одной из главных задач криминалистики является разработка новых методов и технических средств, которые позволят более эффективно раскрывать киберпреступления;

важным направлением развития криминалистики является разработка системы профилактики киберпреступлений, которая позволит предотвратить совершение таких преступлений и снизить уровень преступности в обществе;

криминалистика играет важную роль в судебной практике, поскольку ее методы и средства используются при судебном разбирательстве;

в настоящее время необходимо уделить особое внимание развитию информационных технологий в криминалистике, которые позволят собирать и анализировать большие объемы данных, что, в свою очередь, будет способствовать более эффективному раскрытию преступлений.

К основным направлениям использования информационных технологий в криминалистике относятся:

цифровая криминалистика – использование информационных технологий для сбора, сохранения и анализа цифровых следов, которые могут быть использованы в качестве доказательств в суде;

сетевое направление – исследование преступлений, совершенных в сети Интернет, включая киберпреступления (мошенничество, хакерские атаки и распространение вредоносного программного обеспечения);

биометрическое направление – использование биометрических технологий, позволяющих получить сведения о преступниках (отпечатки пальцев, распознавание лиц и голоса и т. д.);

геоинформационное направление – применение ГИС-технологий для производства следственных действий и проведения оперативно-розыскных мероприятий;

анализ преступлений и прогнозирование преступности (цифровая криминалистическая модель преступлений определенного вида, определение криминалистического поискового портрета и т. д.);

криминалистический анализ данных – применение методов анализа данных и машинного обучения для выявления закономерностей и обнаружения криминальной активности в сети Интернет.

Эти направления являются ключевыми в современной криминалистике и продолжают развиваться с учетом быстрого темпа эволюции информационных технологий.

Таким образом, информационные технологии могут повысить эффективность и качество применения криминалистической техники, обеспечивая быстрый и эффективный поиск следов преступлений, их предварительное изучение, автоматизацию рутинных процессов, интеграцию различных источников информации, создание баз данных и экспертных систем, применение искусственного интеллекта и машинного обучения.

Для успешного внедрения информационных технологий в криминалистическую науку необходимо решить ряд проблем, таких как недостаток финансирования, отсутствие единых стандартов и нормативов, нехватка квалифицированных специалистов, низкий уровень информационной безопасности, юридические и этические ограничения, сопротивление изменениям со стороны сотрудников правоохранительных органов.

Перспективы внедрения информационных технологий в криминалистику связаны с развитием биометрии, цифровой криминалистики, цифрового профайлинга, виртуальной и дополненной реальности, нейрокриминалистики, генетической инженерии, нанотехнологий и др. Эти технологии могут открыть новые возможности для идентификации, реконструкции, моделирования и прогнозирования преступного поведения.

УДК 343.98

А.Е. Середа

КРИМИНАЛИСТИЧЕСКАЯ ИДЕНТИФИКАЦИЯ ЛИЧНОСТИ ЧЕЛОВЕКА ПО БИОМЕТРИЧЕСКИМ ПРИЗНАКАМ ЛИЦА

Идентификация личности человека по биометрической характеристике лица является одним из динамично развивающихся направлений научной мысли. Данная область условно делится на две основных сферы применения технологий: 2D- и 3D-распознавание. Удельный вес технологий распознавания по геометрии и признакам лица в общем объеме мирового биометрического рынка находится в пределах 13–18 %. Лидерами в настоящий момент являются системы Visionic, Viisage и Miros.

Развитием данной технологии занимаются Geometrix, Inc. (3D-сканеры лица, программное обеспечение), Genex Technologies (3D-сканеры лица, программное обеспечение) в США; Cognitec Systems, GmbH (SDK, вычислители, 2D-камеры), Bioscrypt (3D-сканеры лица, программное обеспечение) в Германии; Artec Group (3D-сканеры, программное обеспечение) в России; Synesis в Беларуси. Международный подкомитет по стандартизации в области биометрии (IS0/IEC JTC1/SC37 Biometrics) по состоянию на 2024 г. осуществляет разработку единого формата сведений для распознавания человеческих лиц на основе двух- и трехмерных изображений.

С целью создания модели лица система находит опорные антропометрические точки, определяющие его индивидуальные характеристики. На лице выделяются контуры бровей, глаз, носа, губ и т. д., вычисляется расстояние между ними и строится не просто образ, а множество его вариантов в случае поворота лица, наклона головы и изменения выражения психоэмоционального состояния на лице. Количество моделируемых образов варьируется в зависимости от целей использования.

Минимальное количество опорных точек составляет 68 единиц, однако в некоторых системах их количество составляет 200 единиц и более. В общем случае подобная биометрическая система хранит не фотографии, а наборы цифр, характеризующих лицо, т. е. модель-дескриптор. Идентификация осуществляется путем сравнения полученной системой в процессе работы биометрической модели с хранящимся в базе дескриптором.

Используемый системой дескриптор для идентификации – это уникальный набор характеристик лица в форме массива чисел, независимый от таких параметров, как форма прически, наличие или отсутствие макияжа, возрастные признаки. Данный дескриптор и представляет собой биометрическую модель, которая хранится в базе данных. Восстановить исходное изображение по модели-дескриптору в большинстве случаев невозможно.

