Биометрические технологии. От отпечатков пальцев к форме кисти руки.

Эссе по курсу "Защита информации",
кафедра радиотехники,
Московский физико-технический институт (ГУ МФТИ),
http://www.re.mipt.ru/infsec

Автор: Чикин Николай Владимирович, 314гр.
04.04.2007

Биометрические технологии.

Биометрические технологии – основа безопасности там, где точная аутентификация и защищенность от несанкционированного доступа к обьектам или данным имеют исключительную важность. В настоящее время биометрические технологии обеспечивают наибольшую гарантию идентификации личности. Обусловлено это тем, что в отличие от таких методов аутентификации, как: пароли, пропуска, всевозможные электронные ключи – биометрические признаки человек не может (ну или не может без нанесения увечий) подделать, потерять, украсть и передать в пользование другому лицу.

Что же представляет из себя биометрия как таковая? Биометрия – это множество методов и средств идентификации человека, основанных на физиологической или поведенческой его характеристике. Работа всех без исключения систем биометрической идентификации разделяется на две части. Первая – регистрация объекта – с помощью нескольких измерений со считывающего устройства формируется цифровая модель биометрической характеристики (в зависимости от метода: отпечаток пальца, рисунок радужной оболочки глаза и т.д.). Вторая – распознавание объекта – измерения, считанные при попытке идентификации, преобразуются в цифровую форму, которая затем сравнивается с формой, полученной при регистрации. Сравнение может быть устроено двумя способами:

- с единственной формой: Форма выбирается по предварительному вводимому определенным образом идентификатору, такому как номер или код. Результаты сравнивания возвращаются приложению — так построенная процедура называется верификацией. Процедура обычно возвращает число - вероятность того, что сравниваемые шаблоны принадлежат одной личности. Затем, если эта вероятность выше заранее определенного порога, делается вывод о том, что перед системой не злоумышленник, а лицо, зарегистрированное под введенным кодом.
- со всеми зарегистрированными формами: В качестве результата процедура возвращает несколько наиболее близких к нашей форме (сортируются по вероятности полученной при сравнении). Затем, с использованием какого-либо математического критерия принимается решение о принадлежности данной формы определенному лицу. Такая процедура называется идентификацией.

Все существующие в настоящий момент методы биометрической идентификации и верификации делятся на две группы: динамические и статические. Статические методы используют физиологические характеристики, а динамические используют поведенческие характеристики личности. Далее считаю необходимым осветить в общих чертах наиболее распространенные методы, после чего остановиться поподробнее на двух из них, а именно: идентификации по отпечаткам пальцев и форме кисти руки.

Итак, статические методы идентификации включают:

1. Идентификация по отпечатку пальца. Самый частоиспользуемый метод биометрической идентификации. В основу этого метода положена уникальность рисунка папиллярных узоров на пальцах. Идентификация построена следующим образом: с помощью сканера получается изображение отпечатка. Затем это изображение преобразуется по сложному алгоритму в специальный цифровой код, который называется сверткой. Далее свертка сравнивается с хранимыми кодами.

2. идентификация по расположению вен на ладони. Прибором, считывающим информацию в этом случае, является инфракрасная камера. В итоге на входе программы по формированию свертки появляется рисунок вен на руке человека.
3. идентификация по сетчатке глаза. В данном случае сканируется рисунок кровеносных сосудов глазного дна. Понятно, что этот рисунок наблюдается только при определенных условиях, поэтому при сканировании человек смотрит на удаленный световой источник и специальная камера сканирует его глазное дно.
4. идентификация по радужной оболочке глаза. Рисунок радужной оболочки глаза - уникален для каждого человека, поэтому и было целесообразно построить этот метод. В этом методе важна не только специальная камера, но и надежное программное обеспечение. Ведь именно с помощью программного обеспечения из изображения выделяется рисунок нужной нам радужной оболочки.
5. идентификация по форме кисти руки. Этот метод основывается на распознавание геометрических особенностей кисти руки. Специальный сканер формирует трехмерный рисунок кисти. При анализе этого рисунка выполняются измерения, с помощью которых формируется свертка.
6. идентификация по форме лица. Этот метод чем-то похож на метод идентификации по форме кисти руки. Здесь так же строится трехмерный образ лица. Специальное программное обеспечение выделяет из этого образа контуры глаз, губ и других частей лица. Далее проводятся точные измерения между этими контурами. Именно по этим данным строится свертка.
7. идентификация по термограмме лица. Здесь, как и во всех остальных методах используется уникальный признак, а именно, уникальность распределения артерий на лице. Кровеносные сосуды, покрывающие лицо человека выделяют тепло. Как и в методе идентификации по расположению вен на ладони цифровая картина расположения артерий на лице получается с помощью инфракрасной камеры.

