Биометрическая аутентификация

Виды биометрических аутентификаторов

Биометрические аутентификаторы относятся к разряду «что-то, чем являюсь» и представляют собой анатомические и поведенческие особенности человека. В отличие от паролей, которые можно забыть, или аппаратных ключей, которые можно потерять, биометрические характеристики всегда при аутентифицируемом (исключая особо страшные случаи, когда для предъявления отпечатков пальцев человека подвергают насильственнной ампутации). Еще одним преимуществом аутентификаторов из разряда «что-то, чем являюсь» по сравнению с аутентификаторами, относящимися к классам «что-то, что знаю» и «что-то, что имею», является то, что их нельзя передать другому человеку. Хотя остается криминальная возможность предъявлять носителя биометрических характеристик против его воли для получения доступа к защищенным системам.

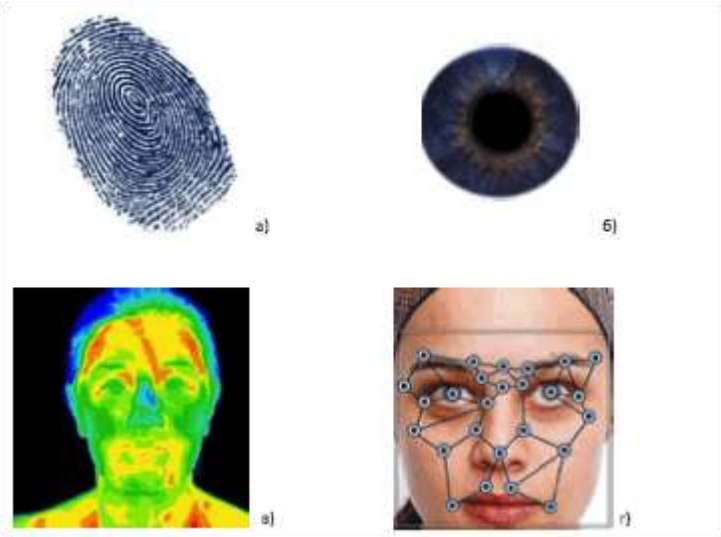

Рис. 2.23. Статические анатомические характеристики: а) отпечатки пальцев; б) рисунок радужной оболочки глаза; в) термограмма лица; г) черты лица

Наиболее часто для распознавания человека используются следующие *статические* анатомические характеристики (рис. 2.23):

- рисунки папиллярных сосудов на пальцах (отпечатки пальцев);
- овал лица, относительное расположение глаз, носа, рта. Для определения уникального шаблона, соответствующего определенному человеку, требуется от 12 до 40 характерных элементов. Шаблон должен учитывать множество вариаций изображения на случаи поворота лица, наклона, изменения освещённости, изменения выражения;
- термограмма лица;
- рисунок радужной оболочки или сетчатки глаза;
- геометрические параметры ладони, рисунок линий ладони.

К числу наиболее «говорящих» *динамических* характеристик (поведенческих черт) человека относятся:

- характеристики речи (рис. 2.24);

- особенности письма вообще и личной подписи, в частности;
- особенности походки;
- особенности набора текста на клавиатуре (скорость ввода парольной фразы, характерные ошибки, временные интервалы между нажатиями разных клавиш и др.).

