ТЕХНИЧЕСКИЕ НАУКИ

УДК 004.8

Разработка системы распознавания лиц для контроля доступа

Е.А. Гулецкий, Д. Оджуньон, Е.А. Маслов
Донской государственный технический университет, г. Ростов-на-Дону, Российская Федерация

Аннотация
На сегодняшний день проблема защиты информации является одной из ведущих. Механизмы ее защиты совершенствуются с каждым годом. Целью данной статьи является моделирование системы контроля доступа на предприятии, описание этапов её создания и предложения по её улучшению с помощью нейросетей для обнаружения маски и очков на лице. Результаты распознавания лица — 99,38 %, масок — 97,7 %, очков — 96,4 %. Для реализации системы был выбран язык программирования Python и библиотеки машинного обучения dlib и TensorFlow.

Ключевые слова: защита информации, распознавание лиц, искусственный интеллект, нейросеть, контроль доступа, TensorFlow, dlib

Для цитирования. Гулецкий Е.А., Оджуньон Д., Маслов Е.А. Разработка системы распознавания лиц для контроля доступа. *Молодой исследователь Дона*. 2024;9(4):46–51.

Development of a Facial Recognition System for Access Control

Egor A. Guletskii, Didier Odjougnon, Egor A. Maslov
Don State Technical University, Rostov-on-Don, Russian Federation

Abstract
Nowadays, the problem of information security is one of the leading ones. Its protection mechanisms are being improved every year. Within the framework of this article, the access control system at the enterprise is modeled, the stages of its creation are described and the improvement using neural networks for detecting masks and glasses on the face is proposed. Recognition results: faces — 99.38%, masks — 97.7%, glasses — 96.4%. The Python programming language and the lib and TensorFlow machine learning libraries were chosen to implement the system.

Keywords: information protection, facial recognition, artificial intelligence, neuronet, access control, TensorFlow, dlib

For citation. Guletskii EA, Odjougnon D, Maslov EA. Development of a Facial Recognition System for Access Control. *Young Researcher of Don.* 2024;9(4):46–51.

Введение. Чтобы избежать утечки или потери секретной информации, требуется организовывать разграничение доступа к ней. Разграничение доступа — это управление и контроль над доступом субъектов к объектам в соответствии с установленными правилами безопасности предприятия. Для создания надежной системы защиты информации необходимо использовать самые передовые технологии. В наше время наиболее перспективно выглядит развитие искусственного интеллекта и, в частности, нейронных сетей. Нейросеть — математическая модель, которая функционирует по принципам работы нервной системы живых организмов. Основное предназначение нейросетей заключается в решении интеллектуальных задач, то есть таких, где отсутствует заранее заданный алгоритм действий и предсказуемый результат [1]. Цель исследования — практическая реализация системы распознавания лиц и её улучшение с помощью нейронных сетей.

Основная часть. Для начала опишем наше видение данной системы распознавания лиц. Есть предприятие с несколькими отделами, которые работают с разными уровнями конфиденциальности информации. У каждого

работника есть определенный уровень доступа к этим отделам. Вся информация о работниках находится в базе данных: ФИО, контактная информация, фотография в профиль и уровень доступа. На входе в каждый отдел установлена камера, которая считывает лицо человека и сравнивает его с фотографиями работников из базы данных. Если совпадений не нашлось, то человек не является работником данного предприятия, поэтому в доступе ему будет отказано. Если человек найден в базе данных и его уровень доступа равен или выше требуемого для входа в данный отдел, то доступ будет предоставлен. В противном случае он получит отказ.

Для реализации данной системы был выбран язык программирования Python из-за простоты в использовании и наличия множества как встроенных, так и сторонних пользовательских библиотек. Камера с распознаванием лиц будет моделироваться через веб-камеру ноутбука и работать в реальном времени. С помощью библиотеки face_recognition на камере будет распознаваться лицо. Данная библиотека предоставляет простые в использовании функции для распознавания и манипуляции с лицами. Она основана на библиотеке dlib и использует глубокие сверточные нейронные сети для анализа лицевых изображений. Face_recognition определяет лицо и его местонахождение на изображении как 4 координаты: left, right, top, bottom. По этим координатам рисуем квадрат, которым будет выделять лицо. После запроса доступа делается скриншот части изображения, которое находится в квадрате, то есть лица. Распознавание будет осуществляться с помощью расчета расстояния Евклида между дескрипторами полученного скриншота и фотографий из базы данных с работниками. Преимущество данного способа заключается в том, что не нужно собирать большой набор фотографий для каждого сотрудника, чтобы система научилась их распознавать.

