Министерство образования Республики Беларусь
Учреждение образования
«Белорусский государственный университет
информатики и радиоэлектроники»

Кафедра защиты информации

А. М. Прудник, Г. А. Власова, Я. В. Рощупкин

БИОМЕТРИЧЕСКИЕ МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ

Рекомендовано УМО по образованию в области информатики и радиоэлектроники в качестве учебно-методического пособия для специальности 1-98 01 02 «Защита информации в телекоммуникациях»

Минск БГУИР 2014

УДК 612.087.1:004.056.5(076)
ББК 5я73+32.811я73
П85

Р е ц е н з е н т ы:
кафедра автоматизированных систем управления войсками
учреждения образования «Военная академия Республики Беларусь»
(протокол №11 от 25.06.2012);

декан факультета электросвязи учреждения образования
«Высший государственный колледж связи»,
кандидат технических наук, доцент С. М. Джержинский

Прудник, А. М.
П85 Биометрические методы защиты информации : учеб.-метод. пособие / А. М. Прудник, Г. А. Власова, Я. В. Рощупкин. – Минск : БГУИР, 2014. – 123 с. : ил.

ISBN 978-985-488-904-7.

Рассмотрены вопросы обеспечения контроля доступа и защиты информации с помошью биометрических методов и средств, общие понятия и определения биометрии. Приведены классификация, а также сравнительный анализ основных (отпечатки пальцев, геометрия руки, радужная оболочка глаза, изображение лица, подпись, голос) и дополнительных биометрических параметров (ДНК, сетчатка глаза и др.), их информационных признаков, этапов сравнения. Рассмотрены виды ошибок систем аутентификации. Проанализированы принципы выбора биометрических параметров для систем контроля доступа, а также виды атак на биометрические системы.

Представленное учебно-методическое пособие будет весьма полезным для студентов телекоммуникационных специальностей и специалистов в области контроля доступа и защиты информации.

УДК 612.087.1:004.056.5(076)
ББК 5я73+32.811я73

ISBN 978-985-488-904-7

СОДЕРЖАНИЕ

1. АУТЕНТИФИКАЦИЯ И БИОМЕТРИЧЕСКИЕ ПАРАМЕТРЫ

Надежная **аутентификация**, т. е. определение личности обращающейся стороны, становится необходимым атрибутом повседневной жизни. Сегодня люди используют ее при совершении самых обычных действий: при посадке на самолет, проведении финансовых операций и т. д.

Существует три традиционных **способа аутентификации** (и/или **авторизации**, т. е. разрешения доступа к ресурсу) [1]:

1) *по собственности* – физическим предметам, таким, как ключи, паспорт и смарт-карты;

2) *по знаниям* – информации, которая должна храниться в секрете и которую может знать только определенный человек, например пароль или парольная фраза. Знания могут представлять собой относительно конфиденциальную информацию, которая может и не быть секретной, например девичья фамилия матери или любимый цвет;

3) *по биометрическим параметрам* – физиологическим или поведенческим характеристикам, по которым можно отличить людей друг от друга.

Три способа аутентификации могут использоваться в комбинации, особенно при автоматической аутентификации. Например, банковская карта как собственность требует знаний (пароль) для совершения операций, паспорт – это собственность с изображением лица и подписью, которая относится к биометрическим параметрам.

Так как предметы могут быть утеряны или подделаны, а знания можно забыть или передать другому человеку, методы определения личности и доступа к ресурсам на основании знаний и собственности являются ненадежными. Для надежной аутентификации личности и безопасного обмена информацией между сторонами следует использовать биометрические параметры. Биометрические параметры человек не может подделать, потерять, украсть или передать в пользование другому лицу без нанесения увечий. В настоящее время биометрические технологии обеспечивают наибольшую гарантию определения личности и составляют основу безопасности там, где точная аутентификация и защищенность от несанкционированного доступа к объектам или данным имеют исключительную важность.

1.1. Общие понятия об аутентификации и биометрических параметрах

Биометрическая аутентификация, или **биометрия** – это наука об аутентификации личности по физиологическим или поведенческим отличительным характеристикам.

Физиологические биометрические параметры, такие, как отпечатки пальцев или геометрия руки, являются физическими характеристиками, которые обычно измеряются в определенный момент времени. *Поведенческие* биометрические параметры, например подпись или голос, представляют собой последовательность действий и длятся в течение определенного периода времени.

Физиологические биометрические параметры достаточно разнообразны и одного их образца обычно бывает достаточно для сравнения. Что касается поведенческих биометрических параметров, то отдельный образец может и не давать достаточных для идентификации личности сведений, но само временное изменение сигнала (под влиянием поведения) содержит необходимую информацию.

Физиологические (статические) и поведенческие (динамические) биометрические параметры взаимно дополняют друг друга. Основное преимущество статической биометрии – относительная независимость от психологического состояния пользователей, малые затраты их усилий и, следовательно, возможность организации биометрической идентификации больших потоков людей.

Сегодня в автоматических аутентификационных системах наиболее часто используются шесть биометрических параметров (табл. 1.1).

Таблица 1.1

Основные биометрические параметры

Физиологические	Поведенческие
Отпечатки пальцев	Подпись
Радужная оболочка	
Геометрия руки	Голос
Лицо	

Также ведутся работы по использованию дополнительных биометрических параметров (табл. 1.2).

Таблица 1.2

Дополнительные биометрические параметры

Физиологические	Поведенческие
ДНК	Походка
Форма ушей	
Запах	
Сетчатка глаза	Клавиатурный почерк
Кожное отражение	
Термограмма	

Биометрические параметры обладают свойствами [2], которые позволяют применять их на практике:

1) *всеобщность*: каждый человек имеет биометрические характеристики;

2) *уникальность*: для биометрии нет двух людей, обладающих одинаковыми биометрическими характеристиками;

3) *постоянство*: биометрические характеристики должны быть стабильны во времени;

4) *измеряемость*: биометрические характеристики должны быть измеряемы каким-либо физическим считывающим устройством;

5) *приемлемость*: совокупность пользователей и общество в целом не должны возражать против измерения/сбора биометрических параметров.

Совокупность этих свойств определяет эффективность использования биометрии в целях защиты информации.

Однако не существует биометрических параметров, абсолютно удовлетворяющих любому из этих свойств, как и параметров, которые бы сочетали в себе все эти свойства одновременно, особенно если принимать в расчет пятое свойство – приемлемость. Это означает, что не существует универсального биометрического параметра, и использование любого биометрического метода защиты определяется назначением и требуемыми характеристиками информационной системы.

Система защиты информации, основанная на биометрической аутентификации, должна удовлетворять требованиям, которые часто несовместимы друг с другом. С одной стороны, она должна гарантировать безопасность, которая предполагает высокую точность аутентификации и низкий уровень ошибок. С другой стороны, система должна быть удобной для пользователей и обеспечить необходимую скорость вычисления. Одновременно должны быть удовлетворены требования к конфиденциальности. При этом стоимость системы должна допускать возможность ее применения на практике.

К числу сложностей, возникающих при разработке и применении биометрических систем, относятся также юридические аспекты использования биометрии, а также проблемы физической безопасности и защиты данных, управления правами доступа и восстановления систем при поломке.

Поэтому любой метод биометрической аутентификации – результат многих компромиссов.

Во всех системах биометрической аутентификации можно выделить две подсистемы (рис. 1.1):

1) *регистрации объекта* (с помощью нескольких измерений со считывающего устройства формируется цифровая модель биометрической характеристики (**биометрический шаблон**));

2) *распознавания объекта* (измерения, считанные при попытке аутентификации, преобразуются в цифровую форму, которая затем сравнивается с формой, полученной при регистрации).

Различают два биометрических **метода сравнения**:

1) **верификация** – сравнение с единственным шаблоном, выбранным на основании определенного уникального идентификатора, который выделяет конкретного человека (например идентификационный номер или код), т. е. сравнение двух биометрических шаблонов один к одному (1:1);

2) **идентификация** – сравнение измеренных параметров (биометрического шаблона человека) со всеми записями из базы зарегистрированных пользователей, а не с одной из них, выбранной на основании какого-то идентификатора, т. е. в отличие от верификации идентификация представляет собой сравнение один ко многим (1 : m).

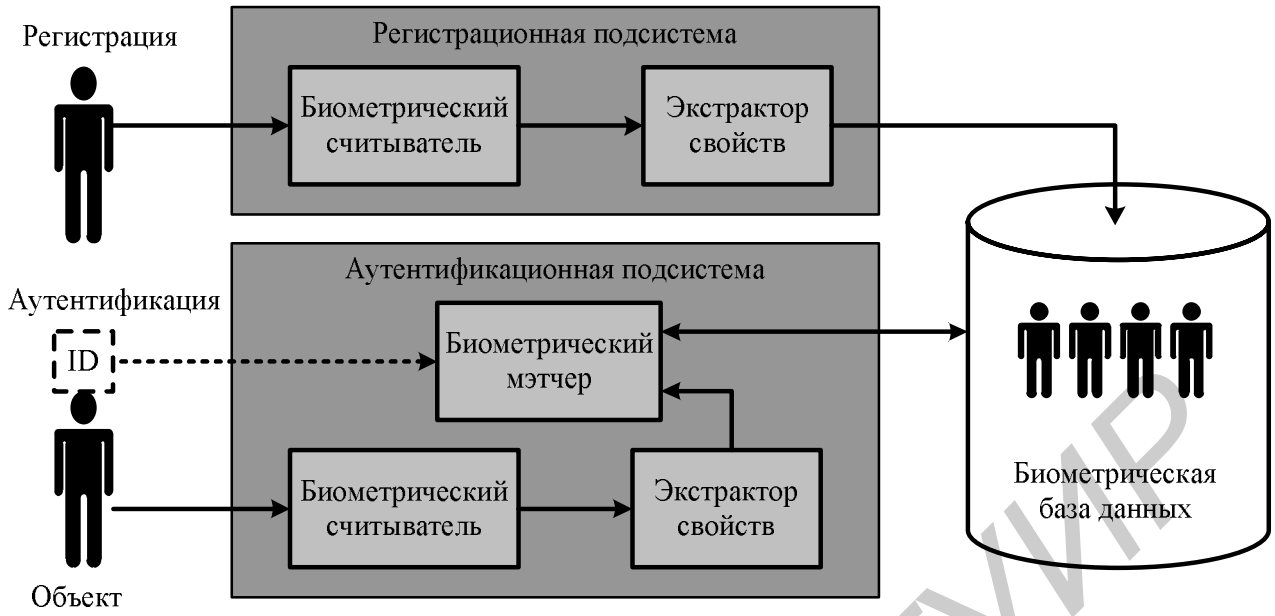


Рис. 1.1. Биометрическая аутентификационная система

Биометрическая регистрация (рис. 1.2) – это процесс регистрации объектов в биометрической базе данных. Во время регистрации биометрические параметры объекта фиксируются, значимая информация собирается экстрактором свойств и сохраняется в базе данных. При помощи определенного идентификационного номера (уникальная комбинация цифр) машинная репрезентация биометрического параметра связывается с другими данными, например с именем человека. Эта часть информации может быть помещена на каком-либо предмете, например на банковской карте.

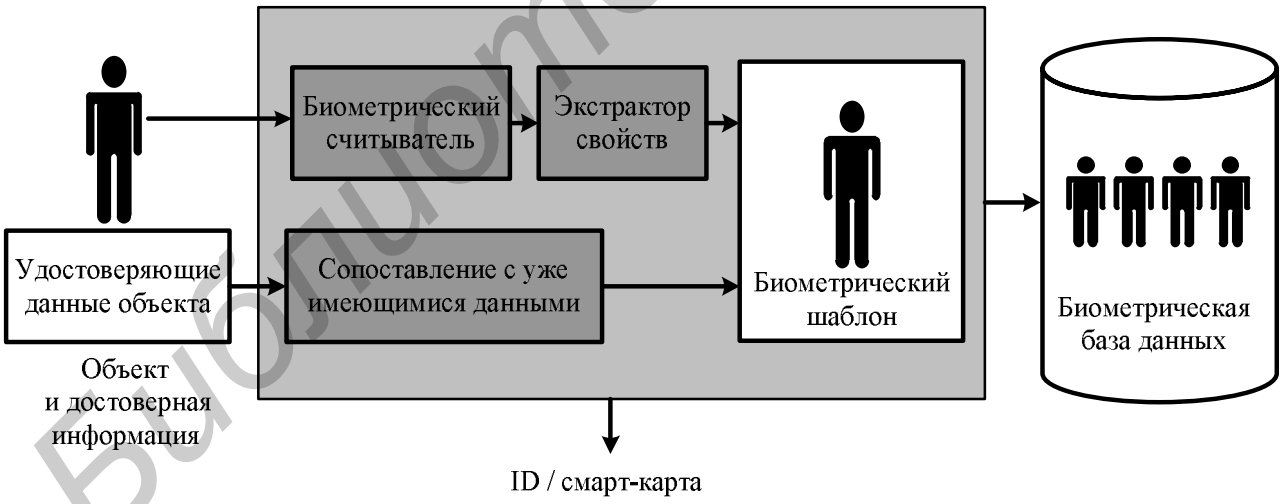


Рис. 1.2. Биометрическая регистрация

Положительная регистрация – регистрация для верификации и положительной идентификации. Цель такой регистрации – создать базу данных легитимных объектов. При регистрации объекту выдается идентификатор.

Отрицательная регистрация – регистрация для негативной идентификации – представляет собой сбор данных об объектах, которые не допускаются к каким-либо приложениям. Базы данных являются централизованными. Биометриче-

ские образцы и другие удостоверяющие данные сохраняются в отрицательной идентификационной базе данных. Это может быть сделано принудительно или тайно, без содействия самого объекта и его согласия.

Регистрация основывается на информации о пользователе в форме «достоверных данных», т. е. из официальных документов или других надежных источников, таких, как свидетельство о рождении, паспорт, ранее созданные базы данных и государственные базы данных преступников. Установление сходства производится человеком, что является потенциальным источником ошибок.

Задача **аутентификационного модуля** – распознать объект на более поздней стадии и идентифицировать одного человека среди многих других либо верифицировать личность, определив совпадение ее биометрических параметров с заданными.

Для **идентификации** система получает биометрический образец от объекта, выделяет из него значимую информацию и ищет в базе данных совпадающие с ним записи. Для биометрической идентификации используются только биометрические характеристики. На рис. 1.3 показаны основные блоки, из которых состоит биометрическая идентификационная система. Шаблоны из базы данных сравниваются с представленным образцом один за другим. В конце процедуры система выдает список идентификаторов, которые имеют сходство с введенным биометрическим параметром.

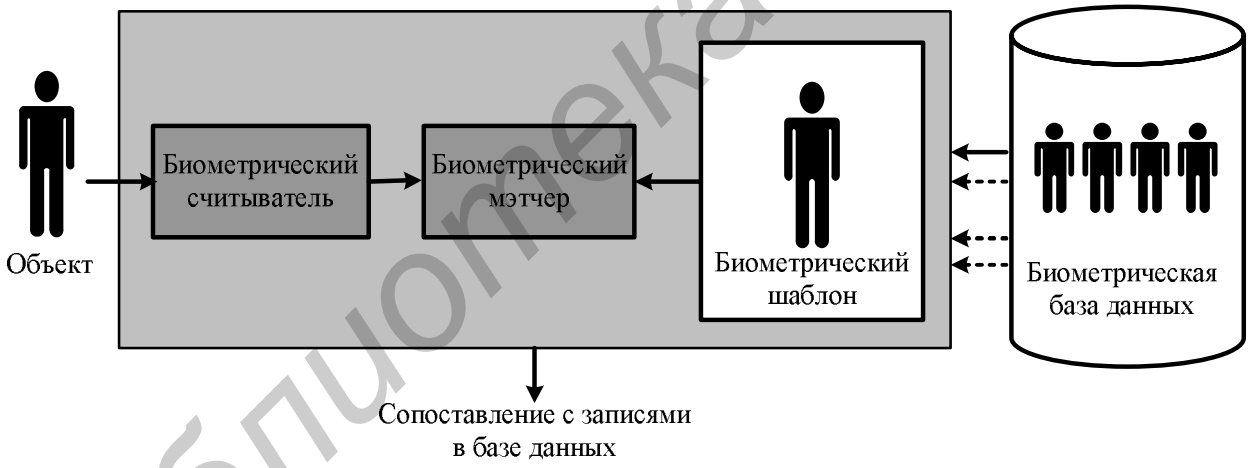


Рис. 1.3. Биометрическая идентификация

Идентификационная система может работать в двух различных режимах:

1) **положительная идентификация** (система определяет, зарегистрирована ли данная личность в базе данных. При этом могут быть допущены ошибки *ложного доступа* или *ложного отказа доступа.* Сходна с верификацией);

2) **отрицательная идентификация** (система проверяет *отсутствие* объекта в некоторой отрицательной базе данных. Это может быть, например, база данных разыскиваемых преступников. Могут возникнуть ошибки пропуска сходства – *ложное отрицание* и ошибки ложного определения сходства – *ложное признание*).

Биометрическая **верификация** отличается от идентификации тем, что представленные биометрические образцы сопоставляются с одной зарегистрированной

записью в базе данных. Пользователь предоставляет какую-нибудь собственность, которая указывает на один биометрический шаблон из базы данных.

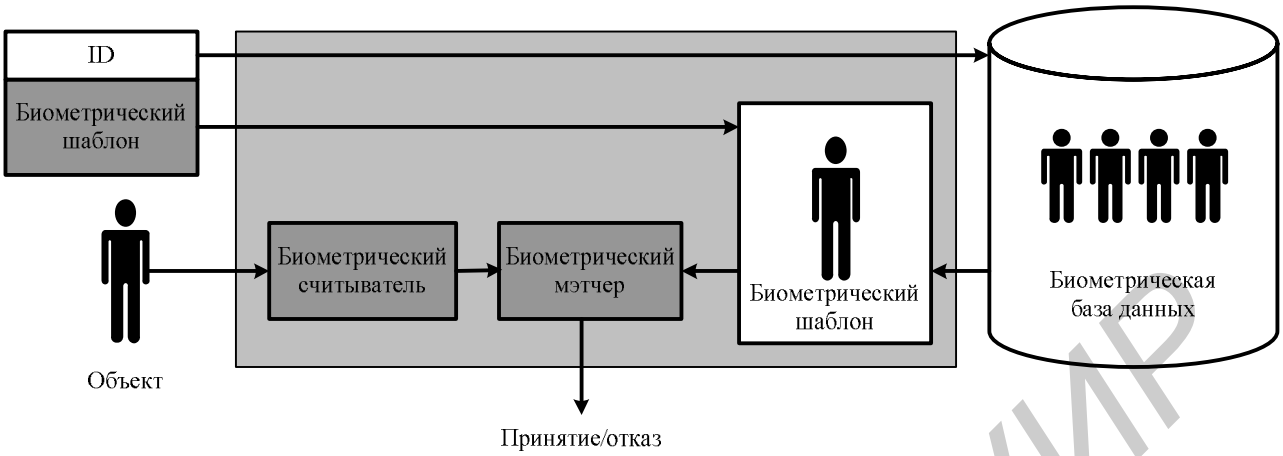


Рис. 1.4. Биометрическая верификация

Для верификации объект представляет какой-либо идентификатор (идентификационный номер, банковскую карту) и биометрические параметры. Система считывает биометрические показатели, выделяет определенные параметры, сравнивает их с параметрами, зарегистрированными в базе данных под номером данного пользователя. После этого система определяет, действительно ли пользователь является тем, кем он себя заявляет, или нет. Презентация уникального идентификатора на рис. 1.1 показана пунктирной стрелкой.

Различают централизованные и распределенные базы данных.

Централизованная база данных хранит биометрическую информацию всех зарегистрированных объектов.

Распределенная база данных хранит биометрическую информацию в распределенном виде (например на смарт-картах). Объект предоставляет системе один биометрический шаблон, записанный на каком-нибудь носителе, например на смарт-карте. Биометрическая система сравнивает этот шаблон с биометрическим образцом, предоставленным человеком.

На практике многие системы используют базы данных обоих типов – распределенную для ежедневной офлайновой верификации и централизованную для онлайновой верификации или для перевыпуска карт в случае потери без повторного измерения биометрических параметров.

Подавляющее большинство людей считает, что в базе данных хранятся образцы 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, который ассоциируется с конкретным человеком, имеющим право доступа. Сканер или любое другое устройство, используемое в системе, считывает определенный 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.

Таким образом, в основе любой биометрической системы лежат считывание (уникальная информация выносится из физического и/или поведенческого образца и составляется биометрический образец), сопоставление (представленный образец сравнивается с сохраненным образцом из базы данных) и принятие решений (система определяет, совпадают ли биометрические образцы и выносит решение о повторении, окончании или изменении процесса аутентификации).

1.2. Аутентификационные протоколы

Работа любой аутентификационной системы реализуется по определенному протоколу. Протокол – это определенная последовательность шагов двух или более сторон, которые собираются решить какую-либо задачу. Порядок шагов очень важен, поэтому протокол регулирует поведение обеих сторон. Все стороны соглашаются с протоколом или по крайней мере понимают его.

Возьмем в качестве примера телефонный разговор. После набора номера звонящий слышит гудки и вслед за этим щелчок, когда на другом конце снимают трубку. По протоколу человек, отвечающий на звонок, должен заговорить первым, сказав «Алло!» или как-то назвав себя. После этого называет себя инициатор. Только выполнив все действия в такой последовательности, можно начать разговор. Если просто поднять трубку и ничего не ответить, разговор может вовсе не состояться, так как общепринятый порядок действий будет нарушен. Даже если звонящий человек услышит щелчок, без словесного подтверждения соединения он не может начать разговор первым. Стандартное начало телефонного разговора является примером протокола.

Аутентификационный протокол – это (автоматизированный) процесс принятия решения, действительно ли удостоверяющие данные объекта являются достаточными для подтверждения его личности, чтобы разрешить ему доступ на основе этих удостоверяющих данных или других знаков. Любой аутентификационный протокол, в котором используются различные методы (и различные биометрические идентификаторы), может быть определен и выполнен на основе представленных удостоверяющих данных [3].

Аутентификационный протокол должен быть [4]:

– *установлен заблаговременно* (протокол полностью определяется и разрабатывается до его применения. Последовательность прохождения протокола и правила, регулирующие работу, должны быть определены. Также должны быть обозначены критерии, по которым будет определяться совпадение аутентификационных удостоверяющих данных);

– *взаимно согласован* (все участвующие стороны должны быть согласны с протоколом и следовать установленному порядку);

– *недвусмысленным* (ни одна из сторон не может нарушать последовательность шагов по причине их непонимания);

– *детальным* (для любой ситуации должен быть определен порядок действий. Это означает, к примеру, что в протоколе предусмотрена обработка исключительных случаев).

В современном мире компьютеры и коммуникации используются как средства получения доступа к услугам, привилегиям и различным приложениям. Операторы таких систем обычно незнакомы с пользователями, и решение о предоставлении или запрете доступа должно в большей степени определяться без вмешательства человека. Пользователь не может доверять операторам и другим пользователям системы вследствие анонимности регистрации и удаленности, поэтому необходимы протоколы, по которым две не доверяющие друг другу стороны смогут взаимодействовать. Эти протоколы, в сущности, и будут регулировать поведение. Аутентификация тогда будет проводиться согласно протоколу между пользователем и системой, пользователь сможет авторизоваться и получить доступ к приложению.

Сам по себе протокол не гарантирует безопасности. Например, протокол, контролирующий доступ в какой-либо организации, может определять часы работы, но не будет способствовать повышению уровня безопасности.

Для надежной аутентификации и обеспечения защиты обмена информацией на основе договоренностей двух сторон могут быть использованы криптосистемы.

1.3. Особенности способов аутентификации

Традиционные методы аутентификации (по собственности, по знаниям и по биометрическим параметрам [1]) использовались задолго до того, как потребовалась автоматическая электронная аутентификация. Эти методы развивались по мере совершенствования технологий печати, фотографии и автоматизации.

P – по собственности. Любой человек, имеющий определенный предмет, например ключ или с магнитной полосой карту, может получить доступ к приложению (т. е. быть авторизован). Например, любой, кто имеет ключи от машины, может на ней ездить.

K – по знаниям. Люди, имеющие определенные знания, имеют право на получение доступа. Аутентификация здесь основана на секретных знаниях, таких, как пароль, шифр замка и ответы на вопросы. Важное слово в данном определении – «секретные»: знания должны храниться в секрете для обеспечения безопасности аутентификации.

Можно выделить несекретную информацию, которая важна для аутентификации. Идентификационный номер пользователя компьютера или банковский счет часто запрашиваются для аутентификации, и так как они не являются секретными, это не предотвращает попыток имитировать их хозяина для получения доступа.

B – по биометрическому параметру. Это характерная особенность человека, которая может быть как-то измерена (или с нее может быть получен образец) в форме биометрического идентификатора и которая отличает человека от всех других людей. Ею сложно обменяться, ее сложно украсть или подделать в отличие от собственности и знаний, ее нельзя изменить.

Собственность и знания в виде (*номер счета, пароль*) = (*собственность, знания*) = (*P*, *K*), являются наиболее распространенным аутентификационным методом (протоколом). Этот метод применяется для контроля доступа к компьютеру, в Интернет, локальную сеть, к электронной и голосовой почте и т. д. При использовании

аутентификационных методов P и K происходит сравнение информации, при этом пользователь (реальный человек) не связывается с более или менее установленной «личностью». Но личность, определяемая по владению собственностью P, связывается с анонимным паролем K, а не с реально зарегистрированным человеком.

Аутентификационный биометрический метод B обеспечивает дополнительную защиту благодаря невозможности замены биометрических параметров, поэтому этот метод, а именно установление подлинности пользователей, является более надежным.

В табл. 1.3 показаны четыре метода аутентификации пользователя, которые широко используются в наше время. Так как биометрические параметры являются неотъемлемыми свойствами человека, их очень тяжело подделать без его ведома и тем более невозможно ими обменяться; кроме того, биометрические характеристики человека могут измениться только в случае серьезной травмы, некоторых болезней или разрушения тканей. Поэтому биометрические идентификаторы могут подтвердить личность пользователя в аутентификационном протоколе, что не способны сделать другие методы аутентификации, в которых используются собственность и знания. При комбинации последнего метода (B) в табл. 1.3 с методом P и/или K мы получим дополнительные биометрические методы, такие, как (P, B) (например, паспорт, смарт-карта и биометрический шаблон); для кредитных карт часто используется сочетание:

$$(P, K, B) \Rightarrow \{P = \text{кредитная карта}, K = \text{девичья фамилия матери}, B = \text{подпись}\}.$$

Таблица 1.3

Существующие методы аутентификации и их свойства

Метод	Примеры	Свойства
То, что мы имеем (P)	Кредитные карты, бэджи, ключи	Можно обменять, сделать дубликат, может быть украдено или потеряно
То, что мы знаем (K)	Пароль, ПИН, девичья фамилия матери, личная информация	Большинство паролей несложно угадать, их можно передать другим и забыть
То, что мы имеем и то, что мы знаем (P и K)	Кредитная карта и ПИН	Можно передать другим, ПИН можно узнать (его нередко пишут на карте)
Уникальные характеристики пользователя (B)	Отпечатки пальцев, лицо, радужная оболочка, запись голоса	Невозможно передать другим, отказ от авторства маловероятен, очень сложно подделать, нельзя потерять или украсть

Границы между собственностью и знаниями могут быть нечеткими. Например, идентифицирующие части предмета (собственности) могут быть оцифрованы и храниться в сжатом виде, как последовательность насечек на ключе. Это в некотором смысле преобразует собственность в знания.

Тем не менее этот метод идентификации относится к физическим, потому что аутентификация производится при помощи физического объекта, а не информации самой по себе, даже если создание экземпляра происходит на основе информации. Номер кредитной карты (который может быть использован и в Интернете и по телефону) – это знание, но кредитная карта (которая используется в банкомате) – это собственность. Кроме того, секретные знания можно тоже отнести к биометрии, так как они измеряемы и являются уникальным свойством человека.

Подпись как биометрический параметр (и в меньшей степени голос) включает в себя знания. Это значит, что подпись может быть изменена по желанию, но и подделать ее будет легче. Это побуждает исследователей, занимающихся проблемами автоматического распознавания подписей, изучать примеры атак злоумышленников, использующих фальсификации.

Фундаментальная разница между биометрической аутентификацией и другими аутентификационными методами – это понятие степени сходства, основа технологии сравнения. Аутентификационный протокол, использующий пароль, всегда выдает точный результат: если пароль правильный, система разрешает доступ, если нет – отказывает. Таким образом, здесь не существует понятия вероятности сходства. Следовательно, не возникает задачи точного определения сходства. Биометрические технологии всегда *вероятностные* и используют статистические методы, чтобы проанализировать вероятность сходства. Всегда сохраняется малый, иногда крайне малый шанс, что у двух людей могут совпасть *сравниваемые* биометрические образцы. Это выражается в терминах коэффициентов ошибок (коэффициентов ложного доступа и ложного отказа доступа) и на вероятности внутренних ошибок (минимальный достижимый коэффициент ошибок для данного биометрического параметра), которые связаны с биометрической аутентификационной системой и биометрическими идентификаторами.

Преимуществом паролей над биометрией является *возможность их смены*. Если пароль был украден или потерян, его можно отменить и заменить новой версией. Это становится невозможным в случае с некоторыми вариантами биометрии. Если параметры чьего-либо лица были украдены из базы данных, то их невозможно отменить либо выдать новые.

Разработано несколько методов отменяемой биометрии. Отменяемая биометрия представляет собой искажение биометрического изображения или свойств до их согласования. Одним из частных вариантов решения может быть, например, использование не всех биометрических параметров. Например, для идентификации используется рисунок папиллярных линий только двух пальцев (к примеру, больших пальцев правой и левой руки). В случае необходимости (например, при ожоге подушечек двух «ключевых» пальцев) данные в системе могут быть откорректированы так, что с определенного момента допустимым сочетанием будет указательный палец левой руки и мизинец правой (данные которых до этого не были записаны в систему – и не могли быть скомпрометированы).

1.4. Гибридные методы аутентификации

Одной из важных проблем биометрической аутентификации является способность сравнивать различные параметры, например, пароли и знания, и биометрические идентификаторы.

Для аутентификации по *гибридному методу* используется один или несколько способов или признаков $T = \{P$ (*по собственности*), K (*по знаниям*), B (*по биометрическим параметрам*)$\}$. Для персональной аутентификации каждый признак, предоставляемый пользователем, нужно сравнить с признаком, сохраненным при регистрации. Чтобы принять решение о сходстве данных признаков, необходимо интегрировать результаты сопоставления разных устройств сравнения, которые верифицируют признаки. Сравнение собственности или простых знаний типа пароля проводится путем точного сравнения.

Следует рассмотреть два вопроса:

1) *объединение удостоверяющих данных* (лучшим вариантом было бы объединение двух или более аутентификационных методов. Соотнесение собственности P или знания K с биометрическими параметрами B сводит задачу биометрической идентификации к биометрической верификации, т. е. уменьшает ее до сопоставления 1:1 вместо сопоставления 1:m);

2) *объединение биометрических параметров* (запрашиваемые удостоверяющие данные могут включать в себя разные биометрические параметры, т. е. $\{B1, B2\}$, где $B1$ – палец, а $B2$ – лицо. Возможность объединения нескольких биометрических параметров является объектом повышенного внимания исследователей и проектировщиков).

Таким образом, использование любого из перечисленных методов – P, K или B – означает, что должна существовать возможность сопоставления посредством верификации собственности и знания и сравнения биометрического параметра. Знаки собственности и знания требуют точного совпадения. Биометрическое сопоставление может быть до определенной степени приблизительным.

1.5. Требования к биометрической аутентификации

Биометрическая аутентификация личности становится трудной задачей, когда требуется высокая точность, т. е. низкая вероятность ошибок. Кроме того, пользователь не должен иметь возможность впоследствии отрицать проведенную им операцию и одновременно испытывать как можно меньше неудобств при прохождении процедуры аутентификации (возможность бесконтактного считывания, дружественность интерфейса, размеры файла-шаблона (чем больше размер образа, тем медленнее идет распознавание) и т. д.). При этом система аутентификации должна соответствовать также требованиям конфиденциальности и быть устойчивой к подделке (несанкционированному доступу). Следует учитывать также устойчивость биометрических аутентификационных систем к окружающей среде (эксплуатационные качества могут терять стабильность в зависимости от окружающих условий).

Таким образом, **основные требования**, предъявляемые к биометрическим системам, следующие:

1) точность (всегда ли система принимает правильное решение об объекте);

2) скорость вычисления и возможность масштабирования баз данных;

3) обработка исключительных случаев, когда биометрические параметры объекта не могут быть зарегистрированы (например, в результате болезни или увечья);

4) стоимость (в том числе затрат на обучение пользователей и персонала);

5) конфиденциальность (обеспечение анонимности; данные, полученные во время биометрической регистрации, не должны использоваться с целями, на которые зарегистрированный индивид не давал согласия);

6) безопасность (защита системы от угроз и атак).

Известно, что наиболее слабое место биометрических технологий – существующая вероятность обмана аутентификационной системы при помощи подражания. Безопасность биометрической аутентификационной системы зависит от силы связей зарегистрированных объектов с более точными «проверенными данными», такими, как паспорт. Она также зависит и от качества самих проверенных данных. Для аутентификации нужно использовать такие биометрические параметры, которые не будут создавать новых уязвимых мест и лазеек в системе безопасности. Если биометрическая аутентификационная система должна гарантировать высокий уровень защиты, нужно серьезно подойти к выбору биометрического параметра. Биометрическая аутентификация должна быть частью комплексной системы безопасности, которая включает в себя в том числе и средства защиты биометрической системы. Безопасность системы обеспечивается путем устранения уязвимостей в *точках атак*, т. е. для защиты «ценных активов» приложения, например, посредством предотвращения *перехвата* информации.

2. ОСНОВНЫЕ БИОМЕТРИЧЕСКИЕ ПАРАМЕТРЫ

Существует шесть наиболее часто используемых (основных) биометрических параметров. В их число входят: пальцы, лицо, голос (распознавание говорящего), геометрия руки, радужная оболочка глаза, подпись.

2.1. Распознавание отпечатков пальцев

Дактилоскопия – это установление личности человека по отпечаткам пальца, а точнее, по так называемому папиллярному узору. Дактилоскопия основывается на том, что, во-первых, отпечаток пальца уникален (за всю историю дактилоскопии не было обнаружено двух совпадающих отпечатков пальцев, принадлежащих разным лицам), а во-вторых, папиллярный узор не меняется на протяжении всей жизни человека.

Кожный покров пальцев рук имеет сложный рельефный рисунок (папиллярный узор), образованный чередующимися валиками (высотой 0,1–0,4 мм и шириной 0,2–0,7 мм) и бороздками-углублениями (шириной 0,1–0,3 мм). Папиллярный узор полностью формируется на седьмом месяце развития плода. Более того, в результате проведенных исследований было установлено, что отпечатки пальцев различны даже у однояйцовых близнецов, хотя показатели ДНК у них идентичные.

Кроме того, папиллярный узор невозможно видоизменить – ни порезы, ни ожоги, ни другие механические повреждения кожи не имеют принципиального значения, ибо устойчивость папиллярного узора обеспечивается регенеративной способностью основного слоя эпидермиса кожи. Поэтому можно утверждать, что сегодня дактилоскопия представляет собой самый надежный способ идентификации личности.

2.1.1. Методы сравнения отпечатков пальцев

Несмотря на многообразие строения папиллярных узоров, они поддаются четкой классификации, обеспечивающей процесс их индивидуализации и идентификации.

В каждом отпечатке пальца можно определить два типа признаков – глобальные и локальные. Глобальные признаки – те, которые можно увидеть невооруженным глазом. Другой тип признаков – локальные. Их называют минуциями – уникальные для каждого отпечатка признаки, определяющие пункты изменения структуры папиллярных линий (окончание, раздвоение, разрыв и т.д.), ориентацию папиллярных линий и координаты в этих пунктах.

Практика показывает, что отпечатки пальцев разных людей могут иметь одинаковые глобальные признаки, но совершенно невозможно наличие одинаковых микроузоров минуций. Поэтому глобальные признаки используют для разделения базы данных на классы и на этапе аутентификации. На втором этапе распознавания используют уже локальные признаки.

2.1.1.1 Принципы сравнения отпечатков по локальным признакам

Этапы сравнения двух отпечатков:

Этап 1. Улучшение качества исходного изображения отпечатка. Увеличивается резкость границ папиллярных линий.

Этап 2. Вычисление поля ориентации папиллярных линий отпечатка. Изображение разбивается на квадратные блоки со стороной больше 4 пкс и по градиентам яркости вычисляется угол *t* ориентации линий для фрагмента отпечатка.

Этап 3. Бинаризация изображения отпечатка. Приведение к черно-белому изображению (1 бит) пороговой обработкой.

Этап 4. Утончение линий изображения отпечатка. Утончение производится до тех пор, пока линии не будут шириной 1 пкс (рис. 2.1).

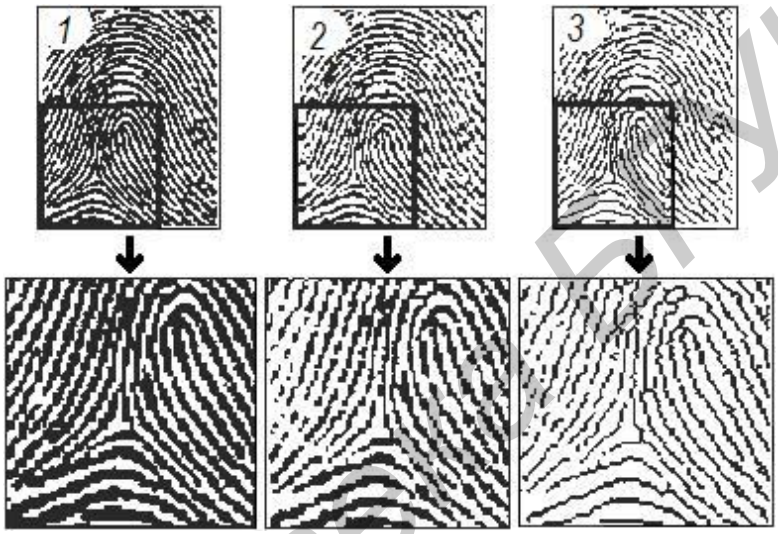


Рис. 2.1. Утончение линий изображения отпечатка

Этап 5. Выделение минуций (рис. 2.2). Изображение разбивается на блоки 9×9 пикселей. После этого подсчитывается число черных (ненулевых) пикселей, находящихся вокруг центра. Пиксель в центре считается минуцией, если он сам ненулевой и соседних ненулевых пикселей один (минуция «окончание») или два (минуция «раздвоение»).

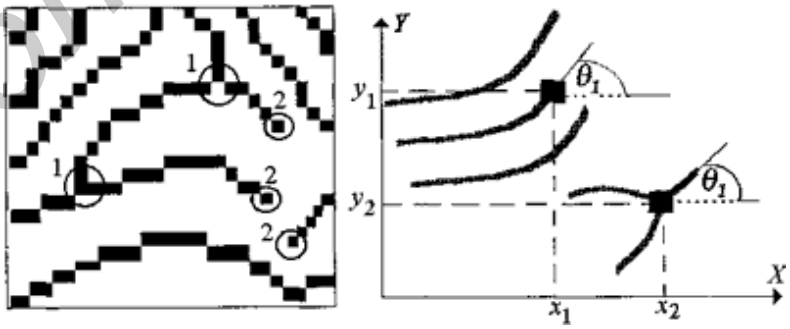


Рис. 2.2. Выделение минуций

Координаты обнаруженных минуций и их углы ориентации записываются в вектор:

$$W(p) = [(x_1, y_1, t_1), (x_2, y_2, t_2)\ldots(x_p, y_p, t_p)],$$

где p – число минуций.

