

Лекция 2

Методы идентификации и аутентификации
Терминология и биометрические методы.

Определения

- Идентификация
- Аутентификация
- Подтверждение подлинности
- Опознавание
- Именованение
- Отождествление

Определения

ЦИЯ

[нем. Identifikation, фр. identification < ср.-лат. identificāre отождествлять].

Отождествление, установление идентичности (см. идентичный) чего-н.

Идентификация «1:N» или «1:1»

Определения

- Идентификация — это процесс распознавания элемента системы, обычно с помощью заранее определенного идентификатора или другой уникальной информации - каждый субъект или объект системы должен быть однозначно идентифицируем.
- Идентификация в информационных системах — присвоение субъектам и объектам идентификатора и / или сравнение идентификатора с перечнем присвоенных идентификаторов.
- Термин «идентификация» в отношении личности пользователей в информационной безопасности часто ошибочно используется на месте понятий аутентификация и авторизация.
- Аутентификация - это проверка подлинности идентификации пользователя, процесса, устройства или другого компонента системы (обычно осуществляется перед разрешением доступа).

Уникальные биометрические характеристики

Нужна ли
аутентификация
при использовании
биометрических
данных?

Биометрические методы идентификации

- Криминалистика. Биометрические идентификаторы используются для распознавания жертв (неопознанных трупов) и защиты детей от киднеппинга.
- Маркетинг. Используются методы биометрии для идентификации владельцев карт лояльности.
- Системы учета времени на работе, в образовательных учреждениях и т.п.
- Системы безопасности. Применяются для контроля доступа в помещение и контроля доступа к информационным ресурсам
- Системы голосования. При функционировании автоматизированной системы голосования требуется надежная идентификация/аутентификация граждан, участвующих в голосовании
- Согласно действующим международным требованиям, например стандарту ICAO, паспорта должны содержать биометрический раздел. Кроме того, с недавнего времени страны Шенгенской зоны начали выдавать биометрические визы.
- Биометрические идентификаторы применяются для учета мигрантов и иностранных работников, что позволяет идентифицировать людей даже при отсутствии документов.
- Для организации справедливого распределения социальной помощи населению (Индия, Пакистан), медицинского обслуживания применяются системы биометрической идентификации граждан.

Биометрические методы идентификации

Идентификация по любой биометрической системе проходит четыре стадии:

- Запись – физический или поведенческий образец запоминается системой;
- Выделение – уникальная информация выносится из образца и составляется биометрический образец;
- Сравнение – сохраненный образец сравнивается с представленным;
- Совпадение/несовпадение - система решает, совпадают ли биометрические образцы, и выносит решение.

Можно выделить два класса методов идентификации:

- Статические методы идентификации
- Динамические методы идентификации

Характеристики биометрических систем

- Ошибка регистрации - Failure to Enroll Rate (FTE) - определяет процент людей, не обладающих возможностью зарегистрироваться в системе. FTE может быть определена для каждого человека в отдельности.
- Если человек вообще не может быть зарегистрирован в системе или после регистрации не может быть распознан, такой случай относят к Failure to Acquire Rate (FTA) - вероятности ошибки сбора данных.
- Вероятность ложного недопуска (ошибка первого рода) - False Rejection Rate (FRR) - для зарегистрированных в системе людей определяет процент случаев отказа в доступе.
- Вероятность ложного допуска (ошибка второго рода) - False Acceptance Rate (FAR) - вероятность допуска не зарегистрированного в системе человека.

Пример значимости FAR и FRR

Можно оценить, как часто будут возникать ложные совпадения, если установить систему идентификации на проходной организации с численностью персонала N человек. Вероятность ложного совпадения полученного сканером отпечатка пальца для базы данных из N отпечатков равна $FAR \cdot N$. И каждый день через пункт контроля доступа проходит тоже порядка N человек. Тогда вероятность ошибки за рабочий день $FAR \cdot (N \cdot N)$. Вероятность ошибки за единицу времени может сильно варьироваться, но если будем считать допустимым одну ошибку в течение рабочего дня, то:

$$FAR \times N^2 \approx 1 \Rightarrow N \approx \sqrt{\frac{1}{FAR}}$$

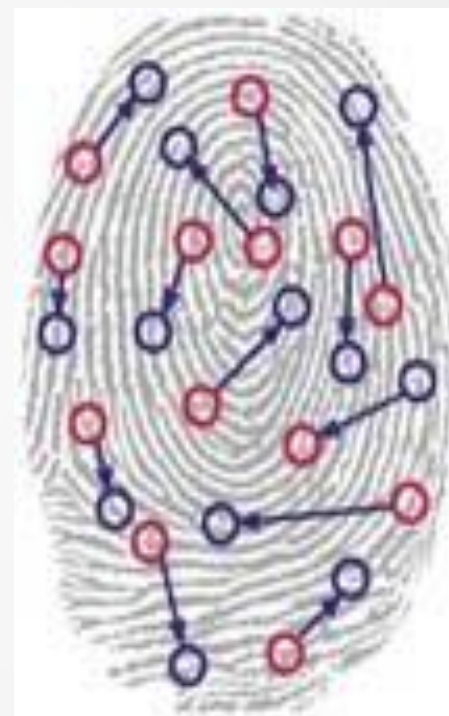
Тогда получим, что стабильная работа системы идентификации при $FAR = 0.1\% = 0.001$ возможна при численности персонала $N \approx 30$.

Дополнительные характеристики биометрических систем

- «Устойчивость к подделке» – это эмпирическая характеристика, обобщающая то, насколько легко обмануть биометрический идентификатор.
- «Устойчивость к окружающей среде» – характеристика, эмпирически оценивающая устойчивость работы системы при различных внешних условиях, таких как изменение освещения или температуры помещения.
- «Простота использования» показывает насколько сложно воспользоваться биометрическим сканером, возможна ли идентификация «на ходу».
- «Скорость работы»
- «Стоимость системы».

По отпечатку пальца

- В основе этого метода лежит уникальность для каждого человека рисунка папиллярных узоров на пальцах. Отпечаток, полученный с помощью специального сканера, преобразуется в цифровой код (свертку), и сравнивается с ранее введенным эталоном. Данная технология является самой распространенной по сравнению с другими методами биометрической аутентификации.



По отпечатку пальца

В качестве источника данных по FAR и FRR использовались статистические данные VeriFinger SDK, алгоритм VeriFinger несколько лет выигрывал международное соревнование «International Fingerprint Verification Competition», где соревновались алгоритмы распознавания по пальцу.

FAR	FRR
0,10%	0,30%
0,01%	0,40%
0,00%	0,60%
0,00%	0,90%

Характерное значение FAR для метода распознавания отпечатков пальцев – 0.001%.

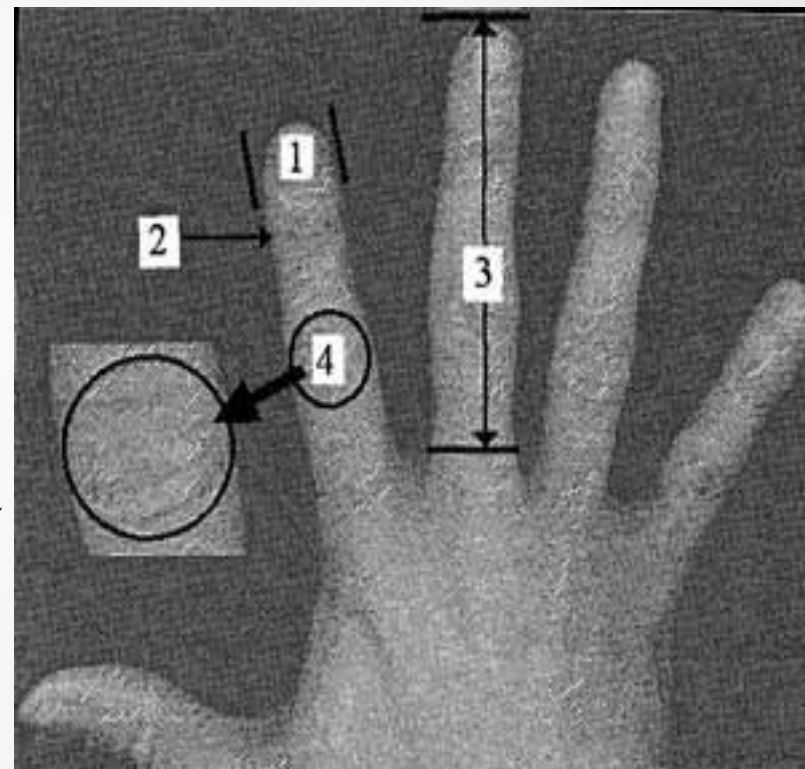
Из приведенной выше формулы получим, что стабильная работа системы идентификации при $FAR=0.001\%$ возможна при численности персонала $N \approx 300$.