Нахождение дескрипторов происходит с помощью библиотеки машинного обучения dlib. Она использует уже обученную нейронную сеть ResNet, которая извлекает ключевые признаки из изображения. Для лица такими признаками являются контуры глаз, бровей, носа, губ и овал лица. В результате получается набор чисел, который и называется дескриптором. Для фотографий одного человека значения дескрипторов будут находиться рядом друг с другом, а для разных людей — далеко. Если полученное расстояние меньше 0,6, то на фотографиях один и тот же человек. Но для более надежного контроля доступа мы уменьшим это значение до 0,5, так как лучше система не распознает работника, чем пропустит злоумышленника.

Преимуществом ResNet является точность и быстрота вычисления. По заявленным данным, точность данной модели на тесте распознавания лиц Labeled Faces in the Wild составила 99,38 % [2].

После нахождения дескрипторов для оценки их близости в dlib используется Евклидово расстояние. Оно вычисляет расстояние между двумя точками в n-мерном пространстве по теореме Пифагора. Для расчета расстояния Евклида используется модуль distance из библиотеки scipy.spatial, который в основном используется для научных расчетов, за счет чего имеет большую эффективность с точки зрения производительности в сравнении с тем же numpy. Для улучшения системы контроля доступа были написаны нейросети, которые распознают маску и солнцезащитные очки на лице, так как они закрывают одни из ключевых признаков, которые определяет модель ResNet, из-за чего распознавание может работать некорректно. Теперь после включения камеры сначала будет проверяться наличие маски или очков на лице. Если таковые были обнаружены, то система попросит сначала снять их, а уже после будет устанавливать личность для предоставления доступа.

Для создания моделей были использованы библиотеки TensorFlow и Keras.

TensorFlow — это мощная платформа с открытым исходным кодом, предназначенная для разработки приложений машинного обучения. Она представляет собой символическую математическую библиотеку, которая использует поток данных и дифференцируемое программирование для обучения и применения глубоких нейронных сетей [3].

Keras — это Python-библиотека, специально разработанная для глубокого обучения. Она упрощает и ускоряет процесс создания и настройки моделей, которые определяют распространение и подсчет информации во время обучения.

Так как вся работа происходит с изображениями, то была использована сверточная нейронная сеть. Сверточная нейронная сеть — это тип искусственной нейронной сети, который особенно эффективен для обработки и анализа изображений и видео. Она используется в различных задачах компьютерного зрения, таких как распознавание объектов, классификация изображений, сегментация, обнаружение объектов и т.д.

Для распознавания маски и очков использовалась одинаковая модель, которая обучалась на разных наборах данных. Сводка данной модели представлена на рис. 1.

Layer (type)	Output Shape	Param #
conv2d (Conv2D)	(None, 128, 128, 16)	448
max_pooling2d (MaxPooling2D)	(None, 64, 64, 16)	0
dropout (Dropout)	(None, 64, 64, 16)	0
conv2d_1 (Conv2D)	(None, 64, 64, 32)	4640
max_pooling2d_1 (MaxPooling2D)	(None, 32, 32, 32)	0
dropout_1 (Dropout)	(None, 32, 32, 32)	0
conv2d_2 (Conv2D)	(None, 32, 32, 64)	18496
max_pooling2d_2 (MaxPooling2D)	(None, 16, 16, 64)	0
dropout_2 (Dropout)	(None, 16, 16, 64)	0
flatten (Flatten)	(None, 16384)	0
dense (Dense)	(None, 512)	8389120
dense_1 (Dense)	(None, 2)	1026

Рис. 1. Сводка модели

Для обучения нейросетей использовались наборы данных, взятые с сайта Kaggle. В наборе данных с масками 12 тысяч фотографий, которые поделены на тренировочные, валидационные и тестовые, а также два класса для распознавания: WithMask и WithoutMask [4]. Для определения очков набор собирался из нескольких, и в итоге в нем получилось около 100 тысяч фотографий. Иерархия такая же, как и в наборе для масок. Классы: WithGlasses и WithoutGlasses [5].

