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

Принципы построения систем биометрической аутентификации

Construction Principles of Biometric Authentication Systems

Зиятдинов Андрей Ильгисович, 112гр.

МФТИ, 2005

Содержание:

1.**Введение.**

Биометрия возникла в конце XIX века как наука, рассматривающая количественные биологические эксперименты с использованием статистических методов.Появление биометрических систем безопасности повлекло за собой повышение интереса к этой науке. Биометрия в первом приближении это конгломерат автоматизированных методов и инструментов идентификации личности путем измерения уникальных физиологических или поведенческих особенностей и их сравнения с эталонами, находящихся в отдельных базах данных.

Биометрические устройства аутентификации существуют уже около двадцати лет. За это время они существенно подешевели. На рынке имеется множество систем биоидентификации,их стоимость варьируется от нескольких десятков до нескольких миллионов долларов. Кроме этого расетет необходимость в системах идентификации человека.

Прежде чем двигаться дальше,обозначим цели,которые автор преследует в своем эссе:

- Предствавить сжатую, но необходимую информацию о биометрических системах,взяв ее из многочисленных источников.Основываясь на ней достигнуть остальных целей.
- Дать критерии(принципы) построения биометрических систем согласно общим критериям создания классических криптографических систем и с учетом специфики биоометрики.
- Обозначить сложившуюся сложность стандартизации биометрических систем,что мешат постановке общих принципов построения таких систем.
- Показать пример сложной биометрической системы и проверить на ней выполнимость выявленных принципов.

2.Основные понятия,термины.

Приведем некоторые определения и термины[7]:

- Биометрия (Biometrics) – прикладная область знаний, использующая при создании различных автоматических систем разграничения доступа уникальные признаки, присущие каждому отдельному человеку.
- Биометрические характеристики (Biometric Parameters) – признаки, присущие каждому отдельному человеку и уникальные для каждого человека.
- Биометрический образец (Biometric Sample) – наблюдение выбранной биометрической характеристики.
- Идентификация (Identification) - это проверка наличия предъявляемого идентификатора в списке зарегистрированных.
- Аутентификация (Authentication) - это проверка принадлежности пользователю (человеку) предъявленного им идентификатора

Термины «индентификация» и «аутентификация» в биометрии близки по смыслу и применимости, поэтому мы будем использовать один из терминов,а именно «индентификация» (Identification).

- Ошибка первого рода (FRR – False Rejection Rate) «не узнать своего», т.е. принимается решение «чужой», хотя на самом деле субъект присутствует в списке зарегистрированных пользователей.
- Ошибка второго рода (FAR – False Acceptance Rate) «пропустить чужого», т.е. принимается решение «свой», хотя, на самом деле, субъект отсутствует в списке зарегистрированных пользователей.

- Ошибка третьего рода, это прочие ошибки. Например, когда принимается решение «чужой», но не по результату сравнения, а по причине невозможности получить изображение папиллярного рисунка дактилоскопическим сканером.[7]

3.Методы биометрической аунтефикации.

На рисунке 1 представлены наиболее распостраненные методы биометрической аунтефикации.

