## 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:

### Биометрическая интеграция