

МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ
Белорусский национальный технический университет

Перспективные методы биометрической аутентификации и идентификации

Учебно-методическое пособие по дисциплине
“Информатика человека и биосистем”
для студентов специальностей

1-55 01 01 “Интеллектуальные приборы, машины и производства”,
1-55 01 02 “Интегральные сенсорные системы”

Учебное электронное издание

Минск ◊ БНТУ ◊ 2009

Авторы:

*В. М. Колешко
Е. А. Воробей
П. М. Азизов
А. А. Худницкий
С. А. Снигирев*

Рецензенты:

Л.М. Лыньков, зав. кафедрой «Защита информации» БГУИР,
профессор, доктор технических наук;
Н.Н. Мурашко, зав. лабораторией Объединенного института проблем
информатики НАН Беларуси, доцент, кандидат технических наук

Учебно-методическое пособие содержит материал для изучения студентами кафедры “Интеллектуальные системы” дисциплины “Информатика человека и биосистем”, который открывает студентам на основе анализа информатики человека, биосистем и изучения природы функциональности информационных процессов в живых организмах перспективные направления исследования, интеллектуальные разработки и методы распознавания многомерных сенсорных образов для систем суперзащиты биометрической аутентификации и идентификации личности. Изложена характеристика перспективных направлений биометрии биосигналов организма и генетического портрета личности с подробным описанием принципов регистрации, обработки и анализа сложных биоинформационных образов, которые полностью защищены от фальсификации эталонной базы данных или имитационных моделей биометрических характеристик в информационных и коммуникационных технологиях, показаны проблемы современной биометрии и пути их преодоления для создания недорогих надежных интеллектуальных систем суперзащиты личности. Представленный материал раскрывает творческий потенциал студентов в направлении изучения информатики человека для разработки и моделирования интегральных сенсорных и интеллектуальных систем.

Белорусский национальный технический университет
пр-т Независимости, 65, г. Минск, Республика Беларусь
Тел. (017) 292-77-52 факс (017) 292-91-37
E-mail: isev@tut.by
Регистрационный № БНТУ/МСФ82 – 2.2009

© БНТУ, 2009

© Колешко В. М., Воробей Е. А., Азизов П. М.,
Худницкий А. А., Снигирев С. А. 2009

СОДЕРЖАНИЕ

| | | |
|-------|-----------------------------------------------------------------------------------------------------------------------------|----|
| 1 | ПЕРСПЕКТИВНЫЕ МЕТОДЫ БИОМЕТРИЧЕСКОЙ ИДЕНТИФИКАЦИИ ЛИЧНОСТИ | 4 |
| 1.1 | Запах тела | 4 |
| 1.1.1 | Происхождение характеристики..... | 4 |
| 1.1.2 | Универсальность, уникальность, постоянство, собираемость | 5 |
| 1.1.3 | Методы идентификации (сбор, обработка и сравнение)..... | 7 |
| 1.1.4 | Перспективы использования электронных носов..... | 14 |
| 1.1.5 | Достоинства | 17 |
| 1.1.6 | Недостатки | 18 |
| 1.2 | Тон сердца | 19 |
| 1.2.1 | Происхождение характеристики..... | 19 |
| 1.2.2 | Универсальность, уникальность, постоянство, собираемость | 20 |
| 1.2.3 | Методы идентификации, методика (сбор, обработка и сравнение)..... | 21 |
| 1.2.4 | Достоинства | 32 |
| 1.2.5 | Недостатки | 32 |
| 1.3 | Дезоксирибонуклеиновая кислота (ДНК) | 33 |
| 1.3.1 | Общая информация | 33 |
| 1.3.2 | Методы идентификации | 34 |
| 1.3.3 | Достоинства | 37 |
| 1.3.4 | Недостатки | 37 |
| 1.3.5 | Характеристики надежности..... | 38 |
| 1.4 | Электроэнцефалограмма (ЭЭГ) | 39 |
| 1.4.1 | Введение | 39 |
| 1.4.2 | Авторегрессионный метод идентификации | 40 |
| 1.4.3 | Обработка данных | 42 |
| 1.4.4 | Выводы | 45 |
| 1.5 | Информационно-волновой обмен в живых организмах | 49 |
| 1.5.1 | Введение | 49 |
| 1.5.2 | Гиперзвуковое автоволновое поле биоорганизма человека (волны в живых организмах) | 52 |
| 1.5.3 | Частоты живых организмов. Акустоэлектронные явления в живых организмах. Волновые характеристики человека | 54 |
| 1.6 | Аутентификация личности в корпоративной компьютерной сети на основе анализа клавиатурного почерка пользователя | 56 |
| 1.6.1 | Аутентификация по наноструктуре пальца | 72 |
| 1.6.2 | Аутентификация пользователя в корпоративной компьютерной сети на основе анализа капиллярного узора пальцев | 74 |
| 2 | ЗАЩИТА ИНФОРМАЦИИ | 81 |
| 2.1 | Введение | 81 |
| 2.2 | Сокращаемые биометрические параметры | 86 |

1 ПЕРСПЕКТИВНЫЕ МЕТОДЫ БИОМЕТРИЧЕСКОЙ ИДЕНТИФИКАЦИИ ЛИЧНОСТИ

1.1 Запах тела

1.1.1 Происхождение характеристики

Запах – это специфическое ощущение присутствия в воздухе летучих веществ, обнаруживаемых химическими рецепторами обоняния, расположенными в носовой полости человека и животных.

Запах для большинства людей – относительно слабо дифференцированное, интегральное ощущение, так как он определяется суммарным эффектом от раздражения обонятельных рецепторов, рецепторов тройничного нерва и рецепторов вомероназального органа; кроме того, возможно, что в ощущение запаха вовлечено восприятие аэрозольной компоненты атмосферы [1].

Как видно на рисунке 1.1, внутри носа есть две воздушные полости или носовые полости. Воздух, включающий одоранты вдыхается через ноздрю и продвигается дальше. Во время вдоха, воздух поднимается в верх полости. Здесь находится небольшой участок из приблизительно 10 млн. специализированных обонятельных клеток. Эти клетки имеют длинные микро-волоски, или реснички, которые торчат из них. Частицы запаха в воздухе задерживаются на ресничках и заставляют обонятельные клетки создавать нервные импульсы, которые перемещаются в обонятельную луковицу. Это центр предварительной обработки, который частично сортирует сигналы прежде, чем они пройдут вдоль обонятельного тракта к мозгу, где они воспринимаются как запахи [3].

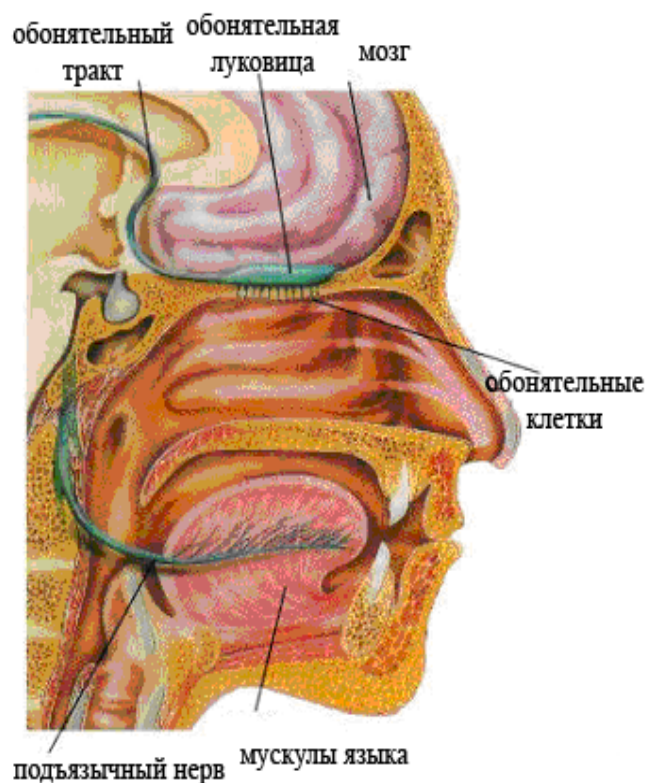


Рисунок 1.1 – Модель обоняния человека

Термином «запах» определяют свойство материальных объектов – физических тел животного, растительного и минерального происхождения, заключающееся в непрерывном отделении (испарении) во внешнюю среду частиц-молекул данного объекта, которые вместе с воздухом попадают в обонятельный орган и воздействуют на него [2].

Люди с отличающимися иммунными генами выделяют различные запахи тела. Каждый человек имеет уникальный запах тела, который является комбинацией приблизительно тридцати различных одорантов [3].

1.1.2 Универсальность, уникальность, постоянство, собираемость

Аромат, который испускает каждый из нас, совершенно неповторим.

Неподражаемый букет состоит приблизительно из 30 – 40 компонентов. Причем состав пота не меняется в зависимости от физической нагрузки или того, что человек ест.

Запах человека, по мнению специалистов, является его химической «подписью», он глубоко индивидуален. Индивидуальный человеческий запах легко проникает в одежду, обувь и долго удерживается.

Запаховые следы и их свойства

Запаховые следы – это газообразные образования, отличающиеся от традиционных материальных следов своей динамичностью. Запаховый след образуется в том случае, если вещество непрерывно из твердого или жидкого состояния переходит в газообразное. Предмет является источником запаха до тех пор, пока с поверхности его отделяются в окружающую среду молекулы вещества. Запаховые следы характеризуются следующими свойствами:

- непрерывность механизма слеодообразования – то есть при наличии источника и соответствующих внешних условий запаховый след образуется непрерывно до тех пор, пока существует источник, в отличие от трасологических следов, возникновение которых происходит в основном одномоментно. Отсюда возможность обнаружения следов зависит от количества пахучего вещества в источнике и внешних условий, в которых происходит слеодообразование;

- подвижность структуры – внутреннее состояние вещества следа, отсутствие связи между его молекулами, их постоянное хаотическое движение и перемешивание между собой и частицами среды. Отсюда интенсивность запаха усиливается вблизи источника и забор его надо производить в непосредственной близости от поверхности источника запаха. В ограниченном объёме (стеклянной емкости) запаховый след будет представлять однородную смесь в любой части емкости;

- рассеиваемость – свойство запахового следа рассредоточиваться в емкости либо пространстве, то есть уменьшать либо увеличивать свой объём и, таким образом, изменять концентрацию запахового вещества в единице объёма. Направление и скорость движения запахового следа зависят от перемещения воздуха. Отсюда последовательное увеличение концентрации запахового

вещества в единице объёма свидетельствует, что приемник движется в направлении нахождения источника запаха;

- делимость – возможность делить запаховый след на части, причем каждая из частей сохраняет качественные характеристики целого. Это позволяет получать из одного источника одновременно либо с разрывом во времени несколько запаховых следов, информационная значимость которых будет одинаковой. Отсюда, если невозможно непосредственно изъять источник запаха, то следует отбирать несколько порций запахового следа для обеспечения повторных исследований. Если имеется законсервированный в емкости запаховый след, то его можно разделить на однородные порции.

Законсервированный запаховый след (помещенный в полиэтиленовую флягу, стеклянную банку) становится относительно неизменяемым и длительное время пригоден для исследований. При необходимости пахучие вещества человека могут быть транспортированы. Запахи, своевременно взятые и законсервированные, можно высылать по почте в обычной упаковке. Пересылать лучше всего предметы одежды (рубашки, платки, обувь и т. п.), так как на них содержится достаточная концентрация пахучих веществ, кроме того, эти объекты наиболее транспортабельны [2].

1.1.3 Методы идентификации (сбор, обработка и сравнение)

Основная задача в распознавании запаха - создать модель, максимально похожую на нос человека. С этой точки зрения, электронные/искусственные носы разрабатываются как системы для автоматического обнаружения и классификации запахов, паров, газов.

Электронный нос можно представить как комбинацию двух компонентов: сенсорной системы и системы распознавания образов. Схематическое представление электронного носа может быть найдено на рисунке 1.2.

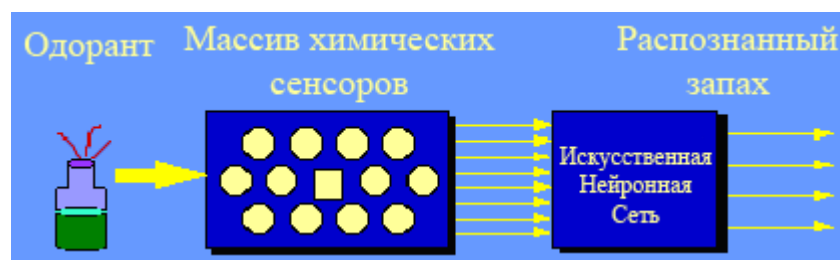


Рисунок 1.2 – Схема электронного носа

Сенсорную систему можно представить как массив химических сенсоров, где каждый сенсор измеряет отдельное свойство, поступающего химического вещества, или как одиночное чувствительное устройство или как совокупность обоих. Основная задача этого компонента заключается в том, чтобы поймать запах. Каждый запах, который попадает на сенсорную систему, создает запись особенного образца запаха. База данных записей строится путем внесения большого количества различных одорантов в сенсорную систему.

Система распознавания образов используется для распознавания. Целью этого процесса является обучение и создание системы распознавания, которая будет способна производить уникальную классификацию или группировку каждого запаха так, чтобы могла быть осуществлена автоматическая идентификация. Этот процесс включает несколько методов: статистический, с использованием искусственных нейронных сетей (ИНС), нейроморфический.

Создание математической модели динамики в обонятельной луковице является тяжелой проблемой. Смоделированный наподобие носа человека, электронный нос полагаться на взаимодействие воспринимаемых химических веществ с массивами чувствительной пленки, которые создают определимый образец.

Сенсорная система

Сенсорная система дает возможность отслеживать конкретный запах из окружающей среды. Эта система представляет собой отдельное сенсорное устройство, подобно газовому хроматографу, спектрометру. В этом случае оно создает массив измерений для каждого компонента. Вторым типом сенсорной системы является массив химических сенсоров. Этот тип является более

подходящим для сложных смесей, поскольку каждый сенсор измеряет отдельное свойство отслеживаемого химического вещества. Также возможен комплекс из отдельного сенсорного устройства и массива химических сенсоров.

Каждый одорант, поступающий в чувствительную систему, создает характерный образец одоранта. База данных шаблонов создается путем внесения большого числа различных одорантов в эту систему. Она используется затем для создания системы распознавания конкретного запаха.

Существует 5 готовых к использованию типов сенсоров:

- Сенсоры удельной электропроводности

Существует два типа сенсоров удельной электропроводности: на основе оксида металла и полимерные. Они показывают изменение сопротивления, когда подвергаются воздействию летучих органических смесей. Из-за низкой стоимости, оба этих класса используются очень широко. Эти сенсоры реагируют на водяной пар, разницу влажности, но не слишком чувствительны к определенным одорантам. В настоящее время, большое количество научно-исследовательских групп работает над вопросом расширения этого типа сенсоров. Проводниковые полимерные сенсоры обычно используются в системах электронного носа. Поскольку проводниковые полимерные сенсоры работают при температуре окружающей среды, им не нужны нагреватели, и, таким образом, их легче создать. Электронный интерфейс прост, и такие сенсоры пригодны для портативных приборов.

- Пьезоэлектрические сенсоры (рисунок 1.3)

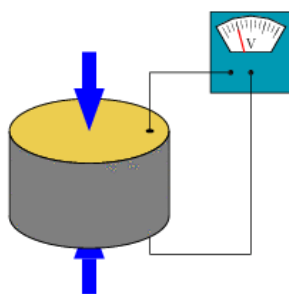


Рисунок 1.3 – Изображение пьезоэлектрического сенсора

Семейство пьезоэлектрических сенсоров (устройства на ПАВ) могут измерять температуру, изменения массы, давление, силу и ускорение. Во время работы образец газа адсорбируется на поверхности полимера, увеличивая массу устройства с полимерным диском, и этим самым снижает резонансную частоту. Снижение обратно пропорционально массе одоранта, адсорбированного полимером. В электронном носе эти сенсоры сконфигурированы как устройства, чувствительные к изменению массы.

- Полевой МОП-транзистор (рисунок 1.4)

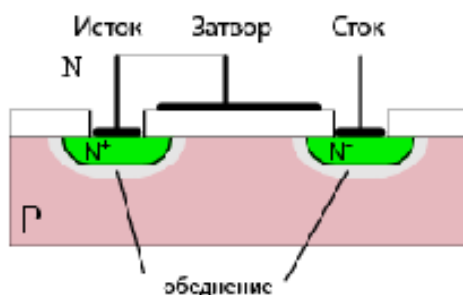
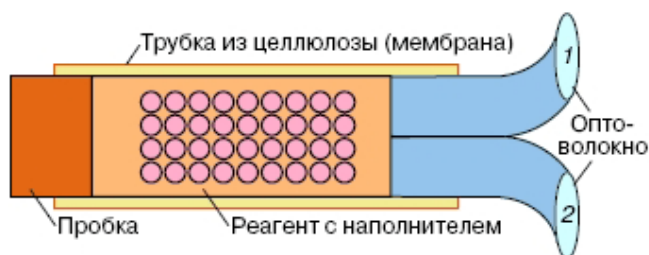


Рисунок 1.4 – МОП-транзистор, работающий в режиме обогащения

Чувствительные к запаху устройства на основе МОП-транзистора основаны на том принципе, что летучие компоненты запаха при контакте с каталитическим металлом могут вызывать реакцию на металле. Продукты реакции могут диффундировать через затвор МОП-транзистора, чтобы изменить электрические свойства устройства. Работая при различных температурах и изменяя тип и толщину оксида металла, можно оптимизировать чувствительность и избирательность.

- Оптоволоконные сенсоры (рисунок 1.5)



1 – падающее излучение от источника; 2 – детектируемое излучение

Рисунок 1.5 – Схема обратимого волоконно-оптического сенсора для определения кислотности среды

Оптоволоконные сенсоры используют стеклянные волокна с покрытием из тонкого химически активного материала, который покрывается внутри них или на их концах. Источник света на узкой полосе частот используется для воздействия на активный материал, который в свою очередь реагирует с изменением в цвете на присутствие одоранта, который необходимо обнаружить и измерить.

Массивы этих устройств с различными цветовыми смесями могут быть использованы как сенсоры для электронного носа. Основное применение такого типа электронных носов – медицина.

- Сенсоры, основанные на спектрометрии

Сенсоры, основанные на спектрометрии, базируются на том, что каждая молекула имеет четкий инфракрасный спектр. Обычно устройства, основанные на таких сенсорах, довольно большие и дорогие.

Система распознавания образов

Система распознавания образов является вторым компонентом электронного носа, используемого для распознавания запаха. Цель заключается в подготовке или построении системы распознавания для создания уникальной классификации или кластеризации каждого одоранта посредством автоматической идентификации.

В отличие от систем человека, электронные носы обучают для идентификации только несколько различных запахов или летучих смесей. Это очень весомый недостаток для использования этих носов при распознавании человека. Достигнутое не дает возможности точно идентифицировать все компоненты человеческого тела.

Процесс распознавания включает несколько методов: статистический, использование ИНС, нейроморфический.

Многие статистические методы являются дополнительными для ИНС и их часто комбинируют для создания классификаторов и кластеров. Они включают анализ главных компонент (АГК), метод наименьших квадратов,

отличительный анализ и анализ кластеров. АГК отдельно разбивает данные на линейные комбинации ортогональных векторов, находящихся на осях, которые максимизируют отличия. Для того чтобы уменьшить объем данных, в образе хранятся только оси с большими отличиями.

Когда ИНС объединяют с массивом сенсоров, число обнаруживаемых химических веществ обычно выше, чем количество типов отдельных сенсоров. Рассматриваемый подход включает обучение классификатора образца для соотношения сенсорных значений с определенными метками запаха. Алгоритм для неконтролируемого обучения не требует заранее определенных классов запаха. Он по существу выполняет разбиение данных на одинаковые кластеры, основанные на измеренных признаках или свойствах.

Нейроморфические методы главное внимание уделяют построению моделей обоняния, основанных на биологии, и выполнении их в электронике. К сожалению, не существует недостаток реалистичных математических моделей биологического обоняния. Таким образом, область нейроморфических моделей обонятельной системы отстает от зрительных, слуховых, моторных моделей. Обонятельная информация обрабатывалась как в обонятельной луковице, так и в обонятельной коре. Обонятельная луковица выполняет предварительную обработку сигнала обонятельной информации, включая запись, дополнительное преобразование и сжатие сигнала. Обонятельная кора выполняет классификацию образцов и распознавания воспринимаемых запахов.

Существует две конкурирующих модели обонятельного кодирования. Селективный рецептор исходит из последних экспериментальных результатов в молекулярной биологии. Его можно рассматривать как преобразователь запаха. Этот метод подобен зрительной системе с точки зрения восприимчивых областей обонятельных рецепторов и митральных клеток в обонятельной луковице. Второй метод заключается в неселективном рецепторе, модель дистрибутивного кодирования, которая основывается на данных, собранных

электрофизиологией и формированием изображения обонятельными луковицами.

Нейроморфический метод превосходит остальные, он включает объединение временной динамики для регулирования идентификации комбинаций запахов.

Система обработки сигналов обоняния и распознавания образов

Целью электронного носа является идентификация образца одоранта и оценка его концентрации (в случае распознавания человека). Это относится к системе обработки сигналов обоняния и распознавания образов. Тем не менее, эти два шага могут быть подразделены на предварительную обработку, выделение признаков, классификацию, и принятие решения. Все эти подпроцессы можно увидеть на рисунке 1.6. Но сначала, необходимо помнить, что база данных ожидаемых одорантов должна быть составлена, и образец должен присутствовать в сенсорном массиве носа.

