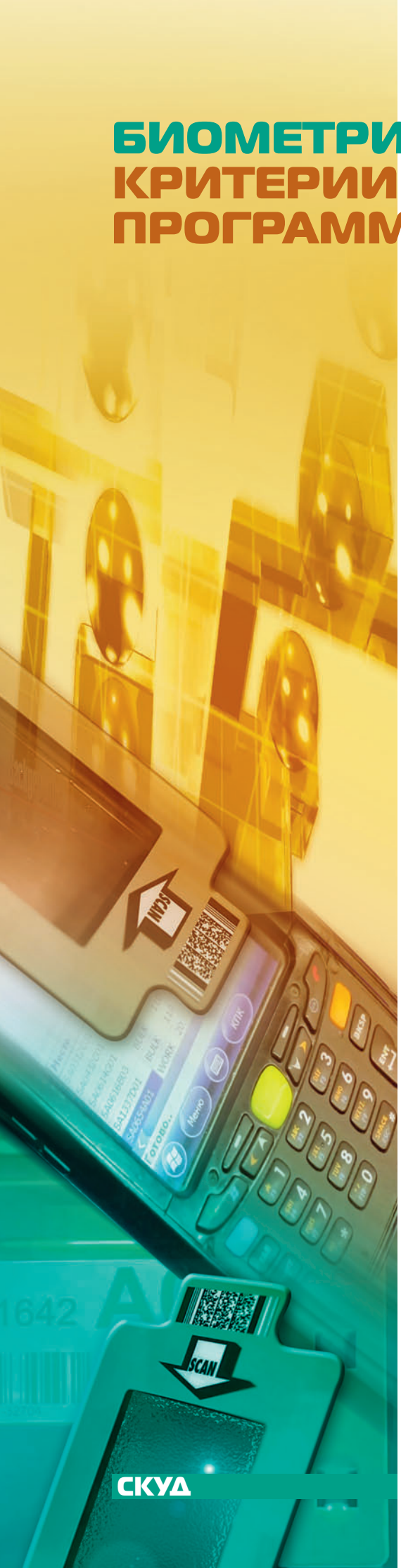
БИОМЕТРИЯ ПО ЛИЦУ. КРИТЕРИИ ВЫБОРА ПРОГРАММНОГО ПРОДУКТА



Маркачев Алексей Владимирович
руководитель продуктового управления биометрических систем ООО «ЦРТ»,
Хрулев Андрей Александрович
директор по специальным проектам ООО «ЦРТ»

Биометрия как средство идентификации личности все активнее используется в повседневной жизни. Мы сталкиваемся с биометрией, когда идем в банк за получением кредита, когда разблокируем смартфон, когда пересекаем границу в аэропорту, когда идем поболеть за любимую команду. Биометрия уже стала удобным и безопасным инструментом подтверждения личности, который невозможно потерять или забыть. Из всего многообразия биометрических характеристик, использующихся для идентификации личности, наиболее доступным и приемлемым для большинства пользователей является изображение лица. Лицо, в отличие от отпечатков пальцев, ДНК, радужной оболочки глаза, не требует специальных сложных технических средств регистрации и может быть получено с использованием обычных камер видеонаблюдения, веб-камер или камер смартфона.

В последние несколько лет на рынке появилось много различных продуктов, позволяющих распознавать лицо человека и проводить его идентификацию для различных задач. К тому же на сегодняшний день спектр возможностей систем распознавания лиц значительно расширился: современные алгоритмы могут не только идентифицировать человека, но и определить его пол, возраст, так называемые системы биометрического профайлинга. К сожалению, даже среди специалистов зачастую бытует мнение, что биометрическое программное обеспечение ограничено только алгоритмами обработки изображений лица и соответствующими программными интерфейсами. Однако на практике такой подход позволяет создать только демонстрационные образцы, показывающие только основные принципы технологии идентификации. Реально действующие системы биометрической идентификации включают в себя также огромный пласт прикладного программного обеспечения, в том числе обработку видеосигнала, управления базами данных, сервисы распределенного взаимодействия, компоненты информационной безопасности, модули формирования поисковых выборок и принятия решения.

В настоящей статье мы хотели бы в основном остановиться на рассмотрении критериев выбора программного обеспечения идентификации по изображению лица, ориентированного на решение пользовательских задач.

