Биоидентификация по лицу в проекции алгоритма системного анализа и обработки информации Виолы-Джонса

Андрей Кашкаров (ak35@yandex.ru)

В статье рассматриваются попытки деанонимизации лиц на основе анализа цифровых данных видеоизображений алгоритма Виолы-Джонса, а также методы, применяемые активистами, ратующими за неприкосновенность частной жизни.

Деанонимизация сегодня

Не всем нравится, что каждый их шаг могут фиксировать с помощью видеокамер и анализировать. Однако в нашем современном мире с большой турбулентностью подобные тенденции – логичный процесс. Когда-то фермеры на Среднем Западе США бастовали против расширения сети железных дорог. Извозчики на лошадях, запряжённых пролетками, двуколками, каретами, чувствовали угрозу в первых автомобилях. В обозримом прошлом, да и теперь словесным нападкам подвергаются ГМО-продукты. Новое всегда вызывает настороженность. В социуме неизбежно возникают группы по интересам, поддерживающие и протестующие против инноваций, когда видят в них – в соответствии со своим местом в социуме и мировоззрением – угрозу личной безопасности. Очень важно видеть и, главное, соблюдать «рамки» использования средств видео- (и иного) контроля в общественных местах. Именно это правовое «поведение» даёт некоторую гарантию и ещё больше надежды на то, что, с одной стороны, защита правопорядка, анонсированная на пользу в первую очередь гражданам, будет лучше организована, а с другой стороны, интересы людей не будут нарушены в правовом поле.

Одним из способов контроля ситуации в общественных местах, осуществляющегося в режиме реального времени с фиксацией записи в цифровом виде, является видеонаблюдение. Считается, что, чем больше видеокамер установлено, чем бóльшая «зона покрытия» обеспечена, тем больший контроль можно осуществить дистанционно и тем быстрее оперативно реагировать на «вызовы времени». Такова одна из важных, пусть и косвенных, причин в обосновании прошедшей реформы МВД со значительным сокращением аттестованных сотрудников. Поэтому количество установленных в России видеокамер – в общественных местах, в подъездах, на дорогах – огромно и продолжает расти. Но кто сказал, что системы анализа данных могут определять только лица? Идентифицировать человека можно многими способами. Созданы алгоритмы, учитывающие одежду, походку, биометрическую информацию, а в перспективе системы контроля и безопасности дистанционно будут определять частоту сердечных сокращений и комплексно анализировать все данные, минимизируя ошибки в определении конкретного человека по его видеоизображению и другим «внешним» данным. Поэтому видеокамеры – лишь элемент системы с высокой интеграцией, впрочем, элемент очень важный, ибо от качества «картинки», способности функционировать в условиях непогоды (туман, осадки), загрязнения (ветер, способствующий пыли) и в условиях ограниченной освещённости зависит результативность всей системы.

Далеко не каждый человек, кто противится «контролю со стороны», в какой бы форме он ни осуществлялся, – правонарушитель. Вообще непримиримых борцов с условной «системой» много, а гарантией безопасности для окружающих является их действие в правовом поле. На этой зыбкой почве можно существовать и взаимодействовать. «Я не люблю, когда мне лезут в душу, особенно – когда в неё плюют», – пел Владимир Высоцкий. Существует право на перемещение, личную жизнь и пр., закреплённое в основном законе страны. При этом защита персональных данных, мягко говоря, несовершенна. Отчего же обо мне собирают информацию без моего согласия, недоумевает законопослушный гражданин, желающий – это его право – оставаться анонимным или неузнанным хотя бы на улице. Оставим за рамками статьи обсуждение мотивации – кому и зачем это надо – и рассмотрим часто встречающиеся (типичные) методы, применяемые «для защиты от камер», а также методы усовершенствования систем видеонаблюдения для купирования подобных методов.

Принцип системы анализа видеоизображений

В 2001 году Полом Виолой и Майклом Джонсом представлен алгоритм, позволяющий обнаруживать объекты на изображениях в реальном времени. Метод и до сего дня является основополагающим в этой сфере, но неоднократно усовершенствован. Алгоритм основан на четырёх принципах получения и обработки данных.

- Используются изображения в интегральном представлении, что позволяет быстро вычислять необходимые объекты.
- Используются признаки Хаара, с помощью которых происходит поиск нужного объекта (в данном контексте – лица и его черт).
- Используется бустинг (от англ. boost – улучшение, усиление) для выбора наиболее подходящих признаков для искомого объекта на данной части изображения.

Все признаки поступают на вход классификатора, который даёт результат «верно» либо «ложь».