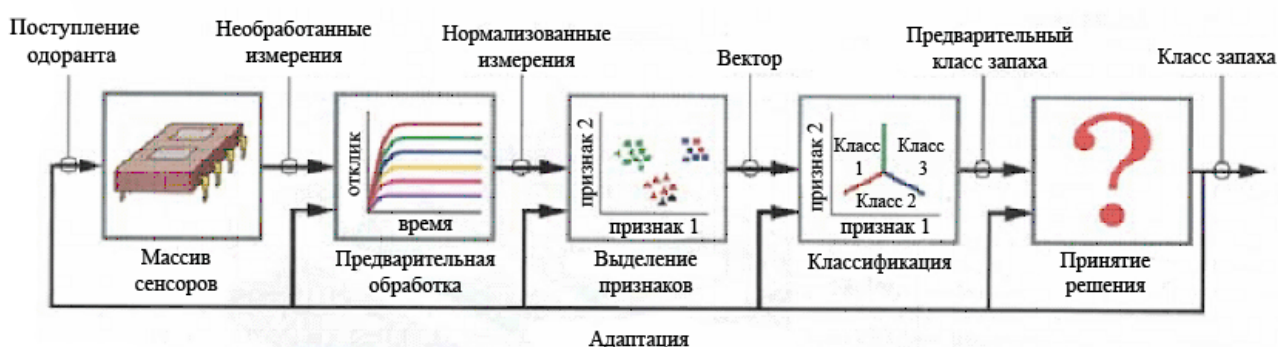


Рисунок 1.6 – Этапы работы системы обработки сигналов обоняния и распознавания образов

Рассмотрим все этапы обработки сигналов и распознавания образов (из рисунка 1.6) более подробно.

1) Предварительная обработка

Предварительная обработка компенсирует сенсорный дрейф, сжимает отклик сенсорного массива и уменьшает изменения от образца к образцу. Типичные методы включают: нормализацию диапазонов реакций сенсора для всех сенсоров в массиве и сжатие промежуточных реакций сенсора.

2) Выделение признаков

Выделения признаков имеет две цели: уменьшение размерности пространства измерения и извлечение информации, необходимой для распознавания образа. Выделение признаков обычно выполняется линейными преобразованиями, такими, как классический АГК.

3) Классификация

Обычно используемый метод для выполнения классификационной задачи – это искусственные нейронные сети (ИНС). Искусственная нейронная сеть является системой обработки информации, которая имеет некоторые характеристики исполнения совместно с биологическими нейронными сетями. Это позволяет электронному носу функционировать подобно функционированию мозга, когда он преобразовывает отклики из обонятельных сенсоров носа человека. Типичный классификатор ИНС состоит из двух или более уровней.

4) Принятие решения

Классификатор создает оценку класса для неизвестного образца вместе с оценкой присвоения конфиденциально расположенного класса. Этап окончательного принятия решения можно использовать, если доступны любые специализированные знания, как например, пороги доверия или риск, связанный с различными классификационными ошибками. Модуль принятия решения может модифицировать назначение классификатора и даже определять, что неизвестный образец не принадлежит ни одному из одорантов в базе данных.

1.1.4 Перспективы использования электронных носов

Несмотря на то, что многие эксперты скептически относятся к открытию, его авторы, итальянские ученые из Рима надеются, что оно поможет разработать быстрый тест для выявления болезни на ранней стадии, пишет журнал NewScientist со ссылкой на итальянские источники.

В результате воздействия различных факторов в дыхании человека могут обнаруживаться специфические соединения. Например, алифатические кислоты находят у людей с циррозом печени, в то время как ди- и триметиламин встречаются в дыхании людей, страдающих почечной недостаточностью. Пациенты, больные раком легких выдыхают смесь веществ-производных алканов и бензола, хотя до сих пор ученым не до конца ясно, почему это происходит.

Обычно для анализа газовых смесей используются такие методы как газовая хроматография и масс спектрометрия, однако они слишком дороги и сложны для применения на практике. А вот электронные носы уже используются для контроля качества в пищевой промышленности. И вот сейчас итальянские исследователи надеются, что подойдут они и для диагностики заболевания.

Как и нос животных и человека, электронный нос использует набор сенсоров, которые хотя и не предназначены для распознавания химических веществ, однако реагируют на общий профиль компонентов в образце. В пищевой промышленности это позволяет различать тонкие запахи и вкусы.

Сенсоры представляют собой кристаллы кварца, покрытые слегка отличающимися друг от другом слоем металлопорфирина, которые привязаны к определенному диапазону летучих органических веществ. Частота естественной вибрации кристаллов зависит от их веса. Эта частота изменяется, когда молекулы из образцов приклеиваются к поверхностям кристаллов. Так что сложная газовая смесь, какой является дыхание человека, вызовет на кристаллах уникальную последовательность вибраций.

Во время испытаний в Риме, результаты которых будут скоро опубликованы в журнале *Biosensors and Bioelectronics*, был использован электронный нос с восьмью сенсорами. В эксперименте принимали участие шестьдесят пациентов госпиталя Forlanini, 35 из них ожидают операции по

удалению крупной опухоли в легких. Каждый тест занял немногим больше минуты, и электронный нос успешно выявил всех больных раком [4].

Электронный нос способен определять инфекции

Американские ученые разработали устройство, которое распознает инфекции, анализируя дыхание пациента. Получив выводы прибора, врачи смогут сразу установить, какой именно болезнью заразился тот или иной человек и назначить эффективный для ее лечения антибиотик.

Специалисты из университета Пенсильвании говорят, что применение устройства делает диагностику намного быстрее, надежнее и проще по сравнению со всеми существующими методами.

Обычно врачам довольно трудно определить, в каком именно лекарстве нуждается пациент, поскольку различия между обычной респираторной инфекцией и пневмонией не всегда очевидны.

Однако новое устройство, по словам разработчиков, позволяет минимизировать врачебные ошибки.

Аромат бактерии

Как выяснили ученые, все бактерии имеют собственный неповторимый запах – точно так же, как каждый человек имеет уникальные отпечатки пальцев. И электронный нос способен различать и сравнивать эти запахи.

Новый прибор уже успешно испытали во время трех разных исследований.

Первые два включали диагностирование пациентов, подключенных к системе искусственного дыхания в хирургической реанимации. Устройство сумело правильно распознать пневмонию в 92% случаев.

Третье исследование началось с диагностирования синусита – широко распространенного заболевания носовых пазух. Электронному носу удалось правильно поставить диагноз в 82% случаев и определить носителей этой инфекции.

По словам специалиста университета Пенсильвании Эрики Талер, новый прибор способен кардинально изменить принципы диагностики пациентов с респираторными инфекциями.

Лучше, чем флюорография

"Учитывая, что мы можем применять сенсорный анализ для определения пневмонии и синусита, есть надежда, что его можно использовать и для других бактериологических инфекций верхних дыхательных путей", – говорит Талер.

Профессор Эндрю Пикок из Британского торакального общества одобрительно отзывается об открытии.

"Легочные специалисты обычно имеют дело только с результатами флюорографии, которая может показать наличие инфекции, опухоли, жидкости или других причин болезни. Если мы сможем быстро и качественно диагностировать инфекцию с помощью компьютерного "носа", это действительно будет шагом вперед", – считает эксперт.

Он, впрочем, добавляет, что эта технология еще должна пройти дополнительные испытания.

Сейчас ученые проводят новые исследования, проверяя, можно ли использовать электронный нос для диагностики других заболеваний, таких как рак легких и недугов, поражающих печень и почки [5].

1.1.5 Достоинства

Достоинства идентификации человека по запаху перед традиционными методами:

- люди с отличающимися иммунными генами выделяют различные запахи тела;
- каждый человек имеет уникальный запах тела, который является комбинацией приблизительно тридцати различных одорантов.

1.1.6 Недостатки

Возможные недостатки [3] идентификации человека по запаху:

- искусственные носы еще не достаточно умны для задачи идентификации человека (современные сенсоры запаха нечувствительны к широкому диапазону смесей);
- высокая стоимость регистрирующих запах устройств;
- сложность конструкции электронных носов.

Вопросы для самопроверки

- 1) Какие Вы знаете методы идентификации по запаху тела человека?
- 2) Какие типы сенсоров чаще всего используются при создании электронных носов?
- 3) В чем заключается отличие сенсорной системы от системы распознавания образов?
- 4) Из каких этапов состоит процесс обработки сигналов и распознавания образов?
- 5) Какие перспективные направления в использовании электронных носов можно выделить?
- 6) Достоинства и недостатки метода.

Литература

- [1] Википедия – свободная библиотека [Электронный ресурс]. – Режим доступа: <http://ru.wikipedia.org>. – Дата доступа: 22.05.2009.
- [2] Белкин, Р.С. Криминалистическая энциклопедия / Р. С. Белкин. – М. – 1997.
- [3] Korotkaya, Z. Biometric Person Authentication: Odor / Z. Korotkaya. – Lappeenranta. – 2003.
- [4] Newsru [Электронный ресурс]. – Режим доступа: NEWSru.com. – Дата доступа: 22.05.2009.
- [5] BBC news [Электронный ресурс] – Режим доступа: <http://news.bbc.co.uk>. – Дата доступа: 22.05.2009.

1.2 Тон сердца

1.2.1 Происхождение характеристики

Сердце – фиброзно-мышечный орган, обеспечивающий ток крови по кровеносным сосудам. У взрослого человека его объем и масса составляют в среднем для мужчин 783 см³ и 332 г, для женщин 560 см³ и 253 г (рисунок 1.7).

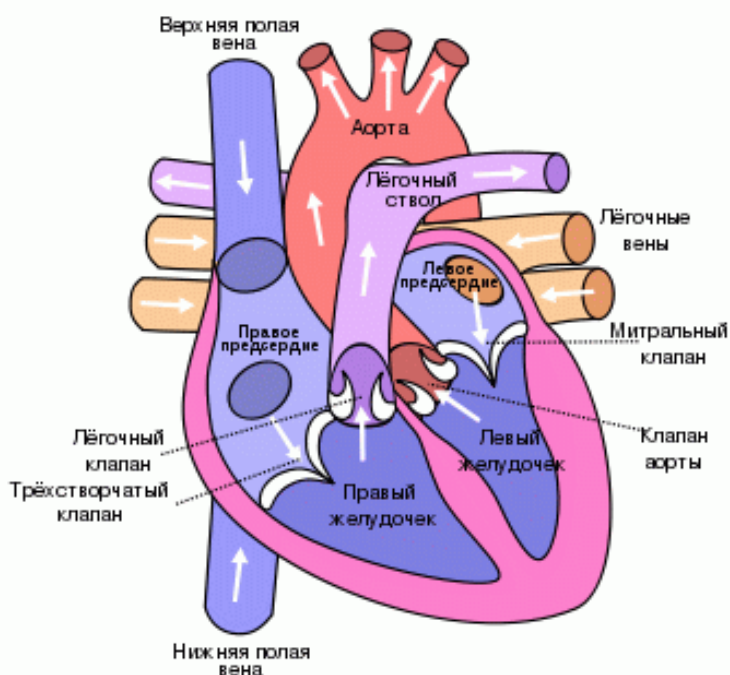


Рисунок 1.7 – Строение сердца человека

Форма определяется возрастом, полом, телосложением, здоровьем, другими факторами. В упрощенных моделях описывается сферой, эллипсоидами, фигурами пересечения эллиптического параболоида и трехосного эллипсоида. Мера вытянутости (фактор) формы есть отношение наибольших продольного и поперечного линейных размеров сердца. При гиперстеническом типе телосложения отношение близко к единице и астеническом – порядка 1,5.

Сердце состоит из четырех камер– левое предсердие, правое предсердие, левый желудочек, правый желудочек, разделенных перегородками. В правое предсердие входят полые, в левое предсердие – легочные вены. Из правого желудочка и левого желудочка выходят, соответственно, легочная артерия (легочный ствол) и восходящая аорта. Правый желудочек и левое предсердие

замыкают малый круг кровообращения, левый желудочек и правое предсердие – большой круг. Сердце расположено в нижней части переднего средостения, большая часть его передней поверхности прикрыта легкими. С впадающими участками полых и легочных вен, а также выходящими аортой и легочным стволом оно покрыто сорочкой (перикардом). В полости перикарда содержится небольшое количество серозной жидкости.

Работа сердца состоит из трёх циклов.

1) Сокращаются предсердия. При этом кровь через открытые клапаны проталкивается в желудочки сердца. Сокращение предсердий начинается с места впадения в него вен, поэтому устья их сжаты, и попасть назад в вены кровь не может.

2) Вслед за предсердиями сокращаются желудочки. Створчатые клапаны, отделяющие предсердия от желудочков, поднимаются, захлопываются и препятствуют возврату крови в предсердия.

3) Пауза (диастола). Во время паузы сердечные камеры заполняются кровью. Из вен кровь попадает в предсердия и частично стекает в желудочки. Когда начнется новый цикл, оставшаяся в предсердиях кровь будет вытолкнута в желудочки – цикл повторится.

Сердечный цикл имеет определенную продолжительность: 0,1 секунды – сокращения предсердия, 0,3 секунды – сокращения желудочков, 0,4 секунды – пауза [1].

1.2.2 Универсальность, уникальность, постоянство, собираемость

Существует возможность идентифицировать человека с использованием тонов (акустических сигналов), издаваемых сердцем (с использованием сердцебиений). Самое главное достоинства такого метода идентификации – практически невозможно подделать тон сердца по сравнению с другими биометрическими методами.

Данный метод состоит из схемы выделения устойчивых признаков, которая базируется на кепстральном анализе. Результаты подтверждают тот факт, что значения параметра тона сердца существенно отличается от таких же параметров, используемых в традиционном кепстральном анализе речи. В частности, тоны сердца должны быть обработаны в течение 0,5 секунды во всем диапазоне частот. Предварительные параметры показали, что при хорошем выборе параметров, точность идентификации достигает 96 %.

Тоны сердца человека являются естественными сигналами и применяются во врачебной практике для контроля и диагностики состояния здоровья на протяжении тысячи лет. В прошлом, исследование тонов сердца было сосредоточено главным образом в изменчивости частоты сердечных сокращений.

Тем не менее, можно предполагать, поскольку тоны сердца содержат информацию о физиологии человека, то такие сигналы обладают возможностью предоставлять уникальное тождество для каждого человека. Подобно ЭЭГ, эти сигналы трудно скрыть, что, следовательно, уменьшает риск фальсификации. Кроме того, тон сердца сравнительно легко получить, устанавливая стандартный стетоскоп на груди, к примеру.

1.2.3 Методы идентификации, методика (сбор, обработка и сравнение)

Сердце человека имеет четыре камеры, две верхние называются предсердиями, а две нижние – желудочками, как показано на рисунке 1.7. Клапаны располагаются между предсердиями и желудочками, и между желудочками и основной артерией сердца. Эти клапаны периодически закрываются и открываются для того, чтобы обеспечить только одно направление распространения потока крови. Обычно создается два тона при протекании крови через сердечные клапаны в течение каждого сердечного цикла. Первый тон сердца S1 является низким, немного вытянутым "lub", вызванным вибрациями, возникающими при внезапном закрытии митрального

и трехстворчатого клапанов как только желудочки сжимаются и выкачивают кровь в аорту и легочную артерию в начале желудочковой систолы. Второй тон S2 – короче и выше "dup", вызывается, когда желудочки прекращают выталкивание, ослабевают и позволяют аортальному и легочному клапанам закрыться сразу после завершения желудочковой систолы. Именно эти звуки считаются сердцебиениями. S1 имеет длительность около 0.15 секунд с частотой 25-45 Гц. С другой стороны, S2 продолжается около 0.12 секунд, с частотой 50 Гц. Рисунок 1.8 показывает форму сигналов S1 и S2.

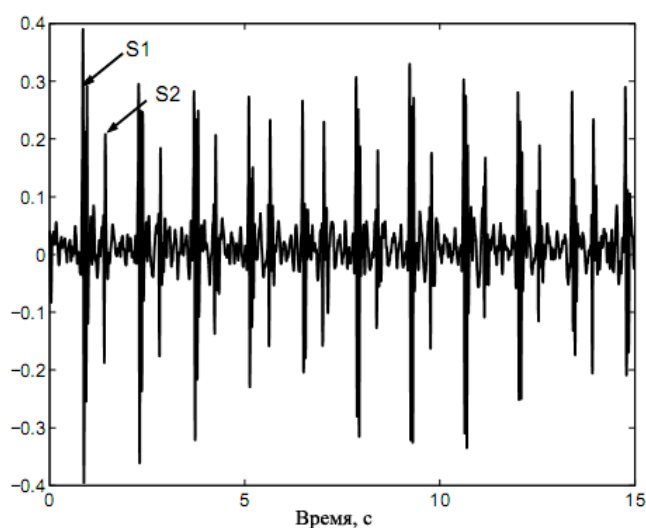


Рисунок 1.8 – Формы тонов S1 и S2

Тоны, связанные с открытием и закрытием клапанов, могут быть обнаружены микрофоном, размещенным непосредственно в различных точках выслушивания на грудной клетке как показано на рисунке 1.9.



Рисунок 1.9 – Точки размещения стетоскопа или микрофона

Временные и спектральные графики нормальных тонов сердца, снятых с пяти различных людей, показаны на рисунках 1.10 и 1.11. Хотя огибающие сигналов похожи, детали форм сигнала во временной и частотной областях достаточно различны. Из рисунка 1.10 может быть видно, что люди могут иметь нормальные или ненормальные тоны сердца или комбинации обоих. Кроме того, человек с ненормальным тоном сердца демонстрирует более отчетливые характеристики формы сигнала. Предварительные наблюдения предлагают такую отличительную черту использования тона сердца для идентификации.

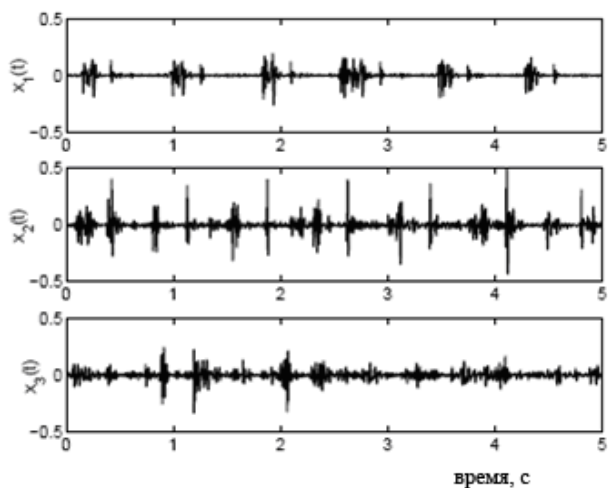


Рисунок 1.10 – Сравнение тонов сердца

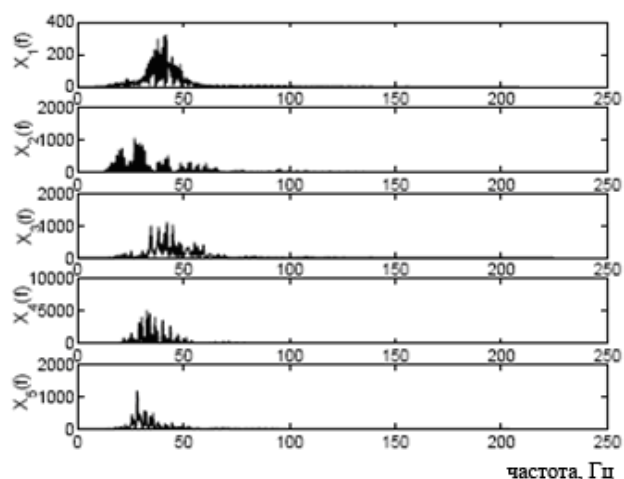


Рисунок 1.11 – Сравнение спектров тонов сердца

Упрощенная схема выбора признаков представлена на рисунке 1.12.

Из-за наложения на компоненты тона сердца шумов и артефактов, вызванными другими внутренними органами, полный анализ тона сердца во временной области затруднен.

Для биометрического применения физиологические свойства тона сердца важнее частоты сердечных сокращений. Будем рассматривать кепстральные характеристики, которые используются во многих приложениях обработки речи, в распознавании речи и идентификации говорящего, в частности. Подобно моделированию речевого сигнала, рассмотрим тон сердца как выход изменяющейся во времени линейной системы (см. рисунок 1.13), где входное возбуждение несет информацию о частоте сердечных сокращений, а передаточная функция изменяется во времени.

