А. Ф. Купин, О. А. Баринова, В. М. Егорова

ИСПОЛЬЗОВАНИЕ СОВРЕМЕННЫХ ПРОГРАММНЫХ СРЕДСТВ РАСПОЗНАВАНИЯ ИЗОБРАЖЕНИЙ В ПРАВООХРАНИТЕЛЬНОЙ ДЕЯТЕЛЬНОСТИ

В статье проанализированы возможности использования программ распознавания образов (лиц, предметов, животных и пр.) для установления обстоятельств совершенного преступления, а также правовые основания их применения. Отмечены два направления получения информации. Первое — данные ресурсов Интернет (в том числе и социальных сетей), второе — изображения, полученные посредством интеллектуальных охранных систем. Отмечается, что техника распознавания изображенных лиц и объектов основана на использовании сверточных нейронных сетей. Приводятся примеры программ, предназначенных для распознавания образов и тренировки нейронных сетей. Делается вывод, что, несмотря на то что многие программы изначально были разработаны в коммерческих целях для осуществления аутентификации пользователей, продаж, либо обеспечения безопасности объектов, они успешно могут быть использованы при производстве оперативно-разыскных мероприятий, а также в качестве образцов при производстве портретных экспертиз в случае их предоставления лицом, назначившим исследование.

Ключевые слова: биометрические характеристики, нейронные сети, Интернет, изображения, распознавание, расследование преступлений

A. F. Kupin, O. A. Barinova, V. M. Egorova

USING OF MODERN SOFTWARE FOR IMAGE RECOGNITION IN LAW ENFORCEMENT ACTIVITY

The article presents an analysis of the possibility of using pattern recognition programs (persons, objects, animals, etc.) to establish the circumstances of the crime. Moreover the article presents legal grounds for the recognition programs using. There are 2 sources of information. The first source — the data obtained from the internet (including social networks), the second — the images obtained using intelligent security systems. It is noted here that the recognition technique is based on the convolutional neural networks using. In addition, the article gives examples of programs that have been developed for pattern recognition and training of neural networks. It is concluded that, despite of the fact that many programs were originally developed for commercial purposes, they can be successfully used during the production of search activities in particular and during the law-enforcement activity in general.

Key words: biometric characteristics, neural network, the Internet, images, recognition, investigation of crimes.

Современная деятельность людей протекает в условиях использования достижений научно-технического прогресса. Так, почти каждый житель мира зарегистрирован в одной или нескольких социальных сетях в Интернете. В них содержатся сведения о личности пользователя: имя, фамилия, телефон, учебное заведение, интересы, а также данные о друзьях. Это позволяет, с одной стороны, людям, находящимся в разных уголках мира, общаться между собой, обмениваться информацией, которая может включать в себя фото- и видеофайлы, с другой — осуществлять поиск лиц по изображениям и их распознавание для установления каких-либо обстоятельств, а также получать сведения о них. Под распознаванием следует понимать способность живых существ обнаруживать определенный объект (образ, предмет, процесс, явление, ситуацию, сигнал) и устанавливать их принадлежность к одному из заранее выделенных классов объектов. Оно может осуществляться путем получения и передачи в мозг зрительной, слуховой, тактильной информации, в котором осуществляется преобразование этих сведений.

Распознавание предметов и лиц в сети Интернет имеет ряд особенностей, среди которых следует выделить:

1) широкое информационное поле сети Интернет, что осложняет ручной поиск идентифицирующих объектов;

2) автоматизированный поиск и распознавание осуществляется путем компьютерных вычислений;

3) большинство информации, в том числе изображения в Интернете, находится в закрытом доступе для обычного пользователя (когда пользователь имеет в социальной сети закрытый профиль).

