Издаётся с 1924 года

РАДИО®

8•2020

МАССОВЫЙ ЕЖЕМЕСЯЧНЫЙ НАУЧНО-ТЕХНИЧЕСКИЙ ЖУРНАЛ

"Радиолюбитель"—"Радиофронт"—"Радио"

"Radio" is monthly publication on audio, video, computers, home electronics and telecommunication

12+

УЧРЕДИТЕЛЬ И ИЗДАТЕЛЬ: ЗАО «ЖУРНАЛ «РАДИО»

Зарегистрирован Министерством печати и информации РФ 01 июля 1992 г.

Регистрационный ПИ № ФС77-50754

Адрес редакции: 107045, Москва, Селивёрстов пер., 10, стр. 1

Тел.: (495) 607-31-18. Факс: (495) 608-77-13

E-mail: **ref@radio.ru**

Группа работы с письмами — (495) 607-08-48

Отдел рекламы — (495) 607-31-18; e-mail: **advert@radio.ru**

Распространение — (495) 607-77-28; e-mail: **sale@radio.ru**

Подписка и продажа — (495) 607-77-28

Бухгалтерия — (495) 607-87-39

Наши платёжные реквизиты:
получатель — ЗАО "Журнал "Радио", ИНН 7708023424,
р/сч. 40702810438090103159
Банк получателя — ПАО Сбербанк г. Москва
корр. счёт 30101810400000000225 БИК 044525225

Подписано к печати 25.06.2020 г. Формат 60×84 1/8. Печать офсетная.

Объём 8 физ. печ. л., 4 бум. л., 10,5 уч.-изд. л.

В розницу — цена договорная.

Подписной индекс:

Официальный каталог ПОЧТА РОССИИ — П4014;

КАТАЛОГ РОССИЙСКОЙ ПРЕССЫ — 89032.

Отпечатано в ОАО «Подольская фабрика офсетной печати»
142100, Моск. обл., г. Подольск, Революционный проспект, д. 80/42.
Зак. 02113-20.

Открытые лица

А. ГОЛЫШКО, канд. техн. наук, г. Москва

"— Мало ли на свете людей, похожих друг на друга...".

— Да, но есть лица, которые никогда не забываются".

(Эрих Мария Ремарк. "Триумфальная арка")

Казалось бы, лишь совсем недавно компьютерная программа научилась отличать изображение собаки от изображения человека, и вот уже речь идёт о точной идентификации человека по его лицу, где бы и в чём бы этот человек ни находился. Распознавание лиц (face recognition) уже используется как для блокировки смартфонов, так и для обеспечения национальной безопасности. Технологических реализаций также немало — от систем на основе IP-камер с функцией встроенного видеоанализа до серверных и облачных решений.

С появлением мощных компьютеров практически все ведомства возвращаются к идентификации посредством сканирования лица. Бум на технологию в ведомствах и спецучреждениях по всему миру пришёлся на середину 2000-х годов. В наши дни популярность технологии распознавания лиц в разных сферах деятельности продолжает расти. К примеру, Сбербанк — один из лидеров в части анонсирования различных громких проектов face recognition. Теперь он узнает тебя из тысячи. Банкомат с идентификацией лиц не даст злоумышленникам снимать деньги с чужих карт. С той же целью банк объявил сбор биометрических данных (аудиозапись голоса, видеозапись лица) клиентов. За 2018 год финансовое учреждение успело протестировать face recognition в московском метро и даже оперативно поймать 42 преступника.

Китай на данный момент можно назвать лидером по эффективности использования камер видеонаблюдения и поиска людей с их помощью, а также в области распознавания лиц полицейскими с помощью специального оборудования. В декабре 2017 г. корреспондент BBC доказал это с помощью эксперимента, в котором его фото внесли в базу, придав ему статус подозреваемого. Полиция в течение 7 мин нашла его в городе с населением 4 млн человек.

За миллионами камер стоит система распознавания лиц и объектов, которая одновременно следит за огромным количеством граждан и гостей страны, передвижением транспортных средств. Эта же система определяет друзей и близких человека исходя из их встреч. В стране работают почти 200 млн камер наблюдения, из которых более 20 млн — новейшие устройства с искусственным интеллектом (ИИ), разработанные в рамках операции Sky Net по поиску коррупционеров, подпольных банков и других преступников.