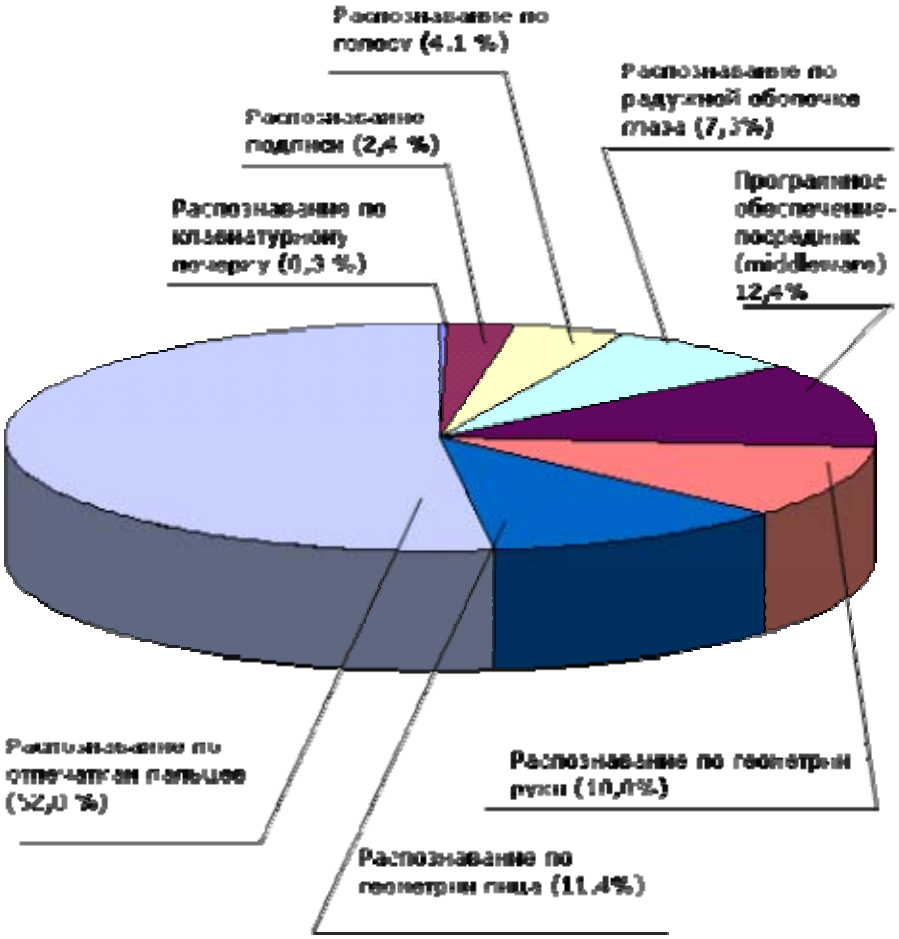

Рис.1

На этом ограничимся в освещении методов биометрической аунтефикации,тем более в задача эссе состоит не в этом.

4. Примеры использования систем биометрической аунтефикации.

Исторически примитивные биометрические системы появились в криминалистике(аунтификация отпечатков пальцев).На сегодняшний день диапазон использования таких систем расширился согласно все новым потребностям человека и компьютеризации[6].

- системы управления доступом;
- информационная безопасность (доступ в сеть, вход на ПК);
- учет рабочего времени и регистрация посетителей;
- системы голосования;
- проведение электронных платежей;

- аутентификация на Web-ресурсах;
- различные социальные проекты, где требуется идентификация людей (благотворительные акции и т. д.);
- проекты гражданской идентификации (пересечение государственных границ, выдача виз на посещение страны и т.п.).

5.Общие прицины работы.

Методы биометрической идентификации должны по своей сути удовлетворять следующим критериям:

- Признак идентификации человека является уникальным, присущим только ему.
- У любого человека должен быть данный признак, по которому можно осуществлять идентификацию.

Однако ничто не совершенно в нашем мире. Существующие алгоритмы идентификации не могут полностью удовлетворить этим требованиям. Поэтому используют оценки надежности для существующих методов.

Ошибки идентификации бывают двух типов:

- Ошибка первого рода, False Reject Rate, FRR
- Ошибка второго рода, False Accept Rate, FAR

За то, какая ошибка будет встречаться в данной системе чаще всего, отвечает чувствительность данной системы, чем она больше, тем дольше будут обрабатываться результаты и тем вероятнее будет ложный отказ. Если же чувствительность будет слишком низкая, то будет возрастать вероятность допуска ненужного человека. Все существующие системы биометрической идентификации являются компромиссом в выборе соответствующей чувствительности прибора. Кроме того, какими-то характерными вероятностями возникновения той или иной ошибки обладают различные методы.

К сожалению, пока не выработана единая система оценки надежности биометрических систем, поэтому трудно, а иногда даже некорректно сравнивать надежность различных методов. Пока возможно только субъективное сравнение различных методов, т.е. только опытным путем убеждаться в их надежности или нет.