Кроме того, существенно осложняет поиск сведений в сети Интернет наличие у ряда пользователей вымышленных данных (имя, фамилия и др.). Указанное обстоятельство обусловлено правом человека на анонимность в сети Интернет, которое Организация Объединенных Наций в своем докладе [1] не так давно признала составной частью прав человека. Необходимость его закрепления возникла из-за событий, связанных со скандалом с участием Эдварда Сноудена и Центральным разведывательным управлением США. Таким образом, закон запрещает следить за гражданами, а также осуществлять несанкционированный доступ к их закрытой информации, размещенной в Интернете. Отсюда возникает закономерный вопрос, связанный с этичностью и законностью поиска лиц в сети Интернет в целях их распознавания. Для того чтобы разобраться в этом вопросе, мы обратились к Декларации о свободе общения в Интернете, принятой комитетом Министров Совета Европы (Страсбург, 28 мая 2003 г.), регламентирующей принципы общения в сети Интернет и анонимности. Указанный документ ратифицирован Российской Федерацией. Так, в соответствии с положениями, изложенными в указанной декларации «в целях обеспечения защиты Интернета от контроля и расширения свободного выражения идей и информации государства-члены должны уважать желание пользователей Интернета не раскрывать свою личность. Это не мешает государствам-членам принимать меры и осуществлять сотрудничество в целях установления лиц, виновных в преступных деяниях, в соответствии с национальным законодательством, Конвенцией о защите прав человека и основных свобод и другими международными соглашениями между правоохранительными органами и органами юстиции» [2].

Кроме того, обращает на себя внимание и тот факт, что в настоящее время в процессе регистрации на каком-либо сайте запрашиваются персональные данные: фамилия, имя, серия и номер паспорта, идентификационный номер налогоплательщика, сведения о местоположении пользователя. В соответствии с требованиями Федерального закона «О персональных данных» № 152, ставя галочку в графе «Я согласен на обработку своих персональных данных», пользователь соглашается с их обработкой и передачей по запросам в случае необходимости. Следовательно, согласно положениям названных выше декларации и федерального закона разрешено осуществление поиска информации в сети Интернет для установления лиц, совершивших преступление, и доказывания их причастности к совершенному деянию.

Однако ручной поиск лиц в сети Интернет — трудоемкий процесс, который не всегда позволяет быстро получить нужную информацию, поэтому автоматизация поиска аналогичных изображений является закономерной тенденцией развития в области интеллектуальных компьютерных систем.

Техника распознавания лиц и объектов на изображении основана на использовании *сверточных нейронных сетей* (далее — СНС) [3]. СНС — это технология компьютерного зрения, базирующаяся на восприятии и обработке изображений человеческим мозгом, т. е. прототип зрительной коры головного мозга. Зрительная кора имеет небольшие участки клеток, чувствительные к конкретным областям поля зрения. Например, некоторые нейроны активируются, когда воспринимают вертикальные границы, а некоторые — горизонтальные или диагональные. В совокупности реакция нейронов на возбудители (графические элементы) составляет зрительное восприятие человека. Таким образом, в основе СНС лежит идея специализированных компонентов внутри компьютерной системы, которые в автоматизированном режиме решают конкретные задачи (ищут специфические характеристики изображения).

Алгоритм обработки изображений состоит в пропускании исходного изображения через серию сверточных, нелинейных слоев, слоев объединения и полносвязных слоев. В результате этой обработки формируется вывод, включающий в себя класс, элементы которого имеют некоторые схожие свойства, отличающие его от элементов других классов. Для этого системе программным способом задаются конкретные показатели (указывается набор классифицирующих признаков), характерные для изображения конкретного объекта (рис.1).

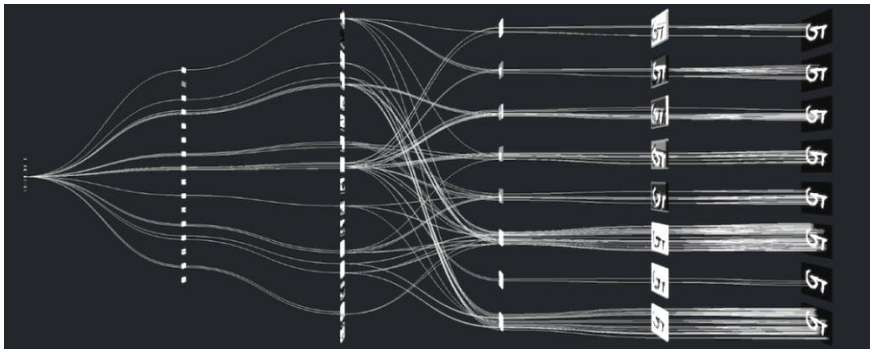

Рис. 1. Общая схема алгоритма работы СНС

После вывода определенного класса, описывающего изображение, осуществляется поиск аналогичных ему образов в имеющейся базе данных изображений. Это могут быть фотографии, субъективные портреты, содержащиеся в сети Интернет или специализированной базе данных криминалистического учета.

