Тройка, семёрка, туз!

Возможные риски идентификации по биометрии

Александр ГОРШКОВ, СВО компании Iris Devices — резидента Инновационного центра «Сколково»

В обществе сформировалось неоднозначное отношение к идентификации человека по биометрическим признакам. Одни считают, что это удобно, другие, что это рискованно. Идентификация по биометрии имеет вероятностное значение, а значит, допускаются ошибки идентификации. К регистрации биометрических данных сложилось негативное отношение: возможные хищения денежных средств со счетов в банке, незаконная слежка или ошибочные обвинения в нарушении закона. Все эти опасения появились не на пустом месте.

ТРОЙКА

Современные биометрические алгоритмы позволяют идентифицировать людей по лицу в значительно более сложных условиях, чем решения 5-7-летней давности. Стала возможна идентификация при больших углах поворота головы от основного фронтального положения. Алгоритмы справляются с возрастными изменениями. На результаты идентификации не оказывает существенное влияние изменение причёски, не требуется нейтральное выражения лица. Но санитарный режим ограничений и обязательное использование медицинских масок сильно сказалось на точности идентификации по лицу. Перекрытие лица защитными масками на 30 и более процентов потребовало от разработчиков новых решений.

Для настройки и проверки алгоритмов требуется большое количество размеченных данных. Такие данные нужны как для обучения нейросетевых алгоритмов, так и для последующего тестирования и подтверждения точности предлагаемых решений. Быстро собрать необходимые объёмы таких данных стало возможно, благодаря введению пропускного режима. Принятые ограничения разрешали пользоваться общественным транспортом только в случае получения цифрового пропуска с указанным в нём номером проездных билетов «Тройка» или «Стрелка», месячного проездного билета или социальной карты[1]. Наличие камер на турникетах метрополитена и привязка конкретного человека к используемой карте создали возможность автоматической разметки большой обучающей базы лиц в масках. Поставленная задача идентификации людей в медицинских масках была решена оперативно.

СЕМЁРКА

Обучение нейросетевых алгоритмов идентификации людей в медицинских масках — это частный случай. Первоначально требовалось собрать большой объём изображений с лицами людей в различных условиях. Для этого разработчики применяли различные ухищрения, в том числе и не совсем легальные, но и не запрещённые на момент их использования.

Чтобы сформировать большой объём размеченных данных, отечественные и зарубежные компании-разработчики биометрической идентификации по лицу обратились к данным из семи основных социальных сетей: Flickr[2], Facebook[3], Instagram[4], WhatsApp[5], Baidu[6], ВКонтакте[7], Одноклассники[8].

Современное законодательство и пользовательские соглашения социальных сетей запрещают несанкционированное использование сторонними компаниями размещаемых в них фотографий. В некоторых случаях и сейчас суды разрешают собирать из социальных сетей открытую персональную информацию о пользователях[9]. В любом случае, наличие уже собранного большого объёма размеченных данных позволило разработчикам не только занять, но и удерживать лидирующие позиции в международных тестах биометрических алгоритмов идентификации по лицу[10]. В современных условиях для удержания лидирующих позиций применяют легальные способы сбора автоматически размечаемых биометрических данных. Например, получение согласия пользователя на использование его фотографий в различных конкурсах, тестах или других развлечениях[11]. Для этих целей было разработано приложение Gradient[12], в котором отрабатывается не только алгоритм идентификации, но и проверяется возможность сужения объёма сравниваемых данных. Аналогичные Gradient приложения разрабатывают многие компании, так, в социальных сетях собирают фотографии пользователей, предлагая им ответить на вопрос: «на какую знаменитость вы похожи»[13] или запустив флешмоб «я 10 лет назад»[14].

ТУЗ

Итак, что же мы имеем на руках?

Наши биометрические данные лица могут быть получены на законных основаниях.

Осталось ответить на три вопроса:

– Необходима ли биометрия для организации слежки за гражданами?

– Возможно ли законное использование биометрических данных для поиска людей?

– Какие есть риски у граждан, сдавших и не сдававших свои биометрические данные в Единую Биометрическую Систему?

Проще всего ответить на первый вопрос. Слежку за своими гражданами государства осуществляли с незапамятных времён, когда о биометрии никто не думал и не знал. Сейчас организовать слежку можно более бюджетными способами, например, при помощи мобильного телефона[15]. Такой контроль возможен даже в тех местах, где нет видеокамер. По понятным причинам это не всегда может быть реализуемо. Матёрый уголовник не возьмёт с собой на преступление телефон. Однако нарушители правил дорожного движения, организаторы незаконных массовых акций или лица, демонстрирующие на видео свои неадекватные действия, имеют смартфоны и размещают отснятый материал в интернете. В этих и аналогичных случаях контроль и поиск людей может быть эффективно реализован с использованием биометрии.

В прессе публикуется информация о многих случаях, когда для поиска нарушителей общественного порядка использовали биометрию[16]. На основании чего осуществляется такой поиск – сказать сложно. Возможно, для этого используется фотография с места событий. Возможно, разыскиваемый человек идентифицируется иным способом, и для его поиска используется фотография не с места события. Более того, для поиска по биометрии не обязательно иметь фотографию конкретного человека, поиск может быть осуществлён по составленному на него фотороботу[17]. В этом случае никакого нарушения законодательства нет, так как за гражданами не осуществляется незаконная слежка. Внедрение новых способов идентификации с каждым годом всё больше и больше мешает нарушителям закона скрываться от правоохранителей.

Если найти человека можно независимо от того, регистрировал он свои биометрические данные в государственных системах или не регистрировал, то принимая решение о сдаче или отказе от сдачи биометрических данных, надо оценить, какие риски возникают в одном и в другом случае.