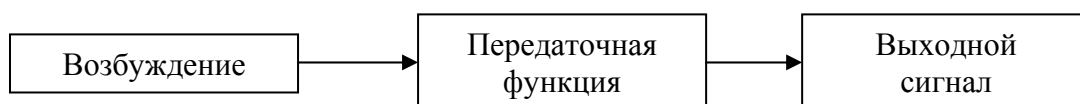


Рисунок 1.12 – Линейная модель тона сердца

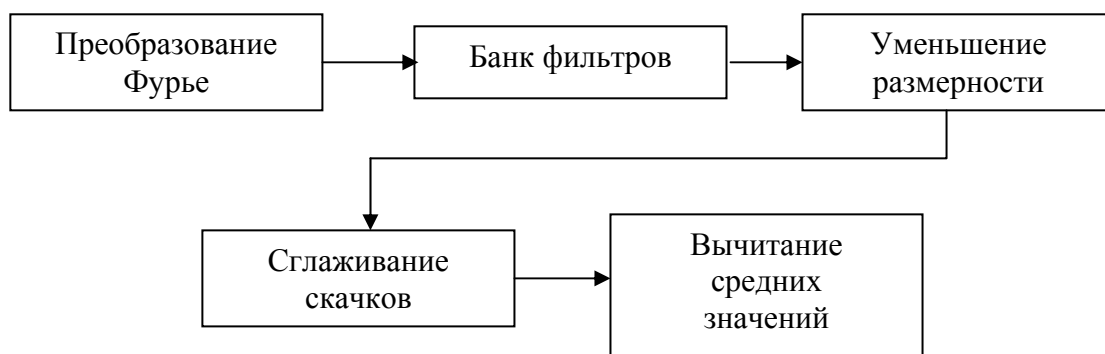


Рисунок 1.13 – Блок-схема процесса извлечения параметров

1) Преобразование Фурье: Как и в случае сигналов речи, примем кратковременное стационарное состояние для тона сердца, которое без труда позволяет провести данный анализ.

$$X[n, k] = \sum_{m=0}^{N-1} x \cdot w[m + (n-1)S] \exp(-j \frac{2\pi}{N} km) \quad (1.1)$$

где n – индекс фрейма;
 k – частотный индекс;
 N – длина фрейма;
 w – окно;
 S – сдвиг фрейма.

В отличие от речевых сигналов, где голосовой тракт изменяется каждые 20-25 мс, тоны сердца более стационарны и следовательно окно должно быть больше. Оказывается, что оптимальная длина окна будет составлять почти 500 мс. Используется только информация о спектральной величине, и игнорируются компоненты фазы, которые обычно более чувствительные к шуму.

2) Банк фильтров: В этом блоке спектр сигнала проходит через набор фильтров. Использование таких банков фильтров мотивировано тем, что спектр звука имеет некоторые особые формы и распределяется по нелинейной шкале в частотной области. Используя банки фильтров со спектральными характеристиками, хорошо сочетаемыми с параметрами сигнала, вклад компонентов шума в частотной области может быть уменьшен. Тем не менее, в отличие от речевого сигнала, спектр тона сердца сконцентрирован в диапазоне 20 - 150 Гц. В таком узком диапазоне требуется полное разрешение для того, чтобы захватить больше информации спектра сигнала.

3) Уменьшение размерности: Выходная спектральная величина сжата в логарифмической области, подвержена преобразованию дискретным косинусом, которое считается эмпирическим принципом главных компонент. Кепстральный компонент $c[n, k]$ может быть записан как:

$$c[n, k] = \sum_{m=0}^{\bar{K}-1} \log(|X[n, m]|) \cos\left(\frac{km\pi}{\bar{K}}\right), k = (1, 2, \dots, \bar{K}) \quad (1.2)$$

где \bar{K} – количество элементов разрешения в частотном диапазоне 20 - 150 Гц.

Уменьшение размерности достигается выбором первых 24 коэффициентов для каждого фрейма. Следует отметить, что более высокие коэффициенты являются вкладками процесса возбуждения, который менее информативен. Назовем эту характеристику Linear Frequency Bands Cepstra (LFBC).

4) Сглаживание скачков: качество записи тона сердца часто страдает из-за импульсных помех, вызванных перемещением стетоскопа. Спектры этих импульсных шумов и тона сердца перекрываются и поэтому стандартные методы фильтрации здесь неэффективны.

5) Вычитание средних значений: Так как положение стетоскопа не может быть зафиксировано все время, всегда присутствуют флуктуации в функции относительной передачи, характеризующейся распространением тонов сердца в регистратор. Для устранения этого влияния применяют вычитание средних значений [2]. Таким образом, кепстральные характеристики записанных сигналов можно представить следующим образом:

$$c_Y[n, k] = c_H[n, k] + c_H[k], \quad (1.3)$$

где $c_H[n, k]$ – натуральный логарифм сигнала, измеренного в неподвижной позиции;

$c_H[k]$ – натуральный логарифм функции относительной передачи.

Классификационная схема

Векторное квантование (ВК) и моделирование гауссового смешивания (МГС) являются стандартными и успешными методами для методики распознавания говорящего.

Основная идея использования векторного квантования заключается в сжатии большого числа кепстральных векторов в небольшой набор кодовых векторов. Шифровальная книга векторного квантования обычно обучается алгоритмом LBG для минимизации ошибки квантования при замене всех векторов признаков соответствующими им соседними кодовыми векторами.

Эвклидово расстояние часто используется как мера ошибки квантования. ВК LBQ может считаться аппроксимацией функции плотности дискретными точками, и основное преимущество этого метода заключается в его возможности архивировать относительно высокую степень идентификации с помощью очень коротких тестовых сигналов.

Существуют и другие методы ВК для универсальной оптимизации шифровальной книги после того, как они будут сгенерированы определенным алгоритмом обучения без оператора. Этот метод называется обучением векторного квантования. В отличие от ВК LBG, алгоритмы LVQ стремятся определить непосредственно классификационные границы между классами, используя правило соседнего ближнего. Тем не менее, решение об идентификации в испытании основывается на последовательности векторов, а не на одном векторе признаков, следовательно, более высокая степень правильной классификации для вектора признаков, заархивированного с помощью LVQ, не всегда улучшает степень идентификации.

Кроме того, затраты на вычисления у LVQ выше, чем у LBQ.

В работе [2] осуществляется быстрая версия LBQ с кодом $N = 2^k$.

Вторым методом сопоставления образцов, использованным в этой работе является МГС, которое может считаться стохастическим обобщением векторного квантования. В отличие от ВК LBQ, метод МГС аппроксимирует непрерывную стохастическую функцию плотности множеством гауссовых стохастических функций плотности.

$$p(\bar{x} | \lambda) = \sum_{i=1}^M p_i \cdot b_i(\bar{x}), \quad (1.4)$$

где \bar{x} – произвольный D-мерный вектор;

$b_i(\bar{x}), i = 1, \dots, M$ – плотности компонентов;

$p_i, i = 1, \dots, M$ – веса совокупности компонент. Каждая плотность компонентов является случайной функцией Гаусса формы

$$b_i(\bar{x}) = \frac{1}{(2\pi)^{D/2} \cdot \sum_i^{1/2}} \cdot \exp \left\{ -\frac{1}{2} \cdot (\bar{x} - \bar{\mu}_i)^T \cdot \sum_i^{-1} (\bar{x} - \bar{\mu}_i) \right\}, \quad (1.5)$$

со средним вектором $\bar{\mu}_i$, и ковариационной матрицей Σ_i . Вес совокупности удовлетворяет условию $\sum_{i=1}^M p_i = 1$. Полная плотность всей совокупности Гаусса параметризуется средним вектором, ковариационной матрицей и весами совокупностей плотностей всех компонентов. Все вместе эти параметры представлены формулой

$$\lambda = \{p_i, \mu_i, \Sigma_i\}, i=1, \dots, M, \quad (1.6)$$

Алгоритм ожидаемой максимизации обычно обусловлен благодаря своей простоте и быстрой сходимости. Отметим, что шифровальная книга ВК LBQ используется в качестве исходной для подгонки МГС алгоритмом ожидаемой максимизации. Для идентификации с использованием тонов сердца модель МГС λ подготавливается для каждого человека, и затем при тестировании, модель [соответствующая конкретному человеку] ссылается на каждый тон сердца как на максимум степени условной вероятности.

Экспериментальная установка

Сигнал тона сердца в работе [2] записывался с использованием электронного стетоскопа Welch Allyn Meditron, который представлен на рисунке 1.14.



**Рисунок 1.14 – Изображение электронного стетоскопа
Welch Allyn Meditron**

Электронный стетоскоп устанавливали на груди участника, сидящего в расслабленном состоянии. Для этого эксперимента было собрано семь наборов данных (от 5 мужчин и 2 женщин): 100 показаний тонов сердца записывались

каждым участником на протяжении двух месяцев. Требовалось, чтобы интервал между каждым записанным тоном сердца составил по крайней мере один час и стетоскоп должен был быть установлен на то же самое место на груди для снятия всех показаний.

Эффективность идентификации

На стадии обучения 6 тонов сердца от каждого человека, записанные в разные дни, использовались для построения моделей. На стадии испытания 70 тонов сердца были произвольно выбраны от каждого человека. Было реализовано два метода: ВК и МГС. Кепстральные характеристики линейного частотного диапазона были использованы в качестве основных для обучения и испытания.

В работе [2] оценивается эффективность идентификации при изменении количества характеристик, количества компонентов смеси, при сравнении LBFC с MFCC, при изменении длины и сдвига фрейма.

- **Количество характеристик**

Среди четырех проверенных расположений, используя различные комбинации характеристик, можно выделить:

1. 24 первых кепстральных характеристик плюс логарифм энергии;
2. 60 кепстральных характеристик плюс логарифм энергии;
3. 60 кепстральных характеристик плюс логарифм энергии, коэффициенты дельта и ускорения;
4. 60 кепстральных характеристик без логарифма энергии.

Как показано на рисунке 1.15, система, базирующаяся на МГС, достигла наилучшего результата 96.01%, используя расположение с 60 кепстральными характеристиками плюс логарифм энергии. Для системы, основанной на векторном квантовании, наилучшим результатом было 93.58%, также используя тот же набор характеристик.

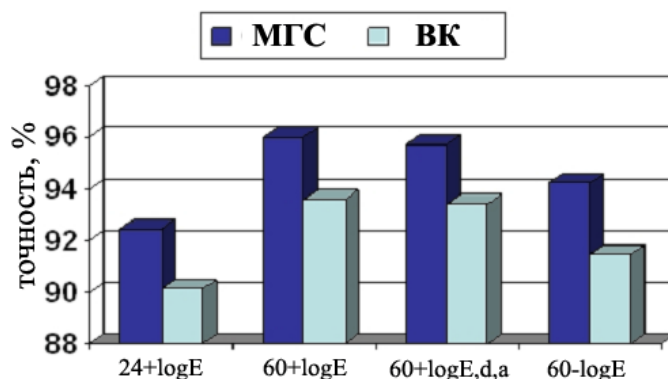


Рисунок 1.15 – Результаты МГС (4 совокупности компонентов) и ВК (16-мерный вектор)

В отличие от распознавания речи, где используются кепстральные характеристики более высокого порядка, которые переносят информацию относительно компонента возбуждения и обычно не являются полезными, эти компоненты, как было обнаружено, являются полезным для анализа тонов сердца. В обеих системах, основанных как на ВК, так и на МГС, системы, использующие 60 кепстральных характеристик дают приблизительно на 3% более высокую точность, чем системы, использующие 24 кепстральные характеристики. Кроме того, использование дополнительных коэффициентов дельта и ускорения не улучшает эффективность системы.

Все это, вероятно, из-за того, что звуковой тракт имеет больший динамический диапазон, чем сердце человека. Логарифм энергии, как было показано, является важным и вносит вклад в степень точности около 2%. Следует отметить, что была использована длина фрейма в 512 мс без наложения.

- Количество компонентов совокупности

Как показано на рисунке 1.16, эффективность системы, основанной на МГС, является наилучшей при использовании 4 компонентов и действительно снижается, если количество компонентов возрастает и наоборот.

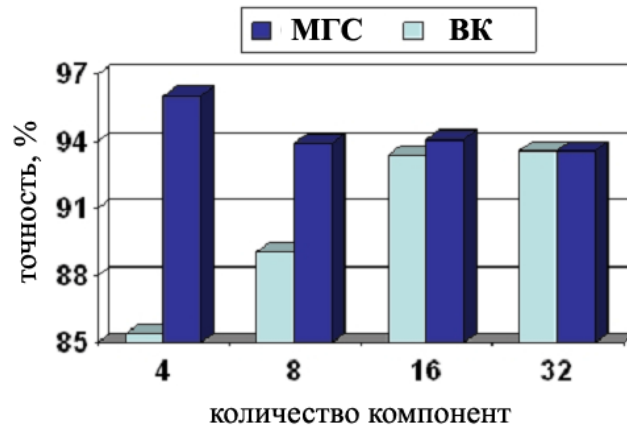


Рисунок 1.16 – Эффективность методов ВК и МГС, основанных на количестве компонент совокупности

Система, основанная на ВК, требует больше компонент и достигает своего наилучшего результата при 16 компонентах. Это вероятно, потому что дискретная аппроксимация стохастической функции плотности при ВК требует больше измерительных точек, чем использование непрерывных гауссовых компонент. Основываясь на этом соображении, можно сделать вывод, что система, основанная на МГС, лучше, как в показателе точности, так и в затратах на вычисления.

- Сравнение с MFCC

Как показано на рисунке 1.17, результаты LBFC превосходят результаты MFCC более чем на 3% как в случае систем, базирующихся на ВК, так и в случае систем, основанных на МГС. Следует отметить, что LBFC и MFCC вычислены с использованием одинаковых длин и сдвигов фрейма.

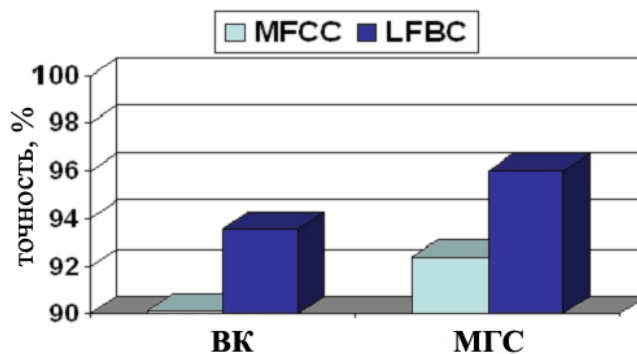


Рисунок 1.17 - Эффективность методов ВК и МГС, использующих параметры LBFC и MFCC

1.2.4 Достоинства

Достоинства перед традиционными методами:

- практически невозможно подделать тон сердца по сравнению с другими биометрическими методами;
- точность идентификации доходит до 98%.

1.2.5 Недостатки

Возможные недостатки:

- трудность снятия характеристики;
- навязчивость.

Вопросы для самопроверки

- 1) Строение сердца.
- 2) Какие существуют методы идентификации человека по характеристикам сердца?
- 3) Из каких этапов состоит процесс извлечения параметров?
- 4) Достоинства и недостатки метода.

Литература

- [1] Википедия – свободная библиотека [Электронный ресурс] – Режим доступа: <http://ru.wikipedia.org>. – Дата доступа: 22.05.2009.
- [2] Human identification using heart sound / P. Koksoon [и др.]; – Singapore.

1.3 Дезоксирибонуклеиновая кислота (ДНК)

1.3.1 Общая информация

Генетическое распознавание, тестирование ДНК, распознавание и профилирование ДНК являются методами, используемыми для идентификации индивидов одного вида используя только образцы их ДНК. Это изобретение было опубликовано сэром Алемом Джеффрисом (Sir Alec Jeffreys) из Университета Лейсестер (University of Leicester) в 1985 году.

Известно, что ДНК любых двух людей почти не отличаются, и преобладающее большинство цепочек в них одинаково. Генетическое распознавание использует тот факт, что существуют сильно отличающиеся повторяющиеся цепочки, называемые минисателлитными ДНК. Число минисателлитных ДНК в локусе (одинаковых участках) у двух людей, не являющимися родственниками, с большой вероятностью различно. За исключением однояйцовых близнецов, генетические профили которых в точности одинаковы, вероятность ошибки, вызванной совпадением, крайне мала. Генетическое распознавание применяется в судебной науке для сличения подозреваемых по образцам крови, волос, слюны или спермы. Были случаи, когда это привело к реабилитации первоначально осужденных подозреваемых. Эта техника находит также применения в идентификации человеческих останков, тестах на отцовство, подборе органов для трансплантации, изучении популяции диких животных, и определении состава и компонентов еды. Генетическое распознавание также позволило более детально изучить первоначальное расселение людей.

В некоторых странах организуются базы данных, содержащих информацию о ДНК осужденных. Также организуются каталоги, участие в которых добровольное. Наиболее обширная база данных «Национальная база данных ДНК» (The national DNA Database – NDNAD) создана в Великобритании. По состоянию на 2005 год она содержала более 2-х миллионов записей. Размер этой базы, а так же скорость роста, дают основания

для беспокойства о возможном нарушении прав человека: ведь полиция имеет очень широкие возможности для сбора и хранения образцов, даже в случае оправдания подозреваемого.

Контрольные образцы

Для того, что бы провести генетическую идентификацию необходимо произвести извлечение ДНК из контрольных образцов. Ими могут служить:

- личные вещи (зубные щетки, бритвы и т.д.);
- банки образцов (крови, спермы, тканей);
- биологические родственники;
- уже идентифицированные человеческие останки.

1.3.2 Методы идентификации

Генетическое распознавание начинается с выделения ДНК из клеток в образцах крови, слюны, спермы или других подходящих жидкостях или тканях. В основе современных техник, при всем их разнообразии, лежит одна идея. В молекулах ДНК стараются обнаружить, а затем извлечь фрагменты, отличающиеся у разных людей – полиморфизмы. Часто для этого используют специально подобранный фермент.

Развитие техники генетического распознавания состоит в поиске новых полиморфизмов и способов их идентификации. Рассмотрим наиболее распространенные методы генного анализа.

1) Полиморфизм по длине фрагментов рестрикции

Первым из методов, который стал применяться в генетической идентификации, является ПДРФ-анализ (полиморфизм по длине фрагментов рестрикции), хотя в последствие он был почти полностью вытеснен современными техниками. В ходе ПДРФ-анализа исходную ДНК разделяют на фрагменты при помощи специального рестрикционного (ограничивающего) фермента. Далее эти фрагменты разделяют в полосы, проводя электрофорез в геле. Затем полосы ДНК перемещают из геля на нейлоновую мембрану.

Мембрану обрабатывают радиоактивным ДНК образцом, который связывается с определенной ДНК последовательностью на мембране. Излишки радиоактивного образца смывают. Рентгеночувствительная пленка, которую помещают рядом с нейлоновой мембраной, выявляет радиоактивные образцы. После проявления пленки получают видимые следы полос, называемые ДНК отпечатком (рисунок 1.18) Используя несколько радиоактивных образцов, предназначенных для обнаружения различных полиморфизмов, можно добиться высокой степени различения.

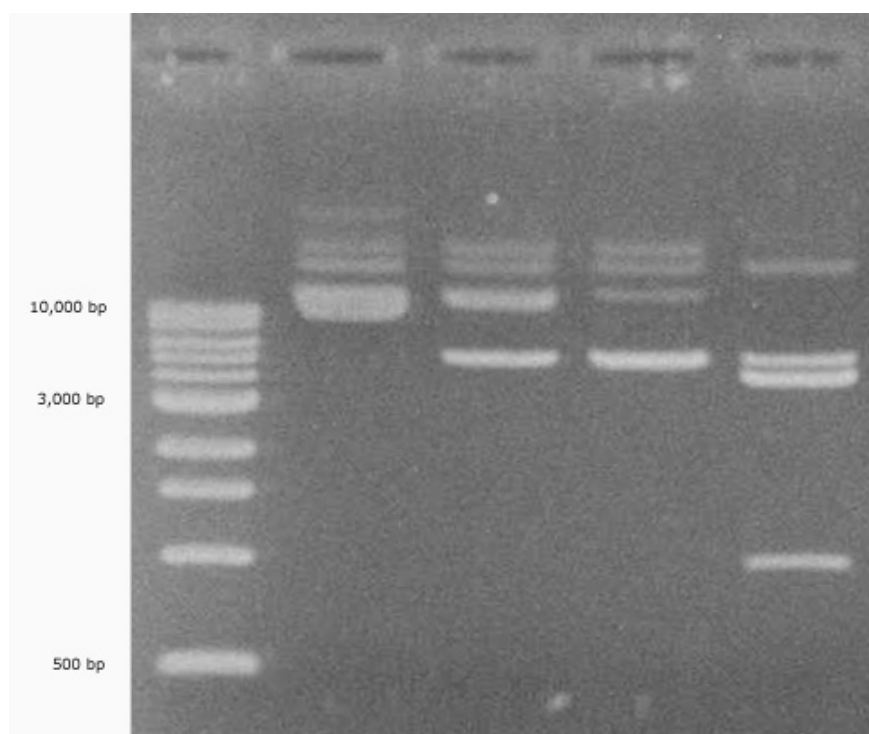


Рисунок 1.18 – ДНК-отпечаток

Основной недостаток ПДРФ-анализа в том, что нельзя заранее определить точные размеры полос, а значит и молекулярный вес фрагментов – он определяется качественно, а не количественно. Так же этот метод требует много времени на анализ и относительно большое количество высококачественного ДНК (пятно крови размером с десятикопеечную монету). Все это делает ПДРФ-анализ трудно применимым.

2) Полимеразная цепная реакция

С открытием ПЦР (полимеразной цепной реакции) распознавание ДНК сделало огромный шаг как в разрешающей способности (способность

установить различия), так и в возможности восстанавливать информацию из малого количества первоначального образца. ПЦР-анализ использует выделение отдельных регионов ДНК при помощи циклического процесса, в котором изменяется температура и используется специальный фермент.

Один из основных недостатков ПДРФ анализа в том, что он слишком медленный и требует большое количество ДНК. В конечном итоге это привело к разработке методов, основанных на ПЦР-анализе, которые используют меньшие количества ДНК при худшем её качестве. Такие системы стали очень популярными из-за простоты в использовании и малом времени получения результата. К недостаткам метода следует отнести сложность определения профиля ДНК для смешанных образцов, т.е. содержащих несколько ДНК.