Существует еще несколько статических методов, такие как: по ДНК, по форме уха, запаху человека. Но мы не будем на них подробно останавливаться и перейдем к краткому рассмотрению динамических методов. Их несколько меньше чем статических:

1. идентификация по голосу. В настоящее время написано множество программ по распознаванию голоса. В методе идентификации по голосу распознавание речи не играет большой роли, здесь более важны частотные характеристики голоса человека. Именно по частотным характеристикам и строится цифровая модель.
2. идентификация по почерку. При идентификации этим методом обычно исследуется подпись человека. Проверяются такие динамические характеристики, как: графические параметры, сила нажима на поверхность, скорость нанесения подписи. По этим характеристикам и строится свертка.

3. идентификация по клавиатурному почерку. Данный метод аналогичен идентификации по почерку, но вместо того, чтобы ставить автограф, человеку необходимо напечатать кодовое слово. Свертка строится по динамике набора определенного слова. Стоит заметить, что данный метод обладает невысокой надежностью, так как со временем динамика набора у отдельно взятого человека может значительно измениться.

Итак, мы кратко рассмотрели основные методы биометрической идентификации. Наиболее обширно изучен на сегодняшний день метод идентификации по отпечаткам пальцев. А наиболее интересный для меня метод – по форме кисти руки. Стоит остановиться на этих двух методах более подробно.

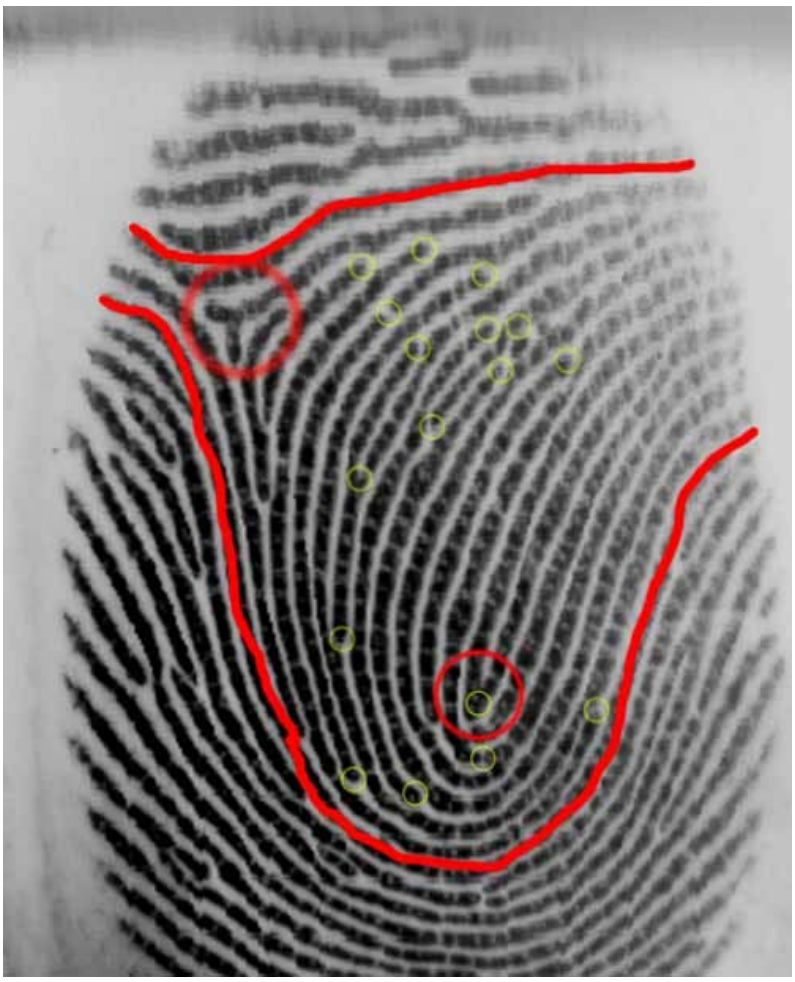
Отпечатки пальцев.