Примеры фотографий лиц в маске и без нее из набора данных показаны на рис. 2.

Рис. 2. Пример изображений из набора данных с масками

Примеры фотографий лиц в очках и без них из набора данных показаны на рис. 3.

Рис. 3. Пример изображений из набора данных с очками

По итогу обучения нейросеть с распознаванием масок показала 97,7 % правильных ответов на тестовом наборе данных. Очки на тестовом наборе распознаются с 96,4 % правильных ответов.

Графики обучения модели распознавания маски на лице представлены на рис. 4.

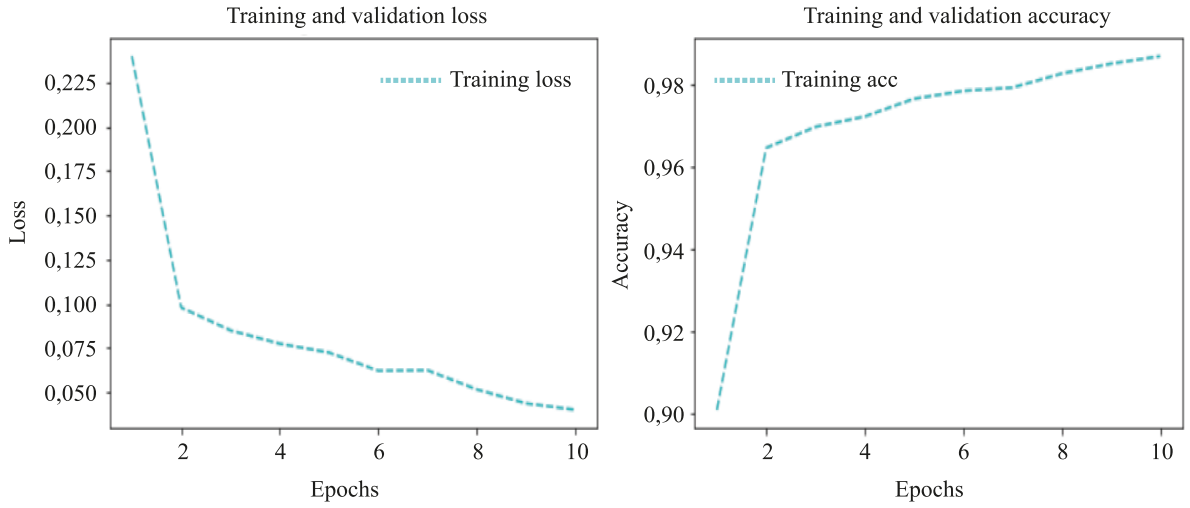

Рис. 4. Графики обучения модели распознавания маски

Графики обучения модели распознавания очков на лице представлен на рис. 5.

