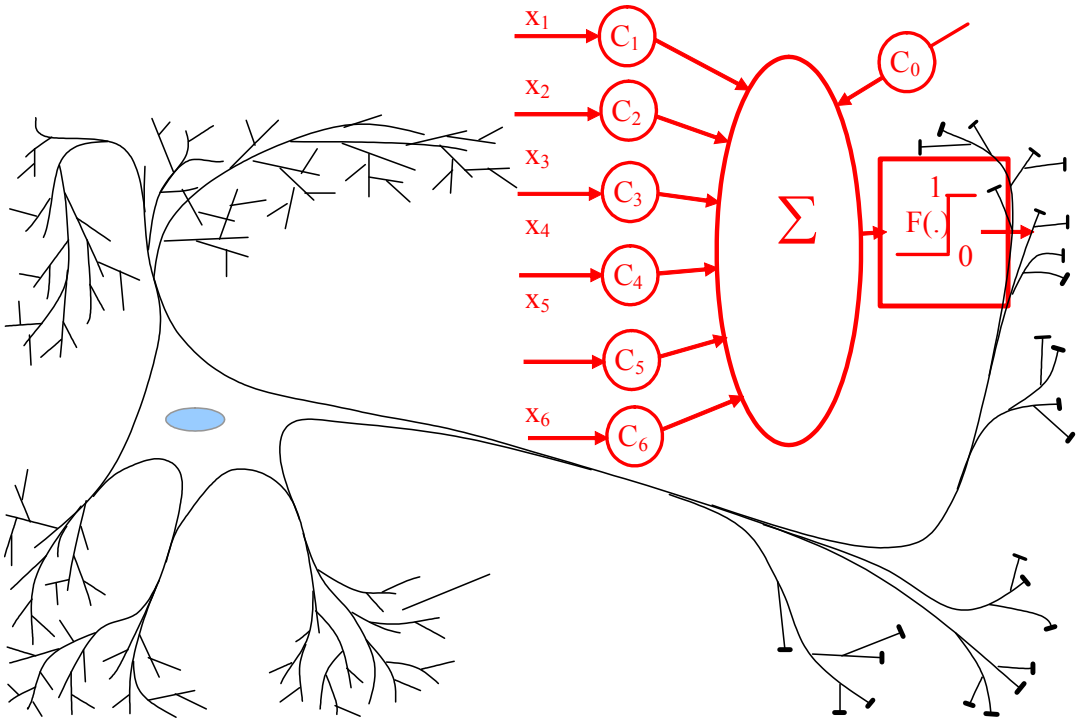
УДК: 519.24; 53; 57.017
И 18
ББК 32.818

Издательство АО «ПНИЭИ»,
электронный вариант книги размещен на сайте
http://пниэи.рф/activity/science/BOOK16.pdf

Иванов А.И.

МНОГОМЕРНАЯ НЕЙРОСЕТЕВАЯ ОБРАБОТКА БИОМЕТРИЧЕСКИХ ДАННЫХ С ПРОГРАММНЫМ ВОСПРОИЗВЕДЕНИЕМ ЭФФЕКТОВ КВАНТОВОЙ СУПЕРПОЗИЦИИ

(монография)



Пенза - 2016

УДК: 519.24; 53; 57.017
И 18
ББК 32.818

Рецензенты:
Доктор техн. наук, проф. Д.В. Пащенко – заведующий кафедрой «Вычислительная техника» ФГБОУ ВО «Пензенский государственный университет»

Доктор техн. наук, проф. С.И. Геращенко – заведующий кафедрой «Медицинская кибернетика и информатика» ФГБОУ ВО «Пензенский государственный университет»

Иванов А.И.
Многомерная нейросетевая обработка биометрических данных с программным воспроизведением эффектов квантовой суперпозиции. Монография. Пенза – 2016 г. Издательство АО «Пензенский научно-исследовательский электротехнический институт» (ОА «ПНИЭИ») – 133 с. http://пниэи.рф/activity/science/BOOK16.pdf

Изложены теоретические и практические аспекты программного моделирования нейросетевых преобразователей биометрия-код, способных поддерживать квантовую суперпозицию множества выходных кодовых состояний искусственных нейронов. Показано, что переход от исследования обычных выходных кодов нейронов в пространство расстояний Хэмминга, упрощает задачу оценки многомерной энтропии нейросетевых преобразователей. Дано описание решений двух континуально-квантовых задач. Первой, является задача извлечения знаний из обученной искусственной нейронной сети. Второй, является задача усиления мощности хи-квадрат критерия на малых тестовых выборках. Сделано предположение о том, что электроэнцефалограммы работы головного мозга человека – это побочный эффект поддержки квантовой суперпозиции и квантовой запутанности естественными нейронами головного мозга.

Рассмотренные в книге нейросетевые вычисления легко реализуются в среде инженерных расчетов MathCAD. Даны примеры программ моделирования квантовых эффектов, возникающих при нейросетевой обработке данных, написанных на языке MathCAD.

Книга рассчитана на студентов, аспирантов, преподавателей и научных работников, занимающихся многомерной обработкой больших объемов «плохих» данных большими искусственными нейронными сетями, находящими в режиме поддержки квантовой суперпозиции.

ОГЛАВЛЕНИЕ.

Предисловие

Создание в прошлом веке квантовой механики привело к переосмыслению многих интуитивно понятных постулатов классической физики и математики. Как один из результатов, в 1980 году нашим соотечественником Юрием Маниным была высказана идея создания квантовых компьютеров на принципиально новом способе вычислений. Под квантовые вычислительные машины были созданы строгие математические алгоритмы, однако для их реализации нужна новая элементная база. Работы по созданию новой элементной базы активно ведутся во всех странах, но задача создания квантовых вычислительных элементов, оказалась технически очень сложной.

Основная идея данной книги состоит в том, что конструкции очень похожие на квантовые преобразования, можно реализовать на макроуровне в нейросетевом базисе. Естественные и искусственные нейроны способны обогащать данные и осуществлять их многомерное квантование. Уверенность в корректности подобной постановки задачи опирается на то, что МЫ, люди, способны за время порядка 0.01 секунды решать 10 000 мерные задачи (формальная запись таких преобразований $f(x_1, x_2, ..., x_{10000})$ без многоточия занимает 5 страниц). Если перевести эти данные в кубиты полноценного квантового вычислителя, то результат окажется ошеломляющим. Получается, что все МЫ, люди, на подсознательном уровне давно освоили континуально-квантовые приемы эффективных образных вычислений очень высокой размерности. Возможности искусственных нейронных сетей искусственного интеллекта нам так же необходимо поднять до возможностей естественного интеллекта.

В данной книге будет изложен положительный опыт нейросетевой биометрии, полученный в начале 21 века, который следует рассматривать как некоторую аналогию квантовым вычислениям, реализованным на обычных вычислительных машинах. Мне кажется, что такая попытка может дать синергетический эффект. Крайне важно то, что квантовые вычисления имеют хорошую математическую основу, такой основы пока нет у нейросетевой биометрии операций с множеством образов людей. С другой стороны, нейросетевые вычислители многомерной обработки образов легко реализуемы на практике и с их помощью можно экспериментально увидеть то, что не является очевидным для полноценных «квантовых вычислителей». Истина находится где-то рядом, уравнение Шредингера не является единственным. Существует множество уравнений, соответствующих реальным объектам и вычислительным программам, порождающим квантовые суперпозиции и квантовую запутанность. Одной из альтернатив уравнению Шредингера являются уравнения, описывающие циклический перебор нейросетевых преобразователей данных. Возможность работы с квантовыми суперпозициями биометрических данных длинной 256 кубит позволяет уже сегодня на обычном компьютере достигать характеристик сопоставимых с характеристиками полноценных квантовых вычислителей.

1. Основные положения квантовой механики и квантовых вычислителей

В начале 20 века существовала планетарная модель атома Резерфорда [1], однако она не была популярной среди физиков. Причиной тому была неустойчивость планетарной модели. Вращающийся вокруг протона электрон должен излучать энергию и упасть на протон. Спас планетарную модель атома Бор, предположивший, что излучение и поглощение энергии электроном происходит квантами (фотонами). Находясь на стационарной орбите, электрон не излучает, соответственно планетарная модель атома абсолютно устойчива. Переход атома из одного состояния в другое происходит скачком электрона с одной стационарной орбиты на другую. При этом происходит поглощение или выделение фотона. Энергия фотона излучения или поглощения зависит от скачка между начальным и последующим состоянием атома. В итоге удалось связать спектральные линии водорода со скачками электронов между орбиталями, что отображено на рисунке 1.

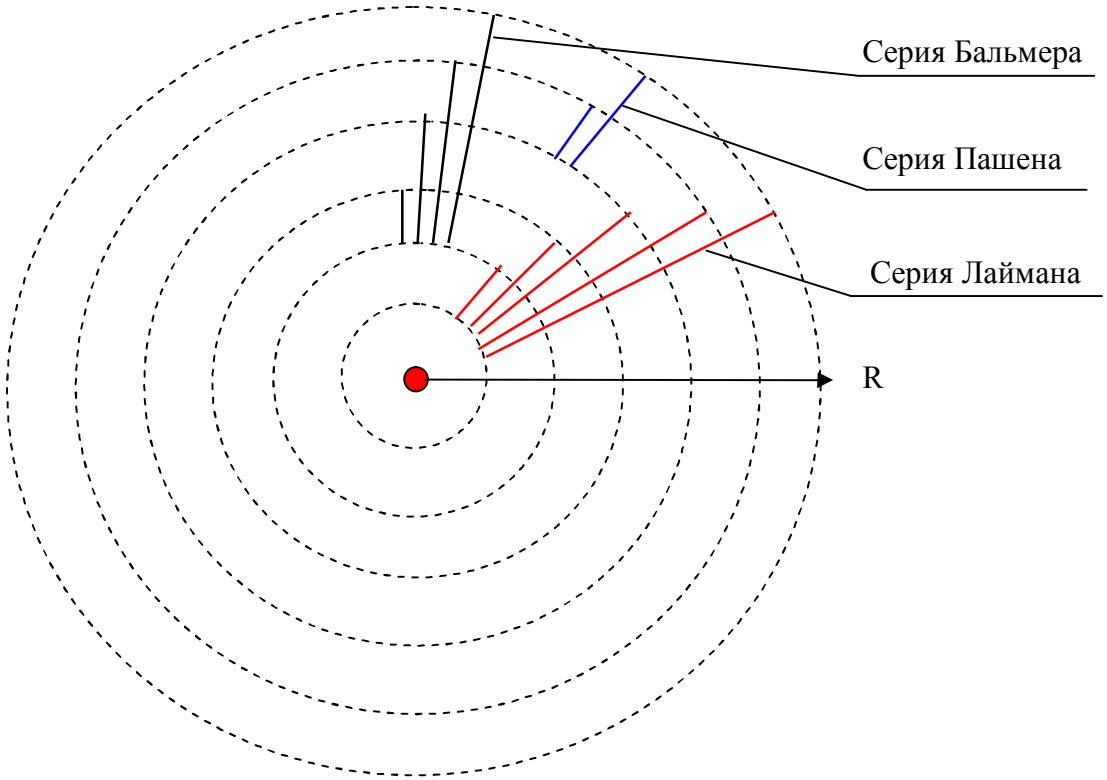


Рис.1. Серии спектральных линий атома Водорода

Естественно, что планетарная модель атома – это весьма существенное упрощение. Однако для водорода эта модель работоспособна и послужила толчком для развития квантовой механики, которое привело к появления волнового уравнения Шредингера. Решением уравнения Шредингера являются волновые функции [2], порождающие континуумы вероятного появления электрона (электронные облака), примеры таких континуумов даны на рисунке 2.

Для нас с вами не имеет значения, как выглядят континуумы положения электрона. Важно только то, что они существуют и в уравнении Шредингера и в планетарной модели. Кроме того, как в планетарной модели, так и в уравнении Шредингера существуют некоторые механизмы квантования. Взаимодействие континуумов и механизмов квантования порождают видимый спектр изменений состояний обоих моделей.

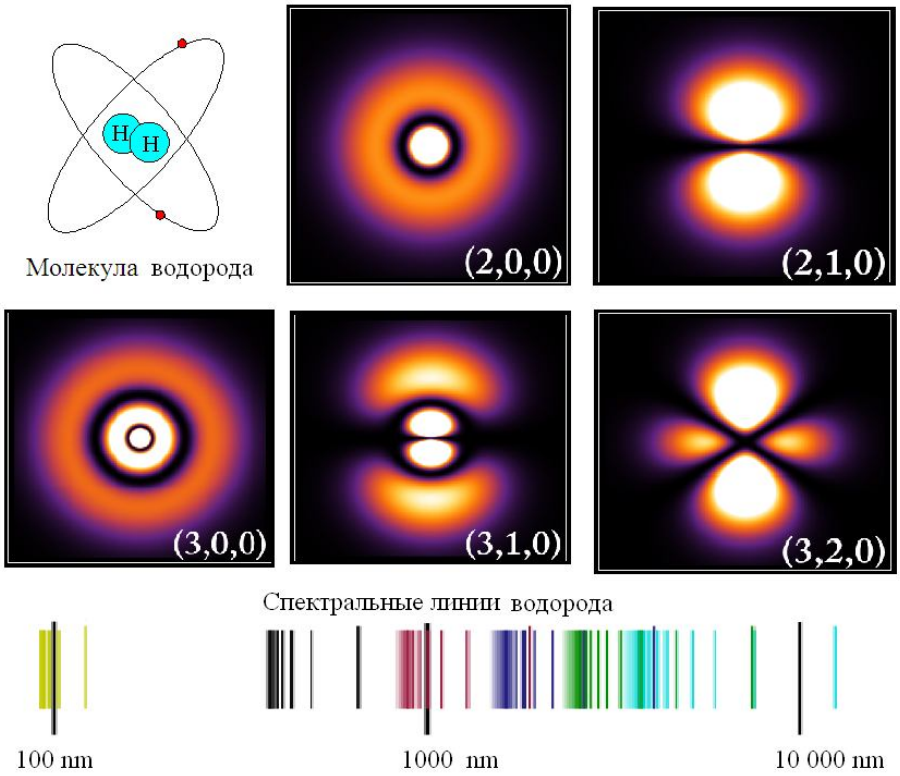


Рис. 2. Решения волнового уравнения для атома водорода, показывающее положение континуумов вероятного появления электронов (электронные облака) для разных значений волновых чисел

Обычно в учебниках по квантовой механике вводят понятие трехмерного квантового бита (кубита) [2, 3, 4], имеющего по 2 состояния спина по каждой из трех координат. Такая конструкция имеет суперпозицию 2^3 состояний. Обычно это отображают сферической орбитой случайного положения электрона, как это показано на рисунке 3. Мгновенное наблюдение положения электрона на сфере может дать любое состояние трех бит, что и рассматривается как суперпозиция 2^3 состояний.

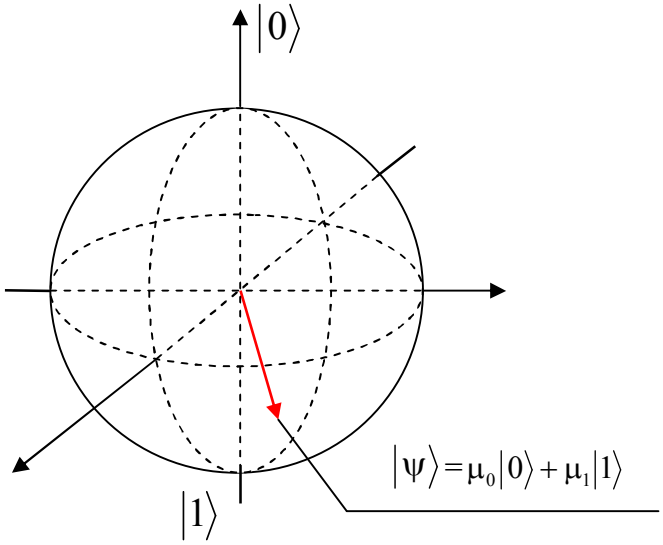


Рис. 3. Графическое отображение одного из состояний кубического бита (кубита) с использованием сферы Блоха

Если перейти к кубиту в место обычной логики, то мы получим ускорение вычислений в 8 раз. Двухкубитный вычислитель должен дать ускорение вычислений в 64 раза. Семикубитный вычислитель должен ускорить расчеты в два миллиона раз.

Исходя из этой логики, наш соотечественник Юрий Манин в 1980 году сформулировал идею создания квантовых компьютеров на новой элементной базе, способной реализовывать кубиты на физическом уровне [4]. Российский квантовый центр в 2013 году создал 7 кубитный макет квантового компьютера, который способен удерживать кубиты в синхронизме не более 0.001 секунды (исполнитель Московский институт стали и сплавов).

Прекрасная идея отказаться от побитных вычислений за счет перехода к обработке на квантовом компьютере более длинных массивов бинарных чисел (нескольких десятков или даже сотен кубических бит), натолкнулась на технические проблемы создания новой элементной базы.

В данной книге я попытаюсь показать, что есть еще один путь увеличения массивов обрабатываемой информации. Это путь использования больших искусственных нейронных сетей. Обычные вычислительные машины разбивают обрабатываемые данные на 8, 16, 32, 64 бита и вынуждены медленно работать, перетасовывая эти биты по заданной программе. Современные искусственные нейронные сети способны работать с биометрическими 416 мерными образами, а так же образами гораздо более высокой размерности. Даже, если каждый из 416 анализируемых биометрических параметров представлять 8 битными словами, потребуется анализ $(2^8)^{416}$ возможных входных состояний. Тем не менее, заранее обученные нейронные сети дают очень быстрое решение высокого качества. Нейронные сети, воспроизведенные программно на обычном компьютере, решают задачи с числом возможных состояний $(2^8)^{416}$ за время порядка 0.001 секунды. При этом, новая элементная база не нужна, нет необходимости разрабатывать новую элементную базу и осуществлять охлаждение ее жидким гелием при последующей эксплуатации.

Вывод. Решение уравнения Шредингера дает описание континуумов вероятного положения электронов (электронных облаков), роль квантователей в этом уравнении играет пространство между континуумами электроны облаков (орбиталей). Ни сами континуумы состояний электрона ни промежутки между ними (квантователи) не наблюдаемы. Легко наблюдаемыми оказываются только результаты взаимодействия системы континуумы-квантователи в форме фотонов излучения или поглощения (виден только спектр линий).

2. **Основные положения нейросетевой биометрии и «нечетких экстракторов»**

Информационное общество предполагает активное использование Интернет ресурсов. Государственные и частные структуры создают на своих сайтах личные кабинеты пользователей. К сожалению, существующая практика парольной защиты доступа к личным кабинетам обладает существенной уязвимостью. Пользователи не способны запоминать длинные случайные пароли. Владелец информационного ресурса не может быть уверен в том, что к личному электронному кабинету получил доступ именно его хозяин. Пароль может быть перехвачен программной закладкой, так же не составляет проблемы подменить IP адрес Интернет пользователя.

Для усиления защиты доступа к электронным кабинетам в настоящее время разрабатываются технологии биометрической аутентификации личности путем преобразования личных биометрических данных человека в его криптографический ключ или длинный пароль доступа. В США, Канаде,

Евросоюзе разрабатываются, так называемые «нечеткие экстракторы», преобразующие рисунок отпечатка пальца [5], голосовой пароль [6] или рисунок радужной оболочки глаза [7] в код криптографического ключа доступа [8].

Общая идея «нечетких экстракторов» состоит в квантовании континуума биометрических данных относительно некоторого порога. При этом, каждый новый пример биометрического образа дает свою кодовую последовательность. Возникает от 10% до 20% ошибок в выходных кодах. Эти ошибки правятся БЧХ кодом с 20 кратной избыточностью [7]. Структура нечетких экстракторов приведена в левой части рисунка 3.

Как видно из рисунка 3, выходной код «нечеткого экстрактора» оказывается коротким, так как после соответствующих преобразований его избыточная часть исчезает. При анализе рисунка радужной оболочки глаза [7] длина био-кода составляет 2048 бит соответственно, после удаления 20 кратной избыточности остается порядка 100 информационных бит. Этого вполне достаточно для криптографических приложений.

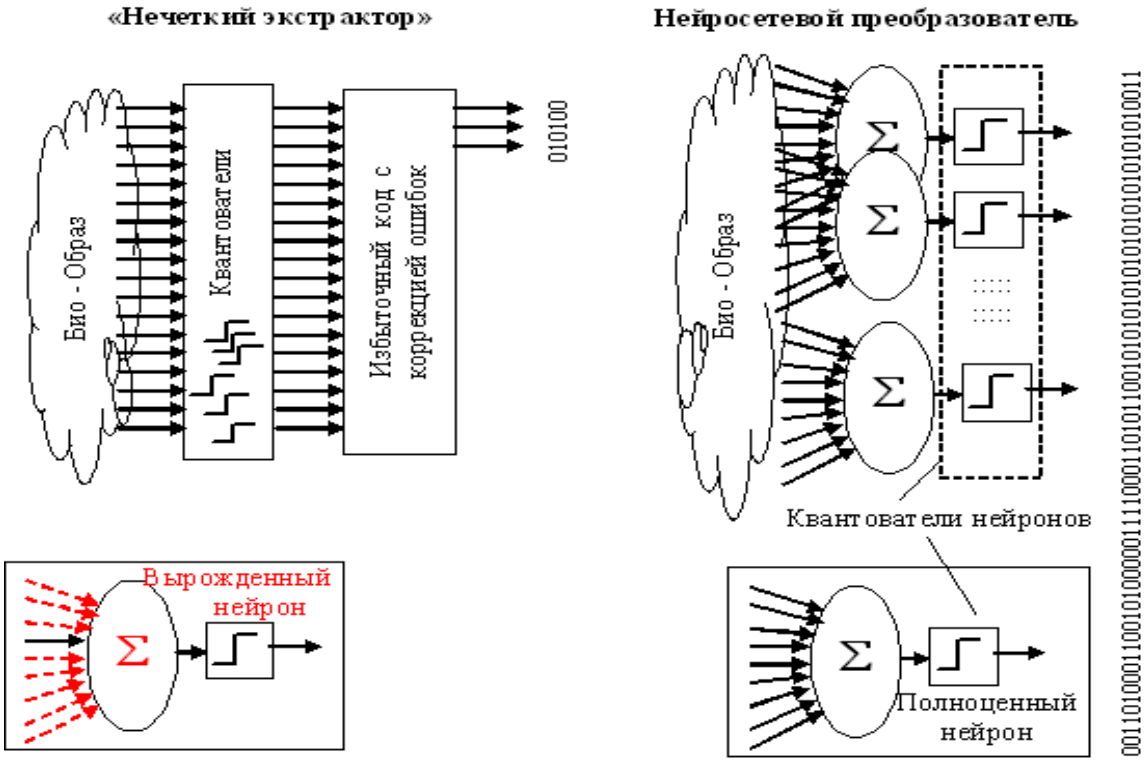


Рис. 3. «Нечеткие экстракторы» как частный случай нейросетевого преобразователя биометрия-код

Положение меняется, если используются рукописные парольные фразы [8], которые позволяют выделить порядка 416 биометрических параметров. В этой ситуации информативная часть БЧХ кода с 20 кратной избыточностью составляет 21 бит, что явно недостаточно для криптографического ключа.

Недостаток слишком «коротких ключей» полностью отсутствует у нейросетевых преобразователей биометрия-код [10], обученных по ГОСТ Р 52633.5 [11]. Их структура приведена в левой части рисунка 3. Принципиальным отличием искусственных нейронных сетей от «нечетких экстракторов» является то, что они квантуют континуумы входных данных после их обогащения. Входной сумматор каждого из нейронов во время настройки обогащает входные данные до уровня, когда квантование состояний «Свой»/«Чужой» происходит практически без ошибок. В связи с этим,

нейросетевые преобразователи биометрии имеют максимально возможную для ОС Windows длину кода доступа – 256 бит или 32 8-ми битных знака пароля доступа.

Формально «нечеткие экстракторы» можно рассматривать как частный случай нейросетевых преобразователей биометрия-код, если рассматривать квантователи «нечетких экстракторов» как вырожденные нейроны с сумматорами, имеющими один вход.

Следует отметить, что по всем показателям «нечеткие экстракторы» оказываются хуже нейросетевых преобразователей биометрия-код [12, 13]. В связи с этим, далее мы будем описывать использование только нейросетевых преобразователей биометрия-код.

Вывод. Очевидно, что и «нечеткие экстракторы» и нейросетевые преобразователи являются макрообъектами, у которых входные континуумы биометрических данных и квантователи легко наблюдаемы. Спектр выходных состояний так же легко наблюдаем. В этом принципиальное отличие макрообъектов от микрообъектов, описываемых уравнением Шредингера. Такие макрообъекты, как «нечеткие экстракторы» и нейросетевые преобразователи, описываются собственными уравнениями, являющимися аналогами уравнения Шредингера. Важно то, что уравнение Шредингера не является единственным. Сколько существует уравнений подобных уравнению Шредингера, на данный момент, неизвестно. На каждом уравнении, порождающем спектр выходных состояний (квантовую суперпозицию), может быть построен свой континуально-квантовый вычислитель.

3. Предварительная подготовка биометрических данных

На рисунке 3 дана упрощенная схема преобразования биометрических данных. В этой схеме облако нечеткого биометрического образа передает данные на входы искусственной нейронной сети. Реально применяется более сложная технология, блок-схема первичных преобразований которой приведена на рисунке 4.

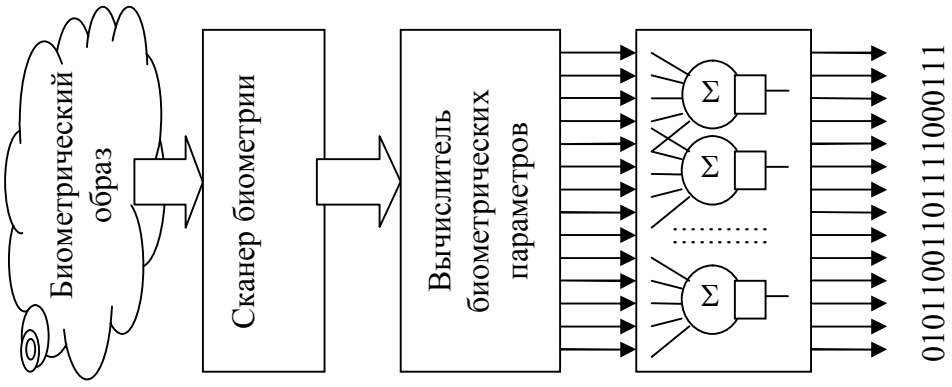


Рис. 4. Блок-схема сканирования и последующих преобразований биометрических данных

Могут быть использованы различные биометрические образы человека:

- рисунок отпечатка пальца [14];
- геометрические параметры лица [15];
- рисунок радужной оболочки глаза [16];
- параметры динамики рукописной подписи [17];
- рисунок подкожных кровеносных сосудов [18];

- данные кисти руки [19];
- данные ДНК [20];
- особенности голоса.

Для ввода биометрических данных используются типовые или специализированные сканеры: встроенный микрофон, графический планшет (чувствительный экран планшета), видеокамера с подсветкой в видимом и инфракрасном свете, сканер рисунка отпечатка пальца, цифровой фотоаппарат высокого разрешения для ввода рисунка радужной оболочки глаза. После сканирования биометрического образа данные передаются в вычислитель для вычисления контролируемых параметров.

Алгоритм извлечения контролируемых параметров может быть уникальным, он определяется производителем средства биометрической идентификации (аутентификации). Например, при анализе динамики рукописного почерка, как параметры контроля могут быть использованы коэффициенты двухмерного преобразования Фурье. На рисунке 5 приведена экранная форма среды моделирования «БиоНейроАвтограф» [9] с образцом введенного с графического планшета рукописного слова.

