УДК 004.932
DOI: 10.26102/2310-6018/2023.43.4.017

Аутентификация пользователей информационной системы по изображению лица

М.Б. Гузаиров, А.С. Исмагилова, Н.Д. Лушников✉

Уфимский университет науки и технологий, Уфа, Российская Федерация

Резюме. Аутентификация относится к классическим средствам управления информационной безопасностью компьютерных систем предприятия, от качества которой зависит безопасность информационной системы. В данной статье описана процедура аутентификации пользователей информационной системы по изображению лица. Разработана архитектура искусственной нейронной сети, сформированы наборы биометрических персональных данных и проведено обучение на основе распознавания пользователей информационной системы по изображению лица. В рамках данного исследования проведена оценка функциональности архитектуры искусственной нейронной сети на международных банках данных (Dataset). При распознавании пользователей информационной системы по изображению лица были извлечены такие дескрипторы, как локальные бинарные шаблоны (LBP) и гистограмма ориентированных градиентов (HOG). Скомпилирована модель обучения нейронной сети на основе категориальной кросс-энтропии, сформирована конфигурация компиляционной модели (размер мини-выборки, количество эпох, функция активации, функция оптимизации). Разработанный программный модуль производит аутентификацию пользователей информационной системы по принципу «свой-чужой». Применение данных дескрипторов изображения позволяет повысить точность распознавания пользователей информационной системы (accuracy) и снизить значение функции потерь (loss). Реализован программный код системы мультимодальной биометрической аутентификации. Для оценки эффективности работы программного модуля приведены показатели ошибок первого и второго рода.

Ключевые слова: аутентификация, биометрия, изображение лица, распознавание личности, информационная система.

Благодарности: исследование проводится при финансовой поддержке ФГБОУ ВО «Московский технический университет связи и информатики» (проект № 40469-20/2022-к) под руководством Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации.

Для цитирования: Гузаиров М.Б., Исмагилова А.С., Лушников Н.Д. Аутентификация пользователей информационной системы по изображению лица. *Моделирование, оптимизация и информационные технологии.* 2023;11(4). URL: https://moitvivt.ru/ru/journal/pdf?id=1465 DOI: 10.26102/2310-6018/2023.43.4.017

Authentication of information system users by facial image

M.B. Guzairov, A.S. Ismagilova, N.D. Lushnikov✉

Ufa University of Science and Technology, Ufa, the Russian Federation

Abstract. Authentication belongs to the classical means of information security management of enterprise computer systems, the quality of which determines the security of the information system. This paper describes the authentication procedure of information system users by facial image. The architecture of an artificial neural network has been developed, biometric personal data sets have been formed and trained based on the recognition of information system users by facial image. As part of this research, the functionality of the artificial neural network architecture has been evaluated using international data banks (Dataset). Descriptors such as Local Binary Patterns (LBP) and Histogram of

Oriented Gradients (HOG) were extracted when recognizing information system users by facial image. A neural network-training model based on categorical cross-entropy was compiled, and the configuration of the compilation model (mini-sample size, number of epochs, activation function, and optimization function) was generated. The developed software module authenticates users of the information system on “friend-or-for” basis. The use of these image descriptors allows increasing the accuracy of user authentication in the information system (accuracy) and reducing the value of loss function (loss). The program code of the multimodal biometric authentication system has been implemented. To assess the efficiency of the software module, the first and second type error rates are given.

Keywords: authentication, biometrics, facial image, identity recognition, information system.

Acknowledgements: the research was funded by the Federal State Budgetary Educational Institution of Higher Education “Moscow Technical University of Communications and Informatics” (project No. 40469-20/2022-k) under the supervision of the Ministry of Digital Development, Communications and Mass Media of the Russian Federation.

For citation: Guzairov M.B., Ismagilova A.S., Lushnikov N.D. Authentication of information system users by facial image. *Modeling, Optimization and Information Technology*. 2023;11(4). URL: https://moitvivt.ru/ru/journal/pdf?id=1465 DOI: 10.26102/2310-6018/2023.43.4.017 (In Russ.).

Введение

Безопасность информационных систем предприятий и обеспечение бесперебойности бизнес-процессов – одни из наиболее актуальных аспектов практически в любой сфере деятельности. Предлагаемые в настоящее время разработки в области информационной безопасности направлены на защиту информационных ресурсов от действий злоумышленников. К таким средствам относятся процессы идентификации и аутентификации с применением биометрических характеристик пользователей информационной системы.