По отпечатку пальца

- Преимущества метода. Высокая достоверность — статистические показатели метода лучше показателей способов идентификации по лицу, голосу, росписи. Низкая стоимость устройств, сканирующих изображение отпечатка пальца. Достаточно простая процедура сканирования отпечатка.
- Недостатки: папиллярный узор отпечатка пальца очень легко повреждается мелкими царапинами, порезами. Люди, использовавшие сканеры на предприятиях с численностью персонала порядка нескольких сотен человек заявляют о высокой степени отказа. Так же присутствует недостаточная защищённость от подделки изображения отпечатка, отчасти вызванная широким распространением метода

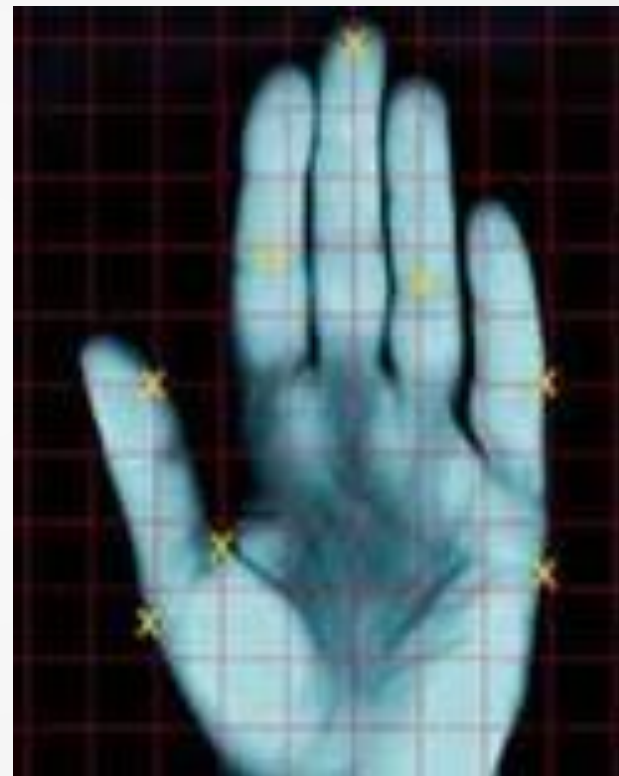
По форме ладони

- Этот метод, достаточно распространённый ещё лет 10 назад и произошедший из криминалистики в последние годы идёт на убыль. Он основан на получении геометрических характеристик рук: длин пальцев, ширины ладони и т.д. Этот метод, — умирающий, а так как у него куда более низкие характеристики.
- Возможное развитие метода м.б. связано с построением 3D изображения руки



По форме ладони

- Метод построен на геометрии кисти руки. С помощью специального устройства, состоящего из камеры и нескольких подсвечивающих диодов, которые, включаясь по очереди, дают разные проекции ладони, строится трехмерный образ кисти руки, по которому формируется свертка и идентифицируется человек.



По расположению вен

- С помощью инфракрасной камеры считывается рисунок вен на лицевой стороне ладони или кисти руки. Полученная картинка обрабатывается и по схеме расположения вен формируется цифровая свертка.



По расположению вен

- Это новая технология в сфере биометрии, широкое применение её началось всего лет 5-10 назад. Инфракрасная камера делает снимки внешней или внутренней стороны руки. Рисунок вен формируется благодаря тому, что гемоглобин крови поглощает ИК излучение. В результате, степень отражения уменьшается, и вены видны на камере в виде черных линий. Специальная программа на основе полученных данных создает цифровую свертку. Не требуется контакта человека со сканирующим устройством.
- Технология сравнима по надёжности с распознаванием по радужной оболочке глаза.
- Значение FRR и FAR приведено для сканера Palm Vein. Согласно данным разработчика при FAR 0,0008% FRR составляет 0.01%. Более точный график для нескольких значений не выдаёт ни одна фирма.

По расположению вен

- Преимущества метода. Отсутствие необходимости контактировать со сканирующим устройством. Высокая достоверность — статистические показатели метода сравнимы с показаниями радужной оболочки. Скрытость характеристики: в отличие от всех вышеприведённых — эту характеристику очень затруднительно получить от человека «на улице», например сфотографировав его фотоаппаратом.
- Недостатки метода. Недопустима засветка сканера солнечными лучами и лучами галогеновых ламп. Некоторые возрастные заболевания, например артрит — сильно ухудшают FAR и FRR. Метод менее изучен в сравнении с другими статическими методами биометрии.

По радужной оболочке глаза

- Рисунок радужной оболочки глаза также является уникальной характеристикой человека. Для ее сканирования существуют специальные портативные камеры со специализированным программным обеспечением. Оpozнaвание происходит следующим образом. Камера захватывает изображение части лица, из которого выделяется изображение глаза. Из изображения глаза выделяется рисунок радужной оболочки, по которому, строится цифровой код для идентификации человека.