В апреле 2017 г. для борьбы с неаккуратными пешеходами в китайском Шэньчжене на них устроили охоту с помощью камер и информационных табло. Информация о них сохраняется в базе и выводится на экран вместе с историей подобных проступков. Весной 2018 г. систему решили улучшить — не просто размещать фото на экране, а добавлять к этому отправку изображения в мессенджер. Однажды китайские полицейские поймали подозреваемого в совершении экономических преступлений за 90 км от города, в котором он скрывался, распознав его в очереди на концерт с 50 тыс. зрителей. После ареста подозреваемый сказал, что не рискнул бы на подобную вылазку, если бы

подозревал о реальных возможностях действующей в стране системы распознавания лиц.

Несмотря на случающиеся промахи, точность машинного распознавания уже нередко превосходит ту, с какой определяют лица люди. В Китае взят курс на систему, способную найти конкретного человека среди 1,3 миллиарда других жителей за 3 секунды с точностью 90 %.

Китайские компании активно внедряют технологию распознавания лиц и в финансовых областях. Финансовый гигант Ping An начал использовать собственную технологию распознавания лиц ещё в 2016 г. в подразделении потребительского кредитования. Технология улавливает еле заметные непроизвольные движения лица, позволяя выявлять мошенников, и сокращать убытки от выдачи кредитов. Технологию стали использовать и банки, тем более что она позволяет выдавать займы там, где у них нет отделений.

При выдаче крупных кредитов Ping An просит заёмщиков пройти онлайн-видеоинтервью продолжительностью до 15 мин. Компания записывает и анализирует ответы, пытаясь выявить признаки подозрительного поведения. Более года назад Ping An сообщала, что с помощью этой технологии уже выдала займы более чем на 500 млрд юаней, сократив среднее время одобрения кредитов с пяти дней до двух часов. Когда клиенты обращаются к Ping An первый раз, компания требует предоставить удостоверение личности с фотографией и снимает их лица, прося совершить некоторые движения, например, открыть рот или поморгать. Затем клиенты могут приобретать страховые продукты онлайн, сканируя лицо смартфоном, или связываться с агентами Ping An по видеосвязи. Технология помогает также Ping An оценить состояние здоровья. Сканирование лица позволяет оценить индекс массы тела человека и понять, обладает он избыточным или недостаточным весом. В зависимости от результата клиент может получить скидку на полис, предполагающий выплату до 1 млн юаней в случае тяжёлого заболевания. В Китае вообще очень популярна физиогномика, т. е. определение по лицу и его выражению типа личности, душевных качеств, состояния здоровья человека.

Интерес к распознаванию лиц логично возник из-за потенциальных выгод. Распознаванием лиц давно интересуются компании Google, Facebook, Apple и прочие IT-гиганты. Соответственно они занимаются активной скупкой подобных проектов:

2012 год. Google покупает разработчика приложения для распознавания лиц PittPatt. В том же году компания выделяет 45 млн долл для поглощения украинской компании Viewdle, занимающейся системами автоматического распознавания лиц.

2012 год. Facebook поглощает сервис по распознаванию лиц на фотографиях Face.com. Предположительная сумма сделки — около 100 млн долл.

2017 год. Apple покупает израильскую компанию RealFace, специализирующуюся на распознавании лиц. Стоимость сделки составила около 2 млн долл.

А что у нас? В РФ в середине 2016 г. случился взлёт приложения и одноименного сервиса FindFace. Используя нейронные сети, разработчики сумели воплотить в жизнь самую смелую мечту пользователей социальных сетей. Увидев человека на улице, вы могли сфотографировать его на смартфон, отправить фото в FindFace и через несколько секунд найти его страничку во "ВКонтакте". Алгоритм совершенствовался и всё лучше и лучше распознавал лица. А начиналось всё с распознавания пород собак по фотографии с помощью технологии распознавания FaceN и приложения Magic Dog.

После успеха приложения FindFace выяснилось, что распознавание лиц интересно практически в любой отрасли: пограничные службы, казино, аэропорты, любые места скопления людей, торговые площадки, парки развлечений и, конечно, у спецслужб.

В мае 2016 г. компания N-Tech.Lab приступила к тестированию сервиса совместно с правительством Москвы. По всей территории столицы разместили десятки тысяч камер, которые в режиме реального времени опознавали прохожих. И теперь вы просто проходите по двору, в котором установлена подобная камера. К ней подключена база преступников и пропавших людей. В случае, если алгоритм определяет, что вы схожи с подозреваемым, сотрудник полиции тут же получает предупреждение.