Применение архитектур искусственных нейронных сетей позволило достичь высоких показателей эффективности биометрических систем с разными наборами биометрических характеристик. Во многих государственных и бизнес-структурах были внедрены методики, алгоритмы и программные решения, предназначенные для авторизации пользователей информационной системы с применением персональных данных с низким уровнем показателей ошибок первого и второго рода, коэффициента переходных ошибок. Для достижения такого уровня эффективности были сформированы разные наборы данных, а также использованы ранее зарекомендовавшие себя лучшие международные практики, исследования и образовательные программы в области информационной безопасности.

Бейкер Д., Рабинер Л.Р. и Цзюан Б.Х. в своих трудах проводили исследования по распознаванию речи с применением статистических данных для распознавания речевых сигналов и метода скрытых марковских моделей [1]. Васильевым В.И. предложены новые методы и алгоритмы машинного обучения в процессах идентификации биометрических систем на базе статических признаков [2]. Шелупановым А.А. и Сабановым А.Г. был приведен анализ цифровой идентификации и аутентификации субъектов доступа применительно к задаче управления доступом к информационным ресурсам, а также предложены критерии доверия к результатам идентификации и аутентификации [3]. Машкина И.В. в своих исследованиях представила новые результаты при распознавании речи, применив метод лидирующих формант при анализе частотного диапазона пользователей информационной системы, а также разработала уникальную архитектуру нейронной сети в задачах распознавания личности по голосу [4]. В работах Ложникова П.С. представлены методы машинного обучения и новые

подходы к применению искусственного интеллекта в процессах биометрической аутентификации [5]. Тодиско М. в своих исследованиях нашел новый извлеченный признак – Q-константный кепстральный коэффициент [6].

Результаты, достигнутые учеными в данной области исследования, являются основополагающими и необходимыми для прогресса в дальнейшем. Целью дальнейших исследований ученых в области авторизации является повышение точности процедуры аутентификации пользователей информационной системы по извлеченным биометрическим характеристикам.

Несмотря на стремительный прогресс информационных технологий, согласно статистическим показателям TAdviser, количество поставленных программных продуктов компаниями в области биометрии за 2022 год составило 13 единиц, что на 55 % (29 проектов) и 79 % (61 проект) меньше, чем за 2021 и 2020 год соответственно. С учетом возрастания уровня киберпреступности также увеличивается перечень критериев и требований к поставщикам продуктов информационной безопасности.

Для повышения точности распознавания в биометрии используются мультимодальные биометрические системы аутентификации[1]. В рамках рассматриваемого исследования разработана и реализована система мультимодальной биометрической аутентификации пользователей, которая состоит из подсистем распознавания личности по изображению лица в режиме онлайн и по голосу с применением архитектур искусственных нейронных сетей с разными наборами биометрических данных. В данной статье представлены результаты, описаны процессы формирования базы биометрических персональных данных и процессы обучения искусственной нейронной сети по изображению лица.

Задача исследования – разработка метода и алгоритма распознавания пользователей информационной системы с помощью мультимодальной биометрической аутентификации.

Разработанная система мультимодальной биометрической аутентификации пользователей реализована на языке программирования Python 3.8. Для составления архитектур искусственных нейронных сетей и их обучения используются такие библиотеки, как Tensorflow, Keras и Pytorch, а для создания главного меню и интерфейса программы – PyQT5 и TKinter.

Распознавание пользователей информационной системы по изображению лица

Процессы биометрической аутентификации являются дополнительным уровнем защиты информации как в информационной системе (локальные сети предприятия), так и в системе контроля и управления доступом (СКУД). При распознавании личности применяются разные типы биометрических характеристик и их комбинации. К одному из типов биометрических характеристик относится распознавание личности по изображению лица. В основе распознавания личности заложено извлечение признаков или дескрипторов, которые можно получить при применении алгоритмов. Так, некоторые ученые в данной области ранее рассматривали и применяли такие алгоритмы, как метод Виолы-Джонса, метод гибкого сравнения на графах, метод главных компонент, основанный на преобразовании Карунена–Лоева [7].

В данной работе предлагается определение пользователей информационной системы по изображению лица посредством извлечения признаков гистограммы ориентированных градиентов (HOG, Histogram of Oriented Gradients) и дескрипторов локальных бинарных шаблонов (LBP, Local Binary Patterns) [8].

[1] ГОСТ Р 54411-2018 «Информационные технологии. Биометрия. Мультимодальные и другие мультибиометрические технологии». М.: Стандартинформ; 2018. 27 с.