По радужной оболочке глаза

- Характеристики FAR и FRR для радужной оболочки глаза наилучшие в классе современных биометрических систем (за исключением, возможно, метода распознавания по сетчатке глаза). Приведены характеристики библиотеки распознавания радужной оболочки, которые соответствуют алгоритму VeriEye. Использовались базы фирмы CASIA, полученные их сканером.
- Характерное значение FAR – 0.00001%. Согласно формуле $N \approx 3000$

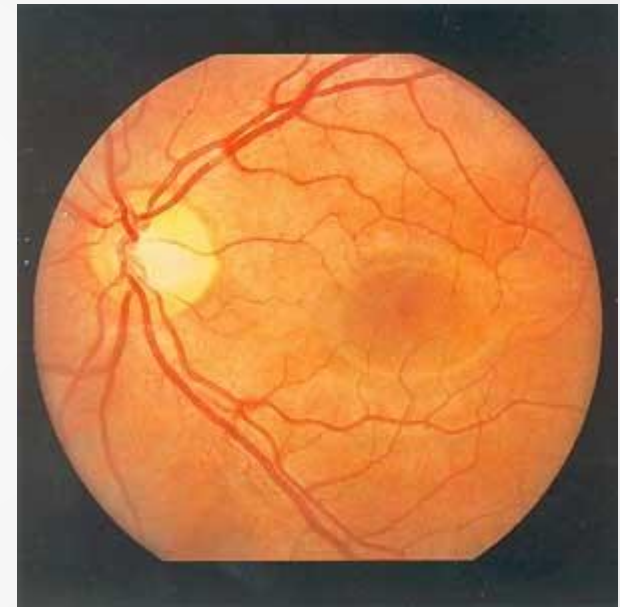
FAR	FRR(Casia1)	FRR(Casia3)
0,10%	0,05%	0,08%
0,01%	0,05%	0,09%
0,00%	0,13%	0,10%
0,00%	0,13%	0,17%
0,00%	0,13%	0,19%

По радужной оболочке глаза

- Преимущества метода. Статистическая надёжность алгоритма. Захват изображения радужной оболочки можно производить на расстоянии от нескольких сантиметров до нескольких метров, при этом физический контакт человека с устройством не происходит. Радужная оболочка защищена от повреждений — а значит не будет изменяться во времени. Так же, возможно использовать высокое количество методов, защищающих от подделки.
- Недостатки метода. Цена системы, основанной на радужной оболочке выше цены системы, основанной на распознавании пальца или на распознавании лица. Низкая доступность готовых решений.

По сетчатке глаза

- До недавнего времени считалось, что самый надёжный метод биометрической идентификации и аутентификации личности — это метод, основанный на сканировании сетчатки глаза. Он содержит в себе лучшие черты идентификации по радужной оболочке и по венам руки. Сканер считывает рисунок капилляров на поверхности сетчатки глаза. Сетчатка имеет неподвижную структуру, неизменную по времени, кроме как в результате болезни, например, катаракты.



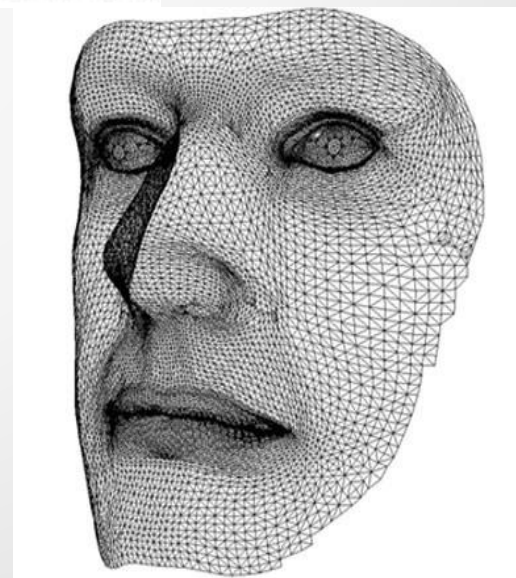
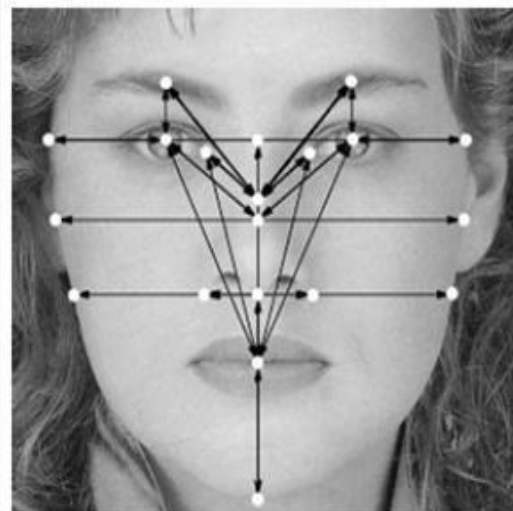
По сетчатке глаза

- Преимущества. Высокий уровень статистической надёжности. Из-за низкой распространенности систем мала вероятность разработки способа их «обмана».
- Недостатки. Сложная при использовании система с высоким временем обработки. Высокая стоимость системы. Отсутствие широкого рынка предложение и как следствие недостаточная интенсивность развития метода.