Прежде всего важно определиться с терминологией, которая используется профессиональным сообществом при анализе и проектировании систем биометрической идентификации. Нормативные документы Российской Федерации (законы, подзаконные акты) вводят понятие видеоидентификации, под которым понимается идентификация физических лиц, являющихся объектами видеонаблюдения, на основании данных видеонаблюдения. При этом видеоидентификация выполняется всегда с определенными заданными вероятностными характеристиками. Так, например, Постановление Правительства РФ от 26.09.2016 № 969 регламентирует, что видеоидентификация должна выполняться с использованием алгоритмов и аппаратно-программных средств, для которых установлены минимально допустимые значения вероятностей идентификации не ниже 85% и вероятностей ошибочной идентификации не более 1%. Таким образом, под видеоидентификацией необходимо понимать только идентификацию личности в автоматическом режиме с использованием специальных алгоритмов и аппаратно-программных средств, а не с помощью визуального контроля оператором.

Биометрические системы могут работать в двух основных режимах: режим идентификации и режим верификации. В режиме идентификации биометрическая система осуществляет сравнение одного или нескольких биометрических образцов с несколькими биометрическими образцами, хранящимися в базе данных. В режиме идентификации система отвечает на вопрос: «Кто ты?». Напротив, в режиме верификации система осуществляет сравнение одного биометрического шаблона с одним (реже не-

сколькими) биометрическим шаблоном, хранящимся в базе данных и принадлежащим определенному человеку. В режиме верификации система подтверждает заявленную личность человека и отвечает на вопрос: «Ты ли это?». Отличительной особенностью режима верификации является использование дополнительного «небиометрического» идентификатора (электронный пропуск, логин, паспорт, абонемент и т. п.), что подразумевает необходимость интеграции программного обеспечения с действующими системами контроля и управления доступом или, например, на стадионах с билетно-кассовыми системами.

Кроме того, биометрические системы могут работать в кооперативном и некооперативном режимах. При кооперативном режиме человек для подтверждения или установления своей личности явным образом должен посмотреть в камеру, при этом, как правило, человек не движется, а в поле зрения камеры находится один или несколько человек. В некооперативном режиме человек может даже не знать о существовании камеры идентификации личности и, естественно, не обязан смотреть в ее сторону. Зачастую в некооперативном режиме идентифицируемый человек находится в движении, в том числе в плотном потоке людей.

Различные условия распознавания лиц в кооперативном и некооперативном режиме диктуют различные требования к программным алгоритмам биометрической идентификации. Так, непрерывное движение людей в поле зрения камер, работающих в некооперативном режиме, требует наличия технологии трекинга лиц, осуществляющей непрерывное сопровождение лица в поле зрения одной камеры и оценку ракурсов отклонения лица от фронтального положения.

Ключевой особенностью качественных биометрических систем, пригодных к промышленной эксплуатации, является наличие полнофункционального компонентного состава, включающего в себя как основные функции: алгоритмы получения и обработки изображений, управление базами данных, сервисы сравнения, механизм уведомлений, модули интеграции, так и вспомогательные функции: мониторинг, анализ и отчетность.

Полноценный алгоритм обработки изображений лица, в свою очередь, должен содержать следующие этапы:

- детектирование – поиск лица в кадре;
- трекинг – сопровождение одного и того же лица в видеопоследовательности;
- оценка качества – выбор лучшего кадра для последующей обработки;
- расчет портретных характеристик – определение ракурсов лица, оценка пола, возраста (при необходимости);
- формирование биометрического шаблона – расчет биометрических признаков на основе выбранной математической модели;
- сравнение биометрических шаблонов – сопоставление полученного биометрического шаблона с шаблонами, хранящимися в базе данных, и расчет меры схожести шаблонов;
- принятие решения – сравнение полученных мер схожести с заданными пороговыми значениями.

Несмотря на общность алгоритмов обработки изображений лица существуют несколько различных методов построения математической модели лица. На сегодняшний день на рынке доминируют три основных подхода: традиционные математические модели, нейросетевые модели и модели, основанные на различных комбинациях.

