Дмитрий Швецов

Основные тенденции развития технологии распознавания лиц

В статье рассмотрены мировые тенденции развития технологии распознавания лиц, которые формируют ландшафт рынка биометрии в 2020 году. В обзоре приведён перечень лучших технологий и провайдеров распознавания лиц, описано влияние искусственного интеллекта на методы идентификации, сделан обзор рынков и доминирующих сценариев использования технологий в 2019–2024 годах. Лучшие инструменты распознавания лиц разработаны и внедрены в Китае, Индии, США, ЕС, Великобритании, Бразилии, России. Представлены современные требования к системам безопасности и к соблюдению конфиденциальности биометрических данных, рассмотрены уязвимости технологий распознавания лиц для взлома и переход к гибридным решениям.

Как работают методы распознавания лица

Распознавание лица – это процесс идентификации или проверки личности человека по его лицу. В основе метода лежат следующие технологии: захват лица, анализ и сравнение модели по основным характерным точкам лица человека.

На сегодняшний день он считается самым естественным из всех биометрических измерений.

Метод раскладывается на следующие основные этапы.

1. Обнаружение лица – анализ видеопотока или изображения для выявления человеческих лиц.
2. Захват лица – преобразование аналоговой информации (лица) в набор цифровых данных на основе алгоритмов определения и оцифровки характерных черт лица человека.
3. Сопоставление лиц – автоматическая проверка принадлежности двух лиц (первого – выявленного при обнаружении, второго – хранящегося в базе данных) одному и тому же человеку.

Данные распознавания лиц для идентификации и проверки

Биометрическая технология применяется для идентификации и аутентификации человека с использованием данных, уникальных и специфических для этого человека. Прежде чем идти дальше, давайте определимся с терминами «идентификация» и «аутентификация».

Идентификация отвечает на вопрос: «Кто вы?»

Аутентификация отвечает на вопрос: «Вы действительно тот, кем себя называете?»

Далее приведём несколько примеров этапов реализации технологий распознавания лиц.

1. В случае анализа биометрических данных лица 2D- или 3D-камера захватывает и фиксирует изображение лица. Затем проводится преобразование аналоговых данных захваченного изображения с применением алгоритма преобразования в цифровые данные для последующего сравнения с оцифрованными шаблонами изображений, хранящихся в базе данных.
2. Автоматизированные системы позволяют проводить идентификацию или проверку личности людей всего за несколько секунд на основе оцифрованных шаблонов их характерных черт лица, таких как расстояние между глазами, переносица, контур губ, ушей, подбородка и т.п.
3. Распознавание лиц может проводиться среди толпы в динамичных и нестабильных условиях. Примером этого могут служить показатели, полученные благодаря системе идентификации лиц в реальном времени (LFIS) Gemalto, алгоритмы которой основаны на многолетнем опыте в области биометрических технологий.
4. Владельцы iPhone X уже знакомы с технологией распознавания лиц. Тем не менее биометрическое решение Face ID, разработанное Apple, было подвергнуто резкой критике в Китае в конце 2017 года из-за его неспособности провести различие между некоторыми лицами китайских граждан.

© Алексей Попов | Dreamstime.com

Рис. 1. Применение технологии OpenFace с открытым исходным кодом

Piyamas Dulmunsumphun | Dreamstime.com

Рис. 2. Визуализация этапов проведения «живого» тестирования систем распознавания лиц

Почему требуется распознавание лиц?

Конечно, существуют и другие сигнатуры человеческого тела, такие как данные отпечатков пальцев, сканирования радужной оболочки глаза, распознавания голоса, оцифровки вен ладони, и информация, полученная в результате внедрения технологий, основанных на анализе поведения людей. Распознавание лиц продолжает оставаться предпочтительным методом биометрической идентификации человека, потому что систему на его основе легко развернуть и внедрить, а пользователю не требуется никакого физического взаимодействия с объектом. К тому же все процессы обнаружения и сопоставления лиц для проверки и/или идентификации выполняются очень быстро.

