## Обзор литературы

### Режимы работы биометрических систем

Биометрическое распознавание может осуществляться в двух режимах – в режиме идентификации или в режиме верификации [Словарь IEEE?]:

* Верификация – это процесс распознавания индивида по его биометрическим признакам при помощи дополнительного источника информации (например, пароль, магнитная карта). Информация, содержащаяся на дополнительном источнике, является индексом в базе данных зарегистрированных пользователей. Распознавание или нераспознавание в данном случае – это результат сопоставления предоставленных биометрических признаков с их образцами, извлечённым по индексу из базы.
* Идентификация – это процесс распознавания индивида только по его биометрическим признакам. Система при этом осуществляет сопоставление с предоставленными образцами всех записей в базе. При этом разные системы могут принимать различные решения о распознавании или нераспознавании индивида в зависимости от степени схожести различных образцов с предоставленным.

В данной работе рассматривается задача идентификации как более ресурсоёмкая и распространённая в реальных системах.

### Базовая архитектура биометрической системы

В простейшем случае биометрическая идентификационная система может быть рассмотрена на компонентном уровне следующим образом (рис. 1) [Гайд ту биометрикс]:



Рис.1. Общая схема биометрической системы. Надо перерисовать протокол на прямоугольник, сканер удалить, экстрактор переименовать в экстрактор шаблонов

* Экстрактор шаблонов, на вход которого подаётся полученное со сканера или иным способом представление биометрического признака (например, растровое изображение отпечатка пальца или сетчатки, цифровая видеозапись походки, цифровая звукозапись голоса и т.д.). Этот модуль выделяет из входящего сигнала особые, отличительные, идентифицирующие признаки данного биометрического образца и составляет из них биометрический шаблон. Этот модуль может быть вырожденным, так как существуют методы непосредственного сопоставления представлений некоторых биометрических признаков (например, сопоставление изображений отпечатков пальцев.
* Биометрическая БД – это база шаблонов зарегистрированных пользователей. Она заполняется в процессе регистрации пользователей, где получение образцов контролируется оператором. Биометрические шаблоны, регистрируемые в базе и получаемые во время эксплуатации системы необязательно должны быть созданы одним и тем же модулем, однако они должны быть сопоставимы между собой. Для этой цели существует ряд стандартов для их представления и хранения (напр., [Стандарт ИСО], [Стандарт ИСО]).
* Биометрический мэтчер – модуль сопоставления отличительных особенностей двух шаблонов между собой. Результатом его работы является некоторая численная метрика, характеризующая степень их схожести. Её значение лежит в интервале [0;1] или может быть к нему нормализовано, при этом 0 означает, что два шаблона не имеют ничего общего, 1 – что с точки зрения выделенных отличительных особенностей они идентичны.
* Протокол принятия решения – модуль, который на основе метрики мэтчера для каждой пары, образованной предоставленным шаблоном и шаблоном из базы, выбирает одну из двух гипотез в качестве истинной: «Два образца принадлежат одному источнику» и «Два образца принадлежат разным источникам». Помимо этого он может выполнять дополнительные действия, специфические для конкретного программного комплекса, например:
* Предоставление доступа в охраняемую систему, если предоставленный образец успешно распознан не более чем с N зарегистрированными пользователями, где N -настраиваемый параметр.
* Выбор из всего множества шаблонов базы подмножества наиболее похожих и передача его на последующую обработку. Биометрические системы такого типа называются классификаторами и будут дополнительно рассмотрены далее.

Выбор гипотезы чаще всего осуществляется путём сравнения метрики с некоторым настраиваемым порогом: если метрика больше порога, выбирается гипотеза принадлежности, в противном случае гипотеза непринадлежности. В более сложных случаях на принятие решения может также оказать влияние оценка качества предоставленного образца. При использовании некоторых видов биометрической интеграции гипотеза выбирается на основе взвешенной суммы метрик нескольких мэтчеров или на основе «голосования»: за истинную принимается та гипотеза, за которую отдали предпочтение большее количество протоколов принятия решения отдельных модулей сопоставления [Гайд ту мультибиометрикс].

