

Алексей Кадейшвили, технический директор компании Вокорд: Российские технологии распознавания лиц готовы выполнять задачи по обеспечению безопасности

17.07.2017 15:34 <http://mskit.ru/interview/i201873/>



Если еще лет пять назад технологии распознавания лиц воспринимались в нашей стране как что-то необычное и модное, то сегодня они уже всюду эксплуатируются коммерческим сектором, решая многочисленные задачи безопасности, контроля доступа, маркетинга и т.п. И готовы решать важнейшие государственные задачи обеспечения безопасности граждан на транспорте, при проведении массовых мероприятий и не только. О биометрических технологиях распознавания по лицу как инструменте обеспечения безопасности мы говорим сегодня с техническим директором компании Вокорд Алексеем Кадейшвили.

Алексей, что послужило такому, можно сказать, взрывному, увеличению спроса на распознавание лиц?

Взрыв случился благодаря сочетанию 2-х факторов. С одной стороны, развитие математических алгоритмов привело к созданию глубоких нейронных сетей, которые оказались крайне эффективны для анализа изображений вообще и изображений лиц в частности, а с другой стороны, в результате неуклонного действия закона Мура появились доступные по цене процессоры, которые позволяют очень эффективно обучать глубокие нейронные сети. В итоге появились стоящие разумных денег и хорошо работающие системы распознавания лиц. Благодаря этому биометрические решения – это доступные и эффективные инструменты для задач розничной торговли, банков, онлайн платежей, страхового бизнеса, маркетинга, и даже для компьютерных игр и кинематографа.

Технологии продолжают развиваться, что повлечет дальнейшее развитие и увеличение количества сервисов, основанных на них.

Есть ли отличия между западными и российскими решениями? Насколько сильна конкуренция и в чем сейчас преимущества тех или иных игроков?

Наука интернациональна. Поэтому новые фундаментальные подходы к анализу изображений на базе глубоких нейронных сетей хорошо знакомы разработчикам, работающим в этой области независимо от их национальной принадлежности. С учетом того, что в России всегда была сильная математическая школа и наши программисты всегда были на мировом уровне, отличий по принципу западные и не западные решения по большому счету нет. На данный момент российские компании занимают ведущие позиции. Поскольку спрос на технологию распознавания лиц высокий, то и конкуренция в этой отрасли растет. По мере совершенствования алгоритмов распознавания все постепенно приходят к одному знаменателю, но алгоритм распознавания не единственный фактор, влияющий на результат.

Любой алгоритм работает с тем изображением, которое ему дают. Поэтому достоверность идентификации зависит и от качества исходной картинке. Если говорить о некооперативном распознавании лиц людей, следующих в потоке, то этот пункт становится определяющим работоспособность системы. Для таких сложных задач необходимы уже специализированные камеры, которые выделяют лица. Современные камеры способны одновременно захватывать до 16 лиц в одном кадре. Качество изображения, полученного с камеры, улучшается с помощью алгоритмов адаптации, благодаря чему повышается достоверность распознавания. Такие аппаратно-программные комплексы и являются конкурентным преимуществом тех производителей, у кого они есть. Одних алгоритмов не достаточно для выполнения задач повышенной сложности, одной из которых является обеспечение безопасности объектов массового нахождения людей.

Правильно ли я понимаю, что российские технологии распознавания лиц готовы выполнять задачи по обеспечению безопасности на уровне государства?

Совершенно верно. Технологии дистанционного распознавания лиц полностью готовы к выполнению таких задач, что подтверждается не только тестовыми испытаниями, которые мы проводили в метро, в аэропортах, на вокзалах, но и внедрениями систем на некоторых транспортных терминалах. Системы дистанционного биометрического распознавания позволяют автоматизировать, ускорить и сделать намного эффективнее обеспечение безопасности самых сложных объектов массового нахождения людей. К ним относятся, в

первую очередь) объекты транспортной инфраструктуры (вокзалы, аэропорты, метро, пересадочные узлы), а также крупнейшие спортивные сооружения, что чрезвычайно важно в преддверии таких крупных международных мероприятий, как Кубок конфедераций и предстоящий Чемпионат мира по футболу 2018 года.

Такая система работает, даже когда человек идет в плотном потоке, специально не останавливаясь перед камерами, т.е. идентификация производится в некооперативном режиме, при этом точность распознавания составляет выше 96 процентов (по опыту наших проектов).

В условиях больших пассажиропотоков решающую роль в предотвращении нештатных ситуаций и минимизации внешних угроз играет быстрота принятия решений. Преимуществом систем дистанционного распознавания лиц, использующих специализированные камеры, является их быстродействие и высокая точность работы. Ведь они способны идентифицировать в толпе лицо человека менее чем за секунду и моментально выдать оператору предупреждение. Таким образом, с их помощью можно выявить подозрительные лица еще на подходе к охраняемому объекту, и тем самым обеспечить его превентивную безопасность.

Более того, системы дистанционного распознавания лиц имеет смысл применять для контроля въезжающих граждан на пограничных пунктах пропуска. Лицо является уникальным идентификатором и если документы, удостоверяющие личность можно подделать, с лицом такой фокус проделать практически невозможно. Но для того, чтобы система работала в полную силу, необходима инфраструктура, изменения в законодательной базе, финансирование и повышение осведомленности о работе систем, их возможностях, о вопросах неприкосновенности личных данных, их защищенности при передаче информации такого рода. Необходим комплексный подход в масштабах государства, который будет охватывать все уровни, начиная с миграционного контроля, заканчивая входом на стадион.

Верно ли утверждение, что технологии распознавания лиц и видеонаблюдения решают разные задачи безопасности? Должны ли они работать в комплексе на важных объектах массового скопления людей?