В настоящее время существуют несколько специализированных баз данных лиц, которые предназначены в основном для тренировки нейронных сетей. К ним относятся:

1) Labeled Faces in the Wild [4], содержащая 13 000 изображений 5 748 человек;

2) YouTube Faces DB [5], содержащая 3 425 видео 1 595 различных людей.

С помощью этих баз данных осуществляется обучение нейронных сетей для достижения наилучшего результата. Кроме того, системы анализируют биометрические характеристики лица, совокупность контрольных точек, которые подлежат сравнению.

Имеется множество программных средств для распознавания лиц и предметов по изображению как зарубежного, так и отечественного производства, которые изначально были разработаны и использовались в коммерческих целях. Среди зарубежных программ особый интерес представляют:

1) *FaceNet* [6] от компании Google. Эта программа использует технологию СНС и анализ биометрических характеристик. Применяется в основном для идентификации пользователей в целях их аутентификации (входа в свой профиль/почту и т. д.). Отметим, что получение необходимой информации с использованием данного ресурса возможно при наличии веб-камеры, соединенной с компьютерном или смартфоном (рис. 2).

Рис. 2. Пример работы программы FaceNet

2) Amazon Rekognition [7] от компании Amazon. В ее основе лежит применение технологии СНС с глубоким анализом изображений. За счет множества «тегов», которые достаточно точно определяются, это программное обеспечение обладает высокой способностью к распознаванию образов (рис. 3).

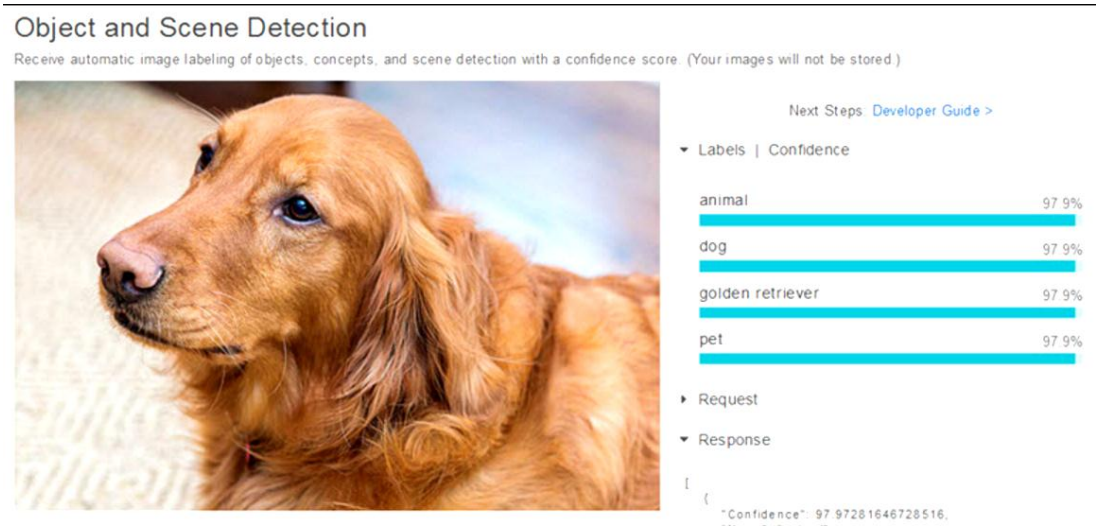

Рис. 3. Пример работы программы Amazon Rekognition

В настоящее время Amazon Rekognition используется преимущественно для подбора аналогичных товаров, поскольку позволяет формировать актуальные предложения для покупателей интернет-магазина Amazon на территории США. Однако если аналог подобной тщательно проработанной системы появится на российском рынке, то его можно будет использовать в процессе расследования преступлений (кражи для отслеживания сбыта краденых вещей через сеть Интернет).

Существуют программы, находящиеся на стадии разработки своих инструментов для распознавания лиц и предметов. Например, компания Yahoo работает над системой *Deep Dense Face Detector* [8], а компания Facebook — над инструментом *DeepFace* [9].