При регистрации пользователей этот вектор считается эталоном и записывается в базу данных. При распознавании вектор определяет текущий отпечаток (что вполне логично).

Этап 6. Сопоставление минуций. Два отпечатка одного пальца будут отличаться друг от друга поворотом, смещением, изменением масштаба и/или площадью соприкосновения в зависимости от того, как пользователь прикладывает палец к сканеру. Поэтому нельзя сказать, принадлежит ли отпечаток человеку или нет на основании простого их сравнения (векторы эталона и текущего отпечатка могут отличаться по длине, содержать несоответствующие минуции и т. д.). Из-за этого процесс сопоставления должен быть реализован для каждой минуции отдельно.

Этапы сравнения:

– регистрация данных;

– поиск пар соответствующих минуций;

– оценка соответствия отпечатков.

При регистрации определяются параметры аффинных преобразований (угол поворота, масштаб и сдвиг), при которых некоторая минуция из одного вектора соответствует некоторой минуции из второго.

При поиске для каждой минуции нужно перебрать до 30 значений поворота (от −15° до +15°), 500 значений сдвига (например, от –250 пкс до +250 пкс) и 10 значений масштаба (от 0,5 до 1,5 с шагом 0,1). Итого до 150000 шагов для каждой из 70 возможных минуций. (На практике все возможные варианты не перебираются – после подбора нужных значений для одной минуции их же пытаются подставить и к другим минуциям, иначе было бы возможно сопоставить практически любые отпечатки друг другу).

Оценка соответствия отпечатков выполняется по формуле

$$K = (D \cdot D \cdot 100\ \%) / (p \cdot q),$$

где D – количество совпавших минуций, p – количество минуций эталона, q – количество минуций идентифицируемого отпечатка.

В случае если результат превышает 65 %, отпечатки считаются идентичными (порог может быть понижен выставлением другого уровня бдительности).

Если выполнялась аутентификация, то на этом все и заканчивается. Для идентификации необходимо повторить этот процесс для всех отпечатков в базе данных. Затем выбирается пользователь, у которого наибольший уровень соответствия (разумеется, его результат должен быть выше порога 65 %).

2.1.1.2 Другие подходы к сравнению отпечатков

Несмотря на то что описанный выше принцип сравнения отпечатков обеспечивает высокий уровень надежности, продолжаются поиски более совершенных и скоростных методов сравнения, как например система AFIS (*Automated fingerprint identification systems* – Система автоматизированной идентификации отпечатков пальцев). В Республике Беларусь – АДИС (автоматическая дактилоскопическая идентификационная система). Принцип работы системы: по бланку «забивается» дактилокарта, личная информация, отпечатки пальцев и ладоней. Расставляются интегральные характеристики (еще приходится редактировать вручную плохие от-

печатки, хорошие система расставляет сама), рисуется «скелет», т. е. система как бы обводит папиллярные линии, что позволяет ей в будущем определять признаки весьма точно. Дактилокарта попадает на сервер, где и будет храниться все время.

«Следотека» и «след». «След» – отпечаток пальца, снятый с места происшествия. «Следотека» – база данных следов. Как и дактилокарты, так и следы отправляются на сервер, и автоматически идет сравнение его с дактокартами, как уже имеющимися, так и нововведенными. След находится в поиске, пока не найдется подходящая дактилокарта.

Метод на основе глобальных признаков. Выполняется обнаружение глобальных признаков (головка петли, дельта). Количество этих признаков и их взаимное расположение позволяет классифицировать тип узора. Окончательное распознавание выполняется на основе локальных признаков (число сравнений получается на несколько порядков ниже для большой базы данных).

Считается, что тип узора может определять характер, темперамент и способности человека, поэтому этот метод можно использовать и в целях, отличных от идентификации/аутентификации.

Метод на основе графов. Исходное изображение (рис. 2.3) отпечатка (*1*) преобразуется в изображение поля ориентации папиллярных линий (*2*). На поле заметны области с одинаковой ориентацией линий, поэтому можно провести границы между этими областями (*3*). Затем определяются центры этих областей и получается граф (*4*). Штриховой стрелкой *г* отмечена запись в базу данных при регистрации пользователя. Определение подобия отпечатков реализовано в квадрате (*5*). Дальнейшие действия аналогичны предыдущему методу – сравнение по локальным признакам.

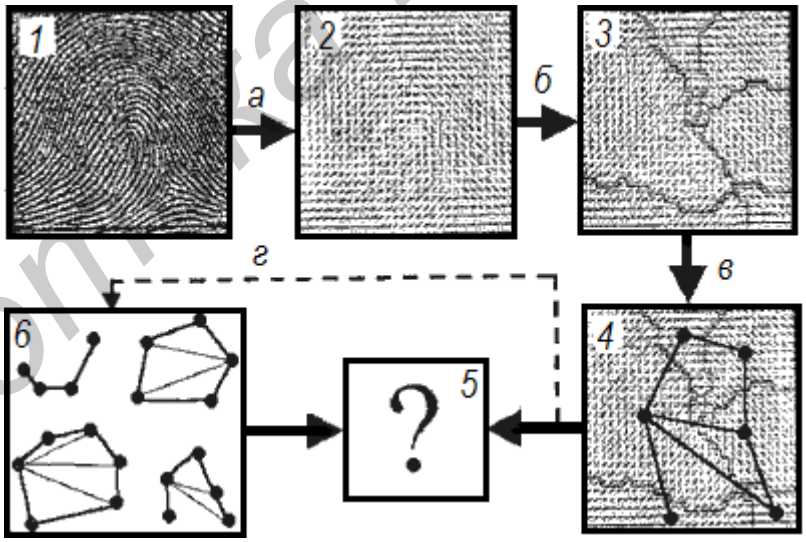


Рис. 2.3. Метод сравнения отпечатков на основе графов

2.1.2. Сканеры отпечатков пальцев

2.1.2.1 Виды и принцип работы

Устройства считывания отпечатков пальцев в настоящее время находят широкое применение. Их устанавливают на ноутбуки, в мыши, клавиатуры, флешки, а также применяют в виде отдельных внешних устройств и терминалов, продающихся в комплекте с системами AFIS.

Несмотря на внешние различия, все сканеры можно разделить на несколько видов:

1. Оптические:

– FTIR-сканеры;

– волоконные;

– оптические протяжные;

– роликовые;

– бесконтактные.

2. Полупроводниковые (полупроводники меняют свойства в местах контакта):

– емкостные;

– чувствительные к давлению;

– термосканеры;

– радиочастотные;

– протяжные термосканеры;

– емкостные протяжные;

– радиочастотные протяжные.

3. Ультразвуковые (ультразвук возвращается через различные промежутки времени, отражаясь от бороздок или линий).

Принцип работы сканера отпечатков пальцев, как и любого другого устройства биометрической верификации, довольно прост и включает четыре базовых этапа:

– запись (сканирование) биометрических характеристик (в данном случае – пальцев);

– выделение деталей папиллярного узора по нескольким точкам;

– преобразование записанных характеристик в соответствующую форму;

– сравнение записанных биометрических характеристик с шаблоном;

– принятие решения о совпадении или несовпадении записанного биометрического образца с шаблоном.

Емкостные сенсоры (рис. 2.4) состоят из массива конденсаторов, каждый из которых представляет собой две соединенные пластины. Емкость конденсатора зависит от приложенного напряжения и от диэлектрической проницаемости среды. Когда к такому массиву конденсаторов подносят палец, то и диэлектрическая проницаемость среды, и емкость каждого конденсатора зависят от конфигурации папиллярного узора в локальной точке. Таким образом, по емкости каждого конденсатора в массиве можно однозначно идентифицировать папиллярный узор.

Принцип действия оптических сенсоров (рис. 2.5) подобен тому, что используется в бытовых сканерах. Такие сенсоры состоят из светодиодов и ПЗС-сенсоров: светодиоды освещают сканируемую поверхность, а свет, отражаясь, фокусируется на ПЗС-сенсоры. Поскольку коэффициент отражения света зависит от строения папиллярного узора в конкретной точке, то оптические сенсоры позволяют записывать образ отпечатка пальца.

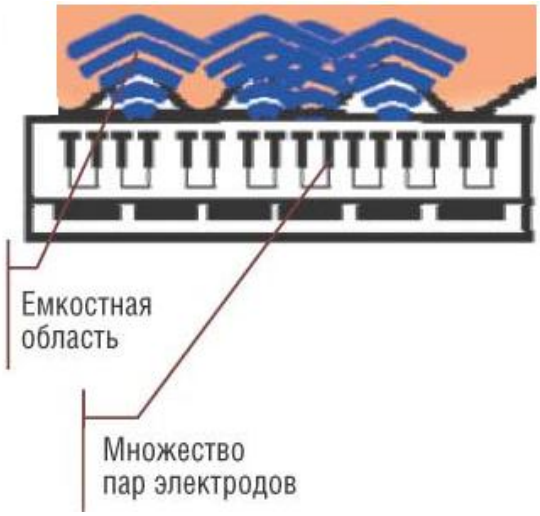


Рис. 2.4. Строение емкостного сенсора

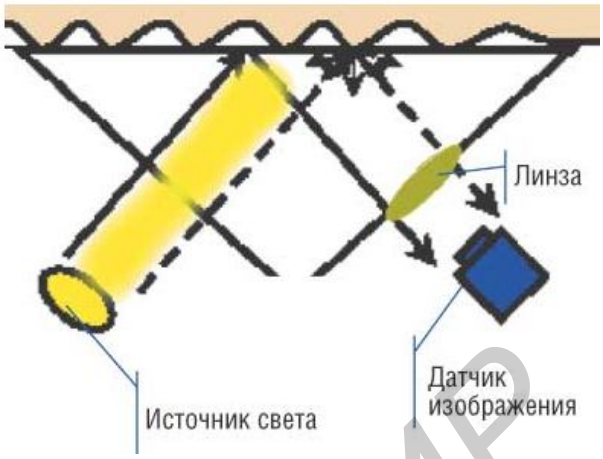


Рис. 2.5. Строение оптического сенсора

Термические сенсоры (рис. 2.6) представляют собой массив пироэлектриков – это разновидность диэлектриков, на поверхности которых при изменении температуры возникают электрические заряды из-за изменения спонтанной поляризации. Температура в межпапиллярных впадинах ниже, чем на поверхности валика папиллярной линии, вследствие чего массив пироэлектриков позволяет в точности воспроизвести папиллярный узор.

В сенсорах электромагнитного поля (рис. 2.7) имеются генераторы переменного электрического поля радиочастоты и массив приемных антенн. Когда к сенсору подносят палец, то силовые линии генерируемого электромагнитного поля в точности повторяют контур папиллярных линий, что позволяет массиву приемных антенн фиксировать структуру отпечатка пальца.

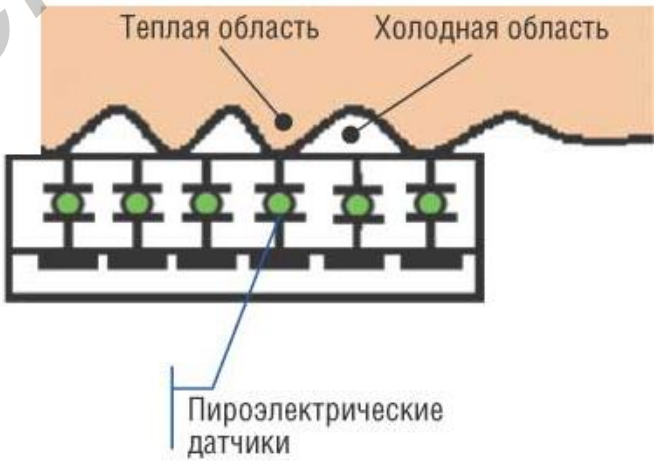


Рис. 2.6. Строение термического сенсора

Рассмотрим более подробно принцип работы протяжных термосканеров – самых популярных в наше время.

В них реализован тепловой метод считывания отпечатков пальцев, основанный на свойстве пироэлектрических материалов преобразовывать разность температур в напряжение. Разность температур создается между ячейками чувствительного элемента под папиллярными гребешками и бороздками. Бороздки не контактируют с чувствительным элементом, поэтому температура чувствительного элемента под бороздками остается равной температуре окружающей среды. Особенностью температурного метода является то, что через некоторое время (около 0,1 с) изображение исчезает, поскольку палец и датчик приходят в температурное равновесие.

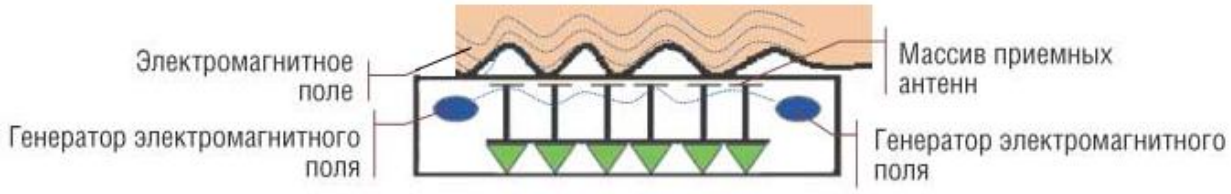


Рис. 2.7. Строение сенсоров электромагнитного поля

Быстрое исчезновение температурной картины является одной из причин применения технологии сканирования. Чтобы получить отпечаток, нужно провести пальцем поперек чувствительного элемента прямоугольной формы (0,4×14 мм или 0,4×11,6 мм). Во время движения пальца скорость сканирования должна превышать 500 кадров/с (задается тактовой частотой). В результате получается последовательность кадров, каждый из которых содержит часть общей картины. Далее отпечаток пальца реконструируют программным способом: в каждом кадре выбирают несколько линий пикселей и ищут идентичные линии в других кадрах, полный образ отпечатка пальца получают совмещением кадров на основе этих линий (рис. 2.8).

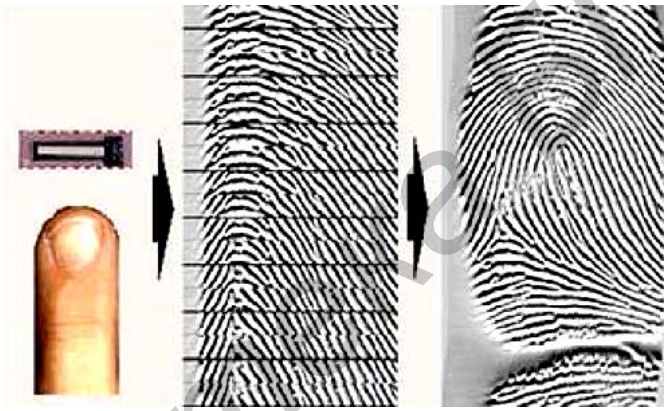


Рис. 2.8. Покадровое считывание картины отпечатка пальца и его реконструкция

Метод покадрового считывания не требует расчета скорости движения пальца по считывателю и позволяет уменьшить площадь кремниевой подложки матрицы более чем в 5 раз, что во столько же раз снижает ее стоимость. Полученное изображение тем не менее имеет высокое разрешение. Дополнительным преимуществом сканирования является то, что окно считывания самоочищается, и после считывания на нем не остается отпечатков пальцев.

Обычно реконструированное изображение имеет размеры 25×14 мм, что соответствует 500×280 точкам. При восьми битах на точку для хранения в формате bmp требуется 140 Кбайт памяти на одно изображение. По соображениям безопасности, а также для уменьшения занимаемого объема памяти в системе распознавания хранят не изображение отпечатка пальца, а эталон, который получают из отпечатка путем выделения характерных деталей.

Алгоритмы идентификации основаны на сравнении предъявляемых образцов с эталонами. При первоначальной регистрации пользователя считывается отпечаток пальца и выделяется эталон, который сохраняется в памяти системы (можно хранить множество эталонов). В дальнейшем при идентификации из считываемых

отпечатков пальцев так же извлекаются наборы деталей, которые в этом случае называются образцами. Образцы сравниваются с множеством хранимых эталонов, и если обнаруживается совпадение, то человек считается идентифицированным. Если образец сравнивается с одним-единственным эталоном, например, чтобы подтвердить личность владельца смарт-карты, такой процесс называется аутентификацией, или проверкой достоверности. Процесс сравнения образца и эталона (идентификация, или аутентификация) выполняется программно и не зависит от технологии, с помощью которой было получено изображение отпечатка.

Программное обеспечение для реконструкции отпечатка пальца поставляется по последовательности кадров (рис. 2.9). Выделение эталона, верификация и идентификация осуществляются с помощью программного обеспечения третьих фирм либо с помощью самостоятельно разработанных программ.

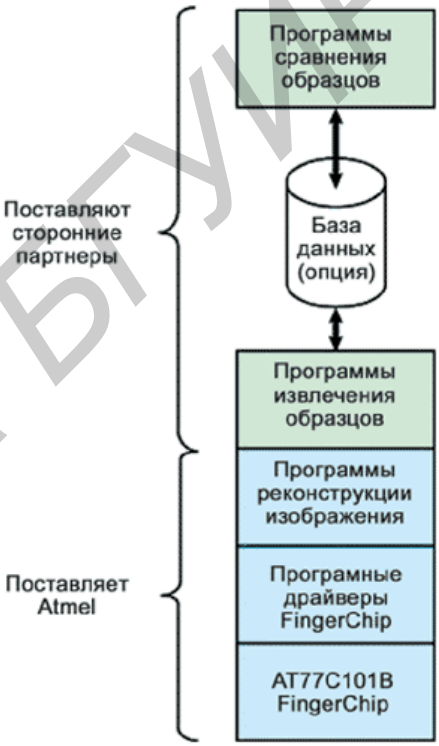


Рис. 2.9. Программное обеспечение *FingerChip*

Тепловая методика считывания обеспечивает высокое качество изображения отпечатка при различном состоянии поверхности пальца: неважно, сухой ли он, истертый, с небольшой разницей уровней между гребешками и бороздками и т. п. Считыватель FingerChip успешно функционирует в жестких условиях, при больших колебаниях температуры, высокой влажности, при различных загрязнениях (в том числе масляных).

В рабочем режиме датчик полностью пассивен. Если разница температур между пальцем и датчиком становится незначительной (менее одного градуса), включается схема температурной стабилизации, которая изменяет температуру считывателя и восстанавливает температурный контраст.

Еще одним достоинством тепловой методики по сравнению с другими методами, особенно емкостными, является отсутствие необходимости плотного контакта между пальцем и считывателем, что позволило использовать специальное покрытие, обеспечивающее защиту от ударов, истирания, влаги и других факторов окружающей среды.

2.1.2.2 Стандарты на отпечатки пальцев

Сейчас в основном используются стандарты ANSI и ФБР США. В них определены следующие требования к образу отпечатка:

– каждый образ представляется в формате несжатого TIF;
– образ должен иметь разрешение не ниже 500 dpi;
– образ должен быть полутоновым с 256 уровнями яркости;
– максимальный угол поворота отпечатка от вертикали не более 15°;
– основные типы минуций – окончание и раздвоение.

Обычно в базе данных хранят более одного образа, что позволяет улучшить качество распознавания. Образы могут отличаться друг от друга сдвигом и поворотом. Масштаб не меняется, так как все отпечатки получают с одного устройства.

2.2. Распознавание по радужной оболочке глаза

2.2.1. Что такое радужная оболочка

Радужная оболочка по форме похожа на круг с отверстием внутри (зрачком). Радужка состоит из мышц, при сокращении и расслаблении которых размеры зрачка меняются. Она входит в сосудистую оболочку глаза (рис. 2.10). Радужка отвечает за цвет глаз (если он голубой – значит, в ней мало пигментных клеток, если карий – много). Выполняет ту же функцию, что диафрагма в фотоаппарате, регулируя светопоток. Радужка входит в состав глаза. Она находится за роговицей и водянистой влагой передней камеры.

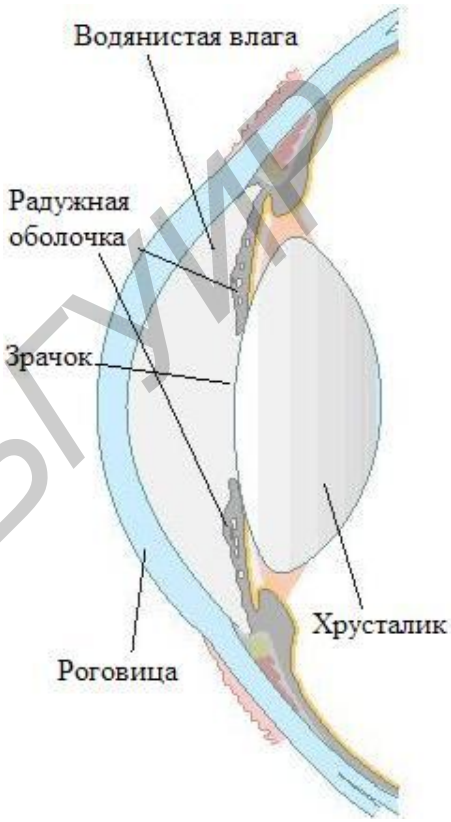


Рис. 2.10. Структура глаза человека

Уникальные структуры радужки обусловлены радиальной трабекулярной сетью (trabecular meshwork); ее состав: углубления (крипты, лакуны), гребенчатые стяжки, борозды, кольца, морщины, веснушки, короны, иногда пятнышки, сосуды и другие черты.

Рисунок радужки в большой степени случаен, а чем больше степень случайности, тем больше вероятность того, что конкретный рисунок будет уникальным. Математически случайность описывается степенью свободы. Исследования показали, что текстура радужки имеет степень свободы равной 250, что гораздо больше степени свободы отпечатков пальцев (35) и изображений лиц (20).

Средние размеры радужной оболочки: по горизонтали – $R \approx 6{,}25$ мм, по вертикали – $R \approx 5{,}9$ мм; размер зрачка составляет $0{,}2 \ldots 0{,}7R$.

Внутренний радиус радужки зависит от возраста, состояния здоровья, освещения и др. Он быстро изменяется. Его форма может достаточно сильно отличаться от круга.

Центр зрачка, как правило, смещен относительно центра радужки по направлению к кончику носа.

2.2.2. Радужная оболочка как биометрический параметр

Во-первых, оболочка имеет очень сложный рисунок, в ней много различных элементов. Поэтому даже не очень качественный ее снимок позволяет точно определить личность человека.

Во-вторых, радужная оболочка является объектом довольно простой формы (почти плоский круг). Так что во время идентификации очень просто учесть все возможные искажения изображения, возникающие из-за различных условий съемки.

В-третьих, радужная оболочка глаза человека не меняется в течение всей его жизни с самого рождения. Точнее, неизменной остается ее форма (исключение составляют травмы и некоторые серьезные заболевания глаз), цвет же со временем может измениться. Это придает идентификации по радужной оболочке глаза дополнительный плюс по сравнению со многими биометрическими технологиями, использующими относительно недолговечные параметры, например геометрию лица или руки.

Радужная оболочка начинает формироваться на 3-й месяц внутриутробного развития. На 8-й месяц она является практически сформированной структурой. Кроме того, она формируется случайно даже у однояйцовых близнецов и гены человека не влияют на ее структуру. Радужная оболочка устойчива после 1-го года жизни – радужка окончательно сформирована и практически не меняется вплоть до самой смерти, если нет травм или патологий глаза.

2.2.3. Радужная оболочка как идентификатор

Свойства радужной оболочки как идентификатора:

– изолированность и защищенность от внешней среды;

– невозможность изменения без нарушения зрения;

– реакция на свет и пульсация зрачка используется для защиты от подделок;

– возможен ненавязчивый, бесконтактный и скрытный метод получения изображений;

– высокая плотность уникальных структур – 3,2 бита/мм^2 или около 250 независимых характеристик (у других методов около 50), 30 % параметров достаточно, чтобы принять решение о совпадении с вероятностью не более 10^{-6}.

2.2.4. Достоинства и недостатки технологии

У идентификации личности по радужной оболочке глаза есть еще одно серьезное преимущество. Дело в том, что некоторые биометрические технологии страдают следующим недостатком. При установке в настройках системы идентификации высокой степени защиты от ошибок первого рода (вероятность ложного допуска – FAR) вероятность появления ошибок второго рода (ложный недопуск в систему – FRR) возрастает до непозволительно высоких величин – нескольких десятков процентов, в то время как идентификация по радужной оболочке глаза полностью лишена этого недостатка. В ней соотношение ошибок первого и второго родов является одним из лучших на сегодняшний день. Для примера можно привести несколько цифр. Исследования показали, что при вероятности возникновения ошибки первого рода в 0,001 % (отличный уровень надежности) вероятность появления ошибок второго рода составляет всего лишь 1 %.

Теоретическая вероятность того, что два разных человека имеют один и тот же рисунок радужной оболочки, приблизительно равна 10^{-78}, в то время как все население Земли составляет менее 10^{10}.

Недостатки технологии. Первым недостатком является относительно высокая стоимость оборудования. И действительно, для проведения исследования нужна как минимум камера, которая будет получать начальное изображение. А стоит это устройство гораздо дороже, чем, например, сенсор отпечатков пальцев. Кроме того, она требует довольно много места для размещения. Все это ограничивает область использования идентификации личности по радужной оболочке глаза. На сегодняшний день она применяется в основном в системах допуска на различные объекты как гражданского, так и военного назначения.

Этапы идентификации по радужной оболочке. *Первым* этапом, естественно, является получение исследуемого изображения (рис. 2.11, 2.12). Делается это с помощью различных камер. Причем стоит отметить, что большинство современных систем предполагает использование для идентификации не одного снимка, а нескольких. Они необходимы для получения более полного изображения радужки, а также могут использоваться при некоторых способах защиты от муляжей.

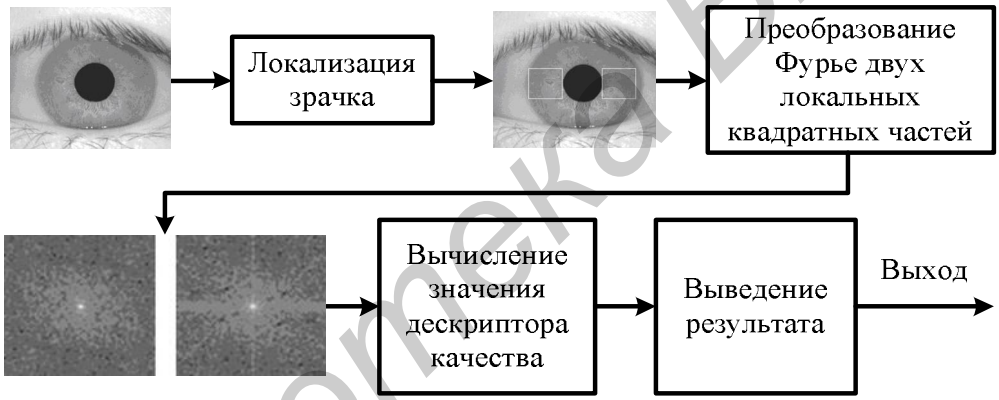


Рис. 2.11. Общий метод оценки качества изображения радужной оболочки

Второй этап – выделение изображения радужной оболочки глаза, что особой сложности не представляет. Как уже говорилось, радужка – это достаточно темная (относительно белка глаза) почти плоская фигура, более или менее похожая на круг. Кроме того, внутри нее должна находиться еще одна окружность, дающая сильные блики (зрачок). Сегодня разработано множество способов точного получения границы радужной оболочки по описанным признакам. Единственной проблемой являются области, закрытые веками. Впрочем, она решается с помощью создания в течение одного сеанса нескольких снимков. Ведь векам присущи непроизвольные движения, дрожание. Таким образом, то, что скрыто на одном снимке, может оказаться видно на другом. Кроме того, на радужной оболочке глаза настолько много разнообразных элементов, что, по некоторым данным, для надежной идентификации достаточно всего лишь 30–40 % из них. Так что многие системы вообще игнорируют закрытые области без заметного ущерба для надежности.

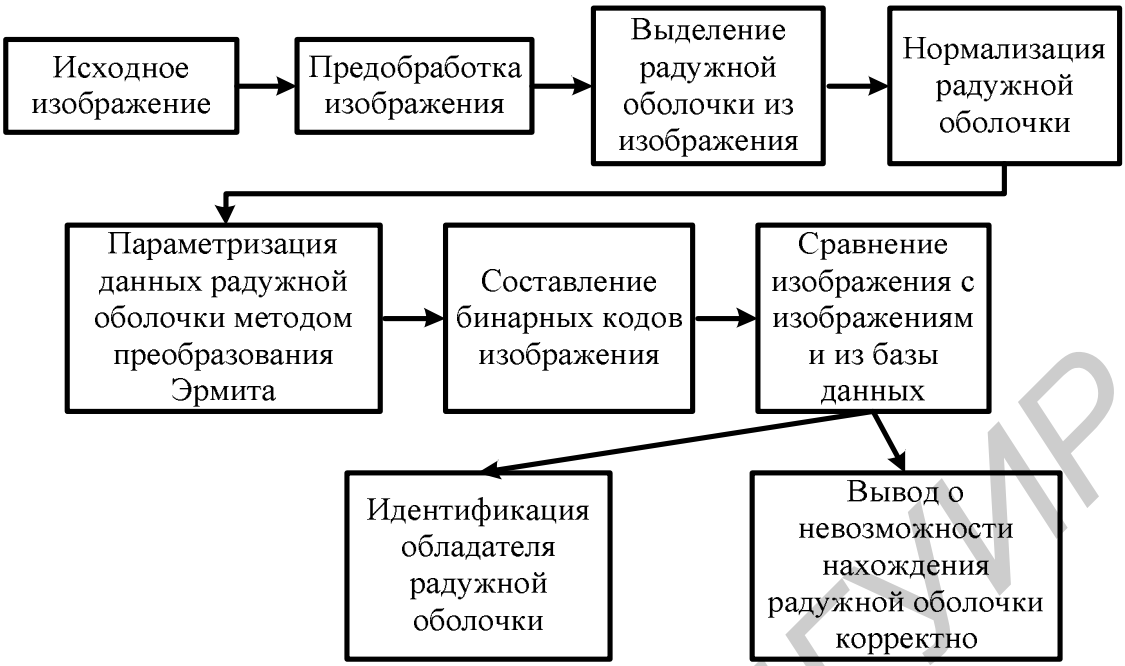


Рис. 2.12. Общая схема идентификации по радужной оболочке глаза

Третий этап идентификации – это приведение размера изображения радужки к эталонному. Это нужно по двум причинам. Во-первых, в зависимости от условий съемки (освещенность, расстояние для объекта) размер изображения может изменяться. Соответственно и элементы радужки тоже будут получаться разными. Впрочем, с этим особых проблем не возникает, так как задача решается путем масштабирования. Вторая причина состоит в том, что под воздействием некоторых факторов может меняться размер самой радужки. При этом расположение ее элементов относительно друг друга становится несколько иным. Для решения этой задачи используются специально разработанные алгоритмы. Они создают модель радужной оболочки глаза и по определенным законам воссоздают возможное перемещение ее элементов.

Четвертым этапом является преобразование полученного изображения радужной оболочки глаза в полярную систему координат. Это существенно облегчает все будущие расчеты. Ведь радужка – это почти круг, а все основные ее элементы располагаются по окружностям и перпендикулярным им прямым отрезкам. Следует отметить, что в некоторых системах идентификации этот этап неявный: он совмещен со следующим.

Пятым этапом в процессе идентификации личности является выборка элементов радужной оболочки глаза, которые могут использоваться в биометрии. Это самый сложный этап. Проблема заключается в том, что на радужной оболочке нет каких-то характерных деталей. А поэтому нельзя использовать ставшими привычными в других биометрических технологиях определения типа какой-то точки, ее размера, расстояния до других элементов и т. д. В данном случае используются сложные математические преобразования, осуществляющиеся на основе имеющегося изображения радужки.

Последним, *шестым* этапом идентификации человека по радужной оболочке глаза является сравнение полученных параметров с эталонами. У этого действия есть одно отличие от многих других подобных задач. Дело в том, что при выделении уникальных характеристик необходимо учитывать закрытые области. Кроме того, часть изображения может быть искажена веками или бликами от зрачка. Таким образом, некоторые параметры могут существенно отличаться от эталонного. Впрочем, эта проблема довольно легко решается благодаря избыточному содержанию на радужной оболочке глаза уникальных для каждого человека элементов – совпадения 40 % из них достаточно для надежной идентификации личности. Остальные же могут считаться «испорченными» и просто-напросто игнорироваться.

2.2.5. Сложности при идентификации по радужной оболочке

Самая большая сложность, с которой пришлось столкнуться разработчикам технологии, – это обеспечение нормальных условий съемки радужной оболочки. Дело в том, что поверхность глаза обычно отражает сторонние источники света, создавая на изображении сильные блики. Естественно, это очень сильно ухудшает точность идентификации. Для того чтобы «перебороть» блики, необходимо использовать собственную подсветку, причем ее яркость должна быть как минимум в несколько раз больше яркости сторонних источников света. В первых системах идентификации для этого использовалась вспышка наподобие тех, которые применяются в фотоаппаратах. Правда, такое решение не нравилось конечным пользователям. Впрочем, современные системы лишены этого недостатка. В них применяется инфракрасная подсветка, не доставляющая пользователям никаких неудобств.

Другой проблемой, связанной со съемками радужной оболочки, является позиционирование глаза. Дело в том, что для получения полного, качественного изображения необходимо, чтобы радужная оболочка находилась на определенном (фокусном) расстоянии от камеры в строго ограниченной зоне. Но ведь в пространстве не прочертишь линии. А как по-другому можно ограничить необходимую зону? Поиском решения этой задачи занималось несколько компаний. В результате появился целый ряд различных разработок. Наибольшее распространение получили четыре из них:

1. Одним из самых простых решений задачи установки глаза пользователя в нужное положение является использование так называемых фиксаторов взгляда. Обычно ими являются небольшие лампочки или направленные светодиоды. Они устанавливаются на сканер таким образом, чтобы свет был виден только при определенном положении глаза (нужном для получения качественного изображения). Таким образом, пользователь сам должен будет найти взглядом фиксатор и ненадолго замереть в этом положении.

2. Другим вариантом является использование прозрачных с одной стороны маленьких зеркал. Для проведения процесса идентификации пользователь должен подойти к сканеру и встать так, чтобы увидеть отражение собственного глаза. С

другой стороны зеркала установлена камера. Таким образом, пользователь сам может установить свой глаз в нужное для идентификации положение.

3. Третий вариант более сложен. В сканер помимо камеры встраиваются несколько дополнительных сенсоров и подсистема распознавания лица. Далее процесс идентификации происходит следующим образом. Сначала пользователь подходит к сканеру. Затем устройство распознает лицо и вычисляет его местоположение. А дальше с помощью голоса или специальных указателей человеку подаются команды о перемещении (влево, вправо, ближе, дальше и т. д.) до тех пор, пока его глаз не попадет в нужную зону. Правда, стоит отметить, что дополнительное оборудование, установленное в сканере, увеличивает его конечную стоимость.

4. Четвертый вариант – самый сложный в реализации. Дело в том, что помимо перечисленного в предыдущем абзаце оборудования сканер оснащается камерой на поворотной подставке. Это очень удобно. Система определяет лицо подошедшего человека и сама наводит камеру и устанавливает ее в оптимальное для съемки положение, т. е. от пользователя для проведения идентификации не требуется предпринимать никаких действий. К сожалению, несмотря на свое исключительное удобство, это решение не получило большого распространения. Дело в том, что сканеры с поворотной камерой сложны в изготовлении, а поэтому стоят достаточно дорого.

Следующей проблемой, с которой столкнулись разработчики систем идентификации личности по радужной оболочке глаза, является возможность применения подделки. Самым простым случаем является предъявление камере фотографии глаза. Кроме того, современные технологии позволяют создавать достаточно точные муляжи этого органа. Для этого необходимы только цифровая фотография лица, зарегистрированного в системе, и некоторое специфическое оборудование. В фантастических фильмах часто показывают, как злоумышленник обманывает систему идентификации, предъявляя ей вырезанный глаз зарегистрированного пользователя. К счастью, на сегодняшний день о таких попытках ничего не известно, тем не менее полностью исключать такую возможность нельзя.

На сегодняшний день разработано несколько различных способов защиты систем идентификации по радужной оболочке глаза от подделок:

1. Регистрация непроизвольных движений глаза и зрачка. Их наличие свидетельствует о том, что сканеру представлен живой человеческий орган. К сожалению, у некоторых людей непроизвольные движения глаза происходят довольно редко. Известны даже случаи, когда они совершались всего один раз в течение несколько минут. Естественно, продлить процедуру идентификации на такое продолжительное время невозможно.

2. Проверка спектра отражения поверхности живого глаза. Дело в том, что значение этого параметра у всегда влажной роговицы значительно отличается от величины той же характеристики мертвого органа или любого искусственного материала (стекло, пластик и т. д.). К сожалению, этот удобный во всех отношениях метод оказался весьма уязвимым. Дело в том, что злоумышленник может обмакнуть свою подделку в жидкость или покрыть ее тонким слоем раствора желатина.

Пока достоверных сообщений о таких атаках не поступало, тем не менее теоретически они представляют серьезную угрозу.

Для борьбы с этой атакой технология отслеживания спектра отражения была доработана. В современных сканерах этот параметр вычисляется не один раз, а несколько. Причем этот процесс происходит в случайно выбранные моменты времени, с разной силой и направлением свечения диодов подсветки. Затем полученные в результате измерений результаты сравниваются с расчетными. Обмануть такую систему уже гораздо сложнее.

3. Так называемая пупилография – технология, используемая в медицине. Суть ее заключается в следующем. Человек смотрит в специальный прибор, который направляет в его глаз короткий световой импульс. При этом зрачок реагирует на излучение, сокращаясь и затем возвращаясь в исходное состояние. График этого процесса называется пупилограммой, по которой врач может определить общее состояние человека (активность, сонливость, наличие серьезного стресса и т. д.).

Именно это и привлекло внимание разработчиков систем идентификации личности по радужной оболочке глаза. Ведь пупилография позволяет помимо защиты от подделок (сокращаться может только живой зрачок) определять состояние человека. А это можно использовать во многих областях. Например, система допуска в кабину пилотов пассажирского лайнера не допустит туда перевозбужденного или сильно раздраженного летчика. То же самое можно реализовать в системах допуска к некоторым важным объектам военного назначения и т. п.

К сожалению, есть у пупилографии и серьезные недостатки. Это несколько неприятные ощущения для пользователя во время подачи светового импульса и относительно длительное время, необходимое на идентификацию (до нескольких секунд на каждого пользователя).

2.3. Распознавание по геометрии руки

В настоящее время в биометрии в целях аутентификации используется только простая геометрия руки – размеры и форма, а также некоторые информационные знаки на тыльной стороне руки (образы на сгибах между фалангами пальцев, узоры расположения кровеносных сосудов).

Вообще с руки можно собрать до 90 информационных знаков, часть из которых не используется в биометрии. Например, уникальный узор на ладони.

Есть два подхода при использовании геометрии руки. Первый (существует с 1976 г.) основан на геометрических характеристиках кисти. Второй (современный) использует кроме геометрических еще и образовые характеристики руки (образы на сгибах между фалангами пальцев и узоры кровеносных сосудов).

Как видно из рис. 2.13, исходными биометрическими признаками руки являются ширина ладони, радиус вписанной в ладонь окружности, длины пальцев, ширина пальцев, высота кисти руки в трех местах (*а*, *б*, *в*).