Вообще говоря, отпечатки пальцев применяются для аутентификации очень давно. Отпечаток большого пальца использовали для заключения сделок еще в Древнем Египте. Научные же исследования публиковались с 1823г.

Каждый отпечаток обладает определенными признаками, по которым и идентифицируют личность. Эти признаки можно разделить на две группы: глобальные и локальные. К глобальным признакам относят признаки, которые может увидеть глаз:

- *Папиллярный узор*.
- *Область образа* - выделенный фрагмент отпечатка, в котором локализованы все признаки.
- *Ядро* - пункт, локализованный в середине отпечатка или некоторой выделенной области.
- *Пункт "дельта"* - начальная точка. Место, в котором происходит разделение или соединение бороздок папиллярных линий, либо очень короткая бороздка (может доходить до точки).
- *Тип линии* - две наибольшие линии, которые начинаются как параллельные, а затем расходятся и огибают всю область образа.
- *Счётчик линий* - число линий на области образа, либо между ядром и пунктом "дельта".

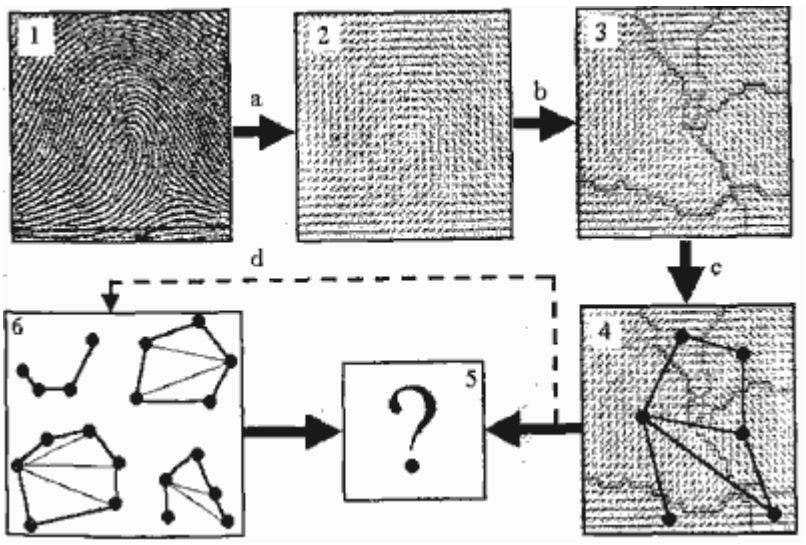
Локальные признаки, или минуции – признаки, уникальные для каждого отпечатка. Эти признаки определяют пункты изменения паппилярных линий, таких как раздвоение или разрыв, ориентацию паппилярных линий и координаты в этих пунктах.



*На данном отпечатке пальца отмечены следующие признаки: две линии - "тип линии"; то, что между ними - может выступать в качестве области образа, но обычно берётся вся площадь отпечатка; красная окружность слева - пункт "дельта"; красная окружность ниже - ядро; жёлтые окружности показывают некоторые минуции. Папиллярный узор - левая петля

Как и на любую другую технологию, на технологию идентификации по отпечаткам пальцев накладываются ограничения и требования с помощью стандартов. Наиболее распространенный стандарт – стандарт ANSI. Он определяет формат, разрешение, уровень яркости, углы поворота и типы минуций.