Разумеется, человека тут же можно найти в социальной сети и "пробить" по любым базам. А теперь представьте, что такие камеры установлены по периметру всего города. Скрыться злоумышленнику не удастся. Камеры есть везде, во дворах, на подъездах, на трассах. Впрочем, умерим оптимизм, не с каждой видеокамеры можно получить качественное распознавание лиц. Важно определённое разрешение, важна высота подвеса камеры. Как минимум лицо нужно увидеть. Впрочем, технологии распознавания непрерывно совершенствуются, и, к примеру, недавно сообщалось о разработке алгоритма, позволяющего распознавать людей в антивирусных масках.

На сегодняшний день только на подъездах московских многоэтажек установлено более 100 тысяч камер, умеющих распознавать лица. Более 25 тысяч установлены во дворах. Разумеется, точные цифры засекречены, но можете не сомневаться — активный контроль распространяется быстрее, чем вы можете себе представить. В целом в Москве системы распознавания лиц устанавливаются повсеместно, от площадей и мест большого скопления людей до общественного транспорта. Все камеры постоянно обмениваются информацией с Единым вычислительным центром Департамента информационных технологий Правительства Москвы. Подозрительные оповещения тут же проверяются правоохранительными органами. Только за время тестирования систем видеоаналитики МВД задержало 90 человек в Москве благодаря тысяче камер на жилых домах. Также полиции удаётся задерживать от пяти до десяти человек в месяц с помощью камер на нескольких станциях метро.

Прообразом технологии распознавания лиц в XIX веке служили сначала "портреты по описанию", а позже — фотографии. Так полиция могла идентифицировать преступников. В 1965 г. специально для правительства США была разработана полуавтоматическая система распознавания лиц. В 1971 г. к этой технологии вернутся, обозначив основные маркеры, необходимые для распознавания лиц, но ненадолго. С тех пор в качестве главного биометрического идентификатора спецслужбы всё же предпочитают проверенную технологию снятия отпечатков пальцев.

С появлением мощных компьютеров практически все ведомства возвращаются к идентификации посредством сканирования лица. Бум на технологию в ведомствах и спецучреждениях приходится на середину 2000-х годов, а в прошлом году технология стала впервые использоваться и в потребительских устройствах.

Учитывая сложность алгоритмов и высокую цену на серверное оборудование, системы распознавания лиц долгое время оставались недешёвым удовольствием. Дополнительно на стоимость решения влияет генерируемый в процессе работы большой сетевой трафик. Помимо затрат на мощные серверы приходилось инвестировать в активное сетевое оборудование и широкополосные каналы связи.

Существует несколько методов, по которым работают системы распознавания лиц, но в целом речь идёт о технологии, способной идентифицировать человека по цифровому изображению или кадру из видеоисточника. Первое, что должна сделать система, — выделить в кадре лицо и с помощью алгоритмов убедиться, что это именно человеческое лицо.

После первоначального детектирования происходит определение различных индивидуальных черт по фиксированным точкам — например, учитывается расстояние между глазами (это умеют делать сотрудники паспортного контроля) и ещё десятки других параметров лица, которые для быстрого сравнения человеку физически недоступны. Далее уже другие алгоритмы ищут по различным заранее созданным базам данных и выдают процент схожести с искомым образцом данных. Если процент схожести достаточно высок, лицо считается распознанным.

Собственно, распознавать можно по-разному. В основе наиболее массовой на сегодня технологии 2D (двумерного) распознавания лиц, лежат плоские двухмерные изображения. Алгоритмы распознавания лиц используют антропометрические параметры лица, графы-модели лиц или эластичные 2D-модели лиц, а также изображения с лица-

ми, представленные некоторым набором физических или математических признаков. Основные базы данных идентифицированных лиц, накопленные в мире, — именно двухмерные. Огромным преимуществом 2D-распознавания лиц является наличие готовых баз данных лиц эталонов и готовой инфраструктуры. К недостаткам относятся высокие коэффициенты ошибок FAR и FRR по сравнению с 3D-распознаванием лиц.

FAR (False Acceptance Rate) — вероятность несанкционированного допуска (ошибка первого рода), выраженное в процентах число допусков системой неавторизованных лиц (имеется в виду верификация). Вероятностные параметры выражаются в абсолютных величинах (10^{-5}), для параметра FAR это означает, что один человек из 100 тысяч будет несанкционированно допущен, в процентах это значение будет 0,001 %.