Сканеры сетчатки глаза получили широкое распространение в системах контроля доступа на особо секретные объекты, так как у них один из самых низких процентов отказа в доступе зарегистрированных пользователей и практически не бывает ошибочного разрешения доступа. По данным компании EyeDentify для сканера ICAM2001 при $FAR=0,001\%$ значение FRR составляет $0,4\%$.

По форме лица

- В данном методе идентификации строится образ (2D, 3D) лица человека. На лице выделяются контуры бровей, глаз, носа, губ и т.д., вычисляется расстояние между ними и строится не просто образ, а еще множество его вариантов на случаи поворота лица, наклона, изменения выражения. Количество образов варьируется в зависимости от целей использования данного способа (для аутентификации, верификации, удаленного поиска на больших территориях и т.д.).



По форме лица

2-D распознавание лица — один из самых статистически неэффективных методов биометрии. Появился он довольно давно и применялся, в основном, в криминалистике, что и способствовало его развитию. В следствие появились компьютерные интерпретации метода, в результате чего он стал более надёжным, но, безусловно, уступал и с каждым годом все больше уступает другим биометрическим методам идентификации личности. В настоящее время из-за плохих статистических показателей он применяется, в мультимодальной или, как ее еще называют, перекрестной биометрии, или в социальных сетях. Для FAR и FRR использованы данные для алгоритмов VeriLoo

FAR	FRR
0,10%	2,50%
0,01%	5%
0,00%	6%
0,00%	9%

По форме лица

- Преимущества метода. При 2-D распознавании, в отличие от большинства биометрических методов, не требуется дорогостоящее оборудование. При соответствующем оборудовании возможность распознавания на значительных расстояниях от камеры.
- Недостатки. Низкая статистическая достоверность. Предъявляются требования к освещению (например, не удастся регистрировать лица входящих с улицы людей в солнечный день). Для многих алгоритмов неприемлемость каких-либо внешних помех, как, например, очки, борода, некоторые элементы прически. Обязательно фронтальное изображение лица, с весьма небольшими отклонениями. Многие алгоритмы не учитывают возможные изменения мимики лица, то есть выражение должно быть нейтральным.

По форме лица

Наиболее классическим методом является метод проецирования шаблона.

Он состоит в том, что на объект (лицо) проецируется сетка. Далее камера делает снимки со скоростью десятки кадров в секунду, и полученные изображения обрабатываются специальной программой.

По полученным снимкам восстанавливается 3-D модель лица, на которой выделяются и удаляются ненужные помехи (прическа, борода, усы и очки).

Затем производится анализ модели — выделяются антропометрические особенности, которые в итоге и записываются в уникальный код, заносящийся в базу данных.

По форме лица

- Преимущества метода. Отсутствие необходимости контактировать со сканирующим устройством. Низкая чувствительность к внешним факторам, как на самом человеке (появление очков, бороды, изменение прически), так и в его окружении (освещенность, поворот головы). Высокий уровень надежности, сравнимый с методом идентификации по отпечаткам пальцев.
- Недостатки метода. Дороговизна оборудования. Имеющиеся в продаже комплексы превосходили по цене даже сканеры радужной оболочки. Изменения мимики лица и помехи на лице ухудшают статистическую надежность метода. Метод еще недостаточно хорошо разработан, особенно в сравнении с давно применяющейся дактилоскопией, что затрудняет его широкое применение.

Полные данные о FRR и FAR для алгоритмов этого класса открыто не приведены.