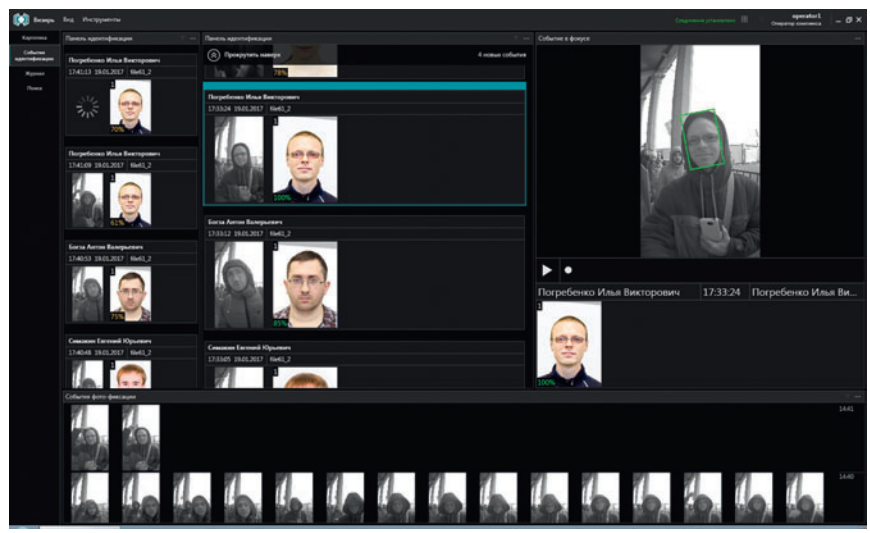
Традиционные модели, основанные на текстурных и геометрических признаках, эффективно работают в условиях фронтального положения лица и теряют свою эффективность при отклонении лица от фронтального положения. Нейронные сети, по сути, представляют собой очень грубую модель человеческого мозга, состоящую из большого количества (от тысяч до миллиардов) элементарных элементов (искусственных нейронов), связанных между собой. Каждый нейрон выполняет простую операцию – преобразует входной сигнал в выходной в соответствии с настраиваемой математической функцией. Меняя параметры этих функций и усиливая или ослабляя связи между нейронами, нейронную сеть можно натренировать на то, чтобы она могла распознавать лица. Нейронные сети могут быть очень эффективны при распознавании лиц с различными ракурсами, но при условии, что набор изображений, на которых проводилось обучение нейросети, содержал большое количество графических данных с теми же самыми ракурсами. Иными словами, применение систем, построенных только на нейронных сетях, возможно только в тех условиях, в которых производилось обучение нейросети.

Комбинированный подход, основанный на фузировании, позволяет минимизировать проблемы каждого метода по отдельности и получить математическую модель, объединяющую эффективность обоих методов. Практическое применение фузированных математических моделей осложнено их высокой ресурсоемкостью, поэтому чаще всего эти модели используются для создания эталонных алгоритмов и решения исследовательских задач, а большинство промышленных систем в настоящий момент построено на нейросетевом подходе.

Выходным сигналом алгоритма распознавания является результат сравнения лица с заданной поисковой выборкой. Формирование поисковых выборок и организация процесса сравнения по большому набору данных в промышленном масштабе должны выполняться прикладным программным обеспечением. При этом скорость сравнения, принятия решения и формирования уведомлений напрямую зависят от архитектуры прикладного программного обеспечения, которое должно обеспечивать возможность распределенных сравнений, высокую отказоустойчивость, защищенность хранимых данных.

На эффективность работы алгоритмов распознавания большое влияние также оказывает качество исходных данных: видеопоток с камеры, видеофайл или фотография из любого источника. При этом исходные данные