Лучшие технологии распознавания лиц

Итак, что же является лучшим программным обеспечением для распознавания лиц? В гонке за биометрическими инновациями несколько крупных мировых проектов претендуют на первое место. Все веб-гиганты в области программного обеспечения: Google, Apple, Facebook, Amazon и Microsoft (GAFAM) – регулярно публикуют свои теоретические открытия в области искусственного интеллекта, распознавания изображений и анализа лиц, пытаясь как можно быстрее расширить наше понимание методов. Самые последние результаты испытаний, проведённых в марте 2018 года Управлением по науке и технике Министерства внутренней безопасности США и известных как «Ралли биометрических технологий», также являются хорошим источником для анализа программного обеспечения распознавания лиц, доступного на рынке.

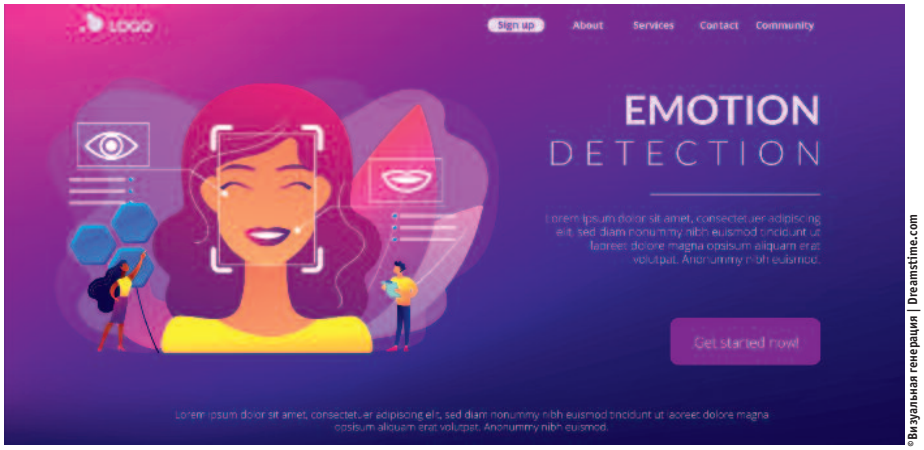
Давайте внимательнее посмотрим на методы распознавания лиц. Так, в 2014 году компания Facebook снова объявила о запуске своей программы DeepFace, которая может определить, принадлежат ли два сфотографированных лица одному и тому же человеку, с точностью до 97,25%. При проведении того же теста с людьми правильные ответы получали в 97,53% случаев, что на 0,28% лучше, чем это делает программа Facebook. В июне 2015 года возможности пакета программного обеспечения FaceNet от Google позволили достичь более высоких показателей. Широко используемый метод в наборе данных «Помеченные лица в дикой природе» (LFW) FaceNet установил новый рекорд точности – 99,63% (0,9963 ± 0,0009). Используя искусственную нейронную сеть и новый алгоритм, разработчики компании из Маунтин-Вью смогли связать изображение лица с его владельцем с почти идеальными результатами.

Эта технология включена в Google Фото и используется для сортировки изображений с пометками на лицах узнанных людей. Доказав свою значимость в биометрической среде, разработчики выпустили неофициальную онлайн-версию с открытым исходным кодом, известную как OpenFace. На рис. 1 представлено одно из многих применений технологии распознавания лиц на базе OpenFace.

Исследования, проведённые специалистами Массачусетского технологического университета (MIT) в феврале 2018 года, показали, что инструменты программных технологий распознавания лиц Microsoft, IBM и Megvii (FACE ++), применяемые в Китае, имеют высокую степень повторяемости ошибок при идентификации женщин с более тёмной кожей по сравнению с мужчинами со светлой кожей. И уже в конце июня 2018 года компания Microsoft объявила в своём блоге, что внесла существенные улучшения в алгоритмы распознавания лиц, которые позволяют избежать подобных ошибок. В свою очередь, в мае 2018 года специалисты компании Ars Technica сообщили, что Amazon уже активно продвигает свой облачный сервис распознавания лиц под названием Rekognition для правоохранительных органов. В пресс-релизе указывалось, что данный сервис в состоянии распознавать до 100 человек, попавших в один кадр, и может сопоставлять лица с базами данных, содержащими десятки миллионов лиц. Но в июле в Newsweek появилось сообщение, что технология распознавания лиц Amazon неверно определила 28 членов Конгресса США как людей, арестованных за преступления.