Гистограмма ориентированных градиентов – это дескриптор используемой функции в компьютерном зрении и обработке изображений с целью обнаружения объектов [9]. Методика подсчитывает появление градиентной ориентации в локализованных частях изображения. Концепция извлечения дескриптора гистограммы ориентированных градиентов заключается в том, что внешний вид и форму локального объекта внутри изображения можно описать распределением градиентов интенсивности или направлениями краев. Изображение делится на небольшие соединенные области, называемые ячейками, и для пикселей в каждой ячейке составляется гистограмма направлений градиента.

Вычисления дескрипторов HOG осуществляются на основе оператора Собеля. Результатом применения оператора Собеля в каждой точке изображения является либо вектор градиента яркости в этой точке, либо его норма.

После фильтрации и предварительной обработки изображения пользователя информационной системы представляется векторное направление каждого пикселя ячейки в гистограмме градиентов HOG. Величина и направление каждого градиента представляется в виде двух матриц размерностью 8x8 с углами в диапазоне от 0 до 180 градусов. Данные показатели сортируются в гистограмме, которая состоит из 9 бинов.

Если угол больше 160 градусов, он находится между 160 и 180. Например, пиксель с углом 165 градусов вносит пропорциональный вклад в бин 0 градусов и бин 160 градусов.

Полученные показатели всех пикселей изображения пользователя информационной системы в ячейках 8x8 складываются для создания 9-биновой гистограммы.

Гистограмма имеет большой вес около 0 и 180 градусов. Таким образом, градиенты изображения указывают либо вверх, либо вниз.

Построение локальных бинарных шаблонов основано на ассоциации каждого пикселя изображения с группой пикселей его окрестности [10]. Применение оператора локальных бинарных шаблонов (LBP) позволяет каждому пикселю полутонового изображения поставить в соответствие бинарный код, который описывает его текстурные характеристики.

Оператор работает с группой пикселей и вычисляет бинарный код для центрального пикселя группы. Применение оператора LBP зависит от количества пикселей окрестности, которыми описывается центральный пиксель области.

В зависимости от конкретной задачи, качества изображения эмпирическим путем выбирается количество значимых пикселей.

Каждый пиксель изображения имеет определенное значение интенсивности. Применение оператора LBP позволяет вычислить бинарный код определенного пикселя, используя значения интенсивностей пикселей–соседей. Каждый квадрат условно описывает пиксель изображения. Получить полутоновое изображение из полноцветного можно с помощью формулы:

$$\mathrm{g} = 0.3\mathrm{R} + 0.59\mathrm{G} + 0.11\mathrm{B}, \quad (1)$$

где R, G, B – значения красного, зеленого и синего цветов соответственно [0, 255]; g – значение интенсивности оттенков какого-либо цвета пикселя.

Значение 0 соответствует черному цвету (отсутствие интенсивности), значение 255 – белому (максимальная интенсивность).

Координаты точек окрестности не всегда попадают точно в центры пикселей, поэтому для вычисления значений этих точек используется билинейная интерполяция.

Пиксели, значения интенсивности которых больше центрального пикселя (или равное ему), принимают значения «1»; значения интенсивности пикселей, которые

меньше центрального пикселя, равны «0». Получается бинарный код, представляющий окрестность пикселя.

Вычисление LBP с радиусом R и количеством пикселей окрестности P производится следующим образом [11]:

$$LBP_{P,R} = \sum_{p=0}^{P-1} s(g_p - g_c)2^p, \quad (2)$$

где $s(x)$ – пороговая функция, g_p – значение интенсивности p–ого пикселя, g_c – значение интенсивности центрального пикселя, p – номер пикселя, $p = 0, \dots, P-1$.

Пороговая функция $s(x)$, в которой $x = (g_p - g_c)$, имеет вид:

$$s(x) = \begin{cases} 1, x \geq 0 \\ 0, \ x < 0 \end{cases}. \quad (3)$$

Применение данного оператора позволяет отслеживать изменения не только каждого пикселя, но и его окрестности для анализа статических свойств человеческого лица.