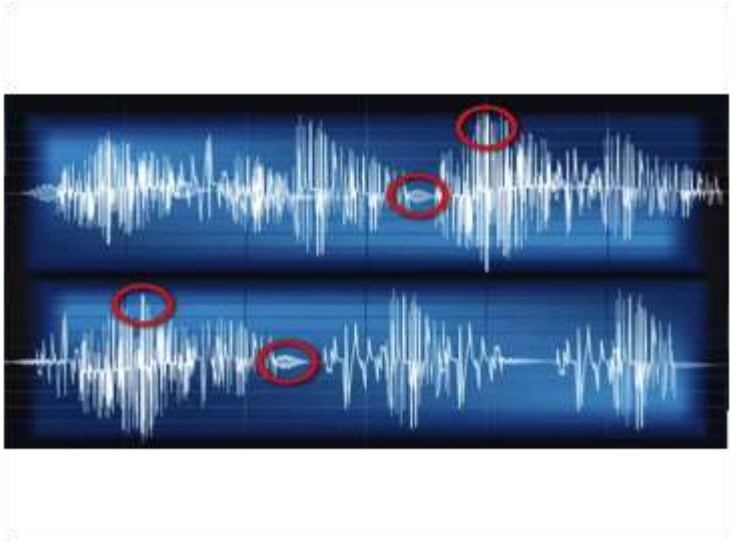

Рис. 2.24. Анализ особенностей речи с целью аутентификации

Алгоритм биометрической аутентификации

Алгоритм биометрической аутентификации аналогично всем остальным способам аутентификации включает ***процедуру регистрации***, во время которой в базу данных системы заносятся характеристики пользователей, необходимые для установления их аутентичности.

Процедура регистрации выполняется с привлечением специальных устройств для взятия ***биометрических образцов***. Эти устройства отражают специфику используемых для аутентификации анатомических признаков: для снятия отпечатков пальцев используются различные виды сканеров, для получения изображений лица и радужной оболочки глаза - фотокамеры, для получения термограммы лица - камеры инфракрасного диапазона, для взятия образцов голоса - звукозаписывающие устройства (рис. 2.25). Затем из биометрического образца с помощью специальной программы извлекают ***шаблон*** - данные, уникально характеризующие конкретного человека. Полученный шаблон, представляющий собой компактный код (в некоторых случаях до нескольких байтов), помещается в базу данных системы.

Рис. 2.25. Примеры конструктивного выполнения сканеров а) прокатный сканер отпечатков одного пальца, б) оптический сканер отпечатков пальцев, в) сканер сетчатки глаза, г) устройство для снятия параметров ладони.

Собственно ***процедура аутентификации*** включает те же действия: взятие биометрического образца и извлечения шаблона - экстракта индивидуальных черт объекта аутентификации. Актуальный шаблон сравнивается с шаблоном из базы данных системы. Если произошло совпадение, то аутентификация произошла успешно (рис. 2.26) .

Остановимся на некоторых «подводных камнях» этой простой схемы, которые могут прояснить причины того, что биометрическая аутентификация все еще не получила того широкого распространения, которое казалось бы она заслуживает. В отличии от паролей и способов аутентификации, использующих электронные ключи, биометрическое распознавание основано не на точном совпадении, а на степени соответствия, поэтому здесь более вероятны ошибки, причем ошибки двух родов.