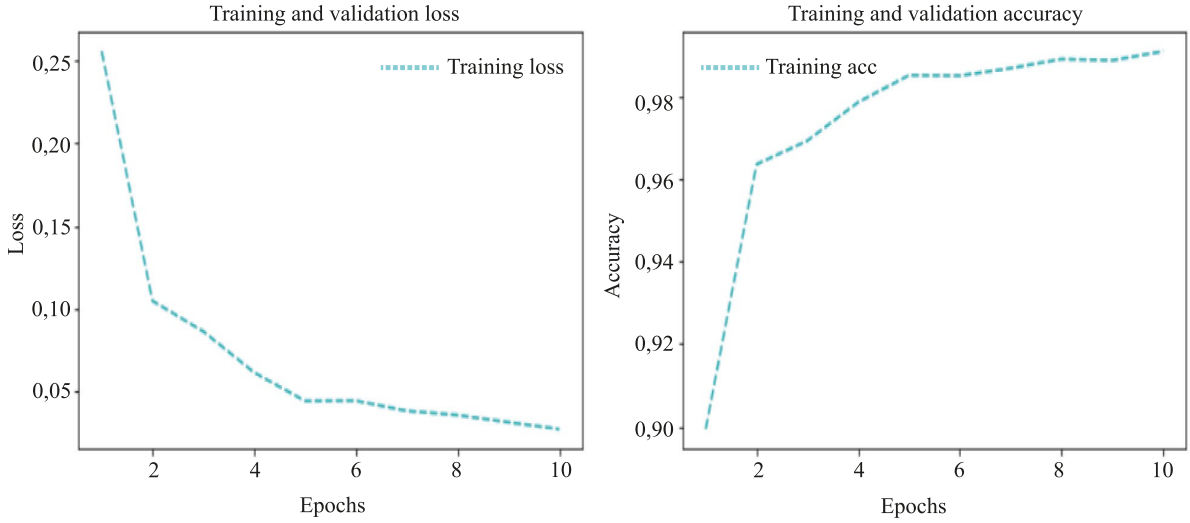

Рис. 5. Графики обучения модели распознавания очков

Пример работы распознавания маски и очков с камеры ноутбука показан на рис. 6.

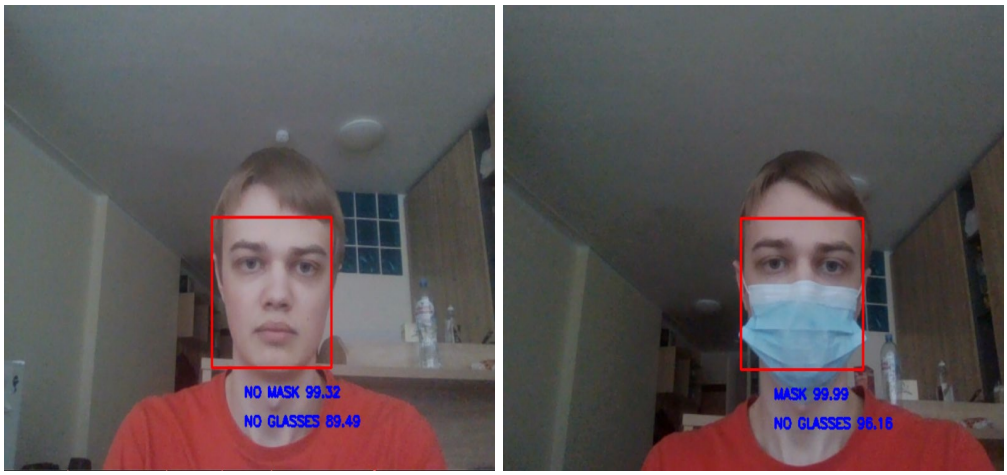

Рис. 6. Распознавание маски и очков через веб-камеру ноутбука

Теперь посмотрим работу системы при запросе доступа к одному из отделов (рис. 7).