- Используются каскады признаков для быстрого отбрасывания окон, где не найдено лицо.

Видеокамера – только «первый» элемент в системе видеоконтроля и поиска. От видеокамеры зависит в основном оптическое качество изображения, в остальном действует система искусственного интеллекта на сервере, постоянно обучаемая и совершенствуемая. К примеру, метро Москвы и Санкт-Петербурга, оснащённые значительным количеством видеокамер наблюдения, считаются наиболее безопасными в мире. Такие системы связаны в реальном времени с пополняемой (корректируемой) базой данных лиц, находящихся в розыске, что, несомненно, в комплексе с другими организационными мероприятиями помогает раскрывать совершённые преступления. Однако как и с какой эффективностью это происходит – предмет другой статьи. Для результативной работы таких систем необходима безупречная связь с облачным (серверным) хранилищем баз данных. Её нарушение приведёт к сбою системы. Здесь достаточно сказать, что алгоритмическое развитие Виола-Джонсовых детекторов для решения прикладных задач распознавания изображений совершенствуется постоянно.

Небезупречные методы

Из методов за анонимизацию и «борьбы против камер» известны следующие. С помощью библиотеки OpenCV и скриптов на Java и Processing подбирались варианты причёсок и макияжа, затрудняющие работу алгоритмов распознавания лиц. Ещё 6–8 лет назад это могло помочь, теперь, в условиях усовершенствованного ПО, контрастные линии и пятна, создающие «ложные цели», не обманывают алгоритмы.

Макияж

Парик и даже самый экстравагантный макияж на манер параллельных чёрных и белых полос, укрупнённого размера «пикселей» – квадратов и прямоугольников, нанесённый на лицо спортивного болельщика рисунок, традиционная этническая раскраска африканских племен, которым было под силу обмануть камеры видеонаблюдения десять лет назад, давно не работает. Современные системы видеоконтроля распознают даже лица, на которые была нанесена боевая индейская раскраска, а также те, что наполовину закрыты маской.

Рис. 1. Пример раскраски лица с помощью средства для неэлектронного сканирования отпечатков пальцев

На рис. 1 представлен пример раскраски лица с помощью средства для неэлектронного сканирования отпечатков пальцев – специальной пасты.

Итак, чередование широких чёрных и белых полос, визуально «ломающих» изображение, что мешает корректному определению его размеров, чёлка, закрывающая глаза, и выдающиеся надбровные дуги, узор, нанесённый на скулы, – не помогут. Макияж привлекает внимание и требует времени для его нанесения. Смена имиджа могла обмануть камеры наружного наблюдения, а этим арсенал правоохранителей отнюдь не исчерпывался.

Маски

Активисты неприкосновенности частной жизни выбирают маски с принтами, балаклавы и даже ортопедические маски для лица. Предполагалось, что при сравнении окраски вокруг глаз на «лицах» в системах, использующих метод Виолы-Джонса, цветная накладка с узором сбивает с толку систему. В итоге программа «думает», что вы – это не вы, а кто-то другой. Маска с рисунком типа «хамелеон в городских джунглях», созданная на стыке высоких технологий и искусства с помощью принта человеческой головы, креативна, она удобна, но недостаточна из-за условно широких разрезов для области глаз и рта. Пример представлен на рис. 2.

По той же причине недостаточно балаклавы, условно закрывающей половину лица, даже если на «маске» нанесён рисунок в виде пискельного

Рис. 2. Иллюстрация маски с принтом

принта лица министра внутренних дел ФРГ (2011–2013) Ганса-Петера Фридриха. Известный политик, занимавший министерский пост в Германии не только в области внутренних дел, запомнился немцам своей обоснованной позицией как сторонник ужесточения контроля над пользователями Интернета. Для результативности «необнаружения» лицо должно быть скрыто полностью. Кроме того, в некоторых странах предметы одежды, скрывающие лицо, находились вне закона до начала пандемии коронавируса.

Специальная одежда

Специальные элементы одежды с высокой отражающей способностью изначально придумали для известных людей как защиту от папарацци. Такой материал изначально содержал тысячи сферических кусочков стекла, отражающих значительную часть видимого светового спектра при фотографировании объекта со вспышкой. В результате на фотографиях видна яркая одежда, а разглядеть, кто в ней, – нельзя. Модифицированная идея, возможно, даст защиту от видеокамер. Как пример материала – светоотражающий бли-

Рис. 3. Рукавицы со светоотражающим эффектом

Рис. 4. «Пятно засветки» на изображении, полученном со старой видеокамеры

стер для безопасности в условиях дорожного движения. На рис. 3 представлены рукавицы со светоотражающим эффектом.