FRR (False Rejection Rate) — вероятность ложного задержания (ошибка второго рода), выраженное в процентах число отказов в допуске системой авторизованных лиц (имеется в виду верификация).

3D-распознавание (Three-dimensional face recognition) производится, как правило, по реконструированным трёхмерным образам. Технология имеет более высокие качественные характеристики. Хотя, конечно, и она не является идеальной. Существует несколько разнообразных технологий 3D-сканирования. Это могут быть лазерные сканеры с оценкой дальности от сканера до элементов поверхности объекта, специальные сканеры со структурированной подсветкой поверхности объекта и математической обработкой изгибов полос, либо это могут быть сканеры, обрабатывающие фотограмметрическим методом синхронные стереопары изображений лиц.

Одним из наиболее исследованных потребителями и экспертами 3D-сканеров является знаменитый Face ID от компании Apple. Опыт использования Face ID крайне интересен и показателен, потому что до недавнего времени, по сути, это было единственное устройство с технологией 3D-распознавания лиц, выпущенное на массовый рынок. 3D-технология от Apple единственная в мире использует вертикально-излучающие лазеры (VCSEL), по слухам, суммарно потрачено на разработку Face ID от 1,5 до 2 млрд долл. Поставщиком VCSEL для Apple выступают две компании — Finisar Corp и Lumentum Holdings.

Разумеется, идеального ничего не бывает. "Моментом истины" для face recognition является, например, задача идентификации близнецов. А вот с нею Face ID, оказывается, не справляется, хотя этого никто и не ожидал. В среднем в мире рождается 13,1 близнецов на 1 тыс. новорождённых, и эта цифра сильно колеблется в зависимости от географического региона. Впрочем, ошибки встречаются даже с близкими родственниками. Так что работа продолжается. Кстати, поначалу Face ID не различал уроженцев Азии, но проблему настолько быстро решили, что компании Apple даже не успели вчинить ни одного иска за расизм (страшно представить, во что бы это вылилось в наши дни).

В целом преимуществом систем 3D является большая точность и меньшее количество ошибок, пока недостижимое для 2D-систем распознавания лиц. Однако выяснилось, что 3D достаточно легко подделать для профессионалов. Даже столь непростой Face ID был взломан вьетнамской компанией Bkav сразу после поступления в продажу. Маска была создана профессионалами с помощью 3D-принтера, а себестоимость её создания оказалась всего 150 долл.

В общем, не рекомендуется использовать 3D-распознавание лиц для защиты от несанкционированного доступа к ноутбукам, смартфонам, помещениям с особым уровнем секретности, все они могут быть с лёгкостью взломаны профессионалами. А ещё 3D-распознавание требует специальных камер для сканирования, которые в несколько раз дороже обычных камер видеонаблюдения, которые используются в 2D-распознавании. Отсутствие готовых баз данных идентифицированных лиц по сравнению с 2D-распознаванием — ещё одна проблема 3D-систем. Ну а по поводу распознавания близнецов уже упоминалось выше. Так что же делать?

Можно, к примеру, проводить распознавание лиц по текстуре кожи лица. Изображения с высоким разрешением — ещё один фактор в совершенствовании технологии распознавания лиц, когда стал возможен очень подробный анализ текстуры кожи. При таком анализе определённая область кожи лица может быть захвачена как изображение, а затем разбита на более мелкие блоки, которые превращаются в математические измеримые пространства, в которых записываются линии, поры и фактическая текстура кожи. Технология может идентифицировать различия между близнецами. В случае объединения распознавания лица с анализом поверхностной текстуры точность идентификация может сильно увеличиться.

Использование тепловизионных камер для целей распознавания лиц на данный момент считается ещё одним перспективным направлением для разработки, однако готовых для внедрения коммерческих решений пока нет. Зато есть коммерческий потенциал, поскольку такие системы позволяют распознавать лица в полной темноте и в условиях недостаточного освещения. Макияж, причёска, борода, шляпа, очки не являются проблемой для тепловизионных камер, с помощью которых можно распознавать близнецов. Не секрет, что пандемия вируса нанесла определённый удар по face recognition, обязав всех граждан ходить в масках. Идентификация может производиться по заранее созданным термограммам определённых лиц. Правда, здесь проблемы те же, что и с 3D-распознаванием, — готовых баз эталонов нет, а оборудование дорогое. Можно вести идентификацию человека по изображениям, полученным с тепловизионной камеры, а в качестве лиц эталонов использовать базу данных обычных 2D-изображений. Решается такая задача с использованием глубоких нейронных сетей.