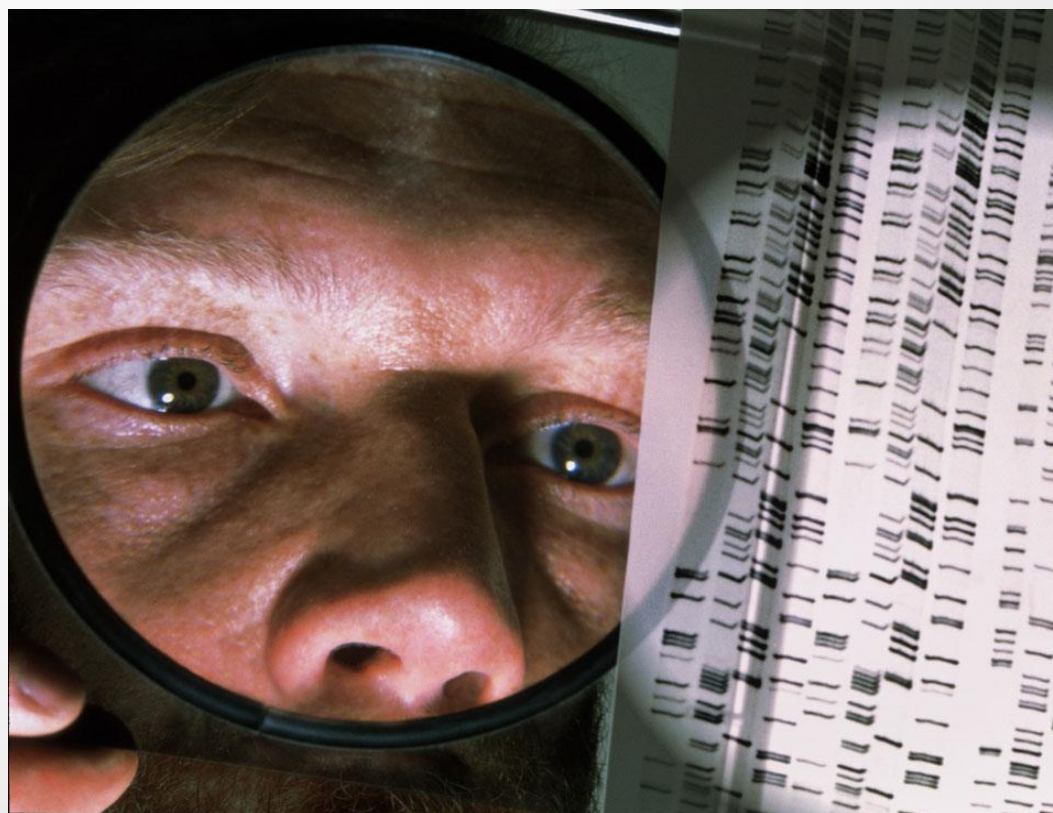
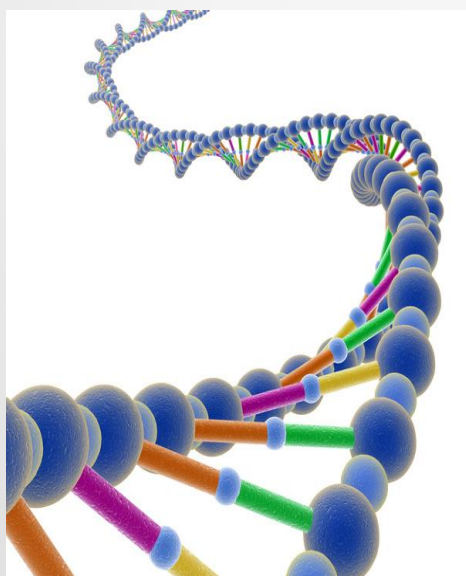
По термограмме лица

- В основе данного способа идентификации лежит уникальность распределения на лице артерий, снабжающих кровью кожу, которые выделяют тепло. Для получения термограммы, используются специальные камеры инфракрасного диапазона. В отличие от идентификации по форме лица, этот метод позволяет различать близнецов.



По ДНК

- Преимущества данного способа очевидны. Однако, существующие в настоящее время методы получения и обработки ДНК, занимают так много времени, что могут использоваться только для специализированных экспертиз.



Сравнение статических методов идентификации

Дополнительные характеристики, которые будет иметь каждая из систем по 10-ти бальной шкале

	Устойчивость к подделке	Устойчивость к окружающей среде	Простота использования	Стоимость	Скорость	Стабильность признака во времени
Рад. оболочка	10	9	8	7	10	10
Дактилоскопия	6	10	9	10	10	9
Лицо 2D/3D	4 9	6 8	6 10	10 5	10 7	8 10
Вены руки	10	7	9	7	8	7
Сетчатка	10	10	6	3	6	9

Сравнение статических методов идентификации

соотношение FAR и FRR (при фиксированном FAR)

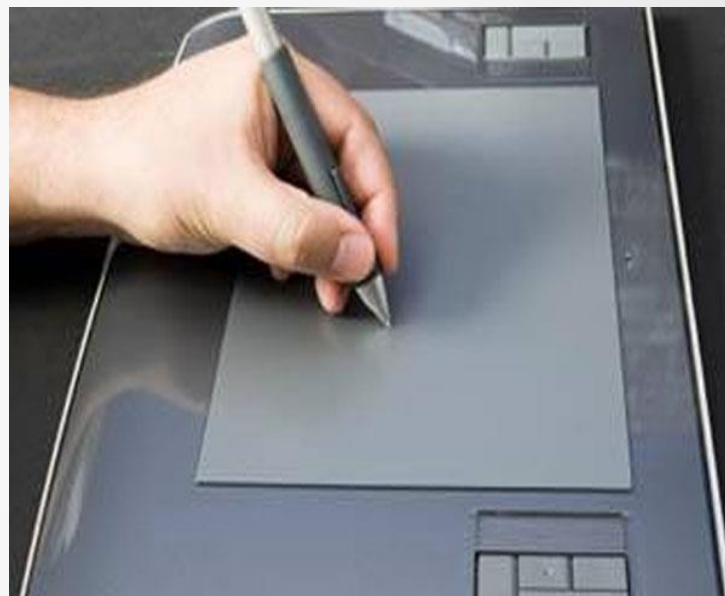
для этих систем:

	0.1%	0.01%	0.001%	0.0001%	0.00001%
Рад. Оболочка	0,07%	0,07%	0,12%	0,15%	0,16%
Дактилоскопия	0,30%	0,40%	0,60%	0,90%	-----
Лицо 2D/3D	2,5%(2D)	5%(2D) ~0,1%(3D)	6%(2D)	9%(2D)	-----
Вены руки	Нет достоверных данных				
Сетчатка	Нет достоверных данных				

По рукописному почерку

Как правило, для этого вида идентификации человека используется его роспись (иногда написание кодового слова). Цифровой код идентификации формируется, в зависимости от необходимой степени защиты и наличия оборудования (графический планшет, экран карманного компьютера Palm и т.д.), двух типов:

- По самой росписи (для идентификации используется просто степень совпадения двух картинок);
- По росписи и динамическим характеристикам написания (для идентификации строится свертка, в которую входит информация по росписи, временным характеристикам нанесения росписи и статистическим характеристикам динамики нажима на поверхность).



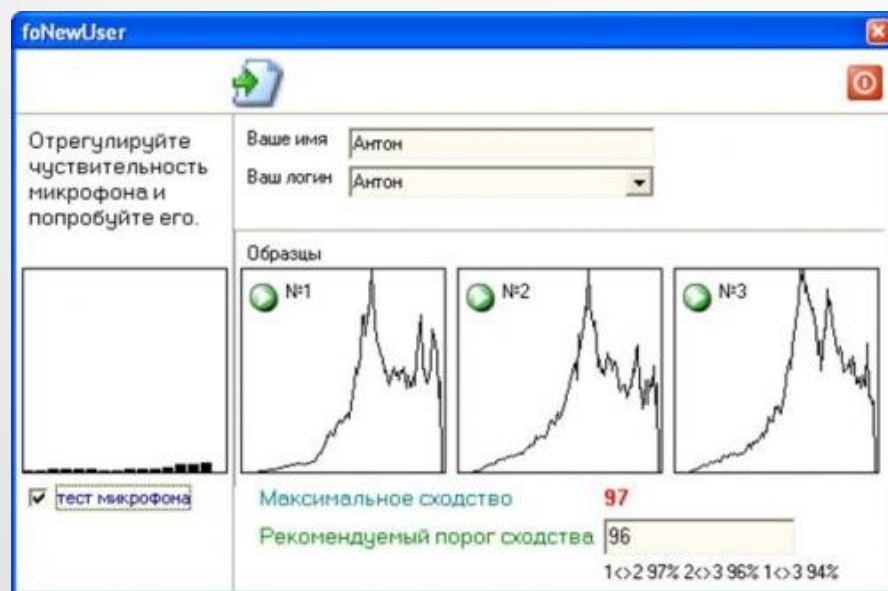
По клавиатурному почерку

Метод в целом аналогичен описанному выше, но вместо росписи используется некое кодовое слово (когда для этого используется личный пароль пользователя, такую аутентификацию называют двухфакторной) и не нужно никакого специального оборудования, кроме стандартной клавиатуры. Основной характеристикой, по которой строится свертка для идентификации, является динамика набора кодового слова.



По голосу

Это одна из старейших биометрических технологий. В настоящее время ее развитие активизировалось, ей прочится большое будущее и широкое использование в построении «интеллектуальных зданий». Существует достаточно много способов построения кода идентификации по голосу, как правило, это различные сочетания частотных и статистических характеристик голоса.