Десять лет назад перспективным шагом в деанонимизации считалась одежда с изображением лиц известных людей. Ввиду усовершенствованных алгоритмов аналитической обработки информации в цифровом виде, сегодня, в 23-м году XXI века, при условии, что видеокамерой считана картинка лица, оба рассмотренных метода неэффективны.

Плащи, накидки, надвинутые на голову капюшоны, в том числе сделанные из материала, не пропускающего тепловое излучение, помогут защититься от видеокамер. Так можно частично укрыться даже от инфракрасных камер, но столь плотно «укрытый» человек в общественных местах привлекает к себе значительное внимание. Такой метод хорош или при разовом использовании, или в то время, когда все пользуются им. Ведь и раскрытый зонт защищает от видеокамер, особенно в движущейся массе на улице (все с зонтами – «сплошное покрытие»), но человек, скрывающийся под зонтом в безоблачную погоду (кроме случаев защиты от солнечного удара), подозрителен априори. К нему, возможно, подойдут сотрудники охраны правопорядка для уточнения данных.

Да, относительно надёжный способ скрыть лицо – сочетание капюшона и больших очков. Лыжная маска, обмотанный вокруг головы шарф или даже пакет с дырками для глаз защищают от популярных систем видеоаналитики. С той же эффективностью они привлекают внимание других людей, особенно охранников и полиции.

Очки

Современные видеокамеры работают не только в видимом человеческому глазу спектре, но и в инфракрасном диапазоне. Они почти универсальны в условиях ограниченного освещения – в закрытых помещениях или тёмных переулках. Вот почему традиционные очки, покрытые светоотражающим материалом и даже оснащённые инфракрасными излучателями, миниатюрными светодиодами и элементами питания, – не панацея в игре за скрытность. То же касается «светового камуфляжа». Эффект для маскировки лиц и «обхода камер» предполагался на основе того, что «ослепить» камеру видеонаблюдения можно включёнными «вокруг лица» инфракрасными светодиодами (ИК-светодиоды). Экспериментаторы монтировали светодиоды по периметру головы, капюшона, и некоторых результатов удалось достигнуть, но только там и тогда, когда применяли старые видеокамеры, формирующие монохромное изображение. На «картинке» вместо лица человека было «засвеченное пятно».

Таким образом, результативность метода зависит от того, какое оборудование экспериментатор намерен «обойти». В современных видеокамерах, применяемых в системах безопасности, предусмотрена функция HLC (High light compensation – компенсация яркой засветки). Технически и упрощённо происходит так: в автоматическом режиме «сканирования» рабочей зоны перед объективом отслеживается точка яркой засветки и делается повторный кадр с игнорированием данных от ячеек матрицы в том же месте.

Если речь идёт о видеокамерах условно старого образца 10-летней давности, шансы обмануть их есть. В некритичных местах, обзоре придомовой территории, на дорогах второстепенного значения, в некоторых ТСЖ используют условно старое оборудование, экономя на его замене. Но в критичной инфраструктуре, в том числе в метро, за сменой оборудования следят ответственно, и там условный способ бесполезен. Кроме того, в некоторых случаях ИК-светодиоды, вмонтированные в очки или расположенные вокруг лица (воротник, капюшон, шапка), не только не скрывают лицо, но и подсвечивают его, обеспечивая более чёткую картинку. Ибо для «засветки лица», чего добивается условный экспериментатор, необходимо смотреть прямо в объектив камеры, а это нечасто случается.

Одна из условных разновидностей метода «засветки» видеокамеры направленным точно на объектив лучом портативного электронного квантового генератора – таково технически точное название «лазерной указки» – и вовсе бесполезно. Светить «лазерным лучом» надо прямо в камеру, но для этого нужно чётко попасть в объектив. Кроме того, современные видеокамеры, с учётом сказанного выше и для защиты от простых методов влияния, оснащены системой цветовых фильтров перед объективом, поэтому ни «лазерный луч», ни принудительная ИК-подсветка вокруг лица объекта им не помеха.

Массивные очки с затемнёнными стёклами и специально подобранным паттерном негативно воздействуют на нейросеть, распознающую лица. К примеру, в 2015 году выпущены очки Privacy Visor с системой линз, отражающих, преломляющих и поглощающих свет. Такая технология не позволяет камере сфокусировать-

ся, «размывает» область вокруг глаз, формируя электронное изображение намного ярче оригинала, по сути, превращая его в «пятно засветки» в области лица – см. рис. 4.