### Системные ошибки

Описанные выше модули случайным образом вносят характерные для них ошибки в биометрический признак на соответствующем этапе обработки. В частности для отпечатка пальца:

* Сканеры – сжатие и растяжение кожи, приводящее к искажению считываемого папиллярного узора, слишком низкая или высокая яркость или контрастность изображения, считывание грязи на оптических сенсорах в качестве папиллярного узора.
* Улучшение изображения и построение шаблона – искажение изображения ввиду неприменимости алгоритма улучшения в данном случае, пропуск существующих отличительных точек, добавление в шаблон ложно найденных.
* Модуль сопоставления – несопоставление двух представлений одной и той же отличительной точки, сопоставление представлений двух разных точек.

Таким образом, метрика, назначаемая мэтчером для пары шаблонов, содержит в себе накопленную ошибку всех предшествующих модулей. Кроме того, сами биометрические признаки недетерминированно изменяются с течением времени, а также от раза к разу случайным образом меняется их получаемое представление. Вследствие этого мы вынуждены рассматривать две случайных величины: распределение итоговой метрики для случая, когда представления принадлежат одному биометрическому признак, и распределение для случая, когда разным (рис.2).



Рис.2. Перевести на русский.

На практике эти распределения получают путём сбора статистики по большому числу сопоставлений.

Кроме того, в системе также выставлен порог метрики, выше которого мы полагаем два образца принадлежащими одному источнику. Видно, что для распределения метрик образцов разных источников существует область, где метрика достаточно велика, чтобы система допустила ошибку и приняла за истину гипотезу о принадлежности вместо гипотезы о непринадлежности. Вероятность такой ошибки, называемая коэффициентом ложного доступа (False Acceptance Rate, FAR, также False Match Rate, FMR) рассчитывается как площадь этой области:

Красивый интеграл

Аналогично, коэффициент ложного отказа доступа (False Reject Rate, FRR, также False Non-Match Rate, FNMR) – это вероятность ошибки системы, принимающей за истину гипотезу о непринадлежности, когда верна гипотеза принадлежности. Он вычисляется по аналогии:

Второй красивый интеграл

FAR считается критическим с точки зрения безопасности объекта, так как чем он выше, тем выше вероятность нарушения режима злоумышленником. С другой стороны FRR характеризует удобство работы алгоритма для зарегистрированного пользователя: при низком значении этого коэффициента он будет распознан, скорее всего, с первого раза.

Конкретное значение порога в данном случае определяет рабочую точку системы в терминах FAR и FRR. Для иллюстрации зависимости FAR и FRR используется рабочая характеристика принимающего устройства (РХПУ), которая может быть выражена как в обычной, так и в логарифмической системе координат.



Рис.3. ФАР и ФРР

РХПУ используется для сравнения качества разных мэтчеров [Гайд ту биометрикс]. Помимо этого РХПУ используется для нахождения рабочей точки системы методом изокост [Лекция нидерландца]. Изокоста определяется как

C\_FAR\*(1-P\_SS)\*FAR+C\_FRR\*P\_SS\*FRR = C\_det

Где C\_FAR – цена ошибки ложного доступа, C\_FRR – цена ошибки ложного отказа доступа, P\_SS – априорная вероятность сопоставления образцов, полученных от одного источника, C\_det – цена распознавания. Точки пересечения изокост с РХПУ – это значения порога, при котором достигается указанная цена ошибки при выбранных весовых коэффициентах. Точка РХПУ, в которой достигается минимальная цена распознавания, является оптимальной. Главным недостатком этого метода является наличие множителя P\_SS, который не является априорным для реальных систем. Тем не менее, точки РХПУ, принадлежащие её выпуклой оболочке, являются локальными минимумами стоимости.

Указанные коэффициенты характеризуют работу алгоритма, то есть вероятность ошибки для единичного сопоставления образцов. В то же время для оценки надёжности всей базы определение этих коэффициентов расширяется:

- FAR(m) – вероятность ложного доступа злоумышленника в систему с m зарегистрированными образцами;

- FRR(m) – вероятность ложного отказа доступа зарегистрированному пользователю в систему в m зарегистрированными образцами.