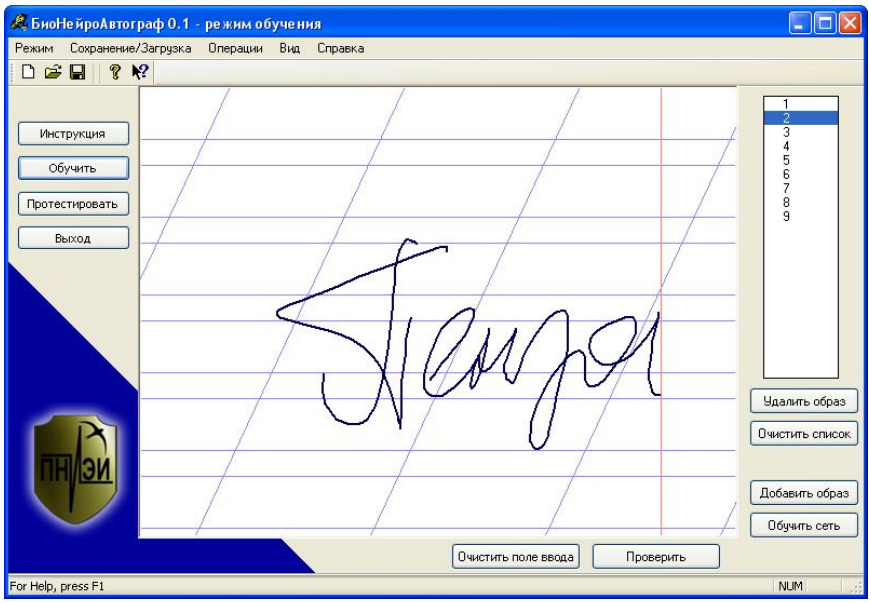


Рис. 5. Экранная форма средства, позволяющего каждому желающему самостоятельно осуществлять преобразование 416 биометрических параметров в код длиной 256 бит

Продукт построен на учете 16 синусных и косинусных гармонических составляющих колебаний пара X(t), Y(t), возникающих при воспроизведении на графическом планшете рукописного слова. Так как рукописный образ двухмерен, вычисляется верхняя часть матрицы двухмерного преобразования Фурье, матрица содержит 416 коэффициентов (рисунок 6 иллюстрирует положение коэффициентов Фурье в матрице преобразования).

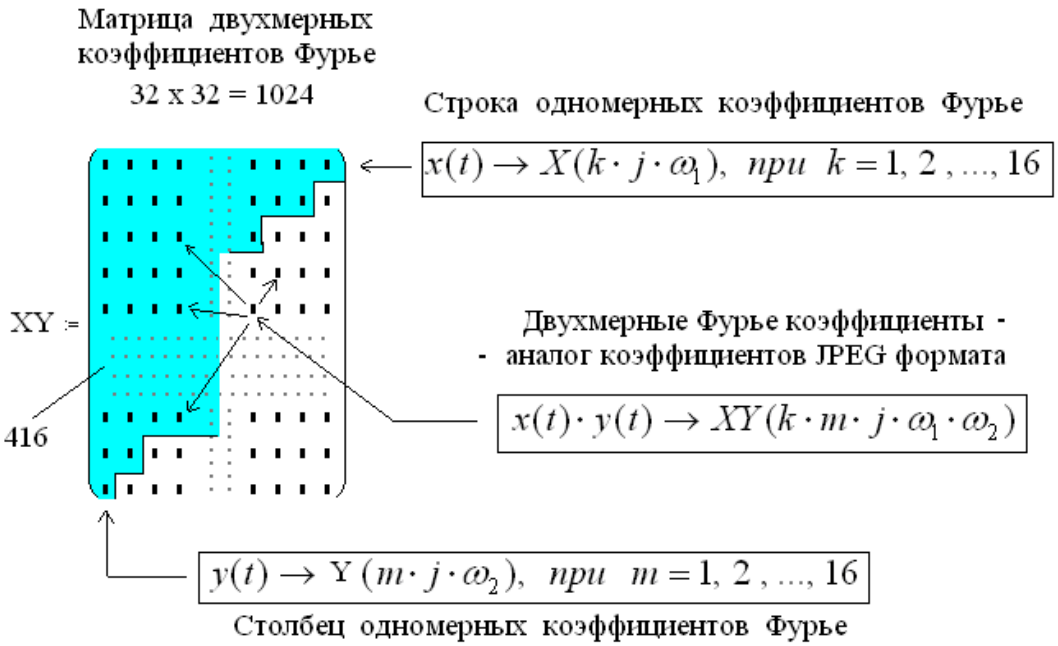


Рис. 6. Матрица двухмерных коэффициентов Фурье, используемых как биометрические параметры в среде моделирования «БиоНейроАвтограф».

Всего матрица имеет 32x32=1024 коэффициентов, большая часть которых мала. Малозначащие коэффициенты обычно находятся в правом нижнем углу матрицы, и не учитываются по аналогии с алгоритмом сжатия изображений стандарта JPEG. Учитываемые при биометрической аутентификации коэффициенты двухмерного преобразования Фурье на рисунке 6 отмечены более темной заливкой.

В среде моделирования «БиоНейроАвтограф» все учитываемые биометрические параметры доступны для наблюдения. После каждой инициации режима «Проверить» они записываются в файл DATA/User/param.txt. То есть, любой пользователь может получить любые объемы своих биометрических данных и использовать их для численной проверки, изложенных в данной книге материалов. К сожалению, нельзя доверять множеству баз биометрических баз данных, размещенных в Интернет. Именно по этой причине был создан источник достоверной информации в виде среды моделирования «БиоНейроАвтограф», размещенный с 2009 года в открытом доступе.

Вывод. Биометрические образы имеют высокую размерность, в частности, рукописный биометрический образ преобразуется общедоступной средой моделирования «БиоНейроАвтограф» в 416 параметров. Это далеко не рекорд, при необходимости размерность анализируемых биометрических параметров может быть увеличена. Например, при анализе радужной оболочки глаза [7] анализируют 2048 биометрических параметров. Данных много, но большинство из них имеет низкое качество (низкую информативность).

4. Информативность биометрических параметров

Различают «плохие» параметры с низкой информативностью и «хорошие» параметры с высокой информативностью. На рисунке 7 даны распределения «плохого» параметра - $p(\nu_1)$ и «хорошего» параметра - $p(\nu_2)$ на фоне распределения данных все «Чужие».

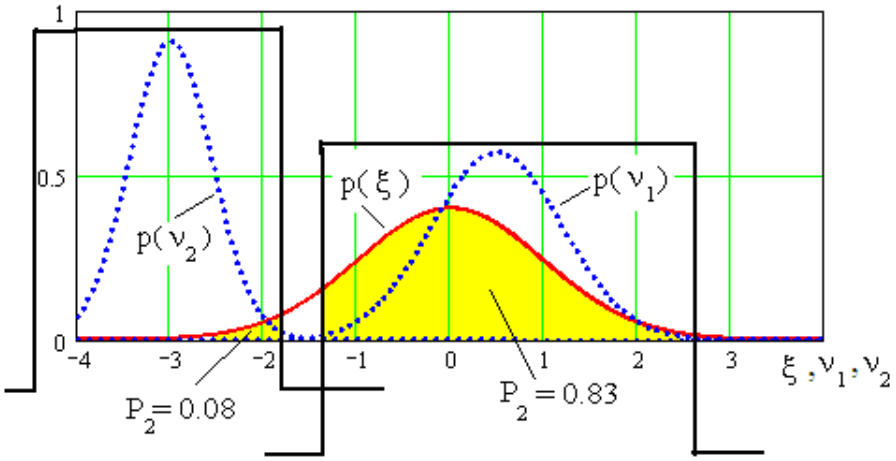


Рис.7. Примеры распределений «плохого» параметра - $p(\nu_1)$ и «хорошего» параметра - $p(\nu_2)$ на фоне распределения данных все «Чужие» - $p(\xi)$

В простейшем случае «нечеткого экстрактора» для распределения каждого параметра выставляется правая и левая граница допустимых значений. В первом приближении можно считать распределения значений биометрических данных нормальными. Это означает, что границы допустимых значений могут быть определены по правилу трех стандартных отклонений от математического ожидания. То есть, пороги верхней правой границы и нижней левой границы должны быть заданы следующим образом:

$$\begin{cases} k_R = E(\nu) + 3 \cdot \sigma(\nu) \\ k_L = E(\nu) - 3 \cdot \sigma(\nu) \end{cases} \qquad (1),$$

где $E(\nu)$ - математическое ожидание биометрического параметра, $\sigma(\nu)$ - стандартное отклонение биометрического параметра.

В этом случае вероятность ошибки первого рода (отказ «Своему») оказывается практически нулевой $P_1(\nu) \approx 0$. Вероятность ошибки второго рода (ложный пропуск «Чужого») вычисляется, как площадь распределения - $p(\xi)$ попавшая в интервал допустимых значений биометрического параметра:

$$P_2(\nu) = \frac{1}{\sigma(\xi)\sqrt{2\pi}} \int_{k_L}^{k_R} \exp\left\{ \frac{-(E(\xi) - u)^2}{2 \cdot \sigma^2(\xi)} \right\} \cdot du \qquad (2).$$

Это означает, что информативность биометрического параметра может быть вычислена по следующей формуле:

$$I(\nu) = -\log_2(P_2(\nu)) \qquad (3).$$

На рисунке 6, площади пропорциональные P_2, отмечены заливкой. Из этого рисунка видно, что первый биометрический параметр менее информативен $I(\nu_1) = 0.27$ бита (площадь заливки велика), куда более информативным является второй биометрический параметр $I(\nu_2) = 3.6$ бита.

Разброс информативности биометрических параметров значителен. Если ориентироваться на применение самых информативных биометрических параметров, то мы будем иметь возможность применять классические решающие правила. В прошлом веке так и поступали, однако хороших данных с большой информативностью очень мало. Как следствие, классические решающие правила не дают решений высокого качества.

Значительно поднять качество принимаемых решений удается, если создавать алгоритмы принятия решений, способные работать с большими

объемами плохих (низко информативных) данных. Идеальный алгоритм обработки данных должен накапливать информацию, полученную по каждому биометрическому параметру. То есть, предельный объем информации идеального решения можно определить следующим образом:

$$\lim(I) \le \sum_{i=1}^{M} I(\nu_i) \qquad (4),$$

где M- число учитываемых при решении параметров (M=416 для среды моделирования «БиоНейроАвтограф»).

Реальный объем информации, извлекаемый существующими решающими правилами, всегда меньше своего предельного значения (4). Все это верно и для нейросетевых преобразователей биометрия-код. В частности, нейросетевые преобразователи с одним слоем нейронов (рисунок 3 и 4) должны обеспечивать выходную информативность каждого нейрона не менее одного бита. Это означает, что число входов у нейрона - m должно выбираться больше чем суммарная информативность преобразуемых им входных данных. Исходя из этого условия, можно вычислить среднюю информативность биометрических параметров. По средней информативности следует оценить необходимое число входов у нейронов:

$$m > \mathrm{round}\left\{\frac{2}{E(I(\nu))}\right\} \qquad (5).$$

Выводы. Одна из основных функции нейрона – это обогащение относительно бедных входных данных. Эту функцию выполняет сумматор. В этом контексте понятно, что для получения «хороших» данных нужно использовать много «плохих» данных. Чем хуже данные, тем больше их нужно для обогащения и тем больше входов должен иметь нейрон. Естественно, что для оценки числа входов – m только информативности недостаточно, нужно учитывать еще и коррелированность входных данных.

Тем не менее, общая тенденция связи числа данных и их информативности верно отражается соотношением (5). Биометрический параметр ν_2 можно использовать без обогащения, его информативность больше одного бита. Для работы с параметрами, информативность которых значительно меньше ($I(\nu_1)$ = 0.27 бита), требуется нейрон, имеющий от 5 до 16 входов. При этом желательно, что бы плохие информативные параметры одного нейрона имели близкую информативность (были бы сопоставимо плохи).

5. Матричное описание нейросетевых преобразователей

В квантовой механике матричное описание линейных операций с континуумами играет важную роль. Воспользуемся аналогичным описанием линейных преобразований континуумов сумматорами искусственных нейронных сетей. При этом, следует иметь в виду, что матричные преобразования квантовой механики низкоразмерны (используются квадратные матрицы 3 порядка), тогда, как матрицы квантово-нейросетевой биометрии асимметричны и имеют очень высокую размерность (416 – ширина матрицы, 256 - высота матрицы по числу элементов):

$$\begin{bmatrix} \mu_{11} & \mu_{21} & \cdots & \mu_{M1} \\ \mu_{12} & \mu_{22} & \cdots & \mu_{M2} \\ \vdots & \vdots & \cdots & \vdots \\ \mu_{1Q} & \mu_{2Q} & \cdots & \mu_{MQ} \end{bmatrix} \times \begin{bmatrix} \nu_1 \\ \nu_2 \\ \nu_3 \\ \vdots \\ \vdots \\ \nu_{M-1} \\ \nu_M \end{bmatrix} = \begin{bmatrix} y_1 \\ y_2 \\ \vdots \\ y_Q \end{bmatrix} \qquad (6).$$

Весовые коэффициенты матрицы в уравнении (6) получаются путем обучения нейронов на примерах образов «Свой» и все «Чужие» любым известным алгоритмом [21], однако, большинство из них имеет высокую вычислительную сложность. Исключением является стандартизованный алгоритм обучения по ГОСТ Р 52633.5 [11], специально созданный для нейросетевых преобразователей биометрия-код. Стандартный алгоритм имеет линейную вычислительную сложность и позволяет полностью автоматизировать обучение.

Задача любого алгоритма обучения состоит в том, что бы повысить информативность данных на выходе сумматоров $I(y_i)$ до величины более одного бита. После этого, выходные данные сумматора можно квантовать. Каждый нейрон на выходе своего сумматора имеет квантователь, преобразующий континуум состояний в два дискретных состояния «0» или «1». Формально, это может быть записано следующим образом:

$$\begin{bmatrix} z(y_1) \\ z(y_2) \\ \vdots \\ z(y_Q) \end{bmatrix} = \begin{Bmatrix} "c_1" \\ "c_2" \\ \vdots \\ "c_Q" \end{Bmatrix} \qquad (7), \qquad \text{где} \quad \begin{cases} z(y) = "0" & \text{если } y \le 0, \\ z(y) = "1" & \text{если } y > 0. \end{cases}$$

Заметим, что в одном и том же выражении (7) содержатся непрерывные (континуальные или аналоговые) данные и дискретные данные «0» или «1», отмеченные кавычками как это обычно делают при программировании.

Необходимость введения кавычек принципиально отличает символику квантовой биометрии от символики квантовой механики. В уравнении Шредингера в явной форме нет операции квантования. Иная ситуация возникает для уравнений, соответствующих нейросетевым преобразователям биометрия-код. В них в явной форме необходимо разделять многомерные континуумы и дискретные поля.

Нейросетевой преобразователь не линеен, он по разному работает с данными «Свой» и «Чужой». Для учета этой особенности приходится иметь две формы его описания в двух разных состояниях. То есть, выражения (6) и (7), созданные для описания работы нейронной сети при воздействии на нее данными примеров образов «Свой», следует дополнить ее описанием при работе с данными все «Чужие»:

$$Z\left(\begin{bmatrix} \mu_{11} & \mu_{21} & \cdots & \mu_{M1} \\ \mu_{12} & \mu_{22} & \cdots & \mu_{M2} \\ \vdots & \vdots & \cdots & \vdots \\ \mu_{1Q} & \mu_{2Q} & \cdots & \mu_{MQ} \end{bmatrix} \times \begin{bmatrix} \xi_1 \\ \xi_2 \\ \xi_3 \\ \vdots \\ \vdots \\ \xi_{M-1} \\ \xi_M \end{bmatrix} \right) = \begin{Bmatrix} "x_1" \\ "x_2" \\ \vdots \\ "x_Q" \end{Bmatrix} \qquad (8).$$

Как будет показано далее статистические свойства кодов "$\overline{c}$" и кодов "$\overline{x}$" кардинально различаются.

6. Особенности работы нейросетевого преобразователя, обученного алгоритмом ГОСТ Р 52633.5

Следует отметить, что алгоритм обучения оказывается быстрым и абсолютно устойчивым из-за того, что он независимо обучает каждый нейрон. Более того, он не является итерационным. Каждый весовой коэффициент вычисляется независимо от других весовых коэффициентов. При этом, знак весового коэффициента вычисляется по знаку математического ожидания биометрического параметра и желаемого дискретного отклика нейрона на образ «Свой»:

$$\begin{cases} \operatorname{sign}(\mu_i) = -1 & \text{if } E(\nu_i) < E(\xi) \wedge ("c_i") = "1", \\ \operatorname{sign}(\mu_i) = +1 & \text{if } E(\nu_i) < E(\xi) \wedge ("c_i") = "0", \\ \operatorname{sign}(\mu_i) = -1 & \text{if } E(\nu_i) > E(\xi) \wedge ("c_i") = "1", \\ \operatorname{sign}(\mu_i) = +1 & \text{if } E(\nu_i) > E(\xi) \wedge ("c_i") = "0". \end{cases} \qquad (10)$$

Модуль весового коэффициента находится путем следующего преобразования:

$$|\mu_i| = \frac{|E(\xi_i) - E(\nu_i)|}{\sigma(\xi) \cdot \sigma(\nu_i)} \qquad (11).$$

Работа алгоритма обучения, с вычислением весовых коэффициентов по формулам (10), (11), иллюстрируется рисунком 7.

На рисунке 7 отображена ситуация, когда 24 коэффициента нейрона среды моделирования «БиоНейроАвтограф» разбиты на 8 групп по 3 коэффициента, далее производится постепенное подключение этих коэффициентов и нормирование стандартного отклонения $\sigma(y(\xi))=1$. В конечном итоге, получается семейство распределений $p(\nu)$, показывающее, что при обучении происходит выталкивание плотности распределения значений данных «Свой» на периферию области распределения значений все «Чужие». Параллельно с выталкиванием происходит сжатие области значений образов «Свой» на выходе обучающегося сумматора нейрона. Оба этих эффекта приводят к росту суммарной информативности $I(y(\nu))$. Распределения $p(\nu)$ на момент начала и окончания обучения на рисунке 8 выделены более толстыми линиями.

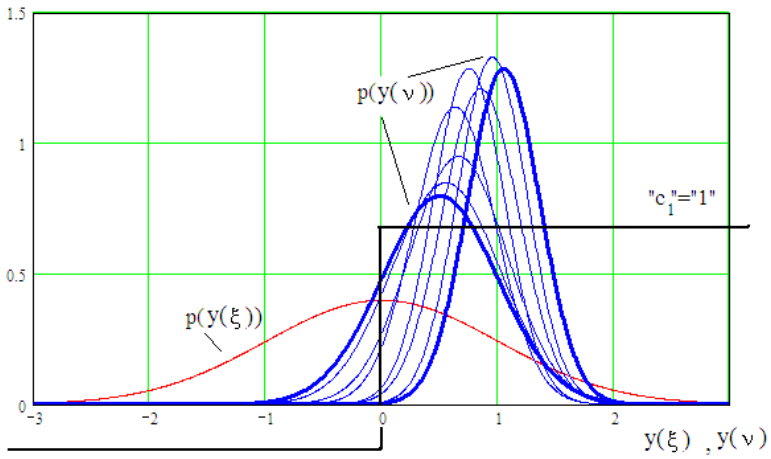


Рис. 8. Работа алгоритма обучения при постепенной замене коэффициентов $\mu_i=1$ на коэффициенты, вычисленные по формуле (11).

Как видно из рисунка 8, квантователь каждого из нейронов срабатывает в центе словаря рукописных образов все «Чужие». Этот момент очень важен, так как только это обеспечивает вероятность ошибок второго рода в каждом выходном разряде нейросети вероятное значение $P_2("x_i") = 0.5$. Именно это свойство нужно, что бы скрывать состояние разрядов кода "c_i" от посторонних.

Стандарт ГОСТ Р 52633.5 рекомендует выбирать случайно связи нейронов со входными биометрическими параметрами. То есть 24, входа каждого из 256 нейронов сети моделирования «БиоНейроАвтограф» выбираются из 416 контролируемых биометрических параметров. При этом, у многих нейронов будут общие связи (пары, тройки, ….). Воспользуемся этим и попытаемся пояснить работу нейронной сети. Будем рассматривать пары биометрических параметров ν_1, ν_{157} и ξ_1, ξ_{157}. Ситуация отображена на рисунке 9.

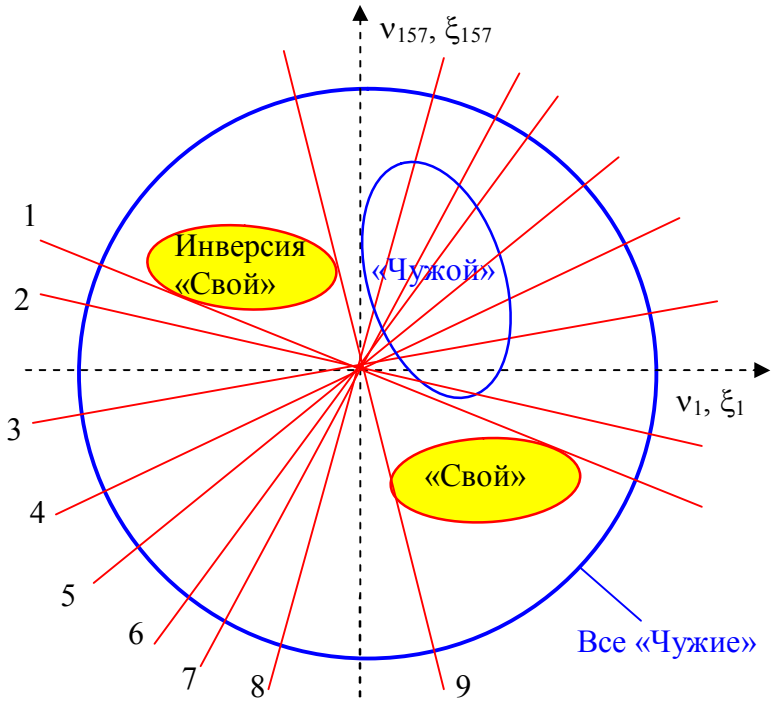


Рис. 9. Двухмерное сечение многомерной области все «Чужие»

Рисунок 8 отражает ситуацию, когда из 256 нейронов 9 нейронов имеют общую пару входных биометрических параметров с номерами 1 и 157. В центрированном $E(\xi_1) = E(\xi_{157}) = 0$ и нормированном пространстве $\sigma(\xi_1) = \sigma(\xi_{157}) = 1$ случайные данные все «Чужие» будут давать круг, так как они не коррелированны. Данные образов «Свой» и «Чужой» коррелированны и будут давать эллипсы.

Геометрический смысл алгоритма обучения ГОСТ Р 52633.5 состоит в том, что каждый нейрон сети делит подконтрольное ему 24-мерное пространство все «Чужие» гиперплоскостями пополам. На рисунке 9 эти гиперплоскости дают прямые линии. Ни одна из разделяющих гиперплоскостей всех 256 нейронов не должна пересекать гиперэллипс образа «Свой» во всех 256-ти 24-мерных подпространствах. Только в этом случае попадание данных «Свой» в любую точку внутри 256-мерного гиперэллипса будет давать на выходе нейронной сети один и тот же выходной код "$\overline{c}$".

Совершенно иная ситуация возникает для образа «Чужой». Как видно из рисунка 9, эллипс «Чужой» многократно пересекают гиперплоскости нейронов. То есть, подавая на вход нейронной сети данные образа «Чужой», мы будем на

выходе нейронной сети наблюдать нестабильный выходной код. Получается, что для образа «Свой» нейронная сеть практически полностью устраняет энтропию выходных кодов, возникающую из-за естественной энтропии входных данных:

$$\begin{cases} H(\nu_1, \nu_2, ..., \nu_{416}) >> 0, \\ H("c_1, c_2, ..., c_{256}") \approx 0 \end{cases} \qquad (12).$$

Для образа «Чужой» и «Свой» энтропии входных данных сопоставимы, а вот энтропии их выходных кодов соотносятся иначе. Энтропия кодов «Чужой» много выше энтропии кода «Свой»:

$$\begin{cases} H(\xi_1, \xi_2, ..., \xi_{416}) \approx H(\nu_1, \nu_2, ..., \nu_{416}), \\ H("x_1, x_2, ..., x_{256}") >> H("c_1, c_2, ..., c_{256}"). \end{cases} \qquad (13).$$

Очень важным моментом является то, что параллельно с образом «Свой» существует его инверсия. Два этих образа друг для друга являются полными инверсиями, как в многомерных континуумах, так и в пространстве выходных кодов. При этом они оказываются неразличимы по энтропии:

$$\begin{cases} H(-\nu_1, -\nu_2, ..., -\nu_{416}) \equiv H(\nu_1, \nu_2, ..., \nu_{416}), \\ H("\neg c_1, \neg c_2, ..., \neg c_{256}") \equiv H("c_1, c_2, ..., c_{256}"). \end{cases} \qquad (14).$$

Вывод. В квантовой математике так же существуют симметричные конструкции, дополняющие друг друга. Часть операций, выполняемых при квантовых вычислениях, построено на учете подобной анти симметрии. Формы записи соотношений симметрии квантовых суперпозиции, порождаемые биометрическими образами, существенно отличаются от квантовых суперпозиций, порождаемых уравнениями Шредингера.

Следует так же подчеркнуть, что соотношения симметрии (14) выполняется далеко не для всех нейронных сетей и не для всех алгоритмов их обучения. Изменение структуры нейронной сети и алгоритма обучения приводит к модификации соотношений симметрии (14) вплоть до исчезновения симметрии (анти симметрии).

7. Высокоразмерное нейросетевое распознавание образов

Во время обучения нейросетевого преобразователя биометрия-код используются порядка 20 примеров образа «Свой» и примерно 200 примеров образов все «Чужие». После обучения получается таблица, содержащая номера связей входов 256 нейронов сети с 416 биометрическими параметрами и весовые коэффициенты - μ_i каждого нейрона, найденные при обучении.

При распознавании образов происходит преобразование данных, вычисляются биометрические параметры, далее это параметры передаются на входы искусственной нейронной сети. Обычно искусственная нейронная сеть воспроизводится программно по данным таблицы связей. Процедура распознавания отображена на рисунке 10. Из этого рисунка видно, что выходной код нейронной сети подается на блок вычисления расстояний Хэмминга. В случае, если выходной код нейронной сети точно совпадает с кодом обучения "$\overline{c}$" (расстояние Хэмминга нулевое), принимается решение об обнаружении биометрического образа «Свой».

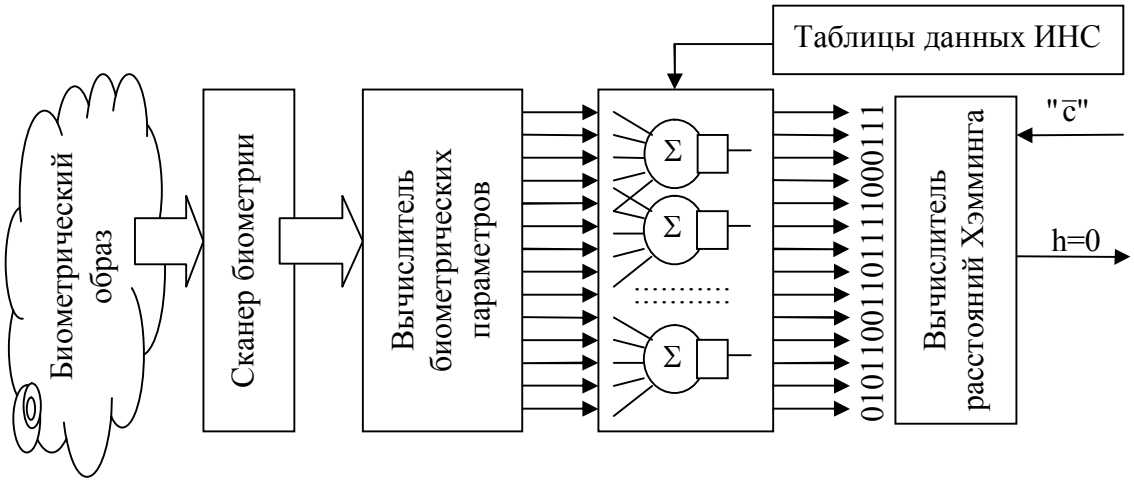


Рис. 10. Блок-схема преобразования данных при распознавании образов

Расстояние Хэмминга вычисляется следующим образом:

$$h = \sum_{i=1}^{256} ("c_i") \oplus ("x_i") \qquad (15),$$

где $\oplus$ - операция сложения по модулю два.