Следует обратить внимание на проблему распознавания искомого пользователя информационной системы. Для осуществления несанкционированного доступа используется обширный арсенал разрабатываемых программных решений [12]. В том числе данные решения применяются в процессах аутентификации пользователей и являются методикой синтеза изображения или голоса (дипфейк) [13]. Данная методика используется для соединения и наложения существующих изображений и видео на исходные изображения (например, FakeApp). Несмотря на то, что данные инструменты используются в других сферах деятельности (в том числе в качестве развлекательного контента), количество киберинцидентов продолжает расти. В связи с этим в рамках данного исследования была разработана модель, предназначенная для противодействия методике синтеза изображения и для противодействия распознаванию пользователей информационной системы по изображениям, распечатанным на бумажном носителе и сохраненных на других устройствах.

Обучение искусственной нейронной сети

Разработанный авторами алгоритм распознавания личности по изображению лица подразумевает формирование базы данных изображений пользователей информационной системы, извлечение признаков и дескрипторов изображения, сравнение извлеченных признаков входного изображения с изображением из базы данных, подсчет расстояния Кульбака-Лейблера (Рисунок 1).

Для повышения точности и качества распознавания личности по изображению лица в рамках данного исследования проведено обучение по составленной архитектуре искусственной нейронной сети.

При распознавании личности по изображению лица после извлечения дескрипторов LBP и признаков HOG разработана искусственная нейронная сеть, которая представляет собой многослойный персептрон с одним скрытым слоем (Рисунок 2). Входной слой содержит 16 нейронов (№ ПС – № пользователя информационной системы, семь фильтров морфологического преобразования изображений и извлечение значимых (доминантных) дескрипторов DLBP, семь фильтров морфологического преобразования изображений и извлечение признаков HOG). Скрытый слой состоит из 72 нейронов (количество пользователей информационной системы, 9-биновая гистограмма каждого признака HOG, количество значимых (доминантных) дескрипторов DLBP).

Dataset обучающей выборки разделен на три папки: test (тестовый набор), train (тренировочный набор) и val (валидационный набор). Каждая из этих папок разбивается на два класса. Под классом подразумевается пользователь информационной системы. Папка каждого класса (пользователя информационной системы) содержит 100 изображений. Так как два класса содержатся в каждой папке обучающей выборки, общий объем базы данных состоит из 600 биометрических образов (изображений).

Рисунок 1 – Блок-схема алгоритма распознавания личности по изображению лица
Figure 1 – Block diagram of the algorithm for identity recognition from facial image

Выходной слой состоит из результатов, который определяет авторизованных пользователей информационной системы (АП) и неавторизованных пользователей (НАП).

В дальнейшем при распознавании авторизованных и неавторизованных пользователей информационной системы сохраняется снимок изображения, созданный в режиме реального времени. После данной процедуры актуальное изображение пройдет предварительную обработку и морфологическое преобразование. В качестве меры различия гистограмм и, соответственно, в качестве погрешности использовано

расстояние Кульбака-Лейблера, предназначенное для распознавания пользователей информационной системы:

$$D_{KL}(f,g) = \sum_{m=1}^{P\,(P-1)+3} f_m \ln \frac{f_m}{g_m}, \quad (4)$$

где f и g – гистограммы изображений, P – число точек в окрестности LBP, m – номер столбца.

