УДК 004.896

БИОМЕТРИЧЕСКАЯ АУТЕНТИФИКАЦИЯ В СИСТЕМАХ БЕЗОПАСНОСТИ С ИСПОЛЬЗОВАНИЕМ КОМПЬЮТЕРНОГО ЗРЕНИЯ

В. А. Ермакович, В. А. Завалей, Е. И. Баяк

Белорусский государственный университет информатики и радиоэлектроники, г. Минск, Республика Беларусь, vladermakovich29@gmail.com, vladzavalej@gmail.com, e.baiak@bsuir.by

В статье представлено описание двух видов биометрической аутентификации в системах безопасности с использованием компьютерного зрения: распознание человека по лицу и радужке глаза. Представлено в статье подробное описание этапов построения таких систем, а также особенности их проектирования. Описаны примеры использования таких методов в различных устройствах для сохранения персональных данных и в зданиях для обеспечения безопасности жизни человека.

Ключевые слова: компьютерное зрение; сверточные нейронные сети; распознавание лица; распознавание радужки глаза; биометрия.

BIOMETRIC AUTHENTICATION IN SECURITY SYSTEMS USING COMPUTER VISION

V. A. Ermakovich, V. A. Zavalei, E. I. Bayak

Belarusian State University of Informatics and Radioelectronics, Minsk, Republic of Belarus, vladermakovich29@gmail.com, vladzavalej@gmail.com, e.baiak@bsuir.by

The article describes two types of biometric authentication in security systems using computer vision: recognition of a person by face and iris. The article provides a detailed description of the stages of building such systems, as well as the design features. Examples of the use of such methods in various devices for storing personal data and in buildings to ensure the safety of human life are described.

Keywords: computer vision; convolutional neural networks; face recognition; iris recognition; biometrics.

1. Введение

Сегодня безопасность информации и доступ к различным местам очень важен. Старые способы проверки личности, такие как пароли или ключ-карты, имеют проблемы: их можно забыть, потерять или украсть.

Это создает проблемы и риски для компаний или организаций в плане безопасности самих сотрудников, а также для объектов, которые имеют сильную значимость.

Биометрическое распознавание предлагает более удобное и надежное решение. Она использует уникальные особенности тела человека для подтверждения того, кто он есть. Лицо, отпечатки пальцев или рисунок радужки глаза у каждого человека свой – как природный «пароль», который всегда с нами и который сложно подделать.

Чтобы компьютер мог «увидеть» и понять эти биометрические особенности (лицо, палец, глаз), нужны специальные технологии. Компьютерное зрение (от англ. Computer Vision (CV)) – это область искусственного интеллекта, которая дает компьютеру анализировать и понимать визуальную информацию, такую как изображения и видео [1].

В этой статье рассмотрены различные современные методы биометрического распознавания с использованием CV, а также их применение.

2. Виды биометрической аутентификации

Биометрически можно распознавать человека с помощью любых конечностей, к примеру руки, пальцы, глаза, нос и т.д. Сейчас самыми популярными видами биометрической аутентификации являются: распознавание лиц (Face Recognition) и распознавание радужки глаза (Iris Recognition).

Face Recognition. Этот вид аутентификации объединяет в себя сразу несколько видов анализа уникальных характеристик лица человека. Распознавание человека происходит на основе его физических особенностей (уникальная форма и расположение носа, глаз, рта, скул; наличие веснушек, шрамов, родинок; текстура кожи и т.д.) и геометрических соотношений между ними [2]. Большим преимуществом у данного вида является его высокая скорость аутентификации, легкость интегрирования в менее мощные системы и устройства. Но есть небольшой ряд недостатков у данного вида биометрической аутентификации, а именно чувствительность к освещению и углу поворота головы, уязвим к подделкам (например, фотографии или 3D-маски без защиты от спуфинга). С первым недостатком многие компании активно борются путем аугментации данных на тренировочной выборке. Также компании прибегают к созданию 3D-модели лица человека, чтобы бороться с такой проблемой. Вопрос уязвимости к созданию подделок до сих пор остается открытым.