Обнаружение нулевого расстояния Хэмминга $h = 0$ является идеальным случаем, однако, в предъявленном образе могут быть небольшие отклонения, которые приводят к появлению незначительного числа ошибок $h = 1, 2, \ldots, h_k$. В пространстве расстояний Хэмминга всегда можно установить порог - h_k принятия решений. При расстояниях Хэмминга менее порога - h_k принимается решение «Свой». Во всех остальных случаях принимается решение «Чужой».

Выводы. Огромное число алгоритмов обучения нейронных сетей в период второй половины 20 века создавались под сети с одним выходом. В этой постановке задачи различать между собой образы «Чужой-1» и «Чужой-k» нельзя. Их отклики сливаются. Нейронные сети с большим числом выходов (преобразователи биометрия-код) оказываются много эффективнее нейронных сетей с одним выходом по двум причинам:

1. многократно снижены требования к обучению каждого из нейронов;
2. стали различимы состояния разных образов «Чужой», что дает дополнительные возможности по исключению коллизий образов «Свой» и все «Чужие».

Важно отметить, что нейронные сети с большим числом выходов в пространстве расстояний Хэмминга ведут себя как квадратичные формы очень высокой размерности. При этом, нейронная сеть размерности 416 входов и 256 выходом имеет абсолютно устойчивый алгоритм быстрого обучения ГОСТ Р 52633.5, тогда как классические квадратичные формы такой размерности настроить технически невозможно.

8. Оценка вероятности ошибок второго рода и энтропии выходных кодов преобразователя биометрия-код

Установив некоторый порог допустимых расстояний Хэмминга, мы фактически корректируем в допустимых пределах выходной код нейронной сети. Понятно, что чем больше порог - h_k тем меньше будет вероятность ошибок первого рода - $P_1(h_k)$. Уже при пороге в 5 бит, среда моделирования «БиоНейроАвтограф» практически перестает ошибаться. Однако, при этом

вероятность ошибок второго рода - $P_2(h_k)$ увеличивается. В связи с этим очень важно уметь вычислять эту вероятность.

Для оценки необходимо подать на входы нейронной сети несколько десятков примеров образов все «Чужие». Схема численного эксперимента приведена на рисунке 11.

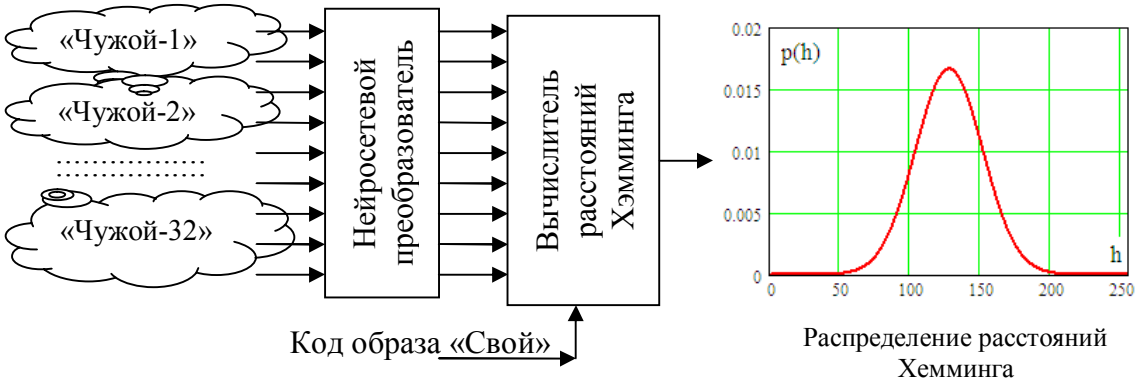


Рис. 11. Оценка вероятности ошибок второго рода, обученного нейросетевого преобразователя

При этом эксперименте мы получаем выборку расстояний Хэмминга $\{h_1, h_2, h_3, \ldots, h_{32}\}$. Эта выборка позволяет вычислить их математическое ожидание - E(h) и стандартное отклонение - σ(h). Располагая этими данными, мы можем воспользоваться рекомендациями ГОСТ Р 52633.3 [22] и определить вероятность ошибок второго рода по следующей формуле:

$$P_2(h_k) \approx \frac{1}{\sigma(h)\sqrt{2\pi}} \int_{-\infty}^{h_k} \exp\left\{\frac{-(E(h)-u)^2}{2(\sigma(h))^2}\right\} \cdot du \qquad (16).$$

Многомерная энтропия выходных кодов нейросетевого преобразователя оценивается через вероятность ошибок второго рода:

$$H("x_1, x_2, ..., x_{256}") \approx -\log_2(P_2(h_k)) \qquad (17).$$

Примечание. При вычислениях энтропии (17) использовалась гипотеза нормального закона распределения значений (16). Она хорошо выполняется для нейросетевых преобразователей биометрия-код, обученных алгоритмом ГОСТ Р 52633.5. Для «нечетких экстракторов» гипотеза нормальности распределения расстояний Хэмминга не применима, однако для них общие принципы вычисления вероятности ошибок второго рода остаются теми же. Отличие состоит только в том, что для «нечетких экстракторов» применять нужно гипотезу бета распределения расстояний Хэмминга. Соответственно, в подынтегральном выражении (16) вместо нормального закона распределения должен использоваться закон бета распределения.

9. Оценка ускорения при вычислении энтропии длинных кодов, полученного за счет использования квантово-континуального преобразования

При описании основ квантовой механики [2] идет постоянное сравнение трехмерных квантовых эффектов с классической физикой Ньютона. Это достаточно убедительный дидактический прием может быть применен и в нашем случае через оценку соотношения времени вычисления энтропии по Шеннону и новым способом через преобразования (16), (17).

Если исходить из вычислений четырехмерной энтропии по Шеннону, то придется пользоваться следующей формулой:

$$H("x_1, x_2, ..., x_4") \approx -\sum_{i=1}^{16} P_i \cdot \log_2(P_i) \qquad (18),$$

где P_i – вероятность появления i-го события.

Так как в формуле (18) присутствую вероятности событий, приходится увеличивать объем выборки для их вычисления. Для оценки вероятностей появления 16 состояний, необходимо иметь выборку хотя бы из 160 событий.

Удвоив размерность задачи, мы получим алфавит, имеющий 256 состояний:

$$H("x_1, x_2, ..., x_8") \approx -\sum_{i=1}^{256} P_i \cdot \log_2(P_i) \qquad (18a).$$

Для оценки вероятности, сопоставимой с величиной $1/256$, необходимо увеличить объем тестовой выборки до величины 2560 опытов. Очевидно, что для достоверной оценки 256 мерной энтропии, придется использовать тестовую выборку размером $2^{256} \times 10$.

Нам же с вами потребовалось выборка, состоящая всего из 32 событий. Отношение

$(2^{256} \times 10)/32 \approx 2^{254}$ является выигрышем при использовании нового способа вычислений. Это огромное ускорение вычислений, связанное с тем, что 256 битные числа свертываются при вычислении расстояний Хэмминга (15) до 8 битных чисел математических ожиданий - E(h) и стандартных отклонение - σ(h).

При новом способе вычислений происходит цифровая обработка 256 битных чисел, далее происходит возврат к континуумам вычисления вероятности по формуле (16). Произошел квантово-континуальный переход, построенный на априорном знании о нормальном законе распределения расстояний Хэмминга. В силу наличия этой априорной информации, мы перешли от наблюдения редких событий по Шеннону к прогнозированию вероятности появления редких событий по формуле (16).

Вывод. Люди за время 0.01 секунды способны решать 10 000 мерные задачи, при этом, для людей оценка рисков найденного решения очень важна. Из всего изложенного выше следует, что уже созданный искусственный интеллект биометрии способен за время порядка 0.01 секунды решать 416 мерные задачи на обычных вычислительных машинах. При этом, за счет 256 мерных операций в пространстве расстояний Хэмминга, искусственный интеллект биометрии способен осуществлять оценку рисков ошибочного принятия решения в 2^{254} раз быстрее, чем классические процедуры Шеннона. В терминах квантовых вычислений [4] достигнутое ускорение составляет 84.7 кубита за время работы 0.01 секунды. В кубитах это примерно в 100 раз лучше, чем дал «полноценный» квантовый компьютер МИСиС (7 кубит, время синхронизма 0.001 секунды, 2013 год.)

10. Информационно-технические ограничения на практически достижимый показатель ускорения вычислений при оценке энтропии

Приведенные выше данные показывают связь коэффициента ускорения вычислений с длиной выходных кодов нейросети преобразователя биометрия-код. Из этих данных создается впечатление, что увеличение числа нейронов с 256 до 512 должно увеличить выигрыш от применения операций в пространстве расстояний Хэмминга.

Если рассматривать более подробно ситуацию, то увеличение длины выходного кода действительно приводит к некоторому росту качества принимаемого решения. Однако, этот рост замедляется по мере увеличения длины

кода [23]. Убедиться в этом удается с помощью численного эксперимента на данных среды моделирования «БиоНейроАвтограф».

Для проведения вычислений необходимо обучить нейросеть рукописному образу, затем необходимо подавать образы «Чужой» на обученную нейронную сеть и запоминать данные, появляющиеся в файле testKeys.txt при каждой инициации режима «Проверить» (смотри рисунок 5). В итоге мы получаем бинарные выходные коды нейронной сети на все предъявленные примеры образов «Чужой».

Располагая этими данными, мы можем вычислить энтропию для ключей постепенно увеличивающейся длины - q от 1 до 256 бит. Кривая изменения энтропии в зависимости от длины ключа приведена на рисунке 12.

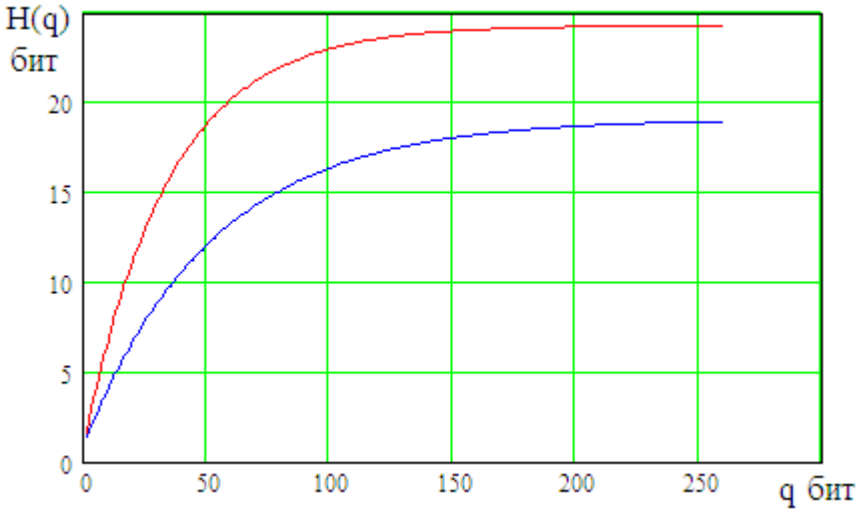


Рис. 12. Рост энтропии выходных кодов в зависимости от длины ключа

Из рисунка 11 видно, что при малых значениях длины ключа – q быстрый (линейный) рост энтропии выходного кода. Рост энтропии снижается по мере увеличения длины ключа. Параметры среды моделирования «БиоНейроАвтограф» не до конца используют потенциал рукописного биометрического образа, однако, дальнейшее увеличение длины ключа незначительно (от 1% до 3%) может увеличить значение энтропии.

Кроме того, каждый биометрический образ имеет свою собственную функцию H(q). Это связано с тем, что каждый биометрический образ «Свой» уникален.

Вывод: То, что кривые роста энтропии, описываются функцией с участком насыщения, свидетельствует о невозможности бесконечного улучшения качества принимаемых решений с ростом длины ключа (числа нейронов в сети). Для каждого биометрического образа существует своя длина ключа, при которой функция H(q) выходит на участок насыщения. Дальнейшее увеличение длины ключа при использовании алгоритма обучения по ГОСТ Р 52633.5 не имеет смысла. Однако, смысл в повышении длины ключа появляется, если обучать нейронную сеть алгоритмом более эффективным, чем стандартный алгоритм.

11. Оценка коррелированности выходных состояний преобразователей биометрия-код

Квантовая механика много внимания уделяет такой категории, как запутанность состояний кубитов и фотонов. Для квантовой биометрии эта тематика так же актуальна. В предыдущем параграфе было показано, что реальная

энтропия 256 выходного кода нейронной сети оказывается меньше. Наблюдается дефект энтропии, обусловленный наличием корреляционных связей между случайными состояниями разрядов. Чем больше корреляция между разрядами кодов, тем меньше энтропия кодов. Оценить корреляцию между разрядами кодов удается через вычисления следующего функционала:

$$R(q) = \left(1 - \frac{H("x_1, x_2, \ldots, x_q")}{q}\right) \qquad (19).$$

В случае, если q=256 разрядов выходных кодов нейронной сети являются белым шумом, то их совместная энтропия составит 256 бит. Корреляционный функционал в этом случае оказывается нулевым R(256)=0. В противоположной ситуации, когда на вход нейронной сети подаются примеры данных образа «Свой», выходная энтропия кодов "$\bar{c}$" оказывается нулевой. Как результат, функционал (19) принимает единичное значение R(256)=1.

Энтропия реальных рукописных образов среды «БиоНейроАвтограф» находится в интервале от 0 бит до 58 бит для самых стабильных и самых уникальных образов рукописного пароля. Это означает, что корреляционный функционал (19) может измениться в интервале от 1 до 0.733.

Получается, что энтропия преобразователей биометрия-код всегда намного меньше, чем идеальная белого шума в 256 бит. Разряды кодов нейронной сети всегда оказываются значительно коррелированны. Связь корреляционных функционалов (19) со средним модулем обычных коэффициентов корреляции $E\{|r|\}$ [24, 25] приведена на номограмме рисунка 13.

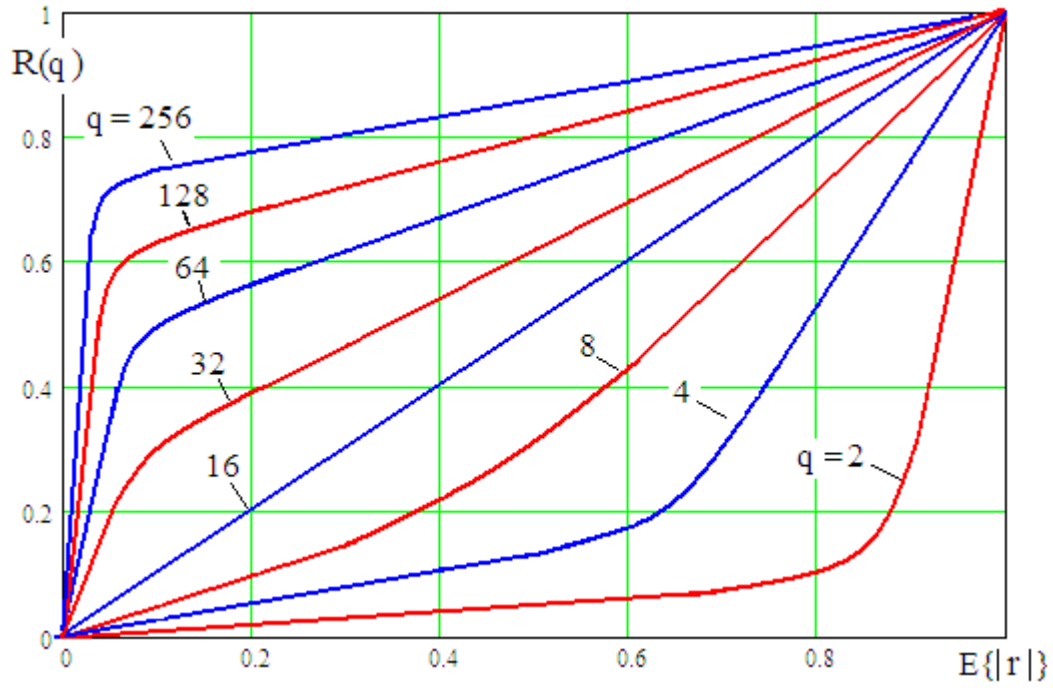


Рис. 13. Номограмма связи корреляционных функционалов R(q) со значением среднего значения модулей обычных коэффициентов корреляции

Из рисунка 13 видно, что размерность q=16 является прямой линией. То есть, проще всего оценивать энтропию биометрических данных используя 16-ти битные фрагменты кодов. Вычислив многократно среднее значение модулей парных корреляционных связей, мы можем найти R(q=16) и далее, пользуясь номограммой рисунка 13 для определения R(q=256). В свою очередь, по значению R(q=256) мы можем восстановить значение 256 мерной энтропии.

Предположительно этот путь в вычислительном отношении является более сложным в сравнении с вычислениями по формулам (16), (17).

Выводы: Пользуясь номограммой рисунка 12, мы можем от значения многомерной энтропии перейти к оценке среднего модуля обычных коэффициентов парной корреляции. При этом, из рисунка 13 видно, что размерность q=16 играет особую пограничную роль между низкоразмерными и высокоразмерными системами. Кривые связи низкоразмерной энтропии и высокоразмерной энтропии со средним модулем обычной корреляции имеют противоположную выпуклость. Они приближаются разными уравнениями в интервале числа выходов от 2 до 16 и в интервале числа выходов от 16 до 256.

12. Формирование баз тестовых биометрических образов

В линейной алгебре, кроме прямой операции перехода из одного пространства в другое, крайне важной является обратная процедура возврата в исходное пространство. Прямая операция выполняется путем умножения вектора координат первого пространства на матрицу преобразований [A], обратная операция выполняется умножением вектора координат во втором пространстве на обратную матрицу $[A]^{-1}$.

Совершенно такая же ситуация складывается и в биометрии. Обладая таблицами нейронной сети и знанием кода «Свой», попытаемся восстановить параметры биометрического образа. Фактически речь идет о возврате в пространство многомерных континуумов из пространства выходных кодов нейронной сети.

Самый простой путь решения этой задачи состоит в создании очень большой базы образов «Чужой» и последующего перебора этой базы до совпадения h= 0, 1, …, h_k. Технические проблемы создания и хранения такой «полной» базы весьма и весьма значительны. Проще всего показать наличие проблемы на нейросетевых преобразователях рисунка отпечатка пальца. В России действует стандарт ГОСТ Р 52633.1 [26], описывающий то, как следует собирать естественные биометрические образы в тестовые базы. Стойкость подобной биометрической защиты находится в интервале от 10^3 до 10^9 попыток подбора в зависимости от числа особых точек на рисунке отпечатка пальца. Как следствие, «полная» тестовая база должна иметь как минимум 10^{10} (десять миллиардов рисунков отпечатков пальца). Собрать такую большую базу можно, если привлечь в качестве доноров биометрии один миллиард людей. Это не реально, как в техническом, так и в экономическом плане.

В связи с этим, приходится использовать малые тестовые базы, содержащие от 1 000 до 10 000 реальных биометрических образов. Этого вполне хватает для поиска самых слабых биометрических образов с низкой энтропией, но недостаточно для решения обратной задачи для сильных биометрических образов с высоким уровнем энтропии выходных кодов.

Выход из создавшегося положения состоит в использовании синтетических биометрических образов, формируемых как образы-потомки путем скрещивания образов-родителей их морфингом, в соответствии с рекомендациями ГОСТ Р 52633.2 [27]. На рисунке 13 приведены примеры образов-потомков, полученные от двух рукописных образов-родителей «знамя»-«север» и двух рукописных образов-родителей «север»-«гусар».

Могут быть использованы разные варианты морфинг скрещивания образов-родителей. В левой части рисунка 14 отображена ситуация, когда из пары образов-родителей создается один образ-потомок, наследующий от родителей их биометрические параметры в равных пропорциях.

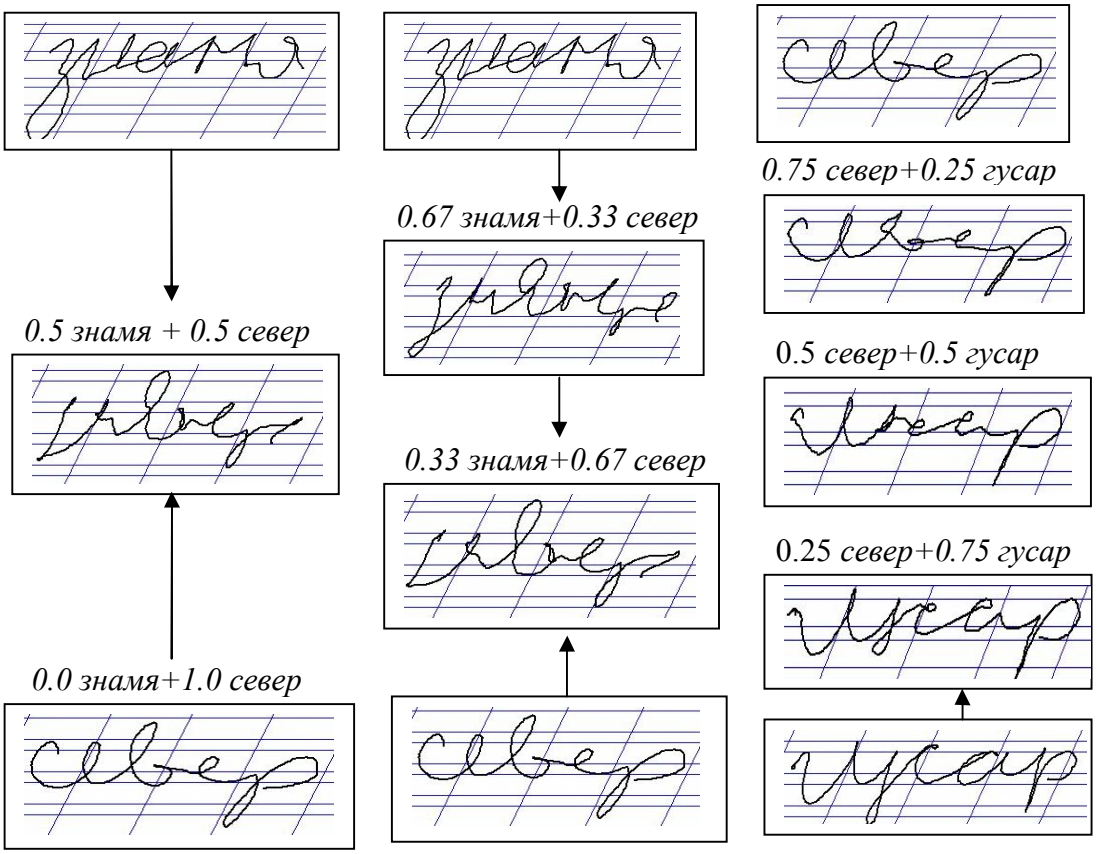


Рис. 14. Примеры синтеза одного, двух и трех образов-потомков
из двух образов-родителей

В принципе, у пары образов-родителей образов потомков может быть больше (по 2, 3, …, n потомков). При этом пространство данных между биометрическими параметрами родителей должно делиться на 3, 4, …, (n+1) частей. Так в центре рисунка 14 отображена ситуация создания двух образов потомков от пары образов-родителей. В этом случае, ближайший к родителю потомок наследует от него 67% каждого параметра. В правой части рисунка 13 отображена ситуация получения от пары родителей трех образов-потомков, в равных пропорциях наследующих биометрические параметры родителей.

Если мы будем иметь исходную базу в 1000 образов и создавать от каждой пары по 2 образа потомка, то получим тестовую базу с 10^6 образов. Для того, что бы получить тестовую базу в 10^9 образов, нужно иметь исходную базу объемом в 20 000 естественных образов и получать от каждой пары образов по 4 потомка.

Выводы. Обычный вычислительный компьютер способен за 1 секунду синтезировать примерно 1 000 000 образов-потомков и 1000 нейронных сетей. То есть, на синтез полной тестовой базы биометрических образов уйдет несколько часов непрерывной работы обычного компьютера, а на последующий просмотр этой базы уйдет несколько месяцев непрерывной работы этого же компьютера. Так в среде моделирования «БиоНейроАвтограф» каждый из 256 нейронов имеет по 24 входа, то есть, все нейроны сети моделируются на компьютере примерно в 10 000 раз медленнее, чем синтезируется один новый биометрический образ-потомок.

13. Итерационное решение обратной задачи нейросетевой биометрии в пространстве расстояний Хэмминга

Забивать память компьютера синтетическими образами, а потом их долго просматривать, не рационально. Более рациональным является совмещение процедуры синтеза биометрических образов и тестирования нейронной сети.

Рассмотрим ситуацию, когда имеется тестовая база, состоящая из 1000 биометрических образов «Чужой». Необходимо решить обратную задачу биометрии, восстановив неизвестный образ «Свой», располагая знаниями о таблицах обученной нейронной сети и зная код "$\overline{c}$". Для решения задачи выполним численный эксперимент по схеме, отображенной на рисунке 10. В итоге мы получим крайнее правое распределение расстояний Хэмминга рисунка 15 (поколение -1).

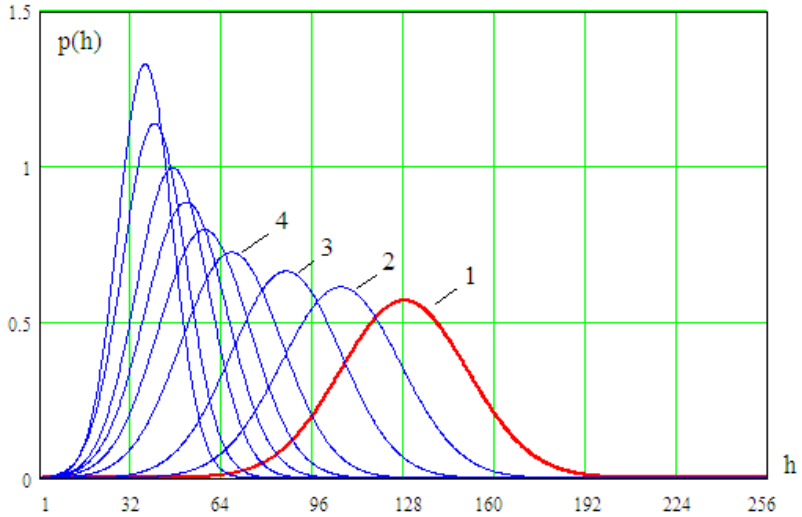


Рис.15. Эволюция распределений расстояний Хэмминга в 8 поколениях при селекции 4.5% образов с минимальным расстоянием Хэмминга

Если мы выбираем 4.5% наиболее близких рукописных образов (45 образов), то для восстановления численности второго поколения достаточно скрестить морфингом все возможные пары образов-родителей, получая от каждой пары по одному образу-потомку.

Восстановив численность второго поколения, мы вновь можем выбрать 4.5% образов наиболее близких образу «Свой» и, далее, восстановить численность третьего поколения. Получается итерационный эволюционный процесс извлечения знаний из искусственной нейронной сети. В процессе эволюции функции плотности распределения значений расстояний Хэмминга двигаются в сторону точки h=1, как это показано на рисунке 15.