3) Полиморфизм по длине фрагментов амплификации

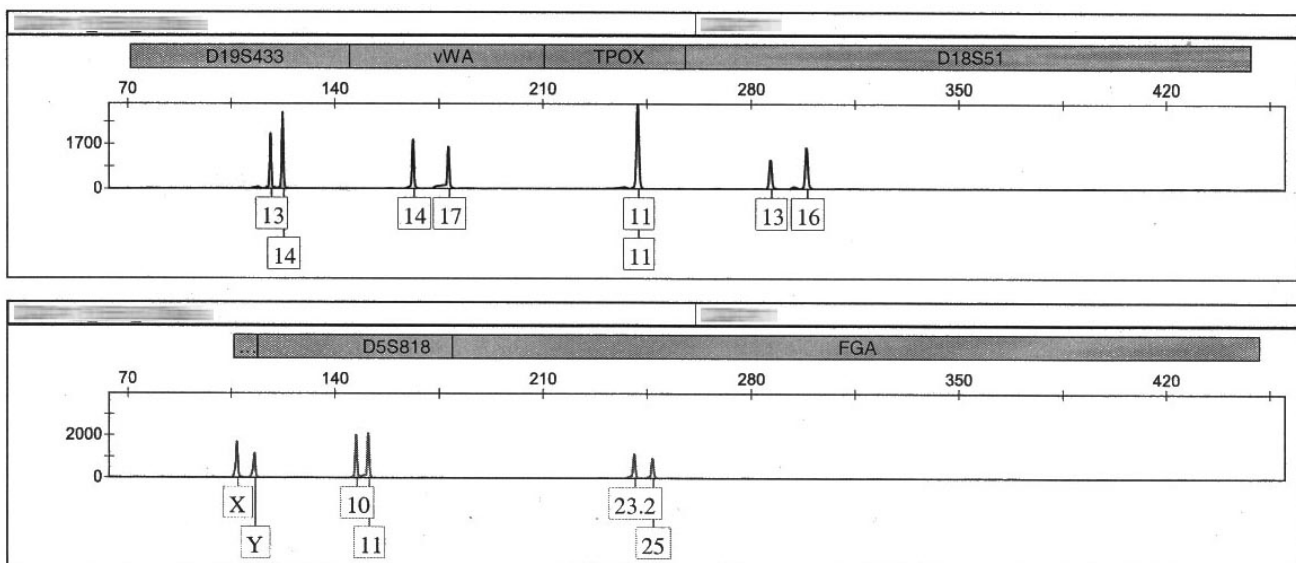
Другой метод, AmpFLP (amplified fragment length polymorphism, полиморфизм по длине фрагментов амплификации) так же вошел в практику в начале 90х. AmpFLP анализ, опять же, является быстрее ПДРФ и использует ПЦР для выделения образцов ДНК. Он основан на особом типе полиморфизмов - VNTR (variable number tandem repeat, варьирующее число tandemных повторов).

AmpFLP анализ легко автоматизируется. Из-за относительно низкой стоимости, и простоты обслуживания, AmpFLP популярен в странах с невысокими доходами. Недостаток в том, что метод может дать достаточно большую ошибку.

4) Короткие повторяющиеся участки

В настоящее время метод STR (short tandem repeat) получил наибольшее распространение. Метод работает с короткими повторяющимися участками. Число повторов в каждом из участков различно. Каждому числу повторений соответствует 5-20% людей. Но если рассматривать большое количество участков, разрешающая способность метода становится исключительно высокой (при рассмотрении 13-ти участков вероятность ложного совпадения

составляет 10^{-18}). Именно это свойство привело к высокой популярности STR анализа.



**Рисунок 1.19 – Частичный STR-профиль человека
(ось X – длина фрагмента, ось Y – интенсивность сигнала)**

Другие методы

При недостатке или очень низком качестве образца используется mtDNA-анализ. В этом методе ДНК извлекается из митохондрий. Дело в том, что в клетке содержится всего 1-2 ядерных ДНК, но много копий митохондриальной ДНК (мтДНК). Благодаря этому, требования к образцу снижаются. Другая особенность – мтДНК передается от матери. Поэтому, мтДНК является очень удобным объектом для изучения родственных связей по материнской линии, эволюции человека, миграции населения, а так же для идентификации людей.

1.3.3 Достоинства

Достоинства перед традиционными методами:

- самый низкий коэффициент ложного допуща.

1.3.4 Недостатки

Возможные недостатки:

- большое время обработки.

1.3.5 Характеристики надежности

К системе предъявляются требования обеспечения как можно более низкого значения FAR-ошибки (10^{-10} и ниже), при достаточно низкой FRR-ошибке (10^{-3}). Действительно, проникновение «чужака» в систему способно принести гораздо более серьезные последствия, чем необходимость повторного прохождения идентификации «своего».

ДНК-идентификация является самым надежным, среди статических биометрических методов аутентификации. В теории вероятность FAR-ошибки находится в пределах от 10^{-10} для RFLP до 10^{-29} при использовании STR. Конечно, при проведении реального анализа, вероятность ошибки возрастает. Но даже при этом, она остается очень низкой, что позволяет использовать процедуру генетического распознавания в таких ответственных ситуациях, как судебная экспертиза.

Методы генетической идентификации очень хорошо подходят для задач, к которым предъявляются повышенные требования надежности вердикта и количеству/качеству первоначальной информации. Повсеместному распространению ДНК-экспертных систем мешают относительная сложность, дороговизна и большие затраты по времени на проведение анализа.

Вопросы для самопроверки

- 1) Что такое ДНК?
- 2) Какие методы идентификации, основанные на ДНК, существуют?
- 3) Достоинства и недостатки метода.
- 4) Характеристики надежности.

Литература

- [1] Урусов А. Генетическая идентификация / Урусов А. // Курс "Защита информации", кафедра радиотехники МФТИ [Электронный ресурс]. – Режим доступа: www.re.mipt.ru/infsec/2007/essay/2007_Genetic_fingerprinting_Urusov.doc – Дата доступа: 16.02.2009.

1.4 Электроэнцефалограмма (ЭЭГ)

1.4.1 Введение

Идентификация личности по сигналам ЭЭГ является одной из новых научных областей, которая может продемонстрировать связь между генетической информацией и ЭЭГ человека. Запись ЭЭГ нетравматична и безопасна; следовательно, ЭЭГ можно использовать как эффективный инструмент идентификации личности. Присутствие генетической информации в ЭЭГ было открыто уже в 1930-х гг. [9]. Тем не менее, оно не исследовалось до 1960-х гг., когда была установлена прямая связь между ЭЭГ человека и его генетической информацией [21]. Большинство предшествующих исследований сосредотачивались на классификации генетически или патологически индуцированных ЭЭГ в целях диагностики, например, при эпилепсии или шизофрении [12]-[20].

Работа [1], напротив, сосредоточена на случаях здоровых людей и ставит своей целью установить взаимнооднозначное соответствие между генетической информацией и некоторыми характерными особенностями зарегистрированных ЭЭГ-сигналов человека. Прямая связь между генетической информацией и ЭЭГ говорит о том, что ЭЭГ должна быть уникальна для каждого человека. Хотя существенных исследований для оценки уникальности ЭЭГ для каждого человека не проводилось, но существуют определенные подтверждения, показывающие, что ЭЭГ, возможно, уникальны [1].

В этом исследовании была сделана попытка выделить подходящие признаки ЭЭГ в качестве биометрических для классификации индивидов с использованием нейронной сети соревновательного типа. В продолжение этого раздела дан краткий обзор данных ЭЭГ и биометрии.

1) Данные ЭЭГ

Мозговые волны (ЭЭГ) – это отклик нейронных клеток на различные раздражители [2]; эти волны на поверхности мозга являются откликами на различные раздражители, и регистрируется сумма всех этих откликов. На кожу головы крепятся несколько электродов для снятия и усиления сигналов. Эти электроды обычно помещаются на стандартные места над главными анатомическими структурами мозга, такими как: лобные, височные и теменные доли [3]. Сигнал ЭЭГ – это временной ряд, имеющий статистические свойства, но эти свойства изменяются во времени, из-за психического состояния и у различных людей.

2) Биометрические характеристики

Любые физиологические признаки, такие как отпечатки пальцев, изображения радужной оболочки или голос [5], которые можно использовать для идентификации личности [4] называются биометрическими. Биометрическая система использует различимые признаки, которыми обладает человек. В работе [5] в качестве идентификационного сигнала использован сигнал ЭЭГ. Извлекаемые признаки – это параметры авторегрессии на определенных промежутках времени. Эти признаки классифицируются нейронной сетью соревновательного типа (Competitive Neural Network).

1.4.2 Авторегрессионный метод идентификации

- *Авторегрессивная модель*

В этой модели последовательность оценивается линейным разностным уравнением во временной области:

$$X(t) = \sum_{i=1}^p a(i)X(t-i) + e(t), \quad (1.7)$$

где текущий член временного ряда $X(t)$ является линейной функцией P предшествующих членов плюс независимый одинаково распределенный (independent identically distributed (i.i.d)) белый шум $e(t)$ [6].

В этой работе применен метод Юла-Уолкера (Yule-Walker) для оценки параметров авторегрессии с использованием критерия наименьших квадратов.

- *Нейронная сеть соревновательного типа*

В нейронной сети соревновательного типа только один из выходных нейронов, имеющий наивысший уровень, победит в состязании.

В этой статье использован усиленный алгоритм обучения. В этом методе присутствует контролер, определяющий нейрон-победитель на обучающей последовательности, но он не определяет реальное значение ожидаемого выхода, поэтому сеть считается безнадзорной. Существует бинарные сигнал ошибки («нуль» или «единица»), например, если ожидаемый нейрон победил, сигнал ошибки – «0», в ином случае сигнал ошибки – «1» и сеть будет пытаться регулировать свои веса до тех пор, пока не победит ожидаемый нейрон.

В выходном слое сети (рисунок 1.20) – N нейронов и каждый нейрон имеет собственный вес (W_n).

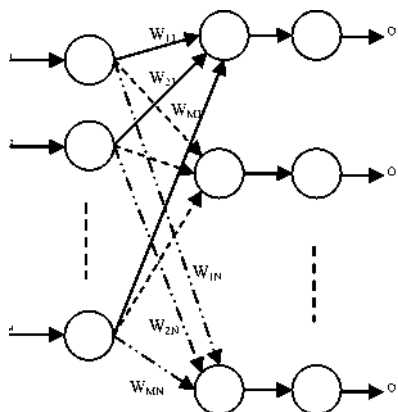


Рисунок 1.20 - Нейронная сеть соревновательного типа

Если дан входной вектор X , выход каждого нейрона рассчитывается по формуле:

$$O_n = e^{\sum_j W_{jn} X_j} \quad (1.8)$$

Нейрон, имеющий наибольшее значение, является победителем. Если нужный нейрон не победил, появляется сигнал ошибки и весовая матрица этого нейрона будет усилена следующим правилом (другие не претерпят никаких изменений):

$$W_n(k) = W_n(k-1) + a(k)(X - W_n) \quad (1.9)$$

где $a(k)$ – обычно небольшое положительное число, называемое тренировочным коэффициентом, этот параметр может изменяться в процессе обучения или оставаться постоянным.

- *Массив данных*

Данные были сняты с 10 здоровых добровольцев (шесть мужчин и четыре женщины). Для каждого человека данные снимаются со 100 каналов на протяжении 24 с частотой дискретизации 170 Гц. Таким образом, для каждого канала записано 4080 отсчетов, которые разделены на восемь периодов по 3 секунды.

1.4.3 Обработка данных

В этой статье [5] предложены два метода получения векторов признаков, одноканальный и многоканальный. Существует небольшая разница между этими методами, но в результатах можно увидеть существенную разницу. Далее представлены оба метода и результаты.

- *Одноканальный метод*

Целью работы было продемонстрировать, что ЭЭГ человека, возможно, уникальна и существует связь между ЭЭГ и генетической информацией. В этом исследовании участвуют 10 человек, произведены 8 измерений по 3 секунды со

100 каналов для каждого человека, т.е. собраны данные 80 измерений с каждого канала.

Целью исследования является извлечение некоторых признаков, по которым можно различить людей. В качестве признаков использованы авторегрессионные параметры каждого измерения. Хотя ЭЭГ по своей природе не является стационарным сигналом, предполагается, что ЭЭГ стационарна в каждом измерении и рассчитываем параметры для каждого измерения. Число параметров различно в различных измерениях.

В одноканальном методе параметры, полученные при каждом измерении, объединяются в вектор, и этот вектор называется вектором признаков. Часть этих векторов подается на контролируруемую нейронную сеть в качестве обучающего множества и после периода обучения все вектора подаются на нейронную сеть в качестве тестовой последовательности. В данном методе 50 векторов из 80 для каждого канала использованы в качестве обучающего множества. Обработка была проведена в системе MATLAB на ПК на базе процессора Pentium 4. В описанных экспериментах был выбран один из 100 каналов, и была проведена обработка всех измерений для каждого человека для выбранного канала.

Специального исследования влияния положения канала на результат не проводилось, но визуальная оценка показывает, что большую точность дают каналы с задней части головы по сравнению с другими каналами. Результаты классификации для случайно выбранных каналов показаны в таблицах 1.1 и 1.2.

Таблица 1.1 – Результаты для одноканального метода

| Канал \ Порядок | 001 | 002 | 003 | 004 |
|-----------------|------|------|------|------|
| 3 | 92.5 | 50 | 62.5 | 55 |
| 5 | 87.5 | 57.5 | 67.5 | 92.5 |
| 7 | 90 | 75 | 65 | 82.5 |
| 9 | 92.5 | 95 | 87.5 | 95 |
| 11 | 90 | 90 | 85 | 97.5 |
| 13 | 92.5 | 90 | 85 | 97.5 |

Процент верной идентификации в зависимости от порядка модели для каналов 001, 002, 003, 004.

Таблица 1.2 – Результаты для одноканального метода

| Канал \ Порядок | 014 | 030 | 050 | 080 |
|-----------------|------|------|------|------|
| 3 | 87.5 | 57.5 | 50 | 85 |
| 5 | 90 | 67.5 | 80 | 87.5 |
| 7 | 82.5 | 62.5 | 90 | 90 |
| 9 | 95 | 87.5 | 95 | 97.5 |
| 11 | 95 | 92.5 | 92.5 | 97.5 |
| 13 | 95 | 92.5 | 92.5 | 97.5 |
| 15 | 95 | 95 | 97.5 | 97.5 |
| 17 | 95 | 95 | 95 | 100 |
| 19 | 95 | 95 | 95 | 97.5 |

Процент верной идентификации в зависимости от порядка модели для каналов 014, 030, 050, 080

- Многоканальный метод

В этом методе была произведена попытка ввести вектор признаков, который давал бы лучший результат классификации. Сформированный вектор является комбинацией параметров авторегрессии различных каналов. Это означает, что после получения параметров авторегрессии для каждого канала, параметры двух, трех или более каналов объединяются в один вектор признаков. Результаты классификации для комбинации из двух случайно выбранных каналов в зависимости от порядка модели показаны в таблицах 1.3 и 1.4, а для комбинации из трех случайно выбранных каналов – в таблицах 1.5 и 1.6. Очевидно, что эти результаты выше, чем для одноканального метода. Таким образом, можно сказать, что сочетание параметрических моделей ЭЭГ для разных каналов демонстрирует большую связь между ЭЭГ и генетической информацией, чем при использовании одного канала. Обратив внимание на порядок модели, можно увидеть, что если он увеличивается до определенного значения (здесь – 11), результат улучшается, но увеличение свыше этого

значения не дает существенного влияния на результат. По всей видимости, необходимая величина порядка зависит от числа испытуемых; и с увеличением числа испытуемых необходим более высокий порядок алгоритма для получения удовлетворительных результатов.

1.4.4 Выводы

В этой работе [5] рассмотрена идентификация личности на основе авторегрессивных параметров, извлеченных из ЭЭГ. Была проведена нейросетевая классификация (реальных) данных ЭЭГ здоровых людей с целью экспериментального исследования связи между ЭЭГ человека и генетической информацией. В этой работе предложены два метода; первый – одноканальный – метод использует авторегрессивные параметры одного канала в качестве вектора признаков, а второй – многоканальный – метод использует комбинацию авторегрессивных параметров различных каналов в качестве вектора признаков. Эти методы дали правильную классификацию порядка 80% - 95% для первого метода порядка 85% - 100% во втором. Очевидно, что комбинация авторегрессивных параметров от различных каналов улучшает классификацию, и при увеличении числа комбинируемых каналов заметно существенное увеличение процента правильной классификации. Эти результаты согласуются с предшествующими исследованиями, показывая то, что ЭЭГ несет генетическую информацию, а также демонстрирует потенциал нашего метода для классификации известных ЭЭГ. Безусловно, требуются обширные эксперименты для получения статистически значимых результатов и подтверждения гипотезы нейрофизиологов о взаимнооднозначном соответствии ЭЭГ и генетического кода.

Общий результат показывает, что данные с задней части головы (над теменными каналами) дают лучшую идентификацию, чем с остальных частей головы. Можно также увидеть, что при увеличении порядка модели больше 11 в эксперименте с 10 подопытными существенных увеличений точности не

наблюдалось; но для большего числа подопытных наименьший подходящий порядок авторегрессивной модели представляется, возможно, большим.

Хотя расчет параметров авторегрессивной модели высокого порядка для большого числа тестируемых с целью идентификации может не быть целесообразным или практичным, единственной целью этой статьи было показать потенциал этих параметров для классификации людей и демонстрация вероятности уникальности ЭЭГ, что раскрывает прямую связь между генетической информацией и ЭЭГ.

Таблица 1.3 – Результаты для многоканального метода

| Канал Порядок | 001,002 | 002,003 | 003,004 | 004,005 |
|------------------|---------|---------|---------|---------|
| 3 | 90 | 57.5 | 70 | 95 |
| 5 | 95 | 77.5 | 95 | 95 |
| 7 | 92.5 | 82.5 | 92.5 | 97.5 |
| 9 | 100 | 90 | 95 | 100 |
| 11 | 100 | 90 | 95 | 100 |
| 13 | 100 | 92.5 | 95 | 100 |
| 15 | 100 | 90 | 95 | 100 |
| 17 | 100 | 87.5 | 97.5 | 100 |
| 19 | 100 | 90 | 97.5 | 100 |

Процент верной идентификации в зависимости от порядка модели приведен в таблице 1.4 для сочетания двух каналов.

Таблица 1.4 – Результаты для многоканального метода

| Канал Порядок | 004,014 | 014,030 | 030,050 | 050,080 |
|------------------|---------|---------|---------|---------|
| 3 | 95 | 87.5 | 77.5 | 75 |
| 5 | 97.5 | 97.5 | 95 | 92.5 |
| 7 | 85 | 92.5 | 92.5 | 95 |
| 9 | 97.5 | 97.5 | 97.5 | 100 |
| 11 | 97.5 | 97.5 | 95 | 100 |
| 13 | 97.5 | 97.5 | 100 | 100 |
| 15 | 95 | 97.5 | 97.5 | 100 |
| 17 | 97.5 | 97.5 | 95 | 100 |
| 19 | 97.5 | 97.5 | 95 | 100 |

Процент верной идентификации в зависимости от порядка модели показано в таблице 1.5 для сочетания двух каналов.

Таблица 1.5 – Результаты для многоканального метода

| Канал Порядок | 001,002,003 | 003,004,005 | 004,014,030 | 014,030,050 |
|------------------|-------------|-------------|-------------|-------------|
| 3 | 87.5 | 87.5 | 90 | 87.5 |
| 5 | 85 | 95 | 97.5 | 97.5 |
| 7 | 90 | 97.5 | 92.5 | 100 |
| 9 | 100 | 100 | 97.5 | 100 |
| 11 | 100 | 100 | 97.5 | 100 |
| 13 | 100 | 100 | 97.5 | 100 |
| 15 | 100 | 100 | 97.5 | 100 |
| 17 | 100 | 100 | 97.5 | 100 |
| 19 | 100 | 100 | 97.5 | 100 |

Процент верной идентификации в зависимости от порядка модели показано в таблице 1.6 для сочетания двух каналов.

Таблица 1.6 – Результаты для многоканального метода

| Канал Порядок | 030,040,050 | 050,060,070 | 040,060,070 | 080,090,100 |
|------------------|-------------|-------------|-------------|-------------|
| 3 | 95 | 92.5 | 95 | 95 |
| 5 | 97.5 | 92.5 | 97.5 | 95 |
| 7 | 97.5 | 92.5 | 100 | 97.5 |
| 9 | 100 | 95 | 100 | 100 |
| 11 | 100 | 95 | 100 | 100 |
| 13 | 100 | 95 | 100 | 100 |
| 15 | 100 | 95 | 100 | 100 |
| 17 | 100 | 95 | 100 | 100 |
| 19 | 100 | 95 | 100 | 100 |

Вопросы для самопроверки

- 1) Что такое ЭЭГ? Основные характеристики ЭЭГ.
- 2) Основная суть авторегрессионного метода идентификации.
- 3) Какие существуют методы обработки данных?
- 4) Основные достоинства и возможные недостатки метода.

Литература

- [1] Mohammadi, G., Person Identification by Using AR Model for EEG Signals / G. Mohammadi [et al.] // Proceedings Of World Academy Of Science, Engineering And Technology. – 2006. – Vol. 11, № 2. – P. 281–285.

1.5 Информационно-волновой обмен в живых организмах

1.5.1 Введение

Одним из фундаментальных свойств живых систем, относящихся к открытым неравновесным системам, является их колебательная природа. Богатство ритмов, обнаруженных во внешней среде, адекватно их обилию, обнаруженному в биологических системах. Так, установлено, что в самых различных биологических, химических и физико-химических процессах происходят синхронные флуктуации различных параметров – макроскопические флуктуации, амплитуда которых коррелирует с космогеофизическими факторами (Шноль С.Э., Намиот В.А., Жвирблис В.Е. и др., 1983; Агулова Л.П., Удальцова Н.В., Шноль С.Э., 1984).