Основой любой системы распознавания лиц является метод кодирования. В ряде случаев используется анализ локальных характеристик для представления изображения лица в виде статистически обоснованных, стандартных блоков данных. Они охватывают пиксели изображения лица и универсально представляют лицевые формы. Фактически в наличии имеется намного больше элементов построения лица, чем количество самих частей лица. Идентичность же лица определяется не только по характерным элементам, но и по способу их геометрического объединения (т. е. относительным позициям).

Полученный математический код индивидуальной идентичности не обозначается каким-либо определенным понятием, однако в практике нередко можно встретить термин Faceprint. Отличие Faceprint от дескриптора в указанном контексте является необозначенным в достаточной степени. В этой связи полагаем целесообразным разграничение по способу применения, особенностям хранения и расшифровки данной информации.

В настоящее время существуют четыре основных метода распознавания лица: 1) Eigenface (собственное лицо, нем.); 2) анализ отличительных черт; 3) анализ на основе нейронных сетей; 4) метод автоматической обработки изображения лица. Надежность работы систем распознавания лиц зависит от следующих факторов: качества изображения; актуальности фотографии, занесенной в базу данных; объема используемой базы данных.

Технологии распознавания лиц хорошо работают со стандартными видеокамерами, которые передают данные, управляются персональным компьютером и требуют минимум разрешения 230 × 240 пикселей на дюйм при скорости видеопотока минимум 3–5 кадров в секунду. Более высокая скорость видеопотока при более высоком разрешении ведет к улучшению качества идентификации.

Этапы решения задачи идентификации личности человека по видеоизображению включают в себя:

1. Локализацию лица в кадре. При сканировании изображения на различных масштабах алгоритм осуществляет поиск признаков, которые могут указывать на присутствие лица. Такие ключевые признаки могут включать в себя контуры, текстуры и особенности яркости участков изображения. После этого каждый участок изображения оценивается на соответствие критериям, определяющим вероятность того, что данный участок содержит лицо. На основе этих оценок участки изображения классифицируются как содержащие или не содержащие лицо.

2. Определение положения головы. На данном этапе уже занесенная в базу данных модель головы сопоставляется с изображением, при этом оцениваются такие параметры, как угол поворота по осям *x*, *y*, *z*, точный замер и смещение изображения в кадре.

3. Отслеживание перемещения лица от кадра к кадру. При наличии нескольких изображений с различных ракурсов алгоритм выбирает оптимальное изображение и сохраняет его в базе данных. Анализ нескольких изображений одного и того же лица с различных ракурсов позволяет достичь высокой точности в процессе распознавания.

4. Сравнение (сопоставление) изображения с базой данных. Сопоставление изображения с базой данных представляет собой завершающий этап в последовательности алгоритмов для идентификации личности человека по видеоизображениям. В процессе данного этапа происходит сравнение изображения с набором данных, содержащих информацию о лицах, а также их характеристиках. После сопоставления программа определяет, есть ли совпадения между представленными биометрическими признаками на изображении и данными в базе.

Основная особенность биометрического способа идентификации состоит в том, что такая идентификация носит принципиально вероятностный характер. Для систем, использующих запоминаемые коды или вещественные идентификаторы, решение о допуске принимается детерминированно. Ошибки здесь возможны только при аппаратных неисправностях или программных сбоях.

В процессе функционирования биометрических систем идентификации лиц принятие решений базируется на вероятностной природе информации, полученной о лицах. Ввиду данного фактора неизбежны ошибки в решениях, и подчеркивается не столько их полное исключение, сколько, скорее, возможное снижение вероятности их возникновения. Важным критерием качества работы и эффективности биометрической системы является уровень таких ошибок.

Ввиду отмеченного характера работы биометрических систем и неизбежности ошибок при принятии решений специалисты, работающие с этими системами в рамках расследования преступлений, должны быть соответствующим образом подготовлены. Необходимы владение навыками анализа и интерпретации результатов, понимание особенностей работы систем распознавания лиц, а также способность оценивать и управлять рисками возможных ошибок.

Во-первых, требуется усвоить технические аспекты работы с такими системами, включая установку, настройку и обработку данных. Кроме того, криминалистам необходимо изучить основы алгоритмов и методов распознавания лиц, а также понимать принципы работы различных типов систем распознавания лиц, включая биометрические технологии. Во-вторых, необходимо развить навыки анализа и интерпретации полученных данных, чтобы эффективно использовать информацию, полученную с помощью систем автоматического распознавания лиц. Это включает в себя умения проводить сравнение и идентификацию лиц, анализировать качество изображений и учитывать факторы, влияющие на точность распознавания.

В этой связи необходимы готовность к работе с большим объемом данных и умения эффективно организовывать и обрабатывать информацию, полученную с помощью систем автоматического распознавания лиц, что также включает в себя умения оценивать надежность и достоверность полученных результатов и использовать их в практике раскрытия и расследования преступлений.