Впрочем, распознавание лиц по текстуре кожи и по тепловизионному изображению пока работает только в лаборатории, и то неидеально. Но ведь это пока...

Для качественной работы технологии распознавания лиц нужно несколько составляющих. Во-первых, сам сервер, на котором будут храниться и база данных, и подготовленный алгоритм сравнения. Во-вторых, продуманная и натренированная нейросеть, которой "скормили" миллионы снимков с пометками. Обучают такие сети простым перебором базы данных изображений. Загружают снимок и представляют его системе — "это Пётр Николаев", затем следующий. Нейронная сеть самостоятельно распределяет векторы признаков и находит геометрические закономерности лица таким образом, чтобы затем самостоятельно узнать Петра из тысяч других фотографий.

Далее основная сложность решения на данный момент заключается не в самих технологиях (алгоритмах), а в реализации. Системы распознавания развиваются в нескольких направлениях, классифицируемых в зависимости от подхода к обработке информации. Подчас трудно выбрать, какая именно система лучше справится с конкретной задачей.

Данные можно обрабатывать в облаке, на локальных серверах, развёрнутых в периметре безопасности предприятия, или непосредственно на камерах. В последнем случае весь анализ осуществляется самой камерой, а на сервер поступает уже обработанная информация. Главное достоинство системы — это высокая точность и возможность подключить к одному серверу большое число устройств. При кажущейся простоте и лёгкости масштабирования у этой технологии тоже есть минусы. Один из них — высокая цена. Плюс к этому, на данный момент нет единого стандарта представления информации, которую специализированные камеры передают на сервер. И набор данных может сильно различаться у разных поставщиков решений.

Идентификация лиц в реальном времени и реальных условиях неразрывно связана с системами видеонаблюдения, где лица буквально выхватываются из снимаемого камерами видеопотока. Представим себе качественную современную камеру видеонаблюдения, размещённую чуть выше среднего человеческого роста в хорошо освещённом месте. Перед ней каждый день проходит примерно одинаковое количество примерно одних и тех же людей. Двигаются они не очень быстро. Снятое видео может храниться в облачном архиве. К камере подключается аналитический модуль — сложное сочетание алгоритмов плюс поль-

зовательский интерфейс. Модуль выхватывает лица из видеопотока, определяет пол, возраст и заносит данные в базу. Постепенно изображений становится больше. Система запоминает все распознанные лица автоматически и заносит их в архив, а пользователь с допуском указывает дополнительные данные: имя, должность, статус и прочие отметки (VIP-гость или вор). Можно загрузить фото нужной персоны, а модуль найдёт в архиве все фиксации этого лица. Как только человек с отметкой вновь проходит перед камерой, система фиксирует это как важное событие и отправляет уведомление заинтересованным пользователям.

Можно ли обмануть алгоритм распознавания лиц? Однозначно на этот вопрос ответить сложно, потому что единственного идеального алгоритма распознавания лиц не существует, а защищаться сразу от всех существующих вряд ли возможно. Большие очки, наклеенная борода, кепка, высокая скорость перемещения, специальный макияж (например, нарисованная на лице решётка, котики, кружочки, палочки и пр.) — всё это способно запутать алгоритмы, причём особенно в совокупности применения. Но в условиях большого города подобным персонажем заинтересуются первые же встречные патрульные полицейские.

Вероятно, в будущем сфера распознавания лиц в системах видеонаблюдения будет регулироваться аналогично текущей практике работы с идентификацией лиц в Интернете. Учитывая развитие технологий, пора закреплять собственное изображение соответствующим патентом и давать разрешение на его использование за плату. Ну а стремящиеся к конфиденциальности люди никуда не денутся, они не загружают в Сеть лишнего.

В мае 2019 г. президент Владимир Путин поддержал стратегию развития ИИ в России. Центром экспериментов должна стать Москва. Среди прочего власти столицы вместе с МВД планируют установить в городе до 200 тыс. камер с технологией распознавания лиц. Что дальше?

Далее, очевидно, везде...

По материалам ***yandex.ru, lifehacker.ru, securityrussia.ru, sigma-is.ru, vedomosti.ru, habr.com, The Wall Street Journal***

Приём статей: mail@radio.ru
Вопросы: consult@radio.ru