На различных иерархических уровнях – от молекулярно-клеточного до организменного – происходят ритмичные изменения во времени самых различных параметров, а само существование организма как единого целого обеспечивается, по современным представлениям, синхронизацией этих параметров. Чем более сложный интегративный характер имеет биологический процесс, тем частота его меньше (период, соответственно, длиннее). По мере снижения иерархического уровня частота колебаний увеличивается. Для каждого организма характерно наличие колебаний в широком диапазоне частот – от ультрафиолетового диапазона до сверхмедленных колебаний с периодами, равными месяцам и годам – соответствует разным биологическим процессам и различным иерархическим уровням организма.

1. Жизнь на Земле зарождалась на фоне сложного электромагнитного излучения. Электромагнитные и акустические поля и волны в процессе эволюции живых организмов оказывали на них существенное влияние.

2. Живые организмы состоят из множества клеток, каждая из которых содержит огромное количество атомов, молекул, заряженных частиц. Сами живые объекты также являются источником электромагнитных и акустических колебаний в широком диапазоне частот. Живые организмы не только активно используют волновые процессы в своей деятельности, но и способны чутко реагировать на внешние воздействия, имеющие волновую природу.

Живые организмы – открытые системы, обменивающиеся с окружающей средой веществом, энергией и информацией. Живые системы являются неравновесными, самоструктурирующимися, самоорганизующимися.

Волна – периодическое во времени и пространстве возмущение какого-либо параметра процесса, распространяющееся с конечной скоростью и несущее с собой энергию без переноса вещества. Периодические колебания могут иметь сложную разнообразную природу: электронную, атомную, молекулярную, химическую, акустическую, электромагнитную.

В живых системах основные физиологические и биохимические процессы изменяются периодически во времени, обуславливая биоритмы с различными периодами (напр., суточные, сезонные ритмы). Подобные процессы могли вырабатываться с течением эволюции и закреплялись в генетическом аппарате живых организмов.

- периодичность, связанная с вращением Земли вокруг оси (смена дня и ночи), изменяет параметры среды – температуру, спектральный состав света, атмосферное давление, магнитные поля, поток космических частиц, ионизирующих воздух, и др.
- ритмы связанные с колебательными процессами деятельности головного мозга – период от 0,5 до 20 ч;
- поведенческие реакции человека ритмы – с периодом 1,66 – 5 сут.;
- трехнедельные ритмы, связанные с активностью вегетативной нервной системы;
- эндогенные ритмы.

Интегральная электрическая активность нейронов головного мозга – электроэнцефалограмма – представляет собой широкополосный шумовой нестационарный процесс.

Колебания с частотой в диапазоне:

8 – 13 Гц и амплитудой 70 – 100 мкВ – α -ритм

14 – 25 Гц 25 мкВ - β -ритм

0,5 – 3 Гц - δ -ритм

4 – 7 Гц - θ -ритм

Информационный поток в биосистеме связан с функционированием двух каналов – медленного биохимического и быстрого физического (электромагнитного и акустического). Самые быстрые химические реакции проходят за 10^{-6} с, в то же время физические: электронная и ионная поляризация диэлектриков (биополимеров) совершается за $10^{-13} - 10^{-11}$ с.

Ритмы функционирования структурных элементов (клеток) живого организма находятся в высокочастотном диапазоне ($10^8 - 10^{13}$ Гц).

В атмосфере земли есть несколько «окон», через которые осуществляется внешнее воздействие и обмен:

- оптическое «окно», пропускающее часть УФ излучения – 290-390 нм;
- видимая область спектра – 390-760 нм;
- ИК-область спектра 760-1500 нм;
- радиоволновое «окно» – электромагнитные волны с длиной волны от 1 см до 50 м.

Резонансные части живой клетки:

- соматические клетки – $2,39 \cdot 10^{12}$ Гц;
- ядро соматической клетки – $9,55 \cdot 10^{12}$ Гц;
- митохондрии из клетки печени – $3,18 \cdot 10^{13}$;
- хромосома интерфазная – $7,5 \cdot 10^{11}$;
- хромосома метафазная – $1,5 \cdot 10^{13}$;
- молекула ДНК – $2,9 \cdot 10^9$;

- рибосома – $2,65 \cdot 10^{15}$;
- клеточные мембраны – $5 \cdot 10^{10}$.

Это совпадает с частотами электромагнитных волн, излучаемых Солнцем и достигающих поверхности Земли.

Рабочие ритмы функциональных систем организма человека проходят в низкочастотном диапазоне (1,6 – 8,2 Гц):

- ритм электрического потенциала желудка и кишечника 3,8 – 4,6 Гц;
- ритм дыхания 6,3 – 7,6 Гц;
- ритм сердечных сокращений ~ 3,2 Гц;
- ритм электрической активности нервно-мышечного аппарата 2,6 – 6,5 Гц;
- ритм управляющих сигналов головного мозга 0,5 – 13 Гц.

1.5.2 Гиперзвуковое автоволновое поле биоорганизма человека (волны в живых организмах)

В организмах животных и человека представлен широкий спектр вибраций, начиная от эластических сверхмедленных колебаний (натяжений) внеклеточных матричных сетей, вовлекающих в этот процесс клеточные стенки, и кончая когерентными колебаниями цитоскелета, мембран, белков и ДНК. Сюда же примыкают, оставаясь несколько особняком, необычные колебательные процессы – автоволны и солитоны. Последние могут возникать в белках, ДНК, РНК, мембранах и структурироваться на биополимерах, воде.

Одна из моделей такого необычного поведения биосистем – так называемые, Довыдовские солитоны, описывающие возбуждение, локализацию и движение электронов вдоль пептидных цепей белковых молекул в форме уединенных волн, дополняет известную модель Фрелиха о возможности высокополяризованного (лазероподобного) состояния колеблющихся диполей макромолекул клетки, возникающих при Бозе-конденсации фононов

электромагнитных колебаний белков (10^{12} - 10^{13} Гц), ДНК (10^9 Гц), мембран (0.5 - 10^{11} Гц) и цитоскелета (0.1 ГГц).

Наличие когерентных форм информационно-полевых взаимодействий в организме приводит к мысли об эндогенном автосканировании самих себя биосистемами с помощью лазероподобных процессов голографической направленности, о тотальном внутреннем безынерционном полевом автоконтроле метаболизма. Когерентность полей биосистемы неразрывна с их интерференцией и соответственно с голографированием, если есть модуляции излучения и среды записи, в качестве которых могут выступать жидкие и металлические среды биосистемы, включая структурированную воду. Отметим, что идея голографирования в организме на уровне памяти головного мозга высказана достаточно давно (Gabor D., Nature, 1968, v. 217a, p. 548), затем обоснована теоретически и экспериментально доказана (Nibili R., Phys. Rev. A., 1987, v. 15, p. 1901-1922).

Главным механизмом коркового голографирования является упругая волновая осцилляция (звук) мембран клеток в точном соответствии с частотами ЭЭГ кросс-мембранными натрий-калиевыми потоками. Мембранно-глиальные вибраторы представляют собой несколько сотен резонаторов, лежащих в объеме коры мозга. Волны такого звука описываются уравнением Шредингера. Дифракция опорных шредингеровских волн на одиночных фиксированных корковых голограммах реконструирует предметные волны в форме нейронной активности, отображающей исходную картину формирования образа при его первичном возникновении (зрительное или акустическое восприятие, формирование мысли и т.д.). Эндогенное голографирование в коре мозга не исключение; оно многообразно и реализуется на разных уровнях биосистемы в рамках принципов изоморфных отображений.

1.5.3 Частоты живых организмов. Акустоэлектронные явления в живых организмах. Волновые характеристики человека

1. Все клетки живых организмов независимо от вида (микробы, растения, клетки животного и человека) излучают электромагнитные волны миллиметрового диапазона, причем волна каждого вируса, микроба, растения и человека строго индивидуальны.

2. Каждый человек рождается с определенной длиной волны или частотой вибрации или частотой вибрации мембраны клетки (от 3 до 7.5 мм или от 42.0 до 75.7 ГГц). Волна человека постоянна на протяжении всей его жизни, как группа крови, и не изменяется. Ввиду того, что диагностика и определение резонансной частоты человека производится на точках фолевского канала, вероятнее всего, что мы имеем дело с интегральной частотой, образующейся из сигналов, идущих из различных клеток и их морфологических структур. Все эти волновые сигналы для данного организма когерентны.

3. У всякой биологической клетки или другой единицы живого организма должны существовать резонансные частоты, лежащие в одном диапазоне, и в то же время, имеющие небольшие различия, обусловленные индивидуальными биологическими особенностями, связанными с разной конфигурацией клеточных мембран, внутриклеточных белковых подструктур, геномом и т.д., т.е. частоты обладают индивидуальной специфичностью, как и отпечатки пальцев.

4. Внутри клетки распределяются не электромагнитные волны, а акустоэлектрические, имеющие длину волны, соизмеримую с периметром клеточной мембраны, т.е. существуют внутриклеточные преобразователи внешних электромагнитных волн во внутренние акустоэлектрические и обратно. Эти преобразователи аналогичны по строению антенным решеткам, используемым в радиотехнике (см. Планарные антенны сотовых телефонов – Chip News, 7, 2000; Нанополосковые антенны). При нарушении

жизнедеятельности клетки по эндогенным причинам, она для гомеостаза осуществляет структурную и функциональную.

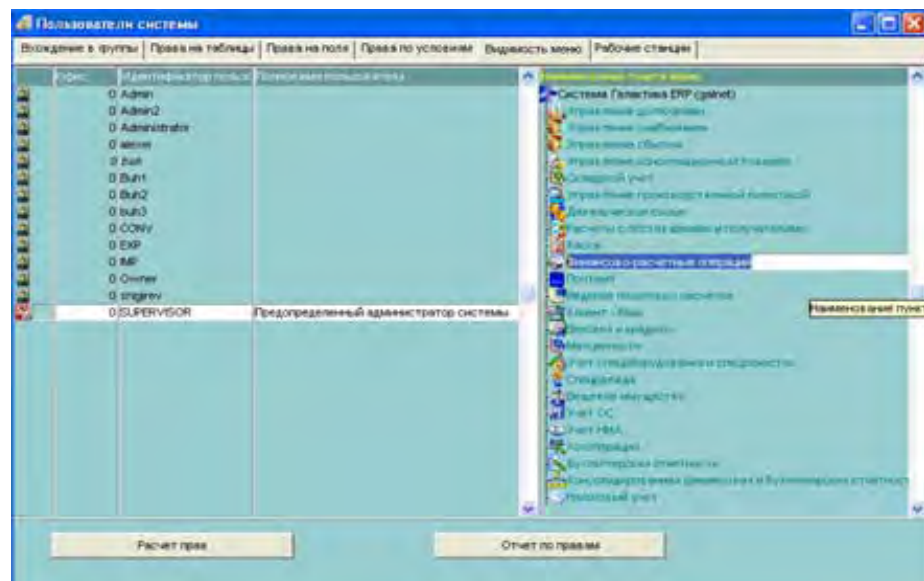
Все биохимические процессы в клетке (за одну минуту в одной клетке протекает 30 тыс. биохимических реакций) протекают строго с определенной скоростью, последовательностью и в заданном направлении только при том ритме колебания мембраны клетки (частоте), которая дается человеку т рождения (при определенной рН-крови). Любые изменения или деформации волновых характеристик мембраны клетки, а также и рН-крови изменяют скорость и последовательность биохимической реакции, частичной или полной замене того или другого фермента. Что спустя годы может проявляться в виде симптомов той или иной болезни, вызывать морфологические изменения в тканях организма.

Вопросы для самопроверки

- 1) Колебательная природа организма.
- 2) Волны в живых организмах.
- 3) Частоты живых организмов. Акустоэлектронные явления в живых организмах. Волновые характеристики человека.

1.6 Аутентификация личности в корпоративной компьютерной сети на основе анализа клавиатурного почерка пользователя

Наиболее распространенной технологией идентификации пользователя в корпоративной компьютерной сети является технология разграничения доступа к информационным ресурсам с помощью различных паролей, назначаемых администратором (рисунок 1.21).



**Рисунок 1.21 – Администрирование пользователей
(система «Галактика ERP»)**

Располагая знанием того или иного пароля, пользователь приобретает возможность использовать определенные службы и приложения, доступ к которым четко обозначен в рамках сетевой политики безопасности, принятой на конкретном предприятии. Однако основным недостатком такой системы является возможность несанкционированного использования паролей с целью получения доступа к конфиденциальной информации.

Особенно болезненные последствия могут иметь место для автоматизированных систем управления предприятием (ERP-систем), когда незаконный доступ к структуре финансовых потоков способен поставить под угрозу сам факт существования конкретной организации. В этой связи,

очевидной становится необходимость использования более совершенных средств защиты информации, к которым следует отнести биометрический метод аутентификации, основанный на распознавании динамической характеристики пользователя, например, его клавиатурного почерка.

В качестве характеристики клавиатурного почерка можно рассматривать временной интервал между нажатиями клавиш. В этом случае мы получаем вектор X , каждый элемент которого i измеряется в секундах. Подобный вектор является, по сути, дискретной последовательностью экспериментальных данных (временным рядом). Данная наблюдаемая реализация системы служит основой для динамического моделирования самой системы. Для реконструкции системы нами была предпринята попытка создания фазового портрета, представляющего собой траекторию в пространстве, образованном в данном случае осью соответствующих временных интервалов, а также осями смещений вышеуказанных интервалов.

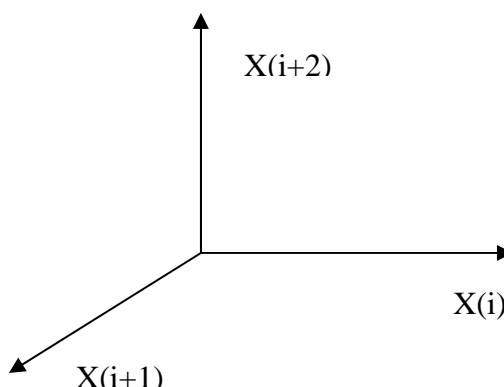


Рисунок 1.22 – Фазовое пространство

Созданная нами программа (среда разработки – MATLAB) производит построение фазовой траектории в вышеуказанном пространстве, характеризующей динамику клавиатурного почерка (рисунок 1.23). Анализ данного фазового портрета осуществляется на основе самоорганизующейся нейронной сети, в механизмах работы которой используется расстояние по Евклиду в качестве меры близости между соответствующими векторами. Таким

образом, мы анализируем проекции фазовой траектории на плоскости $X(i)X(i+1)$, $X(i)X(i+2)$ и $X(i+1)X(i+2)$ соответственно (рисунок 1.24).

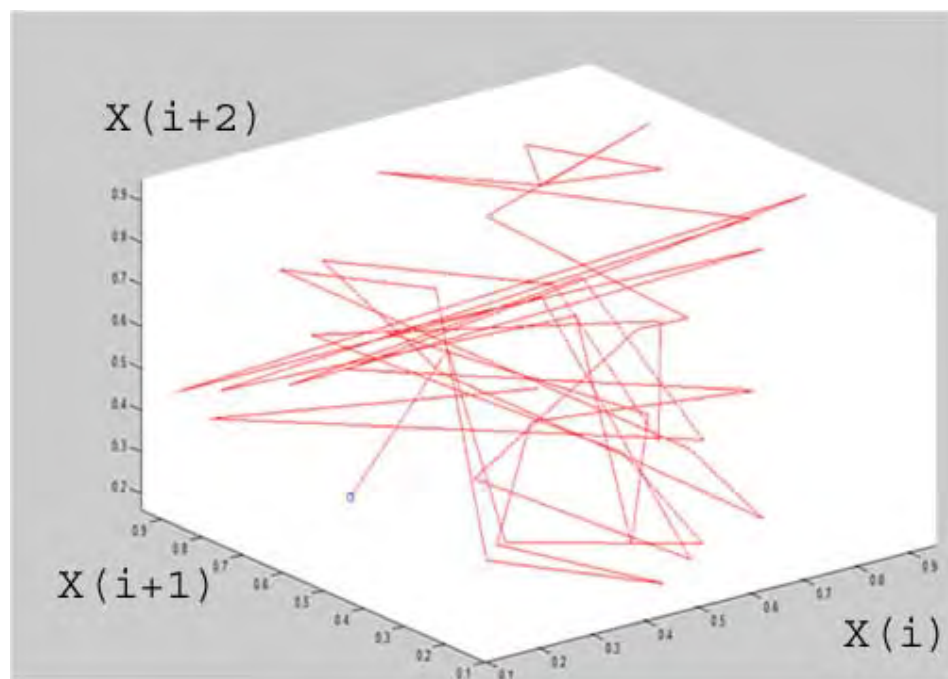


Рисунок 1.23 – Фазовый портрет

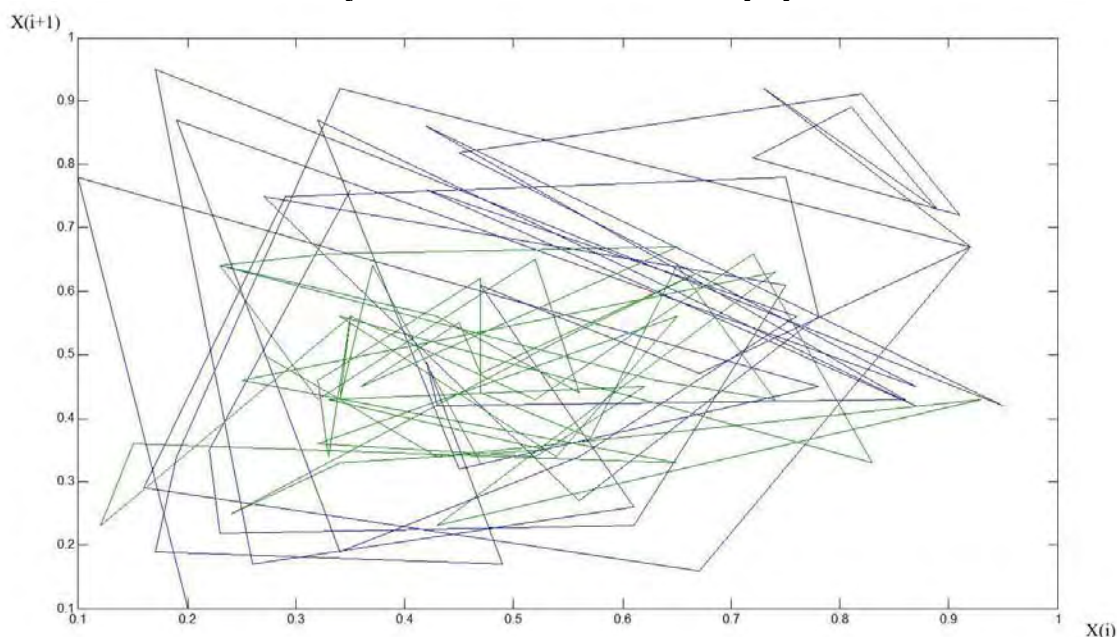


Рисунок 1.24 – Фазовые траектории тестовой (blue) и эталонной (green) реализаций системы (плоскость $X(i)X(i+1)$)

На каждой из трех вышеуказанных плоскостей определяются расстояния по Евклиду между тестовой реализацией системы и эталонной. Усредненные величины найденных расстояний позволяют судить о вероятности принадлежности анализируемого временного ряда конкретному

пользователю. Рассмотрим более подробно принципы функционирования созданной нами модели (рисунок 1.25). Исходный временной ряд содержит реальные значения временных интервалов между нажатиями клавиш за счет использования специально разработанного для этих целей программного приложения, реализованного в программной среде C#. Минимальные требования к операционной системе предполагают использование версии XP SP2.

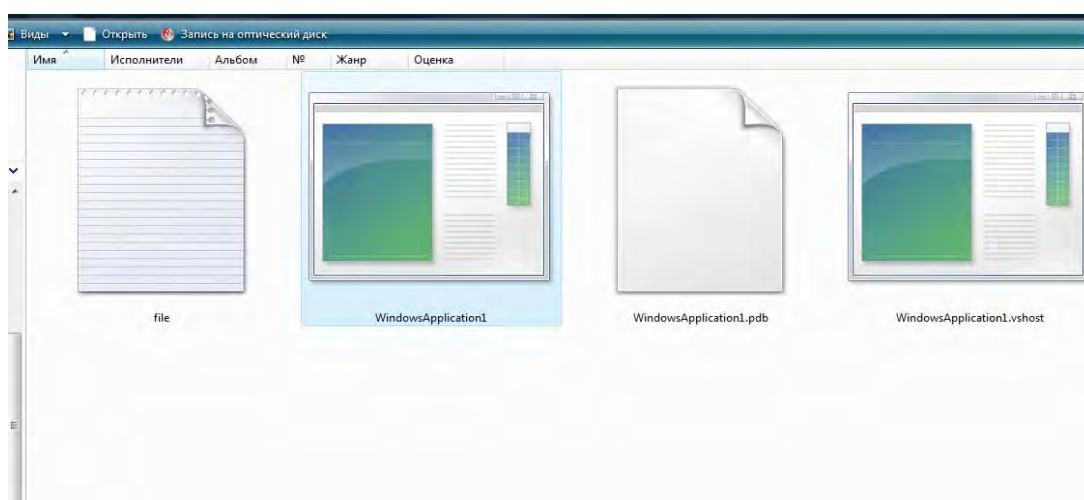


Рисунок 1.25 – Программное приложение для регистрации временных интервалов между нажатиями клавиш (реализация в C#)

Данное приложение запускается из `WindowsApplication1.exe` и позволяет пользователю набирать произвольный текст в отдельном интерфейсном окне и одновременно наблюдать текущее значение временного интервала в миллисекундах между последними нажатиями клавиш (рисунок 1.26).