Практика показывает, что на обычной вычислительной машине эволюционный процесс, имеющий от 30 до 60 поколений, позволяет восстановить образы с расстояниями Хэмминга от 0 до 7. Это эквивалентно полному или почти полному извлечению знаний из искусственной нейронной сети. Время эволюционных вычислений занимает от 20 до 40 минут.

Если считать, что «полная» база из 10^9 биометрических образов перебирается на обычной вычислительной машине за 4 месяца, то за счет использования направленного перебора мы сокращаем время до 40 минут, получая ускорение вычислений в 3 000 раз. Это эквивалентно примерно трем кубитам ускорения вычислений. При этом, внутри каждого цикла выполняется быстрая процедура вычисления вероятности ошибок второго рода,

обеспечивающая ускорение в 84 кубита (смотри раздел 9), то есть, мы имеем ускоритель вычислений в 87 кубит при решении задачи обращения матриц нейросетевых функционалов.

Вывод. Следует подчеркнуть, что все использованные вычислительные процедуры оказываются очень устойчивыми. Именно по этой причине удается обратить матрицу нейросетевых функционалов размерностью 416x256. В линейной алгебре обращение матриц столь высокой размерности технически невыполнимо. Скорее всего – это свойство нейлинейных многомерных пространств нейросетевых преобразований. Видимо, этого же можно добиться, оставаясь в многомерных линейных пространствах, однако, при этом нелинейные стабилизирующие свойства придется передать многомерным наблюдателям.

14. Вычисление частных значений энтропии образов «Чужой-k» нейросетевого преобразователя

Следует отметить, что энтропия нейронной сети, распознающей образ «Свой», сильно зависит от параметров этого образа. Практика показывает, что повышение стабильности параметров образа «Свой» приводит к росту энтропии $H("\bar{x}")$, то же самое происходит, если рукописное слово-пароль содержит уникальные знаки. Формально эту связь запишем, как относительную энтропию $H("\bar{c}"/"\bar{x}")$, имея в виду, что код -"$\bar{c}$" уникален для каждого биометрического образа в некоторой системе защиты информации.

Если подавать на входы нейронной сети, обученной распознавать образ «Свой», примеры образа «Чужой-k», то мы будем получать случайные выходные коды. Это ситуация отображена на рисунке 16.

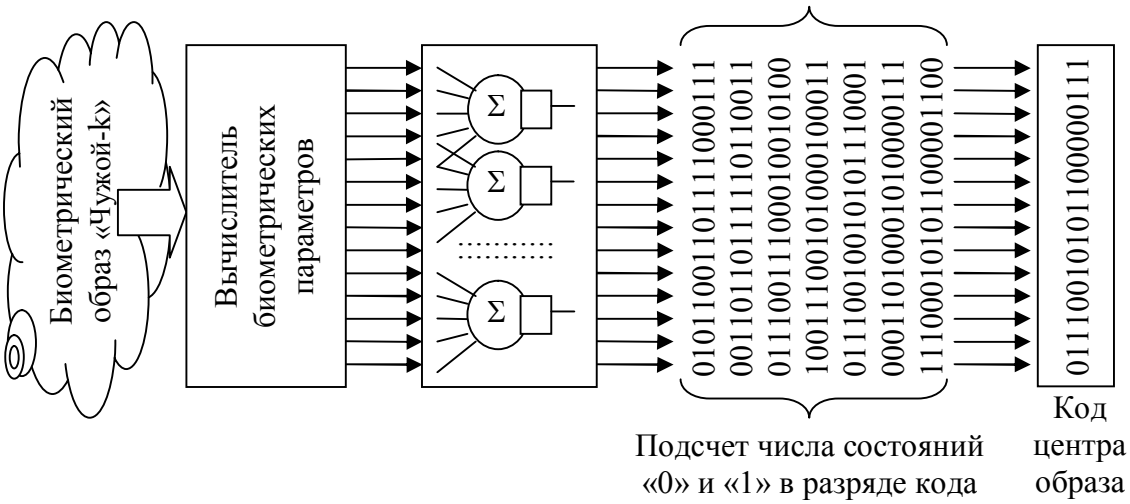


Рис. 16. Поразрядное накапливание состояний кода примеров образа «Чужой-k» при выявлении центра этого множества

Все состояния разрядов выходных кодов "x_{ki}"имеют значительную случайную составляющую, однако, и детерминированная составляющая в состояниях разрядов присутствует. Пользуясь этим можно найти наиболее вероятное состояние каждого из разрядов - "$E(x_{ki})$" или центра кодов «Чужой-k». При вычислении центра необходимо использовать достаточно большое нечетное число кодов. Далее необходимо оценивать вероятность появления

состояний «0_i» и состояний «1_i». Значение кода центра выбирается по наибольшей вероятности появления этих состояний в каждом разряде.

После того, как мы знаем центр образа «Чужой-k», относительно этого центра мы можем вычислить расстояния Хэмминга для кодов все «Чужие»:

$$h = \sum_{i=1}^{256} \left("x_i"\right) \oplus \left("E(x_{ki})"\right) \qquad (20).$$

Очевидно, что пользуясь соотношением (20), мы можем построить плотность распределения значений - p(h) расстояний Хэмминга. По этой плотности распределения можно найти вероятность случайного попадания данных все «Чужие» внутрь гиперэллипса «Чужой-k» по формуле (16). Логарифмический переход к энтропии (17) дает возможность получить распределение частных значений энтропии множества биометрических образов. Пример распределения значений таких частных энтропий $H("\overline{x}_k"/"\overline{x}")$ приведен на рисунке 17.

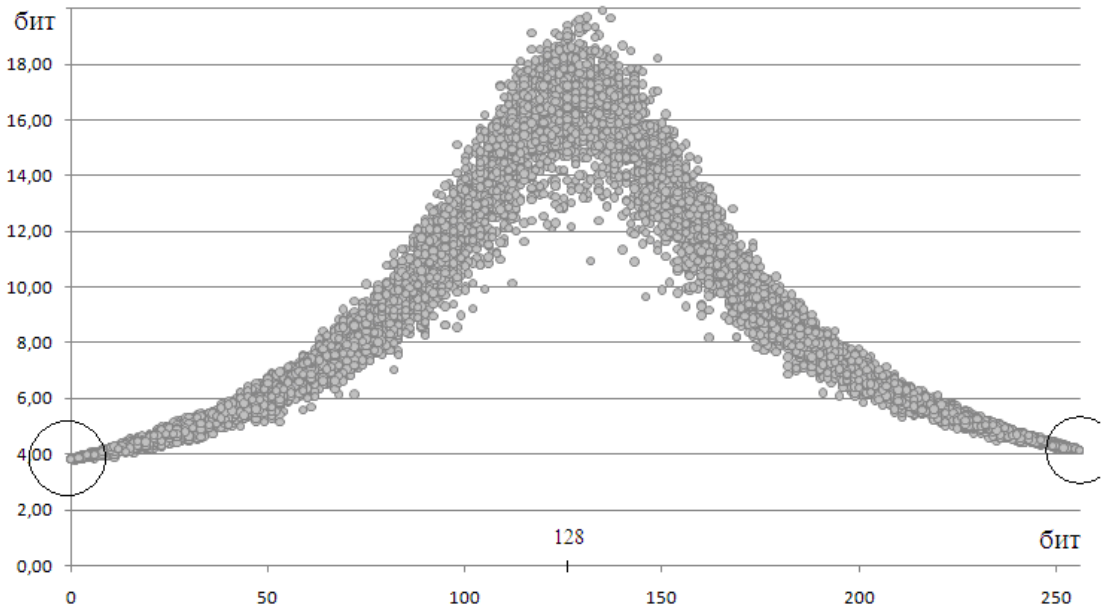


Рис. 17. Распределение значений энтропии биометрических образов «Чужие»

Из рисунка видно, что минимальной энтропией порядка 4 бит обладают две группы образов «Чужой». Одна группа оказывается близка образу «Свой», а вторая группа оказывается близка инверсному образу «Свой». Как следствие, могут использоваться две ветви эволюции [28, 29]. Одна ветвь эволюции должна быть направлена в сторону образ «Свой» и соответствует рисунку 15. Эта ветвь строится на левой группе образов, отмеченных окружностью на рисунке 17.

Вторая ветвь эволюции должна быть направлена в сторону инверсии образа «Свой». Эта ветвь должна строиться путем использования правой группы биометрических образов с минимальной энтропией. Использование двух ветвей эволюции приводит, как минимум, к сокращению в 2 раза требований к размерам исходной тестовой базы.

Выводы. Важнейшим является то, что при использовании двух ветвей эволюции, отпадает необходимость в знании кода $"\overline{c}"$ при обращении матриц нейросетевых функционалов. Вычислительные затраты на обращение матриц нейросетевых функционалов при реализации двух ветвей эволюции удваиваются, что не является техническим ограничением.

Еще одним практически важным следствием этого класса алгоритмов является возможность многопараметрического взаимного сравнения сложных объектов (таких как: университеты, банки, предприятия, регионы, …). Экспертам достаточно коллективно принять решение о худшем или лучшем объекте сравнения. Далее, следует обучить нейронную сеть распознавать эталонный объект. Далее на входы обученной нейронной сети объекта-эталона следует подавать данные других объектов и получить коды-отклики. По кодам-откликам строится распределение значений частных энтропий (рисунок 17), что является взаимным упорядочиванием всех объектов по отношению к объекту-эталону.

15. Многообразие функционалов, способных обогащать «плохие» данные входных многомерных континуумов

15.1. Настройка линейных, обогащающих данные, функционалов

Основная функция сумматоров нейронов – это функция обогащения множества «плохих» данных в континуальной форме, перед тем как осуществить их квантование. Как показано в разделе 4, чем лучше данные, тем меньше входов будет иметь нейрон. Очень «хорошие» данные вообще не нуждаются в обогащении.

Следует так же отметить, что на процесс обучения нейрона влияет размер обучающей выборки. Если обучающая выборка слишком мала, то возникает ситуация, когда обучить нейронную сеть обычными итерационными алгоритмами [21] нельзя. Причина состоит в том, что континуум гладкой функции вероятности или континуум гладкой функции распределения ступенчатыми функциями порождает ошибку приближения (шум квантования). На рисунке 18 приведены примеры таких шумов квантования.

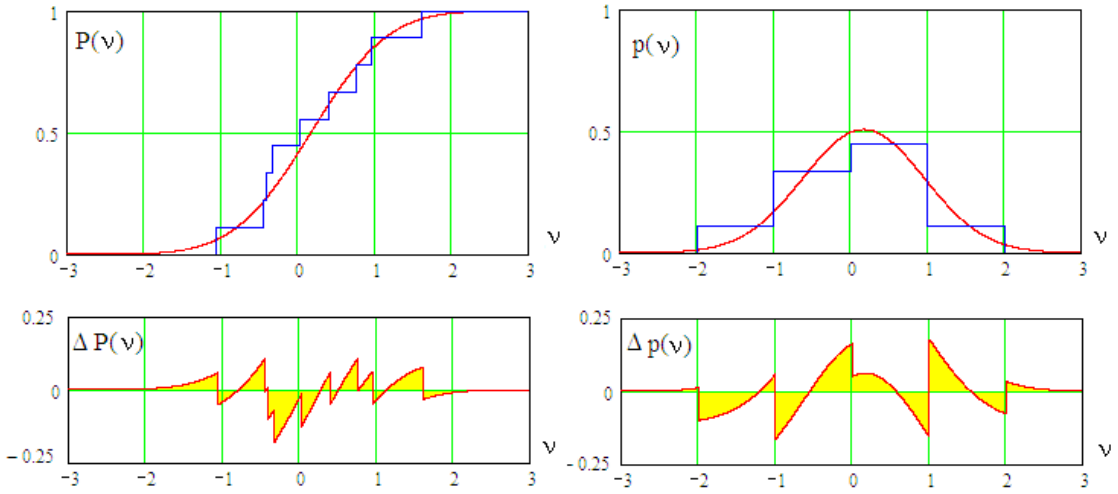


Рис. 18. Примеры шумов квантования, возникающие из-за малой обучающей выборки

Такие эффекты квантования возникают по каждой входной переменной $\{\nu_1, \nu_2, \ldots, \nu_m\}$. Шумы квантования усиливаются при использовании операций дифференцирования и мешают работе итерационных алгоритмов обучения [21].

В частности, для обучения может быть использован итерационный аналог алгоритма ГОСТ Р 52633.5. Этот алгоритм строится на том, что используется показатель качества следующего вида:

$$W = \frac{\left|E(y(\bar{\xi})) - E(y(\bar{v}))\right|}{\sigma(y(\bar{\xi})) \cdot \sigma(y(\bar{v}))} \qquad (21).$$

В каждом такте итерационный алгоритм обучения осуществляют изменение одного из весовых коэффициентов нейроны на величину $\Delta\mu_i$, это приводит к изменению качества обучения на величину ΔW. Если качество выросло, то введенное изменение $\Delta\mu_i$ принимается. При нулевом и отрицательном приращении качества введенные изменения не принимаются. Блок-схема итерационного обучения нейрона отображена на рисунке 19.

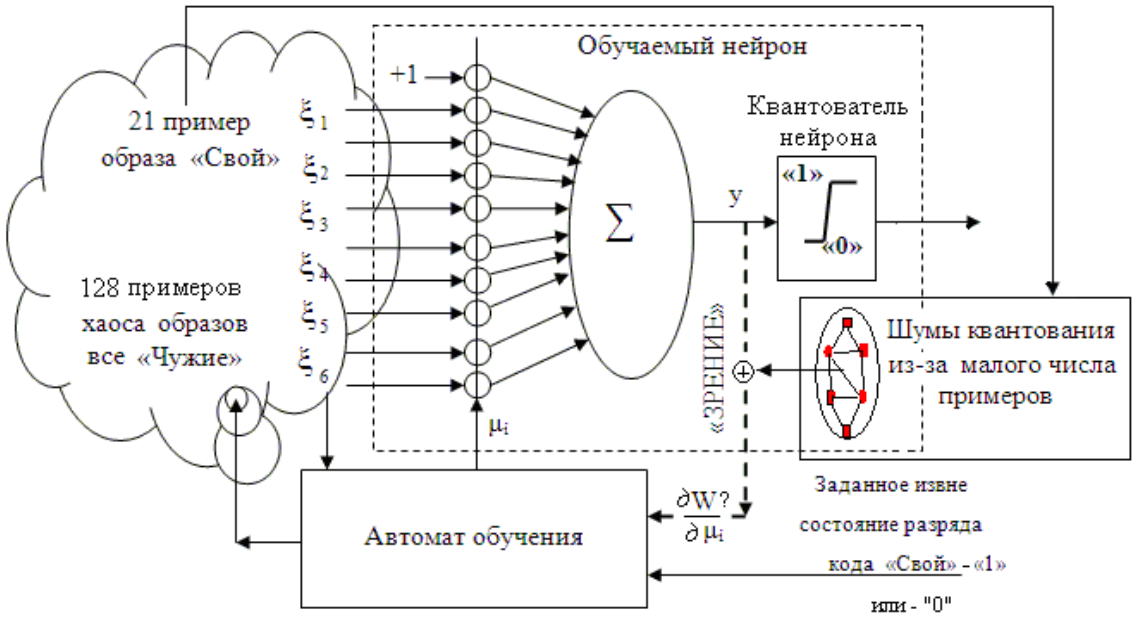


Рис. 19. Блок-схема итерационного алгоритма обучения (автомат обучения видит приращения качества)

Теоретически все алгоритмы итерационного обучения выглядят примерно одинаково, их схема кажется работоспособной, однако, это все справедливо, когда обучающие выборки велики. Когда обучающие выборки малы (недостаточно велики), возникает эффект появления множества ложных локальных максимумов (минимумов) критериев итерационной оптимизации. Эта ситуация отображена на рисунке 20, где даны графики изменения показателя качества (21) на каждой итерации поиска глобального максимума.

Из рисунка видно, что на недостаточной обучающей выборке возникают локальные экстремумы используемого при обучении функционала качества. При этом, размах колебаний между локальными экстремумами сильно зависит от числа примеров в обучающей выборке и числа входов у обучаемого нейрона. В верхней части рисунка 20 дана кривая почти монотонного роста выходного качества сумматора нейрона с 14 входами. Попытка увеличить число входов у нейрона до 15 приводит к потере устойчивости обучения (резко увеличивается колебательная составляющая). Для уменьшения колебательной составляющей следует уменьшить число входов у нейрона или увеличить число примеров в обучающей выборке.

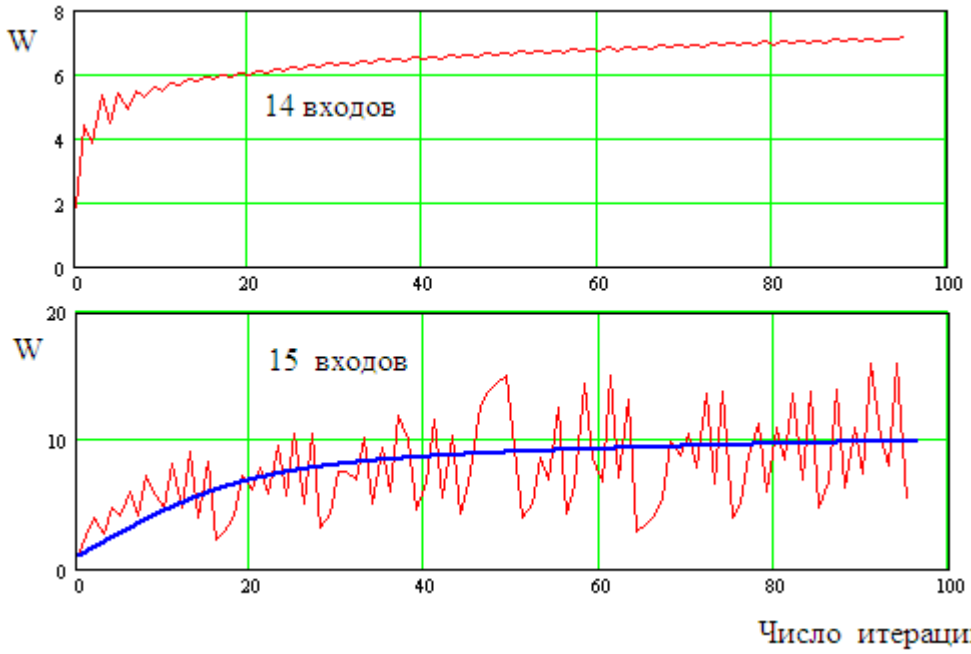


Рис. 20. Графики итерационного алгоритма обучения нейрона на выборке из 16 примеров образа «Свой»

В случае, когда обучающая выборка недостаточна для обучения нейрона со слишком большим числом входов, обратная связь итерационного алгоритма обучения, в основном, занимается оптимизацией многомерной поверхности ошибок квантования вместо оптимизации значимых информационных компонент. Фактически наблюдатель качества данных на выходе сумматора нейрона слепнет из-за негативного влияния шумов квантования обучающих выборок недостаточного объема.

Выводы. Кардинальным способом борьбы с негативным влиянием шумов квантования является полный отказ от использования итерационных алгоритмов обучения. В частности, алгоритм обучения ГОСТ Р 52633.5 не является итерационным и потому абсолютно устойчив, на его основе легко создаются автоматы обучения.

Тем не менее, усредненный результат качества итерационных алгоритмов обучения может оказаться лучше, чем не итерационных. Так среднее значение качества кривой в нижней части рисунка при 100 итерациях составляет W=10 (нижняя часть рисунка 20, толстая линия), тогда как этот же показатель для кривой верхней части рисунка составляет W=7.5. Наблюдается существенный выигрыш итерационных алгоритмов обучения в среднем, вполне возможно, что в будущем появится стандартизованная версия устойчивого итерационного алгоритма обучения нейронов с усреднением множества нейросетевых решений.

15.2. Квадратичные статистические функционалы многомерной обработки биометрических данных

Следует отметить, что кроме линейных функционалов повышения качества континуумов входных данных, ту же самую функцию могут выполнять различные варианты нелинейных функционалов. Самыми распространенными являются квадратичные функционалы, сети с такими функционалами получили наименование сетей радиально-базисных функций [21, 30]. Формально отклик радиального нейрона на j-тый пример образа «Свой» описываются следующим соотношением:

$$y_j^2 = \sum_{i=1}^{m} \frac{(E(\nu_i) - \nu_{i,j})^2}{\sigma^2(\nu_i)} \qquad (22).$$

Таким образом, при формировании нейрона могут быть использованы случайно выбранные биометрические параметры, однако, этот путь нерационален. Если биометрические параметры радиального нейрона сильно коррелированны, то нейрон оказывается малоэффективен.

Показать снижение эффективности квадратичных форм (22) при росте корреляционных связей между биометрическими данными, удается средствами имитационного моделирования. При этом, технически трудно воспроизводить данные с реальными матрицами корреляционных связей [31]. Технически гораздо более простым является умножение случайных данных на симметричную связывающую матрицу [32, 33]:

$$\begin{bmatrix} 1 & a & \cdots & a \\ a & 1 & \cdots & a \\ \cdots & \cdots & \cdots & \cdots \\ a & a & \cdots & 1 \end{bmatrix} \times \begin{bmatrix} \zeta_{1,i} \\ \zeta_{2,i} \\ \cdots \\ \zeta_{m,i} \end{bmatrix} = \begin{bmatrix} \nu_{1,i} \\ \nu_{2,i} \\ \cdots \\ \nu_{m,i} \end{bmatrix} \Rightarrow R_m = \begin{bmatrix} 1 & r & \cdots & r \\ r & 1 & \cdots & r \\ \cdots & \cdots & \cdots & \cdots \\ r & r & \cdots & 1 \end{bmatrix} \qquad (23).$$

В этом случае, данные оказываются равно коррелированными. Если плавно изменять единственный регулируемый параметр связывающей матрицы от 0 до 1, равная коррелированность также меняется от 0 до 1.

Следует отметить, что если данные в выражении (22) независимы и имеют нормальный закон распределения значений, то распределение значений точно совпадает с хи-квадрат распределением [34] $p(y^2) = p(\chi^2)$. Если же увеличивать равную коррелированность данных, то распределения данных квадратичных форм смещается в левую сторону как это показано на рисунке 21.

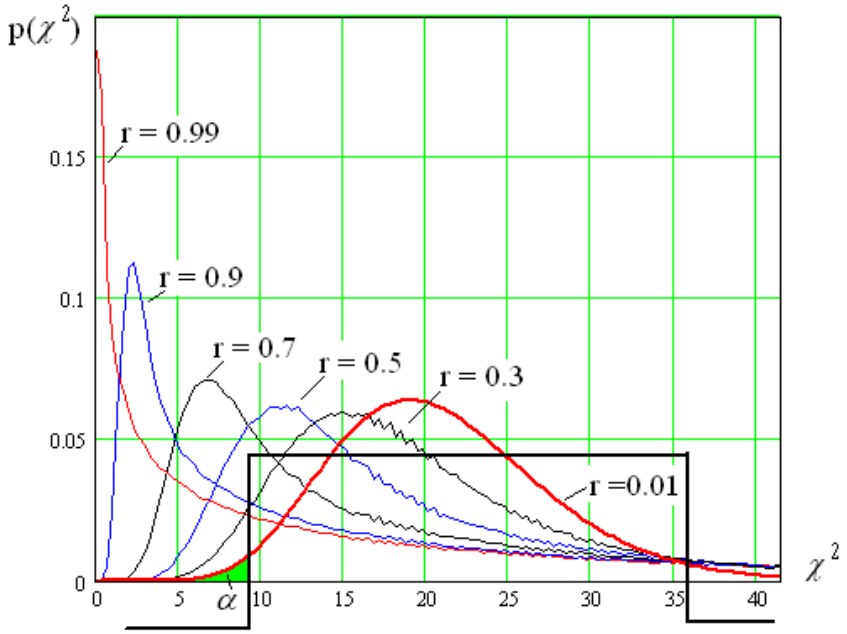


Рис. 21 Распределения хи-квадрат для разного уровня коррелированности данных при m =21 степеней свободы

Смещение распределений в левую сторону эквивалентно снижению эквивалентного числа степеней свободы $\tilde{m}$. Мода хи-квадрат распределений Пирсона на две единицы меньше числа степеней свободы [35, 36]:

$$M(p(\chi^2)) = m - 2 \qquad (24).$$

Получается, что эквивалентное число степеней свободы является функцией коррелированности данных - $\tilde{m}(r)$. Так при равной коррелированности r =0.5 эквивалентное число степеней свободы составляет $\tilde{m}(r = 0.5) \approx 9.5$. Мы видим эффект снижения числа степеней свободы и дробный (фрактальный) характер числа степеней свободы.

Традиционно в справочных руководствах по статистическим расчетам хи-квадрат распределения представлены таблицы доверительных вероятностей [37, 38]. Для зависимых хи-квадрат данных построена аналогичная таблица [34], приведенная ниже.

Таблица №1. Значения хи-квадрат для разных уровней достоверности и разных значениях коррелированности данных при числе степеней свободы m=21

m=21		Квантили доверительной вероятности принятия решения - α										
		0.01	0.02	0.05	0.1	0.2	0.5	0.8	0.9	0.95	0.98	0.99
Равная коррелированность	0.01	8.89	9.90	11.6	13.2	15.4	20.3	26.2	29.6	32.67	36.33	38.95
	0.1	8.56	9.57	11.2	12.9	15.1	20.1	26.3	30.3	33.97	38.67	42.22
	0.2	7.98	8.92	10.5	12.1	14.2	19.3	26.5	31.7	37.18	44.78	50.7
	0.3	7.20	8.08	9.54	11.0	13.1	18.3	26.9	34.0	41.82	52.83	61.57
	0.4	6.37	7.14	8.47	9.85	11.8	17.1	27.6	37.0	47.24	61.26	72.19
	0.5	5.47	6.15	7.34	8.57	10.4	15.8	28.5	40.1	52.57	69.88	83.29
	0.6	4.49	5.08	6.09	7.17	8.80	14.4	29.6	43.4	58.26	78.62	94.83
	0.7	3.49	3.96	4.78	5.68	7.13	13.0	30.7	46.7	63.95	87.60	106.0
	0.8	2.46	2.80	3.41	4.10	5.32	11.8	31.9	49.9	69.24	95.81	116.4
	0.9	1.32	1.52	1.88	2.34	3.32	10.7	33.1	53.3	74.83	104.7	128.2
	0.99	0.17	0.2	0.29	0.53	1.54	9.69	34.5	56.6	80.21	112.6	138.0

Для биометрии ошибка с вероятностью 0.04 вполне допустима, исходя из этого положения, выставим нижний порог срабатывания – 9.90 и верхний порог – 36.33 (первая строка таблицы 1 для r =0.01). Эти пороги обеспечивают состояние «1» с вероятностью 0.98 для образа «Свой». Если мы будем иметь дело с равно коррелированными данными с коэффициентом r =0.5, для достижения таких же характеристик при нижнем пороге срабатывания – 6.15 и верхнем пороге – 69.88. Получается, что рост корреляции с величины 0.001 до величины 0.5 приводит к практически двукратному расширению интервала между порогами. Это существенно увеличивает вероятность ошибок второго рода.

Для того, что бы снизить вероятность ошибок второго рода, необходимо осуществить настройку радиального нейрона. Возможны два пути настройки. Первый путь состоит в устранении корреляционных связей (например, процедурой Грамма-Шмидта [39, 40]). Однако, эта процедура неустойчива при малых объемах обучающей выборки.

Более рациональным является настройка (обучение) нейрона подбором входных данных. Мы можем вычислить матрицу коэффициентов корреляции биометрических данных. Распределение значений коэффициентов корреляции между парами биометрических параметров близко к нормальному. Пример такого распределения приведен на рисунке 21.

