 14. No. 5. Pp. 69–76. DOI: 10.36724/2072-8735-2020-14-5-69-76
5. Antipova S.A. (2021) Development of an access control system based on face recognition. *Software and systems*. No. 2. Pp. 245–256. DOI: 10.15827/0236-235X.134.245-256 (In Russian).
6. Sorokin L.E. (2017) *Informatsionno-analiticheskaya podderzhka upravleniya bezopasnost'yu v mestakh massovogo prebyvaniya lyudei* [Information and analytical support for security management in crowded places] : PhD Thesis Extended Abstract (Technical sciences) : 05.13.10. Moscow. 21 p. (In Russian).
7. Dorofeev K.A. (2022) Comparative analysis of the vulnerabilities of biometric face recognition systems. *Journal of the Ural Federal District. Information security*. No. 3 (45). Pp. 34–46. DOI: 10.14529/secur220304 (In Russian).
8. Iskhakov A.Yu. (2016) *Metodicheskoe i programmno-algoritmicheskoe obespechenie protsessa identifikatsii posetitelei v mestakh massovogo prebyvaniya lyudei* [Methodological and software-algorithmic support for the process of identifying visitors in crowded places] : PhD Thesis Extended Abstract (Technical sciences) : 05.13.19. Tomsk. 22 p. (In Russian).
9. The PLOS ONE Staff (2021) Correction: A survey of U.S. public perspectives on facial recognition technology and facial imaging data practices in health and research contexts. PLoS ONE. Vol. 16. No. 12. Art. ID e0261738. DOI: https://doi.org/10.1371/journal.pone.0261738 (accessed 22.04.2024).
10. Facial Recognition in Healthcare: Unlocking Potential Medical Applications. *Alchera*. 2023. August 14. DOI: https://alchera.ai/en/meet-alchera/blog/facial-recognition-in-healthcare-unlocking-potential-medical-applications (accessed 22.04.2024).

11. Dolgin E. AI face-scanning app spots signs of rare genetic disorders. *Nature*. 2019. January 07. DOI: https://doi.org/10.1038/d41586-019-00027-x (accessed 21.04.2024).
12. Lavrentyeva E. (2022) The big promise AI holds for mental health. *Itrex.* December 13. URL: https://itrexgroup.com/blog/ai-mental-health-examples-trends/ (accessed 20.04.2024).
13. Machine learning solution for checkout-free shopping. *Itrex.* URL: https://itrexgroup.com/case-studies/machine-learning-solution-for-checkout-free-stores/#info (accessed 24.04.2024).
14. AI solutions for education and corporate training. URL: https://itrexgroup.com/services/ai-for-education/#header (accessed 25.04.2024).
15. Borak M. (2023) Nearly 3 in 4 bank customers comfortable with biometric authentication: Entrust survey. *Biometric update.com.* November 10. URL: https://www.biometricupdate.com/202311/nearly-3-in-4-bank-customers-comfortable-with-biometric-authentication-entrust-survey(accessed 23.04.2024).
16. Hellard B. (2020) Clearview AI client list hacked. *ITPro.* February 27. URL: https://www.itpro.com/security/data-breaches/354866/clearview-ai-client-list-hacked (accessed 21.04.2024).