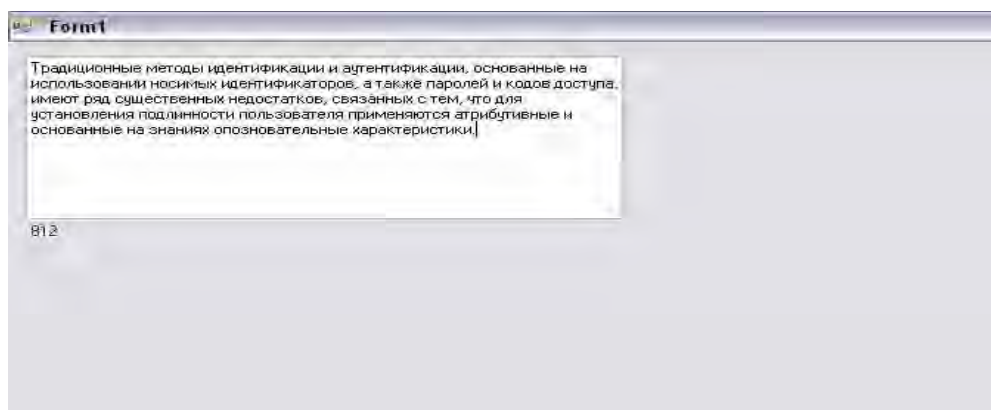


Рисунок 1.26 – Интерфейс ввода текста (приложение на C#)

Параллельно с вводом текста формируется текстовый файл, в который осуществляется динамическая запись значений вышеуказанных интервалов (рисунок 1.27).

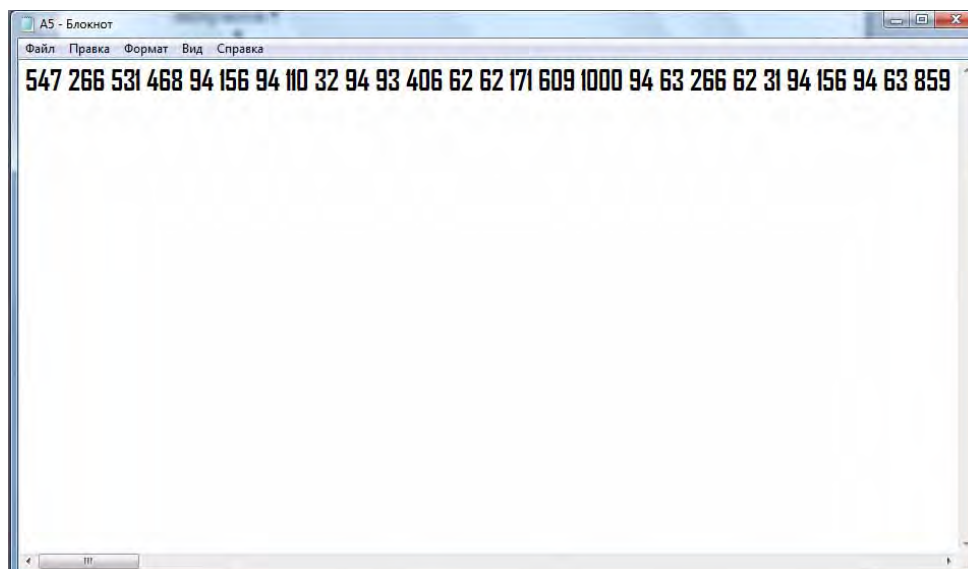


Рисунок 1.27 – Автоматическая запись временного ряда в файл

Сформированный временной ряд является входным вектором для нейронной самоорганизующейся сети. Обучение данной нейронной сети осуществлялось на основе алгоритма нейронного газа. В целях упрощения условий моделирования мы рассматривали ситуацию аутентификации одного пользователя из двух возможных реально существующих пользователей.

Данная нейронная сеть является однослойной, и в ней каждый из двух нейронов соединен с каждым элементом входного вектора, который содержит 100 значений временных интервалов. Изначально весовые коэффициенты определяются произвольным образом, после чего рассчитывается расстояние по Евклиду между входным вектором и векторами весовых коэффициентов, принадлежащих соответствующим нейронам. На каждой итерации нейроны сортируются в зависимости от их расстояния до входного вектора. После сортировки нейроны размещаются в последовательности, соответствующей увеличению удаленности:

$$d_0 < d_1 < d_2 < \dots < d_{n-1}, \quad (1.10)$$

где d_k обозначает удаленность i -го нейрона, занимающего в результате сортировки позицию m в последовательности, возглавляемой нейроном-победителем, которому сопоставлена удаленность d_0 . Победителем признается нейрон, которому соответствует вектор весовых коэффициентов с наименьшим евклидовым расстоянием до входного вектора. Значение функции соседства для i -го нейрона $G(i, x)$ определяется по формуле:

$$G(i, x) = \exp(-(m(i)/\lambda)), \quad (1.11)$$

в которой $m(i)$ обозначает очередность, полученную в результате сортировки, а λ – параметр, уменьшающийся с течением времени. При $\lambda=0$ адаптации подвергается только нейрон победитель, но при $\lambda \neq 0$ уточнению подлежат веса многих нейронов, причем уровень уточнения зависит от величины $G(i, x)$. Нейрон-победитель и все нейроны, лежащие в пределах его окрестности, подвергаются адаптации, в ходе которой их векторы весов изменяются по правилу Кохонена:

$$w_i(k+1) = w_i(k) + \eta_i(k)[x - w_i(k)], \quad (1.12)$$

где $\eta_i(k)$ – коэффициент обучения.

Для достижения хороших результатов самоорганизации процесс обучения начинается с большого значения λ , однако с течением времени его величина значительно уменьшается. Предложено изменять значение $\lambda(k)$ в соответствии с выражением:

$$\lambda(k) = \lambda_{\max} (\lambda_{\min} / \lambda_{\max})^{k/k_{\max}}, \quad (1.13)$$

где $\lambda(k)$ обозначает значение λ на k -ой итерации, а λ_{\min} и λ_{\max} – принятые минимальное и максимальное значения λ соответственно. Коэффициент k_{\max} определяет максимальное заданное количество итераций. Коэффициент обучения i -го нейрона $\eta_i(k)$ изменяется по формуле:

$$\eta_i(k) = \eta_i(0) \left(\frac{\eta_{\min}}{\eta_i(0)} \right)^{k/k_{\max}}, \quad (1.14)$$

в которой $\eta_i(0)$ обозначает начальное значение коэффициента обучения, а η_{\min} – априорно заданное минимальное значение, соответствующее $k=k_{\max}$.

Для возможности работать с нейронной сетью в интерактивном режиме нами был разработан минимальный пользовательский интерфейс, позволяющий конфигурировать структуру нейронной сети и определять ее основные параметры (рисунок 1.28, 1.29).

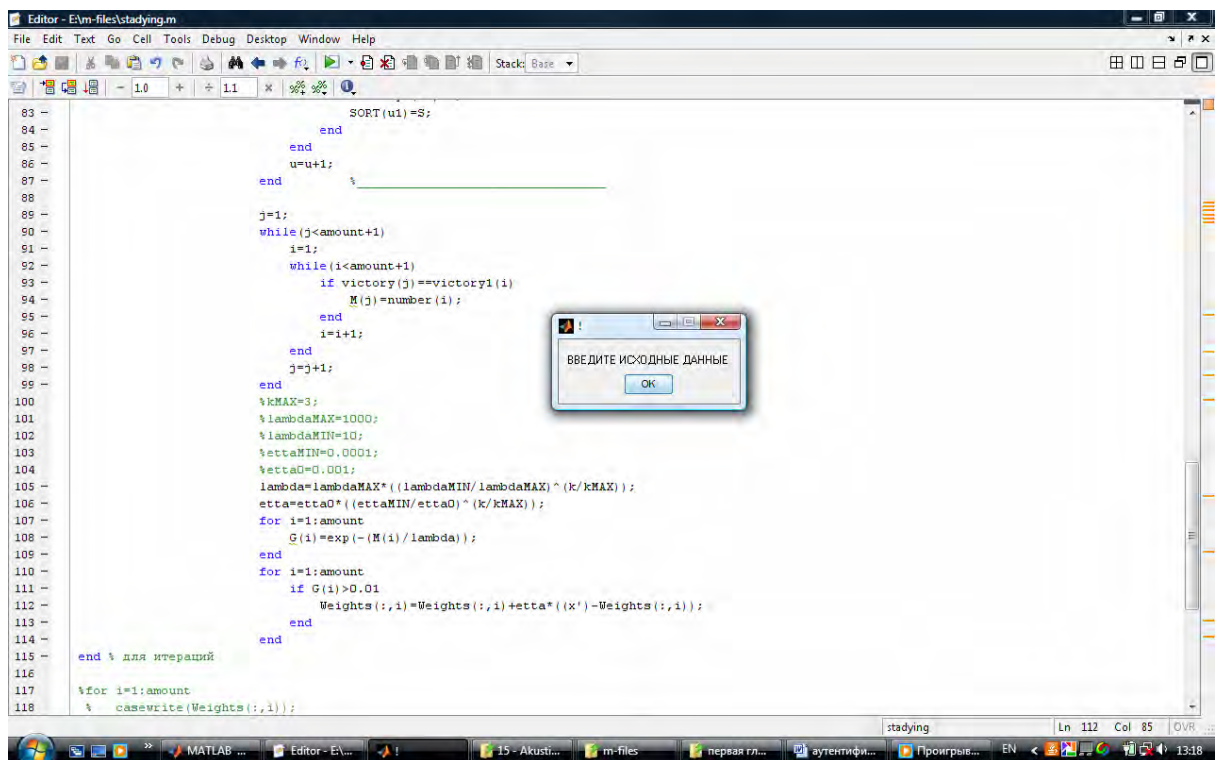


Рисунок 1.28 – Начало работы с нейронной сетью

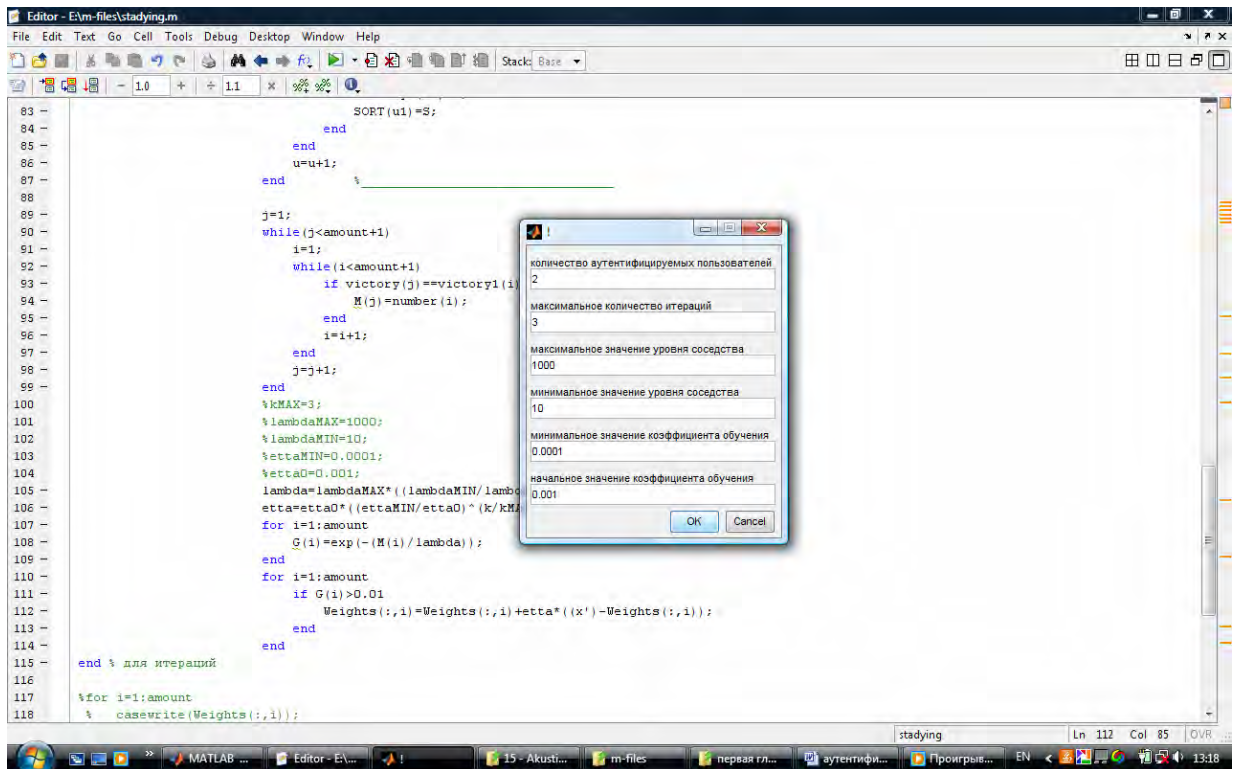


Рисунок 1.29 – Ввод основных параметров нейронной сети

На вход нейронной сети нами последовательно подавались различные векторы – всего сетью в режиме обучения было обработано 50 временных рядов. В итоге была сформирована матрица оптимальных весовых коэффициентов. Данная нейронная сеть использовалась нами для оценки принадлежности анализируемых фазовых траекторий системы тому или иному пользователю. Анализ осуществлялся в трех плоскостях и заключался в поиске расстояний между соответствующими проекциями фазовой траектории и векторами весовых коэффициентов, полученных в ходе процедуры обучения сети. Всего было проанализировано 20 тестовых временных рядов (их принадлежность априорно известна). Ниже представлены изображения, иллюстрирующие результаты проводимой аутентификации пользователей (рисунок 1.30, 1.31).

В результате предварительной работы с моделью можно отметить наличие на текущий момент достаточно невысокого процента корректно обработанных временных рядов – его значение приближается к 60%. Вместе с тем, мы полагаем, что использование подобной технологии аутентификации

пользователя параллельно с применением процедуры разграничения прав на основе паролей способно в значительной степени повысить надежность защиты информационных ресурсов в корпоративной компьютерной сети.

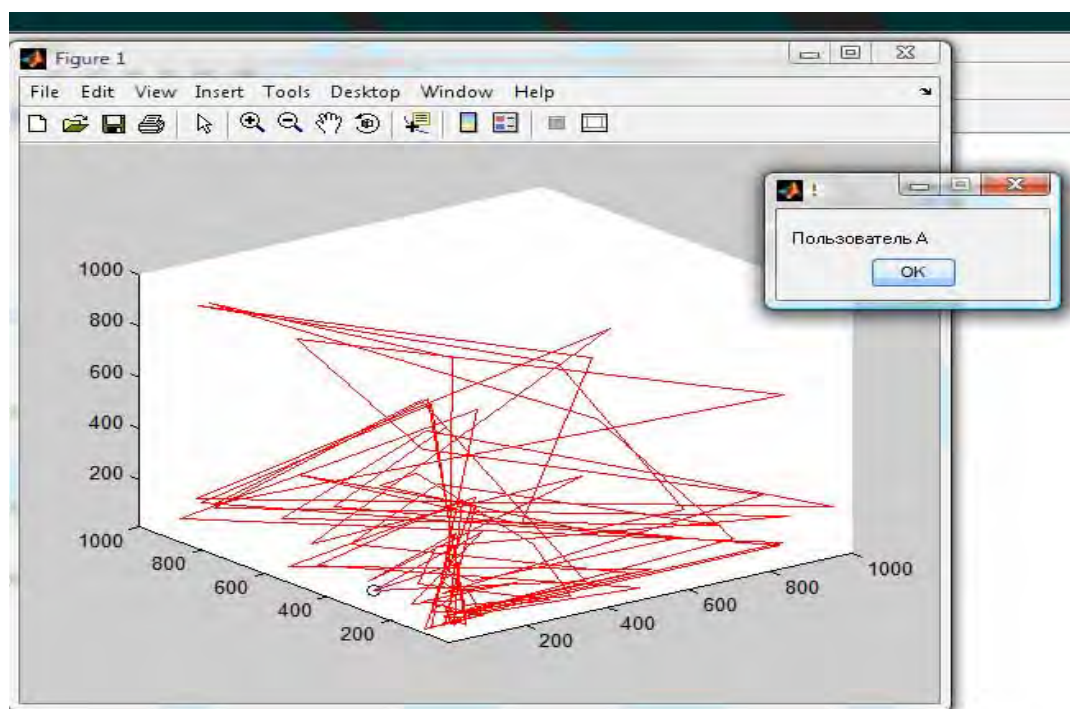


Рисунок 1.30 – Фазовая траектория тестового вектора и результат аутентификации условного пользователя А (пример)

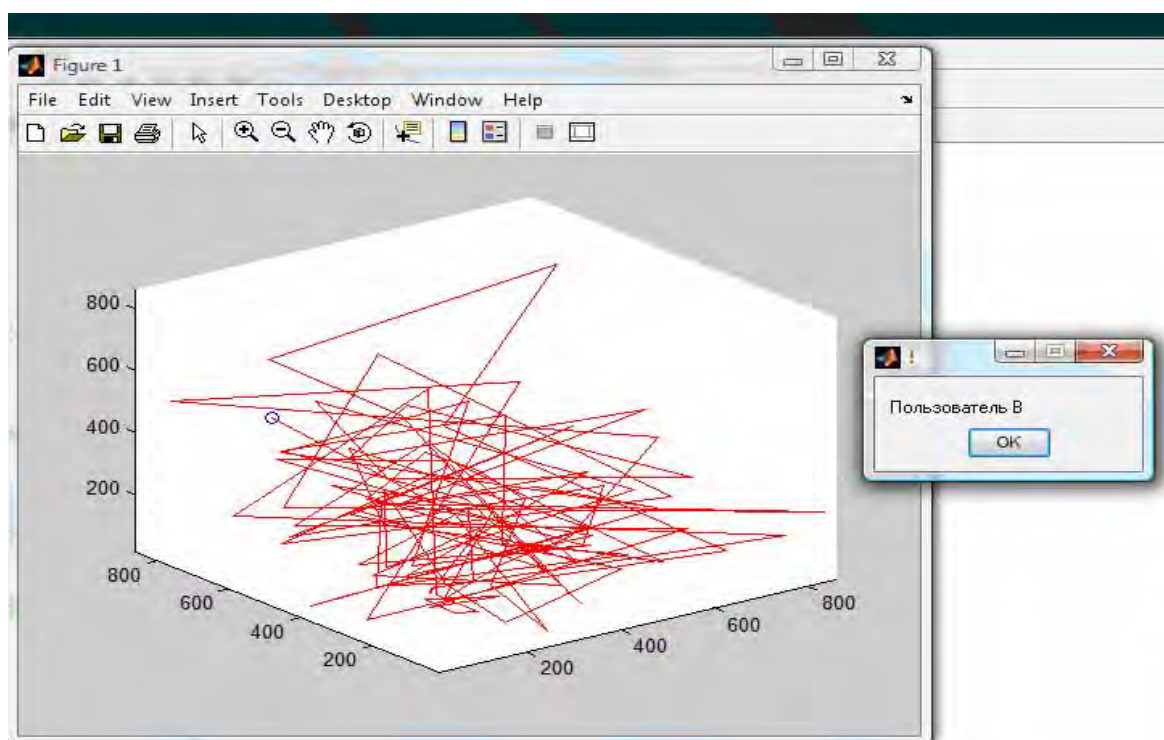


Рисунок 1.31 – Фазовая траектория тестового вектора и результат аутентификации условного пользователя Б (пример)

Пользователь, располагая паролем, получает возможность осуществлять необходимые операции и работать с обозначенным кругом сетевых либо локальных приложений. Вместе с тем, технология аутентификации личности на основе анализа клавиатурного почерка контролирует в режиме реального времени правомочность использования конкретного пароля, причем, даже после его ввода пользователем. Результаты проводимой аутентификации могут храниться на отдельных защищенных сетевых устройствах, что позволит администратору сети обратиться к хронологии действий конкретного пользователя даже в условиях выхода из строя аппаратной части рабочей станции/сервера либо файловой системы журнализации.

В этой связи, нами прилагаются усилия по совершенствованию разработанной модели и механизмов ее функционирования. Прежде всего, планируется провести испытание существующей модели в условиях работы достаточно большого количества операторов. Это, на наш взгляд, позволит более детально проанализировать существующие недостатки нашей модели аутентификации пользователей. Кроме того, следует предпринять шаги по внесению в программу уточняющих признаков, более полно отражающих взаимосвязь динамики клавиатурного почерка с влияющими на нее факторами различной природы.