Систему также характеризует коэффициент ошибочной идентификации (False Identification Rate, FIR(m)) - это вероятность, что вместо одного зарегистрированного пользователя был распознан другой. Эта ошибка не нарушает безопасности объекта, так как некорректно распознанный человек обладает правом доступа к нему, и не сказывается на удобстве пользования, однако может приводить к внутрисистемным ошибкам, в частности, в системах учёта времени или оповещения.

При рассмотрении надёжности биометрических алгоритмов используют также коэффициент правильного доступа (Genuine Acceptance Rate, GAR), который рассчитывается как 1-FRR. В биометрической системе GAR(m), FRR(m) и FIR(m) связаны соотношением

Коэффициент правильного отказа (GRR, Genuine Reject Rate) – это вероятность корректного отказа доступа злоумышленнику. Соотношения для случая системы и алгоритма схожи:

Расчёт параметров простейшей биометрической системы на основе параметров алгоритма, подробно рассмотрен в [Гайд ту биометрикс]. Предполагается, что каждому зарегистрированному пользователю соответствует один шаблон в базе данных. Так как результаты каждого из сопоставлений не зависят от результата других, условная вероятность наступления того или иного события в системе определяется как произведение вероятностей наступления тех или иных событий для отдельных сопоставлений.

Если злоумышленник пытается получить доступ к системе, то ему это удастся со следующей вероятностью:

Так как отпечаток злоумышленника не зарегистрирован, любой из шаблонов в базе может привести к ложному доступу. Система предоставляет доступ в том и только в том случае, когда все успешно сопоставленные шаблоны относятся к одному и тому же пользователю, в данном случае успешно сопоставленный шаблон должен быть единственным.

Поскольку стремятся поддерживать около 1, вероятность ложного доступа приближённо линейно возрастает с ростом числа записей в базе.

Рассмотрим ситуацию, когда доступ к системе получает зарегистрированный пользователь. Правильный доступ будет осуществлён в случае успешного сопоставления с единственным шаблоном:

А ошибочная идентификация произойдёт при удачном сопоставлении остальных m-1 отпечатка и неудачном – единственного соответствующего:

Отсюда вероятность ложного отказа – это вероятность всех остальных случаев:

### Биометрическое объединение

Согласно ГОСТ Р 54411-2011/ISO/IEC/TR 24772:2007, биометрическое объединение или мультибиометрия – это комбинация данных нескольких источников, т.е. датчиков, модальностей [Гост]. Выделяют следующие подвиды мультибиометрических систем:

1. Мультимодальные - распознающие по нескольким различным биометрическим признакам (например, отпечаток пальца + радужка глаза) для повышения его надёжности. Как правило характеристики биометрических признаков не коррелируют друг с другом.
2. Мультиалгоритмические - распознающие по различным характеристикам одного биометрического признака в случае, если уровни ошибок отдельных модулей сопоставления не соответствуют требованиям безопасности (например, распознавание по общей форме узора и минуциям для отпечатков пальцев). В этом случае выбираются наименее статистически коррелирующие друг с другом характеристики.
3. Мультиэкземплярные и системы с мультипредставлениями – распознающие по нескольким представлениям одной и той же модальности, например, по нескольким кадрам для распознавания по лицу, или по их объединению.
4. Мультидатчиковые – распознающие по представлениям, полученным с различных датчиков, например, по нескольким образцам голоса, записанным разными устройствами.