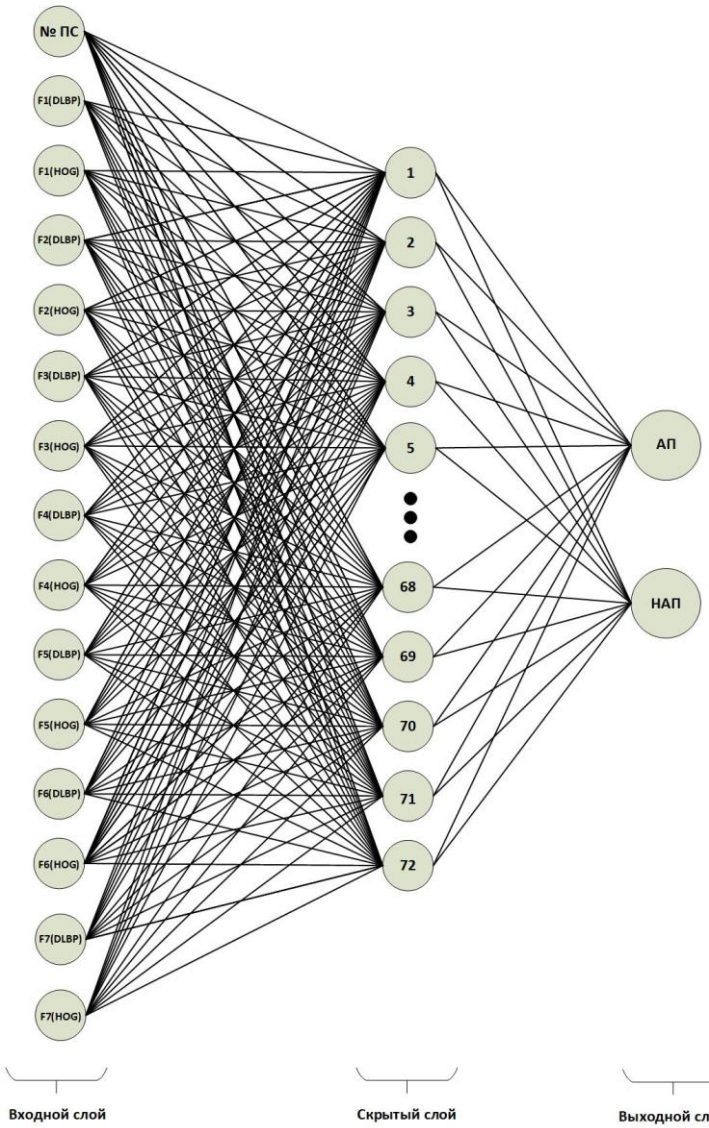

Рисунок 2 – Архитектура искусственной нейронной сети для подсистемы биометрической аутентификации по изображению лица (№ ПС – номер пользователя системы, F1(DLBP):F7(DLBP) – доминантные локальные бинарные шаблоны, F1(HOG):F7(HOG) – гистограмма ориентированных градиентов, АП – авторизованный пользователь системы, НАП – неавторизованный пользователь системы)

Figure 2 – Artificial neural network architecture for biometric authentication subsystem based on facial image (No. US – system user number, F1(DLBP):F7(DLBP) – dominant local binary patterns, F1(HOG):F7(HOG) – histogram of oriented gradients, AU - authorized user of the system, UAU – unauthorized user of the system)

При наличии входных данных можно вычислить значения выходных данных, подставив входное значение в функцию активации. Немаловажно искусственно

подобрать конфигурацию весов искусственной нейронной сети. Корректная конфигурация весов нейронной сети поможет достичь высоких результатов в процессе обучения.

$$H_{1_{\text{вход}}} = (l_1 \times w_1) + (l_2 \times w_2)\,, \tag{5}$$

где $H_{1_{\text{вход}}}$ – входное значение нейрона, l_1 и l_2 – входные нейроны, w_1 и w_2 – весовые коэффициенты.

$$H_{1_{\text{выход}}} = f_{\text{активации}}\left(H_{1_{\text{вход}}}\right), \tag{6}$$

где $H_{1_{\text{вход}}}$ – значение выходного нейрона, $f_{\text{активации}}$ – функция активации.

Результаты

Ошибки первого и второго рода являются основными показателями полученных результатов в системах биометрического распознавания личности. Такие системы могут ошибочно отождествить пользователей системы с неавторизованными пользователями, что является коэффициентом ложного отказа FRR (False Rejection Rate) и, соответственно, ошибкой первого рода. Противоположной ошибкой будет неспособность системы распознать легитимного зарегистрированного пользователя, или опознать подозреваемого в преступлении, что является коэффициентом ложного допуска FAR (False Acceptance Rate) и, соответственно, ошибкой второго рода.

Биометрические технологии характеризуются собственной парой коэффициентов ошибок первого и второго рода:

– p_1^{FAR}– вероятность ложного допуска первой биометрической технологии;
– p_1^{FRR} – вероятность ложного отказа первой биометрической технологии;
– p_2^{FAR} – вероятность ложного допуска второй биометрической технологии;
– p_2^{FRR} – вероятность ложного отказа второй биометрической технологии.

Необходимо рассчитать коэффициенты ошибки первого рода, коэффициент ложного отказа FRR (False Rejection Rate) и ошибки второго рода, коэффициент ложного допуска FAR (False Acceptance Rate) для комбинаций двух технологий. Результирующие вероятности ошибок будут обозначаться:

$$p_{\text{или}}^{FAR}, p_{\text{или}}^{FRR}, p_{\text{и}}^{FAR}, p_{\text{и}}^{FRR}\,. \tag{7}$$

Для подсчета коэффициента ложного отказа следует найти отношение количества отказов в доступе к общему количеству попыток. Коэффициент ложного пропуска является отношением количества успешных попыток авторизоваться в системе как пользователь к общему количеству независимых попыток.