Также можно использовать и другие признаки, например, углы между контрольными точками, средние значения и дисперсию значений исходных признаков.

Особенность геометрического способа – простота и очень компактный размер вектора значений признаков (размер эталона).

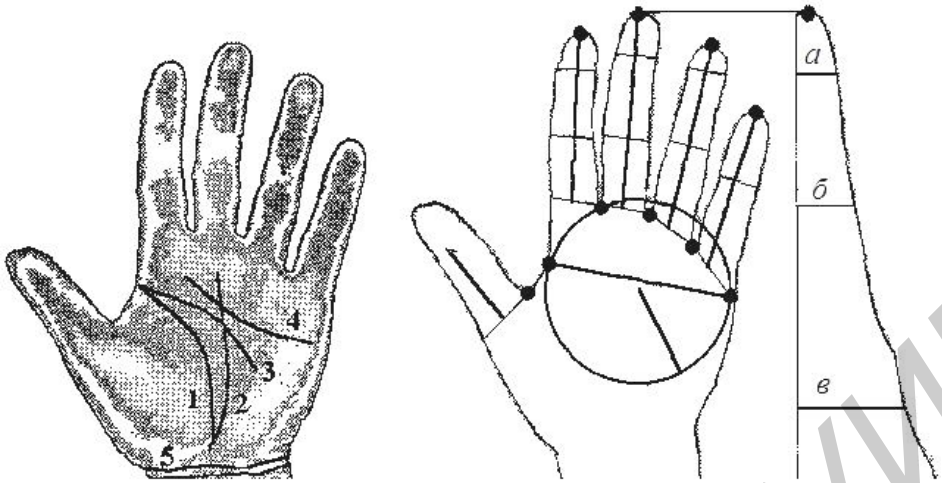


Рис. 2.13. Узор на ладони, состоящий из пяти основных линий (слева), контрольные точки и геометрические признаки руки (справа)

2.3.1. Процесс регистрации и распознавания

1. От пользователя получают несколько силуэтов руки. Для каждого из них вычисляют вектор значений.

2. Все векторы признаков одного человека объединяются в отдельный класс.

3. Признаки эталонного образа являются средними значениями признаков всего класса (т. е. определяется центр класса).

4. Исходные признаки модифицируются – пересчитываются в новые либо редуцируются (сокращается их количество) на основе выборки.

5. Образы-эталоны изменяются соответственно.

6. Новый образ переводится в класс исходных или модифицированных признаков при сравнении с эталоном.

Мерой подобия образов может являться, например, расстояние между новым образом и центрами классов (т. е. вычисляется расстояние от сравниваемого образа до каждого из образов-эталонов различных пользователей). Чем меньше расстояние до какого-либо эталона, тем выше соответствие.

Однако у такого метода есть недостаток – изготовление муляжа не представляет собой больших трудностей.

Во втором подходе с руки снимаются четыре характеристики: три из них – скалярные величины (размеры пальцев), а четвертая – полутоновое изображение складок кожи на сгибе между фалангами (рис. 2.14).

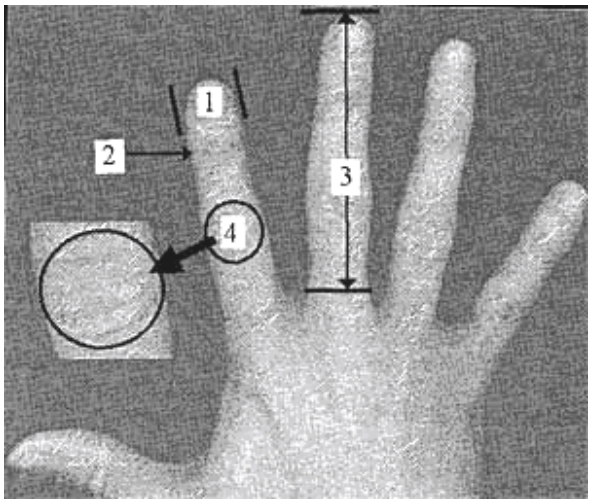


Рис. 2.14. Дополнительные информационные признаки руки

По утверждению компании *Recognition Systems Inc,* занимающейся распознаванием по геометрии руки, вся информация о руке может быть записана девятью байтами.

Использование полутонового изображения сильно затрудняет изготовление муляжа. При этом фирмы, поставляющие такие системы, не раскрывают информации об использующихся характеристиках руки (принцип безопасность через неизвестность).

2.3.2. Достоинства и недостатки геометрического метода

Достоинства:

– «ключ» всегда с пользователем;

– не предъявляются требования к чистоте, влажности, температуре рук;

– пользователь не стесняется «криминалистического» уклона технологии.

Недостатки:

– громоздкость устройств (за некоторым исключением);

– невысокая сложность изготовления муляжа для устройств первого типа (использующих только геометрические характеристики).

2.3.3. Устройства получения информации о руке

В первых двух устройствах (рис. 2.15, *а*, *б*) видно, что для фиксации руки используются специальные штырьки. Других требований нет (к температуре, влажности, чистоте рук). Громоздкость устройств связана с наличием в них видеокамеры, специальной подсветки и уголкового зеркала, отражающего боковой образ руки на объектив камеры. Применяются эти устройства в основном в системах контроля доступа к закрытым помещениями и объектам.

На рис. 2.15, *в* показан процесс идентификации по рисунку кровеносных сосудов (используется инфракрасная подсветка).

Реально эти устройства применялись при контроле доступа в Олимпийскую деревню (г. Атланта, США) на Играх 1996 г. и применяются в международном аэропорту Сан-Франциско, где было установлено более 90 сканеров геометрии руки.

а *б* *в*

Рис. 2.15. Устройства получения информации о руке

Устройство для определения геометрии руки используется следующем образом: сотрудник вкладывает в прорезь закодированное удостоверение или набирает персональный идентификационный номер (ПИН), после чего кладет руку на пластину, расположив пальцы в соответствии с нарисованным на пластине контуром, и ждет, пока не будет закончена проверка. Для того чтобы сотруднику было легче правильно расположить руку, в тот момент, когда рука занимает правильную позицию, на панели устройства зажигаются и гаснут светодиоды. После сканирования руки система принимает решение о соответствии характеристик эталону.

Процесс первоначальной записи эталона геометрии руки сходен с процессом подтверждения с тем лишь исключением, что сканирование осуществляется три раза подряд. Затем полученная информация усредняется и заносится в память как один эталон. Процесс подтверждения индивидуальных характеристик с помощью такого устройства занимает около 4 с, а первоначальная запись эталона геометрии руки – до 1 мин.

2.4. Распознавание лица

Для идентификации личности лучше всего подходят технологии распознавания по лицу. Они ненавязчивы (распознавание человека происходит на расстоянии, без задержек и отвлечения внимания), как правило, пассивны (не требуют каких-либо действий со стороны человека), не ограничивают пользователя в свободе перемещений и относительно недороги. Кроме того, люди обычно легко узнают друг друга по лицам, а значит, и автоматизированные системы не должны испытывать затруднений (на практике все иначе).

По лицу человека можно узнать его историю, симпатии и антипатии, болезни, эмоциональное состояние, чувства и намерения по отношению к окружающим. Все это представляет особый интерес для автоматического распознавания лиц (например, для выявления потенциальных преступников).

2.4.1. Информационные знаки лица

К информационным признакам лица относятся:

– форма лица (круглая, квадратная, треугольная и т. д.);

– соотношение частей лица между собой (лоб, средняя и нижняя части лица);

– форма лба, скул и подбородка;

– форма и размер уха, способ его прикрепления, форма частей уха (мочки, козелок, противокозелок – см. справочник по анатомии);

– симметрия / асимметрия лица;

– форма, величина, (количество) и расположение глаз, рта, носа;

– линии морщин и др.

В зависимости от того, какой портрет используется (в фас, профиль или оба), эти методы комбинируются. В коммерческих системах обычно используют образы лиц в фас (с поворотом в сторону до 15°), а значит, не используют информационные знаки ушей и профиль лица (однако некоторая информация о профиле может быть получена и из изображения в фас – по градиентам яркости).

Глаза и уши также используются в отдельных направлениях биометрии.

2.4.2. Принципы организации базы данных

Качество базы данных определяется на основе следующих признаков:

1) репрезентативность;

2) способ структурирования данных;

3) качество образа:

– размер каждого образа в пикселях;

– контраст и прорисовка деталей лица;

– фон, на котором находится лицо;

– отсутствие помех на лице.

Желательно, чтобы в базе данных были образы с различным поворотом головы, присутствием или отсутствием дополнительных предметов (очки, серьги и т. д.) и с различными выражениями.

Для оценки системы распознавания обычно используется специальная база данных *ORL Database of Faces*. Она отвечает всем этим признакам и доступна многим разработчикам. Эта БД содержит 400 образов по 10 в каждом классе (т. е. всего 40 различных изображений лиц). Каждый образ имеет разрешение 112×92 пикселя и 256 уровней яркости. Все лица представлены на темном фоне. Репрезентативность данных обеспечивается некоторыми изменениями масштаба лица, угла наблюдения и условий освещения.

2.4.3. Методы распознавания

Чаще всего в литературе упоминаются три метода:

1. Корреляционный (метод согласованной фильтрации).

2. Метод на основе преобразований Карунена – Лоэва и понятия «собственных лиц» (*EigenFace*).

3. Метод на основе линейного дискриминантного анализа и понятия *Fisherface* (по имени Роберта Фишера).

Развиваются сейчас методы, ориентированные:

– на репрезентативный характер исходных данных – обучение системы в разных условиях;

– на уменьшение размерности исходных данных;

– на распознавание в сокращенном пространстве признаков.

2.4.3.1 Корреляционный метод

Корреляция – самый простой из вышеперечисленных методов распознавания. Если условия получения новых образов соответствуют условиям получения эталона (освещение, пункт наблюдения лица, наклон, поворот, масштаб, фон и т. д.), то корреляция (соответствие) между ними близка к единице. Уровень распознавания доходит до 96 %. Однако если условия меняются, то линейная корреляция становится бесполезной.

Развитием этого метода является переход от исходных признаков к инвариантам Фурье – Меллина (заменяющих поворот на циклический сдвиг), что позволя-

ет достичь высокой корреляции между образами. Проблемой остается высокая размерность пространства признаков (большой размер эталона). Кроме того, преобразование Фурье – Меллина существенно усложняет вычислительный процесс.

2.4.3.2 Метод на основе преобразований Карунена – Лоэва (ПКЛ)

Этот метод (рис. 2.16) позволяет значительно сократить размер эталона, оставляя только те признаки, которые имеют принципиальное значение для конкретного образа. При этом влияние условий получения образа не так заметно, а сравнение образов упрощается. Уровень правильного распознавания стабильно достигает 80 % даже при значительных изменениях условий.

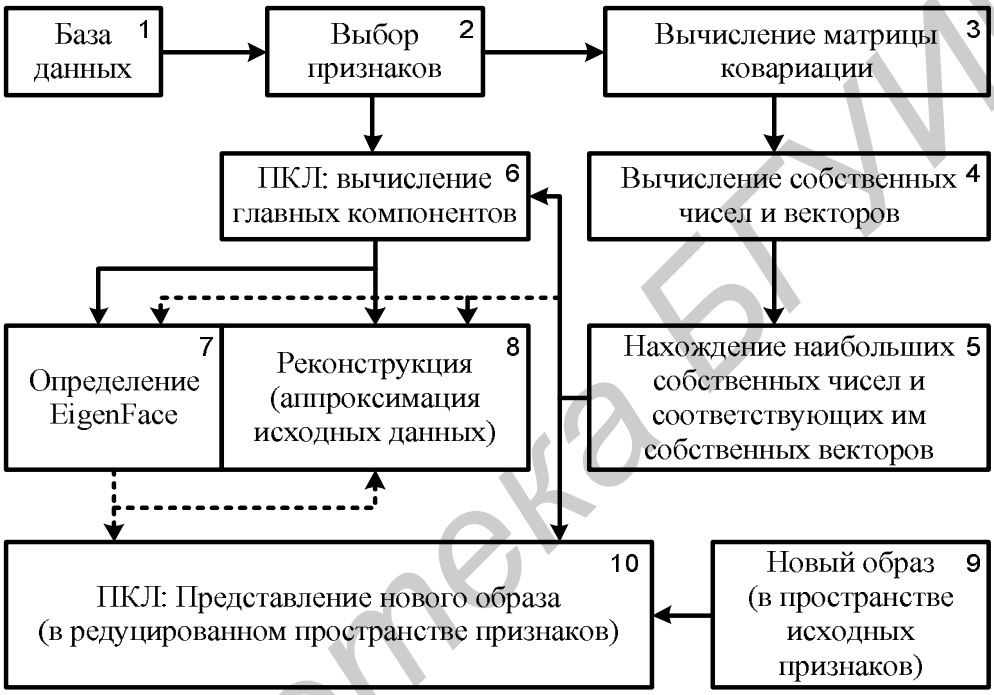


Рис. 2.16. Метод на основе преобразований Карунена – Лоэва

Цель анализа главных компонентов – выявить основные изменчивости в изображениях лиц (использующихся при обучении системы) и описать эти изменчивости несколькими векторами (см. рис. 2.16 шаги 3–5). Основные изменчивости представляются в матрице ковариации, порядок которой соответствует размерности вектора исходных признаков. Основная изменчивость матрицы описывается собственными числами, число которых не больше размерности матрицы. Таким образом, ПКЛ позволяет преобразовать N-мерное пространство признаков в p-мерное ($p \le N$).

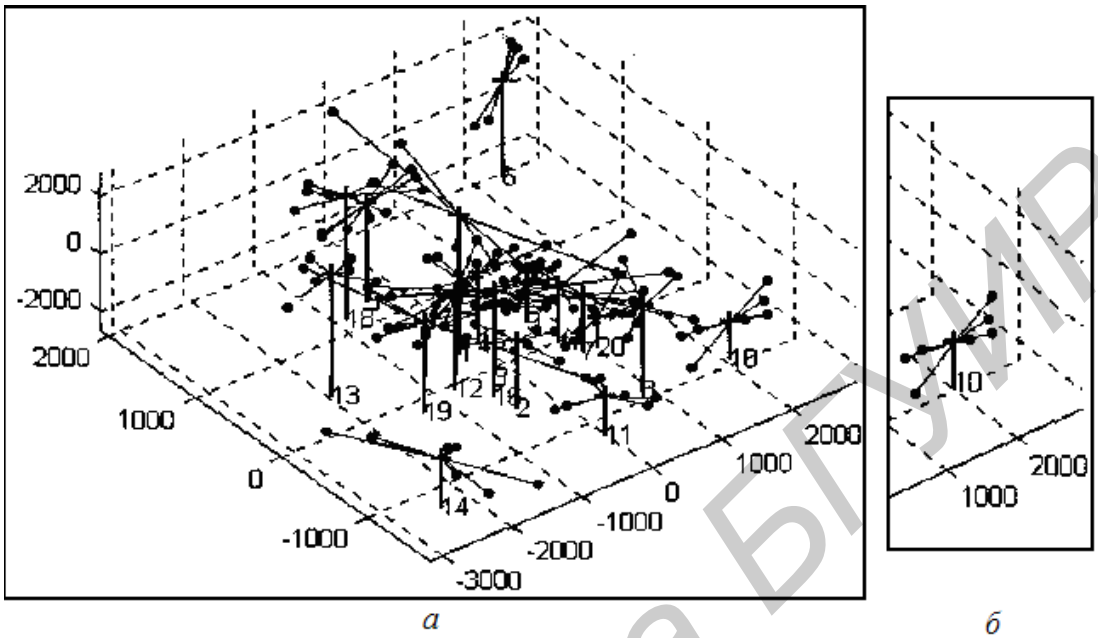
Обратное преобразование Карунена – Лоэва приводит к представлению образов в виде «эластичных моделей лиц».

В редуцированном пространстве признаков значительно проще отделить один образ от другого. Однако кластеризация здесь не всегда возможна. Может получиться редуцированное пространство образов (рис. 2.17, *а*).

На рис. 2.17, *б* выделен образ 10-го класса (класс – массив образов лица одного человека). Вертикальной линией представляется средний образ в классе (центр

класса), а отдельные образы – семь точек. Линиями показан разброс образов относительно центра.

Как можно видеть, различение образов в таком виде не является простой задачей: расстояния между классами не максимизированы, а расстояния внутри класса не минимизированы. Некоторые образы перекрывают чужие классы.



а *б*

Рис. 2.17. Отображение редуцированного пространства признаков в форме 3D:
а – редукция для первых 20 классов образов базы; *б* – образ 10-го класса.
Редукция выполнена для 20 классов образов базы и первых семи образов в классе

2.4.3.3 Метод на основе линейного дискриминантного анализа (ЛДА)

Данный метод, как и предыдущий, позволяет сократить количество признаков, при этом существенно улучшает кластеризацию образов (отделение друг от друга). Это позволяет увеличить уровень распознавания до 99 % даже в сильно отличающихся условиях.

Если взять результат после преобразований Карунена – Лоэва в качестве исходных данных и применить метод ЛДА, можно дополнительно сократить пространство признаков.

В результате преобразований получается пространство признаков, в котором отдельные образы в классе становятся ближе к центру и практически не перекрывают чужую территорию, а сами центры отдалены друг от друга еще больше (рис. 2.18).

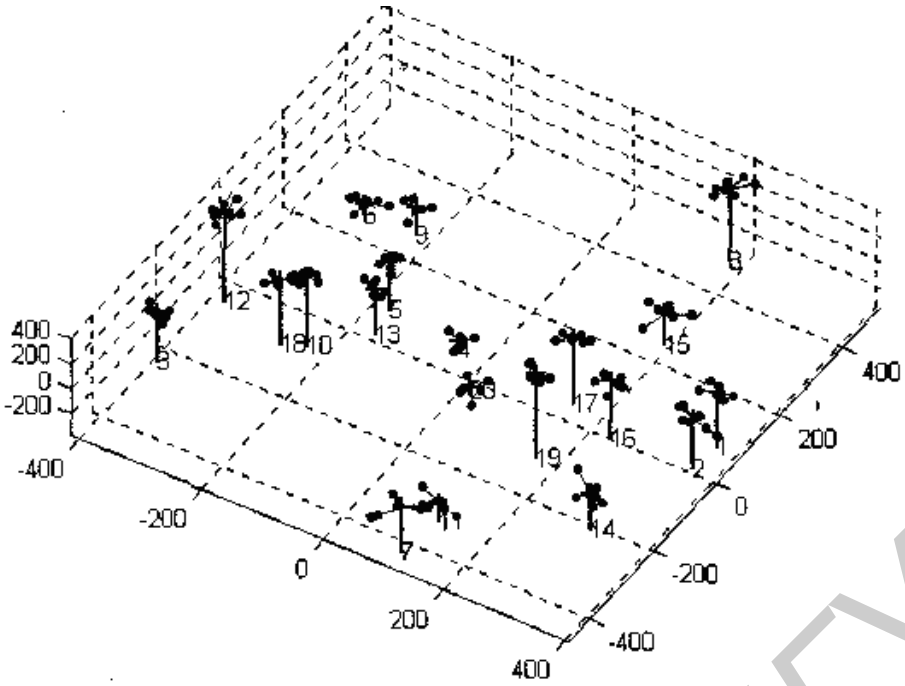


Рис. 2.18. Отображение пространства признаков в форме 3D, полученное методом линейного дискриминантного анализа

2.4.4. Отбор признаков

Выбор и выделение признаков играют в распознавании образов ключевую роль.

2.4.4.1 Категории признаков

Есть три категории признаков: физические, структурные и математические.

Физические и структурные признаки выражаются через формы лица (овал лица, геометрия его основных частей), его цвет, а также цвет волос и т. д. Наиболее часто используемый признак – яркость. К физическим и структурным признакам можно отнести также координаты точек лица в местах, соответствующих смене контраста (брови, глаза, нос, уши, рот и овал).

К математическим признакам относятся спектры исходных образов, статистические характеристики, градиенты изменения яркости и др., полученные в результате математического преобразования исходных признаков.

2.4.4.2 Способы выделения признаков

Способы выделения признаков различаются в зависимости от используемого способа представления и способа его редукции (сокращения).

Первый способ. Яркостные признаки собираются в вектор простым перечислением значений яркости каждого пикселя. Для образа 112×92 пикселя получается матрица порядка 10304. В таком пространстве поиск практически невозможен, поэтому изображение предварительно уменьшается до приемлемых размеров.

Второй способ. Исходный образ рассматривается как набор столбцов и строк, являющихся самостоятельными векторами признаков. Процедура преобразования применяется отдельно для строк и отдельно для столбцов. В результате получается

матрица, имеющая значительно меньший порядок. Кроме того, это повышает и точность распознавания (до 85 %), увеличивает стойкость к изменению яркости, циклическому сдвигу и шумам.

Для еще большей редукции признаков можно применить далее линейный дискриминантный анализ. В результате распознавание доходит до 100 % в больших базах данных.

Среди математических признаков чаще всего используются спектральные признаки, полученные в результате преобразования Фурье. Размер исходного пространства признаков может составить до 200 элементов. При этом для более высокого уровня распознавания преобразования Фурье применяются не для усредненного образа, а для каждого в отдельности.

Также используется сканирование образа поочередно каждой из 25 масок 3×3, 5×5 и т. д. пикселей и составление 25-компонентного вектора признаков. Кластеризация выполняется методом ЛДА (рис. 2.19).

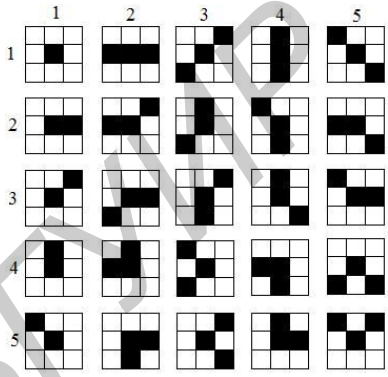


Рис. 2.19. Маски для отбора признаков

Однако для этого способа должны выполняться некоторые требования: от 50 до 100 образов на класс и не менее 100 классов (другими словами, при регистрации каждого из минимум 100 изображений лиц, нужно сделать до 100 снимков, на что уйдет довольно много времени), образы должны быть определенного масштаба, должен быть черный фон, а на людях должна быть одинаковая одежда. Таким образом, эту систему можно применять только в учреждениях, где принята официальная форма одежды.

2.4.5. Анализ локальных признаков

На образе выделяются координаты лица и локальных признаков (например, уголки рта, нос, глаза и т. д.) Координаты признаков и расстояния между ними позволяют описать лицо с помощью точек и параметров, которые затем будут использоваться при распознавании.

2.4.6. Эластичные модели форм лица

Образы из базы данных (рис. 2.20) представляются в виде набора точек, описывающих нижние 2/3 лица (без лба). Точки ставятся в местах смены контраста (яркости).

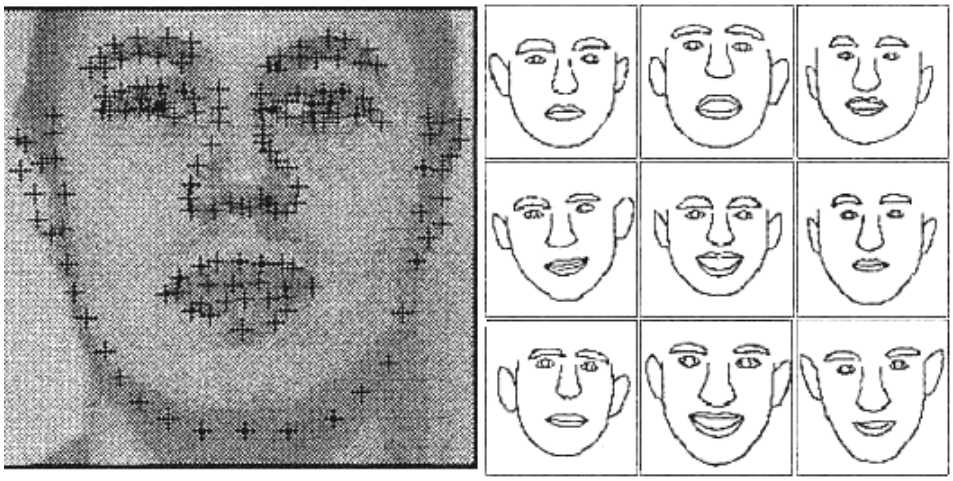


Рис. 2.20. Модели формы лица

Эти модели формы лица используются при регистрации, идентификации, распознавании род/пол, распознавании выражения лица, для виртуальной реконструкции.

После редукции признаков вычисляется усредненная форма лица («эластичная» – известно, в каких пределах она может изменяться). Дополнительными средствами при распознавании являются градиенты яркости.

По эластичной модели можно определить наличие усов, бороды, очков. Утверждается, что уровень распознавания лежит в пределах 86–97 %, определение положения лица – 77–100 %, выражения лица – с точностью до 83 %.

Эластичные модели формы лица можно представить, например, по программе *Poser*, различным программам составления фотороботов, либо на основе рис. 2.21.

Рис. 2.21. Эластичные модели формы лица

2.4.7. Коммерческие системы

Система *Faceit* компании *Visionic*. Распознавание по алгоритмам анализа локальных признаков (главные из них – координаты центров глаз). Данная система применяется для идентификации преступников по видеоданным, получаемым со 144 камер из центра Лондона. Возможно, конечно, и другое применение.

Система *Photobook* компании *Visage*. Используются методы, основанные на «собственных лицах» и реконструкции образов на их основе. Система ориентирована на поиск образов лиц в больших базах данных, для упорядочения БД и для аутентификации человека на основе образа лица, полученного с камеры, либо на основе фотографии с документа.

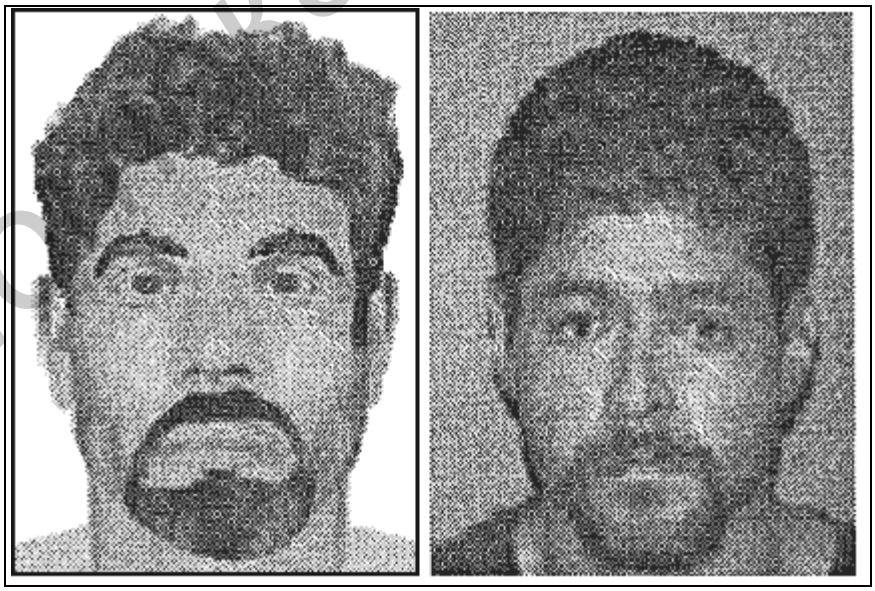
Система *TrueFace* компании *Miros*. Распознавание на основе нейронных сетей. Выделяются неизменяемые части лица.

Система *BioID* компании *DCS AG*. Используются три характеристики человека: изображение лица, голос и движение губ.

2.4.8. Применение систем

Рассмотрим следующую ситуацию.

Для розыска преступника был составлен его фоторобот с помощью системы распознавания лиц *FaceID* компании *ImageWare*, благодаря которой человек был найден быстро.



Слева представлен фоторобот, справа – человек. Нельзя сказать, тот ли это человек, но то, что система позволяет значительно ускорить поиск нужных людей, очевидно.

Системы идентификации по лицу часто используются в аэропортах при прохождении паспортного контроля. Также камеры расставляют в людных местах для поиска преступников.

Эти системы используются в казино для выявления мошенников и на фейс-контроле для недопуска лиц из «черного списка».

2.4.9. Достоинства и недостатки метода

Достоинства метода:

– низкая цена устройств получения видеообраза;

– неназойливость системы;

– бесконтактность;

– незаметность.

Недостатки:

– сложность реализации системы;

– высокая цена устройств получения термографического образа;

– зависимость видеообраза от помех.

2.5. Распознавание человека по голосу

Голос – это поведенческий биометрический параметр, зависящий от физических характеристик. Свойства голоса (такие, как частота, носовой звук, модуляция, интонация и т. д.) являются уникальными особенностями человека.

Идентификация человека по голосу – один из традиционных способов распознавания, применяемый повсеместно. Можно легко узнать собеседника по телефону, не видя его. Также можно определить психологическое состояние по эмоциональной окраске голоса.

Достоинства технологии:

– возможность распознавания на расстоянии (без задержек и отвлечения внимания);

– пассивность; технологии, как правило, пассивны (не требуют каких-либо действий со стороны человека),

– отсутствуют ограничения пользователя в свободе перемещений.

Идентификация по голосу основана на анализе уникальных характеристик речи, обусловленных анатомическими особенностями (размер и форма горла и рта, строение голосовых связок) и приобретенными привычками (громкость, манера, скорость речи).

Голос подвержен существенным изменениям под воздействием эмоциональных факторов (настроение человека) и состояния здоровья (ангина, насморк, бронхит и т. д.). На качестве идентификации могут сказываться внешние условия (например, посторонние шумы от дорожного движения, разговоров других людей). Если для передачи голосовой информации используются линии связи, помехи в них также способны затруднить распознавание пользователя.

Голосовые аутентификационные системы разделяются на категории в зависимости от требований к распознаванию речи:

– *заданный текст* (определенные слова или фразы записываются при регистрации. Слова могут быть секретными, тогда они действуют как пароль);

– *независимость от текста* (системы обрабатывают любую фразу говорящего. Наблюдение может быть продолжительным, и чем больше говорит человек, тем точнее система идентифицирует пользователя. Такие системы могут аутентифицировать пользователя, даже в том случае, если он говорит на другом языке);

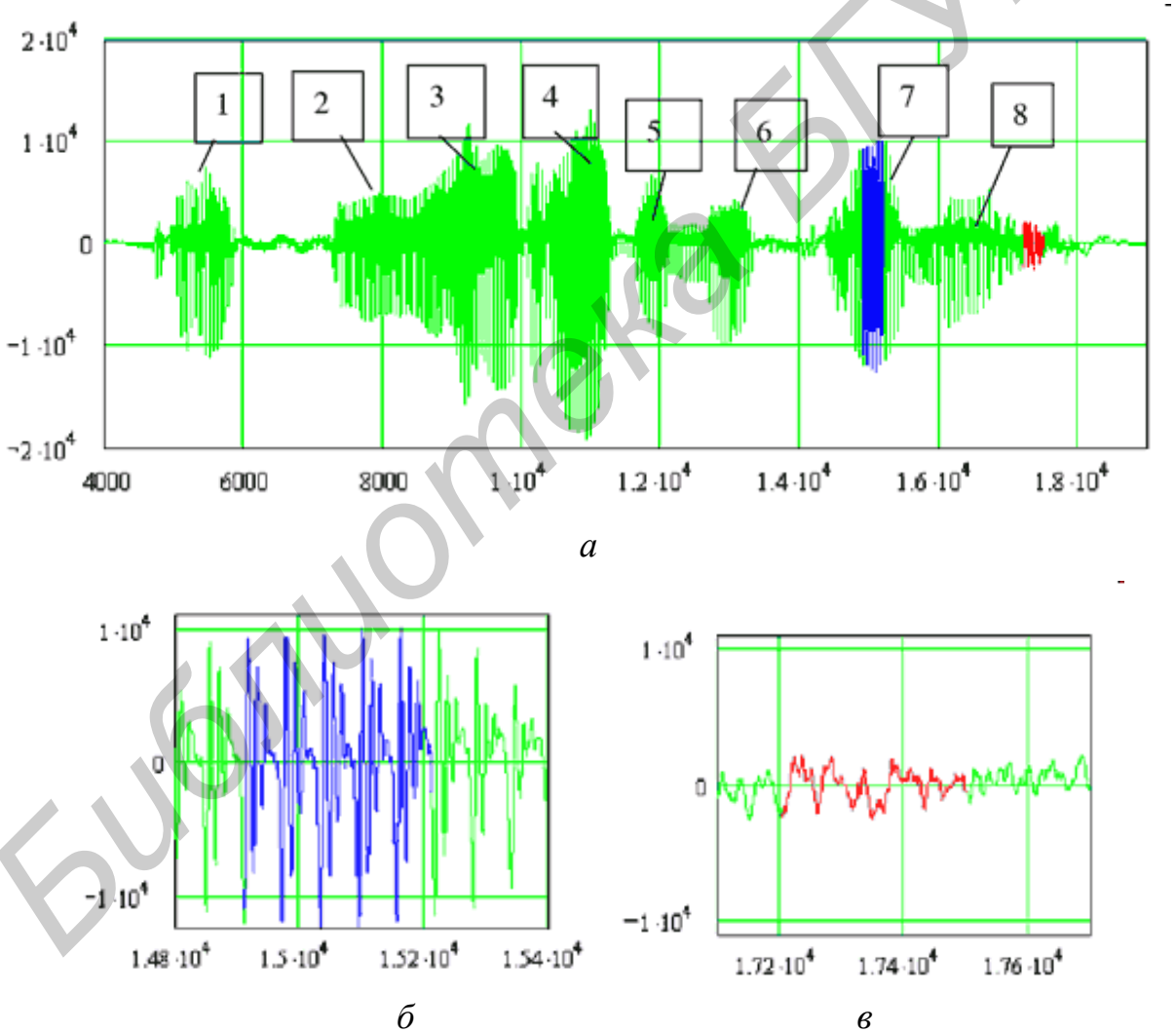
– *диалог* (при этом требуется произнести секретные слова или по крайней мере предоставить информацию, которую нельзя угадать и узнать).

Одна из причин привлекательности технологий распознавания говорящего – это распространенность и низкая стоимость сенсора, необходимого для регистрации речевого сигнала. Микрофоны сейчас присутствуют практически в каждом

устройстве: стационарных и сотовых телефонах, ноутбуках и настольных компьютерах. Все они могут быть использованы в качестве сенсоров.

Рассмотрим структуру речевого сигнала. Каждый всплеск голосового сигнала соответствует некоторому фрагменту речи. Это может быть одна буква, сочетание букв (фонема) или короткое широко распространенное слово. Всего в русской речи есть 42 фонемы, но подходят для идентификации человека не все. Часть фонем огласована. Именно им присущ индивидуальный характер. Это звуки «э», «о», «л», «а», «и» и др. Другая часть фонем – шипящие (шумоподобные). Это «ц», «ч», «ш», «щ» и т. д. Они не являются индивидуальными и их использование при идентификации может привести к снижению качества распознавания.

На рис. 2.22, *а* приведен пример голосовой фразы и выделения из нее восьми фрагментов. Фрагмент фразы, содержащий огласованную фонему, представлен на рис. 2.22, *б*, а фрагмент с шумоподобной фонемой – на рис. 2.22, *в*.



а

б *в*

Рис. 2.22. Пример голосовой фразы и выделения из нее фрагментов

Огласованные фрагменты речи имеют явно выраженный периодический характер. Период и характер колебаний индивидуальны. На рис. 2.23 представлены колебания одной фонемы для двух людей. Как видно из рисунка, для одного и того

же человека графики очень похожи. У другого человека и период тона, и форма внутренних колебаний значительно отличаются от первого.

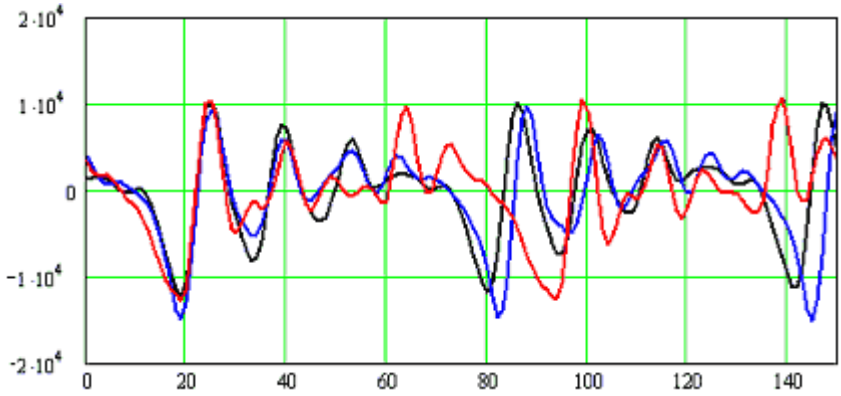


Рис. 2.23. Огласованные фонемы

На сегодняшний день существует два подхода к идентификации человека по голосу, построенные с учетом структуры речевого сигнала.

Индивидуальные различия распределения мощности сигнала по спектру положены в основу первой категории систем биометрической идентификации по голосу. Они строятся на базе набора узкополосных фильтров, выделяющих из голоса колебания разных частот (рис. 2.24).

Полосы пропускания фильтров выбираются при проектировании системы, но они не должны быть слишком узкими, чтобы не зависеть от вариаций частотного спектра голоса. В то же время они не должны быть и очень широкими. Нужно подбирать оптимальную ширину, достаточную для уверенной идентификации. Обычно используют 16 фильтров, полоса пропускания которых расширяется по мере роста значений выделяемых частот. Это связано с нестабильностью высоких частот по энергии (в сравнении с низкими частотами). Итоговый массив данных выходит очень маленького размера (нужно записать только 16 координат вершин по одной оси).

Вторая категория систем основывается на формировании сигнала, имитирующего голосовую фразу с использованием аппарата линейного предсказания.

Огласованные колебания звука имитируются периодическими воздействиями на цифровой фильтр. Период воздействий должен точно соответствовать периоду основного тона голоса. Динамические характеристики цифрового фильтра должны меняться, чтобы получить форму, близкую к голосовой фразе. Число коэффициентов фильтра колеблется от 10 до 12 (a_1, ..., a_{12}). Этого достаточно для качественного воспроизведения речи с сохранением индивидуальных особенностей. Коэффициенты линейного предсказателя вычисляются на выборке из 180–220 отсчетов. Вычисление параметров предсказателя (цифрового фильтра) находят решением системы из 10–12 линейных уравнений.

При имитации огласованных звуков на вход цифрового фильтра подают периодическую последовательность импульсов, промодулированную по амплитуде. В таком случае на выходе фильтра появляются периодические переходные процессы, повторяющие моделируемый звук. При моделировании шипящих на вход фильтра подают случайный шум нужной амплитуды.

При обучении системы на ее вход подают несколько образцов голоса пользователя. Они преобразуются в последовательность импульсов основного тона и соответствующую последовательность коэффициентов линейного предсказателя. Получается массив данных, описывающий индивидуальные особенности голоса человека для данной фразы. Этот массив из коэффициентов и является тем биометрическим эталоном, который записывается в базу данных.

В режиме верификации произнесенная ключевая фраза сравнивается с эталонной с помощью методов вычисления расстояний. Если алгебраическая сумма расстояний не превышает установленного порога идентификации, принимается решение о положительном определении данного голоса. Для систем, которые проводят анализ индивидуального произношения отдельных звуков, решение принимается путем расчета взаимно корреляционной функции параметров эталонных и контрольных фонем по максимуму главного лепестка.