В начале февраля на Business FM рассказали о новом способе хищения денег[18]. У человека похищают телефон и вынимают из него сим-карту. С помощью неё и другого телефона получают доступ к банковским приложениям жертвы. Установленные на похищенном телефоне пароли и другие средства защиты не могут предотвратить восстановление доступа к мобильным приложениям банка на другом телефоне. Со счетов жертвы снимают деньги и берут кредиты. Предотвратить такое мошенничество можно при помощи проверки по биометрии на стороне банка. Но такая возможность есть далеко не у всех банков. В последнее время участились звонки якобы от «банков», целью которых, по некоторым предположениям, является запись голоса собеседника. Воспроизведя при помощи алгоритмов deepfake голос клиента банка, можно будет без хищения телефона получить несанкционированный доступ к счетам жертвы и выполнить перевод денежных средств[19]. Скорее всего у такой схемы нет официально зафиксированных случаев реализации. Это связано с тем, что имеется достаточно много алгоритмов для определения, что идентифицируется живой человек, а не его копия или клон. Некоторые из таких решений имеют сертификат iBeta Quality Assurance[20], единственной лаборатории, аккредитованной для этого Национальным институтом стандартов и технологий[21]. Компаний, которые получили сертификат этой лаборатории, немного: Acuant, Aware, FaceTec, ID R&D и IDmission. Надо отметить, что компания ID R&D[22] основана россиянами.

Одного человека можно обмануть, но обмануть всех невозможно. Если поставить цель, то любую систему рано или поздно можно взломать. Получается, что использование биометрии опасно? На этот вопрос нет однозначного ответа. Если постараться, то можно обмануть даже такую сложно воспроизводимую идентификацию, как по венам ладони[23]. Но обмануть сразу несколько способов идентификации на несколько порядков сложнее, особенно если используются сложно считываемые модальности, например, по радужной оболочке глаз или сердцебиению. На текущий момент Единая Биометрическая Система (ЕБС) включает в себя только две модальности – лицо и голос. Эти модальности были первыми добавлены в ЕБС, так как их было легко собирать и использовать без наличия специализированного оборудования. Архитектура ЕБС разработана таким образом, чтобы в неё можно было легко добавлять новые способы биометрической идентификации и новых вендоров. Ранее обсуждалась возможность добавления в ЕБС решений для биометрической идентификации по рисунку папиллярного узора, рисунку вен и радужной оболочки глаз[24]. В декабре 2020 года были приняты поправки к закону, определяющему использование биометрической идентификации в РФ[25]. В принятых поправках, кроме возможного расширения функционального применения биометрии, сформулированы требования к обеспечению защиты собранных биометрических данных и возможности их удаления из информационных баз, что в будущем позволит сделать использование биометрии более безопасным.

---

[1] https://www.mos.ru/news/item/72877073/

[2] https://tjournal.ru/tech/90175-ibm-ispolzoval-fotografii-iz-flickr-dlya-obucheniya-sistem-raspoznavaniya-lic-polzovateli-servisa-na-eto-ne-soglashalis

[3] https://rb.ru/story/facebook-vs-cambridge-analytica/

[4] https://rg.ru/2020/08/13/instagram-obvinili-v-slezhke-za-polzovateliami.html

[5] https://3dnews.ru/1031270/v-nastolnoy-versii-whatsapp-poyavilas-biometricheskaya-identifikatsiya

[6] https://youtu.be/wr4rx0Spihs

[7] https://rg.ru/2016/03/28/zapushchen-servis-dlia-poiska-profilia-v-socsetiah-po-licu-cheloveka.html
https://www.kaspersky.ru/blog/findface-experiment/11671/

[8] https://vc.ru/social/110259-odnoklassniki-zapustili-funkciyu-vosstanovleniya-profiley-s-pomoshchyu-raspoznavaniya-lic-i-zhestov

[9] https://www.rbc.ru/technology_and_media/12/02/2021/60267e8f9a79474fbd968df3

[10] https://pages.nist.gov/frvt/reports/11/frvt_11_report.pdf

[11] https://deepfakechallenge.com/2021/02/10/6349/

[12] https://lifehacker.ru/gradient-opredelyaet-nacionalnost/

[13] https://geeker.ru/photo/na-kogo-poxozh-iz-znamenitostej/

[14] https://www.pravmir.ru/ya-10-let-nazad-bezobidnaya-igra-ili-sbor-dannyih-o-nas/

[15] https://1prime.ru/telecommunications_and_technologies/20210120/832852747.html

[16] https://tjournal.ru/tech/333457-sistema-raspoznavaniya-lic-v-moskve-teper-ishchet-protestuyushchih-kak-ona-ustroena-i-chto-sdelat-dlya-zashchity?fbclid=IwAR0BtZ3NtQGXlic1wnUK32Mc1cBfsWAhYM6DcAPdgv6ZNXRwOxF8z59QQsk

[17] https://ru.wikipedia.org/wiki/%D0%A4%D0%BE%D1%82%D0%BE%D1%80%D0%BE%D0%B1%D0%BE%D1%82
https://deepfakechallenge.com/2020/07/21/5248/

[18] https://www.bfm.ru/news/464209

[19] https://1prime.ru/telecommunications_and_technologies/20210208/832978157.html

[20] https://www.ibeta.com/

[21] https://www.nist.gov/

[22] https://www.biometricupdate.com/202010/id-rd-passive-biometric-liveness-detection-passes-level-2-ibeta-testing

[23] https://deepfakechallenge.com/palm-and-finger-veins/

[24] https://www.cnews.ru/news/top/2019-05-21_v_edinuyu_biometricheskuyu_sistemu_dobavyat_nomer

[25] https://sozd.duma.gov.ru/bill/613239-7