Основные поставщики биометрических технологий

В конце 2018 года Управление по науке и технике Министерства внутренней безопасности США опубликовало результаты исследований, проведённых в Мэрилендском испытательном центре (MdTF). Исследования проводились на специальном стенде, представляющем собой коридор размером 2×2,5 м, с реальной нагрузкой и тестированием всех 12 программных платформ с установленными на них системами распознавания лиц по фиксированной методике оценки производительности. Решение Gemalto, использующее программное обеспечение для распознавания лиц (LFIS), дало отличные результаты: коэффициент распознавания лица составил 99,44% менее чем за 5 секунд (средний показатель у других производителей – 68%), а показатель истинной идентификации поставщика – 98% менее чем за 5 секунд, по сравнению с другими усреднёнными значениями в 66%, и уровень ошибок 1% по сравнению со средней величиной 3,2%. На рис. 2 представлен один из функциональных экранов приложения, используемого



©Визуальная генерация | Dreamstime.com

Рис. 3. Иллюстрация метода выделения лица и распознавания эмоций

для проведения «живого» тестирования. Оно выполнялось с участием более 300 добровольцев, и в результате были выявлены наиболее эффективные технологии распознавания лиц.

Более подробные данные о тестах производительности приведены в отчёте NIST (Национальный институт стандартов и технологий США), опубликованном в ноябре 2018 года, там содержатся данные о точности и скорости распознавания лиц для 127 алгоритмов разработчиков.

Обнаружение и распознавание эмоций на лице

Распознавание эмоций (на базе статических изображений, захваченных из видеопотока в реальном времени) – это процесс картирования выражений лица (face mapping) с помощью программного обеспечения обработки изображений для выявления эмоций на лице человека, таких как отвращение, радость, гнев, удивление, страх или грусть. На рис. 3 приведена иллюстрация метода распознавания эмоций, который получил популярность в первую очередь из-за частого использования для маркетинговых целей и затем стал использоваться более широко в других отраслях. Отличие метода распознавания эмоций от распознавания лица состоит в том, что во втором случае основная цель – идентифицировать человека, а не эмоцию на его лице. Определение выражения лица или эмоций производится после захвата лиц из видеопотока, а далее они представляются геометрическими фигурами, извлечёнными из преобразованных изображений, таких как селфи, динамические и 3D-модели. Среди провайдеров этих технологий наиболее известны Kairos (распознавание лиц и эмоций для маркетинговых целей продвижения бренда), Noldus, Affectiva, Sightcorp, Nviso и другие.

Повышение «интеллекта» через углублённое обучение

Функция обучения, одна из самых важных в технологиях распознавания лиц, наиболее известна как искусственный интеллект (AI), а если точнее, глубокое обучение, когда система способ-

на учиться на основе собранных данных. Способность к обучению является главным компонентом алгоритмов последнего поколения, который хранит в себе «секретный метод» обнаружения, отслеживания и сопоставления лиц. Также подобные алгоритмы имеют встроенные системы распознавания речи и перевода разговоров в режиме реального времени. Благодаря этим особенностям системы распознавания лиц становятся всё лучше и лучше. Согласно недавнему отчёту NIST за последние 5 лет (2014–2019 гг.) достигнут значительный прирост точности распознавания лиц, который превышает показатели, достигнутые в период 2010–2013 гг. Большинство алгоритмов распознавания лиц в 2019 году уже обгоняют самый точный алгоритм конца 2013 года. В тесте NIST выявлено, что 0,2% поисковых запросов в базе данных с 26,6 млн фотографий не смогли найти правильное изображение по сравнению с 4% ошибок в 2014 году. Это 20-кратное улучшение, достигнутое за четыре года. Алгоритмы искусственной нейронной сети помогают технологии распознавания лиц становиться всё более точной.