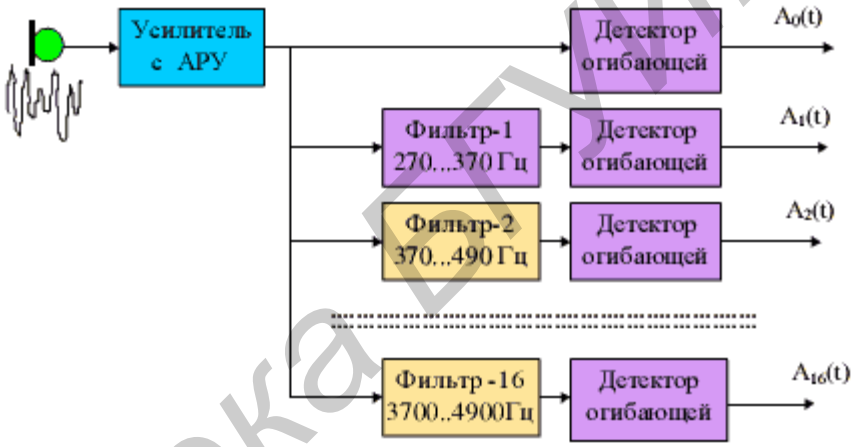


Рис. 2.24. Система идентификации человека по голосу на основе различий в спектре голоса

Большинство разработанных на сегодняшний день систем идентификации личности по голосу построены на основе однократной проверки соответствия требуемой ключевой фразы и произнесенной в первоначальный момент доступа к вычислительной системе.

Данные системы поддерживают два основных режима работы:

1) обучение системы;

2) проверка подлинности при доступе.

В первом режиме (регистрация) пользователю предлагается несколько раз произнести ключевую фразу (пароль), ограниченную, как правило, по длительности (3–4 с). При этом обучение системы идентификации проводится на усредненных речевых отрезках по результатам записи нескольких произношений. Записанный ключ может храниться в полном объеме или сжиматься эффективными алгоритмами, которые позволяют сохранять индивидуальные параметры голоса без искажений. Некоторые системы удаляют из записанной ключевой фразы слабовыраженные речевые участки (паузы, шумы, всплески энергии) путем ее деления на отрез-

ки, соответствующие фонемам базового языка, из которых затем выделяется совокупность требуемых параметров.

Существующие системы распознавания человека по голосу имеют следующие характеристики: ошибки первого рода (недопуск своего) составляют 1–5 % (хотя в зависимости от реализации программного обеспечения могут доходить до 40 %). Количество ошибок второго рода (пропуск чужого) зависит от того, знает ли злоумышленник ключевую фразу (до 1 %, если голоса близки) или нет (0,00000001 %). Сейчас можно использовать голосовую идентифиацию совместно с другими видами защиты. Например, по геометрии лица. Тогда можно отслеживать движение губ и синхронизацию их со звуком.

Голосовую защиту легко пройти, если перехвачена или записана ключевая фраза. Поэтому разработчики сейчас пытаются создать систему, защищенную от перехвата, т. е. опознающую человека по любой фразе.

Один из эффективных путей защиты от перехвата парольной фразы основан на использовании речевой информации, вводимой с ларингофона, контактирующего с телом говорящего. Ларингофон существенно меняет индивидуальную окраску звука в зависимости от места контакта с телом. Отсутствие сведений о зоне съема сигнала (рис. 2.25) усложняет преодоление биометрической идентификации, так как сигнал зависит от местоположения ларингофона. Его нельзя описать современными техническими средствами из-за индивидуального строения и взаимодействия мышц, костей и хрящей конкретного человека. При произношении речевой сигнал колебаниями распространяется внутри тела. Получается сложная система звукопроводов разного типа. В итоге в каждую из зон контакта звук приходит разными путями.

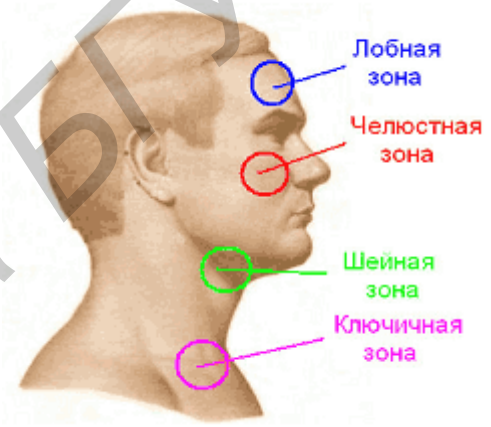
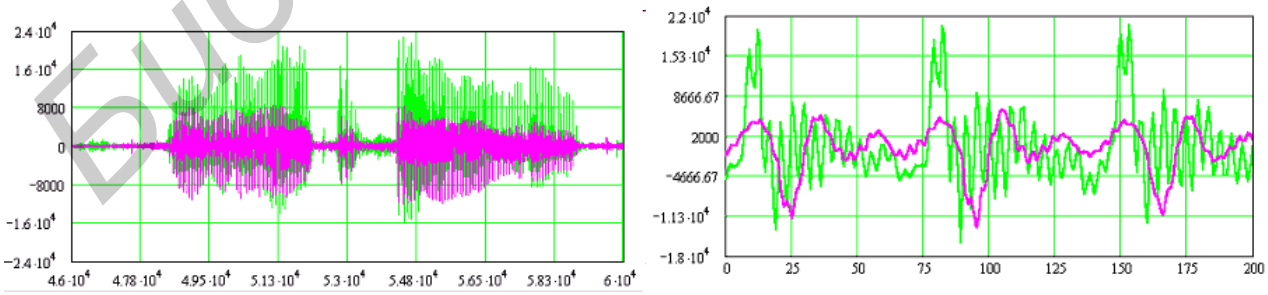


Рис. 2.25. Зоны съема сигнала при помощи ларингофона

На рис. 2.26 показан один и тот же сигнал, снятый с шейной (рис. 2.26, *а*) и ключичной зоны (рис. 2.26, *б*). Видно, что период основного тона повторяется очень точно, но форма колебаний совершенно другая.



а *б*

Рис. 2.26. Речевой сигнал, полученный при помощи ларингофона из различных зон тела человека

2.5.1. Достоинства и недостатки метода распознавания по голосу

Достоинства распознавания по голосу:

– привычный для человека способ идентификации;

– низкая стоимость (самая низкая среди всех биометрических методов);

– бесконтактность.

Недостатки:

– высокий уровень ошибок 1 и 2 рода;

– необходимость в специальном шумоизолированном помещении для прохождения идентификации;

– возможность перехвата фразы «магнитофоном»;

– качество распознавания зависит от многих факторов (интонация, скорость произнесения, психологическое состояние, болезни горла);

– необходимость подбора специальных фраз (с огласованными фонемами).

2.6. Верификация подписи

Верификация подписи – метод, который имеет длинную историю развития. Подпись использовалась еще до появления компьютеров и широко применялась при аутентификации документов и при проведении транзакций с использованием чеков и кредитных карт. Распознавание подписи – это пример распознавания писавшего, которое принималось как неопровержимое доказательство в суде. Подписи могут иметь разную форму, давая возможность подписывающемуся определять «отличительные признаки» и «уникальность» своей подписи, которые будут влиять на КЛД и КЛОД.

Для биометрических параметров необходимыми условиями являются:

– универсальность;

– уникальность;

– постоянство, т. е. неизменность во времени;

– собираемость.

Вопрос о постоянстве подписи довольно спорный, потому что человек может изменить свою подпись в любое время. До известной степени движения мышц руки определяются генетикой и влиянием среды и преобразуются в визуальные и считываемые машиной знаки. Биометрический параметр (как лицо и голос) подвергается влиянию болезней, эмоций или возраста, поэтому данные факторы находятся в процессе изучения. Также не очень ясно, связаны ли параметры, подсчитываемые в процессе верификации подписи, с индивидуальными физическими характеристиками пишущего (которые нельзя подделать).

Как оказалось, подпись – такой же уникальный атрибут человека, как и его физиологические характеристики. Кроме того, это и более привычный для любого человека метод идентификации, поскольку он в отличие от снятия отпечатков пальцев не ассоциируется с криминальной сферой. Одна из перспективных технологий аутентификации основана на уникальности биометрических характеристик движения человеческой руки во время письма.

Технологии автоматизированной верификации подписи можно разделить по способам получения образцов:

1) оффлайновые, или «статистические» подписи сканируются с документов и бумаг. Оффлайновый анализ подписи может быть проведен с отсканированного изображения при помощи камеры или сканера;

2) онлайновые, или «динамические» подписи получаются при помощи специальных устройств; динамические характеристики (положение кончика ручки в процессе письма) можно считывать с высоким разрешением, даже когда ручка не касается бумаги.

Первый способ весьма ненадежен, так как основан на обычном сравнении введенной подписи с хранящимися в базе данных графическими образцами. Из-за того, что подпись не может быть всегда одинаковой, этот метод дает большой процент ошибок. Способ динамической верификации требует намного более сложных вычислений и позволяет в реальном времени фиксировать параметры процесса подписи, такие как скорость движения руки на разных участках, сила давления и длительность различных этапов подписи. Это дает гарантии того, что подпись не сможет подделать даже опытный графолог, поскольку никто не в состоянии в точности скопировать поведение руки владельца подписи. Только настоящий пользователь сможет повторить все эти характеристики за то же время. Копировальная машина или специалист могут с легкостью сделать дубликат вашей подписи и воссоздать ее, но дублировать время и все характеристики подписи практически невозможно.

Отработанная со временем манера личной подписи человека является необходимой характеристикой для воссоздания всех необходимых параметров, которые затем и рассматривает система. Каждый раз, подписывая документы, в подписи могут быть какие-то небольшие вариации, но характеристики, определяемые естественными движениями и особенностями, выработанными в течение долгого времени, создают узнаваемые признаки, которые и делают подпись объектом биометрической идентификации.

Пользователь, используя стандартный дигитайзер и ручку, имитирует свою обычную подпись, а система считывает параметры движения и сверяет их с теми, что были заранее введены в базу данных.

Некоторые методы учитывают данные о колебаниях пера при воспроизведении подписи в трехмерном пространстве (X, Y – координаты и Z – давление на планшет). Системы, использующие одну из функций времени $X(t)$, $Y(t)$ или $Z(t)$, обеспечивают вероятность ошибок 0,1. Если использовать две функции, то получим 0,01. Для трех функций – 0,003.

Другие системы используют не сами функции, а их первую или вторую производную, что, впрочем, незначительно влияет на качество распознавания.

Иногда используются и более сложные сенсоры. Эти устройства записывают направление пятимерных векторов (x, y, p, θ_X, θ_Y), взятых в эквидистантных точках времени. Здесь p – осевое давление ручки, а θ_X и θ_Y – угол ручки в плоскости X–Y.

Эта дополнительная информация очень важна для предотвращения фальсификаций.

Динамическая верификация подписи включает в себя измерение евклидова расстояния между траекторией ручки, параметрами пространственных взаимосвязей и т. д. При совпадении образа подписи с эталоном система прикрепляет к подписываемому документу параметры подписи, содержащие несколько десятков характеристик динамики движения (направление, скорость, ускорение и др.). Эти данные шифруются, затем для них вычисляется контрольная сумма, и далее все это шифруется еще раз, образуя так называемую биометрическую метку. Для настройки системы вновь зарегистрированный пользователь от пяти до десяти раз выполняет процедуру подписания документа, что позволяет получить усредненные показатели и доверительный интервал.

Рассмотрим пример динамического метода, использующего координаты *X*, *Y* и *Z* – давление на планшет.

Пользователь вводит несколько образцов своей подписи. Для каждого образца определяются характеристические точки, соответствующие перегибу линии подписи (рис. 2.27). Затем строятся графики изменения каждой координаты для всех образцов подписи (рис. 2.28). В результате получается набор графиков изменения каждой координаты. После чего проводится масштабирование.

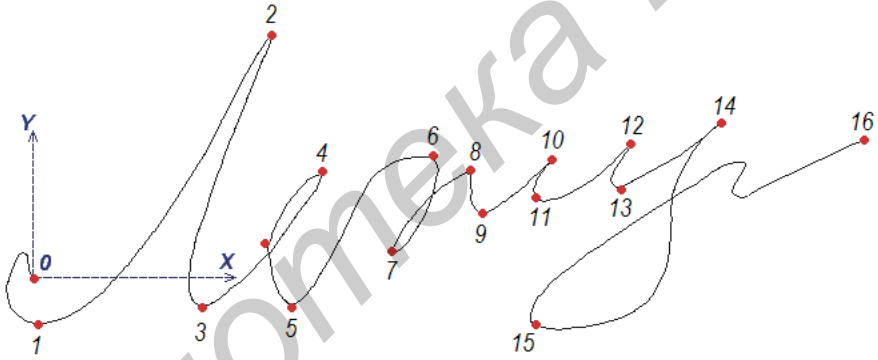


Рис. 2.27. Образец подписи и характеристические точки

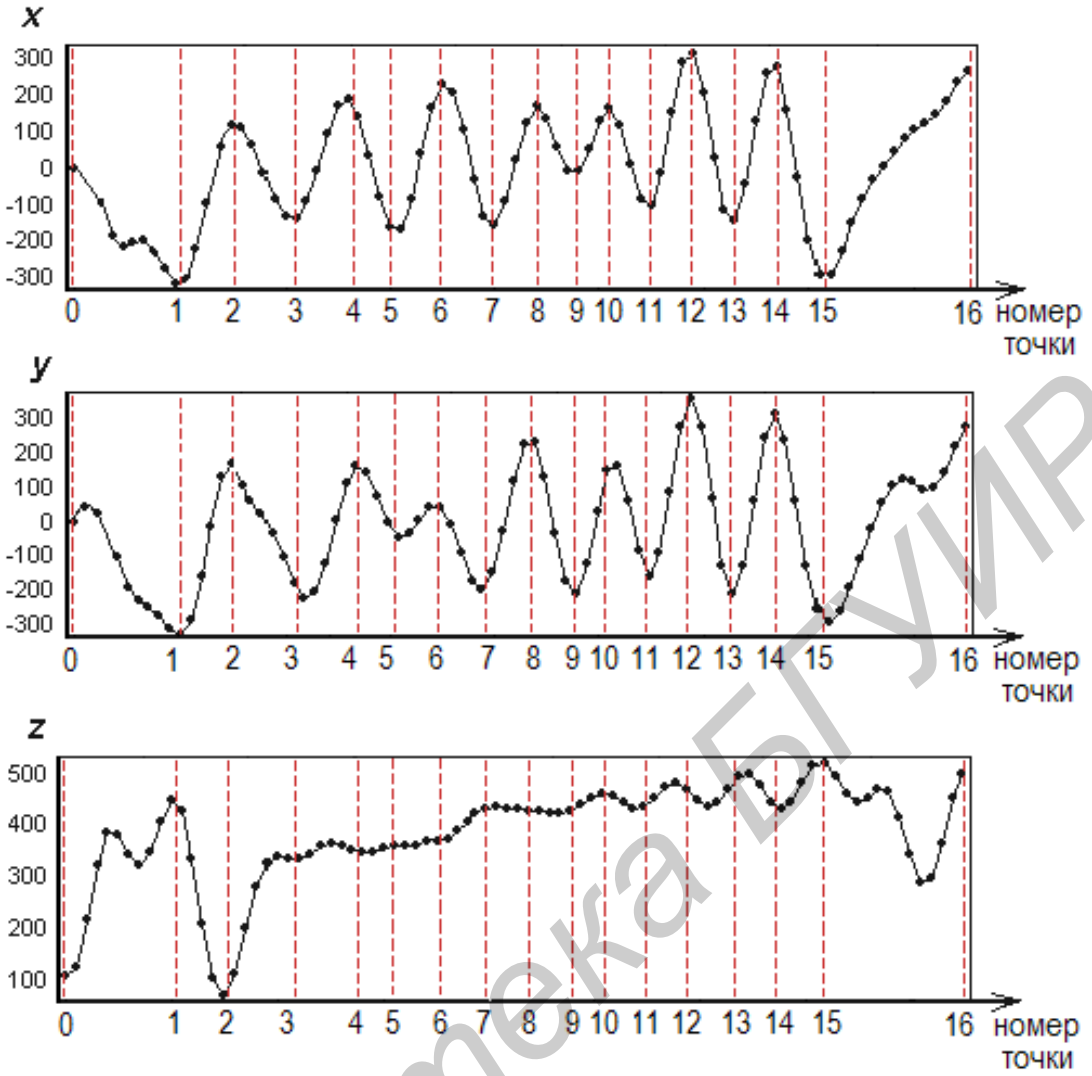


Рис. 2.28. Графики изменения каждой координаты

Для приведения всех реализаций подписи к единому масштабу вычисляются два масштабных коэффициента: амплитудный K_A и частотный K_G для каждой реализации:

$$K_A = \sqrt{\frac{\sum_{i=1}^{G}(A_{\text{ср}i}^2 + B_{\text{ср}i}^2)}{\sum_{i=1}^{G}(A_i^2 + B_i^2)}}; \qquad (2.1)$$

$$K_G = \frac{N}{N_{\text{ср}}}, \qquad (2.2)$$

где $A_{\text{ср}i}$ и $B_{\text{ср}i}$ – коэффициенты ряда Фурье среднего распределения; A_i и B_i – коэффициенты ряда Фурье масштабируемой реализации подписи; G – количество гармоник; N – длина масштабируемой реализации подписи.

В результате получаем масштабированные сигналы, изображенные на рис. 2.29. Как среднее арифметическое масштабированных сигналов получаем эталон подписи (рис. 2.30).

Для принятия решения о принадлежности полученного образца подписи необходимо использовать аппарат теории вероятностей. Количество зарегистрированных пользователей соответствует количеству первоначально выдвигаемых гипотез о принадлежности предъявленного образца подписи к какому-либо эталону. Нахождение наиболее вероятной гипотезы происходит с помощью стратегии Байеса, в которой априорной вероятностью считается апостериорная вероятность, вычисленная на предыдущем шаге.

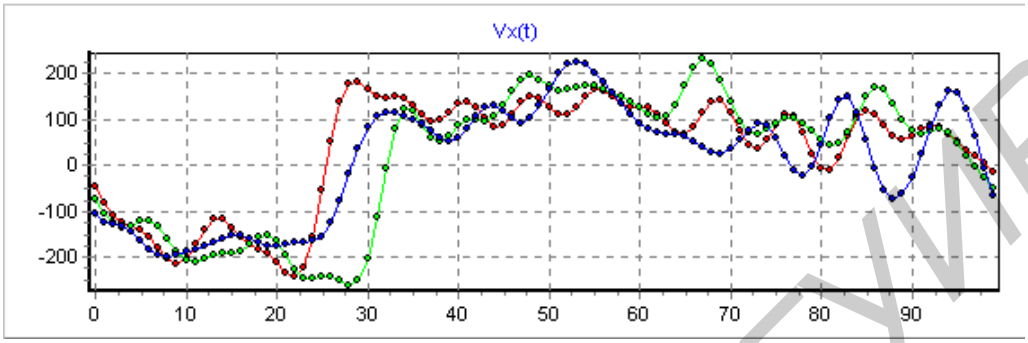


Рис. 2.29. Масштабированные варианты подписи

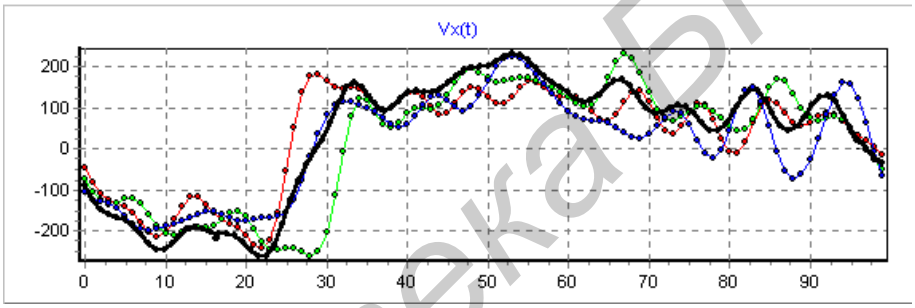


Рис. 2.30. Эталон подписи

$$P(H_i \mid A) = \frac{P(H_i)P(A \mid H_i)}{\sum_{i=1}^{n} P(H_i)P(A \mid H_i)}. \qquad (2.3)$$

Решение принимается на последнем шаге в пользу той гипотезы, для которой апостериорная вероятность оказывается наибольшей.

Условные вероятности на шаге A для каждой гипотезы определяются по нормальному закону распределения:

$$P(A \mid H_i) = \frac{1}{\sqrt{2\pi D}} e^{-\frac{(x-M)^2}{2D}}, \qquad (2.4)$$

где M и D – математическое ожидание и дисперсия определенного сечения i-го эталона.

Для выявления нарушителя, пытающегося подделать подпись, на этапе принятия решения о наиболее вероятном эталоне с помощью стратегии Байеса вводится специальная гипотеза «о подделке подписи».

2.6.1. Достоинства и недостатки метода

Достоинства метода:

– невысокая стоимость;

– относительная привычность для человека. Подпись уже давно является признанным методом, способным подтвердить личность человека. Работу данной системы легко объяснить человеку, и люди ей уже доверяют, так как данный способ идентификации является естественным и ненавязчивым.

Недостатки:

– высокий уровень ошибок 1 и 2 рода;

– необходимость приучения к работе с планшетом перед регистрацией;

– продолжительное время регистрации пользователя;

– пользователи могут изображать нестабильный почерк, если противятся системе.

3. ДОПОЛНИТЕЛЬНЫЕ БИОМЕТРИЧЕСКИЕ ПАРАМЕТРЫ

Рост рынка биометрических систем стимулирует развитие новых технологий идентификации, у каждой их которых есть свои достоинства и недостатки и своя область применения. Далее будут рассмотрены все эти биометрические параметры.

3.1. Идентификация по ДНК

ДНК часто называют почти идеальным биометрическим параметром, так как код ДНК является идентификационной информацией в цифровой форме, которая есть в любой клетке человека.

ДНК (дезоксирибонуклеиновая кислота) – нуклеиновая кислота, которая является основным компонентом хромосом эукариотовых клеток и некоторых вирусов. ДНК часто называют «строительным материалом» жизни, поскольку в ней хранится генетический код – основа наследственности.

В настоящее время для идентификации человека по ДНК почти повсеместно используются так называемые STR-локусы. Аббревиатура STR происходит от английского словосочетания *Short Tandem Repeat* – дословно: короткий тандемный повтор. Локусы данного типа представляют собой цепочки, состоящие из небольших, длиной 2–6 нуклеотидов, одинаковых последовательностей (мономеров), или «повторов». Аллели данных локусов различаются между собой количеством этих повторов. STR-локусы имеют следующие преимущества:

– большое количество аллелей, что способствует снижению вероятности случайных совпадений генотипов разных людей.

– большое количество известных STR-локусов и их относительно равномерное распределение по всем хромосомам человека.

– возможность с помощью современных методов проводить быстрое, точное и недорогое типирование образцов по данным локусам.

Международным стандартом de facto стала система CODIS (*Combined DNA Index System*), состоящая из 13 аутосомных STR-локусов (D3S1358, THOl, D21S11, D18S51, D5S818, D13S317, D7S820, D16S539, CSF1PO, vWA, D8S1179, TPOX, FGA).

Локусы данной системы подобраны так, что частота любого генотипа по ним настолько мала, что на всей Земле не может быть двух человек, имеющих один и тот же генотип по совокупности локусов системы CODIS.

В современных лабораториях генотипирование проводится автоматически с помощью аппаратно-программных комплексов, что позволяет унифицировать процедуру типирования и практически исключить влияние человеческого фактора.

На рис. 3.1 показан пример представления результатов типирования человека аппаратно-программным комплексом 3130 Genetic Analyzer (фирмы *Applied Biosystems*).

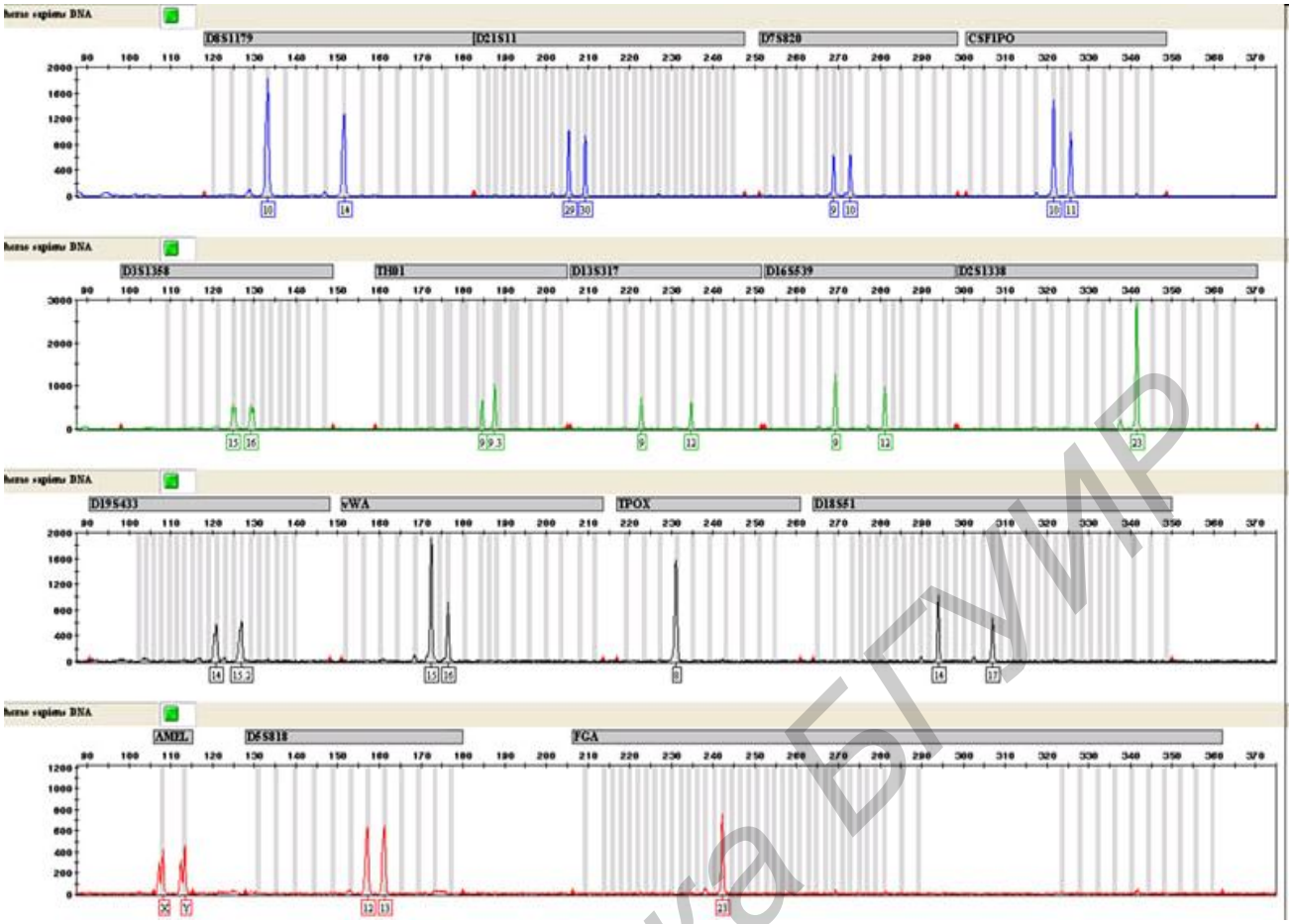


Рис. 3.1. Результаты типирования человека

Типирование проводится по системе локусов AmpFlSTR Identifier (фирма *Applied Bio systems*), содержащей все локусы системы CODIS, дополнительные STR-локусы D2S1338, D19S433, а также локус AMELOGENIN, по которому устанавливается половая принадлежность образца.

Таблица 3.1

Пример профиля результатов типирования человека

Локус	Аллели		Локус	Аллели	
D8S1179	10	14	D2S1338	23	23
D21S11	29	30	D5S818	12	13
D7S820	9	10	FGA	23	23
CSF1PO	10	11	D19S433	14	15,2
D3S1358	15	16	vWA	15	16
THOl	9	9,3	TPOX	8	8
D13S317	9	12	D18S51	14	17
D16S539	9	12	AMELOGENIN	X	Y

Любое различие между зарегистрированным и тестовым образцами говорит о том, что они принадлежат разным людям, вероятность их совпадения можно рассчитать. Обычные тесты оценивают вероятность полного совпадения как один к

триллиону с условием, что близкие родственники (особенно близнецы) могут быть исключены по другим основаниям.

Если в локусе расположено 50 разных аллелей, то человек может иметь 1275 возможных пар этих аллелей. Если рассмотреть 4 независимых локуса, получится 2,6 триллиона комбинаций. Конечно, идентификация по ДНК требует гарантии чистоты образцов и того, что образцы не перепутаются в процессе прохождения процедур.

Недостаток этого параметра в том, что однояйцовые близнецы будут иметь одну и ту же ДНК. Кроме того, с практической точки зрения сравнение людей на основе двух образцов ДНК – медленный (занимающий дни или часы), дорогой и сложный процесс.

Конфиденциальность – одна из главных проблем при идентификации по ДНК, так как в ДНК закодирована информация, которая может быть использована для других целей – незаконного получения информации о медицинских показаниях и предрасположенности человека к болезням, а также о расовой принадлежности и отцовстве. Информация о том, какая аллель присутствует в каждом локусе, не имеет большой ценности, в отличие от полной цепочки ДНК, представленной в оригинальном образце.

3.2. Распознавание сетчатки глаза

Идентификация человека по сетчатке глаза происходит путем сравнения изображений кровеносных сосудов глазного дна – хориоидальной сосудистой сети. Точнее, когда изображение получают только в ближнем инфракрасном диапазоне, сетчатка становится прозрачной, то есть самого изображения сетчатки бывает не видно. Хотя сегодня на рынке представлены и системы, в которых для получения изображения сетчатки используется свет видимого спектра.

История распознавания по сетчатке начинается с работы Саймона и Гольдштейна [5], которые отметили уникальность расположения сосудов глазного дна у каждого человека. Эта методика стала развиваться в промышленном масштабе с середины 1970-х годов.

Компания *EyeDentify* предлагает на рынке автономную систему идентификации по сетчатке, рассчитанную на 3000 человек. Размер шаблона – 96 байт, идентификация субъекта среди 1500 человек может быть выполнена за 5 с. Система не может получить хорошее изображение, если у человека сильный астигматизм или очень плохое зрение. Для получения образца сетчатки глаз человека должен находиться близко к сенсору (на расстоянии до 0,75 дюйма в производственных системах и до 12 дюймов в прототипах).

К сожалению, сенсоры, используемые для идентификации по сетчатке, все еще слишком дороги по сравнению с сенсорами для считывания других биометрических параметров.

Большим преимуществом идентификации по сетчатке является постоянство параметра: на сетчатку не влияет ничего, кроме сильных травм, ее невозможно подделать. Создание поддельной сетчатки чрезвычайно сложно из-за оптических

свойств, которые должны быть воспроизведены. Существуют надежные способы защиты от фальсификации.

В настоящее время появились улучшенные системы идентификации по сетчатке. По информации разработчиков, в современной системе применяется камера с электромеханическим сенсором, который производит измерение естественных отражающих и поглощающих свойств сетчатки с расстояния до 3 см. Изображение сетчатки получается следующим способом: человек смотрит в устройство одним глазом, лампочка 7 мВт освещает сетчатку. Рисунок вен записывается в видимом и ближнем инфракрасном свете (ближний ИК-диапазон, 890 нм).

Компания *Oki Electric* сообщила о разработке инновационной технологии биометрической идентификации пользователей по сетчатке глаза, ориентированной на современные, оснащенные камерой мобильные телефоны. В отличие от предыдущих разработок *Oki* в данной области, предполагающих инфракрасное сканирование сетчатки, новая технология позволяет использовать для решения этой задачи стандартный объектив. Технология будет предложена разработчикам коммерческих решений, которые с ее помощью смогут повысить безопасность платежей, осуществляемых с помощью мобильного телефона.

3.2.1. Достоинства и недостатки метода

Метод идентификации по сетчатки глаза имеет следующие достоинства:

– высокий уровень статистической надежности;

– из-за низкой распространенности систем мала вероятность разработки способа их «обмана»;

– бесконтактный метод снятия данных.

Недостатки:

– сложная при использовании система с долгим временем обработки;

– высокая стоимость системы;

– отсутствие широкого рынка предложения и недостаточная интенсивность развития метода.

3.3. Распознавание по термограммам

Термограмма – изображение, полученное в различных областях инфракрасного спектра, иногда с дополнительным использованием видимого спектра.

Термограммы в биометрии – это изображения частей тела в коротковолновом (0,9–1,7 мкм), среднем (3–5 мкм) и длинноволновом (8–12 мкм) диапазонах инфракрасного спектра. Ранее проводились различные исследования тепловых изображений, в особенности лица и рук. Большое преимущество термограмм перед обычными изображениями – это их независимость от изменения освещения: термограммы лица могут быть сделаны при полном отсутствии света. На термограммы также не влияет изменение внешности, по крайней мере, они нечувствительны к некоторым видам маскировки.

В случае с термограммой считываемая структура находится под кожей, она не зависит от возраста и эмоционального состояния, ее невозможно подделать или изменить за исключением случаев физических увечий.

В основе метода идентификации личности по термограмме лица лежит тепловой рисунок лица, создаваемый тепловым излучением кровеносных сосудов и фиксируемый с помощью инфракрасной камеры. Однако в отличие от венозных и тканевых структур кровоток имеет динамическую природу, что может обуславливать появление или пропадание вторичных кровеносных сосудов.

Кроме того, термограмма лица может изменяться под воздействием температурных условий окружающей среды, а также алкоголя. Преимущество метода идентификации по термограмме лица заключается в том, что этот метод не предполагает использования приборов ИК-подсветки, а функционирует на основе ИК-излучения лица. Данное свойство находит широкое применение в приложениях видеонаблюдения, когда стоит задача обнаружения людей в темноте. Тем не менее специалисты прочат этому методу хорошую перспективу применения в сочетании с другими биометрическими технологиями.

3.4. Распознавание по походке

Походка относится к поведенческим биометрическим параметрам, она изучена еще мало. Достоинство этого метода – возможность распознавания людей на расстоянии с использованием видеозаписи. В первых опытах идентификация проводилась при помощи оборудования, считывающего движения человека. Более поздние исследования тоже основаны на наблюдении за людьми на спонтанно снятом видео.

Благодаря новым исследованиям механизмы распознавания по походке стали более совершенными. Исследования проводились на маленьких группах; оказалось, что результаты распознавания зависят от многих обстоятельств: поверхности, по которой идет человек, точки наблюдения, обуви, скорости перемещения человека и, конечно, его физического здоровья. Некоторая одежда (особенно юбки) может затруднять распознавание.

Всестороннее исследование метода распознавания человека по походке проведено на основе большой базы данных (452 видеозаписей 74 объектов). Основной алгоритм распознавания:

– сначала полуавтоматически определяются ограничивающие прямоугольники для идущего объекта;

– потом из них извлекаются силуэты;

– третий шаг – это сведение ограничивающих прямоугольников к размеру 128×88 пикселей, для того чтобы выполнить сопоставление путем «корреляции» силуэтов.

Разработан так называемый «гайт-код» – код походки, вычисляемый после разделения специальными фильтрами характерных и случайных движений, зафиксированных встроенными сенсорами. В ходе испытаний точность такого способа идентификации превышала 90 %.

Процедура распознавания очень сильно зависит от условий, в которых находится объект, например: будет сложно распознать человека, идущего по какой-либо поверхности (допустим, по бетону), если система была обучена на основе видеозаписи того же человека, идущего по другой поверхности (скажем, по траве). Эта область биометрии требует дальнейшей разработки.

3.5. Распознавание по клавиатурному почерку

Идентификация по клавиатурному почерку – это идентификация человека по его собственному стилю печати. Каждый человек имеет характерные особенности печати: время между нажатиями клавиш и время удержания клавиши является более-менее постоянным для каждого человека и отличает его от других людей.

Существует система на базе искусственных нейронных сетей для различения 15 людей по клавиатурному почерку. Исследователи заметили, что разница между людьми более заметна, если использовать для распознавания временные интервалы между нажатием клавиш и время удержания одной клавиши.

Системы идентификации по клавиатурному почерку основаны на вводе фиксированного слова, но предположительно они могут быть и независимыми от набираемого текста, как системы распознавания голоса.

Уже существуют и коммерческие продукты, основанные на подсчете времени набора текста.

В одной из исследовательских работ предлагается метод идентификации по клавиатурному почерку на основе сменных виртуальных клавиатур. Суть метода заключается в следующем.

При коллективной работе в автоматизированных информационно-управляющих системах каждому оператору предоставляется своя персональная виртуальная клавиатура, отображаемая на экране его компьютера. Вид и состав этой клавиатуры может быть произвольным, например таким же, как и стандартной, но расположение клавиш на клавиатуре отличается для каждого оператора. Вид клавиатуры генерируется системой либо из заранее подготовленного списка, либо на основе реализации некоторого алгоритма, либо случайно. Каждый оператор должен в течение достаточно длительного времени работать на «своей» виртуальной клавиатуре, предоставленной ему системой. Набор символов на виртуальной клавиатуре может выполняться путем перемещения курсора на экране одним из двух способов:

– мышью – нажатием соответствующих виртуальных клавиш кнопкой мыши;

– пятью клавишами на реальной клавиатуре компьютера (стрелки вверх, вниз, вправо, влево, ввод).

Оператор, достаточно длительное время работающий на «своей» виртуальной клавиатуре, приобретает индивидуальные навыки, которые выражаются в определенной картине скоростей ввода отдельных символов и текста в целом. В такой ситуации попытки подмены оператора хорошо идентифицируются системой анализа клавиатурного почерка.

С целью апробации предлагаемого метода была разработана программная тестовая модель системы клавиатурного мониторинга. Для ввода текста использовалась программно изменяемая виртуальная клавиатура, содержащая все алфавитно-цифровые и основные функциональные клавиши, обычно используемые в стандартных клавиатурах.

Работа с виртуальной клавиатурой осуществлялась с помощью компьютерной мыши. При постановке эксперимента в модели были использованы две виртуальные клавиатуры №1 и №2. Расположение клавиш клавиатуры №1 совпадает с расположением клавиш стандартной компьютерной клавиатуры. В клавиатуре №2 алфавитные клавиши расположены в порядке следования букв в алфавите.

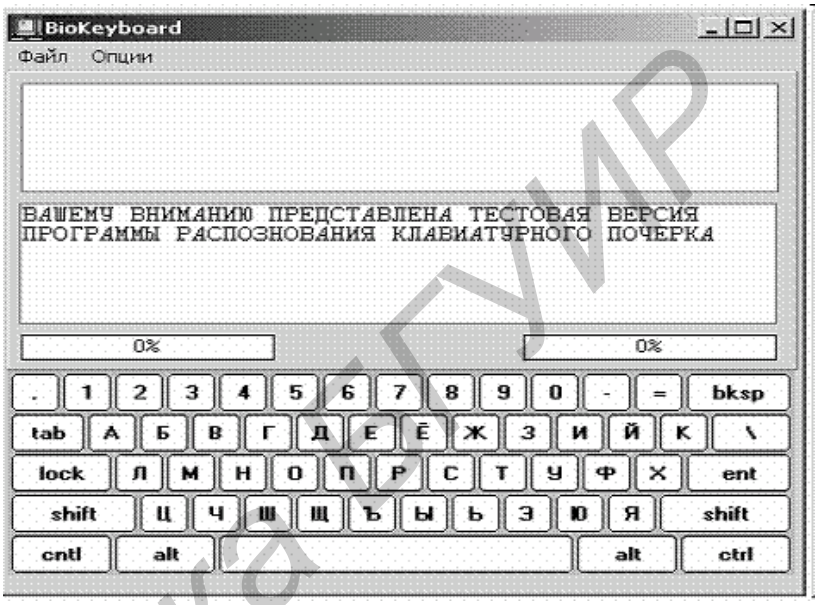


Рис. 3.2. Интерфейс программной модели системы клавиатурного мониторинга

В верхней части интерфейса (рис. 3.2) имеются два текстовых окна. В нижнем окне отображается текст, который необходимо ввести, а в верхнем – текст, который реально вводится.