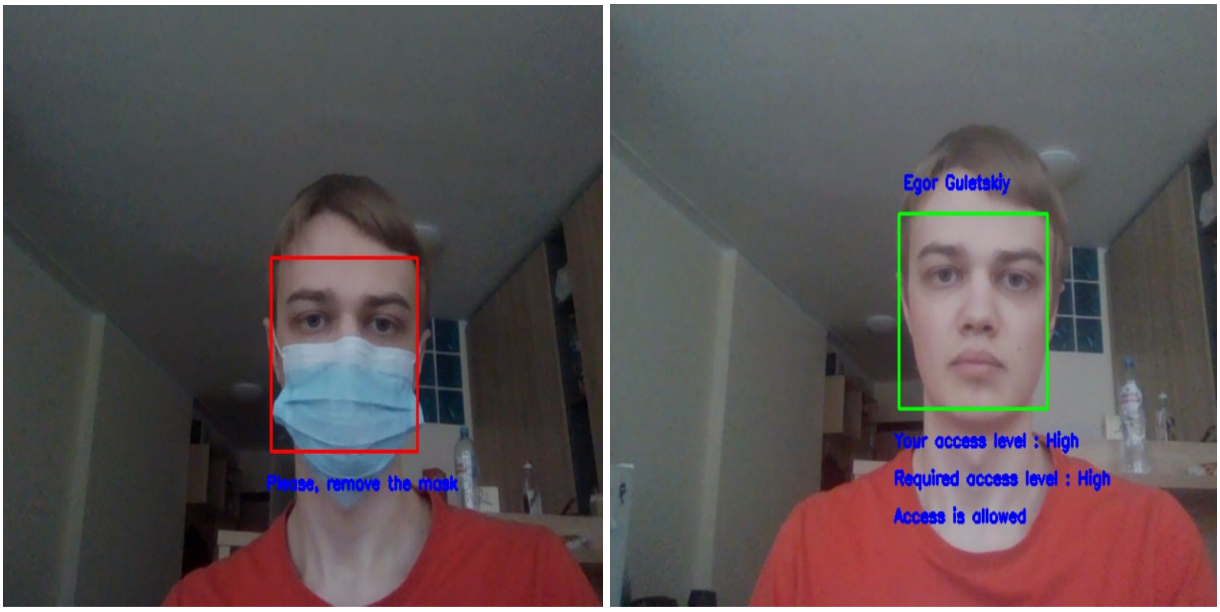

Рис. 7. Работа системы контроля доступа в зону ограниченного доступа

Система обнаружила маску на лице и вывела сообщение о том, что ее необходимо снять. После чего распознала работника и сравнила его уровень доступа с требуемым для входа в отдел. Так как они равны, доступ был предоставлен.

Заключение. В результате данной работы была разработана система распознавания лиц для контроля доступа в зону ограниченного доступа, которая представляет собой эффективное решение для обеспечения безопасности на предприятии. Использование передовых технологий искусственного интеллекта, таких как нейронные сети и алгоритмы распознавания лиц, позволяет достичь высокой точности и надежности системы. Добавление функционала распознавания дополнительных элементов на лице, таких как маски и солнцезащитные очки, улучшает работу системы, за счет чего повышается защита информации и уровень безопасности.

Список литературы

1. *Нейронные сети для начинающих*. Часть 1. URL: https://habr.com/ru/articles/312450/ (дата обращения: 05.04.2024).

2. *Распознавание человека на фотографии с помощью dlib*. URL: https://master--hardcore-noether-529719.netlify.app/deep_learning/2017/08/11/Foto-Verification-with-Dlib.html?ysclid=lvnv2ke6k3855318116 (дата обращения: 05.04.2024).

3. *Библиотека глубокого обучения TensorFlow*. URL: https://habr.com/ru/companies/ods/articles/324898/ (дата обращения: 10.04.2024).

4. *Face Mask Detection ~12K Images Dataset*. URL: https://www.kaggle.com/datasets/ashishjangra27/face-mask-12k-images-dataset (дата обращения: 12.04.2024).

5. *Glasses Classification Dataset*. URL: https://www.kaggle.com/datasets/ashfakyeafi/glasses-classification-dataset/code (дата обращения: 15.04.2024).

Об авторах:

Егор Александрович Гулецкий, студент кафедры кибербезопасность информационных систем Донского государственного технического университета (344003, РФ, г. Ростов-на-Дону, пл. Гагарина, 1), egor.guletskiy@mail.ru

Дидие Оджуньон, студент кафедры кибербезопасность информационных систем Донского государственного технического университета (344003, РФ, г. Ростов-на-Дону, пл. Гагарина, 1), odjougnondidier90@gmail.com

Егор Алексеевич Маслов, студент кафедры кибербезопасность информационных систем Донского государственного технического университета (344003, РФ, г. Ростов-на-Дону, пл. Гагарина, 1), maslov.egor422@gmail.com

Конфликт интересов: **авторы заявляют об отсутствии конфликта интересов.**

Все авторы прочитали и одобрили окончательный вариант рукописи.

About the Authors:

Egor A. Guletskii, Student of the Cybersecurity of Information Systems Department, Don State Technical University (1, Gagarin Sq., Rostov-on-Don, 344003, RF), egor.guletskiy@mail.ru

Didier Odjougnon, Student of the Cybersecurity of Information Systems Department, Don State Technical University (1, Gagarin Sq., Rostov-on-Don, 344003, RF), odjougnondidier90@gmail.com

Egor A. Maslov, Student of the Cybersecurity of Information Systems Department, Don State Technical University (1, Gagarin Sq., Rostov-on-Don, 344003, RF), maslov.egor422@gmail.com

Conflict of Interest Statement: **the authors do not have any conflict of interest.**

All authors have read and approved the final manuscript.