Iris recognition. Данный вид аутентификации является уникальным из-за особенности радужки человека. Узор радужки сложен и формируется

случайным образом еще до рождения самого человека, оставаясь практически неизменным на протяжении всей жизни. Вероятность совпадения узора радужек у двух разных людей крайне мала (рис. 1).

Рис. 1. Радужки глаз двух людей

Из-за этого процесс повторения узора радужки становится очень трудоемким и дорогим процессом. От сюда и вытекают преимущества этого вида аутентификации: большая точность и надежность, независимость от характеристик лица человека, а также трудоемкость и дороговизна самого процесса подделывания. Недостатками этого вида является наличие специальных устройств (специализированные инфракрасные камеры) для работы, большая стоимость внедрения в устройства, неудобство для массового пользования.

3. Этапы и особенности применения компьютерного зрения

Два вида биометрической аутентификации (Face Recognition, Iris Recognition) объединяет общие подходы к построению систем безопасности. Выделяются следующие особенности: детектирование объекта (лицо или глаз), нормализация и предварительная обработка, извлечение признаков, применение нейросетей, проверка «живости» (Liveness Detection) и последнее, это сравнение и принятие решения. Дальше рассмотрим подробнее каждую особенность подробнее.

Детектирование объекта. Первый этап определения расположения лица или глаза человека на изображении или видео. С этой задачей хорошо справляются нейросети направленные на такую задачу (Object Detection), на рис. 2 показан результат детектирования.

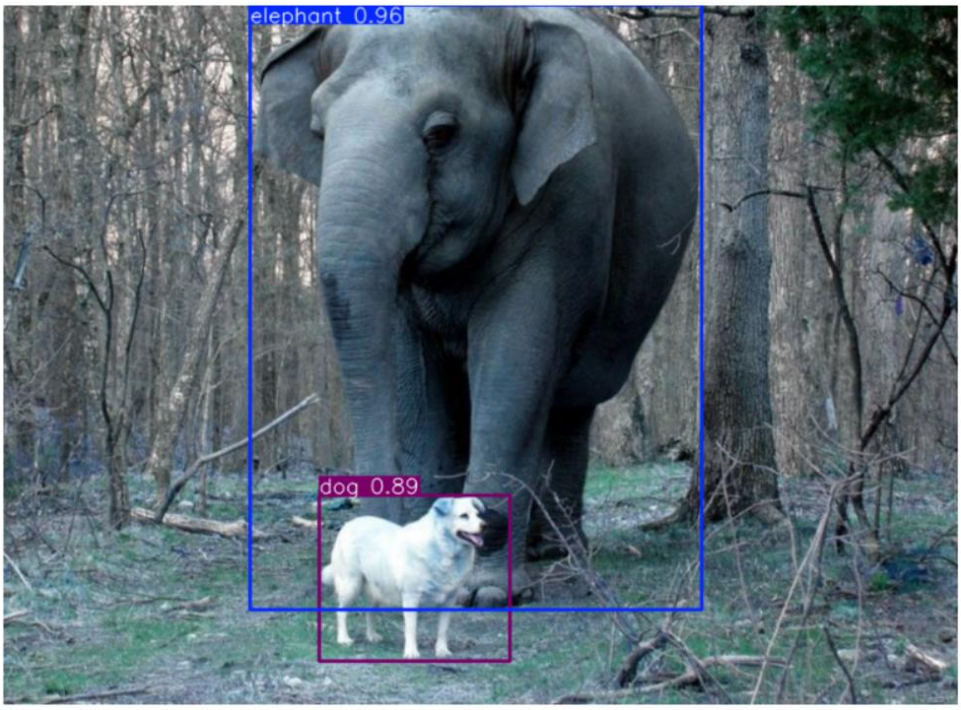

Рис. 2. Пример результата задачи Object Detection

Примером таких моделей является серия YOLO (пример архитектуры показан на рис. 3) [3].