Над цифровой частью виртуальной клавиатуры имеются два окна: левое показывает текущее число введенных символов текста (в процентах), правое – текущее число допущенных ошибок относительно эталона (в процентах).

Для тестирования системы была использована следующая методика:

– на первом этапе после некоторой тренировки на клавиатуре №2 пользователю «свой» предлагалось ввести на этой клавиатуре некоторый произвольный осмысленный текст, состоящий из 10–15 предложений. По результатам ввода формировался биометрический эталон пользователя «свой»;

– на втором этапе пользователь «свой» проверял работоспособность системы и при необходимости изменял точность аутентификации;

– на третьем этапе система тестировалась для пользователя «чужой». В качестве «чужого» использовался другой пользователь, имеющий хорошие навыки работы на стандартной клавиатуре. Этому пользователю предлагалось вводить тот же текст, используя клавиатуру пользователя «свой», т. е. клавиатуру №2. Предполагалось, что для «чужого» ввод с другой клавиатуры будет затруднен.

В результате тестирования система успешно разделяла пользователей на категории «свой» и «чужой». Во время работы «своего» ошибка изменялась от 2 до 15 %. Для «чужого» интервал изменения ошибки аутентификации составил 70–100 %.

3.6. Распознавание формы ушей

Измерение ушей было частью системы Бертильона, в которой обученные наблюдатели определяли тип формы ушей, чтобы использовать его как один из индексов в большой биометрической системе. Есть даже свидетельства применения латентных отпечатков ушей для идентификации преступников. В последнее время больше внимания уделяется форме ушей как биометрическому параметру для автоматической идентификации. Одна группа исследователей использовала технику нахождения краев для получения основной структуры уха, необходимой для проведения сопоставления. Эти авторы также применяли термограммы для исключения зависимости изображения от освещения и волос.

Дополнительный интерес к распознаванию по форме ушей возник в связи с проектом «Идентификация человека на расстоянии».

Анализ основных элементов ушей похож на систему анализа при помощи «собственных лиц». Использование только методики распознавания по форме ушей не так эффективно, как распознавание по лицу; комбинация изображений «лицо плюс ухо» повышает точность идентификации.

3.7. Распознавание по отражению кожи

Один из новых биометрических параметров, появившихся благодаря разработке новых сенсоров, – отражение кожи. В этой методике используется маленький чип, разработанный корпорацией *Lumidigm*, с помощью которого измеряется отражение от кожи ближнего инфракрасного света в диапазоне с длиной волны больше 6 мм. Пока эта технология идентификации применяется отдельно, но в комбинации с распознаванием по отпечаткам пальцев она могла бы обеспечить защиту от подделок. Преимуществом данной технологии является то, что для образца маленького размера требуется и маленький чип – по размеру объема памяти и производительности.

3.8. Распознавание по движению губ

Движение губ во время разговора относится к поведенческим биометрическим параметрам. Оно может использоваться как визуальное дополнение к системе распознавания говорящего; технология аутентификации по движению губ имеет такие же разновидности, что и методика распознавания говорящего: с фиксированным текстом, зависимая от текста и независимая от текста. В последнее время стало проводиться больше исследований в этой области благодаря распространению доступных баз данных.

На рынке представлена биометрическая система компании *BioId*, использующая движения губ. Одно из самых больших достоинств этого метода – возможность легко совместить его с идентификацией говорящего и распознаванием по геометрии лица. Таким образом, можно создать очень точную систему, которую будет сложно обмануть. Подобная тройная биометрическая система предназначена

для контроля физического доступа, она считывает параметры человека, говорящего в микрофон перед камерой. Видеоизображение используется для анализа геометрии лица и движения губ, результаты которого интегрируются с результатами распознавания по голосу.

При определенном освещении и высоком качестве изображения можно получить очень хорошую видеозапись движения губ. Тем не менее, когда условия съемки плохие, определить положение губ в видеоизображении, полученном в свете видимого диапазона, бывает довольно сложно.

Для получения видеоизображения движений губ используются два вида света невидимого диапазона:

– *инфракрасный* (если требуется высокий уровень безопасности, то можно добавить тепловые изображения. Это же касается распознавания походки и формы ушей);

– *длинноволновый инфракрасный* (когда требуется недорогое решение, можно использовать контролируемое длинноволновое инфракрасное освещение).

Этот особый тип активного считывания, как и любая попытка контроля изображения, делает процесс получения биометрического образца заметным и менее пригодным для скрытой сортировки типа.

3.9. Идентификация по запаху тела

Уже давно известно, что человека можно идентифицировать по его собственно запаху. Прогресс в области химического анализа с применением полупроводников привел к изобретению «электронных носов», которые могут измерять концентрацию различных химических элементов (всего 32). Такие сенсоры, конечно, не обладают ни различительной способностью, ни чувствительностью человеческого носа и имеют недостатки – нуждаются в калибровке, плохо работают в условиях перегрузки (при наличии множества различных запахов может произойти даже «отравление»). Также известно, что запах человека зависит от его образа жизни – начиная от питания и состояния здоровья и заканчивая использованием мыла, парфюмерии и дезодорантов. Пока еще неизвестно, можно ли нормализовать эти факторы настолько, чтобы надежная идентификация человека по запаху стала возможной.

4. ОСНОВНЫЕ ОШИБКИ БИОМЕТРИЧЕСКИХ АУТЕНТИФИКАЦИОННЫХ СИСТЕМ

Требования, предъявляемые к биометрическим аутентификационным системам, включают в себя максимально допустимый уровень ошибок. Существует несколько типов биометрических ошибок, выражаемых в уровнях или в процентах, которые необходимо оценить перед разработкой системы и выбором определенного биометрического параметра. Некоторые из этих ошибок являются неотъемлемой характеристикой биометрической аутентификации как разновидности процесса распознавания образов; другие ошибки специфичны для биометрических аутентификационных систем. Очевидно, что любая биометрическая аутентификационная система будет делать ошибки и реальное количество ошибок мэтчера нельзя определить теоретически; статистические расчеты вероятности ошибок можно получить, только используя базы данных биометрических образцов.

4.1. Сопоставление

Мэтчер – это система, которая получает два образца биометрических параметров и проверяет величину их сходства. В верификационной системе эта величина определяет, действительно ли два образца принадлежат одному «реальному» объекту.

Перед тем как двигаться дальше, необходимо дать определение мэтчера. Для этого два реальных образца (например, два отпечатка пальца или два лица) обозначим как β и β', а связанные с ними машинные репрезентации $B = f(\beta)$ и $B' = f(\beta')$, где f – процесс получения образцов сенсором и, возможно, извлечения свойств B и B'. К сожалению, реальные биометрические параметры β и β' – *реально* существующие объекты – это функции времени, и, может быть, еще более важно то, что функция считывания f тоже зависит от времени, в течение которого происходит считывание, а также других факторов окружающей среды, поэтому обозначим эту функцию как f_t. Таким образом, биометрические репрезентации B и B' являются функциями времени:

$$B = B(t) = f_t\left(\beta(t)\right) \quad \text{и} \quad B' = B'(t') = f_{t'}\left(\beta'(t')\right).$$

Таким образом, мы видим, что уникальность биометрического параметра β и уникальность образца или репрезентации B этого параметра на самом деле не являются бесспорными. Степень уникальности сильно варьируется с течением времени от одного биометрического идентификатора к другому (например от пальца к лицу), и поэтому *масштабируемость* свойств разных биометрических параметров очень различается.

Устройство для сопоставления биометрических образцов принимает решение, вычисляя вероятность того, что два представленных образца параметров двух человек (*Объект* 1 и *Объект* 2) являются одинаковыми, т. е. объекты 1 и 2 – это одна и та же личность. Это вычисление – определенное на базе алгоритма измере-

ние сходства. Это измерение зависит от точности считывающего устройства и точности машинной репрезентации биометрического образца. Тем не менее, как будет видно позднее, если при измерении сходства будут выявлены свойства, отличающие одного человека от другого, это различие должно быть связано с вероятностью сходства *Prob* (объект$_1$ ≡ объект$_2$).

Независимо от типа биометрического идентификатора биометрический параметр обрабатывается путем подсчета величины $s(B', B)$, как показано на рис. 4.1; $s(B', B)$ является величиной сходства образцов B' и B, т. е. сходства между β и β'. Проще говоря, устройство сопоставления принимает β и β' как входящие данные и вычисляет величину s:

$$s\left(B', B\right) = s\left(B'\left(t'\right), B\left(t\right)\right) = s\left(f_{t'}\left(\beta'\left(t'\right)\right), f_t\left(\beta\left(t\right)\right)\right). \qquad (4.1)$$

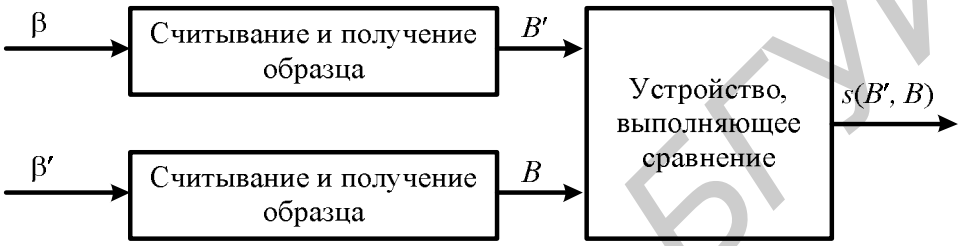


Рис. 4.1. Устройство для сопоставления определяет величину сходства s между образцом B объекта β и образцом B' объекта β'

Обычно B – зарегистрированный (в момент времени t) образец (он может быть и биометрическим шаблоном), который изменяется только при определенных обстоятельствах, а B' – «живой» образец, требующий сопоставления. Величина $s(B',B)$ только выражает некоторую степень подобия, при которой настоящие биометрические параметры β и β' являются одинаковыми. Конечно, если у нас есть вероятностный мэтчер, то $s(B', B)$ можно получить путем подсчета вероятности *Prob*(β ≡ β'), но в общем имеется недостаточный объем информации о сходстве, кроме того, что сходство монотонно возрастает с увеличением вероятности, т. е. чем больше сходство $s(B', B)$, тем больше вероятность, что два биометрических параметра принадлежат одному и тому же β.

Другой способ вычислить величину сходства – это определить расстояние или разницу $d(B', B)$ между образцами B' и B. Такую разницу можно определить с помощью метрики Левенштейна [6] или расстояния между образцами в определенном векторном пространстве биометрических свойств. Его можно преобразовать в величину сходства следующим соотношением:

$$s\left(B', B\right) = \exp\left\{-d\left(B', B\right)\right\},$$

т. е. величина расстояния [0, ∞) преобразуется в величину сходства [0, 1].

4.1.1. Два вида ошибок

В большинстве случаев количество ошибок в системах биометрической аутентификации определяется точностью, с которой внутреннее биометрическое уст-

ройство сопоставления сможет определить, какая из гипотез является истинной. Вводя биометрические образцы, можно построить две гипотезы:

$$\begin{aligned} &\text{Нулевая гипотеза} && H_0 \text{ два образца совпадают,} \\ &\text{Альтернативная гипотеза} && H_a \text{ два образца не совпадают.} \end{aligned} \tag{4.2}$$

В различных биометрических приложениях существуют различные определения гипотез H_0 и H_a, различные решения, которые могут принимать эти приложения, и поэтому разные приложения имеют разные определения ошибок. В связи с этим существует много терминов, выражающих точность приложения, например коэффициент ложного сходства, коэффициент ложного доступа, коэффициент ложного признания и т. д.

Определим коэффициент ошибок биометрического мэтчера на основании правильности принятого им решения относительно двух исходящих данных, как в (4.2). Мэтчер принимает как истинную гипотезу H_0 или гипотезу H_a. Поэтому существует два вида ошибок, которые может сделать мэтчер. Используем терминологию Уэймена [7], так как она позволяет обозначить различие между биометрическим мэтчером и биометрическим приложением:

I. *Ложное сходство* (ЛС) – решение о том, что биометрические параметры принадлежат одной личности, хотя на самом деле это не так; частота появления такой ошибки называется коэффициентом *ложного сходства* (КЛС).

II. *Ложное различие* (ЛР) – решение о том, что биометрические параметры принадлежат разным людям, хотя на самом деле они принадлежат одной личности; частота появления этой ошибки называется коэффициентом *ложного различия* (КЛР).

Такие ошибки называют ошибками *типа* I и II соответственно, в случае ошибки типа I гипотеза H_0 ошибочно принимается за истинную (хотя на самом деле истинна H_a), а в случае ошибки типа II за истинную ошибочно принимается гипотеза H_a (хотя верной является H_0). Эти ошибки и эти термины–*ложное сходство* и *ложное различие* – определены исключительно для гипотез (4.2).

Кроме ошибочных, могут быть приняты и правильные решения. Мы имеем истинное сходство и истинное различие, если принимается правильное решение относительно сходства или различия двух образцов.

4.1.2. Распределение значений

Гипотезы, сформулированные в (4.2), легко преобразовать в уравнения:

$$\begin{aligned} H_0 &: \beta' \equiv \beta, \\ H_a &: \beta' \neq \beta. \end{aligned} \tag{4.3}$$

Чтобы выбрать одну из двух гипотез, подсчитывается величина $s(R', R)$. Следующее решение «да/нет» основывается на некоторой пороговой величине T:

$$\begin{aligned} &\text{Принять } H_0 \text{ как истинную, если } s > T, \\ &\text{Принять } H_a \text{ как истинную, если } s \leq T. \end{aligned} \tag{4.4}$$

Решения типа (4.4) относятся к так называемым «тяжелым» решениям, в этом случае приложению не позволяется выдавать решения типа «неизвестно» или «слишком схожи, чтобы определить». Это называется принятием решения без обработки исключительных случаев.

Достоверность величины различия при сравнении двух биометрических образцов зависит от многих факторов. Существует изменчивость входящего сигнала P реального биометрического образца, а также различие между сенсорами. Особенно много вариаций возникает в процессе получения образца $R = f(\beta)$, так как объект может представить реальный биометрический параметр β в разных вариантах. Поэтому при получении образцов вероятно появление гораздо большего числа вариантов, чем, например, при аутентификации с помощью пароля, где ошибка может возникнуть только при неправильном вводе. Если получены два образца одного и того же биометрического параметра (т. е. $\beta' = \beta$), величина сходства $s(R', R)$ равна единице (или любой другой величине, выражающей сходство), кроме того случая, когда образцы являются копией друг друга. Точно так же, когда имеются два образца параметров двух разных людей $\beta' \neq \beta$, величина сходства $s(R', R) \neq 0$ (или любой другой минимальной возможной величине). Таким образом, когда $\beta' = \beta$, величина сходства высокая, а когда $\beta' \neq \beta$, величина сходства обычно низкая. Это видно на рис. 4.2, где изображено распределение вероятностей $p_n(s)$ величины различия и $p_m(s)$ величины сходства (пороговая величина T расположена высоко, чтобы снизить коэффициент ложного доступа).

Теперь опишем более точно два типа ошибок, которые могут быть допущены:

I. *Ложное сходство.* Принимается решение, что $\beta' = \beta$, так как $s(R', R) > T$, хотя на самом деле $\beta' \neq \beta$. H_0 принимается за истинную, хотя истинной является H_a.

Мошенник каким-то образом сгенерировал высокую величину различия ($s > T$), т. е. объект β' имитирует объект β.

II. *Ложное различие.* Принимается решение, что $\beta' \neq \beta$, потому что $s(R', R) \leq T$, хотя на самом деле $\beta' = \beta$. Гипотеза H_0 признается ложной. H_a принимается за истинную, хотя истинной является H_0.

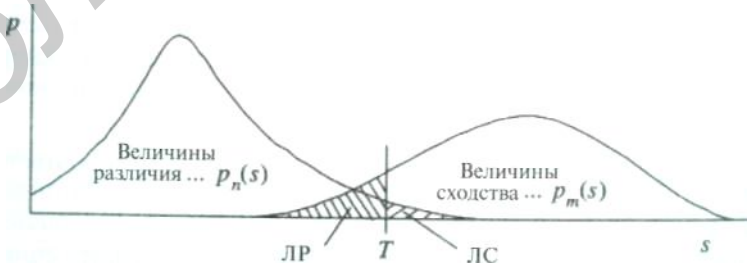


Рис. 4.2. Распределения вероятностей величины различия $p_n(s)$ и величины сходства $p_m(s)$

Подлинный объект может показать уровень сходства s меньше, чем T; такое может случиться, если биометрический параметр p предоставляется в плохом состоянии и, следовательно, запись и цифровой вариант получаются низкого качества. *Коэффициент ложного сходства* (КЛС) и *коэффициент ложного различия*

(КЛР) – это соответственно частота, с которой появляется ложное сходство и ложное различие:

1. КЛС – это период времени, в течение которого биометрический образец β' совпадает с *R*, когда β' ≠ β.

С точки зрения вероятности величина случайного сходства *s* вычисляется из распределения различий $p_n(s) = p(s|H_a)$ на рис. 4.2, при этом $s > T$. КЛС – это заштрихованная область справа под кривой плотности распределения различий $p_n(s)$, т. е. доля времени $s > T$, когда β' ≠ β. Получаем КЛС как функцию *T*:

$$\text{КЛС}(T) = 1 - \int_{s=T}^{\infty} p_n(s)\text{d}s\,. \tag{4.5}$$

2. КЛР – это период времени, в течение которого биометрический образец *R′* не совпадает с *R,* когда β' ≡ β.

Случайная переменная *s* вычисляется из распределения величин сходства $p_n(s) = p(s|H_a)$ на рис. 4.2, где $s < T$, что означает, что КЛР – это заштрихованная область под кривой распределения плотности истинных величин. Эта область является долей времени $s < T$, когда β' ≡ β:

$$\text{КЛР}(T) = \int_{s=-\infty}^{T} p_m(s|H_a)\text{d}s\,. \tag{4.6}$$

К сожалению, для биометрических приложений распределение величины различий и $p_n(s)$ и распределение величины сходства $p_m(s)$ на рис. 4.2 часто перекрывают друг друга, поэтому становится невозможным найти такую пороговую величину, при которой КЛС = 0 и КЛР = 0. Таким образом, пороговая величина *T* в правиле принятия решения (4.4) должна быть выбрана так, чтобы биометрическая система функционировала в «оптимальном» режиме. Выбор этой величины требует оценки последствий двух типов ошибок. В первом приближении биометрический мэтчер должен быть настроен на работу с допустимым коэффициентом ложного сходства и ложного различия для данной совокупности объектов. Эта пороговая величина может быть определена только в процессе обучения и тестирования, где будут представлены более-менее типичные образцы выборки пользователей. На рис. 4.2 рабочая точка *T* выбрана таким образом, что величина коэффициента ЛС меньше величины коэффициента ЛР.

Пороговая величина *T* устанавливает компромисс между КЛС(*T*) и КЛР(*T*), что выражается характеристической кривой РХПУ [8]. При работе мэтчера с высокой *T* получаем низкий КЛС, но высокий КЛР; низкая величина *T* соответственно дает высокий КЛС и низкий КЛР.

Суммарное распределение вероятности *G*(*y*) и *F*(*x*) величин сходства и различия соответственно определяется следующим образом:

$$\begin{aligned} G(y) &= \int_{-\infty}^{y} p(s|H_a)ds, \\ F(x) &= \int_{-\infty}^{x} p(s|H_0)ds. \end{aligned} \tag{4.7}$$

Эти выражения можно использовать как синонимы КЛС и КЛР (рис. 4.3). Обозначения КЛС и КЛР являются общепринятыми в отличие от обозначения ве-

роятности в терминах суммарного распределения ($G(y)$ и $F(x)$). Заметим, что функция КЛР(y) – это не распределение.

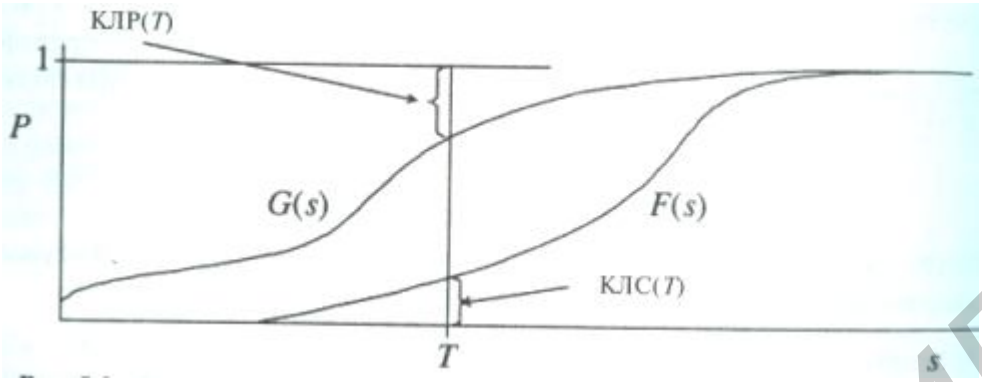


Рис. 4.3. Суммарное распределение вероятности величины различия и сходства $G(s)$ и $F(s)$ ($КЛС(T)$ и $КЛР(T)$ обозначены в точке T)

4.1.3. Вычисление ошибок данных

Результатом работы мэтчера (см. рис. 4.1) будет величина $s(R', R)$, которая как-то связана с вероятностью *Prob* ($\beta' \equiv \beta$). Для оценки работы мэтчера $s(R', R)$ нам нужно получить доступ к данным и подсчитать $G(y)$ и $F(x)$.

Точнее, должен быть набор **X** с M величинами сходства (подлинный, подозреваемый) и набор **Y** с N величинами различий (фальсификатор, легитимный). Нужно вычислить истинное распределение величин сходства $F(s)$ и распределение величин различия $G(s)$. Распределение сходства $F(x)$ рассчитывается на основе величин сходства $\mathbf{X} = \{X_1, \ldots, X_M\}$ следующим образом:

$$F(s) = \frac{1}{M}\sum_{i=1}^{M} 1(X_i \le s) = \frac{1}{M}(\text{количество } X_i \le s). \qquad (4.8)$$

Величина несоответствия (различия) $\mathbf{Y} = \{Y_1, \ldots, Y_N\}$, с другой стороны, дает оценку распределения величины различий $\hat{G}(s)$:

$$\hat{G}(s) = \frac{1}{N}\sum_{j=1}^{N} 1(X_j \le s) = \frac{1}{N}(\text{количество } Y_i \le s). \qquad (4.9)$$

Эти расчеты распределения вероятности называются эмпирическим распределением[1].

Взяв величину распределения, как на рис. 4.2, можно рассчитать вероятность КЛС и КЛР для определенной величины s. Эти вероятности невозможно вычислить точно, их можно только определить, используя тестовые базы данных, которые представляют пользователей и (в идеальном варианте) «врагов», пытающихся проникнуть в систему без авторизации. Истинное значение коэффициента ложного сходства мэтчера при определенной величине s оценить трудно, потому что, не-

[1] Эмпирические суммарные распределения $G(y)$ и $F(x)$ иногда используются вместо КЛС и КЛР, которые также соотносятся с $G(y)$ и $F(x)$ соответственно.

смотря на множество доступных тестовых баз данных, существует очень мало баз с поддельными или имитированными биометрическими параметрами. Случаи мошенничества и фальсификации требуют более внимательного изучения. Единственная область, где подделки изучены очень хорошо, – это верификация подписи, но даже там большая часть имеющегося тестового материала – фальсификации «с нулевым усилием». КЛС и КЛР с заданной величиной T могут быть вычислены, только если есть достаточное количество обучающих данных, которые представляют целевую популяцию. Часто учебные данные неточно отражают картину действительности, поэтому невозможно говорить о точном КЛС и КЛР мэтчера.

Наряду с подсчетом коэффициента ложного сходства и ложного различия должна быть вычислена и степень достоверности этих ошибок. Это позволяет приложениям принимать обоснованные решения (используя теорию принятия решений, анализ рисков и т. д.). Если следовать стандартной процедуре, обучение биометрической системы происходит при условии, что $\beta' \neq \beta$, т. е. при подделке β. Следовательно, тестовые базы данных дают величину сходства значительно меньшую, чем величину подделки, и степень достоверности КЛР обычно намного ниже, чем КЛС. Тип ложного доступа, который имеется здесь в виду, – это коэффициент ложного доступа, обусловленный «атаками с нулевым усилием». Когда биометрическая система атакуется профессиональными мошенниками, коэффициент ложного сходства будет значительно выше. Нужно отметить, что все исследования ошибок по умолчанию используют «усредненный» образ мошенников.

Так как на практике коэффициент ложного сходства для любого биометрического параметра никогда не будет равен нулю, применение биометрического мэтчера не гарантирует невозможность отказа от авторства. Отказ от авторства здесь означает отказ объекта от проведенной транзакции. Так как пароль или собственность могут быть переданы другому лицу, человек может заявить, что аутентификация не была пройдена лично им. Биометрические параметры «подтверждают» присутствие конкретного человека, но с определенной вероятностью ошибок.

4.1.4. Коэффициент ошибок мэтчеров

До настоящего времени определялись ошибки с точки зрения совпадения или несовпадения биометрических образцов, как в выражении (4.3). Биометрический мэтчер может выбрать одну из двух гипотез, используя правило принятия решений (4.4). Для биометрических мэтчеров были отмечены ошибки, связанные с принятием неверной гипотезы ложного сходства или ложного различия, следуя терминологии Уэймена [9].

С другой стороны, можно использовать и общепринятую терминологию распознавания образов – *ложный доступ* и *ложный отказ доступа,* в которых «доступ» и «отказ доступа» связаны с принятием или непринятием нулевой гипотезы, а не с предоставлением или непредоставлением объекту доступа к приложению. Поэтому в биометрии существует два разных определения принятия и отказа:

1) *принятие/отказ* – для гипотез H_0 и H_a с точки зрения теории распознавания образов, как было рассмотрено ранее;

2) *доступ/отказ* – для объекта при попытке получить доступ к приложению (основаны на биометрической аутентификации).

Биометрические приложения отличают от простой проверки гипотез совпадения с использованием мэтчеров, как на рис. 4.1, потому что в приложениях существует процедура регистрации в некоей базе данных **M**.

4.1.5. Определение КЛД и КЛОД, положительная аутентификация

Положительные верификационные («*я тот, кем я себя заявляю*») и положительные идентификационные («*я утверждаю, что я зарегистрирован в базе данных*») системы могут совершать два вида ошибок – ложный доступ и ложный отказ доступа:

1) *ложный доступ* (ЛД) – принятие (заявленной) личности за истинную, хотя на самом деле это мошенник; принятие гипотезы H_0, хотя истинной является H_a. Частота появления ошибок ложного доступа называется *коэффициентом ложного доступа* (КЛД).

2) *ложный отказ доступа* (ЛОД) – принятие (заявленной) личности за неподлинную, хотя на самом деле она таковой не является; принятие гипотезы H_a, хотя истинной является H_0. Частота появления ошибок ложного отказа называется *коэффициентом ложного отказа доступа* (КЛОД).

Когда биометрия используется для обеспечения безопасности интеллектуальной или физической собственности, ошибки имеют точно определенные последствия. В случае ложного доступа не зарегистрированная в базе данных личность получает доступ к приложению, а в случае ложного отказа возникает проблема с удобством использования системы, когда легитимным пользователям отказывается в доступе к приложению или предписывается пройти дополнительную проверку.

4.2. Рабочие характеристики приемного устройства (РХПУ)

Предположим, что интегралы в выражениях (4.5) и (4.6) могут быть вычислены для любой пороговой величины T. Тогда функции КЛС(T) и КЛР(T) дают долю ошибок при некоторой величине T. Зависимость КЛС и КЛР изображается как двухмерная характеристическая кривая:

$$\text{РХПУ}(T) = \left(\text{КЛС}(T), \text{КЛР}(T)\right). \tag{4.10}$$

Примеры таких кривых можно найти на рис. 4.4. Коэффициент ложного сходства и коэффициент ложного различия как функции T выглядят как

$$\text{РХПУ}(T) = \left(\text{КЛС}(T), \text{КЛР}(T)\right) \to \begin{cases} (1,0) \text{ как } T \to -\infty, \\ (1,0) \text{ как } T \to \infty. \end{cases} \tag{4.11}$$

Поэтому, когда пороговая величина T низкая, КЛС будет высоким, а КЛР низким и, наоборот, когда T высокая, КЛР тоже высокий, а КЛС – низкий.

Мэтчер может работать, используя любую пороговую величину T, которая является точкой на кривой РХПУ. Это *рабочая точка* мэтчера, ее можно устано-

вить, выбрав любую из величин – T, КЛС или КЛР, а две другие тогда будут определяться автоматически. Рабочая точка мэтчера часто рассчитывается через T, так как ее можно задать в настройках, а КЛС и КЛР вычисляются уже на основе T. С другой стороны, когда формулируются требования биометрического приложения, или цель работы системы или когда происходит сравнение двух мэтчеров, рабочая точка устанавливается путем выбора КЛС или КЛР, так как пороговая величина – это число, которое имеет значение только для отдельного мэтчера.

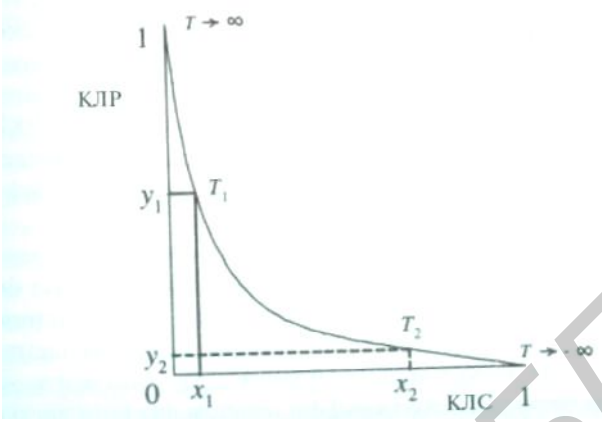


Рис. 4.4. Кривая РХПУ выражает соотношение между КЛС и КЛР

Большинство биометрических идентификаторов не могут гарантировать низкий коэффициент ошибок, достаточный для того, чтобы приложение было и безопасным (с низким КЛС), и удобным (с низким КЛР). Предположим, например, что имеется точная кривая РХПУ мэтчера. На рис. 4.5 показано, что возможен выбор одной из двух возможностей:

– зафиксировать вероятность ложного сходства на некоей (низкой) отметке КЛС = x_1, а вероятность ложного различия будет соответственно КЛР = y_1;

– установить вероятность ложного различия на некоей (низкой) отметке КЛР = y_2, тогда вероятность ложного сходства будет КЛС = x_2.

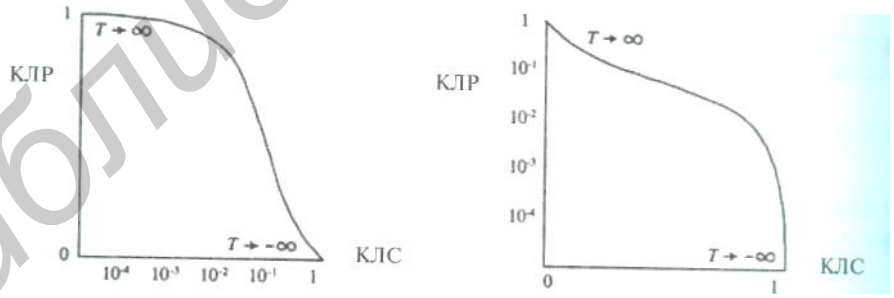


Рис. 4.5. Кривая РХПУ с одним из коэффициентов в логарифмической форме: слева – КЛС, справа – КЛР

Получив тестовые данные и подсчитанные коэффициенты ошибок мэтчера, нужно выбрать рабочую точку, которая определяется пороговой величиной T, чтобы достичь «оптимального» соотношения между вероятностями ложного сходства и ложного различия. Эту процедуру настройки мэтчера можно рассматривать как обучение на основе РХПУ.

4.3. Условия возникновения ошибок, специфичных для биометрии

В дополнение к основным ошибкам типа I и II, которые имеют многочисленные альтернативные названия, существует классификация специфичных для биометрии ошибок, разделяющая ошибки в зависимости от условий их возникновения (табл. 4.1).

1. *Невозможность получения* (НП). У некоторой части целевой аудитории может отсутствовать определенный биометрический параметр, эти люди не имеют возможности предоставить пригодный образец. Есть и более точное определение невозможности получения. Может случиться, что у человека нет того биометрического параметра, который необходимо зарегистрировать (например, человек потерял глаз), или необходимый параметр невозможно измерить (например, отпечатки пальцев укладчика кирпичей будут плохого качества, так как линии на пальцах могут стереться). Но технологии развиваются, и в будущем возможно возникновение устройств, которые смогут справиться с этими проблемами.

2. *Невозможность регистрации* (НР): бывают условия, при которых часть популяции невозможно зарегистрировать из-за технологических ограничений или проблем во время процедуры регистрации [10].

Таблица 4.1

Количественные переменные биометрических приложений

НП	Невозможность получения, ведущая к невозможности регистрации
НР	Невозможность регистрации, ведущая к невозможности использования
НИ	Невозможность использования – значимый фактор для стоимости любой биометрической системы

Эти два типа ошибок являются специфичными для биометрии, поэтому они присутствуют в любом биометрическом сценарии и возникают при использовании как систем верификации, так и систем идентификации. НП и НР являются внутренними свойствами биометрических систем и ограничивают возможности биометрии.

Другой тип ошибок, более характерных для систем добровольной аутентификации, называется *невозможность использования* (НИ). НИ включает в себя коэффициент НР плюс долю популяции пользователей, которая по каким-то причинам не регистрируется или регистрируется, но не может продолжать пользоваться биометрической системой.

Для добровольных биометрических аутентификационных приложений разница между коэффициентами НИ и НР возникает вследствие проблем, связанных с удобством (простотой использования) этих систем. Для недобровольных приложений эти коэффициенты равны (если это возможно). Существует некий нижний предел НП для каждого биометрического параметра, потому что некоторая часть популяции не может продемонстрировать данный параметр или не владеет им. Это относится к *универсальным* свойствам биометрических параметров [11].

Коэффициент НР может быть использован как системный параметр при оценке бюджета приложения. Уровень НР может регулироваться посредством контроля качества биометрических образцов, т. е. повышение качества образцов будет способствовать улучшению коэффициентов ошибок, потому что плохие образцы использоваться не будут.

Для конкретного приложения должна быть определена особая рабочая точка (КЛС, КЛР). Ее невозможно установить заранее. Даже когда установка уже работает, настоящий ложный доступ или ошибочный отказ в сценарии негативной идентификации может быть никогда не определен. Для добровольных приложений уровень НИ, конечно, может быть определен при работе установки. Технические причины высокого уровня НИ скорее всего будут связаны с проблемой удобства использования системы (хотя причины могут быть и нетехнического плана).

С другой стороны, для недобровольных приложений можно измерить уровень НР, что обычно и делается в лабораторных условиях (например, в условиях повышенного контроля и наблюдения). Тестирование систем биометрической аутентификации проводится на добровольцах, и поэтому не совсем ясно, как НИ (которую можно принять за принуждение) влияет на НР. Но с помощью базы данных тестовых образцов можно повышать уровень НР, улучшая и соответствующую кривую РХПУ.

Уровень НР может быть искусственно повышен для определенной установки, что улучшит качество зарегистрированной популяции за счет большей вероятности исключительных случаев (и их обработки) и неудобства. Системная переменная НР делает возможным компромисс между *ручной* и *автоматизированной* аутентификацией, которая, в свою очередь, связана с соотношением стоимости обслуживания системы и стоимости приобретения.

Как будет выглядеть кривая РХПУ биометрической установки, а также ее рабочая точка, полностью зависит от зарегистрированной популяции и желаемого уровня безопасности, который должен быть определен в соответствии с возможностями злоумышленников. Для положительных идентификационных систем ложный доступ может быть не зафиксирован никогда, так же, как и в системах отрицательной идентификации. В таких ситуациях можно применять статистические методы, которые учитывают только значения истинных пользователей, например, кривую суммарного сходства и массы ранговой вероятности (МРВ), которые используются для характеристики работы больших систем.

4.4. Отрицательная аутентификация

До сих пор нулевая гипотеза H_0 принималась за «положительное утверждение». Однако можно изменить гипотезы (4.2) так, чтобы получился сценарий отрицательной аутентификации. Рассматривая два биометрических образца, будем иметь две гипотезы:

Нулевая гипотеза	H_0 два образца не совпадают,	(4.12)
Альтернативная гипотеза	H_a два образца совпадают.	

Путем вычислении величины сходства $s(B, B')$ биометрический мэтчер определит, какая из гипотез истинная.

Такое биометрическое приложение проверяет истинность того, что представленный образец не принадлежит объекту d_n. Это, например, может быть преступник из «списка наблюдения» с реальным биометрическим параметром β и биометрическим образцом B. Проверка гипотез (4.12) определяет открыто или тайно (путем наблюдения), что биометрический параметр β' не является разыскиваемым параметром β. Гипотезы формулируются следующим образом:

$$H_0 : \beta' \neq \beta, \quad H_a : \beta' \equiv \beta. \tag{4.13}$$

Такие возможности часто относят только к биометрической идентификации. Тем не менее, когда говорится о тестировании гипотез (4.12) или (4.13), имеется в виду сопоставление 1:1 с ошибками, которые определяются отдельно. Проверка гипотез (4.13) выполняется с целью выявить наличие биометрического параметра P.

Существует два условия возникновения ошибок при отрицательном аутентификационном сценарии; во время принятия решения могут быть допущены также два типа ошибок (4.13):

1) ложно не замеченный β;

2) неверное соотнесение объекта β' с биометрическим параметром β.

Используя терминологию теории обнаружения, назовем эти ошибки ложным отрицанием и ложным признанием соответственно:

I. *Ложное отрицание* (ЛО) – решение о том, что объект является легитимным, хотя на самом деле он относится к «разыскиваемым» объектам с биометрическим параметром β (т. е. принимается гипотеза H_0, хотя истинной является H_a). Частота, с которой появляется данная ошибка, называется *коэффициентом ложного отрицания* (КЛО).

II. *Ложное признание* (ЛП) – решение, при котором объект принимается за разыскиваемого человека, имеющего параметр β, хотя на самом деле личность является легитимной, принимается гипотеза H_a, хотя истинна H_0 (этот случай также называется ложной тревогой). Частота, с которой появляется данная ошибка, называется *коэффициентом ложного признания* (КЛП).

Здесь в противоположность положительной аутентификации ошибочное соответствие или ложное совпадение называется ЛО (ложным отрицанием), в результате которого может возникнуть нарушение системы безопасности и нежелательная личность получает доступ к приложению. ЛП (ложное принятие) приводит только к неудобствам, так как легитимным объектам отказывается в доступе, вследствие чего требуется дальнейшая биометрическая или другая проверка для получения доступа.