Из рисунка 21 видно, что малых коэффициентов корреляции больше, чем при нормальном законе распределения (верхушка распределения продавлена). В

связи с этим можно выбрать первую строку корреляционной матрицы $\{r(\nu_1,\nu_2), r(\nu_1,\nu_3), \quad , r(\nu_1,\nu_{416})\}$ и оценить их значения. Если считать закон распределения значений коэффициентов корреляции нормальным, то в интервал -0.05< r <+0.05 будут попадать коэффициенты с вероятностью 0.12, что соответствует обнаружению порядка 50 коэффициентов корреляции в выборке из 415 коэффициентов. Таким образом, даже одна строка корреляционной матрицы данных среды моделирования «БиоНейроАвтограф» дает возможность создавать радиальные нейроны с числом степеней свободы до 50.

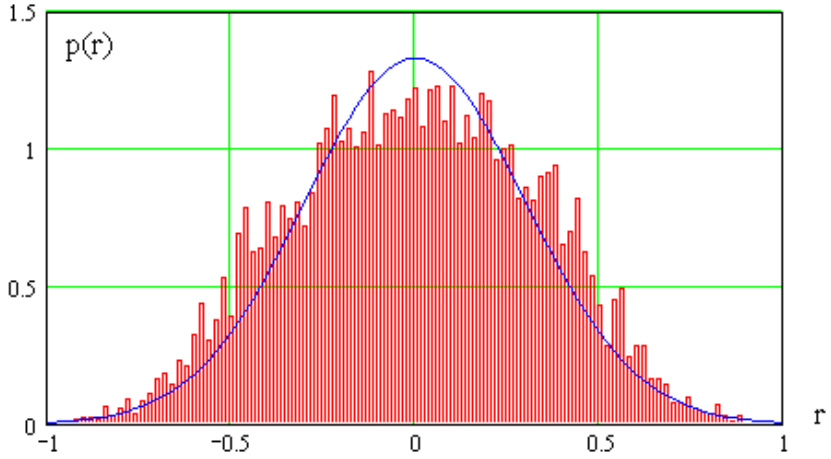


Рис. 22. Пример гистограммы, отражающей распределение значений коэффициентов парной корреляции биометрических параметров 21 примера рукописного слова «*Пенза*»

Число таких нейронов совпадает с числом строк корреляционной матрицы. То есть, при необходимости мы можем получить нейронную сеть с 416 входами и 416 бинарными выходами.

Параметры квантователя квадратичных нейронов (22) могут быть настроены по заранее вычисленным таблицам либо опытным путем, когда предъявляют обученному нейрону примеры образа «Свой», определяют наибольший отклик сумматора и наименьший отклик. Ориентируясь на экстремумы данных «Свой» устанавливают пороги принятия решений с некоторым запасом.

Вывод. Очевидно, что обычные линейные функционалы обогащения входных непрерывных данных нейронов имеют хорошо изученный квадратичный аналог (22) в виде, так называемых, радиально базисных функций [21]. Эти функции прекрасно работают в сетях Пирсона-Хэмминга. Настройка квадратичных функционалов таких нейронов в рамках линейной алгебры является очень трудной задачей, если пытаться строить обратную корреляционную матрицу в квадратичных формах. Все резко меняется, если отказаться от этой идеи, и, вместо обращения корреляционных матриц, осуществлять настройку квадратичных функционалов через поиск независимых параметров. Поиск независимых параметров имеет квадратичную вычислительную сложность. Это весьма и весьма перспективное направление создания новых алгоритмов быстрого и очень устойчивого обучения нейронных сетей.

15.3. Многомерные функционалы Байеса для сильно зависимых континуумов биометрических данных

Выше было показано, что сети квадратичных форм настраиваются выбором поиска слабо коррелированных биометрических данных. Наряду со слабо коррелированными данными существует их противоположность - сильно коррелированные данные (с корреляцией от $-0.9 > r > 0.9$). Эти данные расположены в правой и левой части распределения, приведенного на рисунке 21.

В рамках линейной алгебры полноценные квадратичные формы описываются следующим соотношением:

$$y^2 = (E(\overline{v}) - \overline{v})^T \cdot [R]^{-1} \cdot (E(\overline{v}) - \overline{v}) \qquad (25),$$

где $\overline{v}$ - вектор нормированных биометрических параметров с единичными стандартными отклонениями, $[R]^{-1}$ обратная корреляционная матрица.

Технически обращать корреляционные матрицы большой размерности очень сложно. Обращение матриц большой размерности является плохо обусловленной задачей. Однако, и корреляционные матрицы малой размерности обращаются тем хуже, чем более сильной корреляционной зависимостью обладают биометрические данные. Поясним это на примере матриц для одинаково коррелированных данных пятого порядка. Если коэффициент равной коррелированности составит r = 0.99, то число обусловленности для матрицы пятого порядка составит 496:

$$cond\begin{bmatrix} 1 & 0.99 & 0.99 & 0.99 & 0.99 \\ 0.99 & 1 & 0.99 & 0.99 & 0.99 \\ 0.99 & 0.99 & 1 & 0.99 & 0.99 \\ 0.99 & 0.99 & 0.99 & 1 & 0.99 \\ 0.99 & 0.99 & 0.99 & 0.99 & 1 \end{bmatrix} = 496 \qquad (26); \qquad \overline{\lambda} = \begin{bmatrix} 4.96 \\ 0.01 \\ 0.01 \\ 0.01 \\ 0.01 \end{bmatrix} \qquad (27).$$

Заметим, что число обусловленности – cond[R] является отношением максимального значения компонент собственного вектора сингулярных чисел $\overline{\lambda}$ матрицы [R] к его минимальной компоненте. Для матриц с равно коррелированными данными все (кроме первого) сингулярные числа одинаковы (26). Это означает, что задача одномерна и, в соответствии с парадигмой «бритвы Оккама», следует оставить один контролируемый параметр, отбросив 4 других сильно коррелированных параметров.

Идеология отбрасывания «плохих» параметров доминировала в 20 веке и популярна в настоящее время. Для обоснования снижения размерности задачи нужно было найти и отбросить сильно коррелированные параметры. По этой идеологии, учитывая один из двух сильно коррелированных параметров, нет смысла учитывать второй параметр. На самом деле это совсем не так.

Параллельно с идеологией поиска наиболее информативных параметров, при разработке искусственного интеллекта, многократно (циклически) при синтезе вероятностных рассуждений использовалось правило Байеса [40]:

$$P(v_1, v_2) = P(v_1 / v_2) \cdot P(v_2) = P(v_2 / v_1) \cdot P(v_1) \quad \text{if} \quad 0 < |r(v_1, v_2)| < 1 \qquad (28).$$

Если биометрические параметры независимы, то двухмерная вероятность определяется как произведение вероятностей:

$$P(v_1, v_2) = P(v_1) \cdot P(v_2) \quad \text{if} \quad r(v_1, v_2) = 0 \qquad (29).$$

В ином предельном случае, двухмерная вероятность оказывается одномерной:

$$P(\nu_1, \nu_2) = P(\nu_1) = P(a \cdot \nu_2 + b) \quad \text{if} \quad r(\nu_1, \nu_2) = \pm 1 \qquad (30),$$

где a, b – это коэффициенты линейного преобразования одного параметра в другой.

Очевидно, что правило Байеса можно записать для трехмерной функции вероятности:

$$P(\nu_1, \nu_2, \nu_3) = P((\nu_1, \nu_2)/\nu_3) \cdot P(\nu_3) = P(\nu_1/(\nu_2, \nu_3)) \cdot P(\nu_2, \nu_3) = \ldots \quad (31).$$

То же самое мы можем записать для вероятностей более высоких размерностей.

Следует отметить, что при больших значениях корреляции $r \approx \pm 1$ данные разных биометрических параметров повторяют друг друга [41, 42, 43, 44]. Предположим, что вне диагонали корреляционной матрицы размерами 416x416 удалось обнаружить m сильно зависимых биометрических параметров. В этом случае, мы можем упорядочить их, дав им новые монотонно возрастающие номера $\{\nu_1, \nu_2, \nu_3, ..., \nu_m\}$. При таком обозначении m-мерный функционал Байеса будет выглядеть следующим образом:

$$B = \frac{1}{m^2 - m} \sum_{i=1}^{m} \sum_{j=1}^{m} \left| \frac{|E(\nu_i) - \nu_i|}{\sigma(\nu_i)} - \frac{|E(\nu_j) - \nu_j|}{\sigma(\nu_j)} \right| \qquad (32).$$

Если все m биометрические параметры коррелированны на уровне $|r| \approx 0.99$, то функционал Байеса будет иметь значение близкое к величине $(1 - |r|) \approx 0.01$. Значительное отклонение от этой величины свидетельствует об обнаружении функционалом (32) образа «Чужой». По сути дела, функционал (32) есть не что иное, как корреляционная форма записи m-мерного правила Байеса после симметризации корреляционных связей.

Вывод. Принципиально важным являются то, что многомерные функционалы Байеса дополняют квадратичные нейроны и нейроны с линейными сумматорами. Для обычных нейронов и радиально-базисных нейронов сильно коррелированные данные бесполезны. Их противоположностью является функционалы Байеса, которые работают тем эффективнее, чем выше коррелированность, используемых ими данных. При приближении коррелированности данных к предельным значениям $|r| \approx 0.9999\ldots$ мощность функционалов Байеса становится неограниченно большой (наблюдается асимтота).

Использование m-мерных равно коррелированных данных (26) является ярким подтверждением эффективности функционалов Байеса. Только их применение позволяет для сильно зависимых данных (26) получить мощный 5-мерный функционал. Сети квадратичных форм и сети из нейронов подобные сильно зависимые данные не могут эффективно использовать.

15.4 Перспективы снижения требований к размерам выборки, используемой для оценки младших статистических моментов

15.4.1. Оценка погрешности определения математического ожидания как функции размеров тестовой выборки

Стандартный алгоритм обучения искусственных нейронных сетей по ГОСТ Р 52633.5 [11] построен на вычислении весовых коэффициентов нейронов через значения математического ожидания биометрических параметров и

значения стандартного отклонения. Очевидно, что при вычислении этих статистических моментов на малых выборках будут возникать ошибки.

Если считать, что закон распределения биометрических параметров нормален, то мы можем легко определить, как связана ошибка вычислений с числом опытов. На рисунке 23 приведены результаты численного моделирования ошибки вычислений при разных объемах тестовой выборки, при единичном стандартном отклонении и нулевом математическом ожидании.

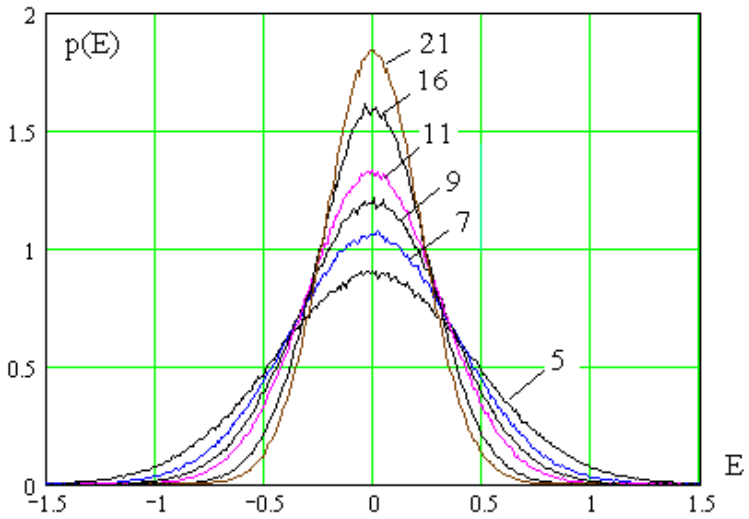


Рис. 23. Распределения значений математических ожиданий при разных объемах выборок, состоящих из n = 5, 7, 9, 11, 16, 21 опытов

Из рисунка 23 видно, что на малых тестовых выборках ошибки оценки математического ожидания могут быть велики. В связи с этим, при вычислениях статистических функционалов и при обучении искусственных нейронных сетей необходимо принимать специальные меры, компенсирующие погрешности вычисления математических ожиданий на малых тестовых выборках.

15.4.2. Компенсация методической погрешности оценки стандартного отклонения

При вычислении стандартного отклонения на малых выборках приходится пользоваться следующей формулой:

$$\sigma(\nu, n) = \sqrt{\frac{1}{n-1}\sum_{i=1}^{n}\left(E(\nu) - \nu_i\right)^2} \qquad (33).$$

Оценить влияние числа опытов - n на погрешность вычисления стандартного отклонения удается через проведение численного эксперимента для генератора нормального шума с единичным стандартным отклонением. Плотности распределения значений оценки стандартного отклонения при разных выборках приведены на рисунке 24.

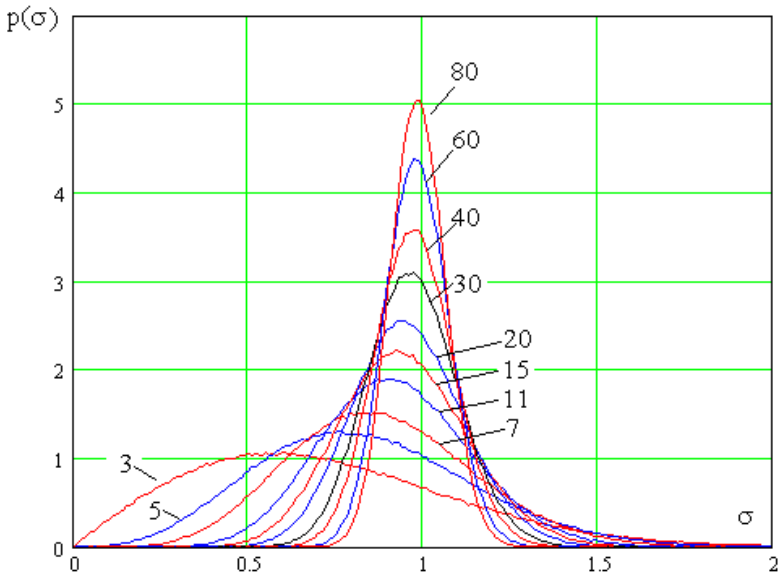


Рис. 24. Плотности распределения значений оценок стандартных отклонений для нормального закона распределения значений при разных объемах тестовой выборки

Из рисунка 24 видно, что при малых тестовых выборках наблюдается существенная асимметрия распределения данных. Эта асимметрия приводит к значительной методической погрешности оценки стандартного отклонения. Вместо наблюдения единичного математического ожидания, мы видим гораздо меньшее его значение, что отражено в таблице 2.

Таблица №2. Математическое ожидание стандартного отклонения

n	3	5	7	11	15	20	30	40	60	80
$E(\sigma(n))$	0.67	0.81	0.865	0.911	0.933	0.948	0.962	0.969	0.976	0.98

То есть методическая аддитивная ошибка оценки стандартных отклонений оказывается отрицательной и описывается следующей функцией:

$$\Delta\sigma(n) = 1 - E(\sigma(n)) \qquad (34).$$

Наиболее удобной формой компенсации методической погрешности (34) является ее приближение некоторой аналитической функцией. Для того, что бы выбрать форму аналитического приближения методической ошибки и оценить точность этого приближения, на рисунке 25 представлены графики, построенные по данным таблицы 2.

Пунктиром на рисунке 25 отображено приближение методической ошибки гиперболой:

$$\Delta\sigma(n) \approx 0.003 + \frac{1}{n} \qquad (35).$$

Пользуясь приближением (35) мы можем скомпенсировать выявленную методическую ошибку:

$$\sigma(v) = \left\{1.003 + \frac{1}{n}\right\} \cdot \sqrt{\frac{1}{n-1}\sum_{i=1}^{n}\left(E(v) - v_i\right)^2} \qquad (36).$$

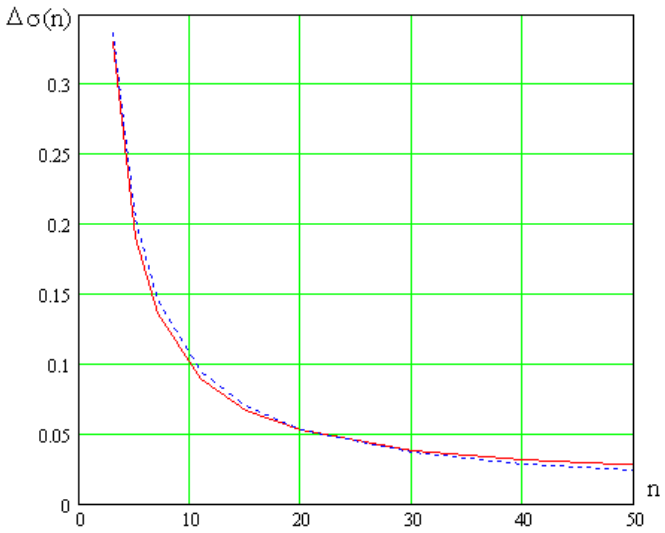


Рис. 25. Зависимость значения методической ошибки (непрерывная линия) от объема тестовой выборки

Выражение (36), в сравнении с классическим способом вычисления стандартного отклонения, позволяет снизить методическую ошибку примерно на два порядка для малых тестовых выборок, содержащих от 3 до 30 примеров биометрических данных [45]. При этом вычисления усложнились незначительно.

15.4.3. Компенсация случайной составляющей погрешности при оценке слабо коррелированных данных

Следует отметить, что по мере роста порядка оцениваемого статистического момента растет погрешность вычислений. Происходит накапливание погрешностей определения моментов более низкого порядка. Так при вычислении стандартного отклонения значительное влияние оказывает ошибка вычисления математического ожидания - ΔE. Когда мы вычисляем коэффициенты парной корреляции по формуле

$$r(\nu_1,\nu_2)=\frac{1}{n}\sum_{i=1}^{n}\frac{\left(E(\nu_1)-\nu_{1,i}\right)\left(E(\nu_2)-\nu_{2,i}\right)}{\sigma(\nu_1)\cdot\sigma(\nu_2)} \qquad (37),$$

на итоговый результат уже влияют четыре ошибки промежуточных вычислений: $\Delta E(\nu_1)$, $\Delta\sigma(\nu_1)$, $\Delta E(\nu_2)$, $\Delta\sigma(\nu_2)$. В результате ошибка вычисления коэффициентов корреляции увеличивается, примеры распределения ошибок даны на рисунке 26.

Из рисунка 26 видно, что самая большая погрешность возникает при определении коэффициентов корреляции независимых данных. Так для выборок из 16 независимых опытов вычисленный коэффициент корреляции попадает в интервал от -0.1 до +0.1 с вероятностью только 0.2. Становится актуальной задача повышения точности вычисления коэффициентов корреляции на малых выборках [46, 47].

Наряду с классическим способом вычисления корреляции (37) могут быть использованы другие вычислительные процедуры, примеры таких процедур приведены в таблице 3.

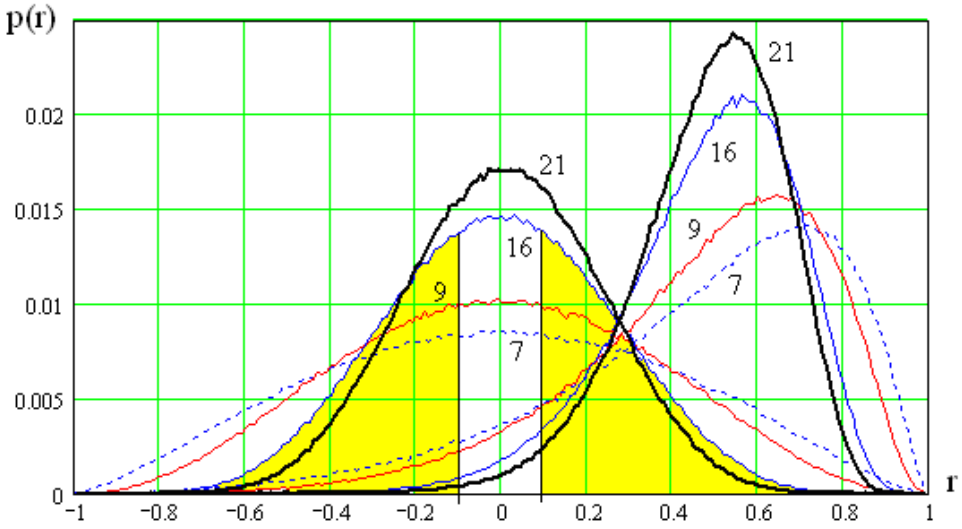


Рис. 26. Распределения значений коэффициентов корреляции для выборок из 7, 9, 16, 21 примеров при двух значениях коэффициентов корреляции r = 0 и r = 0.5

Таблица № 3. Наиболее часто используемые при обработке биометрических данных корреляционные функционалы

№	Название корреляционного функционала	Формула вычисления
1	Классический коэффициент корреляции, вычисленный на - n примерах пар случайных величин	$r(x,y)=\frac{1}{n}\sum_{i=1}^{n}\frac{(E(x)-x_i)\cdot(E(y)-y_i)}{\sigma(x)\cdot\sigma(y)}$, где E(.)- математическое ожидание; σ(.) – стандартное отклонение.
2	Корреляционно-энтропийный функционал второго порядка [33]	$\lvert r(x,y)\rvert=\left\{1-\frac{H(x,y)}{H(x)+H(y)}\right\}$, где $H(x,y)$ - двухмерная энтропия.
3	Функционал отношения большой – D и малой – d осей эллипса плотности распределения данных [37]	$\lvert r(x,y)\rvert=\frac{D-d}{D+d}$
4	Разностный корреляционный функционал Байеса [44]	$\lvert r(x,y)\rvert=\frac{1}{2\cdot n}\sum_{i=1}^{n}\left\lVert\frac{\lvert E(x)-x_i\rvert}{\sigma(x)}-\frac{\lvert E(y)-y_i\rvert}{\sigma(y)}\right\rVert$
5	Корреляционный функционал Херста 49]	$r(x,y)=2^{2X-1}-1$, где X – значение показателя Херста
6	Распределенная фрактально-корреляционная размерность [50, 51]	$C(x,y)=\lim_{\varepsilon\to 0}\frac{\ln\left\{k(\varepsilon)/n^2\right\}}{\ln(\varepsilon)}$, где k(ε)- число точек попарное расстояние, между которыми меньше -ε; n – число точек в выборке.
7	Центрированная фрактально-энтропийная размерность [50, 52]	$R(x,y)=\lim_{\varepsilon\to 0}\frac{H(\varepsilon)}{\ln(1/\varepsilon)}$, где H(ε) – энтропия точек, попавших в окружность радиусом -ε с центом E(x), E(y).

Из литературы по фрактальным вычислениям [49, 50, 51] известно, что оценить коррелированность данных можно измеряя «длину береговой линии» на картах разного масштаба. При этом, мы будем получать дробную (фрактальную) размерность, связанную с коррелированностью данных (строка 5, 6, 7 таблицы 3).

Для расчетов осуществим нормирование исходных данных $\tilde{x}, \tilde{y}$ по их размаху:

$$\begin{cases} x = \dfrac{\tilde{x} - \min(\tilde{x})}{\max(\tilde{x}) - \min(\tilde{x})} \\ y = \dfrac{\tilde{y} - \min(\tilde{y})}{\max(\tilde{y}) - \min(\tilde{y})} \end{cases} \qquad (38).$$

Далее следует упорядочить данные по одной из переменных. В итоге мы получим по две кусочно-ступенчатые линии для каждой из использованных процедур упорядочивания. Примеры пар таких ступенчатых функций приведены на рисунке 27 для одной и той же выборки, состоящей из 16 опытов.

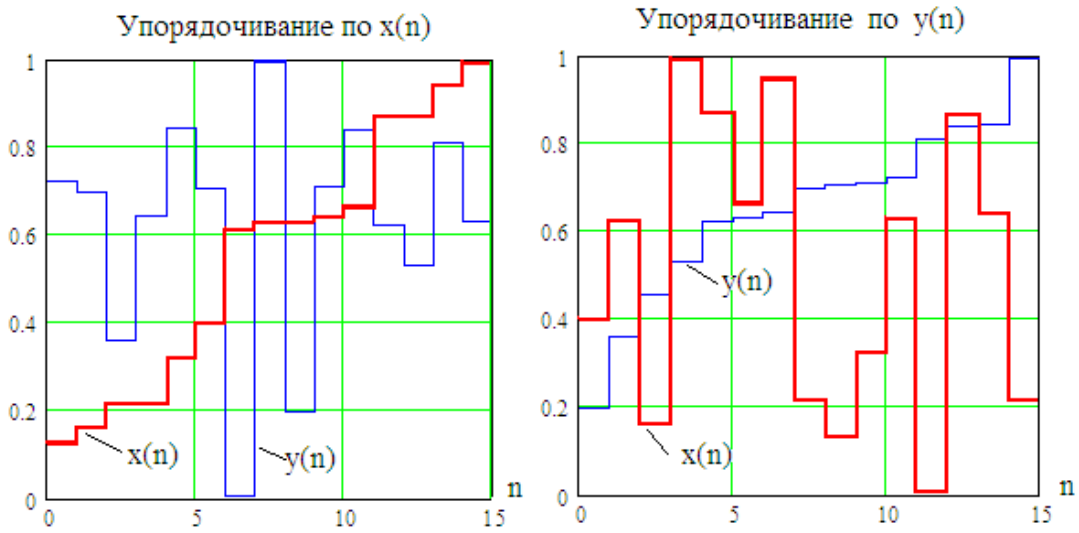


Рис. 27. Соотношение длин случайной и не случайной (упорядоченной) составляющих

Очевидно, что упорядоченная последовательность всегда будет давать монотонно возрастающую ступенчатую функцию меньшей длины, в сравнении с длинной второй не упорядоченной (случайной) компоненты.

Для ситуации, когда произведено упорядочивание данных по переменной – y, длину случайной компоненты – x определим как сумму модулей разности соседних данных:

$$D_x = \sum_{i=0}^{n-1} |x_i - x_{i+1}| \quad при \quad y_i \le y_{i+1} \qquad (39).$$

Для ситуации, когда произведено упорядочивание данных по переменной – x, длину случайной компоненты – y определим аналогично:

$$D_y = \sum_{i=0}^{n-1} |y_i - y_{i+1}| \quad при \quad x_i \le x_{i+1} \qquad (40).$$

Фрактально-корреляционный функционал для оценки слабо коррелированных данных будем вычислять следующим образом:

$$Fr(x, y, n) = \sqrt[3]{1 - \frac{D_x + D_y}{d(n))}} \approx r(x, y) \qquad (41),$$

где d(n) – масштабирующий коэффициент, зависящий от размеров тестовой выборки – n.

Для математического ожидания E(r)=0 и разных размеров тестовых выборок, значения масштабирующих длины коэффициентов приведены в таблице № 4. В этой же таблице даны стандартные отклонения распределения ошибок, получаемых при вычислениях по формуле (41) и вычислениях по стандартной формуле.

Таблица №4. Значения нормирующих коэффициентов и стандартных отклонений для фрактально-корреляционных функционалов, при разных объемах тестовой выборки и нулевой коррелированности проверяемых пар данных

n	d(n)	σ(Fr)	σ(r)		**n**	d(n)	σ(Fr)	σ(r)
7	5.05	0.510	0.365		**20**	11.57	0.446	0.214
8	5.62	0.491	0.361		**21**	11.70	0.444	0.221
9	6.14	0.503	0.347		**22**	12.65	0.438	0.207
10	6.73	0.458	0.347		**23**	12.82	0.454	0.213
11	7.18	0.473	0.319		**24**	13.42	0.447	0.204
12	7.54	0.486	0.314		**25**	13.91	0.434	0.208
13	8.43	0.469	0.297		**26**	14.35	0.427	0.209
14	8.44	0.455	0.269		**27**	14.95	0.449	0.194
15	9.27	0.452	0.271		**32**	17.43	0.423	0.191
16	9.51	0.434	0.257		**36**	18.56	0.420	0.176
17	10.31	0.457	0.246		**49**	24.78	0.416	0.162
18	10.53	0.423	0.254		**64**	30.71	0.380	0.135
19	10.88	0.475	0.223		**128**	55.57	0.377	0.096

Из таблицы № 4 видно, что стандартное отклонение фрактально-корреляционного функционала на малых выборках примерно в полтора раза больше, чем стандартное отклонение классического коэффициента корреляции. Кажется, что описанная выше работа напрасно выполнена. Мы получили еще один вариант вычисления коэффициента корреляции, который ведет себя много хуже, чем общепринятая классическая формула Пирсона (37).