Рынки систем распознавания лиц

Согласно данным исследования, опубликованного в июне 2019 года, к 2024 году мировой рынок распознавания лиц будет приносить $7 млрд дохода при совокупном годовом росте (CAGR) в 16% за период 2019–2024 гг. Например, к 2019 году рынок оценивался в $3,2 млрд. Двумя основными факторами этого роста являются контроль безопасности в государственном секторе и множество других приложений для различных сегментов рынка. Благодаря этому исследованию были определены ведущие поставщики систем распознавания лиц, такие как Accenture, Aware, BioID, Certibio, Fujitsu, Fulcrum Biometrics, Gemalto, HYPR, Idemia, Leidos, M2SYS, NEC, Nuance, Phonexia и Smilepass.

Приложения распознавания лиц можно распределить на три ключевые категории.

1. Системы безопасности для правоохранительных органов

Этот рынок испытывает высокие темпы роста в связи с возросшей активностью в борьбе с преступностью и терроризмом. Преимущества систем распознавания лиц для полиции очевидны, с их помощью можно выявлять правонарушителей и предотвращать преступления. Правоохранительные органы используют технологии распознавания лиц при выдаче документов, удостоверяющих личность, и чаще всего в сочетании с другими биометрическими данными, такими как отпечатки пальцев. Сопоставление лиц используется при прохождении пограничного контроля для сравнения фотоизображения на цифровом биометрическом паспорте с лицом владельца. Биометрическая технология распознавания лиц также может использоваться полицией для проверок, хотя в Европе её применение строго контролируется. В 2016 году «человек в шляпе», ответственный за теракты в Брюсселе, был найден благодаря программному обеспечению распознавания лиц ФБР. Полиция Южного Уэльса провела эту операцию на финале Лиги чемпионов УЕФА в 2017 году.

В США в 30 штатах разрешают правоохранительным органам проводить поиск в своих базах данных водительских прав и удостоверений личности с фотографиями. ФБР имеет доступ к фотогра-

фиям водительских прав из 18 штатов. Специализированные дроны с установленными на них мобильными камерами позволяют во время массовых мероприятий на больших площадях сочетать технологии распознавания лиц и, например, анализ неадекватного поведения двух и более граждан. Так, согласно данным из журнала Keesing Journal of Documents and Identity за июнь 2018 года, некоторые системы парящих беспилотников могут нести камеры с хорошим объективом весом до 10 кг, при этом система может опознать подозреваемого на расстоянии 800 м с высоты 100 м. Специализированные дроны могут быть с беспроводной передачей данных и с аккумуляторным питанием, а также с проводным подключением через кабель питания к вычислительным средствам оператора на земле. В таком случае дрон становится устройством с неограниченным временем автономной работы. Связь с пунктом наземного управления не может быть перехвачена, поскольку для передачи данных также используется кабель.

2. Системы для здравоохранения

Значительные успехи были достигнуты в области здравоохранения. Благодаря применению методов глубокого обучения и анализа лиц теперь стало возможно:

- более точно контролировать приём лекарств пациентом;
- обнаруживать генетические заболевания, такие как синдром делеции 22q11.2 (DS 22q11.2), с вероятностью до 96,6%;
- поддерживать процедуры лечения и обезболивания.

3. Инструментарий для маркетинга и розничной торговли

Использование технологии распознавания лиц в этой области, безусловно, было наиболее ожидаемым. Впервые её применение произошло в торговле, и одной из самых «горячих» тем в 2020 году станет «Знай своего клиента» (KYC). Эта важная тенденция в торговле сочетается с последними достижениями маркетинга в сфере обслуживания клиентов. Благодаря установленным в торговых точках камерам можно анализировать поведение покупателей и улучшать процесс их обслуживания. Например, недавно разработанная сотрудниками Facebook аналитическая система позволяет служащим отдела продаж формировать квалифицированные предложения покупателям на основе информации, полученной из их профилей в социальных сетях. Американский универмаг Saks Fifth Avenue уже несколько лет использует такую систему, а судя по сообщениям в СМИ, магазины Amazon GO тоже стали применять этот метод. В китайской розничной сети, начиная с 2017 года в KFC в Ханчжоу, технологический гигант Alibaba уже протестировал платёжную систему для продажи жареной курицы на базе алгоритмов распознавания лиц.