На рис. 4.6 показано, что значения величин в среднем выше, когда вводимый биометрический параметр совпадает с нежелательным объектом d_n (выбрана низкая пороговая величина T, чтобы уменьшить коэффициент ложных отрицаний). Конеч-

но, это распределение выглядит так же, как распределение на рис. 4.2. Разница между отрицательным и положительным аутентификационным приложением в том, что ошибки несовпадения при отрицательной аутентификации ведут к ложному отрицанию, тогда как при положительной аутентификации ошибки несовпадения ведут к ложному отказу. Поэтому, если требуется высокий уровень безопасности, рабочая точка *T* для отрицательной аутентификации будет находиться ниже, чем для положительной аутентификации, чтобы уменьшить количество ложных отрицаний.

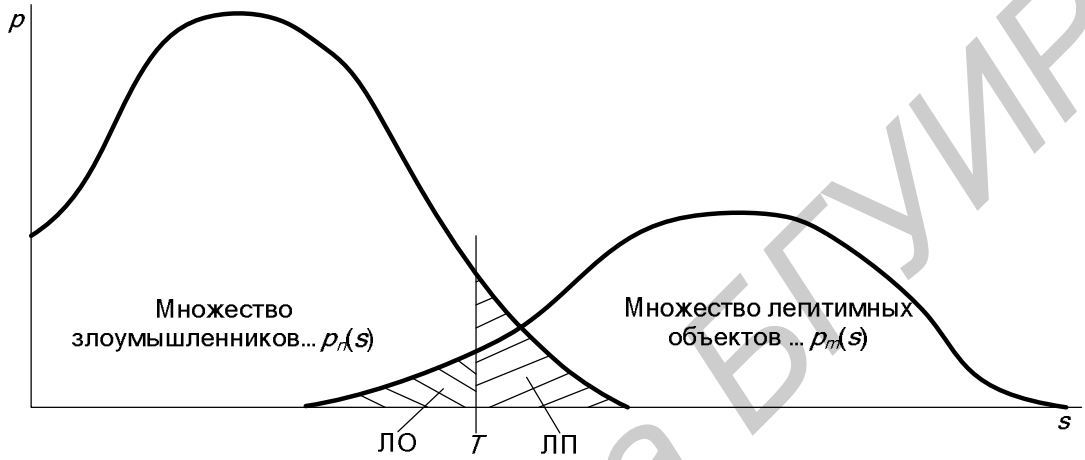


Рис. 4.6. Распределение $p_m(s)$ множества легитимных объектов и распределение $p_n(s)$ множества нежелательных объектов d_n

Термины «ложное признание» (ЛП) и «ложное отрицание» (ЛО) будут использоваться исключительно для «сортировочных» приложений (т. е. для отрицательной идентификации). Термины «ложный доступ» (ЛД) и «ложный отказ доступа» (ЛОД) будут использоваться для положительной аутентификации (верификации или идентификации).

4.5. Компромиссы

Два типа ошибок, которые способна допустить верификационная система, могут иметь разные последствия, затрагивающие разных людей. Ложный доступ означает вхождение в систему неавторизованной личности, что снижает безопасность системы. Ложный отказ доступа означает, что авторизованный пользователь не может попасть в систему, это не влияет на безопасность, но причиняет беспокойство пользователю и может иметь другие последствия, препятствуя человеку заниматься своими делами.

Поэтому компромисс между КЛД и КЛОД – это компромисс между безопасностью и удобством. Если взять эти крайности и установить КЛС = КЛД = 1, получится, что КЛОД = 0, т. е. система будет очень удобной, но абсолютно ненадежной, и доступ будет предоставляться всем желающим. И наоборот, установив КЛР = КЛОД = 1, получим КЛД = 0, тогда система будет абсолютно «опасной», но ни один человек не сможет получить доступ в нее.

4.5.1. Удобство против безопасности

В биометрической литературе возникла путаница относительно определения «удобства», так как удобство может быть характеристикой двух разных понятий:

1) *удобство биометрического параметра* – это некое расплывчатое понятие, касающееся удобства обращения пользователя с биометрическим параметром. Проблема в том, что биометрические параметры, наиболее удобные в этом смысле, т. е. те, которые можно получить без участия пользователя, например лицо или голос, являются слабыми по характеристикам, у них более высокие КЛС и КЛР по сравнению со сложными биометрическими параметрами, такими, как отпечатки пальцев или радужная оболочка;

2) *удобство аутентификации* – степень легкости, с которой правильно зарегистрированный пользователь проходит аутентификацию и получает доступ к приложению. Это понятие включает в себя готовность системы к работе протекание самого процесса аутентификации, обработку исключительных случаев и случаи ложного различия (т. е. ложный отказ доступа).

Из вышесказанного становится ясно, что высокий коэффициент ложного отказа доступа будет создавать неудобства для легитимных пользователей, следовательно, можно определить удобство аутентификационной системы так

$$\text{Удобство} = 1 - \text{КЛОД}. \tag{4.14}$$

Чем выше КЛОД, тем ниже удобство приложения, так как больше объектов идентифицируются неверно и, следовательно, им отказывается в доступе или в процедуре обработки исключительных случаев.

Также КЛД часто используется для измерения безопасности верификационных систем:

$$\text{Безопасность} = 1 - \text{КЛД}. \tag{4.15}$$

Следовательно, компромисс между безопасностью и удобством присутствует в любой биометрической системе, его можно показать при помощи РХПУ.

4.5.2. Стоимость против безопасности положительной аутентификации

Возможно, более важным является соотношение безопасности и стоимости биометрической аутентификационной системы и связанные с ним ошибки. Очевидно, что, при установлении КЛОД = 0 и КЛД = 1 получаем очень дешевую, но абсолютно ненадежную систему и наоборот, при КЛД = 0 и КЛОД = 1 биометрическая система не примет ни одного пользователя и придется прибегнуть к дорогостоящей ручной обработке.

Поэтому КЛОД можно использовать для измерения стоимости аутентификационной системы: *Стоимость* = КЛОД.

Чем выше КЛОД, тем дороже приложение, так как большое количество объектов будет неверно идентифицировано и, следовательно, им будет отказано в доступе или в процедуре обработки исключительных случаев. Как и в выражении (4.15), КЛД выступает в качестве меры безопасности.

Поэтому в любой биометрической аутентификационной системе присутствует компромисс между безопасностью и стоимостью, и, применяя числовое определение, этот компромисс можно выразить в РХПУ.

Это означает, что использование одного и того же биометрического мэтчера в качестве и безопасного, и удобного приложения не обязательно будет самым лучшим вариантом. Это можно увидеть, например, на кривых РХПУ (рис. 4.7). Там кривая РХПУ мэтчера *а* соответствует более безопасному мэтчеру, так как для низкого КЛС (КЛД), близкого к оси *y*, связанный с ним КЛР (КЛОД) ниже, чем параметры мэтчера *б.* Если удобство важно, мэтчер *б* может быть настроен для работы в области низкого КЛР (кривая РХПУ приближается к оси *x*) в области повышенного уровня удобства. В этой области низкого КЛР мэтчер *б* имеет более низкий КЛС.

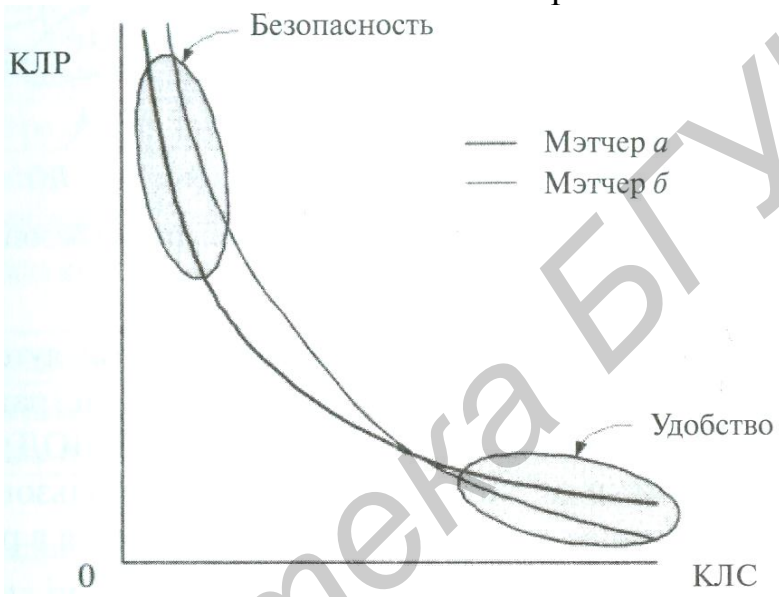


Рис. 4.7. РХПУ мэтчеров *а* и *б*

Обычно при разработке системы ее рабочая точка выбирается путем установки КЛС (для безопасности) или КЛР (для удобства), и поэтому только часть кривой РХПУ основного мэтчера является важной. Некоторые биометрические системы создаются для работы только на одной рабочей точке кривой, другие системы могут быть разработаны для других точек.

Более того, рабочая точка не обязательно должна быть статичной. Например, процедуры отбора, как в аэропортах, могут быть мультимодальными, т. е. демографические характеристики, текст, звук, видео – все это может быть задействовано. В зависимости от демографических особенностей биометрическая аутентификация может работать на разных рабочих точках кривой РХПУ. Это пример динамического аутентификационного протокола, где ошибки сопоставления в приложении каким-либо образом оптимизированы с помощью выбора разных КЛС и КЛР для разных множеств *s*.

Компромисс между КЛС и КЛР – это компромисс между безопасностью и удобством (см. рис. 4.7). Мэтчер *а* выигрывает по удобству, мэтчер *б* – по безопасности. Поэтому при разработке биометрической аутентификационной системы в первую очередь нужно задать вопрос: «Что важнее для данного приложения –

безопасность или удобство?» Это может случиться с приложениями добровольной аутентификации, для которых удобство пользования является решающим фактором успеха. Как показывает рис. 4.8, когда более важным фактором является безопасность, нужно установить КЛС = x_1, который подразумевает некий довольно высокий КЛР ≤ y_1. Следовательно, если от системы прежде всего требуется удобство использования, нужно установить низкий КЛР = y_2, а соответствующий (низкий) уровень безопасности будет тогда выражен как КЛС ≤ x_2.

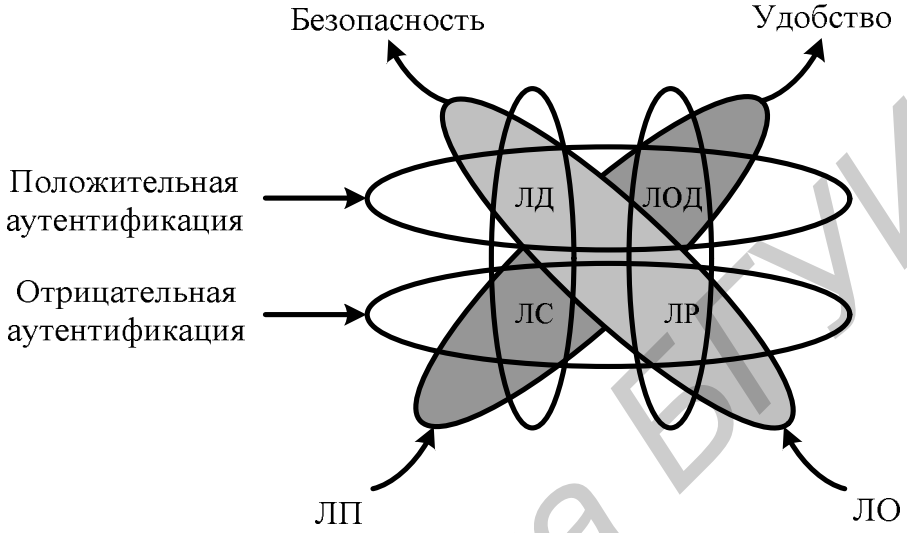


Рис. 4.8. Влияние разных ошибок на снижение уровня безопасности или удобства

Важно запомнить, что КЛР (КЛОД) биометрической аутентификационной системы часто задается без учета НР (невозможности регистрации) и НП (невозможности получения). Использование выражения (1 – КЛОД) как меры «удобства» тогда ведет к заблуждениям, потому что неудобство пользователя, который не может применять биометрическую систему, не принимается в расчет.

4.5.3. Стоимость отрицательной аутентификации

Для сортировочных систем (или отрицательной аутентификации)

$$\text{Безопасность} = 1 - \text{КЛО},$$

т. е. чем ниже шансы нежелательного объекта d_n проникнуть в систему, тем выше безопасность системы. Удобство такой отрицательной аутентификационной системы можно определить как

$$\text{Стоимость} = \text{КЛП},$$

т. е. легитимный объект d был ошибочно признан подозрительным и ему причинены неудобства, так как он скорее всего подвергнется дополнительной проверке. Для отрицательного идентификационного сценария, когда КЛО и КЛП слишком высоки, аутентификационные системы становятся неудобными для всех пользователей, так как точки контроля достичь невозможно.

В этой процедуре объекты не «принимаются» приложением, а наоборот, отсеиваются те из них, которые не являются нежелательным объектом d_n. Мы называем сходство с d_n «позитивным», а отличие от него – «негативным». Поэтому

ошибки такой системы – это ложное признание, т. е. признание сходства входящего объекта с d_n, и ложное отрицание – ошибочное признание объекта как отличного от d_n. Эти ошибки показаны в табл. 4.2, а все компромиссы – на рис. 4.8.

Таблица 4.2

Пары количественных ошибок для биометрических мэтчеров типа 1:1, аутентификационных приложений и сортировочных систем

ЛС	Ошибочное сходство двух биометрических параметров
ЛР	Ошибочное различие двух биометрических параметров
ЛД	Ложный доступ, предоставляемый злоумышленнику, влекущий за собой проблемы с безопасностью
ЛОД	Ложный отказ доступа авторизованному пользователю в **M**, причиняющий неудобство
ЛО	Ложное отрицание сходства в **N**, нарушающее безопасность системы
ЛП	Ложное признание сходства в процессе сортировки базы данных **N**, причиняющее неудобство пользователю; также называется ложной тревогой

В табл. 4.3 приведен список двух аутентификационных сценариев и связанных с ними ошибок и их последствий для приложения. Для положительной аутентификации ЛД, причиной которого является ЛС, становится проблемой безопасности, а ЛОД, вызванный ЛР, снижает удобство использования системы. Для негативной аутентификации ЛО, вызванный ЛР, станет проблемой безопасности, а ЛП, вызванный ЛС, будет проблемой удобства. Когда объекту d отказывается в доступе по причине ложного отказа или ошибочного сходства с нежелательным объектом d_n, это причиняет неудобство и объекту, и персоналу, обслуживающему биометрические системы.

Таблица 4.3

Параметры ошибок для двух видов приложений

Положительная аутентификация	Отрицательная аутентификация
ЛД = ЛС $\Rightarrow$ проблема безопасности	ЛО = ЛР $\Rightarrow$ проблема безопасности
ЛОД = ЛР $\Rightarrow$ проблема удобства	ЛП = ЛС $\Rightarrow$ проблема удобства

Заметим, что причины ЛД и ЛП одни и те же – появление ложного сходства, последствия которого сильно различаются. В случае ЛД возникают проблемы с безопасностью системы, а при ЛП – с удобством ее использования. Причиной ЛО и ЛОД является ложное различие, но ЛО станет проблемой безопасности, в то время как ЛОД – проблемой удобства. Определение ошибок зависит от приложения и, следовательно, от определения гипотез H_0 и H_a.

5. АТАКИ НА БИОМЕТРИЧЕСКИЕ СИСТЕМЫ

Биометрические системы помогают справиться с проблемами, характерными для существующих методов аутентификации. Биометрические параметры могут улучшить удобство или безопасность системы, а в идеальном случае – и то и другое. Тем не менее слабые места есть в любой биометрической системе независимо от желания разработчиков. Такие недостатки будут обнаруживаться в процессе работы системы, когда система будет подвергаться атакам, которые направлены в эти слабые места.

В отличие от систем с паролями, которые подвергаются грубым атакам путем подбора пароля, биометрические системы удачно атаковать гораздо труднее. Для защиты биометрических систем полезно использовать стандартные техники кодирования, однако в них существуют некоторые специфические точки атак.

В удаленных автоматизированных приложениях, например в электронной коммерции, злоумышленники могут иметь достаточно времени, чтобы совершить ряд попыток на безопасном расстоянии от сервера до того, как они будут замечены, либо они могут атаковать клиента физически. На первый взгляд, биометрические установки, находящиеся под наблюдением, как, например, в аэропорту, не могут подвергаться атакам грубой силы. Но они могут подвергаться атакам воспроизведения. Разработаем общую модель распознавания образов, которая позволит изучать слабые места в системе безопасности. Понимание этой проблемы требуется при разработке биометрической системы, кроме того, нужно не забывать о взаимосвязи между удобством и безопасностью.

Биометрические аутентификационные системы выглядят как система, изображенная на рис. 5.1.

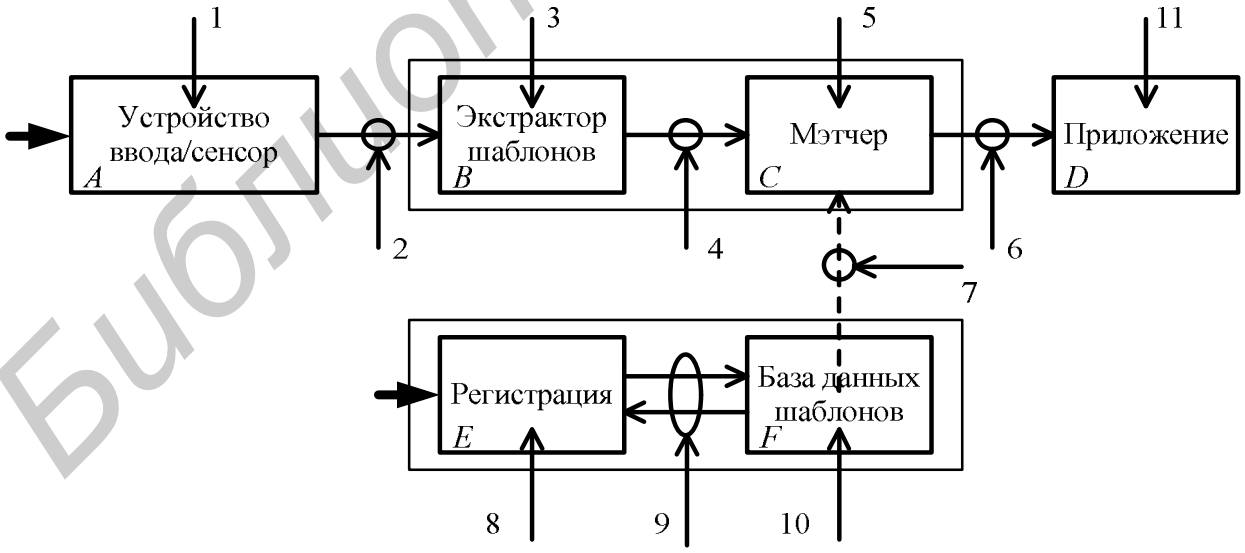


Рис. 5.1. Составляющие аутентификационной и регистрационной систем и точки атак

Устройство ввода измеряет биометрический образец человека. Этот образец преобразуется в машинную репрезентацию (которая сама может быть образцом)

при помощи экстрактора свойств. Эта машинная репрезентация сопоставляется с другой репрезентацией, предварительно сохраненной во время регистрации.

5.1. Модель распознавания образов

Биометрическая система может быть представлена как система распознавания образов [12, 13]. Фазы работы системы распознавания образов показаны на рис. 5.1 и обозначены как *A*, *B*, *C*, *D*; регистрация представлена двумя этапами – *E* и *F*. Описание таких автоматизированных систем можно найти в [1, 14].

Любую биометрическую систему можно описать как четырехступенчатую (см. рис. 5.1). Рассмотрим эти ступени более детально:

A. На первом этапе происходит получение образца. Этот процесс может быть простым, как запись речи по телефону, или таким же трудоемким, как получение образцов крови для анализа ДНК.

Сам процесс и его логистика являются наиболее важными факторами, оказывающими влияние на удобство использования определенной биометрической системы. В то же время, контроль получения сигнала оказывает большое влияние на качество образца и, следовательно, на точность системы. Часто трудность заключается в том, чтобы контролировать получение сигнала, не причиняя больших неудобств пользователю.

B. Вторая ступень – это обработка биометрического образца для получения цифровой машинной репрезентации, которую затем можно будет сопоставлять с другими репрезентациями. Этот процесс может сводиться только к сохранению биометрического образца или же может быть таким сложным, как вычисление структуры совокупности индексов [15].

Проблема конструирования репрезентации является сложной задачей и требует дальнейшего исследования.

C. На этой ступени происходит вычисление величины сходства между двумя или более репрезентациями: между одной репрезентацией вводимого образца и одной или более сохраненными (зарегистрированными) репрезентациями (из базы данных *F*). Есть несколько факторов, которые определяют, насколько точно будет вычислена эта величина для определенного вводимого образца. К ним относятся качество образца, точность, с которой может быть получена репрезентация из биометрического образца, и эффективность работы мэтчера при сопоставлении двух репрезентаций. Еще один фактор – это качество обучающих данных, которые используются для оптимизации процесса сопоставления.

На этой стадии также происходит принятие решения о сходстве или различии. Это решение лучше принимать, предварительно определив, какое приложение будет использоваться.

D. Это приложение, которое защищено биометрической аутентификационной системой. Это может быть система контроля иммиграции, банкомат, учетная запись компьютера и т. д.

На этой стадии желаемая достоверность решения выбирается как рабочая точка, т. е. как приемлемый уровень коэффициента ложного доступа (КЛД), от ко-

торого зависит и коэффициент ложного отказа доступа (КЛОД). Это компромисс между безопасностью и удобством, основанный на статической или динамической стратегии поведения.

Регистрация и организация базы данных биометрических образцов являются столь же важными аспектами приложения, как повседневная работа аутентификационной системы. Как показано на рис. 5.1, хотя регистрация *E* – более сложный процесс, чем в парольных системах, базу данных биометрических образцов *F* можно считать аналогом базы с сохраненными паролями.

E. Процедура регистрации и логистика – это очень важные аспекты биометрической системы. В отличие от системы паролей в ней не так просто сделать перерегистрацию личности с новым образцом, поэтому регистрация в биометрической системе требует особого внимания.

F. База данных биометрических образцов *F* бывает либо распределенной (например, запись информации на личных смарт-картах [16]), либо централизованной. Выбор архитектуры биометрической системы также зависит от множества факторов.

На рис. 5.1 показаны 11 основных точек атак на аутентификационные системы. Мы разделили эти точки атак на несколько классов.

5.2. Атаки на биометрические идентификаторы

Многие атаки (угрозы) на биометрические приложения основаны на том, что биометрические данные, которые обрабатывает система, на самом деле не принадлежат атакующему, т. е. он либо подражает другой личности, либо изменяет данные, сохраненные в биометрической системе.

Угроза №1 возникает тогда, когда злоумышленник предоставляет биометрические данные сенсору *A*. Атака может быть принудительной, когда системе незаконно представляется настоящий биометрический параметр. Бывают имитационные атаки, когда злоумышленник изменяет свои биометрические параметры (особенно голос или лицо) для того, чтобы выглядеть как подлинный пользователь. Существуют также атаки воспроизведения, когда сенсору предоставляются записанные биометрические параметры подлинного пользователя.

Принудительные атаки – это предоставление биометрических данных законного пользователя на незаконных основаниях. Наиболее распространенный случай – принуждение злоумышленником подлинного пользователя пройти идентификацию в системе. Средства аутентификации получаются насильственным путем от истинного пользователя с целью получения доступа в систему со всеми сопутствующими привилегиями, например, пользователь банкомата может быть вынужден отдать свою пластиковую карту и сообщить ПИН под дулом пистолета. Желательно выявлять такие атаки, не подвергая опасности жизнь пользователя. Выявление можно производить при помощи анализа уровня стресса пользователя, или же система может иметь собственную службу контроля безопасности. Такие атаки можно предотвратить при помощи аудио- и видеозаписи всех транзакций.

В обществе могут возникать опасения, что мошенники могут нанести физический вред пользователям, например, отрезать палец. Пока это возможно, разработчики биометрических систем ищут способы противостоять таким атакам путем определения «живости» параметра – измерения движения радужной оболочки, электрической активности, температуры и пульса в пальце [17]; наблюдения за изменением выражения лица или методом «вызова-ответа» в системах распознавания сетчатки глаза. С ростом возможностей вычислительной техники совершенствуются технологии определения подделок, однако и методы преступников тоже становятся более изощренными.

Если человек изменяет свою внешность, чтобы выглядеть как авторизованный пользователь, это называется имитационной атакой (сходство может быть не признано истинным при сценарии сортировки). Лицо и голос являются основными объектами имитации, так как многие люди умеют очень хорошо подражать чужим голосам и изменять свою внешность, что может заставить систему дать им (ложный) доступ. Но есть люди, чьи параметры невозможно хорошо имитировать. При сценарии сортировки же достаточно изменить внешность с помощью грима или пластической операции, чтобы система не опознала человека. В этом случае атакующий становится причиной ошибки ложного отрицания. Другие биометрические параметры имитировать гораздо сложнее, хотя несколько групп исследователей [18] сообщили об удачных атаках на систему, распознающую отпечатки пальцев, с помощью резиновых имитаций.

Комбинация разных биометрических параметров также снижает частоту атак имитации, так как возникает необходимость имитировать большее количество характерных свойств легитимного пользователя. Особенно это относится к одновременному распознаванию лица, речи и движений губ: получить (или синхронизировать) все три параметра в таком виде, чтобы их можно было воспроизвести, будет гораздо сложнее, чем если бы они использовались по одному, особенно если система проверяет взаимодействие (и синхронизацию) между ними.

Если не принимать в расчет стоимость, то все биометрические параметры могут быть объектами имитации. Легкость подражания варьируется от очень простой имитации до практически невозможной и, конечно, прежде всего зависит от работы самой системы и от коэффициентов ошибок, свойственных данному биометрическому параметру.

Атаки воспроизведения – это предоставление предварительно записанной биометрической информации. Чаще всего такие атаки представляют собой запись голоса человека, говорящего фиксированный текст-пароль. Такие простые атаки можно предотвратить при помощи текстов-подсказок. Для того чтобы обмануть старые системы распознавания лица, было достаточно предоставить им фотографию пользователя. В современных системах используется трехмерное изображение, и они чувствительны к изменению выражения лица, что требует более изощренных способов имитации, например, держать перед камерой жидкокристаллический экран.

Включение биометрических параметров в аутентификационный протокол может случайно создать новые уязвимые места в системе безопасности. Это как раз

те точки атак, которые будут рассмотрены ниже. Также мы увидим, что биометрические системы имеют такие же точки атак, как и у парольных систем.

5.3. Фронтальные атаки

Внешняя часть системы – это то место, где происходит большая часть действий во время аутентификации. Эта часть системы отвечает за преобразование считываемого биометрического сигнала в определенный вид инвариантной репрезентации и сопоставление ее с соответствующим шаблоном. Этот процесс предоставляет несколько возможностей для атак.

Угроза №2 направлена на канал связи между сенсором и биометрической системой. Здесь снова могут иметь место атаки воспроизведения – предоставление предварительно сохраненных биометрических сигналов – или электронная имитация. Можно обмануть сенсор, воспроизводя видеоизображение отпечатка пальца или лица или подавая аудиосигнал на выход микрофона. Если есть физическая возможность добраться до этой точки, то атаковать ее проще, чем атаковать сенсор, – сымитированный сигнал может быть получен и воспроизведен в этой точке. Однако современные технологии цифрового кодирования и временные отметки способны защитить систему от такого рода атак. Более того, система может определить лучшую степень сходства по сравнению со старыми данными. Электронные имитации на этой стадии могут представлять собой внедрение изображения отпечатка пальца, которое было искусственно создано на основе информации о расположении деталей, записанной на смарт-карте.

Угроза №3 – это «троянский конь», направленный в экстрактор свойств *B,* который в результате атаки будет генерировать заранее определенный набор свойств в определенное время и в особых условиях, т. е. после того как свойства были выделены из входящего сигнала, их заменяют другим синтезированным набором свойств (при условии, что репрезентация известна).

Точка атаки №4 – это канал связи между экстрактором свойств и мэтчером. В случае с отпечатками пальцев, если детали передаются на удаленный мэтчер (например, при использовании смарт-карт [16] для сохранения шаблонов), угроза атаки в этой точке становится реальной.

Точка атаки №5 – это снова «троянский конь»: мэтчер атакуется для генерации искусственно завышенной или заниженной величины совпадения, т. е. здесь происходит манипуляция решением мэтчера. Например, злоумышленник может заменить биометрические данные на компьютере данными, которые всегда будут давать истинное сходство (для определенного пользователя).

5.4. Обман

На уязвимое место аутентификационной системы, которое нередко остается незамеченным, направлена следующая атака.

Угроза №6 – подмена исходящей информации из модуля мэтчера *C* (точка №6, см. рис. 5.1). Решением модуля сопоставления может быть вывод о сходстве

или различии или только вероятность сходства, когда окончательное решение принимается приложением. Точка атаки №6 будет одной и той же в обоих случаях.

Некоторые проблемы, с которыми сталкиваются все идентификационные системы (основанные на собственности, знаниях или биометрии), очень похожи. Подделки в аутентификационной системе могут принимать разные формы. Некоторые из них – это просто лазейки в системе – возможности нелегитимного доступа, которые не заметили разработчики установки. Другой вариант – это использование намеренно объединенных механизмов, чтобы превзойти все методы аутентификации, использующиеся в системе, и, таким образом, не получить отказ доступа при любой стратегии, внедренной в систему (в интрасистему). Виды мошенничества можно классифицировать следующим образом:

– *тайное соглашение* (в любом приложении определенный оператор системы имеет статус суперпользователя, который позволяет ему обойти аутентификационный компонент обработки и отменить решение, принятое системой. Эта возможность представлена в системе для обработки исключительных случаев, например для аутентификации людей, у которых нет пальцев);

– *скрытое получение образцов* (это возможно, если средства идентификации могут быть получены без участия законного пользователя и использованы не по назначению. Существует множество примеров скрытого получения персонального идентификационного номера (ПИНа) в банкоматах. Это можно назвать атакой имитации, но в этом случае используются только параметрические данные, а биометрические параметры не имитируются. Однако непонятно, как можно украсть чужой шаблон отпечатков пальцев, просто глядя на них, и тем более предоставить его аутентификационной системе. Более вероятно, что злоумышленник сделает дубликат собственности или узнает пароль, например, подделает смарт-карту или узнает ПИН, которые должны использоваться наряду с биометрическим параметром (который, в свою очередь, тоже был подделан);

– *отказ* (может случиться, что истинный пользователь, проходя идентификацию при помощи легитимных средств, например смарт-карты, чтобы получить доступ к ресурсам, может получить отказ в доступе, т. е. налицо случай ложного отказа доступа из-за того, что биометрические аутентификационные шаблоны были скомпрометированы. Так как данный случай не является настоящим обманом – к защищаемым ресурсам не был предоставлен неавторизованный доступ, – это нарушает только функционирование системы, не разрушая ни один из ее компонентов).

Многие из этих проблем не могут быть решены полностью. В данное время попытки уменьшить количество случаев мошенничества при аутентификации ориентированы на процесс и на конкретную проблему. Необходимо сосредоточить усилия на создании последовательных и высокотехнологичных решений защиты. Особенно это относится к биометрическим аутентификационным системам, где процесс биометрических измерений и окружающая обстановка могут достаточно эффективно отпугивать злоумышленников. Использование разных биометрических параметров дает надежду на решение многих из перечисленных выше проблем.

5.5. Внутренние атаки

Базы данных зарегистрированных пользователей могут быть локальными или удаленными, т. е. распределенными на нескольких серверах. Незаконные модификации одной или более машинных репрезентаций в базе данных могут привести к авторизации злоумышленника или по крайней мере к отказу в доступе человеку, связанному с искаженным (или вставленным/удаленным) шаблоном (при условии, что репрезентация является известной).

Угроза №7 – это еще один вид атак, направленный на канал связи между центральной или распределенной базой данных и аутентификационной системой. Атака направлена на канал, по которому из базы данных *F* биометрические репрезентации посылаются мэтчеру. Атака имеет целью изменить репрезентацию перед тем, как она попадет в мэтчер.

Процессы в блоках *E* и *F* представляют собой очень важную для биометрической аутентификационной системы функцию – регистрацию подходящих объектов или список контроля доступа. «Чистота» базы данных *F* крайне важна, так как сама аутентификационная система настолько безопасна, насколько безопасна база данных. Здесь можно выделить три точки атак:

Точка атаки №8 – это центр регистрации или приложение (элемент *E* на рис. 5.1). Процессы регистрации и аутентификации схожи в том смысле, что они оба исполняют аутентификационный протокол, и поэтому регистрация подвержена атакам в точках 1–6.

Эта точка атаки – канал (как и точка атаки №10). Контролирование этого канала позволяет атакующему аннулировать (биометрическую) репрезентацию, которая была отправлена из биометрической базы данных *F* в *C*.

Десятая угроза – это атака на саму базу данных *F*. База данных зарегистрированных биометрических репрезентаций доступна локально или удаленно и может быть распределена на нескольких серверах. В этой точке возможна незаконная модификация одной или нескольких репрезентаций. Это может привести к авторизации злоумышленника, к отказу в доступе человеку, связанному с искаженным шаблоном (опять же при условии, что формат репрезентации известен), или к удалению известного «разыскиваемого» лица из списка сортировки.

В этой точке также существует возможность атак на конфиденциальную информацию – на секретные данные биометрической аутентификационной системы, т. е. на список контроля доступа или на базу данных членов. Эти атаки нацелены не на приложение, а на базу данных биометрической аутентификационной системы. Особенности защиты конфиденциальности биометрической установки предоставляют возможность для таких атак.

В случае сговора между злоумышленником и супервизором регистрационного центра могут быть легко зарегистрированы новые созданные или украденные личности, что может привести к серьезным последствиям. Эта угроза также актуальна и для систем, где аутентификация происходит вручную. Эта угроза напрямую зависит от того, насколько реальна имитация того или иного биометрического параметра, т. е. от свойственного ему уровня ЛД. Процесс регистрации должен быть

более безопасным, чем процесс аутентификации, он должен проводиться под наблюдением компетентного и доверенного лица.

Также нужно помнить и о защите приложения или системы.

Как отмечено в [19], приложение *D* также является точкой атак. Это означает, что для биометрической аутентификационной системы должны применяться те же методы защиты, что и для традиционных аутентификационных систем.

Самой большой угрозой для биометрической аутентификационной системы является представление, физическое или в электронном виде, подделанного или предварительно полученного биометрического параметра. Это угроза, на которую необходимо обратить внимание, особенно в процессе регистрации, т. е. необходимо определить, насколько легко может быть зарегистрирована новая созданная личность. В частности, особое внимание нужно уделить угрозам №1 и 2, которые представляют собой воздействие на устройство ввода или на канал связи. Электронная имитация становится более вероятной, однако ее можно предотвратить с помощью системы «вызова-ответа», а также посредством скрытия данных.

Тот факт, что биометрические шаблоны системы хранятся либо в централизованной, либо в распределенной на смарт-картах базе данных, не обязательно оказывает влияние на безопасность биометрической системы, так как эту часть системы можно защитить, используя традиционные технологии. Хотя смарт-карты обеспечивают дополнительную секретность информации благодаря распределению базы данных *F*, злоумышленник в этом случае может получить достаточно времени для подделки смарт-карты. Часто биометрические данные хранятся одновременно на смарт-картах и на центральном сервере (например, для перевыпуска карт в случае потери), что открывает новые возможности для атак.

Проблема безопасности биометрических данных должна быть решена путем разработки специальных технологий «кодирования личностей». Закодированные таким способом шаблоны могут сопоставляться в зашифрованном домене, тогда не будет возможности проследить подлинную личность. Определение подделок среди биометрических параметров тоже является темой для серьезного исследования, которая пока еще недостаточно изучена.

5.6. Другие атаки

Парольные системы могут подвергаться атакам грубой силы. В них количество знаков в пароле пропорционально его силе, которая выражает количество попыток, в среднем необходимых, чтобы взломать аутентификационную систему. Так как люди обычно выбирают простые пароли, атака методом подбора обычно проще, чем предполагает теоретическая сила пароля. Для биометрических параметров существует понятие, «эквивалентное» понятию силы пароля, которое называется коэффициентом внутренних ошибок. Атаки с расчетом на коэффициент внутренних ошибок могут быть направлены на точки №2 или 4 (см. рис. 5.1), но, как правило, в аутентификационных системах количество попыток, даваемых пользователю для предоставления биометрического параметра, бывает ограничено.

Ниже приведено еще несколько типов атак [20].

Восхождение на холм – это ситуация, когда биометрические данные предоставляются снова и снова с небольшими изменениями, эти изменения подготавливаются заранее, что улучшает результат. Более сложная версия – это попытка моделирования возвратных величин для получения более быстрых результатов. В конце концов величина сходства достигает пороговой. Этот метод подходит для взлома электронных систем, когда злоумышленник не имеет сведений о биометрических данных легитимного пользователя. Такие атаки можно предотвратить при помощи запрета повторных попыток. Также есть и другие способы: система может выдавать на вопрос о сходстве только ответ «да/нет», или же можно квантовать величины сходства или добавлять в них небольшое количество шума.

Заглушающая атака похожа на атаку с применением грубой силы, направленной на слабые места алгоритмов, чтобы получить сходство для неверных данных. Например, при атаке на систему распознавания отпечатков пальцев злоумышленник может представить отпечаток с сотнями деталей в надежде, что по крайней мере пороговое число N из них будет признано схожим с сохраненным шаблоном (при условии, что мэтчер не признает негодными такие репрезентации).

Комбинированная атака – это атака, когда неавторизованный пользователь пытается получить доступ в защищенную зону путем одновременного входа в систему с законным пользователем. Эта атака может быть связана с физической угрозой, или же это может быть простое «следование по пятам». Данный вид атак определенным образом связан с насилием, как атаки в точке №1 (см. рис. 5.1).

Незаконная регистрация – опасность, актуальная для всех систем безопасности, – это разрешение регистрации (или предоставление прав доступа) злоумышленнику. Если злоумышленник один раз предоставит удостоверяющие данные, позволяющие ему зарегистрироваться, система безопасности не будет впоследствии препятствовать его доступу.

5.7. Комбинация смарт-карт и биометрических параметров

Смарт-карты могут играть важную роль в аутентификационных системах, основанных на биометрических параметрах. Пока биометрические параметры являются самыми надежными, но не пользующимися доверием средствами аутентификации, смарт-карты могут хранить биометрические данные и другие сопутствующие сведения, осуществлять свои функции и безопасно взаимодействовать со считывающими устройствами. В аутентификационных системах, которые должны гарантировать высокий уровень безопасности, можно использовать одновременно биометрические параметры и смарт-карты, объединяя таким образом преимущества обеих технологий.

Обычная смарт-карта состоит из процессора и памяти, как показано на рис. 5.2. Смарт-карты бывают двух основных типов – контактные и бесконтактные. Контактные карты должны иметь физический контакт со считывающим устройством. Для считывания информации с бесконтактной смарт-карты достаточно провести ее рядом со считывающим устройством. Гибридные карты могут иметь оба интерфейса. На протяжении последних лет смарт-карты эволюционировали от про-

стых карт памяти до более сложных систем с 32-битным процессором и криптопроцессором, обеспечивающим шифрование данных и генерацию цифровых подписей.

Эти и другие преимущества делают смарт-карту хорошим средством обеспечения защиты информации. Безопасность данных в памяти смарт-карты обеспечивается благодаря комбинации программных и аппаратных способов защиты. С помощью встроенной электроники смарт-карта защищает данные от нежелательных изменений во время считывания или записи информации. Химические и электронные повреждения памяти определяются аппаратными средствами путем проверки целостности памяти и программными средствами – при помощи вычисления контрольных сумм. Защита информации на карте от незаконного считывания также обеспечивается аппаратными и программными механизмами. Смарт-карты с криптопроцессорами являются надежными устройствами для хранения информации.