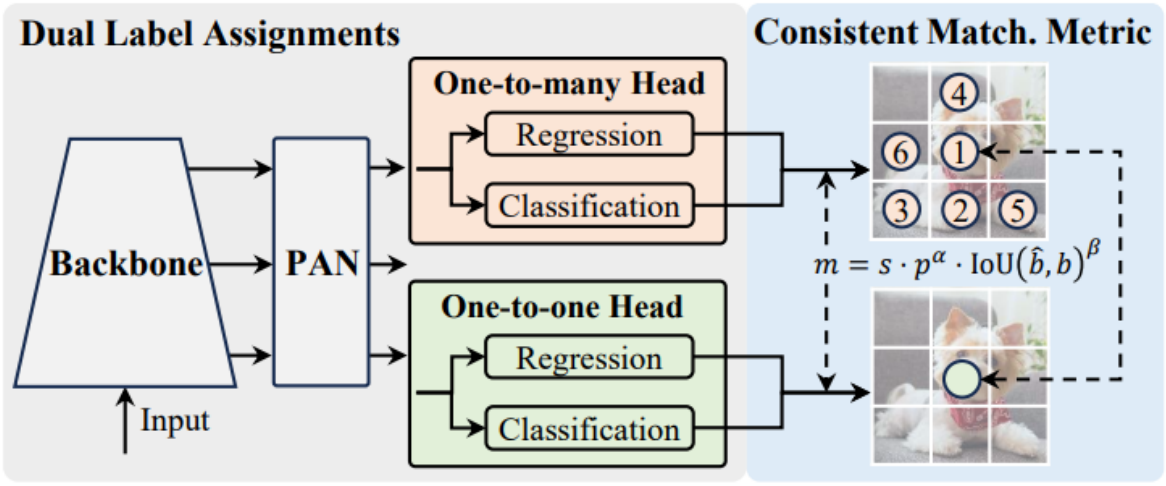

Рис. 3. Архитектура модели YOLOv10 [3]

Backbone отвечает за извлечение признаков, использует улучшеную версию CSPNet (Cross Stage Partiel Network) для улучшения градиентного потока и сниежния вычислительной избыточности.

Neck производит объединение признаков из разных масштабов и передачи их в головую. Включает в себя еще PAN (Path Aggregation Network),

PSA (Partial Self-Attention) для эффективного слияния многомасштабных признаков.

One-to-Many Head генерирует несколько прогнозов для каждого объекта во время обучения, чтобы обеспечить расширенные контрольные сигналы и повысить точность обучения.

One-to-One Head генерирует один наилучший прогноз для каждого объекта во время вывода, чтобы исключить необходимость в NMS (Non-Maximum Suppression), тем самым сокращая задержку и повышая эффективность.

Нормализация и предварительная обработка. На этом этапе происходит распределение ключевых точек (рис. 4) [2] для задачи Face Recognition и устранение теней, шумов на самом изображении.

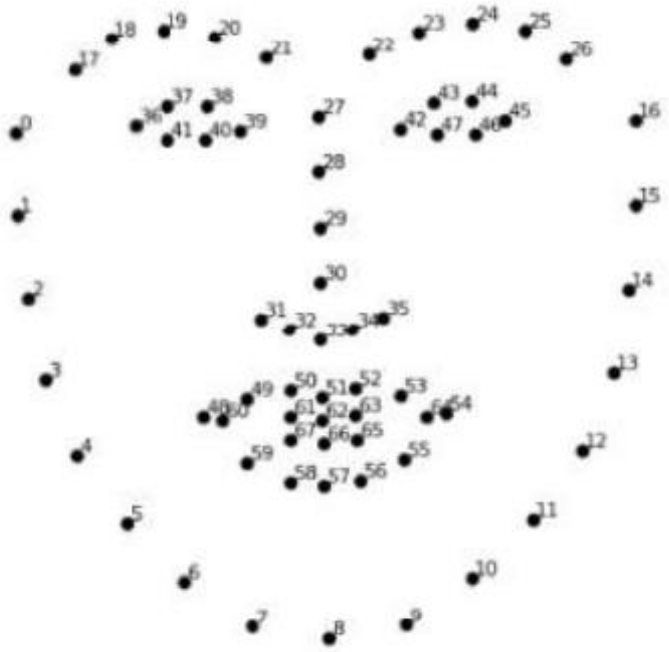

Рис. 4. Пример распределения ключевых точек [2]

Для задачи Iris Recognition происходит преобразование радужки — «растяжение» кольцевого узора в прямоугольную нормализованную форму.