Задача обеспечения безопасности одна, а вот способы её решения разные. В этом смысле и распознавание лиц и интеллектуальная видеоаналитика представляют собой звенья одной цепи, поскольку призваны предотвращать возникновение нештатных ситуаций, вовремя оповещать сотрудников об их возникновении, и предоставляют пользователям внушительный набор аналитических инструментов и архивных материалов для проведения расследований.

Интеллектуальное видеонаблюдение – это широкое понятие, включающее в себя самый разный функционал: детектирование движения, обнаружение оставленных и унесенных предметов, детектирование появления человека в заданной области, распознавание номеров транспортных средств и многие другие вещи. Видеонаблюдение уже давно стало незаменимым помощником служб безопасности, и области его применения, и функционал будет расширяться.

Системы распознавания лиц – это тоже часть интеллектуального видеонаблюдения. Применение двух разных систем в комплексе существенно увеличивает эффективность служб безопасности. На примере это выглядит следующим образом. Допустим, злоумышленник предпринимает попытку проникнуть в «закрытую» зону аэропорта, которая оборудована системой биометрической идентификации по лицу, и контроль, и управление доступом осуществляется без сканеров и ID-карт. Системы видеоаналитики зафиксируют появление человека в охраняемой зоне, а камера с функцией выделения лиц тут же сделает снимок его лица и сохранит в архив его биометрический шаблон, по которому его всегда можно будет распознать. Если этот человек уже внесен в базу как «подозреваемый» или находится в «черном списке», система автоматически оповестит охрану о его появлении.

В архиве сохраняются все события, которые зарегистрировала система: сколько раз и кто заходил или пытался зайти в помещение, в какие зоны и т.п., таким образом можно отследить все перемещения интересующего человека по территории аэропорта, просто нажав две кнопки.

В России уже есть примеры реального использования систем распознавания лиц для обеспечения безопасности в местах массового скопления людей?

Да, примеры реального использования систем распознавания лиц есть, и их количество с каждым годом увеличивается. Есть внедрения на спортивных объектах. Например, с 2015 года аппаратно-программный комплекс биометрического распознавания лиц обеспечивает безопасность крупнейшего многофункционального спортивного комплекса Сибири «Арены Омск». В 2016 году система была успешно задействована в обеспечении безопасности финального этапа Кубка мира по биатлону в Югре и сегодня установлена на спортивных объектах Ханты-Мансийска.

На новом железнодорожном терминале города Адлера, железнодорожных вокзалах и автовокзале Рязани в рамках программы «Безопасный город» установлены и работают системы дистанционной биометрической идентификации лиц. Как я уже отмечал выше, интерес проявляют службы безопасности аэропортов, метрополитенов, погранслужба и другие организации, но информация о таких проектах для широкой общественности закрыта.

Что касается гражданских отраслей, то системы распознавания лиц используются в ритейле. Например, в некоторых магазинах DIY (DoItYourself) сети они успешно борются с организованными воровскими группами.

Где еще, по Вашему мнению, технологии принесут ощутимую пользу?

Как я уже отметил выше, у дистанционного распознавания лиц большое будущее. Сфера его применения ни в коем случае не ограничивается безопасностью. Технология будет востребована в банках и ритейле для улучшения взаимоотношений с клиентами, в рекламе для создания интерактивной контекстной рекламы, в маркетинговых исследованиях, в кинематографе и компьютерных играх.

Какие существуют трудности при выполнении проектов по внедрению систем распознавания лиц? Одинаковы ли они для разных стран? Что нужно учитывать?

В силу того, что биометрия только начинает внедряться в нашу повседневную жизнь, у пользователей и обывателей возникает очень много вопросов и, в первую очередь, это касается неприкосновенности личных данных. Что будет, если преступники украдут базу биометрических шаблонов, насколько безопасно передавать эти данные по сетям и т.п. Хочу успокоить общественность: в архиве хранится не изображение лица человека, а биометрический шаблон – небольшой набор цифр, по которому можно «узнать» человека, но из которого невозможно восстановить его фотографию.

В разных странах, безусловно, разные требования к неприкосновенности частной жизни и новое, тем более биометрическая идентификация по лицу, довольно часто встречается «в штыки», но нынешняя ситуация такова, что властям придется сделать выбор в пользу интеллектуальных систем распознавания.

В то же время, в некоторых странах Латинской Америки вводятся биометрические удостоверения личности (e-ID), а в Евросоюзе разрабатывается система электронного контроля пересечения границ для стран, входящих в Евросоюз (проект «умных границ»). В Европе самые высокие темпы роста перехода на электронные документы.

Предпосылки к массовому внедрению систем есть. И мы придем к тому, что системами дистанционного распознавания лиц будут оборудоваться объекты транспортной инфраструктуры, пограничные пункты пропуска, стадионы и многие другие объекты массового нахождения людей.

На что обращать внимание при выборе систем распознавания лиц?

Во-первых, нужно сравнивать вероятность распознавания разных алгоритмов при заданном значении вероятности ложных срабатываний. Причем смотреть это нужно на данных максимально близких к реальным условиям эксплуатации. Во-вторых, нужно смотреть на скорость работы алгоритма и требования к вычислительным ресурсам. Это основные параметры.

Несколько слов о перспективах развития систем распознавания лиц - ваш прогноз.

Следующий шаг – это распознавание эмоций, скажем так, перспектива следующего десятилетия. Дальнейшее развитие получит и мультибиометрия, как результат сотрудничества нескольких разработчиков. Разные технологии, которые подразумевает понятие «биометрия», имеют разные подходы и анализируют разные уникальные характеристики. Преимущество комбинированного использования нескольких биометрических характеристик позволяет идентифицировать человека даже в случае, если один из биометрических образцов по какой-то причине не может быть получен.