Принципиально важным является то, что рассматриваемые в данной статье формулы вычисления коэффициентов корреляции различны. Разные формулы вычисления дают разные ошибки, что приводит к слабой корреляции погрешностей. То есть, можно взять пару разных формул и попытаться скомпенсировать независимую случайную составляющую погрешности. Например, объединение обычного коэффициента корреляции – r(x,y) и его фрактального аналога может быть осуществлено по следующей формуле:

$$R(x,y,n)=\left\{1-\frac{1}{b(n)}\right\}\cdot r(x,y)+\frac{1}{b(n)}Fr(x,y,n) \qquad (42).$$

Коэффициенты b(n) заранее вычисляются так, что бы минимизировать стандартное отклонение выражения (42). Значения минимизированных стандартных отклонений и значения коэффициентов минимизации приводятся в таблице №4.

Сравнивая данные таблиц № 4 и № 5 не трудно заметить, что стандартное отклонение σ(R) уменьшается примерно на 20% по сравнению со стандартным отклонением классической формулы - σ(r) для выборок из 16 примеров. Мы наблюдаем ощутимое повышение точности вычислений без увеличения размеров

тестовой выборки. Все это является подтверждением того, что ошибки функционалов Δr и ΔFr слабо коррелированны. Именно по этой причине их сборка (42) позволяет поднять точность вычислений.

Таблица № 5. Значения коэффициентов в корректирующей формуле (42), стандартного отклонения - $\sigma(R)$ и процент снижение ошибки вычислений – $\Delta\%$, который дает совместное использование двух разных формул вычисления коэффициентов корреляции.

n	b(n)	$\sigma(R)$	$\Delta\%$		**n**	b(n)	$\sigma(R)$	$\Delta\%$
7	2.98	0.285	28.1%		**20**	5.16	0.183	16.9%
8	2.76	0.313	15.3%		**21**	5.18	0.194	15.6%
9	2.84	0.272	27.6%		**22**	5.16	0.179	15.6%
10	3.24	0.299	16.1%		**23**	5.06	0.182	17.0%
11	3.16	0.258	23.6%		**24**	6.04	0.180	13.3%
12	3.96	0.267	17.6%		**25**	5.88	0.182	14.3%
13	3.24	0.232	27.4%		**26**	7.48	0.180	16.1%
14	3.80	0.234	19.0%		**27**	6.36	0.172	12.8%
15	3.46	0.220	22.6%		**32**	7.24	0.172	11.0%
16	3.40	0.221	20.4%		**36**	8.24	0.155	12.9%
17	3.64	0.216	22.2%		**49**	10.52	0.145	11.7%
18	4.44	0.227	11.9%		**64**	8.62	0.123	9.8%
19	4.12	0.185	20.5%		**128**	18.1	0.091	5.2%

Таким образом, усложнив в два раза алгоритм вычисления, удается примерно на 20% снизить ошибки вычисления коэффициентов корреляции на наиболее часто встречающихся в биометрии выборках из 16 опытов. Это эквивалентно тому, что тестовая выборка выросла с 16 примеров до 24 примеров (на 50%). Столь значительный рост размеров тестовой выборки крайне важен для биометрических приложений. Пользователи воспринимают биометрическую защиту как дружественную, если она не требует от них значительных затрат ресурсов на ее обучение и тестирование.

15.5. Многомерные функционалы, построенные по аналогии с критериями проверки статистических гипотез

В рамках математической статистики в 20 веке было разработано множество критериев проверки статистических гипотез. Толчком к развитию этого направления математических исследований послужила работа Пирсона, создавшего в 1900 году хи-квадрат критерий [35, 36]. Позднее были созданы множество иных общих и специализированных статистических критериев. Часть общих критериев (инвариантных к виду теоретического закона распределения) приведены в таблице 2.

При классической постановке задачи проверки статистических гипотез, используется экспериментально полученная функция вероятности $P(\hat{u})$ в виде ее ступенчатого приближения (рисунок 17). Сравнивать ступенчатое приближение функции вероятности - $P(\hat{u})$ с его непрерывным аналитическим представлением - $\tilde{P}(u)$ мешает шум квантования:

$$\Delta P(u) = P(\hat{u}) - \tilde{P}(u) \qquad (42).$$

Очевидно, что шумы квантования сильно зависят от размеров тестовой выборки –m. Монотонное увеличение числа примеров в тестовой выборке $m \to \infty$ приводит к монотонному снижению мощности шумов квантования:

$$\lim_{m\to\infty}\left(\int_{-\infty}^{+\infty}\left\{\Delta P(u)\right\}^2 \cdot du\right) = \lim_{m\to\infty}\left(\int_{-\infty}^{+\infty}\left\{P(\hat{u}) - \widetilde{P}(u)\right\}^2 du\right) \to 0 \qquad (43),$$

если эмпирическая и теоретическая функции вероятности совпадают. Если это не так, то соотношение (43) не может стремиться к нулю, оно становится равным некоторой конечной величине.

Заметим, что выражение (43) фактически является критерием Крамера-фон Мизеса (вторая строка таблицы 5). Все статистические критерии фактически строятся на учете статистик шумов квантования, ярким примером этого является критерий Колмогорова-Смирнова (1933 г.):

$$\sup_{-\infty<u>\infty}\left|P(\hat{u}) - \widetilde{P}(u)\right| = \sup_{-\infty<u>\infty}\left|\Delta P(u)\right| \qquad (44),$$

а так же критерий Купера (1960 г.):

$$\sup_{-\infty<u>\infty}\left\{P(\hat{u}) - \widetilde{P}(u)\right\} + \sup_{-\infty<u>\infty}\left\{\widetilde{P}(u) - P(\hat{u})\right\} = \sup_{-\infty<u>\infty}\left\{\Delta P(u)\right\} + \sup_{-\infty<u>\infty}\left\{-\Delta P(u)\right\} \qquad (45).$$

Очевидно, что мощность точечных критериев (44), (45) будет всегда меньше, чем интегральных критериев таблицы 5. Вычисление данных в точке (цифровое дифференцирование) подчеркивает случайные ошибки, а интегральные процедуры (процедуры цифрового накапливания) подавляют случайную составляющую шумов квантования.

Таблица № 5. Статистические критерии проверки гипотезы о соответствии эмпирической функции вероятности - $P(\hat{u})$ некоторому ее аналитическому описанию - $\widetilde{P}(u)$

№	Название критерия и год создания	Формула вычисления критерия
1	Хи-квадрат критерий Пирсона 1900 г.	$= N\sum_{i=1}^{m}\left(n_i/N - \widetilde{P}_i\right)^2/\widetilde{P}_i$, где N –число опытов, m –число интервалов гистограммы, n_i – число отсчетов, $\widetilde{P}_i$ - теоретическая вероятность попадания в i-тый интервал.
2	Критерий Крамера-фон Мизеса 1928 г.	$= \int_{-\infty}^{+\infty}\left\{P(\hat{u}) - \widetilde{P}(u)\right\}^2 \cdot du$
3	Критерий Смирнова-Крамера-фон Мизеса 1936 г.	$= \int_{-\infty}^{+\infty}\left\{P(\hat{u}) - \widetilde{P}(u)\right\}^2 \cdot d\widetilde{P}(u)$
4	Критерий Джини 1941 г.	$= \int_{-\infty}^{+\infty}\left\|P(\hat{u}) - \widetilde{P}(u)\right\| \cdot du$
5	Критерий Андерсона-Дарлинга 1952 г.	$= \int_{-\infty}^{+\infty}\frac{\left\{P(\hat{u}) - \widetilde{P}(u)\right\}^2}{\widetilde{P}(\hat{u}) \cdot \left\{1 - \widetilde{P}(u)\right\}} \cdot d\widetilde{P}(u)$
6	Критерий Ватсона 1961 г.	$= \int_{-\infty}^{+\infty}\left\{\widetilde{P}(u) - P(\hat{u}) - \int_{-\infty}^{+\infty}\left[\widetilde{P}(u) - P(\hat{u})\right] \cdot d\widetilde{P}(u)\right\}^2 \cdot d\widetilde{P}(u)$

7	Критерий Фроцини 1978 г.	$=\int_{-\infty}^{+\infty}\left\|P(\hat{u})-\tilde{P}(u)\right\|\cdot d\tilde{P}(u)$
8	Критерий среднего геометрического, сравниваемых функций вероятности 2014 г. [53, 54, 55]	$=\int_{-\infty}^{+\infty}\sqrt{P(\hat{u})\cdot(1-\tilde{P}(u))}\cdot du$

Однако, все классические статистические критерии одномерны, то есть они построены для анализа одной переменной. В биометрии такая постановка задачи не актуальна, в биометрии нужен многомерный статистический анализ групп биометрических данных.

Для биометрии нужны функционалы, которые при настройке должны давать минимальный отклик для данных образа «Свой» и как можно более значительный отклик для образов «Чужой». Добиться этого удается в том случае, если осуществить центрирование и нормирование биометрических данных по отношению к образу «Свой»:

$$\begin{cases} \nu_i = \dfrac{\nu_i - E(\nu_i)}{\sigma(\nu_i)}, \\ \xi_i = \dfrac{\xi_i - E(\nu_i)}{\sigma(\nu_i)} \end{cases} \qquad (46).$$

При этом, параметры централизации (вектор математических ожиданий - $\overline{E}(\nu)$) и параметры нормализации (вектор стандартных отклонений - $\overline{\sigma}(\nu)$) вычисляются на нескольких примерах обучающей выборки образа «Свой». После нормировки (46) примеры образа «Свой» должны иметь все параметры с близкими к нулевому математическими ожиданиями $E(\nu_i)\approx 0$. При этом, стандартные отклонения этих параметров должны стать близкими к единице $\sigma(\nu_i)\approx 1$. Для примеров образов «Чужие» центрирование и нормирование данных не происходит $E(\xi_i)\neq 0$, $\sigma(\xi_i)>1$.

Формально после нормировки (46) мы можем считать многомерные данные каждого примера образа «Свой» одномерной обучающей выборкой. Тогда становятся применимы все известные статистические критерии одномерной обработки. Применяя известные критерии, мы можем оценить то, на сколько различаются распределение данных образа «Свой» - $P(\nu)$ и распределения таких же данных образа «Чужой» - $P(\xi)$. На рисунке 28 приведено распределение 21 параметра примера образа «Свой» не участвовавшего при нормировке - $P(\nu)$ и 21 параметра образа «Чужой» - $P(\xi)$.

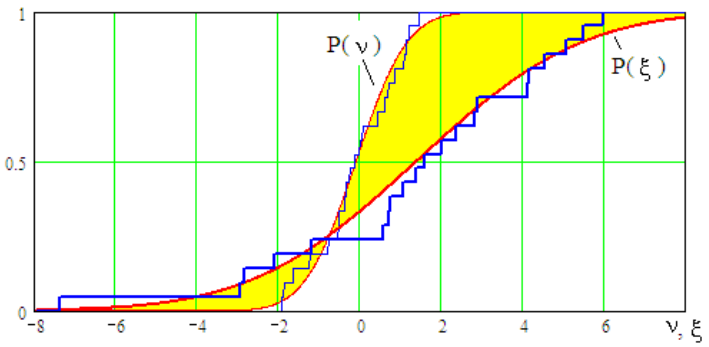


Рис. 28. Примеры функций вероятности множества биометрических параметров - $\hat{\nu}_i, \hat{\xi}_i$ для одного примера двух биометрических образов в виде дискретных и непрерывных функций вероятности

Из рисунка 28 видно, что непрерывные функции вероятностей $P(\nu)$, $P(\xi)$ сильно различаются (различие между их аналитическими описаниями отмечено заливкой), то есть из любого известного статистического критерия таблицы 2 может быть построен свой m-мерный функционал некоторого статистического «нейрона». Если будет использован функционал обогащения данных Крамера-фон Мизеса [57, 58] в нейронах, то мы получим сеть нейронов Крамера-фон Мизеса (KfM). Каждый из таких нейронов с функционалом KfM, квантует данные после их интегрирования:

$$\begin{cases} z\left\{\int_{-\infty}^{+\infty}\{P(\nu)-P(\xi)\}^2 d\xi\right\}=\text{"0"} \quad \text{if} \quad \int_{-\infty}^{+\infty}\{P(\nu)-P(\xi)\}^2 d\xi > k, \\ z\left\{\int_{-\infty}^{+}\{P(\nu)-P(\xi)\}^2 d\xi\right\}=\text{"1"} \quad \text{if} \quad \int_{-\infty}^{+\infty}\{P(\nu)-P(\xi)\}^2 d\xi \le k \end{cases} \qquad (47).$$

Порог квантования выбирается так же, как у других нейронов. Примеры образа «Свой» должны давать значения меньше порога сравнения.

В том случае, когда обогащение континуумов входных данных нейронов осуществляется функционалами Джини (строка 4 таблицы 5), эти конструкции имеет смысл называть сетями нейронов Джини [59, 60].

Статистических функционалов нейронов, построенных как подобие классических статистических критериев проверки гипотез, много. Таблица 5 при желании может быть расширена. Рассматриваемые функционалы необходимо уметь сравнивать между собой. Для взаимного сравнения желательно использовать точку, где функционалы оказываются слабее всего. Это точка полного совпадения математических ожиданий $E(\nu) = E(\xi) = 0$ и полного совпадения динамического диапазона изменения переменных ν, ξ. В этом случае различаются только функции вероятности $P(\nu)$, $P(\xi)$. Для того, что бы сравнить мощность функционалов, был проведен численный эксперимент. В ходе эксперимента на функционалы подавались данные с нормальным распределением - $\overline{\nu}$ и с равномерным законом распределения - $\overline{\xi}$. Принятие решения осуществлялось в точке равновероятных ошибок первого и второго рода $P_1 = P_2 = P_{EE}$. В итоге, в логарифмической шкале получаются практически линейные функции, описывающие снижение вероятности ошибок по мере увеличения входной размерности – m. Данные приведены на рисунке 29.

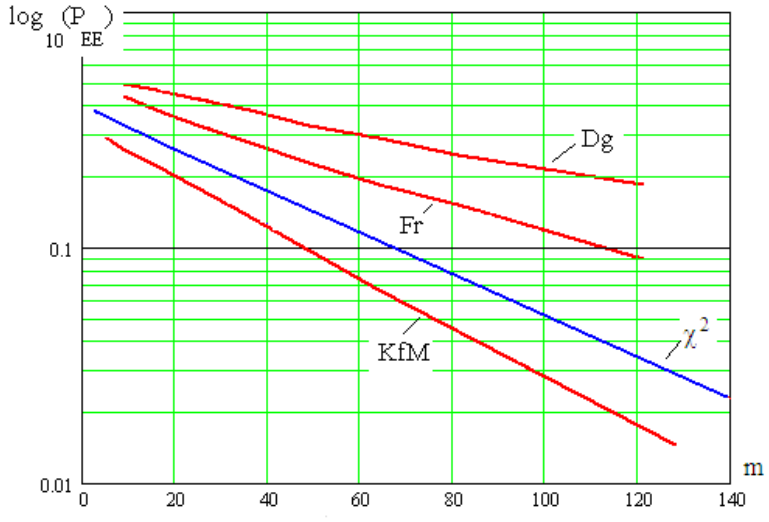


Рис. 29. Сопоставление мощностей интегральных статистических функционалов, как функции входной размерности для аналогов критериям Джини (Dg), Фроцини (Fr), хи-квадрат (χ^2) и Крамера-фон Мезиса (KfM)

Интересным является то, что в интегральных критериях функции вероятности можно заменить на их дифференциальные аналоги (на плотности распределения значений). Формальная замена преобразует таблицу 5 в таблицу 6.

Таблица № 6. Статистические критерии проверки гипотезы о соответствии наблюдаемой дифференциальной плотности вероятности $p(u)=\frac{dP(u)}{du}$ некоторому ее аналитическому описанию $\tilde{p}(u)$

№	Название критерия и год создания	Формула вычисления критерия
1	Дифференциальный вариант критерия Крамера-фон Мизеса	$=\int_{-\infty}^{+\infty}\{p(u)-\tilde{p}(u)\}^2\cdot du$
2	Дифференциальный вариант критерия Смирнова-Крамера-фон Мизеса	$=\int_{-\infty}^{+\infty}\{p(u)-\tilde{p}(u)\}^2\cdot\tilde{p}(u)\cdot du$
3	Дифференциальный вариант критерия Джини 2006 г. [31]	$=\int_{-\infty}^{+\infty}\lvert p(u)-\tilde{p}(u)\rvert\cdot du$
4	Интегро-дифференциальный вариант критерия Андерсона-Дарлинга	$=\int_{-\infty}^{+\infty}\frac{\{p(u)-\tilde{p}(u)\}^2}{\tilde{P}(u)\cdot\{1-\tilde{P}(u)\}}\cdot\tilde{p}(u)\cdot du;$
5	Дифференциальный вариант критерия Ватсона	$\int_{-\infty}^{+\infty}\left\{\tilde{p}(u)-p(u)-\int_{-\infty}^{+\infty}[\tilde{p}(u)-p(u)]\cdot\tilde{p}(u)\cdot du\right\}^2\cdot\tilde{p}(u)\cdot du$
6	Дифференциальный вариант критерия Фроцини	$=\int_{-\infty}^{+\infty}\lvert p(u)-\tilde{p}(u)\rvert\cdot\tilde{p}(u)\cdot du$
7	Критерий среднего геометрического плотностей сравниваемых вероятностей 2016 г. [53]	$=\int_{-\infty}^{+\infty}\sqrt{p(u)\cdot\tilde{p}(u)}\cdot du$
8	Квадрата критерия среднего геометрического плотностей вероятности 2016 г. [54]	$=\int_{-\infty}^{+\infty}p(u)\cdot\tilde{p}(u)\cdot du$

Подобная замена увеличивает число возможных для использования функционалов обогащения данных. Как показано на рисунке 30, в ряде случаев дифференциальные функционалы имеют мощность существенно выше интегральных функционалов.

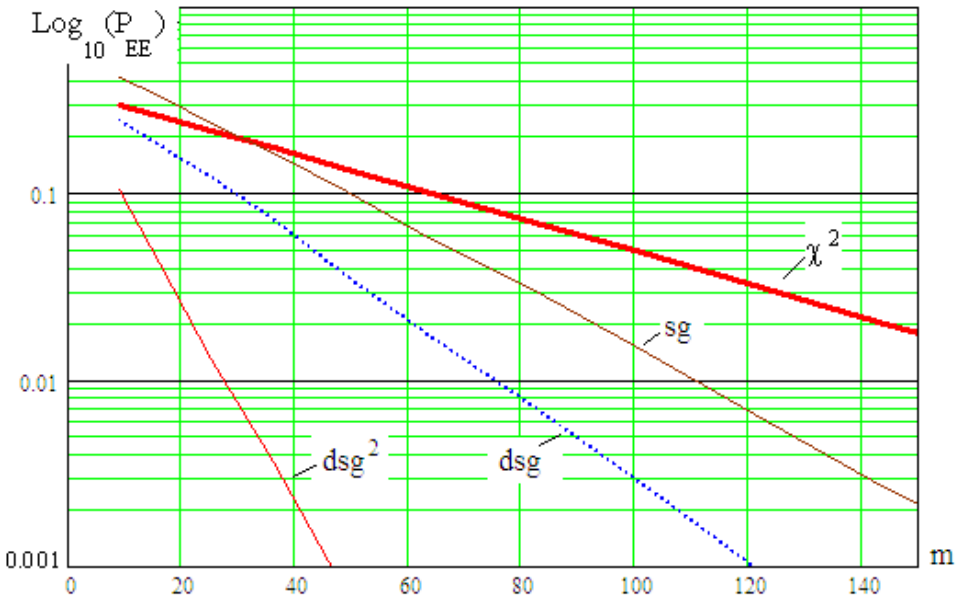


Рис. 30. Эталонная мощность хи-квадрат критерия (толстая линия) в логарифмической шкале равновероятных ошибок, sg – интегральный функционал среднего геометрического, dsg –дифференциальный вариант функционала среднего геометрического

Как видно из рисунка 30, квадрат среднего геометрического сравниваемых функций распределения дает наибольшую мощность (dsg^2), обеспечивая минимальное значение равновероятных ошибок первого и второго рода на малых выборках. Видимо, это самый мощный на текущий момент статистический критерий [56].

Впервые эффект повышения мощности при переходе от интегрального варианта критерия Джини к его дифференциальному аналогу, численно доказан Ю.И. Сериковой [59, 60, 61]. Позднее К.А. Перфилов [53 -:- 56] подтвердил наличие такого же эффекта для статистических критериев среднего геометрического. Для иных критериев наличие этого эффекта не проверялось.

Вывод. В предыдущем разделе 15.2 было показано, что функционалы Пирсона, квадратичные функционалы, квадратичные формы – это одно и то же. Исходя из этого, все иные статистические функционалы (критерии) так же могут быть использования для создания нейронов, обогащающих входные данные и затем их квантующие. Существуют сотни различных статистических критериев. Возникает проблема их отбора для селекции перспективных нейронов для многомерной статистической обработки биометрических данных. Решить эту проблему удается, приводя различные статистические критерии (функционалы) к одним и тем же условиям. На данный момент создается впечатление, что дифференциальные статистические критерии (использующие сравнение плотностей распределения значений) мощнее интегральных критериев (использующих сравнение экспериментальной и теоретической функции вероятности). На сколько это положение соответствует истине, могут подтвердить независимые исследователи.

Естественно, что все эти исследования должны проводиться для малых обучающих и тестовых выборок.

16. Корректирующие возможности нейросетевого преобразователя путем дополнительного исследования состояний разрядов

Очевидно, что идеальной настройки нейрона нельзя добиться на малой обучающей выборке примеров образа «Свой». Реальные преобразователи биометрия-код с вероятностью 0.9 дают верный код ключа. С вероятностью 0.1 получается почти верный код, отличающийся от эталона в 1, 2, 3 битах. Возникает необходимость в правке небольшого числа ошибочных разрядов. Эта ситуация иллюстрируется рисунком 31.

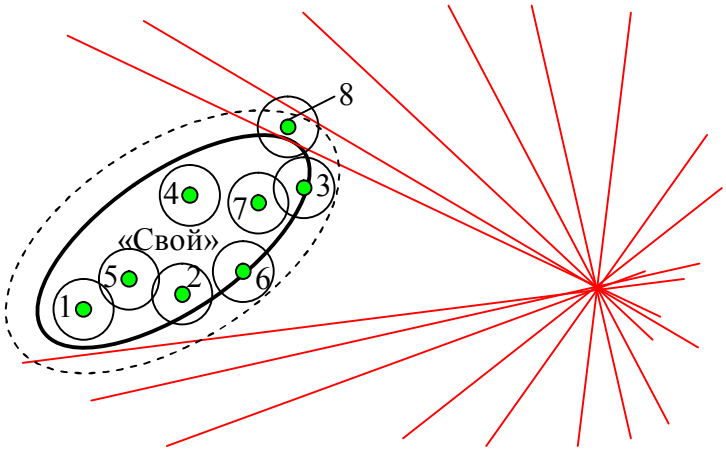


Рис. 31. Обнаружение нестабильных разрядов кода путем добавления тестового малого шума во входные данные

Из рисунка 31 видно, что обучение проводилось на малом числе из 7 примеров образа «Свой». По этой причине 8-ой пример, не участвовавший в обучении, дал в одном из разрядов выходного кода ошибочное состояние.

Наличие ошибки в коде мы можем обнаружить, сравнивая код «Свой» с выходными данными нейросетевого преобразователя. Обнаружив неверный разряд кода, мы должны принять решение о возможной его корректировке.

Для принятия такого решения необходимо размыть биометрические данные проверяемого образа аддитивным белым шумом с амплитудой 30% от стандартного отклонения данных вектора, проверяемых биометрических параметров - $\overline{v}$. Схема такого численного эксперимента приведена на рисунке 32.

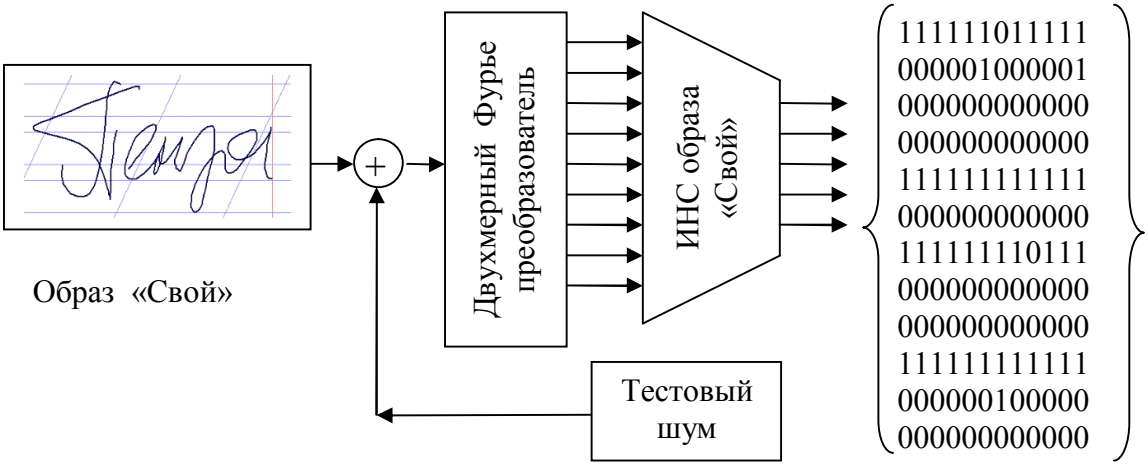


Рис. 32. Отклик обученной нейронной сети на известный ей образ «Свой», размытый тестовым шумом

При этом образуется некоторая гиперсфера просмотра окрестностей вокруг точки вектора проверяемых биометрических параметров, как это отражено на рисунке 31.

Как правило, точки всех примеров биометрического образа, участвовавших в обучении преобразователя при 10% размывании данных, дают стабильный код. На рисунке 31 для точек примеров 1, 2, …, 7, участвовавших в обучении, их гиперсферы не пересекают линий (проекций разделяющих гиперплоскостей). По данным рисунка 31 нестабильными оказываются два разряда выходного кода (сфера точки - 8 пересекает две линии). Если неправильный разряд выходного кода нестабилен, то мы имеем право, корректировать его.

Очевидно, что корректировка оказывается тривиальной, если мы храним в таблицах нейросетевого преобразователя код его отклика "$\bar{c}$". В приложениях биометрической аутентификации этого делать нельзя (код нельзя компрометировать). Однако могут быть построены специальные корректирующие коды, использующие безопасное хранение синдромов ошибок в виде фрагментов хэш-функций [62, 63]. Пользуясь записанными фрагментами хэш-функций, эти коды осуществляют перебор нестабильных разрядов, восстанавливая значение малого числа нестабильных разрядов.

Вывод. Ранее мы рассматривали значение кода на выходе нейросетевого преобразователя и делали вывод об обнаружении образа «Свой» по нулевому расстоянию Хэмминга. Теперь выяснилось, что определить образ «Свой» можно вообще не зная его кода. Достаточно «просматривать» окрестности данных анализируемого примера. Подав на вход преобразователя шум, составляющий 30% от естественной нестабильности данных и не обнаружив каких-либо изменений в коде, мы вынуждены признать тестируемый образ как «Свой». Появляется еще одна ветвь алгоритмов идентификации образов.