Были проведены эксперименты – их результаты есть в открытом доступе, – уточнившие выводы: система успешно анализирует в цифровом виде изображение – определяет человека в солнцезащитных очках, но некорректно – с ошибками идентифицирует обладателя «новой модели». Однако за семь прошедших лет алгоритмы опознавания видеоизображений преодолели и этот «защитный» механизм любителей анонимности.

Рис. 5. Изображение костюмов Гилли

Что в перспективе

Как известно, на каждое действие найдётся противодействие. В наше время, чтобы надёжно «спрятаться» от систем видеонаблюдения, скрытия одного лишь лица недостаточно. Приверженцы персональной конспирации работают над созданием специальных съёмных элементов одежды с интегрированными экранирующими материалами и мембранами. На одежду нашивается специальный капюшон, маскирующий лицо и не пропускающий тепло. На картинке от «тепловых радаров» объект будет похож на всадника без головы.

Можно ли остаться невидимым при применении тепловизора?

Тепловизор, как электронное устройство, преобразующее сканированный температурный фон в визуальную картинку на дисплее, применяют в том числе охотники в составе индивидуального устройства наблюдения или как элемент интегрированной электронной системы наблюдения. Отдельные виды специализированных устройств могут видеть даже сквозь стены толщиной 1-2 кирпича. Устройства могут работать в разных режимах – контроль общего фона (слабый ИК-сигнал) и узконаправленный (мощный). Когда охотник сканирует участок природы в режиме поиска животного, используется общий режим. Когда объект уже определён, переходят в режим узконаправленного сканирования для определения характеристик. Как разновидность поискового электронного устройства, тепловизоры эффективны для охотников на расстоянии до 1 км на местности. Что касается защиты от обнаружения при облачении в костюм Гилли, то многое зависит от характеристик тепловизора, массы спрятавшегося человека, расстояния до него и, главное, его деятельности: при отсутствии физических движений и поиске в «общем» поисковом режиме современного тепловизора с расстояния 1 км вы почти невидимы.

Однако при использовании любого теплоизоляционного материала человек, «играющий в прятки», сталкивается с тем, что в местах соприкосновения защитного костюма с телом появляется пот – тепловой след. Материал так или иначе будет впитывать от тела тепло и влагу, и тогда человек имеет меньше шансов остаться незамеченным тепловизором на нейтральном тепловом фоне. Отсюда важно как качество тепловизора, так и качество маскировочного костюма-халата, а также время, проводимое в нём.

Один из вариантов уйти от тепловизора – плащ-накидка из строительного материала – утеплителя с односторонним фольгированным покрытием. Эффект даёт и теплоизоляционная пленка, которую используют спасатели («космическая плёнка»). Плёнка скрывает «спрятавшегося» 1-2 минуты, затем в тепловизор, сканирующий на расстоянии, становятся видны бесформенные пятна – тепловые следы от живого тела.

Ещё один относительно доступный способ – костюм Гилли; на сленге его называют костюм кикиморы или «леший». Но, как мы знаем, одна и та же местность в разное время года имеет своеобразные цветовые характеристики – вид поздней осени в средней полосе России с голыми ветками лиственного леса на фоне серо-коричневой почвы будет отличаться от насыщенной июльской «зелёнки». Чтобы скрыться на местности с преобладанием соответствующего ландшафта и красочных тонов, подбирают костюм Гилли под цветовой тон времени года и местности. Назовём его условно – маскировочный халат, что по назначению вполне подходит.

На рис. 5 представлено изображение костюмов Гилли.

В представленном «костюме», помимо основы из хлопка, прилегающей к телу человека или нижнему белью, хорошо видна маскировочная мишура, закреплённая к основному материалу. «Мишура» скрывает тепло, излучаемое живым существом, от «электронного глаза» тепловизора, реагирующего на тепловой фон посредством сканирования отражённых лучей инфракрасного спектра. Так как с основой маскировочного халата соприкасаются только «внутренние» элементы «мишуры», «внешние» сохраняют условную нейтральность по температуре. Таким образом, «мишура» маскирует тепловой фон человека, и чем она насыщеннее и гуще, тем лучше качество маскировки. Для создания эффекта невидимки для тепловизора «лохмотья» костюма должны быть «роскошными», а не жидкой имитацией, как в некоторых дешёвых вариантах производства КНР.

Литература

1. *Кашкаров А.П.* Системы видеонаблюдения. Практикум. Ростов н/Д: Феникс, 2014. 123 с.
2. *Кашкаров А.П.* Видеокамеры и видеорегистраторы – для каждого дома и автомобиля. М.: ДМК Пресс, 2014. 118 с.