Расширение количества новых пользователей

В то время как Соединённые Штаты только сейчас предлагают самый большой рынок для внедрения технологии распознавания лиц, в Азиатско-Тихоокеанском регионе уже наблюдается быстрый её рост. Лидирующие позиции в этом секторе занимают Китай и Индия.

Распознавание лиц в Китае

Технология распознавания лиц – перспективная и весьма востребованная в Китае, от банков и аэропортов до полиции. Сейчас власти расширяют программу «солнцезащитных очков» для распознавания лиц, поскольку полиция начинает тестировать её на окраине Пекина. Китай также создаёт и совершенствует сеть видеонаблюдения по всей стране. Так, в конце 2018 года было использовано более 200 млн камер наблюдения, а в конце 2020 года ожидается установка 626 млн камер. Это связано прежде всего с внедрением в Поднебесной системы социального рейтинга, которую поддерживает и развивает правительство Китая. Вся информация о пользователях, получаемая в рамках данного проекта, в том числе и биометрические данные, аккумулируется в виде индивидуальных профилей граждан (рис. 4) и хранится в централизованной базе данных. В первую десятку городов с наибольшим количеством уличных камер на человека вошли Чунцин, Шэньчжэнь, Шанхай, Тяньцзинь и Цзинань. По версии Guardian от 2 декабря 2019 года, Лондон – № 6 в этом списке и Атланта – № 10. По данным газеты The New York Times от апреля 2019 года, китайская полиция сотрудничает с компаниями, занимающимися искусственным интеллектом, такими как Yitu, Megvii, SenseTime и CloudWalk. Амбиции Китая в области искусственного интеллекта, в частности технологий распознавания лиц, весьма высоки. Страна стремится стать мировым лидером в области искусственного интеллекта к 2030 году.

Распознавание лиц в Азии

Во время проведения Олимпийских игр 2020 года в Токио распознавание лиц и другие биометрические методы идентификации приобретут первостепенное значение в целях оптимизации логистики и безопасности. Эта технология будет использоваться для повышения скорости идентификации аккредитованных спортсменов, персонала и журналистов для автоматического предоставления им разрешённых доступов, что повышает безопасность и исключает влияние человеческого фактора.

В настоящее время в Сиднее в аэропортах проходят испытания системы распознавания лиц, чтобы помочь пассажирам быстрее и более безопасно пройти все этапы пограничного контроля. В Индии созданная в рамках проекта Aadhaar биометрическая база данных является крупнейшей в мире. В рамках проекта уже собрано уникальное количество цифровых биометрических шаблонов. В базе зарегистрировано 1,2 млрд идентификационных номеров жителей. Управляющая компания UIDAI с сентября 2018 года применяет лицевую аутентификацию в виде дополнительной услуги в тестовом режиме, а затем будет добавлен ещё ряд факторов аутентификации, таких как отпечаток пальца, анализ радужной оболочки глаз, рисунок

Рис. 4. Иллюстрация методов получения биометрических данных

Рис. 5. Иллюстрация работы системы идентификации по походке

вен ладоней и поведенческий анализ людей по походке. На рис. 5 представлена иллюстрация модели распознавания человека по походке на основе свёрточных нейронных сетей. В 2020 году правительство Индии планирует развернуть в стране самую крупную в мире систему распознавания лиц. Национальное бюро контроля преступности (NCRB) выпустило техническое задание на разработку общенациональной системы распознавания лиц. Согласно требованиям к системе, опубликованным в виде 160-страничного документа, она будет централизованным веб-приложением, размещённым в центре данных NCRB в Дели. К нему будет предоставлен доступ всем полицейским участкам страны. Глобальная система сможет автоматически идентифицировать людей из видеопотоков и изображений CCTV. Бюро заявляет, что развёртывание этой системы существенно облегчит полиции поимку преступников, поиск пропавших людей и многое другое.