Рис. 1. СКД обнаруживает в кадре лицо и сравнивает его с фото из базы



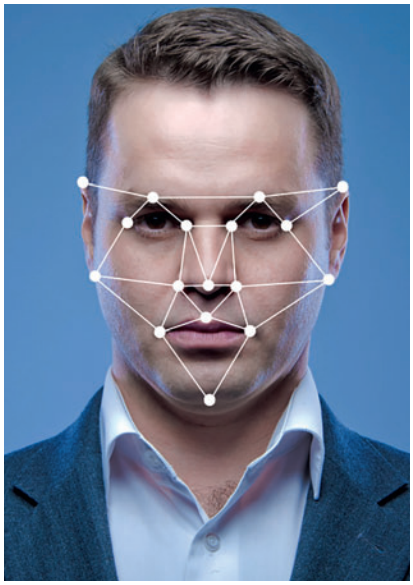


Рис. 2. Построение биометрической модели

могут быть искажены применением алгоритмов сжатия (MJPEG, H.264, H.265 и др.), разрушающих структуру геометрии лица и приводящих к значительному снижению вероятности распознавания (особенно при использовании кодека H.264). Наибольшей эффективности алгоритмов распознавания можно достигнуть при обработке несжатых видеопотоков, получить которые можно только с камер машинного зрения (например Basler Ace). Кроме того, камеры машинного зрения имеют большой сенсор размером до дюйма, позволяющий получать высококонтрастные изображения даже в условиях низкого освещения (менее 100 лк), например, в условиях подземных переходов, станций метрополитена, железнодорожных вокзалов. Вместе с тем применение обычных IP-камер с кодеком MJPEG также может давать хорошие результаты распознавания, сопоставимые с результатами, получаемыми при использовании камер машинного зрения, но только при контролируемых условиях освещенности. Применение IP-камер с кодеком H.264 для идентификации лиц не позволяет получить приемлемые результаты распознавания.

Очень важно понимать, что использование камер машинного зрения не является панацеей. При проектировании системы видеоидентификации на реальном объекте проектировщик должен внимательно подойти к вопросам освещения зоны регистрации, организации структурированного прохода людей, размещая камеры видеоидентификации напротив турникетов, рамок металлодетекторов, вдоль длинных коридоров. Вопрос размещения камер требует специальной проработки на начальном этапе проектирования комплексной системы безопасности. Зачастую специалисты службы безопасности смешивают требования к размещению видеокамер системы телевизионного наблюдения и системы видеоидентификации. Видеокамеры системы телевизионного наблюдения размещают таким образом, чтобы обеспечить максимально возможный обзор периметра и территории объекта наблюдения, по возможности исключив слепые зоны. Видеокамеры системы видеоидентификации должны быть направлены на поток людей, их основная задача – увидеть лицо человека. Поэтому при размещении видеокамер и проектировании инфраструктуры системы видеоидентификации необходимо:

- правильно выбрать ширину контролируемого прохода;
- учесть преимущественные направления движения потока людей;
- рассчитать оптическую систему;
- подобрать подходящие модели камер и соответствующих им объективов;
- произвести оценку предполагаемой нагрузки на систему видеоидентификации, исходя из средней и пиковой плотности потока людей;
- разработать архитектуру распределенных вычислений и соответствующую схему потоков данных, исходя из которых подготовить спецификацию вычислительного оборудования для развертывания программного обеспечения.

Все эти задачи могут быть эффективно решены соответствующими специалистами, имеющими практический опыт внедрения систем видеоидентификации на реальных объектах.

Одними из самых сложных объектов с точки зрения практического внедрения систем видеоидентификации являются стадионы. Система видеоидентификации на стадионе является по сути системой контроля и управления доступом и решает сразу несколько задач, работая как в режиме идентификации (сравнивая лица болельщиков с базой данных футбольных хулиганов), так и в режиме верификации (подтверждая личность владельца футбольного абонемента). Важнейшим критерием успешной работы системы видеоидентификации на стадионе является скорость идентификации и принятия решения, т. к. в условиях интенсивного потока болельщиков любая задержка на турникете может привести к скоплению людей и возможному срыву матча. Высокая пропускная способность системы контроля и управления доступом с функцией видеоидентификации достигается не столько благодаря скорости работы алгоритма распознавания, сколько благодаря правильной архитектуре прикладного программного обеспечения, реализующего возможность выполнения фонового распознавания лиц, выбора лучшего кадра из результатов трекинга, распределенного сравнения шаблонов, глубокой интеграции с внешними системами. Такие системы уже успешно внедряются в России на футбольных стадионах и хоккейных аренах.

Если видеоидентификация успешно работает в таких тяжелых условиях, как на стадионах, то она может эффективно работать и на обычных проходных офисов и предприятий, предоставляя такие преимущества, как отсутствие необходимости носить с собой электронный пропуск и запоминать сложные пароли. В ближайшие годы следует ожидать значительного проникновения биометрии в нашу повседневную жизнь, распознавание лиц дополнит традиционные способы взаимодействия человека и машины, сделав их более удобными и безопасными. Через 5-10 лет использовать биометрию для прохода через турникеты, для открытия дверей, для доступа к веб-сайтам будет также естественно, как сегодня приложить карточку к считывателю.

Рис. 3. Обнаружив лицо из черного списка, СКД уведомляет службу безопасности