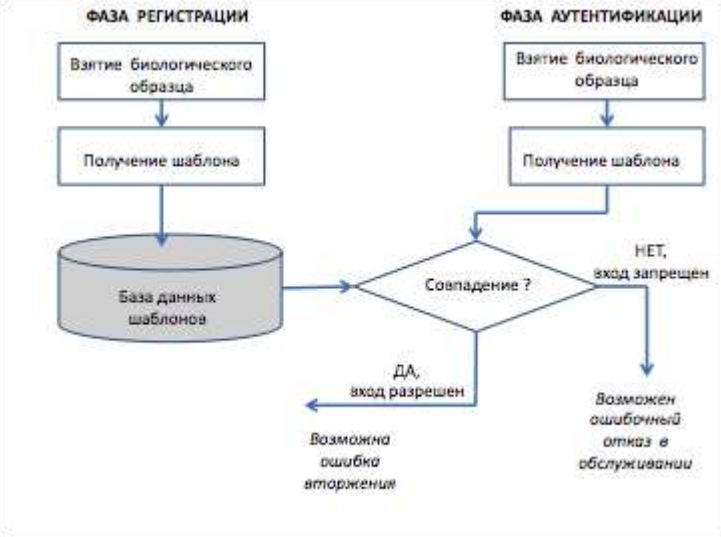

Рис. 2.26. Алгоритм биометрической аутентификации

Во-первых, система может *отказать в обслуживании легальному пользователю*, если его отличительные биометрические черты изменились. А вероятность этого отнюдь не нулевая. Например, вы можете порезать палец и быть отлученным от доступа к своему компьютеру в течение недели, а то и двух. На качество отпечатка пальца может повлиять наличие крема, чернильного пятна, мозоли и проч. и проч. Если вы выполняете голосовую аутентификацию, то на нее может повлиять болезнь, внешняя температура, влажность, шум – музыка, работа транспорта и др. Особенно эти проблемы проявляются при аутентификации в мобильных устройствах – планшетах, телефонах, ноутбуках.

Во-вторых, система аутентификации может *позволить злоумышленнику осуществить вторжение*. Ошибки такого рода могут возникать как из-за того, что индивидуальные особенности аутентифицируемого были неправильно оценены системой как совпадающие с характеристиками другого человека, так и в результате атак, предпринятых на систему аутентификации. Помимо нарушений безопасности универсального характера (инсайдеры, DoS, трояны, вирусы и др.) биометрические системы могут быть подвергнуты атакам, эксплуатирующим специфические уязвимости таких систем. В частности, существует угроза использования подделки в ходе взятия биометрического образца, например в сканер или другое устройство распознавания может быть представлены модель пальца или реальный мертвый палец, искусственное воссоздание лица, обманным путем полученные

образцы голоса и др. Для противодействия этому виду атак разрабатываются различные методы распознавания неживого состояния объекта, у которого берутся пробы.

Другим видом атак на систему биометрической аутентификации являются несанкционированный доступ и копирование шаблонов из базы данных. Обладание шаблоном в некоторых случаях дает возможность злоумышленнику решить обратную задачу - генерации биометрического образца, который, будучи представлен во время аутентификации, даст значение шаблона, совпадающее с похищенным из базы данных.

Обеспечение безопасности биометрических аутентификаторов имеет еще один аспект – защита персональных данных. Закон строго регламентирует их использование, поскольку украденные биометрические данные могут использоваться для слежки за человеком или его компроментации. Поэтому в базах данных современных биометрических систем шаблоны создаются таким образом, чтобы из них нельзя было восстановить исходные биометрические характеристики, а следовательно, использовать в криминальных целях. То есть процедура получения шаблона из исходного биометрического образца должна работать подобно односторонней хеш-фунции – быстрое получение компактного уникального дайджеста (шаблона) и отсутствие возможности обратного вычисления по дайджесту исходного значения функции (биометрического образца).

В табл. 2.6 представлены некоторые достоинства и недостатки биометрических систем аутентификации.

Табл. 2.6. Достоинства и недостатки биометрических систем аутентификации

Достоинства	**Недостатки**
Пользователю удобно использовать аутентификатор, который всегда «с собой»	Вероятностный характер распознавания приводит к ложным срабатываниям
Аутентификатор не может быть передан другому человеку	Биометрические параметры могут со временем изменятся по разным причинам: болезнь, возраст, изменение состояния внешней среды
Аутентифицируемый, пройдя аутентификацию, не сможет в дальнейшем отречься от своих действий	Возможна подмена, насильственное изъятие и фабрикация биометрического материала
Многие современные электронные устройства (компьютеры, телефоны и др.) готовы для внедрения биометрической аутентификации, поскольку изначально оснащены средствами снятия биометрических образцов: фотокамерами, звукозаписывающими системами.	Единожды скомпрометированный биометрический аутентификатор нельзя сменить на другой
Биометрические параметры достаточно просто могут быть использованы в двухфакторной аутентификации, например в комбинации с паролем	Сложности обеспечения безопасности персональных данных человека