Стандарты

- WBF – Windows Biometric Framework. Данный API предоставляется компанией Microsoft начиная с ОС Windows 7 и Windows Server 2008 (для серверных версий). На данном этапе поддерживается только работа со сканерами отпечатков пальцев,
- BSAPI – собственный API компании UPEK (теперь это часть компании Authentec), который является кросс-платформенным, поддерживая Windows, OS X, Linux.
- ANSI — стандарты являющиеся результатом работы ряда структур из США. Тем не менее, многие из них стали международными, и теперь поддерживаются ISO.
 - ANSI/NIST-ITL 1-20079 - разработан для облегчения обмена данными между силовыми структурами США. В этом стандарте рассматривается метод кодирования информации о татуировках, шрамах, лицах и отпечатках.
 - NISTIR 6529-A10 - определяет формат контейнера биометрических данных (CBEFF - Common Biometric Exchange Formats Framework), но не формат самих данных. Этот стандарт написан с учетом того, чтобы он мог применяться для любого типа биометрии. В данный момент идентификатор этого документа ANSI INCITS 398. Следует заметить, что CBEFF описывает метод хранения гетерогенных типов биометрии, что позволяет внедрять системы, которые базируются на несколько типах биометрических признаков (multimodal biometrics).
 - ANSI INCITS 377-2009 – метод трансформации сырых данных отпечатка в области (клетки), с последующим расчетом математических функций, которые описывают кривые в каждой области.
 - ANSI INCITS 381 – формат хранения изображения отпечатка пальца и ладони. Данный формат используется Microsoft в Windows Biometric Framework¹¹. Следует подчеркнуть, что ОС Windows доминирует на рынке операционных систем, выбор этого формата заставляет других игроков рассмотреть добавление поддержки этого формата, особенно если существует требование взаимодействовать с Windows-системами.
 - ANSI INCITS 378 – декларирует формат хранения данных о минуциях отпечатка, а так же дает точное определение термина «минущия». Формат предусматривает возможность паковать в едином блоке информацию о разных пальцах, или разные виды одного пальца. Это компактный формат - общий размер данных о двух пальцах (по 27 и 22 минуции) – 342 байта.
 - ANSI INCITS 379 – определяет формат хранения данных об ирисе. Определяет метод хранения изображения в декартовой и в полярной системе координат, методы сжатия, количество цветов в палитре изображения, и т.д.
 - ANSI INCITS 396 – определяет формат хранения данных о геометрии руки. Данный стандарт является базой стандарта ISO/IEC NP 19794-10, который находится в стадии разработки.
 - ANSI INCITS 385 – определяет формат хранения данных о геометрии лица. В нем определяются типы фотографий лица, метрики качества фотографий, способы анализа изображения человеком и компьютером.
 - ANSI INCITS 442-2010 – определяет примитивы для удаленного доступа к биометрическим данным.
 - ANSI INCITS 429

Стандарты

- BioAPI является стандартом BioAPI Consortium, разработанным специально для унификации программных интерфейсов программного обеспечения разработчиков биометрических устройств.
- AAMVA Fingerprint Minutiae Format/National Standard for the Driver License/Identification Card DL/ID-2000 - американский стандарт на формат представления, хранения и передачи отпечатков пальцев для водительских прав. Совместим со спецификациями BioAPI и стандартом CBEFF.
- CBEFF (Common Biometric Exchange File Format) — единый формат представления биометрических данных, который предлагается для замены биометрических форматов, используемых производителями различных сегментов рынка биометрических систем, в своем оборудовании и программном обеспечении.
- CDSA/HRS (Human Recognition Services) - биометрический модуль в архитектуре Common Data Security Architecture, разработанной Intel Architecture Labs и одобренного консорциумом Open Group. CDSA определяет набор API, охватывающих разные компоненты защиты, в список которых благодаря HRS добавлена и биометрия. CDSA/HRS совместим со спецификациями BioAPI и стандартом CBEFF.
- ANSI/NIST-ITL 1-2000 Fingerprint Standard Revision – американский стандарт, определяющий общий формат представления и передачи данных по отпечаткам пальцев, лицу, нательным шрамам и татуировкам для использования в правоохранительных органах США.

Стандарты

- ГОСТ Р ИСО/МЭК 19794-2-2005 «Автоматическая идентификация. Идентификация биометрическая. Форматы обмена биометрическими данными. Часть 2. Данные изображения отпечатка пальца
- ГОСТ Р ИСО/МЭК 19794-4-2006 «Автоматическая идентификация. Идентификация биометрическая. Форматы обмена биометрическими данными. Часть 4. Данные изображения отпечатка пальцев»
- ГОСТ Р ИСО/МЭК 19794-5-2006 «Автоматическая идентификация. Идентификация биометрическая. Форматы обмена биометрическими данными. Часть 5. Данные изображения лица».
- ГОСТ Р ИСО/МЭК 19794-6-2006 «Автоматическая идентификация. Идентификация биометрическая. Форматы обмена биометрическими данными. Часть 6. Данные изображения радужной оболочки глаза».

Обилие биометрических методов

Распределение биометрического рынка в последние годы. В каждом втором источнике эти данные колеблются на 15-20 процентов, так что это всего лишь оценочное представление. Так же тут под понятием «геометрия руки» скрываются два разных метода.