Ошибка ложного отказа может возникать только в том случае, если получено ошибочное решение ложного отказа. Вероятность ошибки ложного отказа определяется произведением двух вероятностей[2]:

$$p_{\text{или}}^{FRR} = p_1^{FRR} \times p_2^{FRR}\,. \tag{8}$$

Вероятность ложного допуска FAR при использовании подхода, представленного ранее[2], будет выше:

$$p_{\text{или}}^{FAR} = 1 - [1 - p_1^{FAR}] \times [1 - p_2^{FAR}] = p_1^{FAR} + p_2^{FAR} - p_1^{FAR} \times p_2^{FAR}\,. \tag{9}$$

[2] ГОСТ Р 50779.10-2000. «Статистические методы. Вероятность и основы статистики. Термины и определения». М.: Стандартинформ; 2000. с. 25-26.

Ошибка ложного допуска может возникать только в том случае, если получено решение ложного допуска. Объединенная вероятность ошибки ложного допуска является произведением вероятностей ошибок[2]:

$$p_{\text{и}}^{FAR} = p_1^{FAR} \times p_2^{FAR} . \quad (10)$$

Ошибки ложного допуска при использовании подхода, представленного выше[2], будут меньше. Но вероятность ложного отказа, которая может быть выражена как дополнение к вероятности того, что система не вызовет ложный отказ доступа, оказывается выше, чем для каждой технологии по отдельности:

$$p_{\text{и}}^{FRR} = 1 - [1 - p_1^{FRR}] \times [1 - p_2^{FRR}] = p_1^{FRR} + p_2^{FRR} - p_1^{FRR} \times p_2^{FRR} . \quad (11)$$

Для корректности оценки эффективности используемой методики извлечения дескрипторов и характеристик изображений лица пользователей информационной системы приведены показатели ошибок первого и второго рода на разных наборах сформированной базы данных изображений, состоящей из 100, 200 и 600 изображений (Рисунок 3).

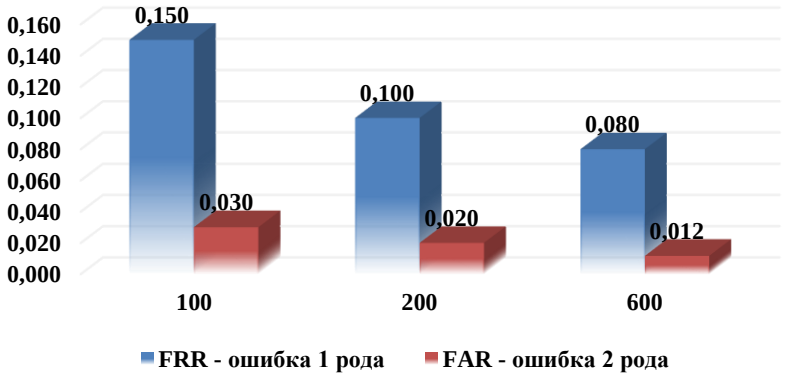

Рисунок 3 – Ошибки 1 и 2 рода при распознавании пользователей информационной системы по изображению лица на разных наборах данных
Figure 3 – Errors of the 1st and 2nd kind in recognizing users of an information system from facial images on different datasets

Обсуждение

Ранее специалистами в области идентификации и аутентификации обучение проводилось на ранее сформированных базах данных, таких как:

– Labeled Faces in the Wild Home (1 609 изображений лица);
– IMDB Wiki Faces Dataset (более 500 000 изображений лица);
– CelebFaces Attributes (более 200 000 изображений лица);
– встроенный DataSet библиотеки Keras.

В рассматриваемом исследовании основной целью обучения является распознавание пользователей информационной системы по изображению лица. В связи с этим данное исследование будет проводиться в дальнейшем при наибольшем количестве изображений. Но следует отметить, что в результате проведенных экспериментальных работ при наибольшем количестве изображений программное обеспечение имеет положительную динамику и повышается уровень эффективности распознавания личности по выбранному биометрическому признаку. Соответственно, показатели ошибок первого и второго рода в данном исследовании ниже, чем в ранее

проведенных исследованиях с применением представленных банков данных изображений лица.

Заключение

Представлены алгоритм и структура программного комплекса мультимодальной биометрической технологии аутентификации пользователей информационной системы, разработана архитектура искусственной нейронной сети при распознавании пользователей информационной системы по изображению лица. Результатом исследования является разработанная авторами модель распознавания пользователей информационной системы по биометрическим признакам с высокими показателями эффективности.