В основе этих систем лежат соответствующие уровни или схемы биометрического объединения:

1. Объединение представлений – это интеграция нескольких представлений одной и той же модальности в одно итоговое представление. Оно осуществляется перед экстракцией шаблона. Фактически такое объединение активно используется в протяжных сканерах отпечатков пальцев [multibiometrics], где для снятия отпечатка необходимо провести по считывающей поверхности сканера небольшого размера всей подушечкой пальца, обычно сверху вниз. Чувствительные элементы этих сканеров не фиксируют изображение непрерывно, но делают снимки через определённые интервалы времени, после чего изображения накладываются друг на друга. Получившееся наложение фрагментов и будет итоговым изображением. Такой тип объединения используется и в случае с непротяжными видами скнаеров (оптическими, емкостными, пьезоэлектрическими) для получения более полного изображения отпечатков [ссылка на статью].
2. Объединение признаков – это объединение нескольких биометрических шаблонов или отдельных выделенных особенностей нескольких шаблонов в один итоговый шаблон. Такая интеграция проводится перед модулем сопоставления и может быть выполнена как для шаблонов, полученных из одного образца разными алгоритмами, так и для шаблонов, полученных из разных представлений одного образца (например, от разных сканеров). В первом случае объединение требует проведения нормализации особенностей, то есть переводу всех выделенных особенностей в единую область определения. Очевидно, что такая интеграция невозможна для случаев мультимодальной биометрии с некоррелирующими или несовместимыми модальностями [multibiometrics].

Объединение шаблонов может быть выполнено двумя способами:

1. Обновление шаблона – это дополнение имеющейся в текущем шаблоне информации данными из нового шаблона без эксплицитного учёта ошибок и повторов, например, нахождение средних значений в шаблонах, описывающих геометрию ладони.
2. Улучшение шаблона – это сопоставление с целью выделения повторяющихся и отбрасывания ошибочно найденных признаков, в результате которого формируется итоговый шаблон, обладающий более высоким качеством.
3. Объединение степеней схожести или рангов – это вычисление итогового ранга (для ранжирующих систем) или степени схожести (для сопоставляющих систем) из данных подсистем согласно определённому правилу. Степени схожести, полученные для различных алгоритмов, подвергаются нормализации перед интеграцией. Решение о распознавании или нераспознавании принимается на основе результата объединения.

В литературе [мультибиометрикс, фингерпринтс] встречаются следующие правила:

для интеграции рангов:

1. Максимальный ранг
2. Правило Борда
3. Взвешенная сумма (веса могут подбираться на этапе обучения, например, с помощью логистической регрессии)
4. Другие

Для степеней схожести:

1. Произведение
2. Сумма
3. Максимум
4. Минимум
5. Те же с применением леммы Неймана-Пирсона
6. Объединение нейронными сетями
7. Метод k-ближайших соседей
8. Метод опорных векторов
9. Деревья принятия решений
10. Другие
11. Объединение на уровне принятия решения – это интеграция решений отдельных подсистем на основе некоторого правила. Это объединение осуществляется после работы модуля принятия решения и, как следствие, применимо для случая мультимодальной биометрии. Встречаются следующие правила объединения:
12. Логическое И
13. Логическое ИЛИ
14. Голосование
15. Взвешенное голосование

Более сложным случаем объединения на уровне принятия решения является объединение биометрических модулей в многоуровневую или в последовательную систему. Последовательная система в случае недостаточной достоверности сопоставления на предшествующих этапах (алгоритмах) делает сопоставление дополнительных характеристик на последующих этапах. Многоуровневая система регулирует значения порогов успешного сопоставления последующего уровня на основе результатов предыдущего уровня сопоставления – повышает при неудаче и понижает при успехе.

## Отпечаток пальца как биометрическая модальность

У людей, обезьян и некоторых других млекопитающих на ладонных и подошвенных поверхностях, в том числе и на пальцах, располагаются рельефные линии, называемые папиллярными. Выступающие линии этого рельефа называются гребнями, а участки между ними – впадинами. Отпечаток пальца – это двумерное изображение гребневого (папиллярного) узора ногтевой фаланги пальца.