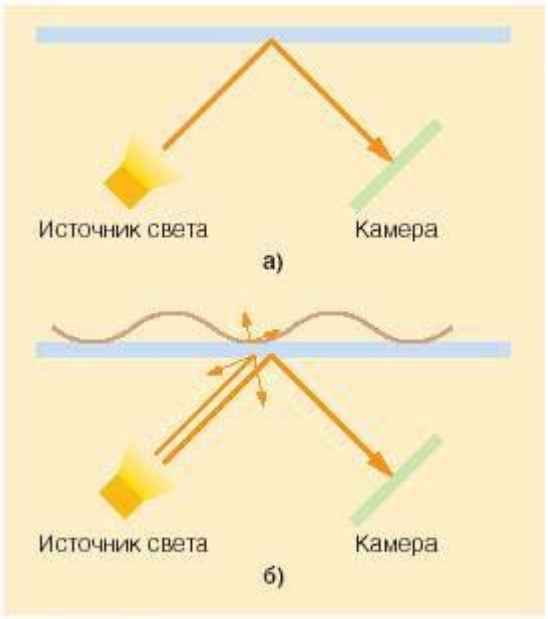
Вообще говоря, разные отпечатки могут иметь одинаковые глобальные признаки, но их всегда можно отличить по локальным признакам. Существует множество методов сравнения отпечатков, таких как сравнение по локальным признакам, сравнение по глобальным признакам и др. С развитием информационных технологий большое распространение получил алгоритм сравнения на основе графов. Коротко пояснить работу этого алгоритма поможет следующий рисунок.



На этом рисунке под номером 1 показано исходное изображение отпечатка, полученное с помощью сканера. Далее из этого изображение получают изображение поля ориентации паппилярных линий(2). На этом рисунке четко можно определить некоторые области, на которых ориентация одинаковая(3). Следующий шаг - определить центры этих областей. Соединив найденные центры, получаем определенного вида граф (4). В базе данных (6) хранятся все зарегистрированные отпечатки в виде графов. Остается только сравнить их с полученным нами графом.

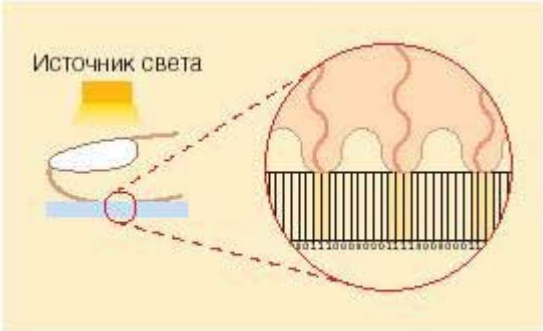
Следует уделить особое внимание приборам, помогающим получить изображение (1) – сканерам. Сканеры по своим конструктивным особенностям делятся на:

- Оптические:
  - FTIR-сканеры



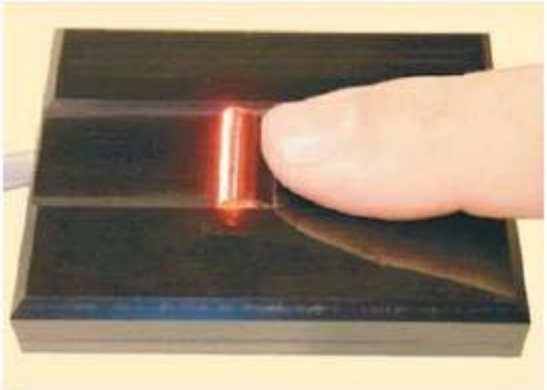
Принцип работы FTIR-сканеров

  - Оптоволоконные



Механизм работы оптоволоконных сканеров

- Оптические протяжные



Практическая реализация оптического протяжного сканера.