Рассмотрены основные компоненты языков программирования, в том числе библиотеки, необходимые для обучения искусственных нейронных сетей, обработки элементов и данных, которые также могут быть графически представлены. Для решения поставленных задач данного исследования были установлены компоненты, предназначенные для обработки входных изображений, базы данных изображений лица пользователей информационной системы. К числу необходимых ресурсов данного языка программирования также следует отнести графический редактор, с помощью которого были сконструированы интерфейс, индикация загрузки и анимация заставки.

СПИСОК ИСТОЧНИКОВ

1. Lawrence R. Rabiner, Ronald W. Schafer. *Theory and Applications of Digital Speech Processing.* Prentice Hall; 2010. 1056 p.
2. Васильев В.И., Жумажанова С.С., Ложников П.С., Сулавко А.Е. Оценка идентификационных возможностей биометрических признаков от стандартного периферийного оборудования. *Вопросы защиты информации.* 2016;112(1):12–20.
3. Шелупанов А.А., Сабанов А.Г. *Идентификация и аутентификация в цифровом мире.* М.: Горячая линия-Телеком; 2022. 355 с.
4. Машкина И.В., Белова Е.П. Разработка нейросетевой базы данных биометрических образов для системы аутентификации по голосу. *Проблемы информационной безопасности. Компьютерные системы.* 2019;(2):86–93.
5. Ложников П.С., Сулавко А.Е., Еременко А.В., Волков Д.А. Экспериментальная оценка надежности верификации подписи сетями квадратичных форм, нечёткими экстракторами и персептронами. *Информационно–управляющие системы.* 2016;84(5):73–85. DOI: 10.15217/issn1684–8853.2016.5.73.
6. Todisco M., Delgado H., Evans N. A new feature for automatic speaker verification anti-spoofing: Constant Q cepstral coefficients. In: *Odyssey 2016: The Speaker and Language Recognition Workshop, 21–24 June 2016, Bilbao, Spain.* Bilbao: ISCA SIG; 2016. p. 283–290.
7. Горбунов А.Л. Визуальная когерентность в дополненной реальности. *Advanced Engineering Research (Rostov-on-Don)*. 2023;23(2):180–190. DOI: 10.23947/2687-1653-2023-23-2-180-190.
8. Korkmaz S., Binol H. Classification of molecular structure images by using ANN, RF, LBP, HOG, and size reduction methods for early stomach cancer detection. *Journal of Molecular Structure.* 2018;(1156):255–263. DOI: 10.1016/j.molstruc.2017.11.093.
9. Korkmaz S., Akjijek A., Binol H.B., Korkmaz M. Recognition of the stomach cancer images with probabilistic HOG feature vector histograms by using HOG features. In: *2017 IEEE 15th International Symposium on Intelligent Systems and Informatics (SISY), 14–16 September 2017, Subotica, Serbia.* IEEE. p. 339–342. DOI: 10.1109/SISY.2017.8080578.

10. Девицына С.Н., Елецкая Т.А., Балабанова Т.Н., Гахова Н.Н. Разработка интеллектуальной системы биометрической идентификации пользователя. *Экономика. Информатика.* 2019;46(1):148–160.
11. Анисимова А.С., Аникин И.В. Интеллектуальная система биометрической аутентификации пользователя по динамической рукописной подписи. В сборнике: *Международный форум Kazan Digital Week–2022, 21–24 сентября 2022, Казань, Россия.* Казань: Научный центр безопасности жизнедеятельности; 2022. с. 280–285.
12. Van Hoorick B., Vondrick C. *Dissecting Image Crops*. Columbia University, New York; 2020.
13. Raveendra M., Nagireddy K. DNN Based Moth Search Optimization for Video Forgery Detection. *International Journal of Engineering and Advanced Technology.* 2019;9(1):1190–1199.