Основным источником данных для получения информации об отпечатке пальца в автоматизированных системах является его двумерное растровое изображение. Каждый элемент (пиксел) этого изображения характеризуется цветом в оттенках серого (от 0 до 255, где 0 – чёрный цвет, 255 – белый) и целочисленными координатами в системе координат, где началом отсчёта является левый верхний пиксел изображения, ось абсцисс направлена вправо, ось ординат – вниз. Из криминалистической практики идёт традиция, согласно которой гребни на изображении – это линии тёмного цвета, а впадины – светлые области. Следует отметить, что некоторые сканеры захватывают отпечатки в обращённых цветах, поэтому полученные изображения необходимо инвертировать перед использованием [ну я не знаю, Локар?]. Здесь также важно отметить, что когда речь идёт об угле наклона тех или иных объектов отпечатка, угол считается от оси абсцисс и возрастает при повороте против часовой стрелки, что находит своё отражение, например, в формулах параллельного переноса [хэндбук].

Приступая к описанию отличительных особенностей отпечатка пальца, следует также разграничить понятия «направление» (direction) и «ориентация» (orientation) [Статья Мальтони]. Говоря об ориентации объекта в двумерном пространстве, будем иметь в виду некоторую прямую линию, на которой лежит этот объект. Направление объекта – это вектор с началом в его координатах, лежащий на этой прямой линии. Так как из точки вдоль прямой вектор можно направить двумя способами, мы будем выбирать то или иное направление в зависимости от задачи.

В 19 веке была выдвинута гипотеза об уникальности и неизменности во времени каждого отдельного отпечатка. Гипотеза неизменности была впоследствии подтверждена (во время роста ребёнка в отличие от пространственных соотношений между линиями топология его отпечатков не меняется, во взрослом возрасте отпечатки пальцев изменяются только под влиянием глубоких порезов или иных серьёзных травм), однако гипотеза уникальности до сих пор остаётся недоказанной. Её считают эмпирически достоверной на основе следующих фактов:

1. За всё время применения дактилоскопии в криминалистической практике не было выявлено случаев идентичности двух отпечатков, принадлежащих разным источникам [ФБР]
2. Результаты моделирования отпечатков различными способами [Джейн] указывают на низкую вероятность (порядка 10^-28) недостоверности гипотезы.

Вместе с тем, в криминалистической практике не принято говорить об идентичности двух отпечатков. Вместо этого говорят о результатах теста отношения правдоподобия, например, идентичность двух отпечатков в 3 миллиона раз вероятнее их неидентичности [Нидерландец1].

### Отличительные особенности отпечатков пальцев

В изображении отпечатка пальца выделяют отличительные особенности на трёх уровнях: глобальном, локальном и сублокальном.

На глобальном уровне основной отличительной особенностью является общий вид папиллярного узора. Согласно классификации Гальтона-Генри [Генри 1900, чо] выделяют 5 основных типов зоров: правую и левую петли, завиток, арку и приподнятую арку (см. Рис.). Эксперты-криминалисты в рамках данных классов выделяют и более частные [эта ссылка из тырнета]. К глобальным отличительным особенностям относят также положение ядер и дельт. Согласно ГОСТ Р ИСО/МЭК 19794-2-2005, ядро – самая верхняя точка на внутреннем загнутом гребне отпечатка пальца, расположенная, в общем случае, в пределах самого внутреннего загиба петли [ГОСТ]. Необходимо отметить, что в литературе такое определение соответствует точке «верхнего ядра» [Джейн], однако в завитках также встречается и «нижнее ядро» (рис.3, с), и речь в таком случае идёт о самом нижней точке. Дельта – точка на гребне, расположенная ближе остальных к точке расхождения двух граничных папиллярных гребей [ГОСТ]. Менее формально дельту можно определеить как точку на гребне, вокруг которой можно выделить три различных направления расхождения папиллярных линий. Общий вид узоров, ядра и дельты используются в алгоритмах классификации отпечатков.



Рис. Схематичное изображение различных типов папиллярных узоров: левая петля, правая петля, завиток, арка, приподнятая арка

На локальном уровне собираются отличительные особенности, относящиеся к отдельным линиям или группам линий. К таким особенностям относятся точки, в которых нарушается непрерывность гребневых линий – точки, где линии заканчиваются или разедляются надвое (рис.). Согласно ГОСТ Р ИСО/МЭК 19794-2-2005 эти особенности называются контрольными точками или минуциями. В дальнейшем в тексте мы будем пользоваться только термином «минуция» как более широко употребимым.



