Биометрические технологии

Биометрические технологии -

- основаны на биометрии, измерении уникальных характеристик отдельно взятого человека. Это могут быть как уникальные признаки, полученные им с рождения, например: ДНК, отпечатки пальцев, радужная оболочка глаза; так и характеристики, приобретённые со временем или же способные меняться с возрастом или внешним воздействием. Например: почерк, голос или походка.

Немного истории

До 11 сентября 2001 года, биометрические системы обеспечения безопасности использовались только для защиты военных секретов и самой важной коммерческой информации. Ну а после потрясшего весь мир террористического акта ситуация резко изменилась. Сначала биометрическими системами доступа оборудовали аэропорты, крупные торговые центры и другие места скопления народа. Повышенный спрос спровоцировал исследования в этой области, что, в свою очередь, привело к появлению новых устройств и целых технологий.

Выделяют две группы систем по типу используемых биометрических параметров.

- использование статических биометрических параметров: отпечатки пальцев, геометрия руки, сетчатка глаза и т. п
- Использование динамических параметров: динамика воспроизведения подписи или рукописного ключевого слова, голос и т. п.

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.

Подавляющее большинство людей считают, что в памяти компьютера хранится образец отпечатка пальца, голоса человека или картинка радужной оболочки его глаза. Но на самом деле в большинстве современных систем это не так. В специальной базе данных хранится цифровой код длиной до 1000 бит, который ассоциируется с конкретным человеком, имеющим право доступа. Сканер или любое другое устройство, используемое в системе, считывает определённый биологический параметр человека. Далее он обрабатывает полученное изображение или звук, преобразовывая их в цифровой код. Именно этот ключ и сравнивается с содержимым специальной базы данных для идентификации личности.

Практическое применение

Биометрические технологии активно применяются во многих областях связанных с обеспечением безопасности доступа к информации и материальным объектам, а также в задачах уникальной идентификации личности. Биометрические технологии в скором будущем будут играть главную роль в вопросах персональной идентификации во многих сферах. Применяемые отдельно или используемые совместно со смарт-картами, ключами и подписями, биометрия скоро станет применяться во всех сферах экономики и частной жизни.

Биометрия определяет целый ряд важных терминов:

- FAR (False Acceptence Rate) — процентный порог, определяющий вероятность того, что один человек может быть принят за другого (коэффициент ложного доступа)(также именуется «ошибкой 2 рода»). Величина 1 − *FAR* называется специфичность.
- FRR (False Rejection Rate) — вероятность того, что человек может быть не распознан системой (коэффициент ложного отказа в доступе)(также именуется «ошибкой 1 рода»). Величина 1 − *FRR* называется чувствительность.
- Verification — сравнение двух биометрических шаблонов, один к одному. См. также: биометрический шаблон
- Identification — идентификация биометрического шаблона человека по некой выборке других шаблонов. То есть идентификация — это всегда сравнение один ко многим.
- Biometric template — биометрический шаблон. Набор данных, как правило в закрытом, двоичном формате, подготавливаемый биометрической системой на основе анализируемой характеристики. Существует стандарт CBEFF на структурное обрамление биометрического шаблона, который также используется в BioAPI

Технологии

- Отпечатки пальцев - отпечатки всех пальцев каждого человека уникальны по рисунку папиллярных линий и различаются даже у близнецов. Отпечатки пальцев не меняются в течение всей жизни взрослого человека, они легко и просто предъявляются при идентификации.
- Радужная оболочка глаза - Ученые также провели ряд исследований, которые показали, что сетчатка глаза человека может меняться со временем, в то время как радужная оболочка глаза остается неизменной. И самое главное, что невозможно найти два абсолютно идентичных рисунка радужной оболочки глаза, даже у близнецов.
- Сетчатка глаза - Ранее в биометрии имел применение рисунок кровеносных сосудов на сетчатке глаза. В последнее время этот метод распознавания не применяется, так как кроме биометрического признака несет в себе информацию о здоровье человека.

- Форма кисти руки - проблема технологии: даже без учёта возможности ампутации, заболевание под названием «артрит» может сильно помешать применению сканеров.
- Распознавание голоса - проблема технологии: некоторые люди не могут произносить звуки, голос может меняться в связи с заболеванием.
- Почерк - классическая верификация (идентификация) человека по почерку подразумевает сличение анализируемого изображения с оригиналом. Именно такую процедуру проделывает например оператор банка при оформлении документов. Очевидно, что точность такой процедуры, с точки зрения вероятности принятия неправильного решения (см. FAR & FRR) невысокая