- Роликовые

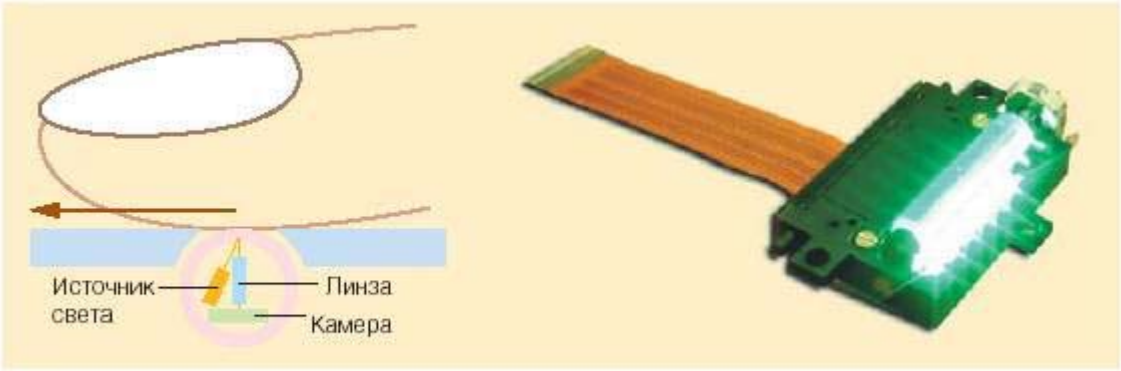
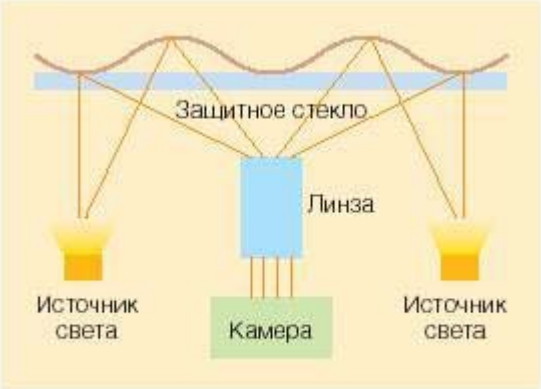


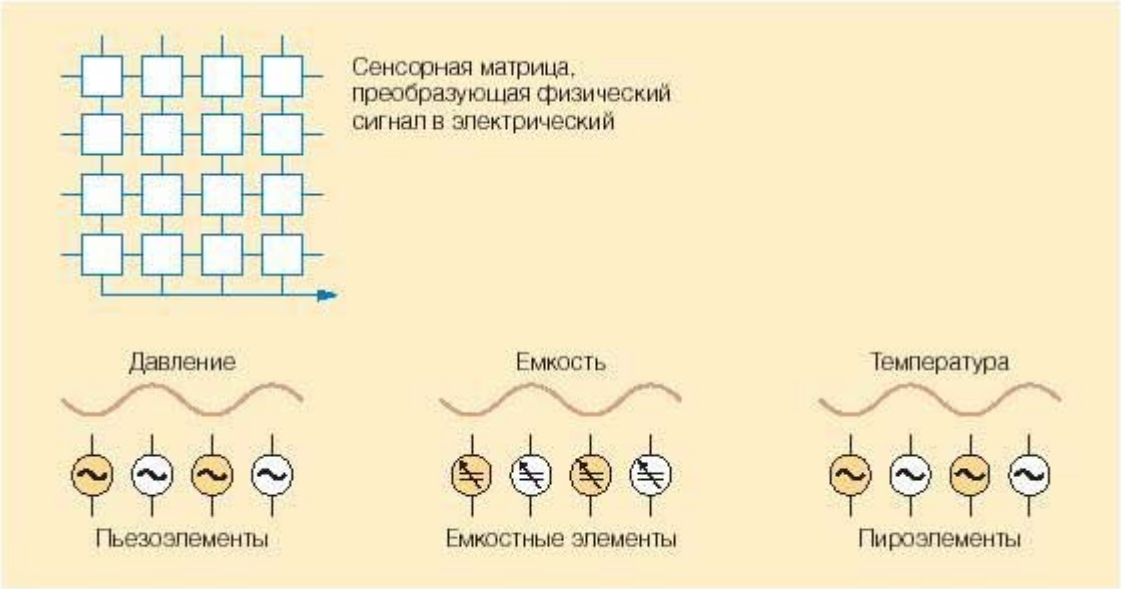
Схема роликового сканера (слева) и его реализация (справа)