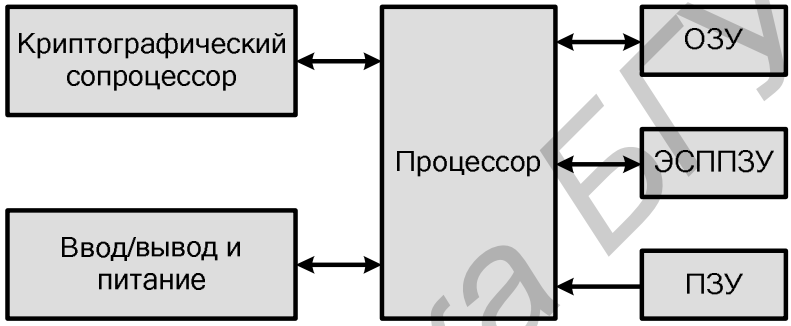


Рис. 5.2. Системная архитектура смарт-карты

Рассмотрим комбинацию биометрических параметров и смарт-карт в двухфакторной аутентификационной системе. Такие системы всегда более безопасны, чем однофакторные. Если пользователь теряет карту, доступ запрещается до того момента, пока он не получит новую карту. Потерянная карта, даже если она попадает в чужие руки, не представляет угрозы для системы, так как для того чтобы ее использовать, необходимо предоставить и биометрический параметр.

Во время регистрации объекта биометрический шаблон будет сохранен на смарт-карте вместе с другой информацией. Для аутентификации пользователя системе должны быть предоставлены смарт-карта и реальный биометрический параметр. Тогда она генерирует шаблон для сопоставления из предоставленного ей биометрического параметра, расшифровывает шаблон, хранящийся на смарт-карте, и проверяет сходство между ними. Если все данные находятся в одном месте, это заметно снижает количество взаимодействий с сервером базы данных.

Хранение биометрической информации на смарт-картах имеет дополнительные преимущества в области конфиденциальности. Как было отмечено выше, при централизованном хранении биометрических образцов существует вероятность злоупотребления ими с целью, неизвестной владельцу биометрического параметра (точка атаки №10, см. рис. 5.1). Большие базы биометрических данных могут быть проданы или отданы неизвестным лицам, которые будут использовать их в собственных целях. Смарт-карты дают возможность распределить данные, тогда контролировать их будут сами владельцы карт. Более того, не существует централизован-

ных баз данных, которые, если скомпрометирован хотя бы один пользователь, могут признать недействительной всю базу.

Если есть возможность безопасного хранения информации, можно записать много другой информации, которая будет оказывать поддержку биометрическому приложению. Например, в аутентификационной системе, распознающей отпечатки пальцев, на смарт-карте могут быть сохранены свойства отпечатков пальцев вместе с пороговой величиной, которая использовалась во время сопоставления. То же самое и в системе распознавания лица: можно сохранить шаблон лица и ожидаемые изменения его параметров. Для систем распознавания голоса этот метод предоставляет дополнительное преимущество. Кроме репрезентации записи голоса, можно сохранить и общую голосовую модель. Эти параметры могут быть извлечены устройством обслуживания и использоваться для голосовых команд.

Смарт-карты о которых говорилось выше, не предполагают наличия большого количества памяти или большой производительности. Самые современные смарт-карты могут иметь до 64 Кбайт памяти ПЗУ и тактовую частоту 32 МГц. Но их оперативная память ограничивается 1–2 Кбайтами, что препятствует запуску таких приложений, как обработка входящих биометрических сигналов. Тем не менее уже сейчас возможно разработать мэтчеры, которые могли бы работать на смарт-картах. Приложения, работающие на смарт-картах, фактически полностью защищены от атак. Когда мэтчер работает на смарт-карте, зарегистрированный шаблон не передается за пределы карты, и поэтому безопасность операции возрастает. Для считывания решения, вычисленного мэтчером на смарт-карте, можно использовать безопасный протокол.

Несколько новых приложений применяют комбинацию смарт-карт и биометрических параметров, например, карту общего доступа Министерства обороны США и визы, защищенные от искажений. Безопасность смарт-карт и низкое энергопотребление даже при 128-битном аппаратном шифровании делают их привлекательными для использования во многих аутентификационных приложениях.

5.8. «Вызов-ответ»

Одной из разновидностей угроз, существующих для биометрических аутентификационных систем, являются атаки воспроизведения в точках №2 и 4 (см. рис. 5.1). Возможный метод защиты от этих атак – использование протокола «вызов-ответ»: для авторизации пользователь должен правильно ответить на вызов системы. Система может запросить секретные данные, что защищает ее от атак воспроизведения.

Например, верификация голоса с помощью свободного текста [21] поможет избежать простых атак воспроизведения. Преимущества обучаемых синтезированных (с аудио- и видеоматериалами [22, 23]) алгоритмов в то же время предоставляют возможность для атак даже на такие сложные системы. Механизм «вызов-ответ» может применяться и для других биометрических параметров. Системы интерактивной аутентификации отпечатков пальцев могут использовать потоковое видеоизображение отпечатков [24]. Конечно, даже такие системы могут подверг-

нуться атакам. Очень сложно предсказать, окажется атака удачной или нет. Тем не менее, когда имитация становится сложной, это, по крайней мере, устраняет случайные атаки.

Существует множество вариантов механизма «вызов-ответ». Рассмотрен [25] механизм «вызов-ответ», используемый при аутентификации по сетчатке, который выдает информацию, например число, которое должно быть опознано и напечатано пользователем. Это предотвращает использование «украденных» глаз и означает, что любая механическая подделка будет довольно сложной. Другой подход [26] основывается на вызовах, посылаемых сенсору, который должен обладать достаточными возможностями, чтобы дать ответ. Этот метод можно применять для большинства кремниевых сканеров отпечатков пальцев [27, 28], так как защищенный локальный процессор может быть интегрирован без особых усилий.

Взаимодействие «вызов-ответ» между человеком и компьютером либо между двумя компьютерами является частью аутентификационного протокола $A_П(P, K, B)$ и попадает в категорию динамических аутентификационных протоколов.

5.9. Сокращаемые биометрические параметры

Если биометрическая аутентификация выполняется недостаточно тщательно, систему можно обмануть, представив или запросив и передав биометрические идентификаторы для регистрации поддельных личностей; также можно получить доступ в приложение посредством генерации биометрических идентификаторов. Дело в том, что если биометрический идентификатор каким-то образом был однажды скомпрометирован, то он скомпрометирован навсегда, что влияет на конфиденциальность и безопасность системы.

5.9.1. Конфиденциальность

Автоматические методы биометрической аутентификации были разработаны, протестированы и установлены в разного рода крупных приложениях контроля финансового и физического доступа. Логично, что проблемы конфиденциальности (секретности данных в терминах безопасности) в процессе биометрической аутентификации должны рассматриваться в работах по безопасности [3, 26]. Существуют две взаимосвязанные проблемы [11]:

1. *Конфиденциальность.* Любая биометрическая технология обычно воспринимается как негуманная и представляющая угрозу для конфиденциальности. Хотя биометрические технологии становятся более безопасными, сам процесс прохождения аутентификации уже предполагает предоставление частной информации, например, где находится человек, что покупает и т. д. В случае биометрической аутентификации эта проблема становится еще серьезней, потому что биометрические свойства могут предоставить дополнительную информацию о состоянии здоровья человека или его чувствительности к тем или иным раздражителям. Например, по состоянию сосудов сетчатки можно узнать о наличии у человека диабета или повышенного артериального давления [29], поэтому нужно всегда помнить, что биометрические системы не предназначены для сбора такой информации.

2. *Защита информации.* Когда биометрические данные предоставляются определенной системе, содержащаяся в них информация не должна использоваться для других целей, кроме тех, для которых она была собрана. При использовании любой (сетевой) информационной системы очень трудно гарантировать, что биометрические данные будут использоваться только в целях, для которых они предназначены. Очень сложно определить, насколько легко верификационные базы данных личностей могут быть связаны с базами данных преступников.

Проблемы конфиденциальности и защиты информации касаются следующих аспектов:

1) существует большое количество собранной информации. Проблема касается каждого бита сохраненной информации о людях, особенно когда она связана с такими индивидуальными особенностями, как биометрические параметры;

2) традиционные проблемы безопасности, такие, как сохранность и конфиденциальность данных, имеют отношение к нарушениям секретности информации;

3) биометрические базы данных могут быть использованы для перекрестных сопоставлений, например: сопоставление с базами данных организаций, обеспечивающих правопорядок, таких, как ФБР или СИН. Проблема защиты информации становится действительно серьезной, когда аутентификационные базы данных сопоставляются с базами данных преступников (рис. 5.3).

Рис. 5.3. Перекрестное сопоставление больших баз данных связано с проблемой конфиденциальности

Эти проблемы усугубляются тем, что биометрические параметры не могут быть изменены. Одно из свойств, делающих биометрические параметры такими привлекательными для аутентификации, – их неизменность во времени – является и их недостатком. Если кредитная карта была каким-то образом дискредитирована, банк может просто дать клиенту новый номер карты. Когда дискредитирован биометрический параметр, его нельзя заменить на новый. У человека есть много пальцев, но только одно лицо. Техника, называемая сокращением биометрических параметров или шифрованием личности, может помочь решению проблемы конфиденциальности [26].

5.9.2. Намеренные повторяющиеся трансформации

Работы по данной теме [12, 30] предлагают ряд решений для обеспечения безопасности биометрических параметров, среди которых есть и «сокращение биометрических параметров». Это намеренное повторяющееся искажение биометрического сигнала, основанное на выбранной трансформации. Биометрический сигнал

искажается одним и тем же способом при каждом предъявлении, т. е. во время регистрации и при каждой последующей аутентификации. В этом случае в каждой регистрации может использоваться разная трансформация, поэтому выполнение перекрестного сопоставления становится невозможным. Более того, если один из вариантов биометрического параметра дискредитирован, можно изменить тип его трансформации для создания нового варианта (измененной репрезентации), чтобы заново зарегистрировать по существу новую личность. Такие трансформации являются необратимыми. Поэтому даже если известно точное изменение и полученный результат, первоначальный (неискаженный) биометрический параметр восстановить невозможно.

Сокращаемые изменения можно применять для трансформации биометрических сигналов и свойств, которые используются для представления биометрических параметров, т. е. биометрический сигнал должен быть трансформирован сразу после получения, либо сигнал может быть обработан обычным способом, а выделенные свойства уже могут подвергнуться трансформации.

5.9.3. Искажение сигнала

Эта категория относится к искажениям (предпочтительно необратимым) необработанного биометрического сигнала после того, как он получен сенсором, например, оригинала записи голоса или изображения отпечатков пальцев.

Изображения лица и отпечатков пальцев могут быть зарегистрированы в измененной форме. Такие изменения можно произвести разными способами. Например, на изображение могут быть наложены монотонно повторяющиеся точки. Измененное изображение тогда получается путем случайного перемещения этих точек по определенной схеме. Заметьте, что объект может быть зарегистрирован в старой аутентификационной системе с изображением отпечатков пальцев или лица в измененном виде. Старые аутентификационные системы не имеют информации о том, что изображение было трансформировано. Кроме того, при сопоставлении этих измененных изображений с любой другой существующей базой данных отпечатков пальцев или лиц личность владельца отпечатков пальцев или лица не будет идентифицирована. Пример трансформированных отпечатков пальцев приведен на рис. 5.4. Другие примеры измененных изображений биометрических параметров можно найти в [31].

Рис. 5.4. Два отпечатка пальца (*а*, *б*). Оригинал изображения был искажен одним и тем же способом (*в*) и (*г*). (*в*) и (*г*) выглядят одинаково, хотя не совпадают с (*а*) и (*б*)

Заметьте, что для изменения изображения для аутентификации отпечатки пальцев или изображение лица должны быть преобразованы в канонический вид перед тем, как подвергнуться искажению. Это можно

сделать путем определения основных точек, таких, как расстояние между глазами на лице.

Радужная оболочка – цветная область вокруг зрачка – другой параметр, который мы сейчас рассмотрим. Параметр, полученный из изображения радужной оболочки пользователя, представлен на рис. 5.5. Аутентификация и идентификация пользователя при помощи радужной оболочки происходят путем разработки бинарного кода, кода радужки, c = '0100101110...011' на базе обработанного изображения радужной оболочки. Тогда идентификация может происходить очень быстро даже в больших базах данных зарегистрированных пользователей, так как сравнивать такие коды очень просто (расстояние Хэмминга). Если радужная оболочка человека дискредитирована, она дискредитирована навсегда. Поэтому желательно иметь сокращаемую версию изображения кода радужки.

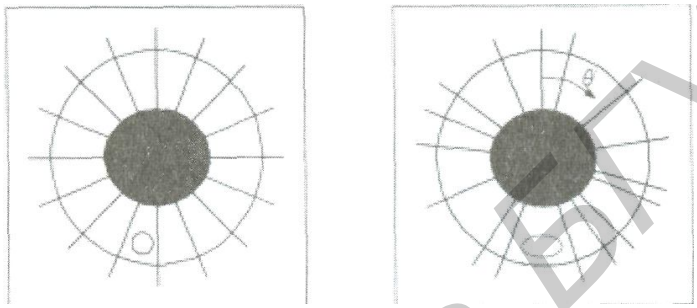
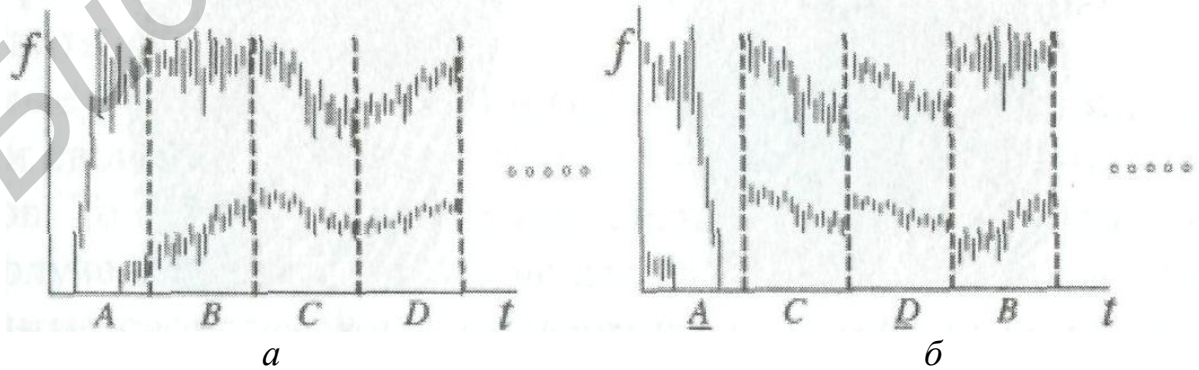


Рис. 5.5. Оригинал изображения радужной оболочки может быть зашифрован разными способами

Подобные техники трансформации можно применять для сигналов, которые не являются изображениями. На рис. 5.6 продемонстрирован двухмерный оригинал биометрического голосового сигнала $D(f, t)$. В каждой точке времени t_0 $D(f, t_0)$ показывает частоту голосового сигнала, как на спектрограмме.

Запись голоса, произносящего фиксированный текст, на рис. 5.6 можно разделить на временные отрезки *A, B, C, D* соответственно последовательности времени (*A, B, C*, *D*). На этом рисунке временные отрезки имеют равную длину, но это не обязательное условие. Зашифрованный голосовой сигнал представляет собой последовательность (*A, C, D, B*). Подчеркнутое *A* означает, что отрезок *A* воспроизводится в обратном порядке. Заметьте, что для такого шифрования голоса требуется минимальная регистрация записи голоса.



а *б*

Рис. 5.6. Оригинал записи голоса:
а – голос зашифрован при помощи деления сигнала на отрезки; б – голос зашифрован путем случайной перегруппировки сегментов и воспроизведения их в обратном порядке

5.9.4. Искажение свойств

Обработанные биометрические сигналы (шаблоны) также могут быть преднамеренно искажены. Ниже представлен пример необратимого искажения точечного образа. Например, рассмотрим множество деталей отпечатка пальца:

$$S = (x_i, y_i, \theta_i); \quad i = 1,...,M . \tag{5.1}$$

Необратимая трансформация преобразует множество S в новое множество S' так, чтобы первоначальное множество S не могло быть восстановлено из S':

$$S = (x_i, y_i, \theta_i); \quad i = 1,...,M \rightarrow S' = (X_i, Y_i, \Theta_i); \quad i = 1,...,M . \tag{5.2}$$

На рис. 5.7 показано, как x-координаты множества точек S могут быть трансформированы путем преобразования $x \rightarrow X$ или $X = F(x)$. Такие многочленные необратимые трансформации

$$Y = G(y) \quad \text{и} \quad \Theta = H(\theta) \tag{5.3}$$

могут быть использованы для остальных координат множества точек из выражения (5.2).

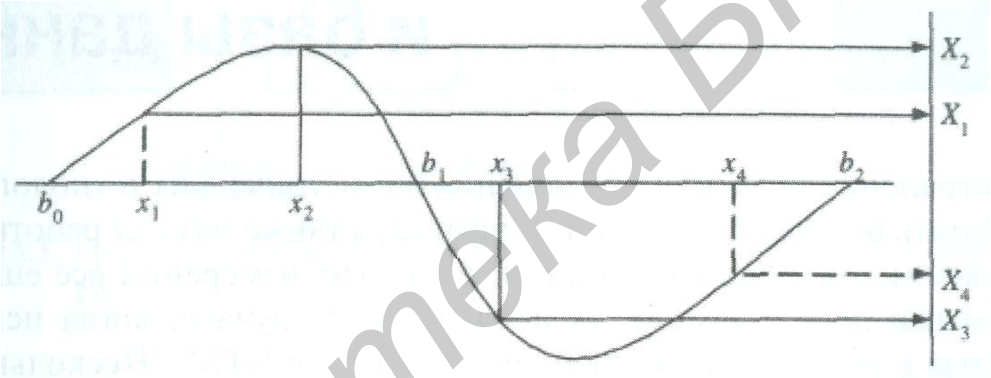


Рис. 5.7. Изображение одной координаты многомерного множества точек в новой плоскости координат

5.9.5. Отношение к сжатию и шифрованию

Сокращение биометрических параметров значительно отличается от сжатия сигнала с использованием стандартных техник обработки сигнала. При сжатии сигнал временно теряет свои пространственные характеристики, т. е. две точки в первоначальном несжатом сигнале не останутся на сопоставимом расстоянии в сжатой области. Тем не менее после декомпрессии оригинала они восстановятся до первоначального вида или восстановятся приблизительно, если сжатие было низкого качества. В случае сокращения биометрического параметра большая часть геометрии сохраняется.

Сокращение биометрических параметров также сильно отличается от технологий шифрования. При шифровании преследуется цель восстановить первоначальный сигнал на другом конце защищенной сети. Тогда как при данном необратимом искажении первоначальный сигнал не восстанавливается, и на самом деле сделать это должно быть невозможно.

Более того, существующие биометрические системы не могут сразу аутентифицировать сжатый или зашифрованный сигнал, в то время как сокращенные сигналы могут обрабатываться с помощью существующих программ, как будто они представлены в обычном виде.

6. ВЫБОР БИОМЕТРИЧЕСКОГО ПАРАМЕТРА

Выбор биометрического параметра основывается не только на коэффициентах ошибок. В зависимости от приложения на него влияет множество других факторов. Цена, дополнительные расходы, безопасность системы, несомненно, зависят от выбора биометрического параметра, поэтому он имеет такое большое значение. Точность является определяющим аспектом в выборе биометрического параметра, но нет оснований считать ее самым важным фактором (рис. 6.1).

Рис. 6.1. Выбор «правильного» биометрического параметра

В подразд. 6.1 мы проведем сравнительный анализ шести наиболее широко используемых биометрических идентификаторов, рассмотренных в разд. 3, но вначале сопоставим их с точки зрения других важных качеств и свойств, помимо коэффициентов ошибок. Во второй раздела проанализируем требования отдельных сценариев приложений и их влияние на выбор биометрических параметров.

Здесь мы имеем дело с более-менее объективной оценкой биометрических систем. Тем не менее она не обязательно оказывает влияние на продажи. С точки зрения производителей, эстетика может быть крайне важным фактором [32].

6.1. Свойства биометрических параметров

На основе нескольких внутренних и внешних свойств биометрических параметров и сенсоров, необходимых для принятия биометрического сигнала, можно сравнить шесть традиционных биометрических параметров, как показано в табл. 6.1.

Одно из наиболее важных, хотя и не поддающихся количественному определению свойств, – первый указанный в таблице параметр – *степень разработанности.* Данное свойство связано со стадией разработки технологии получения и распознавания биометрических образцов, а также с пониманием процессов, которые оказывают влияние на их разнообразие. Если биометрический параметр изучался какой-либо наукой ранее, то он лучше разработан по сравнению с теми, которые стали изучаться только в рамках биометрии.

Таблица 6.1

Сравнение свойств
шести популярных биометрических параметров

Характеристика	Палец	Лицо	Голос	Радужная оболочка	Рука	Подпись
Степень разработанности	Очень высокая	Средняя	Средняя	Средняя	Высокая	Средняя
Тип сенсора	Контактный	Незаметный	Незаметный	Незаметный	Контактный	Контактный
Размер сенсора	Маленький	Маленький	Очень маленький	Средний	Большой	Средний
Цена сенсора (дол. США)	<200	<50	<5	<300	<500	<300
Размер шаблона	<500	<1000	2000	256	<100	200
Масштабируемость	Высокая	Средняя	Низкая	Очень высокая	Низкая	Высокая

Другой связанный с предыдущим аспект – это использование биометрических параметров в системах, управляемых людьми; вопрос об обработке «отклоняющихся от нормы» случаев был изучен на большом количестве разнообразных образцов.

Время, затрачиваемое на сопоставление образцов, безусловно, является значительным фактором, но в данном случае время не рассматривается как биометрическое свойство само по себе. Время обработки очень сложно определить точно, потому что оно зависит от особенностей конкретного алгоритма и производительности используемого процессора. Более того, время вычисления уменьшается по мере того, как процессоры становятся более совершенными.

6.1.1. Свойства сенсора

Как указано в табл. 6.1, существует несколько аспектов, касающихся сенсоров, которые необходимо принять во внимание при выборе биометрической системы:

– *тип сенсора.* Для получения биометрического сигнала может быть использован контактный или бесконтактный сенсор. Бесконтактные сенсоры можно применять в скрытых приложениях для наблюдения, тогда как контактные сенсоры требуют содействия пользователя при предоставлении биометрического параметра. Таким образом, бесконтактные сенсоры удобнее контактных;

– *размер сенсора.* Некоторые биометрические сенсоры, такие, как микрофон или скрытые камеры, могут быть очень маленькими. Но иногда для надежного принятия сигнала необходим целый комплекс оптических установок (например, для радужной оболочки), что приводит к увеличению размера сенсоров. Иногда физическая безопасность считывающего устройства в автоматических установках, работающих с биометрическими параметрами, очень важна. Подобные дополни-

тельные требования приводят к увеличению размера (и цены) сенсора. Устройства, считывающие геометрию руки, из всех сенсоров для традиционных биометрических параметров являются самыми большими, так как они должны получать полное изображение ладони в длину, ширину и высоту;

– *цена сенсора.* Аспект, непосредственно связанный с размером сенсора, – это его цена. Хотя стоимость биометрических сенсоров падает с каждым годом, относительная стоимость одних сенсоров по сравнению с другими остается неизменной. В таблице указана только цена основного сенсора, которая не включает в себя другие сопутствующие расходы: на кабели, стойки, пользовательские интерфейсы и техническое обслуживание, необходимое для бесперебойной работы системы.

6.1.2. Размер шаблонов

Шаблон – это машинная репрезентация биометрического образца. Шаблон определенным образом описывает полученный биометрический образец, для того чтобы можно было провести как можно более точное автоматизированное сопоставление. Размер этой репрезентации в байтах является важным фактором, который может повлиять на выбор биометрического параметра. Маленькие шаблоны дают возможность использовать небольшие устройства W их хранения, такие, как магнитные карты, и позволяют создавать распределенные базы данных.

В дополнение к шаблону алгоритм сопоставления часто предполагает применение других данных, например идентификационного номера. Иногда для создания более компактного шаблона можно использовать техники сжатия; шифрование или цифровая подпись, напротив, сделают размер шаблона больше. Сохранение биометрической репрезентации во время работы было обозначено как онлайновое, а хранение сжатых биометрических записей в биометрических базах данных было названо офлайновым. Приблизительный размер шаблонов можно найти в предпоследней строке табл. 6.1, там же обозначен онлайновый размер сохранения. Указываются только размеры шаблонов (для онлайнового сохранения) рассмотренных биометрических параметров.

Размеры шаблонов разных биометрических параметров сильно различаются, от самого маленького для радужной оболочки до большого – для голоса; это также является причиной существующих расхождений в данных, представленных в опубликованных работах. Например, в [33], приводятся следующие размеры (в байтах): радужная оболочка – 256, палец – 512–1024, геометрия руки – 9. Используя данные примеры и ориентируясь на другие имеющиеся подобные данные, мы показали требования к сохранению шаблонов в последней строке табл. 6.1.

Размер шаблона слишком мало говорит об индивидуальных особенностях, о битовой силе или коэффициенте ложного доступа биометрического параметра. В целом можно ожидать, что маленький шаблон будет иметь меньшую различительную силу, чем большой, но если репрезентация непригодная, большой шаблон может содержать меньше полезной информации, чем маленький, и иметь худший коэффициент ложного доступа.

Как было отмечено выше, в целях обеспечения безопасности и конфиденциальности желательно сохранять машинные репрезентации или аутентификационные удостоверяющие данные, включающие биометрические образцы, в распределенной базе данных, например, хранить их на смарт-картах, которые будут находиться в собственности людей, зарегистрированных в базе данных. В этом случае биометрический образец всегда будет находиться со своим хозяином. Для пользования централизованными базами данных необходимо определенное доверие между пользователями приложения и владельцем базы данных и оператором – пользователь должен быть уверен, что его биометрический образец не будет доступен никому другому.

С точки зрения хранения биометрических данных первой проблемой в биометрической аутентификации становится разница процедур верификации и идентификации. В процессе идентификации происходит сопоставление биометрических презентаций типа 1:*m,* тогда как во время аутентификации выполняется сопоставление типа 1:1. Это означает, что для идентификации требуются большие централизованные базы данных **M** и в *m* раз больше операций сопоставления.

Существует алгоритм для сопоставления отпечатков пальцев, который находит образцы в базах данных с большим *m* при помощи трансформирующейся кластеризации [34]. Его можно применять с использованием геометрических хеширующих схем, которые работают с увеличивающимся *m,* требуя больше места для хранения значительного размера машинных репрезентаций. В основе такого подхода лежит соотношение пространства-времени. Иногда требования к месту для хранения базы экспоненциально зависят от *m* [15].

6.1.3. Масштабируемость

Масштабируемость в пятой строке (см. табл. 6.1) связана с внутренними свойствами биометрического параметра и имеет отношение к коэффициентам ошибок.

Хорошо масштабируемые биометрические параметры могут быть использованы для идентификации людей в больших популяциях для обеспечения приемлемых коэффициентов ошибок или предотвращения затрат большого количества времени. Плохо масштабируемые биометрические параметры могут использоваться только в маленьких базах данных и приводить к большому количеству ошибок при работе с большими базами данных. В больших биометрических базах данных не должны содержаться образцы плохого качества, так как тогда при аутентификации будет слишком часто возникать необходимость в обработке исключительных случаев.

Лицо и отпечатки пальцев могут быть не настолько более точными по сравнению с другими биометрическими параметрами, как это принято считать. По степени точности биометрические параметры делят на сильные (радужная оболочка и отпечатки пальцев) и слабые (рука, голос, лицо).

Для того чтобы слабые биометрические параметры перешли в класс сильных, необходим серьезный прогресс в сфере биометрических технологий, небольших

усовершенствований здесь будет недостаточно. Технологии сегодня развиваются слишком медленно, чтобы в ближайшем будущем ожидать повышения точности слабых биометрических параметров до приемлемого уровня для использования их в приложениях, требующих высокой безопасности; активное изучение этих «приемлемых» биометрических параметров в последнее время является тому подтверждением.

Нужно отметить, что в определенных случаях высокая масштабируемость бывает нежелательна, так как снижается приемлемость биометрического параметра из-за проблем с конфиденциальностью. Использование сильных биометрических параметров в верификационных системах, контролирующих пользование университетскими столовыми и общежитиями или присутствие и время работы персонала, предполагает предоставление людьми биометрических образцов, которые потенциально могут быть применены для идентификации в некоторых других базах данных (например, в базах органов защиты правопорядка), что может вызывать опасения по поводу конфиденциальности.

6.2. Свойства приложения

Очень сложно определить «наилучший» параметр без учета типа приложения, в котором он будет использоваться, поэтому рассмотрим традиционные категории биометрических приложений.

Существует множество приложений, где биометрическая аутентификация может обеспечить повышение уровня безопасности. Это, например, точки контроля доступа на границах разных уровней безопасности и авторизация для проведения разного рода транзакций. Для каждого типа приложений необходимо ответить на следующие вопросы:

1. Что именно защищает приложение?
2. Кем являются авторизованные пользователи и операторы?
3. Кто представляет угрозу для приложения?
4. Какой будет цена нарушения безопасности?
5. Какой является действительная стоимость безопасности?
6. Какой будет дополнительная «стоимость» неудобства пользователей?

Обсудим разные виды приложений, ориентируясь на эти вопросы.

В табл. 6.2 указаны различные приложения и оценена важность ряда аспектов разных биометрических параметров для этих приложений. Такие характеристики, как *невозможность регистрации* и *размер шаблона*, приведены в первом столбце, а в других столбцах определена их важность для разных приложений. Отрицательные стороны биометрических параметров и их свойств указаны в левом столбце таблицы, а типы приложений приведены в верхней строке:

Оценка	**Приложение *А***	**Приложение *Б***
Недостатки	*Маленькие*	*Средние*

Градация «маленькие – большие» определяет важность недостатка для приложения *А* или *Б*. В этом случае недостаток является маленьким по важности для приложения *А,* но средним по важности для приложения *Б*.

Точность как биометрическое свойство вычисляется путем использования разных спецификаций ошибок. В таблице приведены характеристики качества работы системы на двух разных рабочих точках вместо одной, как в случае с коэффициентом равных ошибок. Это позволяет получить общее представление о соотношении между удобством и безопасностью, которое можно ожидать от каждого приложения. Оценки, данные в этой таблице, субъективны и приводятся только для примера.

1. Количество ЛД на 10 000 (при КЛОД = 10 %): количество ложных доступов на 10 000 при стандартном коэффициенте ложного отказа доступа, равном 10^{-1}.

Число 100 означает, что 100 мошенникам из каждых 10 000 будет дан доступ, т. е. 1 % из всех возможных взломов системы будет успешным. Это может быть «средней» рабочей точкой для создания системы контроля доступа, которая редко подвергается атакам злоумышленников, но для приложений с высоким уровнем безопасности это значение будет «низкой» рабочей точкой.

2. Количество ЛД на 10 000 (при КЛОД = 1 %): количество ожидаемых ложных доступов на каждые 10000 атак, когда уровень КЛОД настроен на 1 % от всех проб.

Обычно числа в этом ряду – самые большие для больших приложений с большими группами пользователей. Кредитные карты и приложения типа банкоматов требуют высокого уровня безопасности, но не стоит забывать и об удобстве для пользователя. Такой низкий коэффициент ложного отказа доступа не является желательным для других приложений, так как пользователи из-за этого станут испытывать большие неудобства.

Некоторые приложения рассмотрим более подробно. Приблизительно можно разделить на три группы с разными требованиями:

1) контроль физического доступа и системы авторизации для маленьких групп;

2) контроль физического доступа для больших групп пользователей;

3) авторизация транзакций для больших групп пользователей.

Таблица 6.2

Оценка важности свойств различных приложений

Оценка важности	Физический доступ	Продажа товаров	Доступ в аэропорту	Кредитные карты	Банкоматы
Внутренние свойства					
Необходимая кооперация	Низкая	Низкая	Высокая	Низкая	Средняя
Социальные штампы	Средне	Мало	Средне	Много	Много
Заметность	Средняя	Низкая	Средняя	Высокая	Средняя
Недостаток популяции людей	Маленький	Маленький	Средний	Средний	высокий
Свойства образцов					
Неудобство	Среднее	маленькое	Среднее	высокое	высокое
Необходимое сходство	Маленькое	Маленькое	Высокое	Среднее	Среднее
Время считывания	Большое	Среднее	Большое	Среднее	Среднее
Невозможность регистрации	Средняя	Низкая	Средняя	Высокая	Высокая
Невозможность получения	Средняя	Средняя	Высокая	Высокая	Высокая
Свойства сопоставления 1:1					
Количество ЛД на 10 тыс. (при КЛОД = 10 %)	Среднее	Большое	Большое	Большое	Среднее
Количество ЛД на 10 тыс. (при КЛОД = 1 %)	Среднее	Маленькое	Большое	Среднее	Большое
Размер шаблона (в байтах)	Маленький	Маленький	Средний	Большой	Большой
Свойства технологии					
Цена инсталляции	Средняя	Низкая	Средняя	Высокая	Высокая
Цена продолжительной работы	Средняя	Низкая	Средняя	Высокая	Высокая
Цена сопоставления	Низкая	Низкая	Средняя	Средняя	Средняя

Физический доступ

Обычно это приложения с небольшим количеством зарегистрированных пользователей. Стоимость неправильной аутентификации может исчисляться миллионами долларов. Пользователь приложения должен каждый раз кооперироваться с системой, потому что этот тип аутентификации требуется в ежедневной работе. Эти аутентификационные приложения не являются добровольными, в них существует относительно статичный список контроля доступа. Обычно для этих приложений удобство пользования является не особенно значимым.

Проверка в аэропорту

Эти приложения составляют отдельный класс, так как в них последствием ошибки аутентификации может стать угроза жизни. В них обычно представлены все виды пользователей. Это делает разработку биометрических аутентификационных систем для аэропортов сложной и дорогой.

Однако здесь высокая стоимость установки и работы системы имеет среднюю важность.

Кредитные карты и пользование банкоматами

Сценарии таких приложений сильно отличают их от двух других уже рассмотренных типов. Приложения для кредитных карт и банкоматов обычно имеют большое количество зарегистрированных пользователей; последствия неправильной аутентификации могут быть равны примерно 500 дол. США, т. е. денежное исчисление риска в 10^{-4} раз ниже по сравнению с приложениями первого типа.

В этом случае проблемой является одобрение приложения пользователями. Пользователи не имеют желания кооперироваться с приложением, если конкуренты предлагают альтернативные системы (возможно, вообще не требующие предъявления биометрических параметров), которые легче использовать. Более того, отсутствие ответственности за мошенничество с банковскими картами и банкоматами отнюдь не способствует тому, чтобы пользователи кооперировались с трудными в использовании биометрическими системами. В этих приложениях удобство биометрического параметра очень важно, а цена его применения должна быть низкой.

6.3. Способы оценки

Теперь, после сравнения свойств различных биометрических параметров и требований, предъявляемых разными видами приложений, вернемся к основному вопросу, а именно, как происходит выбор биометрического параметра.

Конечно, ответить на него будет непросто; как было отмечено ранее, существует ряд факторов, которые нужно принять во внимание. В этом подразделе рассмотрим простую систему сопоставления биометрических параметров с точки зрения эффективности использования в конкретном приложении. Она не является строгим аналитическим инструментом, но позволяет учесть наиболее важные характеристики приложения.

6.3.1. Вычисление различий

Рассмотрим простой метод для выбора «наилучшего» биометрического параметра для приложения, основанный на составлении таблицы, похожей на табл. 6.2, но в верхней строке ее будут вписаны не типы приложений, а биометрические параметры:

Оценка	Биометрический параметр *X*	Биометрический параметр *Y*
Недостатки	Маленькие	Средние

Отметки «маленькие – средние – большие» – это оценка важности определенного недостатка или отрицательного свойства для конкретного биометрического параметра *X* или *Y*. Недостаток в этом примере имеет низкую значимость для параметра *X* и среднюю – для параметра *Y*.

Табл. 6.3 – это пример применения данного метода. Оценки показателей точности даются в цифрах, потому что имеется РХПУ этих параметров. Например, рассмотрим два первых числа в столбце «палец»:

1) при КЛОД = 10^{-1} КЛД = 10^{-5}, поэтому количество ложных доступов на 10 000 проб составляет $10^{-5} \times 104 = 0{,}1$;

2) если для дополнительного удобства пользователей настроить КЛОД на 10^{-2}, КЛД повышается до 10^{-3} и количество ложных доступов становится $10^{-3} \times 104 = 10$.

И соответственно для двух верхних чисел столбца «лицо»:

1) при настройке КЛОД = 10^{-1} имеем КЛД = 10^{-3} и, следовательно, 10 ложных доступов на 10 000 проб (так как $10^{-3} \times 104 = 10$);

2) при КЛОД = 10^{-2} КЛД = 10^{-1}, поэтому получаем $10^{-1} \times 10^{4} = 1000$ ложных доступов.

Эти цифры приблизительны и нужны только для того, чтобы показать, как можно использовать такую таблицу, – они не являются результатом каких-либо строгих тестов, они также не связаны с каким-то определенным алгоритмом или технологией.

В табл. 6.3. описаны недостатки различных биометрических технологий. Это только примерная оценка, коэффициенты ошибок являются приблизительными, не связаны ни с каким определенным алгоритмом или системой

Чтобы использовать эту таблицу как матрицу в расчетах, словесные характеристики нужно заменить цифровыми значениями. Например, примем высокую значимость за 10, среднюю – за 3, низкую – за 1.

Хотя в таблице уже есть несколько цифровых значений, нужно преобразовать их так, чтобы их можно было сравнить с другими характеристикам. Для этого можно использовать следующие вычисления:

1) $C = C = v / 100$ – для размеров шаблонов;

2) $C = C = 10 \times \log_{10} v$ – для ожидаемых вторжений в систему при КЛОД = 10 %;

3) $C = C = \max(0{,}10 \times \log_{10} v + 10)$ – для ложного отказа доступа, равного 1 %.

Таблица 6.3

Недостатки разных биометрических технологий

Недостатки биометрических параметров	Палец	Лицо	Голос	Радужная оболочка	Рука	Подпись
Внутренние свойства						
Необходимая кооперация	Высокая	Низкая	Низкая	Средняя	Высокая	Высокая
Социальные штампы	Много	Мало	Мало	Средне	Средне	Мало
Заметность	Средняя	Низкая	Низкая	Средняя	Средняя	Низкая
Недостаток популяции людей	Маленький	Маленький	Средний	Маленький	Средний	Средний
Свойства изображений						
Неудобство	Маленькое	Маленькое	Маленькое	Среднее	Среднее	Среднее
Необходимое сходство	Большое	Маленькое	Маленькое	Среднее	Высокое	Высокое
Время считывания	Маленькое	Маленькое	Среднее	Среднее	Среднее	Среднее
Невозможность регистрации	Средняя	Низкая	Средняя	Высокая	Низкая	Низкая
Невозможность получения	Средняя	Средняя	Средняя	Средняя	Низкая	Низкая
Свойства сопоставления 1:1						
Количество ЛД на 10 тыс. (при КЛОД = 10 %)	0,1	10	300	0,001	10	300
Количество ЛД на 10 тыс. (при КЛОД = 1 %)	10	1000	1000	0,1	100	1000
Размер шаблона (в байтах)	500	1000	2000	250	100	200
Свойства технологии						
Цена инсталляции	Низкая	Низкая	Низкая	Средняя	Средняя	Средняя
Цена продолжительной работы	Низкая	Низкая	Низкая	Средняя	Низкая	Низкая
Цена сопоставления	Средняя	Низкая	Низкая	Низкая	Средняя	Низкая

Можно сопоставить столбец оценки (см. табл. 6.2) со столбцом недостатков (см. табл. 6.3) и вычислить математическое скалярное произведение, чтобы получить степень различия. Ниже это сделано для столбцов «Физический доступ» и «Палец» (табл. 6.4).