Когда распознавание лиц укрепляет правовую систему

Этические и социальные проблемы, возникающие в связи с защитой персональных данных, радикально зависят от использования технологий распознавания лиц. Неужели эти технологические достижения, достойные научно-фантастических романов, действительно угрожают нашей свободе? Например, в Европейском союзе и Великобритании общий регламент защиты персональных данных (GDPR) обеспечивает основу для жёсткого контроля практики применения персональных данных.

О каких-либо расследованиях личной жизни граждан, их привычек, путешествий и деловых поездок не может быть и речи, и любое такое вторжение в личную жизнь влечёт за собой серьёзные штрафы. Применяемый с мая 2018 года регламент GDPR поддерживает принцип гармонизированной европейской структуры, в частности, защиты права предоставления и обработки биометрических данных.

Биометрические данные и их защита в США

Вашингтон стал третьим штатом США (после Иллинойса и Техаса), который официально защитил биометрические данные с помощью нового закона, введённого в июне 2017 года. Калифорнийский закон о защите прав потребителей (CCPA), принятый в июне 2018 года и вступивший в силу 1 января 2020 года, окажет серьёзное влияние на права на неприкосновенность частной жизни и защиту прав потребителей не только для жителей Калифорнии, но и для всей страны, поскольку закон часто представляется в качестве образца для федерального закона о конфиденциальности данных. В этом смысле CCPA обладает потенциалом стать таким же значимым, как GDPR в Европе. В июле 2018 года президент Microsoft Брэдфорд Л. Смит сравнил технологию распознавания лиц с лекарствами, отпуск которых строго регламентирован, и призвал Конгресс изучить её и контролировать её использование. «Мы живём в стране законов, и правительство должно играть важную роль в регулировании применения этой технологии», – написал г-н Смит. Совсем недавно, в мае 2019 года член парламента США Александрия Окасио-Кортез озвучила свои «абсолютные» опасения на слушании в Комитете по технологии распознавания лиц (влияние на гражданские права и свободы).

Запреты распознавания лиц (Сан-Франциско, Сомервилл и Окленд)

Проблемы конфиденциальности и гражданских прав в стране обострились, так как распознавание лиц приобретает всё большую популярность в качестве инструмента правоприменения, и 6 мая 2019 года г. Сан-Франциско проголосовал за запрет на распознавание лиц. Это первый в своём роде запрет на использование распознавания лиц. Указ о запрете надзора, подписанный Советом наблюдателей Сан-Франциско, запретил городским учреждениям Сан-Франциско использовать эту технологию с июня 2019 года. Запрет касается и правоохранительных органов. Как сообщает Boston Globe от 27 июня 2019 года, городской совет Сомервилла (штат Массачусетс) проголосовал за запрет использования распознавания лиц, что сделало город вторым сообществом, принявшим такое решение. 16 июля того же года Окленд (Калифорния) принял такое же решение и стал третьим городом США, где запретили использование технологии распознавания лиц. Интересно отметить, что полицейское управление Окленда не использует эту технологию и не планирует её применять. После постановлений Сан-Франциско, Сомервилла и Окленда дискуссия во многих городах становится всё громче, и не только в США. Портленд (Орегон) рассматривает вопрос о запрете в 2020 году. Портленд может стать первым городом, который распространит его на частные магазины, авиакомпании и места проведения мероприятий.

Далее вместе – к гибридным решениям

В будущем решения для идентификации и аутентификации будут опираться на все аспекты биометрических технологий. Это приведёт к созданию биометрического микса, или биометрической смеси, способной гарантировать полную безопасность и конфиденциальность для всех заинтересованных сторон в экосистеме. Такой подход в значительной степени соответствует требованиям безопасности к цифровому банкингу и предотвращению мошенничества с помощью программного обеспечения для оценки рисков в финансовой сфере. Для пользователей онлайн-банкинга или электронных услуг правительства к этому решению могут быть добавлены геолокация, IP-адрес устройства и другие компоненты цифровых технологий. ●

Автор – сотрудник фирмы ПРОСОФТ
Телефон: (495) 234-0636
E-mail: info@prosoft.ru