REFERENCES

1. Lawrence R. Rabiner, Ronald W. Schafer. *Theory and Applications of Digital Speech Processing.* Prentice Hall; 2010. 1056 p.
2. Vasiliev V.I., Zhumazhanova S.S., Lozhnikov P.S., Sulavko A.E. Otsenka identifikatsionnyh vozmozhnostei biometricheskikh priznakov ot standartnogo periferiinogo oborudovaniya. *Voprosy zashchity informatsii = Information security questions.* 2016;112(1):12–20. (In Russ.).
3. Shelupanov A.A., Sabanov A.G. Identifikaciya i autentifikatsiya v tsifrovom mire. Moscow, Gortachaja linita-Telekom; 2022. 355 p. (In Russ.).
4. Mashkina I.V., Belova E.P. Development of the biometric images neural network database for voice authentication system. *Problemy informatsionnoi bezopasnosti. Kompiuternye sistemy = Problems of information security. Computer systems.* 2019;(2):86–93. (In Russ.).
5. Lozhnikov P.S., Sulavko A.E., Eremenko A.V., Volkov D.A. Experimental evaluation of reliability of signature verification by quadratic form networks, fuzzy extractors and perceptrons. *Informatsionno–upravlyaiushhie sistemy = Information and control systems.* 2016;84(5):73–85. DOI: 10.15217/issn1684–8853.2016.5.73. (In Russ.).
6. Todisco M., Delgado H., Evans N. A new feature for automatic speaker verification anti-spoofing: Constant Q cepstral coefficients. In: *Odyssey 2016: The Speaker and Language Recognition Workshop, 21–24 June 2016, Bilbao, Spain.* Bilbao: ISCA SIG; 2016. p. 283–290.
7. Gorbunov A.L. Visual Coherence for Augmented Reality. *Advanced Engineering Research (Rostov-on-Don).* 2023;23(2):180-190. DOI: 10.23947/2687-1653-2023-23-2-180-190. (In Russ.).
8. Korkmaz S., Binol H. Classification of molecular structure images by using ANN, RF, LBP, HOG, and size reduction methods for early stomach cancer detection. *Journal of Molecular Structure.* 2018;(1156):255–263. DOI: 10.1016/j.molstruc.2017.11.093.
9. Korkmaz S., Akjijek A., Binol H.B., Korkmaz M. Recognition of the stomach cancer images with probabilistic HOG feature vector histograms by using HOG features. In: *2017 IEEE 15th International Symposium on Intelligent Systems and Informatics (SISY), 14–16 September 2017, Subotica, Serbia.* IEEE. p. 339–342. DOI: 10.1109/SISY.2017.8080578.
10. Devitsyna S.N., Eletskaya T.A., Balabanova T.N., Gakhova N.N. The development of intelligent biometric identification system user. *Ekonomika. Informatika = Economics. Information technologies.* 2019;46(1):148–160. (In Russ.).
11. Anisimova A.S., Anikin I.V. Intelligent biometric user authentication system based on dynamic handwritten signature. In: *Mezhdunarodnyi forum Kazan Digital Week–2022, 21–*

24 September 2022, Kazan, Russia. Kazan: The scientific centre of children's personal and social safety; 2022. p. 280–285. (In Russ.).
12. Van Hoorick B., Vondrick C. *Dissecting Image Crops*. Columbia University, New York; 2020.
13. Raveendra M., Nagireddy K. DNN based moth search optimization for video forgery detection. *International Journal of Engineering and Advanced Technology.* 2019;9(1):1190–1199.

ИНФОРМАЦИЯ ОБ АВТОРАХ / INFORMATION ABOUT THE AUTHORS

Гузаиров Мурат Бакеевич, доктор технических наук, профессор, Уфимский университет науки и технологий, кафедра управления информационной безопасностью, Уфа, Российская Федерация.
e-mail: mbguzairov@gmail.com
Author ID: 6504475472

Murat B. Guzairov, Doctor of Technical Sciences, Professor, Ufa University of Science and Technology, the Department of Information Security Management, Ufa, the Russian Federation.

Исмагилова Альбина Сабирьяновна, доктор физико-математических наук, профессор, Уфимский университет науки и технологий, заведующий кафедрой управления информационной безопасностью, Уфа, Российская Федерация.
e-mail: ismagilovaas@yandex.ru
ORCID: 0000-0002-8539-5974

Albina S. Ismagilova, Doctor of Physical and Mathematical Sciences, Professor, Ufa University of Science and Technology, Head of the Department of Information Security Management, Ufa, the Russian Federation.

Лушников Никита Дмитриевич, аспирант, ассистент, Уфимский университет науки и технологий, кафедра управления информационной безопасностью, Уфа, Российская Федерация.
e-mail: luschnikovnikita@yandex.ru
ORCID: 0000-0002-1409-4736

Nikita D. Lushnikov, Postgraduate Student, Assistant Lecturer, Ufa University of Science and Technology, Ufa, the Russian Federation.

Статья поступила в редакцию 06.11.2023; одобрена после рецензирования 16.11.2023; принята к публикации 30.11.2023.

The article was submitted 06.11.2023; approved after reviewing 16.11.2023; accepted for publication 30.11.2023.