Рис. Минуции и поры на отпечатке пальца

Из двух основных типов минуции можно составить более сложные [типы], однако в автоматизированной дактилоскопии, особенно при взаимодействии нескольких систем, используются эти два [ГОСТ]. Минуция полностью описывается следующей четвёркой: координаты X и Y, направление и тип (окончание или разветвление). На практике тип считается менее надёжной характеристикой минуции и может не использоваться [MCC]. Известны алгоритмы, которые также не используют и направление минуции [Wegstein].



Рис. Эластическая деформация одного и того же отпечатка

Множество минуций конкретного папиллярного узора, их взаимное расположение и направление при отсутствии эластических деформаций кожи являются тем инвариантом, который отличает данный узор от остальных. Процедура получения отпечатка связана с физическим контактом пальца со считывающей поверхностью, вследствие чего в изображения папиллярного узора попадает только подмножество минуций, взаимное расположение которых может быть искажено эластической деформацией (сжатием или растяжением) кожи в области контакта. Сухая или жирная кожа, а также повреждения эпидермиса также могут быть препятствиями для надёжного извлечения минуций из изображения. Автор был свидетелем срабатывания оптического сканера на остаточные потожировые следы на сканирующей поверхности как на приложенный палец, а также их наложения на отпечаток следующего приложенного пальца.

Другим важным источником информации об отпечатке пальцев является поле ориентаций папиллярных линий [хэндбук]. Всё изображение делится на, в общем случае, прямоугольные непересекающиеся фрагменты, в пределах которых считается, что линии не меняют своей ориентации в двумерном пространстве либо меняют настолько незначительно, что остаётся возможность её аппроксимации. Интуитивно ориентацию в каждом фрагменте можно представить как линию, вдоль которой направлены папиллярные линии выбранного фрагмента. Более формально её можно определить через линейно симметричное изображение [Бигун Vision with Direction].

Определим изображение как скалярную функцию f, принимающую вещественный вектор . Пусть - единичный вектор, соответствующий некоторому направлению на области определения f. f называется линейно симметричным изображением, если существует такая функция одной переменной g, что . Тогда – направление линейной симметрии. Ориентация – это линия, перпендикулярная направлению линейной симметрии.

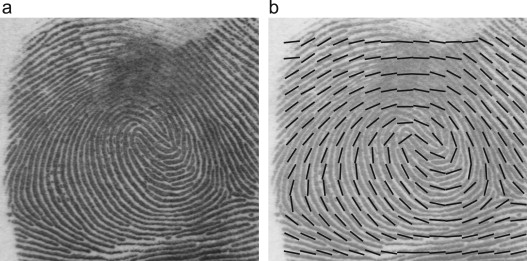


Рис.Пример поля ориентаций

Направление папиллярных линий в окрестности некоторой точки может также выделяться с помощью свёрток изображения с набором фильтров Габора, разделения окрестности точки на концентрические кольца с фиксированным числом секторов или сетку с квадратными ячейками и подсчётом среднего отклонения цветов пикселов в каждом секторе или ячейке [FingerCode, квадратный FingerCode], однако такой подход используется значительно реже.

Поле ориентаций не учитывает расстояния между соседними гребнями. По этой причине в качестве отличительных особенностей могут быть использованы спектральные данные интенсивностей пикселов в соответствующей ячейке. Их получают, например, с помощью дискретного преобразования Фурье, фильтрации Габора или выбора спектральных составляющих из дискретного набора косинусоидальных функций [ГОСТ].

Изучение сублокального уровня связано с выделением особенностей отдельных участков линий или впадин, а потому возможно с помощью сканеров высокого разрешения [Хэндбук]. На детальных изображениях видно (рис. С порами), что папиллярные линии не являются однородными, в них можно наблюдать множество белых впадин, соответствующих протокам потовым желёз (порам). Их расположение также считается уникальным [поры].