Ниже представлена функция для обучения самоорганизующейся нейронной сети:

`function stadying`

```
Q_2='ВВЕДИТЕ ИСХОДНЫЕ ДАННЫЕ';  
warn1=msgbox(Q_2, '!');  
uiwait(warn1);
```

```
input1='количество аутентифицируемых пользователей';  
input2='максимальное количество итераций';  
input3='максимальное значение уровня соседства';  
input4='минимальное значение уровня соседства';  
input5='минимальное значение коэффициента обучения';
```

```
input6='начальное значение коэффициента обучения';
```

```
M_2=inputdlg({input1 input2 input3 input4 input5 input6},'!',1);
```

```
M_22=char(M_2);  
casewrite(M_22,'E:\m-files\data.txt');
```

```
data_string=textread('E:\m-files\data.txt','%s');  
amount=str2num(data_string{1});  
kMAX=str2num(data_string{2});  
lambdaMAX=str2num(data_string{3});  
lambdaMIN=str2num(data_string{4});  
ettaMIN=str2num(data_string{5});  
etta0=str2num(data_string{6});
```

```
Weights=zeros(100,amount); % исходная матрица весовых коэффициентов
```

```
user1=textread('E:\m-files\A1.txt','%s');  
user2=textread('E:\m-files\B1.txt','%s');
```

```
for i=1:100  
    A_string(i)=str2num(user1{i});  
end
```

```
for i=1:100  
    B_string(i)=str2num(user2{i});  
end
```

```
A(:,1)=A_string';  
B(:,1)=B_string';
```

```
Weights(:,1)=A;  
Weights(:,2)=B; % сформирована исходная матрица весовых коэффициентов  
% _____
```

```
x_string=textread('E:\m-files\Enter.txt','%s'); % Входной вектор x
```

```
for i=1:100  
    x(i)=str2num(x_string{i});  
end
```

```
for k=1:kMAX % количество итераций для алгоритма нейронного газа
```

```
for v=1:amount
```

```
D(v)=dist(x,Weights(:,v)); % поиск расстояния между входным вектором и  
соответствующим нейроном
```

```
end
```

```
victory=D;
```

```
u=1;
```

```
victory1=victory;
```

```
for i=1:amount
```

```
    number(1,i)=i-1;
```

```
end
```

```
SORT=number; % _____
```

```
while(u<amount+1)
```

```
    for u1=1:amount
```

```
        if victory1(u)<victory1(u1)
```

```
            l=victory1(u1);
```

```
            L=SORT(u1);
```

```
            s=victory1(u); % сортировка вектора расстояний
```

```
            S=SORT(u);
```

```
            victory1(u)=l;
```

```
            SORT(u)=L;
```

```
            victory1(u1)=s;
```

```
            SORT(u1)=S;
```

```
        end
```

```
    end
```

```
    u=u+1;
```

```
end % _____
```

```
j=1;
```

```
while(j<amount+1)
```

```
    i=1;
```

```
    while(i<amount+1)
```

```
        if victory(j)==victory1(i)
```

```
            M(j)=number(i);
```

```
        end
```

```
        i=i+1;
```

```
    end
```

```
    j=j+1;
```

```
end
```

```
lambda=lambdaMAX*((lambdaMIN/lambdaMAX)^(k/kMAX));
```

```
etta=etta0*((ettaMIN/etta0)^(k/kMAX));
```

```
for i=1:amount
```

```
    G(i)=exp(-(M(i)/lambda));
```

```
end
```

```
for i=1:amount
```

```

        if G(i)>0.01
            Weights(:,i)=Weights(:,i)+etta*((x')-Weights(:,i));
        end
    end
end % для итераций

for i=1:amount
    casewrite(Weights(:,i));
end

```

Также показан алгоритм работы функции для анализа фазовой траектории:

```

function recognition
% for 3D
WT=textread('E:\files\Enter.txt','%s'); % входной вектор (временной ряд)

w=zeros(100,1);

for i=1:100
    w(i)=str2num(WT{i}); % вектор чисел
end

X=zeros(98,1); % x
Y=zeros(98,1); % y
Z=zeros(98,1); % z

for i=1:98
    X(i,1)=w(i,1); % ось x
end

for i=1:98
    Y(i,1)=w(i+1,1); % ось y
end

for i=1:98
    Z(i,1)=w(i+2,1); % ось z
end

comet3(X',Y',Z') % фазовая траектория

% сравнение траекторий на плоскостях XY, YZ, ZX

```

```

Ideal_string=textread('E:\m-files\result.txt','%s');

for i=1:100
    Ideal(i,1)=str2num(Ideal_string{i*2-1});
end
for i=1:100
    Ideal(i,2)=str2num(Ideal_string{i*2});
end

for i=1:98
X_userA(i,1)=Ideal(i,1);
X_userB(i,1)=Ideal(i,2); % ось x
end

for i=1:98
    Y_userA(i,1)=Ideal(i+1,1);
    Y_userB(i,1)=Ideal(i+1,2); % ось y
end

for i=1:98
    Z_userA(i,1)=Ideal(i+2,1);
    Z_userB(i,1)=Ideal(i+2,2); % ось z
end

%Плоскость
XY_____

Dist_X_userA=0;
Dist_Y_userA=0;
Dist_X_userB=0;
Dist_Y_userB=0;

for i=1:98
    Dist_X_userA=Dist_X_userA+((X(i)-X_userA(i))^2);
    Dist_Y_userA=Dist_Y_userA+((Y(i)-Y_userA(i))^2);
    Dist_X_userB=Dist_X_userB+((X(i)-X_userB(i))^2);
    Dist_Y_userB=Dist_Y_userB+((Y(i)-Y_userB(i))^2);
end

Dist_XY_userA=sqrt(Dist_X_userA+Dist_Y_userA); % Расстояние на
плоскости XY (пользователь A)

```

```
Dist_XY_userB=sqrt(Dist_X_userB+Dist_Y_userB); % Расстояние на
плоскости XY (пользователь B)
```

```
%ПЛОСКОСТЬ
XZ_____
```

```
Dist_X1_userA=0;
Dist_Z1_userA=0;
Dist_X1_userB=0;
Dist_Z1_userB=0;
```

```
for i=1:98
```

```
    Dist_X1_userA=Dist_X1_userA+((X(i)-X_userA(i))^2);
    Dist_Z1_userA=Dist_Z1_userA+((Y(i)-Z_userA(i))^2);
    Dist_X1_userB=Dist_X1_userB+((X(i)-X_userB(i))^2);
    Dist_Z1_userB=Dist_Z1_userB+((Y(i)-Z_userB(i))^2);
```

```
end
```

```
Dist_XZ_userA=sqrt(Dist_X1_userA+Dist_Z1_userA); % Расстояние на
плоскости XZ (A)
```

```
Dist_XZ_userB=sqrt(Dist_X1_userB+Dist_Z1_userB); % Расстояние на
плоскости XZ (B)
```

```
%ПЛОСКОСТЬ
YZ_____
```

```
Dist_Y2_userA=0;
Dist_Z2_userA=0;
Dist_Y2_userB=0;
Dist_Z2_userB=0;
```

```
for i=1:98
```

```
    Dist_Y2_userA=Dist_Y2_userA+((Y(i)-Y_userA(i))^2);
    Dist_Z2_userA=Dist_Z2_userA+((Y(i)-Z_userA(i))^2);
    Dist_Y2_userB=Dist_Y2_userB+((Y(i)-Y_userB(i))^2);
    Dist_Z2_userB=Dist_Z2_userB+((Y(i)-Z_userB(i))^2);
```

```
end
```

```
Dist_YZ_userA=sqrt(Dist_Y2_userA+Dist_Z2_userA); % Расстояние на
плоскости YZ (A)
```

```
Dist_YZ_userB=sqrt(Dist_Y2_userB+Dist_Z2_userB); % Расстояние на
плоскости YZ (B)
```

```
Dist_userA=(Dist_XY_userA+Dist_XZ_userA+Dist_YZ_userA)/3 % среднее  
расстояние между траекториями
```

```
Dist_userB=(Dist_XY_userB+Dist_XZ_userB+Dist_YZ_userB)/3
```

```
DIST=[Dist_userA Dist_userB];
```

```
victory=DIST;
```

```
u=1;
```

```
victory1=victory;
```

```
for i=1:2
```

```
    number(1,i)=i;
```

```
end
```

```
SORT=number; % _____
```

```
while(u<3)
```

```
    for u1=1:2
```

```
        if victory1(u)<victory1(u1)
```

```
            l=victory1(u1);
```

```
            L=SORT(u1);
```

```
            s=victory1(u); % сортировка вектора расстояний
```

```
            S=SORT(u);
```

```
            victory1(u)=l;
```

```
            SORT(u)=L;
```

```
            victory1(u1)=s;
```

```
            SORT(u1)=S;
```

```
        end
```

```
    end
```

```
    u=u+1;
```

```
end % _____
```

```
j=1;
```

```
while(j<3)
```

```
    i=1;
```

```
    while(i<3)
```

```
        if victory(j)==victory1(i)
```

```
            M(j)=number(i);
```

```
        end
```

```
        i=i+1;
```

```
    end
```

```
    j=j+1;
```

```
end
```

```
users_phase={'Пользователь А'
```

```
            'Пользователь В'};
```

```
index=M(1); % порядковый номер победителя
```

```
    mess_phase=msgbox(users_phase{index}, '!').
```

1.6.1 Аутентификация по наноструктуре пальца

Нанотехнология и технические средства, основанные на научных результатах теории помехоустойчивого кодирования, теории распознавания образов, криптографии, современной сенсорной и компьютерной технике и интеллектуального интерфейса представляют собой самый надежный способ защиты материальных объектов, безопасности аутентификации и идентификации личности [1-3]. Наноструктура поверхности объекта позволяет не только полностью защитить информацию, которую она хранит, но также исключает ее подделку или фальсификацию. Принцип суперзащиты личности по наноструктуре поверхности объекта основывается на том, что любой объект, в том числе, например, палец человека, характеризуется совокупностью отдельных признаков, однозначно связанных с набором некоторых физических, химических и биологических характеристик.

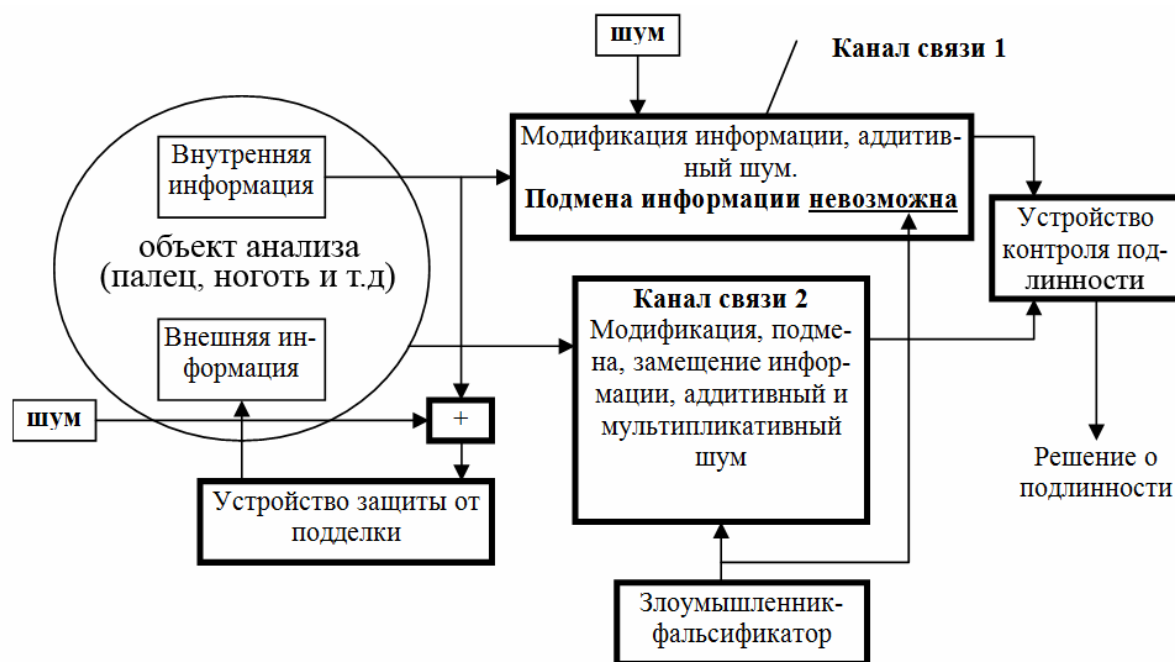
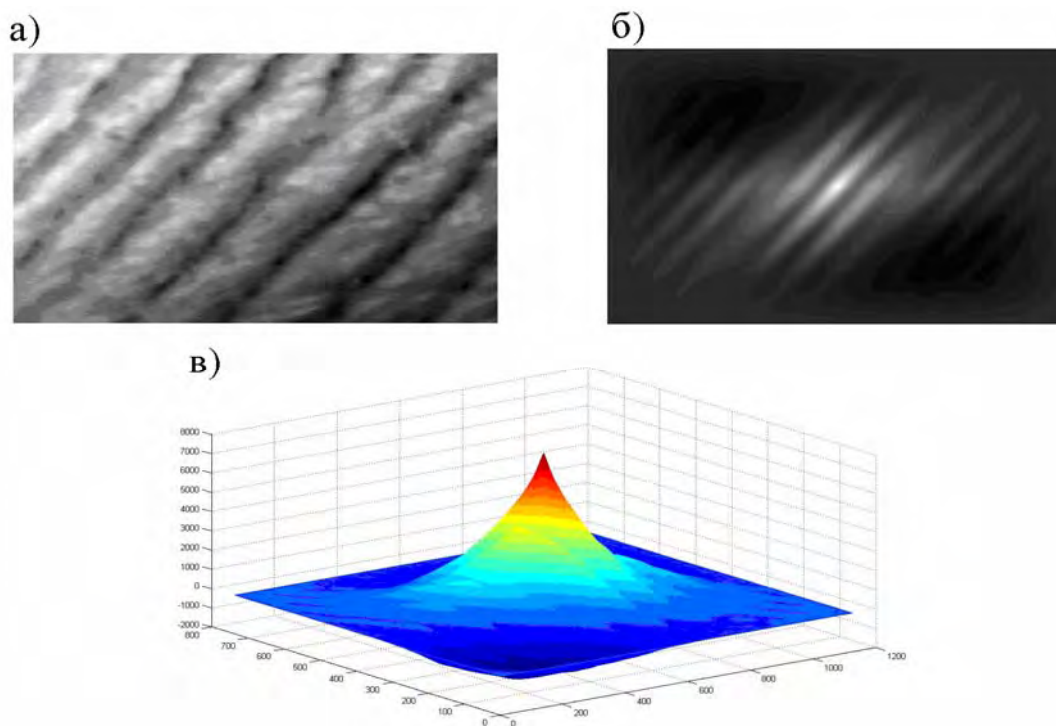


Рисунок 1.32 – Объекты биометрии – канал связи

При этом палец человека, как и любой материальный объект, в процессе жизнедеятельности человека подвержен внешним влияниям (ссадины, порезы), которые искажают традиционные биометрические характеристики и приводят к

расхождению защитных признаков проверяемого и эталонного объектов. Окончательно внешние факторы приводят к ложному распознаванию системой несанкционированных, нарушенных или фальшивых данных (рисунок 1.32).

Для минимизации ошибки применяется принцип анализа групповых признаков микро-наноструктуры биометрического информационного образа, т.е. совокупность полностью совпадающих физико-химических и биологических характеристик наноструктуры пальца. Микро-наноинформационные образы, например, микрорельеф поверхности пальца с наноузором и линий микропор, после формирования эталонов для расчета функции двух(трех)мерной взаимной корреляции точности принадлежности к определенному классу объектов представляет собой модель суперзащиты биометрических образов объекта от фальсификации защищенной базы (рисунок 1.33).



а – изображение отпечатка пальца, б – изображение двумерной функции взаимной корреляции между отпечатком пальца и эталонным изображением, в – изображение трехмерной функции взаимной корреляции между отпечатком пальца и эталонным изображением

Рисунок 1.33 – Технология суперзащиты биометрических данных

Кроме того, для распознавания могут быть использованы механическая (затухание волн, их отражение), электронная (контактная разность потенциалов экзоэмиссия и др), газовая (запах, вкус); оптическая составляющие (отражение, преломление и др.) с наноразрешением измеряемых параметров, которые позволяют сформировать эталонные образы для сравнения с текущим объектом. Злоумышленник не в состоянии подменить данные, например, наноструктуры пальца, а защита внешнего канала криптографическими методами (синхронные, асинхронные, нейрокриптография) позволяют обеспечить суперзащиту и высокую биометрическую безопасность.

1.6.2 Аутентификация пользователя в корпоративной компьютерной сети на основе анализа капиллярного узора пальцев

На современном этапе развития биометрических технологий все более широкое применение находит технология, способная идентифицировать человека по расположению кровеносных сосудов в его пальцах. В данной технологии используется не поверхностный рисунок пальца, а более глубокий, на основе вен и капилляров. Считается, что подобная технология может более достоверно определять человека по сравнению с другими существующими системами биометрической идентификации. Стоит отметить, что ученые сходятся во мнении относительно уникальности капиллярного рисунка у каждого человека – он действительно уникален (рисунок 1.34).



Рисунок. 1.34 – Капиллярный узор руки

Этот факт, в свою очередь, определяет значительную сложность процедуры возможной фальсификации подобного рисунка, что делает данную технологию более совершенной по сравнению с технологией анализа дактилоскопических отпечатков. Центральным звеном технологии распознавания пользователя на основе капиллярной сетки пальцев является механизм определения принадлежности анализируемого графического образа (капиллярного узора) определенному пользователю. Нами была предпринята попытка создания компьютерной модели, осуществляющей процедуру аутентификации пользователя на основе анализа капиллярной картины его пальцев. Данная модель базируется на использовании нейронной сети, на вход которой поступает анализируемый графический образ. Предполагается, что полученное в результате сканирования изображение является монохромным, что позволяет поставить ему в соответствие бинарную матрицу, единицы в которой соответствуют более темным участкам капиллярной сетки, а нули – более светлым.

Основная идея функционирования данной сети состоит в минимизации расстояния Хемминга между тестовым множеством, подаваемым на вход, и векторами обучающих выборок, закодированных в структуре сети [4]. Первый слой имеет однонаправленное распространение сигналов от входа к выходу и фиксированные значения весов, а второй слой состоит из нейронов, связанных обратными связями по принципу «каждый с каждым», так что при этом существует ненулевая связь входа нейрона со своим собственным выходом. Веса нейронов во втором слое также постоянны, а разные нейроны связаны отрицательной (подавляющей) обратной связью. С собственным выходом нейрон связан положительной (возбуждающей) обратной связью, поэтому нейроны в этом слое функционируют таким образом, что в каждой фиксированной ситуации активизируется только один нейрон, а остальные пребывают в состоянии покоя. В первой фазе функционирования сети на ее вход подается вектор, состоящий из 100 элементов. После предъявления этого

вектора на выходах 10-ти нейронов первого слоя (аутентифицируется один пользователь из десяти) генерируются сигналы, задающие начальные состояния 10-ти нейронов второго слоя. Величины данных сигналов представляют собой соответствующие расстояния по Хеммингу (рисунок 1.35).

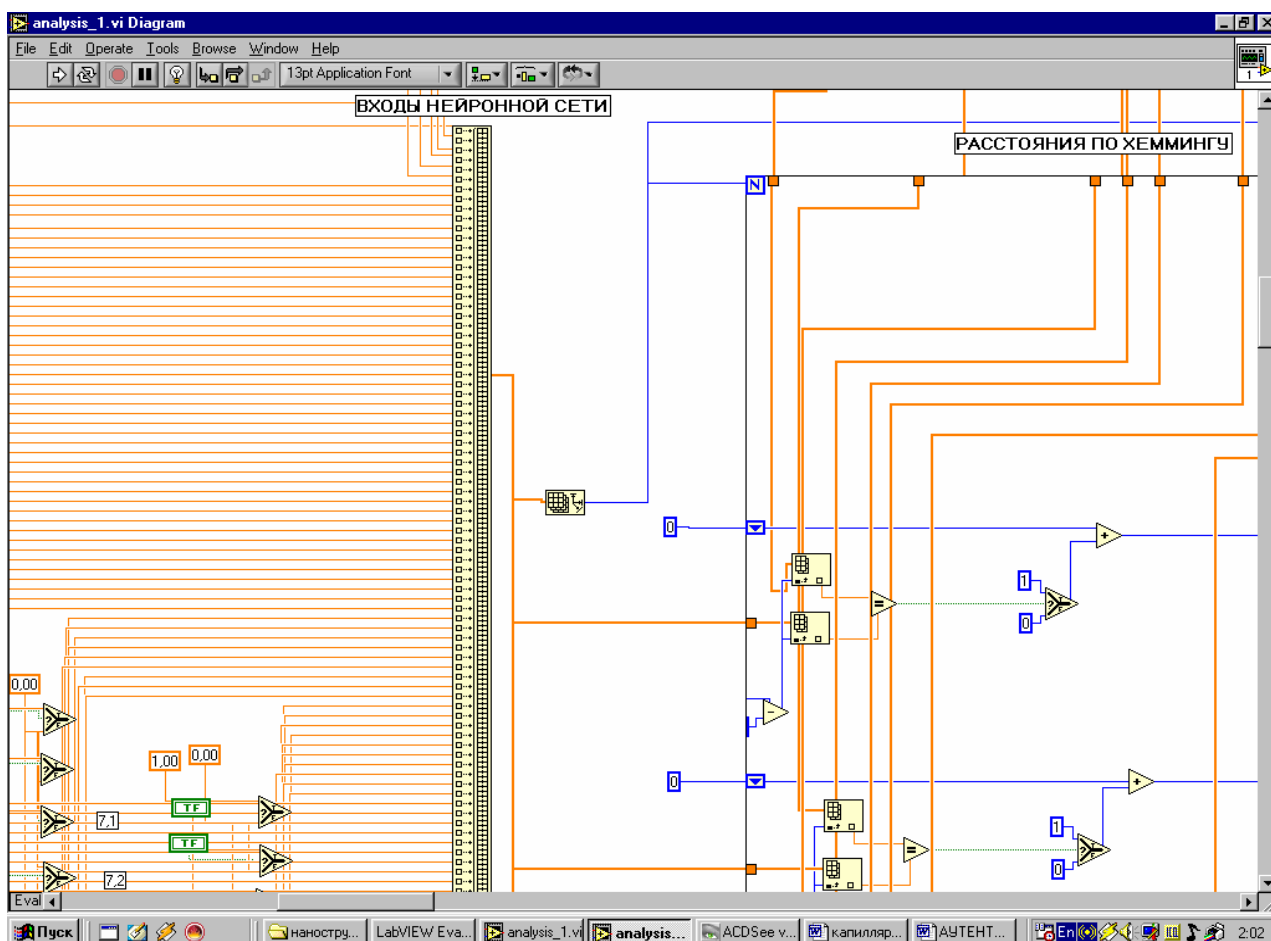


Рисунок 1.35 – Программная реализация в графической среде LabVIEW первой фазы функционирования нейронной сети (определение расстояния по Хеммингу)

Во второй фазе запускается итерационный процесс внутри второго слоя, который завершается в момент, когда все нейроны, кроме одного, перейдут в нулевое состояние. Окончательно нейрон-победитель связан с соответствующим пользователем, аутентификация которого была осуществлена успешно (рисунок 1.36). Данная программная реализация позволяет моделировать предоставление на вход нейронной сети соответствующего

графического образа, и наблюдать реакцию сети в виде ответа относительно принадлежности моделируемого капиллярного узора одному из десяти пользователей.