17. Показатель стабильности разрядов выходного кода нейросетевого преобразователя для примеров образа «Чужой»

Если подавать примеры образа «Свой» на обученный преобразователь, то на его выходе будут появляться практически одинаковые выходные коды (см. рисунок 32). Совершенно иная ситуация возникает, когда на обученную нейронную сеть подаются примеры одного образа «Чужой-k». В этом случае, каждый разряд выходного кода имеет не равновероятные состояния:

$$\begin{cases} P("0_i") + P("1_i") = 1, \\ P("0_i") \neq P("1_i") \end{cases} \qquad (48).$$

Эта ситуация отображена на рисунке 28.

Как было показано ранее (смотри раздел 14, рисунок 16), для кодов образа «Чужой-k» можно вычислить центр, накапливая состояния в каждом разряде. Можно поступить иначе и оценивать показатель стабильности состояний каждого i-го разряда:

$$w("x_i") = 2 \cdot \left| \frac{1}{2} - P("1_i") \right| = 2 \cdot \left| \frac{1}{2} - P("0_i") \right| \cdot \quad (49).$$

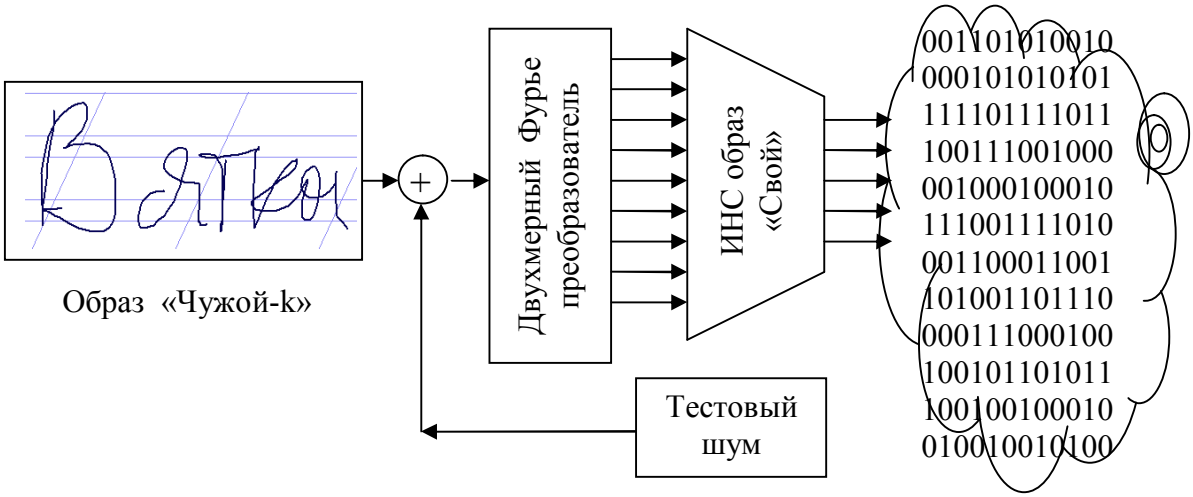


Рис. 33. Отклик искусственной нейронной сети на неизвестный ей образ «Чужой», размытый тестовым шумом

В случае, если разные состояния i-го разряда равновероятны $P("0_i") = P("1_i")$, показатель стабильности разряда оказывается нулевым. В иных предельных случаях $P("0_i") = 1$ или $P("1_i") = 1$ показатель стабильности оказывается единичным $w("x_i") = 1$. Оценивать показатель стабильности можно по одному примеру, тогда используется схема тестирования, приведенная на рисунке 33 (амплитуда шума в этом случае должна совпадать со стандартным отклонением данных образа «Чужой-k». Можно пойти по другому пути, предъявляя искусственной нейронной сети примеры пары образов «Свой» и «Чужой-k» или потомки этих образов. И в том, и в другом случае, получаются гистограммы распределения показателей стабильности, приведенные на рисунке 34.

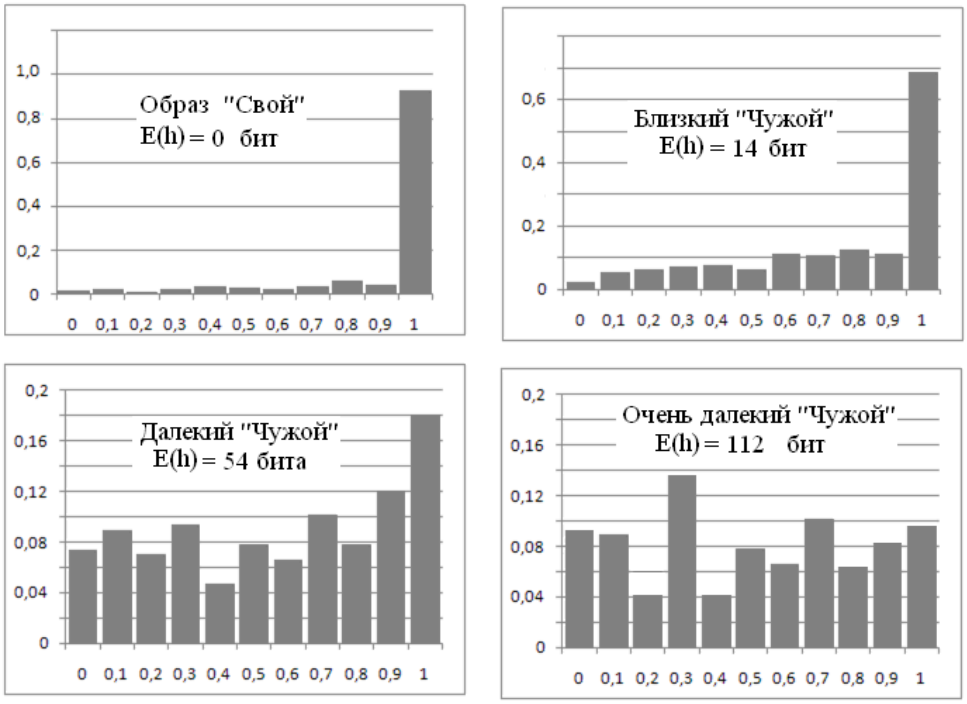


Рис. 34. Падение показателя стабильности разрядов кодов «Чужой» по мере удаления образа «Чужой» от образа «Свой»

Как видно из рисунка 34, коды образа «Свой» обладают рекордной стабильностью. Каждый разряд кодов «Свой» изменяется редко, показатель стабильности всех разрядов близок к единице. При незначительном отклонение образа «Чужой» от образа «Свой» разряды выходного кода остаются достаточно стабильными. По мере удаления центра кодов образа «Чужой» от кода образа «Свой», показатель стабильности разрядов падает. Наиболее нестабильными разряды выходного кода «Чужой» становятся при расстоянии Хэмминга равным половине разрядов в коде - E(h)≈128 бит. Далее, при увеличении расстояний Хэмминга, происходит обратный процесс повышения стабильности разрядов выходного кода. Для инверсного выходного кода - E(h)=256 мы получаем распределение, соответствующее левому верхнему распределению стабильности разрядов кода образа «Свой».

По сути дела, форма распределения показателей стабильности выходных кодов «Чужой-k» является некоторой метрикой энтропии этих кодов (смотри рисунок 17). Чем стабильнее состояния разрядов кода, тем меньше его энтропия. Наибольшая энтропия оказывается для образов «Чужой-k» с центром E(h)≈128 бит до образа «Свой» или инверсии образа «Свой».

Расстояния Хэмминга и средний показатель стабильности разрядов кода дополняют друг друга. Пользуясь этим, мы можем построить функционал Хэмминга, одновременно учитывающий и расстояние Хэмминга, и показатель стабильности сравниваемых разрядов [64, 65]:

$$h(w) = \sum_{i=1}^{256} w("x_i") \cdot \left[("x_i") \oplus ("c_i")\right] \qquad (50).$$

Мощность взвешенного расстояния Хэмминга много выше мощности обычного расстояния Хэмминга. Получается, что мы можем улучшать качество принимаемых решений не только за счет накопления информации в континуальных функционалах (раздел 15), но и при использовании функционалов (50), построенных для дискретных данных.

Так в разделе 13 мы рассматривали решение обратной задачи нейросетевой биометрии в пространстве расстояний Хэмминга. Если мы ту же самую задачу будем рассматривать в пространстве взвешенных показателями стабильности функционалов Хэмминга (41), число итераций сокращается. Как будет показано далее, применение функционалов Хэмминга (41) оказывается выгодным еще и при корректировке ошибок, возникающих при разделении близких образов-соседей.

Вывод. Кроме метрики расстояний Хэмминга существует метрика стабильности разрядов Хэмминга. Обе эти метрики дополняют (усиливают) друг друга. Каждая из этих метрик может использоваться самостоятельно или совместно (50).

18. Сравнение корректирующих способностей классических избыточных кодов и нейросетевых средств распознавания образов на фоне шумов

Объем аналоговой (континуальной) информации намного выше, чем объем дискретной (квантованной) информации. Именно это обстоятельство позволяет нашему естественному интеллекту распознавать образы на фоне значительного уровня помех. Так на рисунке 35 даны изображения символов «*a*» при различном уровне помех [66].

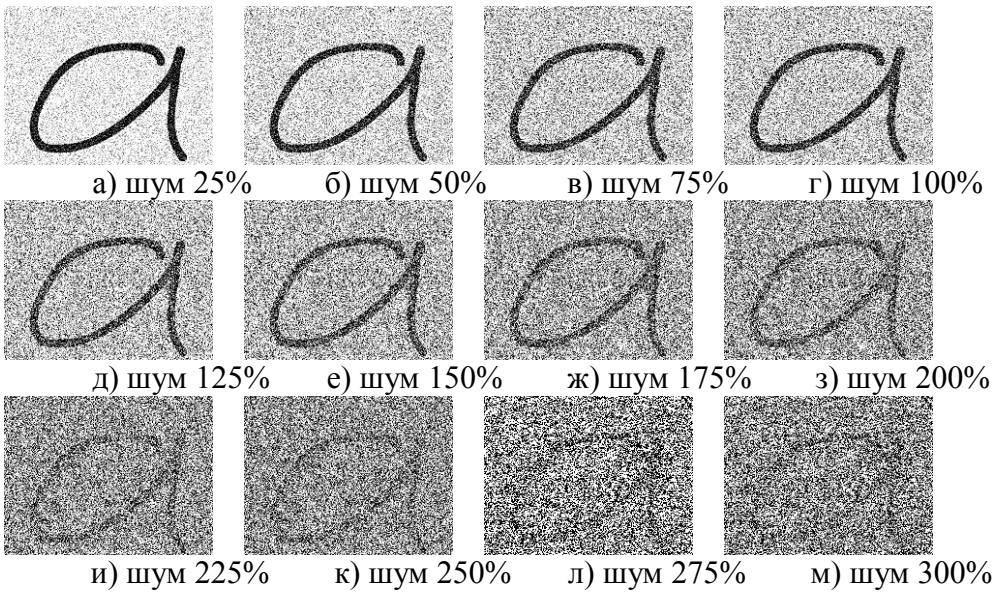


Рис. 35. Зашумленные изображения тестового начертания буквы «*а*» с уровнем шума от 25% до 300%

Как видно из рисунка 35, человек легко распознает образ рукописной буквы «*а*» на уровне шумов от 25% до 100% (верхняя треть рисунка). Более того, этот рукописный символ легко узнается людьми даже при уровне шумов от 125% до 200% (средняя строка образов рисунка 35). При более высоком уровне шумов (третья строка рисунка) людям нужно вглядываться, для того, что бы узнать очертания букв. То есть, люди при большом шуме, переходят в специальный режим «шумоочистки», вглядываясь более пристально в распознаваемое изображение.

То, что люди лучше роботов распознают зашумленные изображения, сегодня используются средствами борьбы с программными роботами. Докажи, что ты не робот, угадай «капчу». Естественно, что для распознавания «капчи» нужен более сложный анализ изображений, чем простое подавление шумов.

Одна нейронная сеть не может выполнять сложные операции, такие как: учет наложения других изображений, нелинейная деформация пространства. Однако, подавлять шумы нейронные сети способны намного эффективнее, чем классические коды, построенные для обнаружения и исправления ошибок. Для определенности будем сравнивать нейронные сети с кодами Боуза-Чоудхуры-Хоквинчхема (БЧХ) [67, 68]. Корректирующая способность кода БЧХ зависит от длины блока, обрабатываемого кодом. На рисунке 36 дана связь относительного значения числа обнаруженных и исправленных ошибок в процентах от избыточной части кода в блоке длиной 512 ошибок.

Из рисунка видно, что классические избыточные коды БЧХ с 50% избыточностью исправляют 5% ошибок. Однако, эти коды оказываются не способны корректировать более 11% ошибок, даже при очень большой избыточности в 3000%.

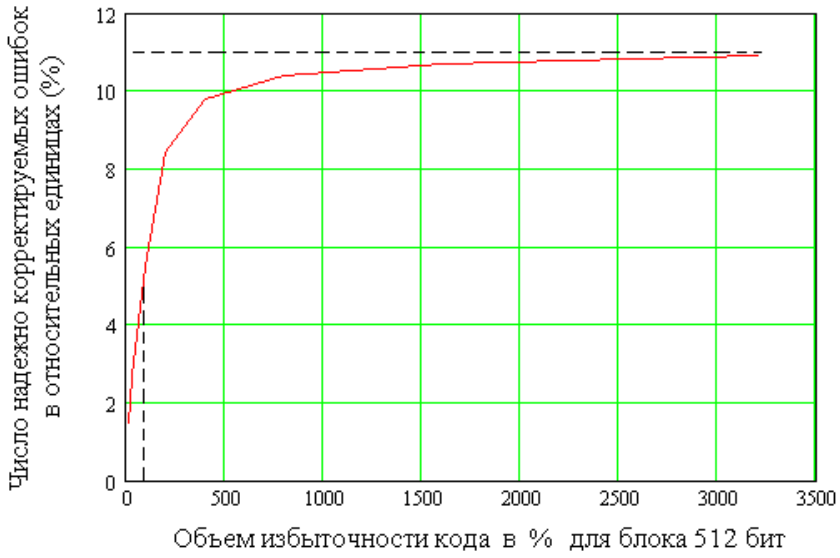


Рис. 36. Связь относительного числа надежно восстанавливаемых ошибок в % и относительного объема избыточной части кода БЧХ

Если мы откажемся от работы только с дискретными состояниями кодов и увеличим объем используемой информации за счет применения сети искусственных нейронов, появляется возможность исправлять большее число ошибок. Для того, что бы показать это будем сравнивать корректирующую способность «нечетких экстракторов» с нейросетевыми преобразователями биометрия-код (рисунок 3, раздел 2).

Настройка порогов «нечетких экстракторов» производится на основании знания статистики допустимых изменений того или иного контролируемого биометрического параметра. В свою очередь, получить статистику параметров можно только опираясь на данные примеров образа «Свой». Если примеров недостаточно, то точно вычислить математическое ожидание и стандартное отклонение мы не можем. Как следствие, мы не можем точно указать пороги области «Свой» для параметра - ν. Эта ситуация отображена на рисунке 37, где приведено распределение данных «Свой» при выборке в 8 примеров и выборке в объеме 1000 примеров. В таблице 7 даны вероятности ошибок первого рода для «нечетких экстракторов», построенных с использованием кодов БЧХ с 20-ти кратной избыточностью.

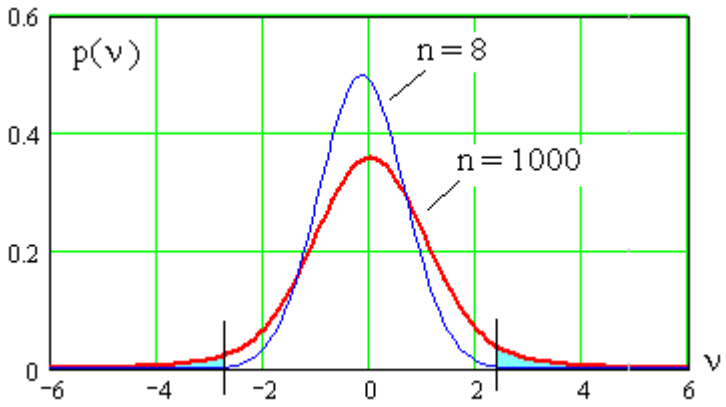


Рис. 37. Пример ошибочно выставленных допустимых границ биометрического параметра из-за малого числа примеров, на которых были вычислены статистические моменты

Таблица №7. Вероятность ошибок первого рода - P_1 для «нечетких экстракторов» и нейросетевых преобразователей биометрия код на разном числе примеров обучения данных образа «Свой»

Число примеров	8	10	12	14	16	18	20	22	24
Нечеткий экстрактор P_1	0.192	0.134	0.093	0.071	0.047	0.038	0.022	0.019	0.016
ИНС h = 0 P_1	0.086	0.079	0.071	0.065	0.052	0.049	0.047	0.044	0.043
ИНС h = 1 P_1	0.039	0.035	0.028	0.026	0.026	0.020	0.018	0.016	0.015

Для читателей, которые захотят проверить данные таблицы 7, сообщаем, что расчеты вероятностей ошибок велись с учетом «тяжелых хвостов» распределения биометрических данных, описываемых смесью двух нормальных законов распределения значений [69]:

$$p(v) = \frac{1}{\sigma(v)\sqrt{2\pi}} \left\{ 0.8 \cdot \exp\left\{ \frac{-\left(E(v)-v\right)^2}{2 \cdot \left(0.8 \cdot \sigma(v)\right)^2} \right\} + 0.2 \cdot \exp\left\{ \frac{-\left(E(v)-v\right)^2}{2 \cdot \left(1.6 \cdot \sigma(v)\right)^2} \right\} \right\} \qquad (51),$$

где $E(v)$ - математическое ожидание биометрического параметра, $\sigma(v)$ - стандартное отклонение биометрического параметра.

Правый и левый пороги сравнения данных выставлялись с учетом наличия «тяжелых хвостов»:

$$\begin{cases} k_L = E(v) - 3.3 \cdot \sigma(v) \\ k_R = E(v) + 3.3 \cdot \sigma(v) \end{cases} \qquad (52).$$

Для того, что бы оценить потенциальные размеры словарей «нечетких экстракторов» и нейросетевых преобразователей биометрия-код, необходимо найти для них распределения расстояний Хемминга.

Распределение значений расстояний Хэмминга приведены на рисунке 33 в нормированной системе координат:

$$\mathrm{h} = \frac{\mathrm{h}}{\max(\mathrm{h})} \qquad (53).$$

Распределение нормированных расстояний Хэмминга для образа «Свой» «нечеткого экстрактора» имеет математическое ожидание $\mathrm{E(h)} = 0.0296$ и стандартное отклонение $\sigma(\mathrm{h}) = 0.0160$.

Для «нечетких экстракторов» образы «Чужие» дают распределение расстояний Хэмминга с математическим ожиданием - $\mathrm{E(h)} = 0.1480$ при стандартном отклонении $\sigma(\mathrm{h}) = 0.0380$. Для решающего правила, обеспечивающего равновероятные ошибки первого и второго рода $\mathrm{P_{EE}} = \mathrm{P_1} = \mathrm{P_2} \approx 0.022$, порог сравнения должен быть задан k=0.08.

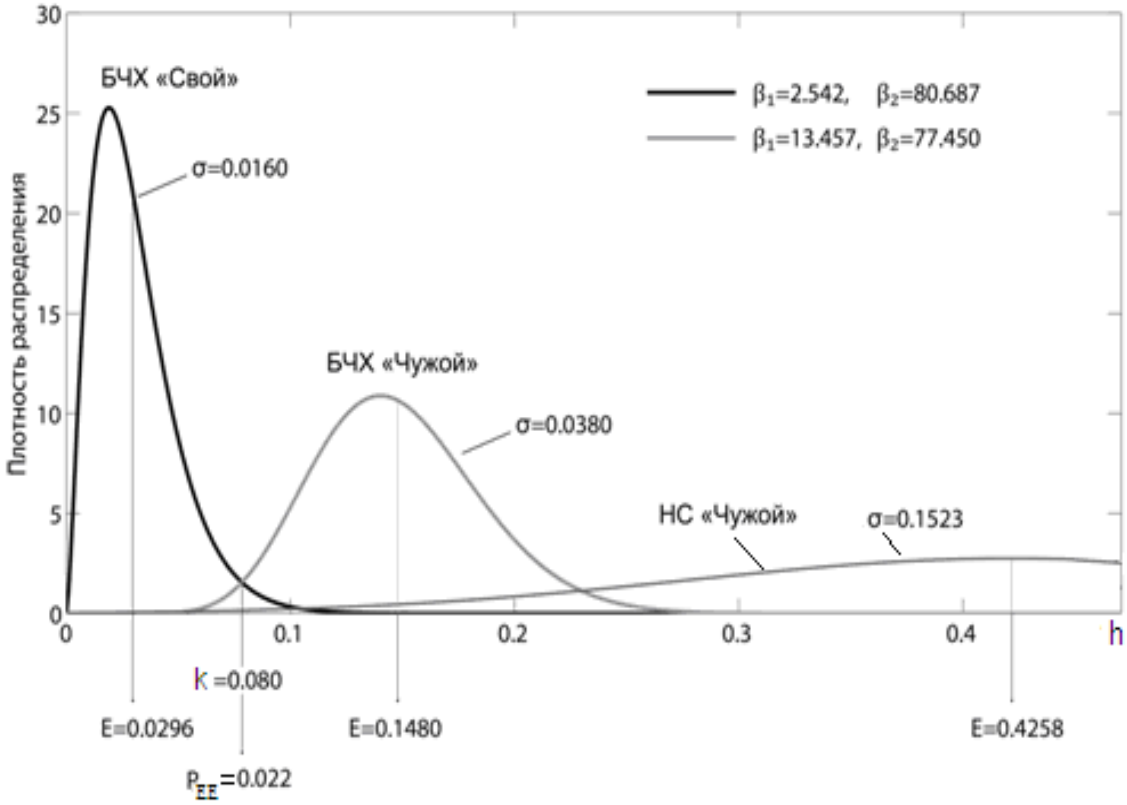


Рис. 38. Распределения расстояний Хэмминга в нормированной системе координат

Эти соотношения позволяют утверждать, что для участвовавшего в численном эксперименте рукописного образа *«Пенза»* (рисунок 5, раздел 3) БЧХ кода с 2-х кратной избыточностью будет вполне достаточно для корректировки большинства ошибок. Однако, при этом примерно 2.2% образов «Чужой» будут приняты как образ «Свой». Последнее означает, что «нечеткий экстрактор» с БЧХ кодом корректировки данных будет способен различать между собой не более 43 рукописных образов из 5 букв (словарь будет иметь не более 43 образов для $P_{EE} \approx 0.022$).

При совершено таких же условиях и том же пороге сравнения k=0 нейросетевой преобразователь биометрия-код среды моделирования «БиоНейроАвтограф» дает вероятность ошибки первого рода $P_1 \approx 0.047$, что хуже, чем обеспечивает «нечеткий экстрактор» для выборки из 20 примеров обучения (таблица 7). Однако, если принять порог k=0.01, то вероятность ошибки значительно улучшается до величины $P_1 \approx 0.018$.

И в том и в другом случае распределение расстояний Хэмминга образов «Чужие» близко к нормальному закону с математическим ожиданием $E(h) = 0.4258$ и стандартным отклонением $\sigma(h) = 0.1523$. Эти параметры нормального закона распределения значений для порога k=1 дают вероятность ошибок второго рода $P_2 \approx 0.0028$.

Если мы установим порог k=0.08 (как это показано на рисунке 38 БЧХ распределений), то вероятность ошибки второго рода составит $P_2 \approx 0.005$ при практически нулевой вероятности ошибок первого рода. Это означает, что для нейросетевых преобразователей биометрия-код словарь должен иметь объем в 200 образов. Это примерно в 4 раза больше, чем аналогичный показатель для «нечетких экстракторов».

Вывод 1. Если при создании средств искусственного интеллекта идти по пути использования «нечетких экстракторов» с классическими БЧХ кодами корректировки ошибок, то мы будем иметь словарь примерно в 4 раза меньше, чем аналогичный словарь у нейросетевых преобразователей. При этом, вероятность ошибочного перепутывания между собой соседних образов у нейронных сетей будет в 4 раза меньше, чем у «нечетких экстракторов».

Расплатой за эти технические преимущества является усложнение вычислительной обработки данных. БЧХ коды - это очень простые конструкции, прекрасно работающие в реальном масштабе времени. Вместо одной программы реализующей БЧХ корректор приходится использовать базу из 200 заранее обученных искусственных нейронных сетей. В первом приближении можно считать, что программная реализация БЧХ корректора и эмулятора одной нейронной сети сопоставимы по их вычислительной сложности. Тогда мы будем иметь примерно 200 кратное усложнение программной реализации нейросетевого корректора ошибок. Для того, что бы снизить затраты вычислительных ресурсов, придется переходить на специальную нечеткую адресацию проверяемых нейронных сетей при поиске в базе нейронных сетей ближайших к предъявленному образу соседей.

Вывод 2. Сегодня БЧХ коды используются для корректировки ошибок в защищенных криптографией каналах связи. Если помеха выросла и БЧХ код не справляется с коррекцией ошибок, то, как дублирующий вариант, может быть использован нейросетевой корректор ошибок. Такой дублер будет работать много медленнее, но он будет способен править гораздо большее число ошибок. Катастрофических потерь информации, когда сообщение нерасшифровывается из-за не исправленных ошибок, будет меньше.

19. Разделение близких образов-соседей с применением двух нейронных сетей

На первом этапе работы нейросетевых корректоров ошибок, необходимо найти образы, близкие к распознаваемому образу. На рисунке 39 приведены примеры двух образов соседей и проекций секущих гиперплоскостей нейронной сети, обученной распознавать образ «Свой».

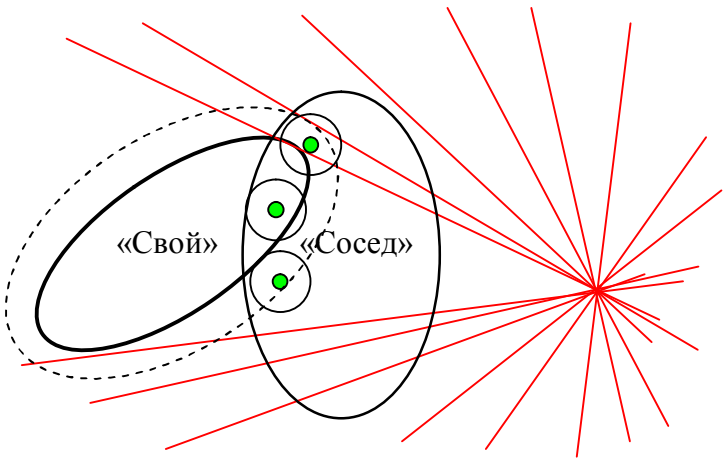


Рис. 39. Два соседних образа, на каждом из которых должна быть обучена своя сеть нейронов

Следует отметить, что после обучения искусственной нейронной сети распознаванию образа «Свой», мы всегда имеем возможность ее протестировать. Для этого достаточно воспользоваться тестовой выборкой примеров «Свой» и «Чужой», не использованных при обучении. На этих выборках могут быть построены соответствующие распределения Хэмминга, как это показано на рисунке 40.