Все существующие методы можно разделить на три группы:

- Статические методы, основанные на распознавании каких-либо физиологических и генетических признаков человека, которые присуще только ему и являются неотъемлемыми. Например: сравнение структур ДНК, распознавания отпечатков пальцев, сетчатки глаза, формы лица и т.д.
- Динамические методы, основанные на распознавании поведенческих (динамических) характеристик человека, таких как динамика печати на клавиатуре, динамика подписи, речь и т.д.
- Комбинационные методы,совмещение первых двух.Обладает большей надежностью. [7]

6. Постановка проблемы построения биометрических систем.

В предыдущем пункте была выявлена принципиальная проблема – нет единой системы определения надежности биометрической системы,главной ее

характеристики.Это заставляет разработчиков все время искать компромисс, «играя» чувствительностью системы.Поэтому существуют такие зарактеристики как FRR и FAR.

Кроме того, интероперабельности в биометрической аутентификации до сих пор не существует, несмотря на старания консорциума BioAPI Consortium выработать стандартные интерфейсы для интеграции биометрических систем.

Это все значительно осложняет разработку данных систем.

Далее попробуем обозначить этапы построения биометрических систем аунтефикации и рассмотреть конкретный пример.

7.Этапы(принципы) построения ситемы биометрической аунтефикации.

Чтобы рещить задачу биометрической идентификации, исследователи (научные работники) и разработчики биометрических систем (инженеры) разбивают ее на несколько этапов. При биометрической идентификации в широком смысле должен быть решен ряд весьма важных вопросов,являющимися по своей сути принципами построения таких систем[1,4]:

- Обозначить вид контролируемых биометрических параметров.
- Избрать метод измерения контролируемых биометрических параметров.
- Определить математические преобразования (представления), позволяющие эффективно извлекать биометрические данные из исходной измерительной информации
- Построить математическая модель, увязывающая между собой стабильную и нестабильную часть контролируемых биометрических параметров
- Выбрать состав принимаемых во внимание биометрических параметров в разрабатываемой системе
- Четко определен вид решающего правила и заданы его параметры
- Произвести статистическую оценку уровней ошибок первого и второго рода для среднестатистического пользователя разрабатываемой биометрической системы

8. Пример сложной биометрической системы ,на которой отслежены основные принципы построения таких систем.

В качестве примера возмем метод хранения ключевой информации на основе смешивания ключевой и биометрической информации[5].

Требования к рассматриваемой системе

- значительная вычислительная сложность получения криптографического ключа без соответствующих биометрических параметров;
- сложность получения криптографического ключа, не основанная на секретности алгоритма;
- высокая точность восстановления ключевой информации при известных биометрических параметрах;
- скорость восстановления ключевой информации.

Зная это,попробуем отследить этапы(принципы) построения этой системы,см. п. 7.

Видно,какие парметры биометрической части ситемы будут важны : FRR , FAR.

Из общего характера требований к системе следует, что для определенности в качестве биометрического признака выберем голосовой пароль. Голосовой пароль имеет значительную область применения, возможность использования простой аппаратуры для регистрации голоса, возможность смены скомпрометированного голосового пароля и т.д.

Для оцифровки аналогового речевого сигнала использовался метод импульсно-кодовой модуляции (PCM) с частотой дискретизации порядка 11 КГц и размером отсчета N=16 бит.Удаление пауз и шумных сегментов. Оцифрованный сигнал содержит сложную смесь различных фонем произнесенного слова, пауз и фоновых шумов. Известно, что в задаче идентификации диктора шумные звуки и паузы являются неинформативными и должны быть удалены

Метод может быть описан следующим образом. Существует два этапа функционирования метода - регистрация и аутентификация пользователя.На рис. 2 представлен процесс аутентификации