Среди отечественных программных средств распознавания следует выделить:

1. *FindFace Pro* [10] от компании NTechLab, который также работает на основе СНС и анализа биометрических характеристик. Сегодня используется в процессе поиска лиц по изображению в социальной сети «ВКонтакте» (см. рис. 4—5), в том числе правоохранительными органами при расследовании и раскрытии преступлений. Это связано с тем, что, как ранее было сказано, информация, введенная пользователем в процессе регистрации в социальной сети, сохраняется на сервере, и ее практически невозможно скрыть из поисковых запросов. Кроме того, согласно пользовательскому соглашению социальной сети, которое в соответствии с требованиями Федерального закона «О персональных данных» № 152 является обязательным, эти сведения могут распространяться по запросам правоохранительных органов.

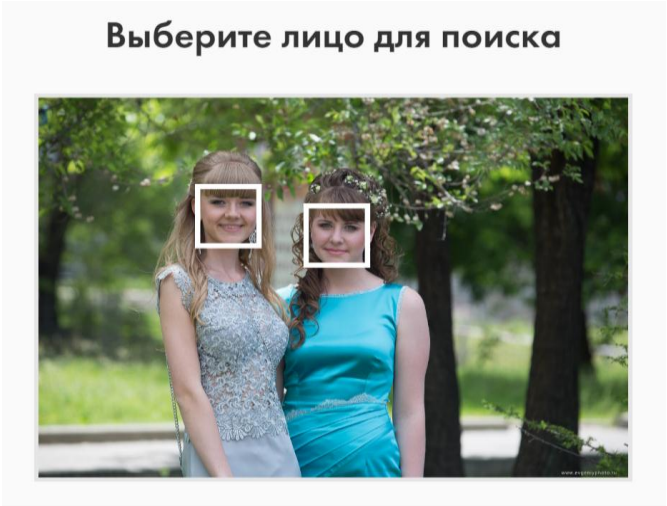

Рис. 4. Этап выбора искомого лица на фотографии средствами FindFace.ru

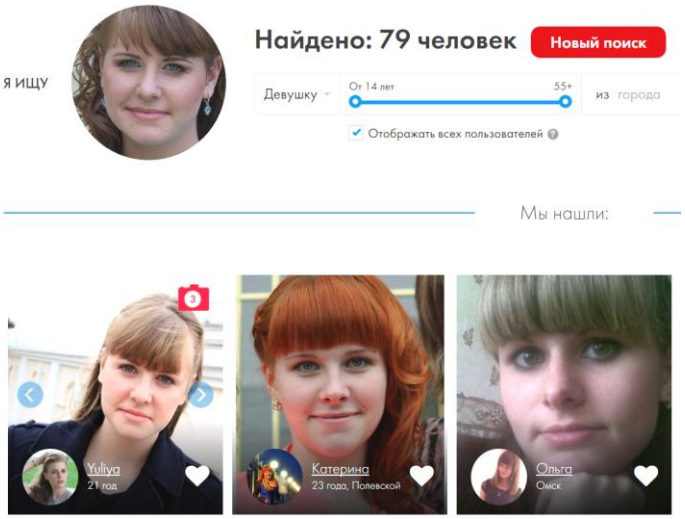

Рис. 5. Результаты поиска средствами FindFace.ru

2. Face-Интеллект [11], входящая в состав Интегрированной системы безопасности «Интеллект». Этот программный продукт сложно назвать средством поиска в сети Интернет, поскольку он представляет собой скорее интеллектуальную охранную систему и, как и предыдущие рассмотренные инструменты Face-Интеллект, работает на основе анализа биометрических характеристик и применения нейронных сетей. Используется для обеспечения безопасности в местах массового скопления людей (метро, вокзалы, аэропорты, торговые центры и т. п.) за счет автоматизации фейс-контроля, необходимого для поиска правонарушителей. Сущность работы программы заключается в том, что изображения лиц, попавших в поле зрения видеокамер, в автоматизированном режиме сохраняются в базу данных и на основании биометрических характеристик сравниваются с содержащимися в ней сведениями. В результате при наличии сходства с правонарушителями создается отчет с данными результатов поиска, включающий статистику его появлений в поле зрения различных камер.

3. Программные средства компании Vocord [12]. К ним относятся*Vocord FaceControl 2D* и *Vocord FaceControl 3D,* которые осуществляют распознавание лиц в реальном времени и используются для обеспечения безопасности объектов. Эти программные продукты имеют сходные характеристики с инструментом Face-Интеллект, однако их особенностью является способность улучшения качества изображения в области лица. Они поставляются в составе программно-аппаратного комплекса, включающего в себя набор камер слежения, которые в совокупности составляют интеллектуальную систему видеонаблюдения с функцией распознавания лиц.