Можно увидеть, что несоответствие между приложением и биометрическим параметром составляет 135. Для сравнения: если сделать такие же вычисления для столбца «лицо», получим величину несоответствия 201. Более низкое значение говорит о том, что отпечаток пальца будет предпочтительней распознавания лица в этом конкретном приложении контроля физического доступа.

Таблица 6.4

Вычисление величины различия путем установки
цифровых значений и суммирования

Вычисление величины различия	Физический доступ	О	×	Ч	Палец
Внутренние свойства					
Необходимая кооперация	Низкая	1	10	10	Высокая
Социальные штампы	Средне	3	30	10	Много
Заметность	Средняя	3	9	3	Средняя
Недостаток популяции людей	Низкий	1	1	1	Низкий
Свойства образцов					
Неудобство	Среднее	3	3	1	Низкое
Необходимое сходство	Низкое	10	10	10	Высокое
Время считывания	Большое	10	10	1	Маленькое
Невозможность регистрации	Средняя	9	9	3	Средняя
Невозможность получения	Средняя	9	9	3	Средняя
Свойства сопоставления 1:1					
Количество ЛД на 10 тыс. (при КЛОД = 10 %)	Среднее	0	0	0	Среднее
Количество ЛД на 10 тыс. (при КЛОД = 1 %)	Среднее	30	30	10	Большое
Размер шаблона (в байтах)	Маленький	5	5	5	Большой
Свойства технологии					
Цена инсталляции	Средняя	3	3	1	Низкая
Цена продолжительной работы	Средняя	3	3	1	Низкая
Цена сопоставления	Низкая	1	3	3	Средняя
Сумма			135		

Однако существует множество способов настроить систему таким образом, чтобы она выдавала абсолютно разные результаты. Можно изменить относительные оценки различных свойств при работе с определенным приложением (изменить табл. 6.2). Можно установить разные уровни недостатков определенного биометрического параметра (изменить табл. 6.3). Интерпретацию символических оценок как числовых факторов можно отрегулировать, например, используя (10, 5, 2) вместо (10, 3, 1). Или можно использовать одни числовые значения для таблицы оценок, а другие – для таблицы недостатков. Наконец, преобразование вероятностей и размеров образцов в цифры является в большей степени произвольным. Точная настройка даже нескольких из этих факторов поставщиком решения (про-

давцом) может показать, что именно данный биометрический параметр является самым лучшим для данного приложения.

Возможно, что лучшим приложением такого рода вычислений будет выражение чувствительности системы.

Рассмотрим значения в столбце «произведение». Большие значения указывают на те свойства биометрических параметров, которые не подходят для данного приложения и указывают на его слабые места. В табл. 6.4 число 30 связано с социальными штампами и количеством ЛД на 10 тыс. (при КЛОД = 1 %). Оценка обозначена как О, числовое значение – как Ч, произведение – «×»

Можно предположить, что использование отпечатков пальцев для контроля физического доступа будет ассоциироваться у людей с опознанием преступников.

Вторая проблема связана с тем, что при работе системы с низким уровнем ЛОД, общий КЛД будет не таким, как хотелось бы. Поэтому можно запустить систему с более высоким значением ЛОД, например, в 10 % (при этом неудобство пользователей будет возрастать), чтобы получить приемлемый уровень безопасности (хороший КЛД). Точно так же при подобных вычислениях для лица получаем 60 в столбце произведения при количестве ЛД на 10 тыс. (при КЛОД = 10 %) и 90 – при количестве ЛД на 10 тыс. (при КЛОД = 1 %). Это значит, что самой большой проблемой при распознании лица в данном приложении будет низкий уровень безопасности. Чтобы решить эту проблему, можно попробовать ограничить размер популяции пользователей другими способами.

6.3.2. Сравнительные тестирования биометрических параметров

Часто независимые организации, проводящие сравнительные тесты, или координаторы соревнований сами уточняют методы оценки. Приведем два примера.

6.3.2.1 Голос

В сравнительных испытаниях устройств, распознающих голос, которые проводились Национальным институтом стандартов и технологий (НИСТ) [35, 36], использовалась следующая формула расчета стоимости для определения победителя:

$$\text{Стоимость} = \sum_{\text{сост.ош}} C_{\text{сост.ош}} P_{\text{сост.ош}} P_{\text{сост}} , \qquad (6.1)$$

где $C_{\text{сост. ош}}$ – это стоимость, связанная с состоянием ошибки; $P_{\text{сост. ош}}$ – вероятность возникновения этого состояния; $P_{\text{сост}}$ – изначальная вероятность возникновения состояния «*сост*». $P_{\text{сост}}$ – попытка определить вероятность ошибок.

Вероятность того, что мошенник попытается получить доступ в систему в зоне с высокой преступностью (например в городе), будет выше по сравнению с зонами с низкой преступностью (например, в небольшом городке или в деревне), т. е. в случае оценки верификации говорящего НИСТ определяет следующие величины:

$C_{\text{потери}}$	$C_{\text{ложная тревога}}$	$P_{\text{сост}}$
10	1	0,01

Стоимость потери (ложный отказ доступа) в 10 раз превышает стоимость ложной тревоги.

Несмотря на то что выражение (6.1) используется для оценки алгоритмов распознавания говорящего, это выражение можно применять и в сравнительных исследованиях других биометрических мэтчеров.

6.3.2.2 Палец

В недавно опубликованных результатах сравнительных испытаний систем верификации отпечатков пальцев FVC 2002&2000 [37] было отмечено несколько параметров ошибок, по каждому из которых был определен победитель. Организаторы адаптировали понятия коэффициента ложного сходства (КЛС) и коэффициента ложного различия (КЛР). Параметры ошибок, которые подверглись оценке, следующие:

1) коэффициент равных ошибок (КРО) – это рабочая точка или пороговая величина *U*, где КЛС = КЛР;

2) нулевой коэффициент ложного сходства – самый низкий КЛР, при котором не бывает случаев ложного сходства;

3) КЛР, для которого КЛС < 1 %;

4) КЛР, для которого КЛС < 0,1 %;

5) среднее время регистрации отпечатка пальца;

6) среднее время сопоставления двух отпечатков.

Все эти оценочные параметры одинаково важны, но чтобы правильно оценить все величины, необходимо разработать подходящий тест. Чтобы протестировать каждый биометрический мэтчер, используя критерии оценки работы устройства, понадобится как минимум база данных.

6.4. Доступность и цена

Кроме свойств, указанных в табл. 6.2, существует ряд других вопросов, которые необходимо принять во внимание. Приведем несколько примеров.

При обсуждении стоимости биометрических сенсоров было отмечено, что стоимость решения сильно отличается от общей стоимости владения (ОСВ). Общая стоимость владения включает в себя затраты на обслуживание сенсора, текущую работу оборудования и т. д. Эта цифра будет больше стоимости решения, которая является только частью необходимых затрат.

Самая первая проблема, связанная со стоимостью биометрических аутентификационных систем, определяется различием процедур верификации и идентификации. При идентификации сопоставление биометрических репрезентаций происходит по типу 1:*m,* а при верификации – по типу 1:1. Это означает, что для идентификации требуется большая централизованная база данных, коммуникационная инфраструктура и в *m* раз больше вычислительных ресурсов, чем при верификации. Другая важная проблема, связанная со стоимостью, – это выбор между одним или несколькими биометрическими аутентификационными протоколами.

С использованием биометрических параметров в аутентификационных системах связано много издержек. Большая часть средств уходит на обучение системы. Стоимость регистрации пользователей может быть включена в стоимость обучения системы или в стоимость технической поддержки. Большая часть обучения системы (ее точная настройка) – это и есть большая часть ее работы, которая составляет (особенно для крупномасштабных систем) значительную долю стоимости технической поддержки в течение всего времени ее эксплуатации. Поэтому общее обучение определяется следующим образом:

– *обучение системы* – это улучшение, усовершенствование и настройка биометрического мэтчера во время установки. Эти работы должны почти полностью выполняться непосредственно на месте установки аутентификационной системы, что может стоить дорого; во время обучения должны быть достигнуты необходимые коэффициенты ложного доступа и ложного отказа доступа. В процессе обучения может потребоваться контроль качества снятия метрических образцов. Это может отразиться на удобстве всего процесса и негативно повлиять на пропускную способность и, таким образом, повысить стоимость, особенно стоимость регистрации;

– *регистрация объекта* – это процесс обучения системы с использованием биометрии репрезентации объекта. Как было замечено выше, это очень важная задача. Когда безопасность является принципиальным требованием для приложения, процесс регистрации должен быть защищен так же хорошо, как и процесс аутентификации. Регистрацию необходимо проводить в более безопасной и доверительной обстановке, чем саму аутентификацию. Регистрация – это процесс, который нужно очень хорошо контролировать, так как он может сильно влиять на стоимость системы.

Кроме перечисленных, есть еще и другие факторы, оказывающие влияние на стоимость системы в процессе ее эксплуатации:

1. *Процессы, связанные с регистрацией.* Когда зарегистрированная популяция биометрического приложения станет стабильной, стоимость регистрации может снизиться (большинство регистрации происходит сразу после начала работы приложения). Поддержание целостности базы данных является трудоемким и длительным процессом; проблемы с базой данных возникают из-за действий пользователей, представляющих разные категории зоопарка Доддингтона [38], а также осторожных злоумышленников и из-за ошибок персонала. Очевидно, что получение биометрических образцов, особенно во время регистрации, должно проводиться очень аккуратно, тем более когда m становится большим;

2. *Невозможность регистрации (HP).* Коэффициент невозможности регистрации очень сложно подсчитать до того, как система будет разработана и установлена. HP требует обработки исключительных случаев и может быть источником дополнительных издержек.

Когда биометрическая аутентификационная система работает с высоким уровнем HP, преобразование системы из добровольной в принудительную может стоить очень дорого.

3. *Обучение пользователя.* От пользователя требуется определенный уровень понимания приложения. Неправильное использование приложения может иметь катастрофические последствия и сказаться на пропускной способности системы. Маркетинговые издержки могут составлять значительную часть стоимости биометрической установки.

4. *Труд супервизора.* В зависимости от сложности работы, от инспекторов и операторов биометрических аутентификационных систем требуется определенный уровень знаний и навыков.

Часто биометрическое приложение контролируется человеком. Оператор обычно следит за качеством получаемых образцов биометрических параметров и выполняет обработку исключительных случаев, например при невозможности получения образца (НП). При необходимости операторы также могут проводить визуальное сопоставление параметров.

5. *Обслуживание устройства.* Человеческий труд необходим для технической поддержки приложения. Сюда включается как работа высококвалифицированных технических специалистов, так и труд менее квалифицированного персонала, выполняющего такие важные задачи, как очистка биометрических сканирующих устройств.

Затраты на биометрическую систему складываются из нескольких пунктов и включают в себя не только стоимость сенсора или мэтчера. Поддержка работы системы, обеспечиваемая супервизорами и операторами регистрации/аутентификации, может существенно увеличить общие затраты.

Таким образом, упомянутые выше факторы, влияющие на стоимость, зависят от выбранного биометрического параметра. Более того, на общую стоимость оказывают влияние отличительные особенности каждого биометрического параметра, такие, как степень изученности, масштабируемость, размер и цена сенсора, а также размер шаблона. Это делает расчет прибыли и расходов на содержание' биометрической системы очень сложной задачей.

6.5. Преимущества и недостатки биометрических параметров

Может существовать несколько биометрических параметров, которые будут хорошо подходить для конкретного приложения с точки зрения объективных и субъективных оценок. Каждый биометрический параметр имеет определенные положительные и отрицательные качества, которые нужно учитывать при выборе параметра для конкретного приложения. Положительные и отрицательные стороны каждого из шести традиционных биометрических параметров обсудим более подробно.

6.5.1. Отпечатки пальцев

Преимущества биометрического параметра:

– отпечатки пальцев уже давно используются для идентификации личности в криминалистике. Тем не менее недавно были найдены новые сведения, ставящие под сомнение точность существующих методов анализа отпечатков;

– существует большая база данных отпечатков пальцев, хотя в ней в основном зарегистрированы преступники. Кроме того, департаменты транспорта Калифорнии, Колорадо, Флориды и Техаса работают над тем, чтобы ввести практику использования отпечатков пальцев в водительских правах и записях данных;

– отпечатки пальцев прекрасно подходят для применения в суде экспертизе, например, широко распространен метод изучения латентных отпечатков пальцев [39]. Преступники часто оставляют на месте преступления отпечатки пальцев (в машинах, на дверных ручках, стекле, оружии), которые позволяют воссоздать картину событий;

– образцы отпечатков пальцев легко получить, используя простые средства; размер и цена считывающих устройств для отпечатков пальцев продолжают уменьшаться. Преобразование отпечатков в цифровые изображения становится проще, качественнее и дешевле. Сейчас существуют доступные по цене сканеры отпечатков пальцев (меньше 100 долл. США), которые широко используются во многих приложениях контроля доступа.

Недостатки биометрического параметра:

– с отпечатками пальцев связаны устойчивые социальные предрассудки, в сознании людей некоторых стран они ассоциируются с уголовными преступлениями. Эта ассоциация в некоторых случаях может быть и преимуществом, но чаще препятствует расширению сферы применения отпечатков пальцев как биометрического параметра;

– в некоторых культурах отпечатки пальцев все еще ассоциируются с безграмотными людьми, которые используют их вместо подписи;

– качество отпечатков пальцев может быть разным в зависимости от возраста, загрязненности рук, потертости кончиков пальцев, к тому же пальцы могут быть ампутированы, т. е. необходимо учитывать связь между образом жизни человека и качеством отпечатков его пальцев;

– для получения изображения отпечатка пальца нужно нажать пальцем на поверхность считывающего устройства. Это приводит к техническим трудностям и к проблемам, связанным с чистотой сенсора и гигиеной;

– изредка встречаются люди, у которых нет пальцев. Очевидно, что у этих людей невозможно получить образцы.

6.5.2. Лицо

Преимущества биометрического параметра:

– изображения лиц широко используются в паспортах и водительских удостоверениях – для расширения возможностей аутентификационного протокола на основе собственности; поэтому общество легко принимает практику использования лица в качестве биометрического идентификатора;

– системы распознавания лиц наименее заметны при получении образца, они не требуют ни физического контакта, ни осведомленности объекта;

– для распознавания лиц могут использоваться существующие базы данных фотографий, видеокассет или других носителей;

– распознавание лица, по крайней мере теоретически, может проводиться путем сортировки людей в толпе без их желания и в реальном времени;

– данный биометрический идентификатор прекрасно подходит для верификационных приложений, работающих с небольшими группами людей.

Недостатки биометрического параметра:

– при получении биометрических образцов для автоматизированных аутентификационных систем лицо должно быть хорошо освещено контролируемыми источниками света. Это только первая проблема в длинном списке технических трудностей;

– лицо как биометрический параметр плохо подходит для чистого идентификационного протокола. Этот параметр лучше применять для верификации, когда не требуется очень высокая точность результатов;

– обмануть распознающую систему можно при помощи маскировки, что может стать причиной ложных отрицаний в приложениях сортировки, т. е. нежелательная замаскированная личность не будет идентифицирована;

– существуют и некоторые негативные ассоциации с преступным миром, так как изображения лиц уже долгое время применяются при создании картотек преступников. Тем не менее изображение лица традиционно широко используется для паспортов, билетов и т. д.

6.5.3. Голос

Преимущества биометрического параметра:

– как и лицо, голос является «натуральным биометрическим параметром» – одним из тех, которые люди применяют, чтобы идентифицировать друг друга; при определенных обстоятельствах (телефонная связь), решения, принимаемые машиной, могут быть проверены относительно неквалифицированным оператором;

– образцы голоса, как и изображение лица, могут быть получены абсолютно незаметно;

– общество легко принимает голос как биометрический идентификатор, частично из-за его натуральности, частично из-за того, что он не ассоциируется с криминальным миром;

– для обработки голоса не требуется дорогое оборудование, с ним легко работать, используя повсеместно распространенную телекоммуникационную инфраструктуру. Поэтому голос хорошо подходит для систем безопасности;

– голос позволяет использовать инкрементальные аутентификационные протоколы. Например, протокол может предписывать получение большего количества голосовой информации, когда требуется боле высокий уровень конфиденциальности;

– голос как биометрический идентификатор работает более точно и громко, когда сочетается с верификацией посредством знаний; в аутентификационном протоколе это называется разговорным биометрическим параметром;

– голос позволяет проводить проверку личности на протяжении некоторого периода времени, т. е. голос можно аутентифицировать в течение всего разговора.

Недостатки биометрического параметра:

– существует вероятность имитации голоса профессиональным мошенником. Эта проблема еще недостаточно хорошо исследована; в отличие от подписи для голоса не существует тестов для изучения реальных злоумышленников;

– по мере улучшения устройств искусственного синтеза речи [40] становится все более возможным создание несуществующих личностей с машинными голосами (когда регистрация и аутентификация происходят на расстоянии). Обучаемые устройства синтеза речи позволят создать автоматические системы, которые смогут имитировать голос конкретного человека, говорящего заданный текст;

– распознавание голоса зависит от качества аудиосигнала. Системы идентификации говорящего нечувствительны к фоновому шуму, канальному шуму (шуму телефонных линий, радиоволн или компрессии) и искажениям, создаваемым микрофонами;

– некоторые люди не могут говорить по причине болезней, физических недостатков или психических расстройств, глухоты, а также из-за временной потери голоса.

6.5.4. Радужная оболочка глаза

Преимущества биометрического параметра:

– радужная оболочка сейчас считается наиболее точным биометрическим параметром, особенно когда подсчитываются ЛД. При обработке радужной оболочки возникает очень мало случаев ложного доступа, поэтому она хорошо подходит для чистой идентификации;

– получение образца радужной оболочки происходит незаметно на расстоянии при помощи камер, считывание осуществляется без физического контакта и особого неудобства для пользователя;

– с радужной оболочкой не связано негативных ассоциаций, ее отличает высокая степень одобрения пользователей. В том числе и потому, что она никогда не использовалась в судебной экспертизе;

– продавцы утверждают, что обучение системы распознавания радужки не требует больших затрат. Как было отмечено выше, хотя регистрация – это основная часть тренировки системы, она не обладает теми преимуществами, которыми должна обладать.

Недостатки биометрического параметра:

– существует очень мало действующих баз данных радужных оболочек. Так как на данный момент нет инфраструктуры, необходимой для создания систем аутентификации по радужной оболочке, подобный проект потребует очень больших денежных вложений. Хотя радужка может быть хорошим биометрическим параметром для идентификации, крупномасштабные исследования в этой области затруднены из-за отсутствия тестовых баз данных;

– так как радужная оболочка имеет маленький размер, для получения ее образца требуется больше усилий со стороны пользователя или применение дорогостоящего оборудования;

– из-за очков или контактных линз проведение аутентификации радужной оболочки может быть затруднено; объект должен будет их снять;

– радужную оболочку нельзя использовать при расследовании преступлений;

– есть люди, которые потеряли один или оба глаза, а также люди, которые не могут контролировать свои моторные реакции, поэтому они не смогут быть зарегистрированы в такой системе.

6.5.5. Рука

Преимущества биометрического параметра:

– похоже, что этот параметр уже является признанным, потому что он используется для верификации в Диснейворлде, в Службе иммиграции и натурализации США, а также в различных университетах, например в Университете Джорджии;

– считается, что измерение геометрии руки является простой операцией;

– проведена по крайней мере одна сценарная оценка геометрии руки как биометрического параметра [41], результаты которой показывают: она является подходящим биометрическим параметром для верификации. Хотя о свойственных этому параметру коэффициентах ошибок известно довольно мало;

– геометрия руки, являясь относительно слабым биометрическим параметром, может быть использована для верификации в обстоятельствах, когда более сильные параметры могут причинять излишние неудобства пользователям.

Недостатки биометрического параметра:

– как и в случае с отпечатками пальцев, для получения образцов нужно прижать руку к поверхности сенсора (хотя есть и другие способы). Такой метод может вызвать опасения по поводу гигиены;

– существует всего одна сценарная оценка геометрии руки как биометрического параметра. Ученые спорят о том, действительно ли геометрия руки является биометрическим параметром;

– некоторые люди по разным причинам потеряли руку или пальцы.

6.5.6. Подпись

Преимущества биометрического параметра:

– подпись является биометрическим параметром, создаваемым человеком; методы ее подделки хорошо изучены, поэтому подделку можно определить, даже когда ее делает опытный мошенник;

– на стадии регистрации уже существует некоторая возможность определить подделанную подпись;

– обучение происходит быстро, и люди понимают (так же, как и в технологиях распознавания речи), что система должны быть обучена, интуитивно понимают, как нужно зарегистрироваться, чтобы не получить ложный доступ;

– верификация подписи проходит быстро, а для хранения шаблонов требуется мало места;

– на верификацию подписи не влияет язык, на котором говорит объект;

– подпись, по сути, является комбинацией информации и биометрического параметра, информационная компонента (что и как написано) может быть изменена пользователем;

– сильное сжатие не влияет на качество образца подписи (даже при размере 100–150 байт).

Недостатки биометрического параметра:

– практика ставить подписи на документах широко распространена во всем мире. Это наводит на мысль, что подпись является недостаточно надежным параметром для защиты аэропортов и т. д.;

– индивидуальные особенности подписей хорошо изучены, в том числе на основе качественных подделок. К сожалению, тестирования систем распознавания подписи проводятся недостаточно аккуратно, и их результаты не позволяют сделать выводы о масштабируемости подписи как биометрического параметра;

– для достижения желаемой точности необходимо применять ручку, пишущую в пятимерном пространстве, которая фиксирует давление и угол наклона. Это дорогостоящее оборудование. Эффективность использования подписи для контроля доступа при сегодняшнем состоянии технологий не изучена;

– некоторые люди страдают от паралича, а другие не имеют хороших моторных реакций для координации письма.

6.6. Биометрические мифы и ошибочные представления

Ниже приведен список некоторых наиболее распространенных мифов и ошибочных представлений, которые распространились, возможно, благодаря как противникам, так и сторонникам биометрии.

Биометрический параметр *X* является наилучшим для любых приложений

Не существует одного параметра, подходящего для всех случаев. Каждое приложение или сценарий имеют множество характеристик, включая цену, точность, удобство и одобрение пользователей. Мы рассмотрели их в этой главе.

Биометрический параметр *X* является уникальным для каждого человека

Отличительные особенности тела человека, называемые биометрическими параметрами, обусловлены наследственностью и изменениями в процессе развития. Количество вариаций каждой из генетических переменных или особенностей развития изменяется от одного биометрического параметра к другому, такое случайное развитие индивидуальных особенностей позволяет говорить об их уникальности, если их изучать достаточно основательно.

В данном учебно-методическом пособии рассматриваются определенные технологии идентификации со свойственными им ограничениями, обусловленными особенностями процесса получения образцов, требованиями к хранению шаблонов, методами сравнения считываемой информации, а также изменчивостью биометрических параметров во времени. Как невозможно найти двух людей с одинаковыми

биометрическими репрезентациями, так же нереально, что из двух образцов биометрических параметров одного и того же человека получатся одинаковые репрезентации. Эта проблема решается при помощи «толерантности», что позволяет сопоставить биометрические параметры, вместо того чтобы измерять шум или временные изменения, но одновременно и повышает вероятность совпадения биометрических репрезентаций разных людей, таким образом нивелируя понятие уникальности биометрических параметров.

Одно число может измерить точность работы системы

Если бы это было так, то сравнение систем было бы простой операцией. В биометрической системе всегда присутствует компромисс между разными видами ошибок. Следовательно, существуют рабочие области для разных типов мэтчеров. Отмечено, что один мэтчер может быть лучше другого в одной рабочей области и хуже в другой.

Таким единственным числом может быть, например, коэффициент равных ошибок (КРО) – рабочая точка, в которой КЛД = КЛОД = КРО.

Наша система – это система «подключи и работай»

Биометрическая аутентификационная система разработана и обучена на основе баз данных биометрических образцов. Такая система при установке может функционировать с определенной точностью. Однако настройка системы на работу с определенным считывающим устройством и на конкретные условия получения образцов, а также обучение системы в процессе эксплуатации повышают точность работы приложения.

Реальную точность работы системы можно предсказать

Как было отмечено выше, система должна быть обучена на тренировочных биометрических данных. Лучше всего обучать систему на данных, которые получены от реальной популяции пользователей при обстоятельствах, в которых будет работать система.

Для предсказания точности работы системы необходимо было бы создать точную модель популяции пользователей и окружающей среды. Такие модели невозможно создать на основе доступных баз данных и даже тестовая эксплуатация не позволяет смоделировать все обстоятельства, которые могут возникнуть в процессе работы системы.

Системы с лучшими КЛД и КЛОД – самые точные

Поставщики решений и энтузиасты слишком часто объявляют о новых рекордах точности работы систем, которые могут ввести в заблуждение.

Во-первых, данные, используемые для оценки точности работы системы, могут быть получены в неестественных контролируемых условиях. Самым простым способом получить объективные оценки является тестирование с применением общедоступных баз данных. Во-вторых, когда результаты предоставляются на основе стандартного набора данных, они часто получаются не на полном наборе данных, а на подмножествах; кроме того, они могут быть получены без соблюдения стандартного тестового протокола. Может выясниться, что эти подмножества отобраны

на основе непродуманных критериев, тогда результаты нельзя обобщать на всю базу данных.

Несколько биометрических параметров лучше, чем один

Считается, что биометрическая идентификация человека может потенциально выиграть от использования нескольких биометрических параметров и образцов во время процесса идентификации. На самом деле вовсе не обязательно, что от этого улучшится скорость/цена/точность работы системы.

Наша биометрическая система не использует пороговую величину принятия решения

Любая система нуждается в критерии, который бы позволил определить, когда два биометрических образца получены от одного объекта. Определить его можно при помощи тестовой или обучающей настройки. Обучение системы само по себе устанавливает оптимальную пороговую величину принятия решения.

Наш экстрактор свойств может использоваться в любом устройстве

Этот вопрос особенно актуален для систем распознавания отпечатков пальцев, многие из которых используют похожие репрезентации деталей для идентификации. Несмотря на кажущееся сходство, разные алгоритмы извлечения черт дают несколько отличающиеся результаты. Следовательно, алгоритмы извлечения свойств и устройства сопоставления лучше всего разрабатывать совместно, настраивая друг на друга.

Большие шаблоны повышают точность сопоставления

Размер репрезентации биометрического идентификатора редко влияет на точность работы; единственным значимым фактором для точности системы является величина перекрытия переменных биометрических идентификаторов, полученных от разных людей, а также то, насколько личный идентификатор остается неизменным (например, запись роста человека с точностью до миллиметра не помогает его идентифицировать).

Распознавание лиц может предотвратить терроризм

Технологии распознавания лица на данный момент еще недостаточно разработаны. Сравнение пассажиров со списком «разыскиваемых преступников» ведет только к появлению большого количества случаев ложного признания. Было проведено несколько тестов на распознавания лиц в аэропортах и других публичных местах в США [42, 43], которые показали, что эти технологии требуют дальнейших исследований.

Использование биометрических параметров означает 100-процентную безопасность

Обычные биометрические мэтчеры несовершенны, и это статистически гарантирует, что при большом количестве вводимых подделок система пропустит некоторые из них. Ни одна система не защищена на 100 %, особенно если учесть вероятность атак, совершаемых профессиональными злоумышленниками которые

используют различные методы, такие, как социальная инженерия, заговоры и принуждение.

Биометрические системы не угрожают конфиденциальности

Конфиденциальность может поддерживаться технологией, но не гарантироваться ею. Соблюдение тайны зависит от стратегии поведения системы. Это не означает, что использование биометрических параметров не может способствовать защите секретной информации. Хорошо разработанная биометрическая система работает на основе продуманных процедур, которые действительно защищают права пользователей.

Биометрические системы нарушают конфиденциальность

Многие люди боятся, что биометрия, обещающая идеальную идентификацию, на самом деле нарушает их право на конфиденциальность. Биометрические системы действительно могут быть использованы в тоталитарных обществах, однако от конкретной биометрической системы, политики страны и законодательства будет зависеть, насколько процедуры идентификации будут нарушать конфиденциальность. На практике биометрические технологии могут применяться для защиты секретной информации, например путем использования дополнительных способов защиты информации о состоянии здоровья или путем проведения аутентификации без раскрытия личных данных. Эти способы позволяют сохранить конфиденциальность в отличие от широко распространенных методов идентификации по номеру социального страхования, девичьей фамилии матери или по водительскому удостоверению (что дополнительно дает доступ к адресу и дате рождения).

Биометрические сенсоры негигиеничны или даже вредны

Многие биометрические сенсоры требуют физического контакта, но соприкосновение с ними не более опасно с точки зрения гигиены, чем контакт с деньгами, клавиатурой, дверными ручками и т.д. Сканеры радужной оболочки и сетчатки светят в глаз лазером, а системы, использующие обычное освещение, тем более не могут нанести вред.

ЗАКЛЮЧЕНИЕ

Распознавание людей – это вид деятельности, который составляет основу нашего общества и культуры, так как для многих видов приложений необходимым условием является гарантия идентичности личности и ее авторизация. Биометрическая идентификация, или биометрия, основана на идентификации отличительных признаков человека.

По мере того как компьютеризированные методы аутентификации становятся все более востребованными, автоматическое распознавание лица, пальцев, голоса и т. д. начинает применяться все более широко.

С одной стороны, технологии биометрии могут представлять угрозу для частной жизни, но, с другой стороны, они используются при разработке современных решений, предназначенных для защиты конфиденциальной информации. Биометрия как наука и как прикладная технология становится все более востребованной.

ЛИТЕРАТУРА

1. B. Miller. Vital signs of identity. IEEE Spectrum, 31 (2) : 22–30,1994.

2. R. Clarke. Human identification in information systems: Management challenges and public policy issues. Information Technology & People, 7(4) : 6–37, December 1994.

3. R. M. Bolle, J. H. Connell, S. Pankanti and N. Ratha. On the security of biometrics authentication. IBM Technical Report, 2002.

4. C. P. Pfleeger. Security in Computing. Prentice Hall PTR, Upper Saddle River, NJ, 1996.

5. C. Simon and I. Goldstein. A new scientific method of identification. New York State Journal of Medicine, 35(18), September 1935.

6. A. K. Jain, L. Hong and R. M. Bolle. On-line fingerprint verification. IEEE Transanctions on Pattern Analysis and Machine Intelligence, 19(04):302-313, April 1997.

7. J. L. Wayman. A scientific approach to evaluating biometric systems using mathematical methodology In Proceedings of CardTech/SecureTech., P. 477–492, Orlando, FL, May 1997.

8. W. W. Peterson, T. G. Birdsall and W. C. Fox. The theory of signal delectability. Transactions of the IRE, PGIT-4 : 171–212, April 1954.

9. J. L. Wayman. National Biometric Test Center Collected Works. National Biometric Test Center, San Jose, CA, August 2000.

10. Biometrics Working Group. Best practices in testing and reporting performance of biometric devices, http : //www.afb.org.uk/bwg/bestprac.html, 2000.

11. A. K. Jain, R. M. Bolle and S. Pankanti (Eds.). Introduction to biometrics (Chapter 1). In A. K. Jain, R. M. Bolle and S. Pankanti, editors, Biometrics: Personal Identification in Networked Society, P. 1–41. Kluwer Academic Publishers, Boston, MA, 1999.

12. R. M. Bolle, J. H. Connell and N. K. Ratha. Biometric perils and patches. Pattern Recognition, (12) : 2727–2738, December 2002.

13. N. Ratha, J. H. Connell and R. M. Bolle. An analysis of minutiae matching strength. In J. Bigun and F. Smeraldi, editors, Proceedings 3rd IEEE International Conference on Audio- and Video-Based Biometric Person Authentication, P. 223–228. Springer Verlag, Heidelberg Berlin, June 2001.

14. A. K. Jain, L. Hong and S. Pankanti. Biometrics identification. Communications of the ACM, 43(2) : 91–98, 2000.

15. R. Germain. Large scale systems. In A. K. Jain, R. M. Bolle and S. Pankanti, editors, Biometrics: Personal Identification in Networked Society, P. 311–326. Kluwer Academic Press, Boston, MA, 1999.

16. N. Ratha and R. Bolle. Smartcard based authentication. In A. Jain, R. Bolle and S. Pankanti, editors, Biometrics, Personal Identification in Networked Society, P. 369–384. Kluwer Academic Publishers, Boston, MA, 1999.

17. D. Setlak. Fingerprint sensor having spoof reduction features and related methods. US Patent Number : 5, 953, 441, September 1999.

18. T. Matsumoto, H. Matsumoto, K. Yamada and S. Hoshino. Impact of artificial «gummy» fingers on fingerprint systems. In Proceedings ofSPIE Vol. #4677, Optical Security and Counterfeit Deterrence Techniques IV, P. 244–251, January 2002.

19. I. Kansala and P. Tikkanen. Security risk analysis of fingerprint based verification in PDAs. In Proc. IEEEAutoID 2002, P. 76–82, Tarrytown, NY, March 2002.

20. A. Kong, A. Griffith, D. Rhude, G. Bacon and S. Shahs. Department of Defence & Federal Biometric System Protection Profile for Medium Robustness Environments. Technical Report Draft Version 0.02, US Department of Defence, March 2002.

21. H. S. M. Beigi, S. H. Maes, U. V. Chaudhari and J. S. Sorensen. IBM model-based and frame-by-frame speaker recognition. In Speaker Recognition and its Commercial and Forensic Appications, Avignon, April 1998.

22. R. Donovan. Trainable Speech Synthesis. PhD thesis, Cambridge University, Engineering Department, Cambridge, UK, 1996.

23. H. P. Graf. Sample-based synthesis of talking heads. In Proc. IEEE ICCV Workshop Recognition, Analysis, and Tracking of Faces and Gestures in Real-Time Systems, P. 3–7, Vancouver, BC, July 2001.

24. C. Dorai, N. Ratha, and R. M. Bolle. Detecting dynamic behavior in compressed fingerprint videos: Distortion. In Proc. IEEE Computer Vision and Pattern Recognition, P. 320–326, June 2000.

25. R. Hill. Retina identification. In A. K. Jain, R. M. Bolle and S. Pankanti, editors, Biometrics: Personal Identification in Networked Society, P. 123–142. KJuwer Academic Press, Boston, 1999.

26. N. K. Ratha, J. H. Connell and R. M. Bolle. Enhancing security and privacy in biometrics-based authentication systems. IBM Systems Journal, 40(3) : 614–634, 2001.

27. W. Bicz, Z. Gurnienny and M. Pluta. Ultrsound sensor for fingerprints recognition. In Proc. of SPIE, Vol. 2634, Optoelectronic and electronic sensors, P. 104–111, June 1995.

28. T. Rowley. Silicon fingerprint readers: A solid state approach to biometrics. In Proc. of the CardTech/SecureTech, Orlando, FL, Vol. 1, P. 152–159, Washington D. C., May 1997.

29. S. J. McPhee, M. A. Papadakis, L. M. Tierney and R. Gonzales, editors. Current medical diagnosis and treatment. Appleton and Lange, Stamford, CT, 1997.

30. N. K. Ratha, J. H. Connell and R. M. Bolle. Biometrics break-ins and band-aids. Pattern Recognition Letters, 24(13) : 2105–2113, September 2002.

31. R. M. Bolle, N. Ratha and J. H. Connell. Biometric authentication: Security and privacy. In Proc. 1st Workshop on Pattern Recognition in Information Systems, PRIS 2001, P. 2–11. ICEIS PRESS, July 2001.

32. B. Fader. Note: Apply moisterizer only after gaining access. New York Times, February, 24, P. C5, 2003.

33. T. Ruggles. Comparison of biometric techniques. Technical report, The California State Legislature, http://biometric-consulting.com/bio.htm, April 1996. Revised May 8, 2001.

34. G. C. Stockman, S. Kopstein and S. Benett. Matching images to models for registration and object detection via clustering. IEEE Transanctions on Pattern Analysis and Machine Intelligence, 4(3) : 229–241, May 1982.

35. J. P. Campbell (Ed.). NIST 1999 Speaker Recognition Workshop. Digital Signal Processing, 10(1–3), January/April/July 2000.

36. M. Przybocki and A. Martin. The 1999 NIST Speaker Recognition Evaluation Speaker Detection and Speaker Tracking. EUROSPEECH 99 6th European Conference on Speech Communication and Technology, Budapest, Hungary, September 1999.

37. D. Maio, D. Maltoni, R. Cappelli, J. L. Wayman and A. K. Jain. FVC2000: Fingerprint verification competition. IEEE Transactions on Pattern Analysis and Machine Intelligence, 24(3) : 402–412, 2002.

38. G. Doddington, W. Liggett, A. Martin, M. Przybocki and D. Reynolds. Sheep, goats, lambs and wolves: A statistical analysis of speaker performance. In Proceedings of IC-SLD'98, NIST 1998 speaker recognition evaluation, Sydney, Australia, November 1998.

39. FBI, U.S. Department of Justice, Washington, D.C. 20402. The Science of Fingerprints, Classification and Uses, 1984.

40. R. W. Sproat. Multilingual Text-to-Speech Synthesis: The Bell Labs Approach, Lucent Technologies Staff, Bell Laboratories, Lucent Technologies, Murray Hill, NJ, USA. Kluwer Academic Publishers, Boston, MA, October 1997.

41. T. Mansfield, G. Kelly, D. Chandler and J. Kane. Biometric product testing final report. Technical Report CESG Contract X92A/4009309, Centre for Mathematics and Scientific Computing, National Physics Laboratory, Middlesex, UK, March 2001.

42. ACLU Reports. Drawing a blank: Tampa police records reveal poor performance of face-recognition technology. January 2002.

43. J. Scheeres. Airport Face Scanner Failed, http://www.wired.eom/news/privacy/0, 1848,52563,OO.html, May 2002.

Св. план 2012, поз. 49

Учебное издание

Прудник Александр Михайлович
Власова Галина Александровна
Рощупкин Яков Викторович

БИОМЕТРИЧЕСКИЕ МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ

УЧЕБНО-МЕТОДИЧЕСКОЕ ПОСОБИЕ

Редакторы *Т. П. Андрейченко, Е. С. Чайковская*
Корректор *Е. Н. Батурчик*
Компьютерная правка, оригинал-макет *В. М. Задоля*

Подписано в печать 22.09.2014. Формат 60×84 1/16. Бумага офсетная. Гарнитура «Таймс».
Отпечатано на ризографе. Усл. печ. л. 7,32. Уч.-изд. л. 7,5. Тираж 100 экз. Заказ 346.

Издатель и полиграфическое исполнение: учреждение образования
«Белорусский государственный университет информатики и радиоэлектроники».
Свидетельство о государственной регистрации издателя, изготовителя,
распространителя печатных изданий №1/238 от 24.03.2014,
№2/113 от 07.04.2014, №3/615 от 07.04.2014.
ЛП №02330/264 от 14.04.2014.
220013, Минск, П. Бровки, 6