- Бесконтактные



Обобщенная схема работы бесконтактного сканера

- Полупроводниковые:



Обобщенная схема работы полупроводниковых сканеров

Работа полупроводниковых сканеров основана на том, что полупроводники меняют свойства в местах контакта.

- Ультразвуковые.

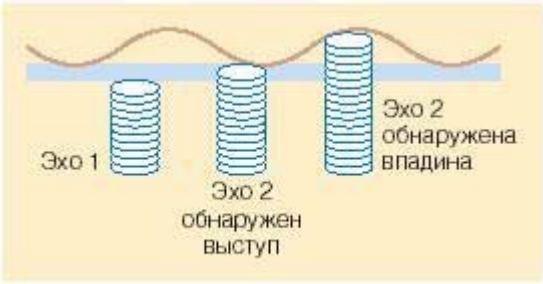


Схема работы ультразвукового сканера

Используется то обстоятельство, что ультразвук возвращается через различные промежутки времени, отражаясь от бороздок или линий.

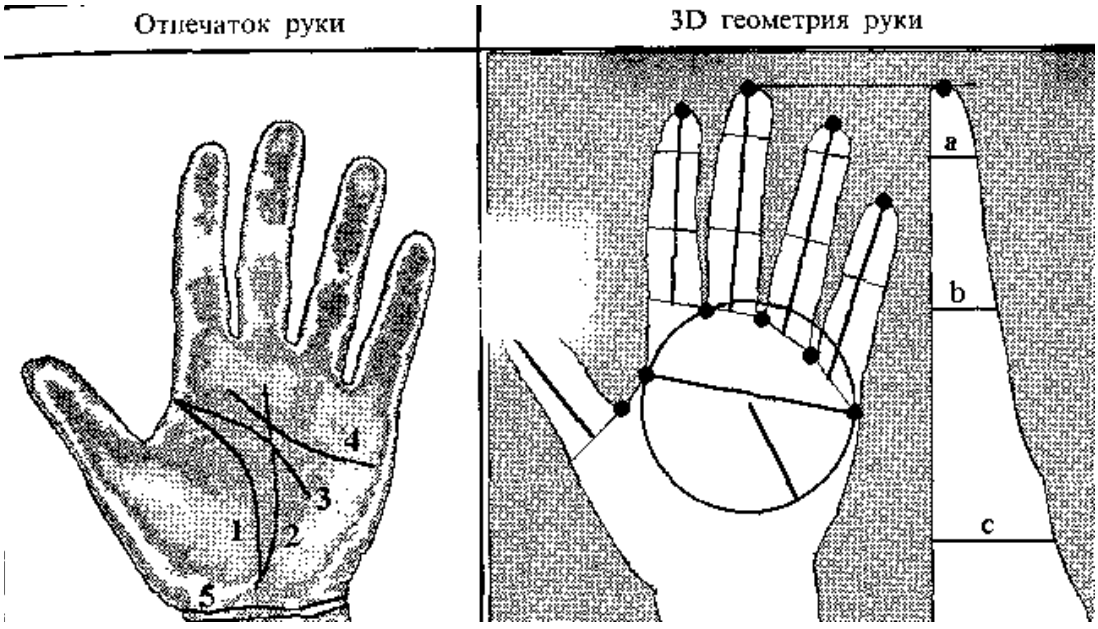
Наиболее распространены оптические сканеры, хотя они обладают меньшей надежностью, чем остальные. Например, их можно обмануть, если просто подышать на сканер, так как при этом восстановится отпечаток предыдущего человека, прошедшего аутентификацию. Полупроводниковые и ультразвуковые сканеры менее распространены, так как они дороже оптических сканеров, хотя и обладают таким преимуществом как быстродействие.