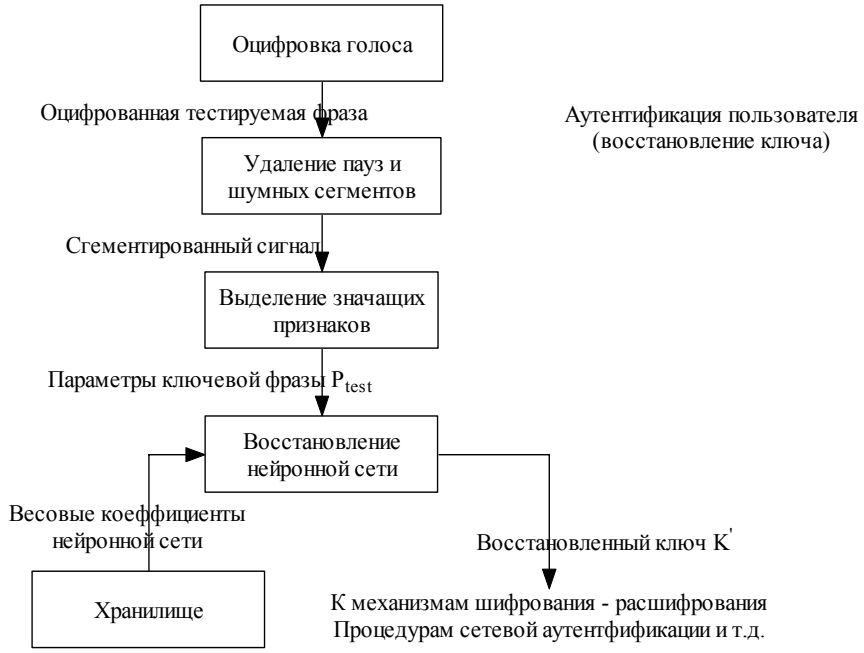

Рис. 2

Что касается мат. метода, использована нейронная сеть с архитектурой MLP с различными алгоритмами обучения на основе обратного распространения ошибки.

За более побробной информацией обращатьс к источнику [5].

Итак, проанализируем полученный для данной системы результаты:

$FAR = 2.4 \cdot 10^{-13}$,

$FRR = 0.4770$,

Время выполнения процесса регистрации ≈ 1430 с.

Объем памяти хранения параметров нейронной сети 160 Кб.

Время выполнения аутентификации = 0.9 с

и сделаем соответсвующи вводы.

9.Заключение.

Системы биометрической аунтефикации черезвычайно подходят для задач,где требуются сложность получения информации и высокая точность ее восстановления,что подтверждает сам (превосходный!)результат $FAR = 2.4 \cdot 10^{-13}$.Однако при это ошибка «пропустить чужого» достаточно велика : $FRR = 0.4770$.Зачеченное расхождение говорит лишь о том,что универсальных биометрических систем, как и глобальных принципов их построения в плане надежности, пока не существует.

Но с другой стороны,для прикладных задач(например,рассмотренная в [5]),биометрика просто незаменимый интструмент.

Отметим также сугубо инженерную сложность совместимости и интеграции.Это я вляется проблемой рассмотренной системы в частости и общей проблемой в проектировании всех систем биометрической аунтефикации.

10. Ссылки на литературу:

1. Презентации по распознаванию отпечатков пальцев: распознавание http://re.mipt.ru/infsec/2005/handout/2005_Fingerprint_Chernomordik/2005_Fingerprint_recognition__Chernomordik.ppt
2. 2002 CSI/FBI Computer Crime and Security Survey, Richard Power: http://www.gocsi.com/press/20020407.html
3. DigitalPersona White Paper Guide to Fingerprint Identification :www.digitalpersona.com
4. Режимы биометрической идентификации и аутентификации по аналогии с классической идентификацией : http://biometr.chat.ru/GL-1/3/m_42.html
5. Доклад Республиканской научно-практической конференции «Современные управляющие и информационные системы», посвященной 60-летию Академии наук Республики Узбекистан (г. Ташкент, 2-3 октября 2003 г.) : http://www.bilimdon.uz/library/publ.php?s=view&id=182
6. http://www.bre.ru/security
7. http://www.bellabs.ru/SF/Biometry.html