Извлечение признаков. После нормализации и предварительной обработки происходит извлечение признаков. Этой задачей занимаются сверточные нейронные сети (convolutional neural network (CNN)), например, FaceNet, ArcFace, VGGFace / VGGFace2 и другие. Данные модели обучены на больших выборках различных лиц и поэтому могут хорошо извлекать признаки. Для извлечения признаков с изображения, где расположен глаз, используется сеть IrisNet и производные архитектуры (также обучены извлекать признаки с радужки глаз человека) [4].

Liveness Detection. Не мало важным идет проверка «живости», т.е. защита от обмана. В основном это детектирование моргания у человека, мимики, инфракрасная съемка или анализ глубины. Стоит заметить, что данная проверка может стоить довольно много, так как для этого может понадобиться дополнительное оборудование или затраты на разработку. В основе этой проверки лежат рекуррентные нейронные сети (Recurrent neural network (RNN)) и сверточные нейронные сети, а также может использоваться алгоритм отслеживания движения ключевых точек.

Сравнение и принятие решения. На этом заключительном этапе после получения признаков и проверки «живости» идет определение, находится ли человек в базе данных, где лежат характеристики каждого сотрудника или пользователя конкретного устройства. Сравнение происходит с помощью метрик: евклидово расстояние, косинусное сходство, мера Хэмминга и т.д. Также устанавливается порог, если значение полученной метрики меньше, то данные о человеке отсутствуют в базе данных, а если значение метрики больше — о человеке есть сведения.

4. Примеры использования

Достаточно легко найти места, а также устройства, где используется биометрическая аутентификация с использованием компьютерного зрения. Пропускные пункты на различные предприятиях, домофоны в современных домах имеют аутентификацию через сканирование лица. На более важные места, которые могу нести большую ценность для организации, компании или даже человека, используется аутентификацию через сканирование глаза человека.

На большинство телефонов сейчас устанавливаются системы распознавания лица, к примеру, Apple FaceID, Samsung Face Recognition, Xiaomi Face Unlock и другие. Стоит отметь, что лучшая система распознавания лица для телефонов это Apple FaceID, так как она основывается на построении 3D-модели лица с высокой точностью. На данный момент такую же точность имеет японская модель NEC NeoFace, которую используют в аэропортах и правоохранительных органах [5].

5. Заключение

В данной статье были рассмотрены два вида биометрической аутентификации с помощью компьютерного зрения, это распознавание человека через его лицо и радужку его глаза. Были подробно описаны этапы построения таких систем, а также особенности в их проектировании. Были также выявлены преимущества и недостатки каждого вида. Преимущества распознавания лица в его быстродействии, в легкости встраивания в более

мелкие устройства, но есть проблемы с распознаванием, когда неправильное освещение, угол наклона камеры, а также уязвим к подделке. У распознавания через радужку преимущества в высокой точности из-за уникальности радужек у людей, но проблема в трудоемкости и дороговизне такой системы, а также массово такую систему тяжело использовать, нежели распознавание через лицо человека. Были также рассмотрены примеры использования таких систем в устройствах и в помещениях.

Библиографические ссылки

1. *Voulodimos A.* Deep learning for computer vision: A brief review // Computational intelligence and neuroscience. 2018. Т. 2018, № 1. Article no. 7068349.

2. *Boyko N., Basystiuk O., Shakhovska N*. Performance evaluation and comparison of software for face recognition, based on dlib and opencv library // Proceedings of the IEEE Second International Conference on Data Stream Mining & Processing (DSMP). 2018. P. 478–482.

3. *Wang A*. Yolov10: Real-time end-to-end object detection // Advances in Neural Information Processing Systems. 2024. Vol. 37. P. 107984–108011.

4. *Omran M., AlShemmary E. N*. An iris recognition system using deep convolutional neural network // Journal of Physics: Conference Series. 2020. Vol. 1530, № 1. Article no. 012159.

5. *Klontz J. C., Jain A. K*. A case study of automated face recognition: The boston marathon bombings suspects // Computer. 2013. Vol. 46, № 11. P. 91–94.