Как видим, рассмотренные программно-аппаратные комплексы способны осуществлять автоматический поиск и распознавание лиц по определенным параметрам, находящимся в базе системы, и включают в себя модули распознавания и модули поиска в видеоархиве. Они способны различать пол, цвет кожи, особенности походки, имеют возможность интеграции в другие программные комплексы.

Кроме рассмотренных программ правоохранительными органами в целях розыска правонарушителей используется программно-аналитический модуль Зеус [13], нацеленный на мониторинг профилей в социальных сетях, включая полный доступ к личным сообщениям и другой информации. Данный аналитический модуль не обладает способностью поиска по изображениям среди фотографий пользователя, но способен формировать базу данных, с которой в последующем может работать Vocord FaceControl.

При наличии сведений о контактах лица (телефон, e-mail, логин Skype), можно установить информацию о нем с помощью поисковой системы Яндекс или Coogle. Для этого необходимо найти данные об искомом субъекте, которые вбиваются в тот же поиск или дополняют существующий запрос. В итоге становится доступной новая информация о пользователе.

В завершение отметим, что большинство существующих сегодня программных продуктов, изначально созданных для аутентификации лиц и предметов в сети Интернет, могут быть использованы при производстве следственных действий для установления лиц, совершивших преступление. К числу таких следственных действий

относится и получение образцов для сравнительного исследования, необходимых для назначения и производства портретных экспертиз. Если на практике получение образцов для сравнительного исследования затруднено, то данные профиля, содержащиеся в сети Интернет, позволят в некоторых случаях установить информацию о наличии у сравниваемых лиц братьев (сестер) близнецов патологических и косметико-хирургических изменений признаков внешности.

Кроме того, информация, содержащаяся в сети Интернет, может быть использована в оперативных целях для собирания сведений о лице, представляющем интерес, и при правильном ее документировании, представлена в качестве доказательств в уголовном, гражданском и арбитражном процессах.

Список библиографических ссылок

1. Kaye D. Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression. URL: https://ru.scribd.com (дата обращения: 24.02.2017).
2. Декларация о свободе общения в Интернете, принятая комитетом министров совета Европы. URL: http://medialaw.asia/document/-2358 (дата обращения: 24.02.2017).
3. Хабрахабр: Что такое сверточная нейронная сеть. URL: https://habrahabr.ru/post/309508/ (дата обращения: 24.02.2017).
4. Labeled Faces in the Wild. URL: http://vis-www.cs.umass.edu/lfw/index.html (дата обращения: 24.02.2017).
5. YouTube Faces DB. URL: https://www.cs.tau.ac.il/~wolf/ytfaces/ (дата обращения: 24.02.2017).
6. Schroff F., Kalenichenko D., Philbin J. FaceNet: A Unified Embedding for Face Recognition and Clustering. URL: https://arxiv.org/pdf/1503.03832.pdf (дата обращения: 24.02.2017).
7. Amazon Rekognition. URL: https://aws.amazon.com/ru/rekognition/ (дата обращения: 24.02.2017).
8. Farfade S. S., Saberian M., Li L.-J. Multi-view Face Detection Using Deep Convolutional Neural Networks. URL: https://arxiv.org/pdf/1502.02766.pdf (дата обращения: 24.02.2017).
9. MIT Technology Review. URL: https://www.technologyreview.com (дата обращения: 24.02.2017).
10. FindFace.Pro. URL: https://findface.pro/ru/ (дата обращения: 24.02.2017).
11. Face-Интеллект. URL: http://www.itv.ru/products/intellect/faceintellect/ (дата обращения: 24.02.2017).
12. Вокорд. URL: http://www.vocord.ru/directions/face_detection/ (дата обращения: 24.02.2017).
13. Главное управление МВД РФ по Свердловской области // Закупка № 016210002131600011. URL: http://zakupki.gov.ru (дата обращения: 24.02.2017).
14. FindFace.ru. URL: https://findface.ru (дата обращения: 24.02.2017).
15. Wen Y., Zhang K., Li1 Z., Qiao Y. A Discriminative Feature Learning Approach for Deep Face Recognition. URL: http://ydwen.github.io/papers/WenECCV16.pdf (дата обращения: 24.02.2017).