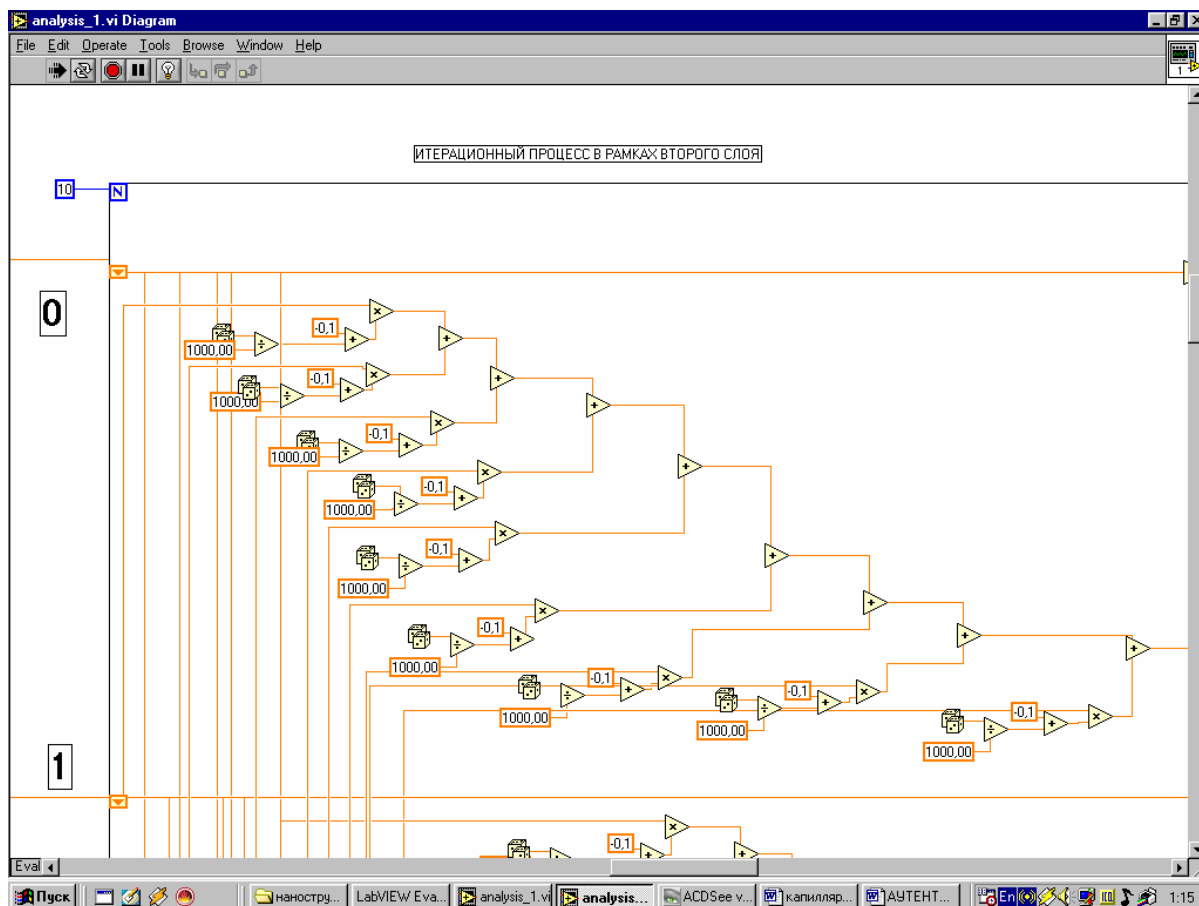


Рисунок 1.36 – Программная реализация в графической среде LabVIEW второй фазы функционирования нейронной сети (итерационный процесс)

В ходе тестирования нейронной сети более 90% анализируемых бинарных множеств были обработаны корректно, что свидетельствует о значительной эффективности использования подобного механизма для аутентификации пользователей на основе анализа графических образов (капиллярных узоров). Для удобства работы в графической среде программирования LabVIEW нами был разработан оптимизированный интерфейс (рисунок 1.37) [5]. Пользователь может создавать упрощенную модель капиллярной сетки, делая определенные области изображения темнее

или светлее. На изображениях, приведенных на рисунке 1.38, представлена графическая информация особенностей технологии получения капиллярной картины, а также пример реального капиллярного рисунка, полученного путем сканирования поверхности пальца реального субъекта исследования.

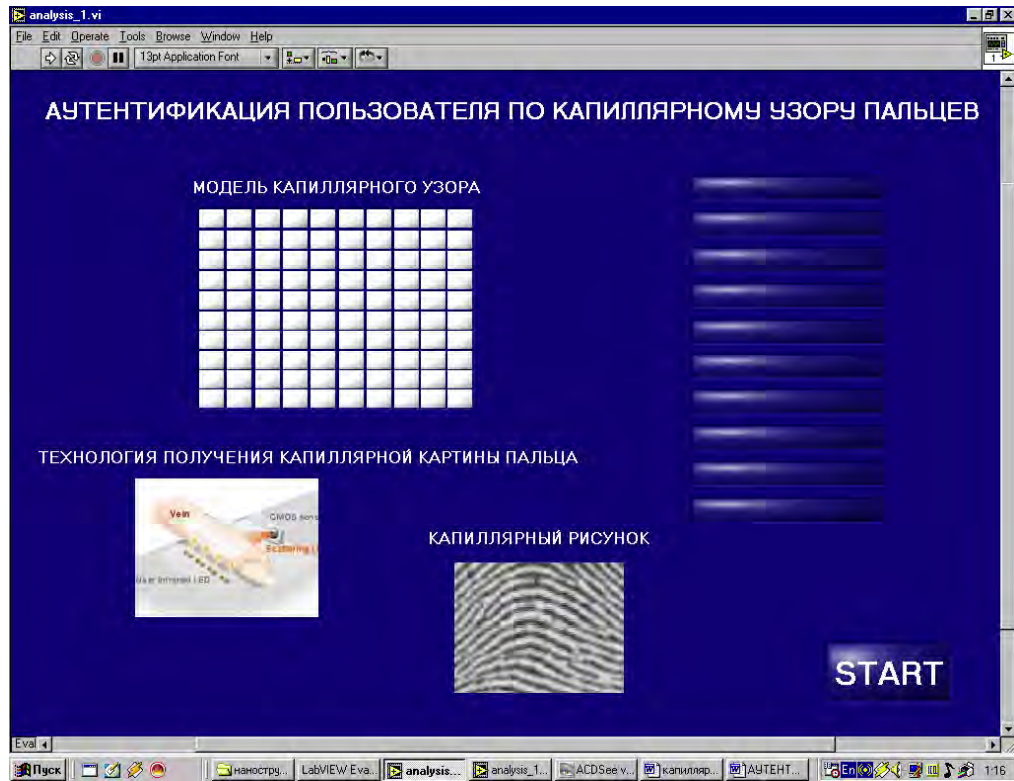


Рисунок 1.37 – Интерфейс пользователя для работы с нейронной сетью



Рисунок 1.38 – Аутентификация пользователя А (а) и Н (б)

Кнопка «start» позволяет запускать и приостанавливать работу модели. В правой части экрана расположены элементы интерфейса, сигнализирующие о результатах аутентификации в режиме реального времени. Таким образом, эффективность технологии аутентификации пользователя по капиллярному узору пальцев может быть повышена, на наш взгляд, за счет параллельного использования метода аутентификации пользователя на основе динамики клавиатурного почерка, базирующегося на нелинейно-динамическом анализе временных рядов, а также традиционной технологии распознавания по дактилоскопическим отпечаткам пальцев. Совместное использование вышеуказанных подходов должно в значительной степени способствовать повышению безопасности и уровня прозрачности действий отдельных пользователей, а также безопасности всей корпоративной компьютерной сети в целом.

Вопросы для самопроверки

- 1) Каковы основы динамического моделирования по характеристиками клавиатурного подчёрка? Как проводится построение фазового портрета системы?
- 2) Самоорганизующиеся нейронные сети. В чем состоит правило Кохонена?
- 3) В чем сущность супертехнологии защиты по наноструктуре поверхности объекта? Какая информация может при этом сниматься с пальца?
- 4) В чем заключаются преимущества и недостатки биометрии по капиллярному узору? Принцип работы подобных устройств распознавания.

Литература

- [1] Колешко, В.М. Контроль в технологии микроэлектроники / В.М. Колешко, П.П. Гойденко, Л.Д. Буйко. – Минск, Наука и техника, 1979. – 312 с.
- [2] Колешко, В.М. Микроэлектронные преобразователи информации на поверхностных акустических волнах / В.М. Колешко, Ю.В. Мешков. – М.: ЦНИИ «Электроника», 1985. – 95 с.
- [3] Колешко В.М. Компьютерная диагностика информатики человека / В.М. Колешко, Н.В. Хмурович, А.А. Хмурович. – Минск, БИТА, 1996. – 60 с.
- [4] Осовский, С. Нейронные сети для обработки информации / С. Осовский; пер. с польского И.Д. Рудинского. – М.: Финансы и статистика, 2004. – 344 с.
- [5] Тревис, Дж. LabVIEW для всех / Дж. Тревис; пер. с англ. Клушин Н.А. – М. : ДМК Пресс; ПриборКомплект, 2004. – 544 с.

2 ЗАЩИТА ИНФОРМАЦИИ

2.1 Введение

Любая биометрическая система может быть описана как четырехступенчатая (рисунок 2.1).

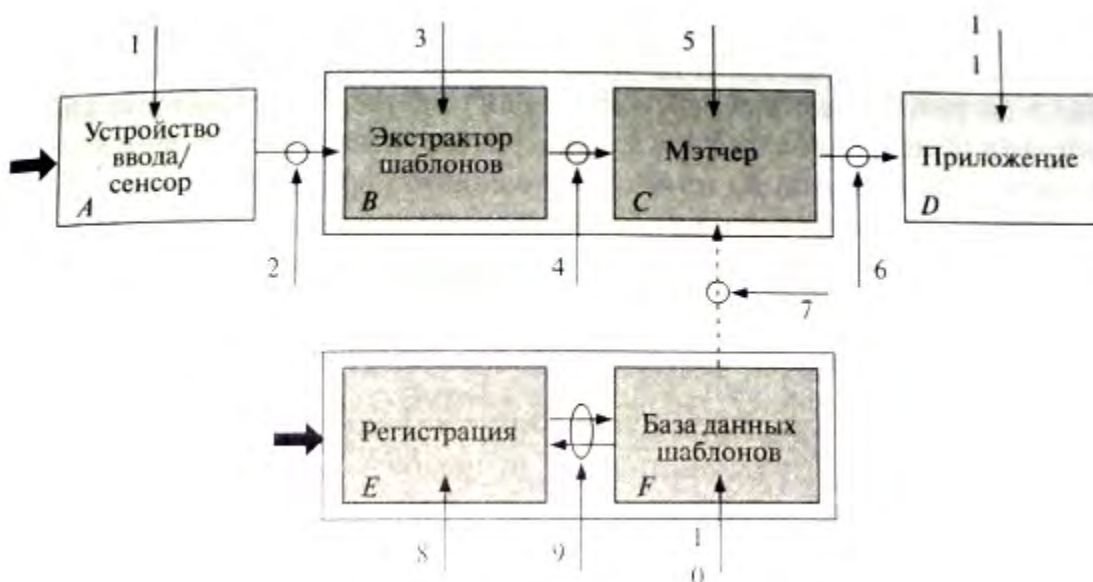


Рисунок 2.1– Составляющие аутентификационной и регистрационной систем и точки атак

Рассмотрим эти ступени более детально:

- а) 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. С другой стороны, 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.

- б) 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.

Проблема конструирования репрезентации является сложной задачей и требует дальнейшего исследования.

в) На третьей 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.

г) 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, то есть как приемлемый уровень коэффициента ложного доступа (КЛД), от которого 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 рисунке 1.39, хотя регистрация P - более сложный процесс, чем в парольных системах, базу данных биометрических образцов F можно считать аналогом базы с сохраненными паролями.

д) 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.

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

Атаки на биометрические идентификаторы

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

1. 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.

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:

2. 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, – симитированный 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.

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

4. 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 для сохранения шаблонов, угроза атаки в этой точке становится реальной.

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

Обман

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

6. Угроза № 6 – подмена исходящей информации из модуля мэтчера S (точка б). 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.

Внутренние атаки

Базы данных зарегистрированных пользователей могут быть локальными или удаленными, то есть 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.

7. 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 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:

8. Точка атаки № 8 – это центр регистрации или приложение. Процессы регистрации и аутентификации схожи в том смысле, что они оба исполняют аутентификационный протокол, и поэтому регистрация подвержена атакам в точках 1-6.

9. 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 .

10. 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.

2.2 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.

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. Существуют две взаимосвязанные проблемы:

Любая биометрическая технология обычно воспринимается как негуманная и представляющая угрозу для конфиденциальности, 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 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, поэтому нужно всегда помнить, что биометрические системы не предназначены для сбора такой информации.

И все же существуют проблемы конфиденциальности, связанные с биометрической аутентификацией. Когда возникает проблема с правами на секретность информации и биометрических параметров, лучше всего вспомнить Томаса Джефферсона, который сказал: «Если мы не можем защитить все наши права, позвольте нам защитить то, что мы можем».

Существует тенденция к централизации регистрации: вещи, которые должны всегда быть с владельцем, теперь очень тщательно регистрируются, например университетские степени и академические справки, документы на дома (теперь регистрируемые в самом городе), паспорта и т. д. Информация об этих данных находится в доверенных организациях.

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 (рисунок 2.2).



Рисунок 2.2 – 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.

Намеренные повторяющиеся трансформации

Работы по данной теме 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, то есть 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. То есть биометрический сигнал должен быть трансформирован сразу после получения, либо сигнал может быть обработан

обычным способом, а уже выделенные свойства могут подвергнуться трансформации. В следующих двух разделах описаны два вида трансформаций, хотя, конечно, существуют и другие варианты.

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 рисунке 2.3, где изображения на рисунках 2.3, в и 2.3, г выглядят одинаково, хотя не совпадают с 2.3, а и 2.3, 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 как, например, расстояние между глазами на лице.



Рисунок 2.3 – Два отпечатка пальца (а, б) с искаженным одним и тем же способом оригиналом изображения (в, г)

Радужная оболочка – цветная область вокруг зрачка – другой параметр, который мы сейчас рассмотрим. Параметр, полученный из изображения радужной оболочки пользователя, представлен на рисунке 2.4. Аутентификация и идентификация пользователя при помощи радужной оболочки происходят путем разработки бинарного кода, кода радужки, $s = '0100101110...011'$ 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. Рисунок 2.4 показывает пример, где изображение радужки справа является намерено искаженной версией изображения слева.

Подобные техники трансформации можно применять для сигналов, которые не являются изображениями. На рисунке 2.5 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 рисунке 2.5 можно разделить на временные отрезки A, B, C, D соответственно последовательности времени (A, B, C, D) . На этом рис. временные отрезки имеют равную длину, но это не обязательное условие. Зашифрованный голосовой сигнал представляет собой последовательность $(\underline{A}, C, D B)$. Подчеркнутое \underline{A} означает, что отрезок \underline{A} воспроизводится в обратном порядке.

Заметьте, что для такого шифрования голоса, как на рисунке 2.5, требуется минимальная регистрация записи голоса.

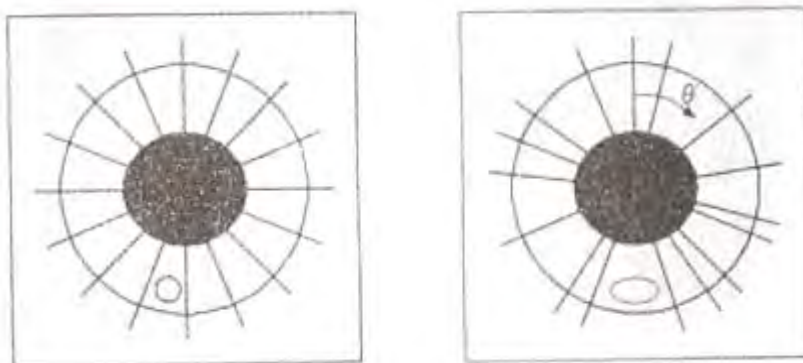


Рисунок 2.4 – Оригиналу изображения радужной оболочки может быть зашифрован разными способами

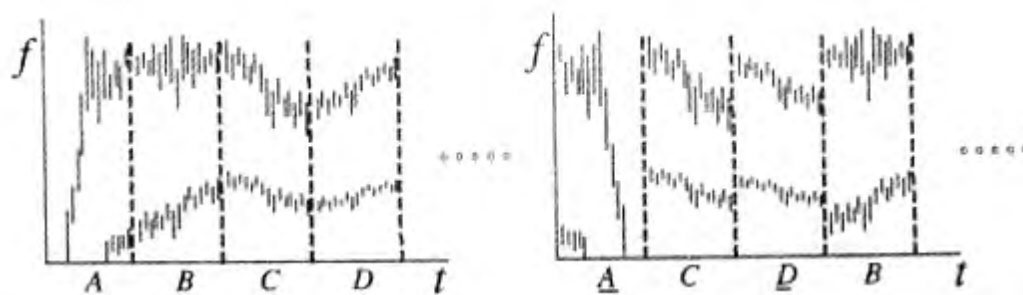


Рисунок 2.5 – Оригиналу записи голоса (слева) зашифрован при помощи деления сигнала на отрезки

Зашифрованная запись голоса (справа) создается путем случайной перегруппировки сегментов и воспроизведения их в обратном порядке.

Искажение свойств

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

$$S = \{(x_i, y_i, q_i); i = 1, K, M\} \quad (2.1)$$

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

$$S = \{(x_i, y_i, q_i); i = 1, K, M\} \rightarrow S'' = \{(X_i, Y_i, Q_i); i = 1, K, M\} \quad (2.2)$$

Рисунок 2.6 показывает, как x -координаты множества точек S могут быть трансформированы путем преобразования $X = F(x)$. Такие многочленные необратимые трансформации:

$$Y = G(y), Q = H(q) \quad (2.3)$$

могут быть использованы для остальных координат множества точек из выражения. Здесь используется полином третьего порядка.

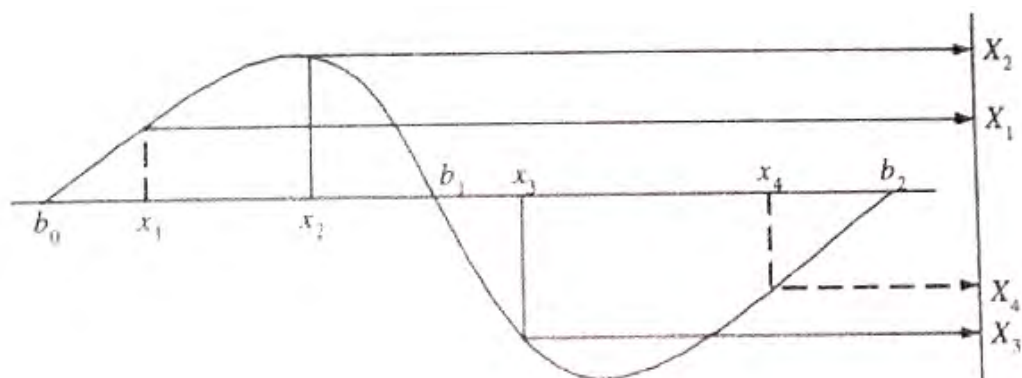


Рисунок 2.6 – Изображение одной координаты многомерного множества точек в новой плоскости координат

Сжатие и шифрование

Сокращение биометрических параметров значительно отличается от сжатия сигнала с использованием стандартных техник обработки сигнала. При сжатии сигнал временно теряет свои пространственные характеристики. То есть 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 необратимом искажении, которое мы используем, 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.

Вопросы для самопроверки

- 1) Ступени биометрической системы.
- 2) Какие существуют угрозы и атаки на биометрические идентификаторы?
- 3) Проблемы конфиденциальности и защиты информации.
- 4) Проблемы искажения сигналов и свойств.
- 5) Проблемы сжатия и шифрования.

Литература

- [1] Руководство по биометрии / Р.М. Болл [и др.]; – Москва: Техносфера, 2007. – 368 с.