В итоге можно отметить, что сканеры отпечатков пальцев совсем не собираются сдавать позиции на рынке биометрических приборов, так как по соотношению цена/надежность им нет равных.

Форма кисти руки.

В биометрике в целях идентификации человека большое распространение получил метод аутентификации по геометрии руки. Ключевыми признаками здесь являются размер, форма руки, а также определенные информационные знаки на тыльной стороне руки.

Существует два основных подхода к использованию геометрических характеристик кисти руки. Первый из этих подходов основан чисто на геометрических характеристиках руки. Второй же вводит еще и образовые характеристики руки (образы на сгибах между фалангами пальцев и узоры кровеносных сосудов).



Узор на ладони, состоящий из пяти основных линий (слева), контрольные точки и 17 геометрических признаков руки (справа)

Основными геометрическими признаками являются: ширина ладони, радиус вписанной в ладонь окружности, длины пальцев, ширина пальцев, высота кисти руки в трёх местах. Все эти признаки объединяются в так называемый вектор значений. Метод идентификации по вектору значений достаточно прост. В начале с пользователя снимают несколько силуэтов его руки. Для каждого из этих силуэтов формируется свой вектор значений. На основе нескольких векторов значений создается специальный класс. Далее

все признаки в классе усредняются, и получаются признаки эталонного образа (или, говорят, находится центр класса). В процессе работы исходные образы могут модифицироваться. При сравнении нового образа с эталоном, в случае успеха он может быть помещен в класс исходных признаков. Сравнивать же между собой два образа можно по нескольким критериям. Наиболее очевидный из них – наименьшее расстояние от исследуемого образа до эталона. Более сложный метод – снимать четыре характеристики, три из которых – характерные размеры, а четвертая – полутоновое изображение складок кожи на сгибе между фалангами. Такой метод сильно затрудняет обман прибора. Стоит отметить, что в принципе более подробной информации по используемым характеристикам и алгоритмах сравнения найти не удастся, потому что компании, занимающиеся распознаванием по руке, не разглашают эту информации из соображений защиты от обмана их устройств.
В заключение стоит отметить, что метод идентификации по геометрии руки, построенный с использованием полутонового изображения обладает высокой надежностью. Кроме того, сканеры геометрии рук не выдвигают никаких требований к характеристикам рук (чистоте, температуре рук) и не наводят пользователей на мысли о криминалистике, как в случае сканеров отпечатков пальцев.

Литература.

1. http://ru.wikipedia.org/wiki/%D0%91%D0%B8%D0%BE%D0%BC%D0%B5%D1%82%D1%80%D0%B8%D1%87%D0%B5%D1%81%D0%BA%D0%B8%D0%B5_%D1%82%D0%B5%D1%85%D0%BD%D0%BE%D0%BB%D0%BE%D0%B3%D0%B8%D0%B8
2. http://wiki.oszone.net/index.php/%D0%91%D0%B8%D0%BE%D0%BC%D0%B5%D1%82%D1%80%D0%B8%D1%8F._%D0%92%D0%B2%D0%B5%D0%B4%D0%B5%D0%BD%D0%B8%D0%B5
3. http://wiki.oszone.net/index.php/%D0%91%D0%B8%D0%BE%D0%BC%D0%B5%D1%82%D1%80%D0%B8%D1%8F._%D0%9E%D1%82%D0%BF%D0%B5%D1%87%D0%B0%D1%82%D0%BE%D0%BA_%D0%BF%D0%B0%D0%BB%D1%8C%D1%86%D0%B0
4. http://wiki.oszone.net/index.php/%D0%91%D0%B8%D0%BE%D0%BC%D0%B5%D1%82%D1%80%D0%B8%D1%8F._%D0%93%D0%B5%D0%BE%D0%BC%D0%B5%D1%82%D1%80%D0%B8%D1%8F_%D1%80%D1%83%D0%BA%D0%B8
5. http://www.gsm-guard.net/press2_1.html