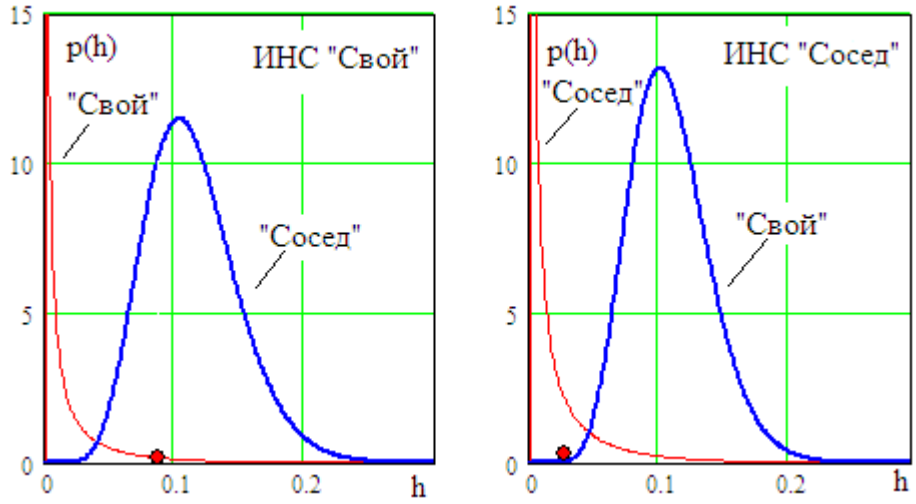


Рис. 40. Два положения одного примера биометрического образа при его двухсторонней проверке с использованием двух разных нейронных сетей

То же самое мы можем сделать для второй нейронной сети, обученной распознавать образ «Сосед». Имея эту априорную информацию, мы можем решить к какому из двух образов с наибольшей вероятностью принадлежит проверяемый образ. На рисунке 35 проверяемый образ отображен точкой. Тривиальным решением этой задачи является ситуация, отображенная в правой части рисунка 40, где проверяемая точка оказалась вне интервала данных «Свой».

Получается, что для принятия решения необходимо анализировать положение проверяемого образа в двух системах отсчета расстояний Хэмминга. Можно выбирать ту систему, где результат является наиболее очевидным. Либо следует принимать решения, учитывая положение проверяемого образа в обоих системах [70]. Использование принятия решений по двум нейронным сетям теоретически может повысить качество в $\sqrt{2}$ раз. По индукции можно предположить, что принятие решений с учетом 3, 4, 5 ближайших соседей так же возможен, однако, оценить рост качества итогового решения по нескольким нейронным сетям затруднительно. Тем не менее, факт остается фактом. Принятие решения с учетом группы нейронных сетей, окружающих исследуемый образ всегда точнее, чем принятие решения по результатам работы одной нейронной сети.

Тот факт, что каждая искусственная нейронная сеть через ее тестирование получает свое статистическое описание в виде распределений расстояний Хэмминга (рис. 40), является важным технологическим преимуществом перед людьми-экспертами. Люди-эксперты, анализируя рукописные образы, не могут оценить значения вероятности ошибок своих решений. Автоматизированные экспертные системы анализа подлинности автографов [71, 72, 73] дают не только решение, но и оценку вероятности его возможных ошибок.

Вывод. Коллектив нейронных сетей, окружающий нейронную сеть образа «Свой» работает намного эффективнее, чем одна нейронная сеть. Видимо, это одна из причин высокой эффективности распознавания образов людьми. Нейронные сети сами по себе статичны, однако, если заставить их уточнять решение, то возникает динамика (нужно просматривать окрестности данных), а так же нужно просматривать то, как на эти данные будут откликаться соседние нейронные сети. Именно по этой причине у человека мозг находится в постоянной активности, судить о которой мы можем по электроэнцефалограмме.

20. Циклический континуально-квантовый усилитель мощности хи-квадрат критерия

Для людей крайне важным является быстрая оценка рисков появления тех или иных событий. Когда люди обучены распознавать сложные статистические образы, они принимают решения по очень малым тестовым выборкам. Иначе обстоит дело со стандартными процедурами проверки статистических гипотез по критерию хи-квадрат [35, 36]. Хи-квадрат критерий традиционно считается ориентированным на большие тестовые выборки, состоящие из 200 примеров и более.

Покажем, что столь большие тестовые выборки могут быть значительно уменьшены, если принять меры по сглаживанию шумов квантования, возникающих из-за малого объема тестовой выборки. Пример ошибки квантования, возникающей при формировании гистограммы, приведен в верхней части рисунка 41.

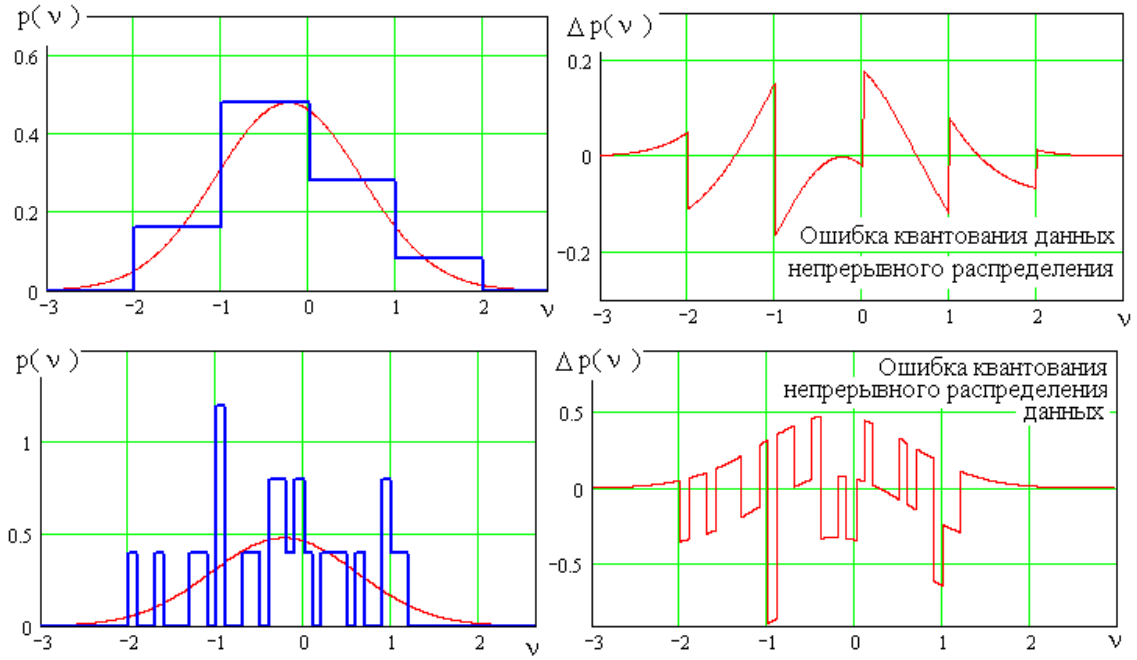


Рис. 41. Использование 10-ти кратного сужения интервалов гистограммы, приводит к росту ошибки квантования

Мощность хи-квадрат критерия зависит от числа степеней свободы - m. Обычно, показатель числа степеней свободы выбирают по следующей формуле:

$$m = k - 3 \qquad (54),$$

где k- число столбцов гистограммы.

В этом случае плотность распределения хи-квадрат критерия по Пирсону описывается следующим соотношением.

$$p(\chi^2, m) = \left\{ \frac{1}{2^{\frac{m}{2}} \cdot \Gamma\left(\frac{m}{2}\right)} \left\{ x^{\frac{m}{2}-1} \cdot \exp\left(\frac{-x}{2}\right) \right\} \right\}, \qquad (55)$$

Попытаемся увеличить в 10 раз число степеней свободы (число столбцов гистограммы). Технически это выполнимо, однако, при этом появляется много

пустых столбцов гистограммы (смотри нижнюю часть рисунка 41) и вырастает шум ошибки квантования.

Уменьшить амплитуду шума квантования и заполнить пустые интервалы столбцов гистограммы удается, если запустить сглаживающий цифровой фильтр [74, 75, 76]. Эта процедура приводит к появлению еще одной модификации хи-кавадрат критерия со сглаживающим шумы квантования линейным усредняющим фильтром по скользящему окну с нечетным числом отсчетов. Программная реализация такого фильтра для окна сглаживания в 9 отсчетов занимает две строки в среде математического моделирования MatCAD:

$$\begin{cases} i := 4,\ldots,(last(g)-4); \\ g1_i := \dfrac{g_{i-4}+g_{i-3}+g_{i-2}+g_{i-1}+g_{i-0}+g_{i+1}+g_{i+2}+g_{i+3}+g_{i+4}}{9}. \end{cases} \qquad (56),$$

где g_i - отсчеты гистограммы со слишком узкими столбцами, $g1_i$ - выходные отсчеты сглаживающего данные фильтра. Результаты работы сглаживающего фильтра приведены на рисунке 42.

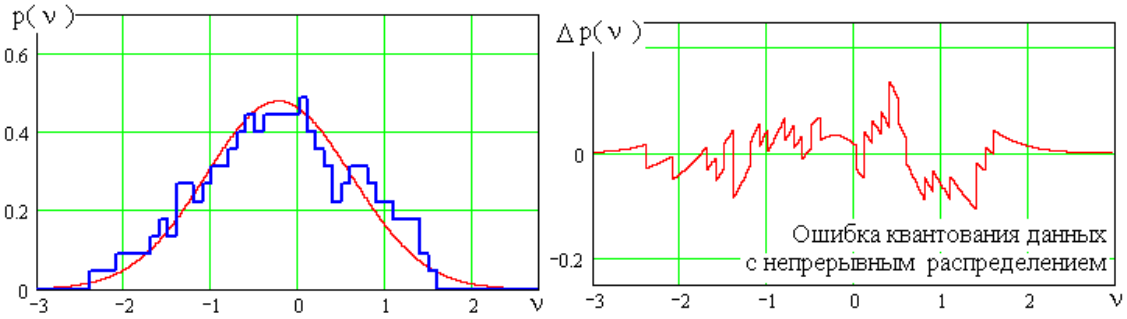


Рис. 42. Результат работы сглаживающего фильтра с окном усреднения 9 отсчетов

Как видно из рисунка 42, после сглаживания данных, пустые столбцы гистограммы практически исчезают, значительно снижается амплитуда шума квантования. По этой причине сглаженный хи-квадрат критерий работает с данными, распределенными примерно по 60 столбцам гистограммы рисунка 42, вместо всего 4 столбцов гистограммы рисунка 41 .

Увеличение числа столбцов гистограммы примерно в 10 раз приводит к тому, что существенно падает вероятность ошибок сглаженного хи-квадрат критерия на малых тестовых выборках. На рисунке 43, отображены функции понижения равновероятных ошибок в логарифмической шкале для обычных гистограмм, состоящих из 6 столбцов и сглаженных гистограмм, имеющих примерно 60 не пустых столбцов (рисунок 42).

Из рисунка 43 следует, что мощность хи-квадрат критерия со сглаживанием при выборке в 30 примеров, оказывается примерно в 22 раза выше, чем тот же критерий дает без сглаживания. То есть, при 30 примерах сглаженного хи-квадрат критерия вероятности ошибок P_{EE} будут такими же, как при 660 примерах обычного хи-квадрат критерия без сглаживания. Таким образом, сглаживая данные цифровым фильтром (47), мы получили весьма и весьма эффективный усилитель мощности хи-квадрат критерия.

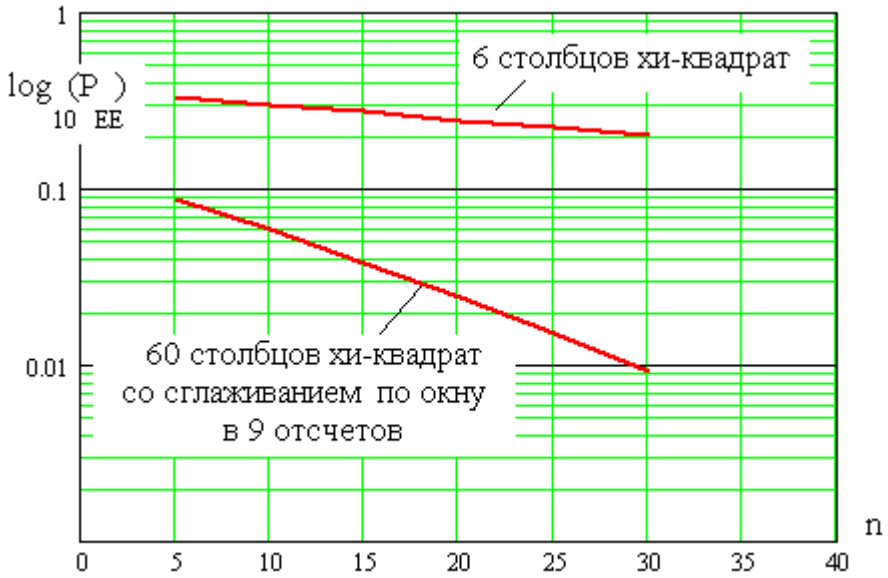


Рис. 43. Мощность хи-квадрат критерия в логарифмической шкале равновероятных ошибок

Приведенные на рисунке 43 линии снижения равновероятных ошибок, были получены средствами имитационного моделирования. Были использованы генератор с нормальным и генератор с равномерным законом распределения значений. Получая от таких генераторов 1 000 000 выборок по 16 отсчетов, мы можем для каждой выборки построить гистограмму из 6 столбцов с равными интервалами - Δx. При этом, ширину столбцов гистограммы будем выбирать следующим образом:

$$\Delta x = \frac{\max(x) - \min(x)}{6} \qquad (57).$$

Тогда край первого левого столбца гистограммы всегда будет совпадать с минимальным значением - min(x) в каждой выборке, а правый край последнего столбца всегда будет совпадать с максимальным значением в выборке – max(x). Получившиеся при таком численном эксперименте функции распределения значений отображены на рисунке 44.

Для нас принципиально важным является то, что при синтезе данных, приведенных на рисунке 44, их синхронизация производится только по отношению к минимальному значению в тестовой выборке. Математическое ожидание данных в тестовой выборке и стандартное отклонение данных в тестовой выборке никак не связано с положением интервалов, на которых строится гистограмма.

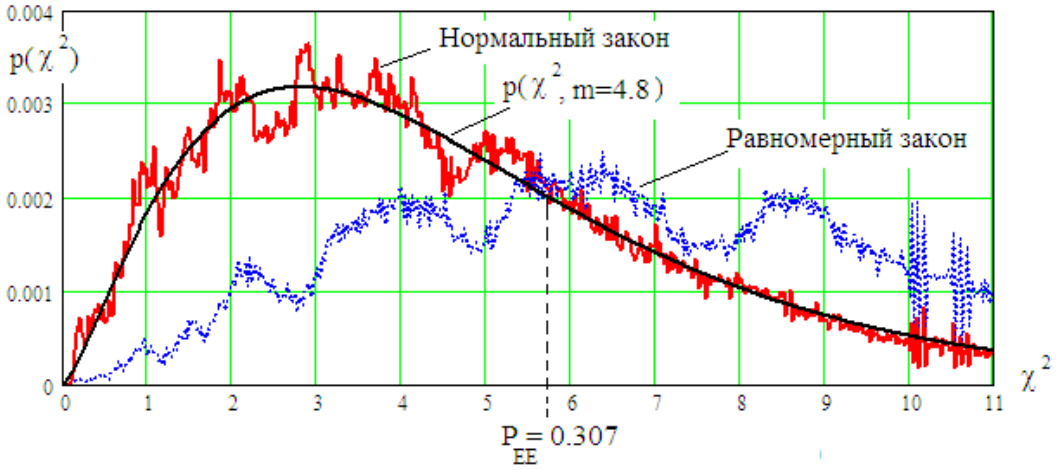


Рис. 44. Плотности распределения значений хи-квадрат критерия Пирсона, получившиеся в результате численного эксперимента для выборок из 16 примеров и гистограмм, состоящих из 6 столбцов без сглаживания

Из рисунка 44 видно, что данные имеют существенную случайную составляющую, которую экспериментаторы ошибочно рассматривали, как следствие ограниченного объема численного эксперимента в 1 000 000 повторений. То, что причина не эта, легко проверить. Достаточно в 100 раз увеличить число повторений. При этом, амплитуда колебательная составляющей должна уменьшиться в 10 раз, а гладкая составляющая $p(\chi^2, m = 4.8)$ должна сохраниться. Этого не происходит, рост размеров выборки практически не меняет вид функции распределения значений.

Еще одним важным фактом является появление дефекта размерности детерминированной составляющей плотности распределения значений -Δm. Шесть столбцов гистограммы должны давать (m=6-3=3) три степени свободы в выражении (55). Дефект размерности данных рисунка 44 составляет Δm=4.8-3=1.8.

Причиной дефекта числа степеней свободы является то, что на малых выборках хи-квадрат критерий имеет дискретный спектр конечного числа состояний. На это ранее никто не обращал внимание из-за того, что хи-квадрат считался непригодным для малых выборок. Для того, чтобы убедиться в дискретности спектра, необходимо осуществить синхронизацию столбцов гистограммы и математического ожидания данных в тестовой выборке. Для этой цели ширину столбцов гистограммы будем выбирать пропорционально стандартному отклонению:

$$\Delta x = \sigma(x) \qquad (58).$$

Положение столбцов гистограммы будем привязывать к промежутку между третьим и четвертым столбцами [69, 70, 71]:

$$\max(\Delta x_3) = \min(\Delta x_4) = E(x) \qquad (59).$$

Выполнение условий (58) и (59) приводит к превращению непрерывного спектра (смотри рисунок 53) в дискретный спектр, приведенный на рисунке 45.

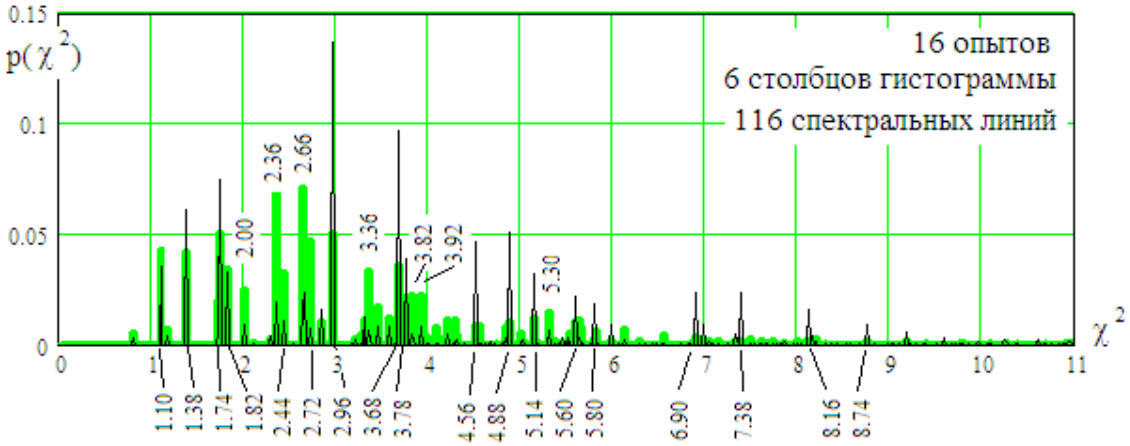


Рис. 45. Дискретный выходной спектр «молекулы Пирсона», имеющий 116 спектральных линий в интервале значений от 0 до 11

После того, как мы перешли от привычного всем непрерывного спектра состояний хи-квадрат критерия к его дискретному отображению, мы имеем право рассматривать уравнения распределения Пирсона (46) и квантователь Пирсона (таблица №2 строка 1), как некоторый эквивалент уравнению Шредингера. И уравнение Пирсона и уравнение Шредингера описывают континуально-квантовые эффекты, которые могут быть использованы для создания континуально-квантовых вычислительных машин. В такой постановке задачи можно говорить о «молекуле Пирсона» [77, 78, 79], порождающей спектр уникальных выходных состояний.

Следует подчеркнуть, что положение пиков выходного спектра состояний «молекулы Пирсона» целиком и полностью определяется настройкой параметров квантователя. Изменение плотности распределения входных континуумов не приводит к изменению положений спектральных линий, они только меняют свою интенсивность. Причем изменение интенсивности спектральных линий может быть «положительным» (усиливать разницу интегральных спектров рисунка 39). Так же возможно «отрицательное» соотношение одинаковых по значению спектральных компонент (уменьшать разницу интегральных спектров).

Из рисунка 45 видно, что спектральные компоненты χ^2={2.00, 2.36, 2.44, 2.66, 2.72, …} имеют большую высоту для нормального закона распределения значений (толстые линии). Рядом с этими состояниями спектра находятся противоположные состояния χ^2={1.38, 1.74, 2.96, 3.68, 3.78, …}. Для этих состояний амплитуда компонент спектра оказывается выше, если внутренний континуум имеет равномерный закон распределения значений (тонкие линии). Так же присутствуют «нейтральные» компоненты спектра χ^2={1.10, 1.82, 2.90, …}, для которых высота столбцов толстых и тонких линий примерно одинакова. Эта группа компонент обладает почти нулевой информативностью, опираясь на эти спектральные составляющие нельзя идентифицировать вид закона распределения значений.

Первую группу спектральных линий χ^2={2.00, 2.36, 2.44, 2.66, 2.72, …} следует рассматривать, как группу линий с «положительной» информативностью, а вторую группу χ^2={1.38, 1.74, 2.96, 3.68, 3.78, …} следует рассматривать, как группу с «отрицательной» информативностью. Интегрирование вероятностей по группе с «положительной» информативностью и «отрицательной» информативностью приводит к ухудшению ситуации (растет вероятность ошибок P_{EE} до величины 0.307). Спектральные составляющие с «положительной» и «отрицательной» информативностями подавляют друг друга при их

интегрировании. Для существенного усиления мощности интегрального варианта хи-квадрат критерия ($P_{EE} << 0.307$), необходимо отдельно интегрировать компоненты спектра с «отрицательной» и «положительной» информативностью. Формально это можно сделать путем обучения двух искусственных нейронных сетей распознаванию спектра нормального закона первой нейронной сетью и спектра равномерного закона распределения второй сетью нейронов.

Спектральный анализ на сегодняшний день является важнейшим инструментом идентификации веществ, присутствующих в пробах в микроскопических объемах. Пользуясь спектральным анализом, криминалисты способны доказать, что на весах взвешивали криминальный золотой песок. Достаточно смочить ватку спиртом, протереть ею чашу весов, затем сжечь ватку и сфотографировать спектр пламени, горящей ваты. Наличие спектральных линий золота однозначно укажет на факт его микроскопического присутствия.

Этот пример интересен тем, что для того, что бы заставить говорить «котов Шредингера» сделанных из золота, пришлось их сжечь. Мало заставить работать тот или иной континуально-квантовый вычислитель, необходимо обеспечить его достаточно длительную работу (обеспечить необходимое время синхронной работы молекул вычислителя) и иметь надежный механизм считывания результата вычислений.

Для машины Пирсона необходимо обеспечить возможность ее циклической работы. Если мы имеем выборку из 16 примеров и осуществляем вычисления по формуле Пирсона (таблица 2 первая линия), то получаем результат с равными вероятностями ошибок $P_1=P_2=P_{EE}=0.307$ (смотри рисунок 39) при пороге принятия решений $\chi^2 = 5.75$.

Если бы у нас было очень много данных, например, 16 независимых выборок по 16 примеров (всего 256 опытов), то мы получили бы очень маленькую вероятность ошибок:

$$P_1=P_2=P_{EE}=(0.307)^{16}\approx 0.0000000062 \qquad (60).$$

К сожалению, добиться этого нельзя, если имеется выборка, состоящая всего из 21 опыта. Тем не менее, мы можем осуществить 20 349 не повторяющихся внутренних малых выборок по 16 опытов из исходной большой выборки в 21 опыт. В это число войдут сильно коррелированные выборки, различающиеся между собой всего 1, 2, 3, …, 6 опытами. Их число составит:

$$C_{16}^1 + C_{16}^2 + ... + C_{16}^6 = 14\ 892.$$

То есть, мы имеем остаток 20 349-14 892=5 475 выборок по 16 опытов с относительно низкой взаимной корреляцией данных. Если бы корреляция была нулевой, то вероятность ошибок стала бы астрономически малой величиной $(0.307)^{5475}$. Однако, наличие остаточных корреляционных связей данных в 5 475 выборках, не позволяет добиться столь малых величин вероятности ошибок. Тем не менее, циклический 5 475 кратный запуск континуально-квантовой машины Пирсона предположительно должен позволить увеличить мощность хи-квадрат критерия от 300 до 3000 раз.

Вывод. Одной из загадок наших с вами интеллектуальных возможностей является то, как работают люди-эксперты. Они делают верные выводы по малым объемам очень «плохих» данных. Кажется, что обыкновенная статистика никогда не сможет давать сопоставимые результаты с человеком-экспертом. Выше я попытался показать, что резервы классической статистики далеко не исчерпаны. Переходя к учету дискретных состояний спектра хи-квадрат критерия, можно значительно увеличить мощности этого статистического критерия. Мне кажется, что человек-эксперт глубоко анализирует ситуацию примерно таким же образом. Сколько возможных состояний при этом он учитывает, зависит от его знаний (от его квалификации). У наших естественных мозгов есть возможность при

необходимости раздельно исследовать наиболее информативные спектральные составляющие, заранее зная, какая из них имеет «положительную» и какая имеет «отрицательную» информативность.

21. Общие положения создания многомерных вычислителей, использующих суперпозиции квантовых состояний выходов искусственных нейронов

21.1. Наблюдение суперпозиции квантовых состояний отдельных бинарных нейронов (одного кубита)

Параметры биометрического образа, после их вычисления оказываются статичными, квантователи каждого нейрона так же являются статическими элементами. Это специфика нейросетевых преобразователей биометрия-код. В этом отношении классические модели квантовой механики (квантовой вычислительной техники) противоположны нейросетевым преобразователям.

У нейронных сетей легко наблюдаемы континуумы входных данных, параметры обогащающих функционалов и параметры квантователей. При этом, оказываются недоступны для наблюдения континуумы выходных квантовых состояний каждого из нейронов. Однако, как было показано в предыдущих разделах, наблюдать континуумы квантовых состояний (кубиты) и даже спектры псевдо-молекул технически возможно.

Для полноценных квантовых вычислителей все по другому. У настоящих молекул и квантовых вычислительных элементов нельзя наблюдать континуумы (их можно только вычислить), нельзя наблюдать параметры квантователей (их можно только вычислить), нельзя наблюдать суперпозицию квантовых состояний, но можно наблюдать выходные спектры (излучения или поглощения).

Будем рассматривать обученную ИНС, как искусственную статическую псевдо-молекулу, у которой видны ее выходные квантовые состояния. Будем исходить из того, что статические состояния этой молекулы при температуре абсолютного нуля ($T=0.0^0$) определяются вектором входных континуальных биометрических параметров $\bar{\nu}$ образа «Свой» (вектором входных континуальных биометрических параметров $\bar{\xi}$ образа «Чужой») и таблицами настройки ИНС.

В этом случае, статическое воздействие вектором $\bar{\nu}$ на ИНС молекулу дает статическое выходное квантовое состояние "$\bar{c}$". Другое статическое воздействие вектором $\bar{\xi}$ на ИНС молекулу дает статическое выходное квантовое состояние "$\bar{x}$". В статике различить коды "$\bar{c}$" и"$\bar{x}$" можно только сравнивая их со статическим эталоном по расстоянию Хэмминга (формула (15), раздел 8).

Для того, что бы наблюдать динамику состояний выходных кодов (континуумы квантовых состояний) необходимо увеличить температуру искусственной ИНС молекулы до 10% от нормальной температуры, когда шумы биометрических данных станут естественными (будут иметь естественные стандартные отклонения $\sigma(\nu_i)$ и $\sigma(\xi_i)$).

Если мы подадим на входы ИНС молекулы смесь биометрических параметров - $\bar{\nu}$ с 10% шумом от естественного, состояния выходных кодов мало изменятся. В силу того, что ИНС молекула стабилизирует данные примеров «Свой», мы получим почти стабильные квантовые суперпозиции. В обозначениях, используемых при описании квантовых вычислителей [4], это можно записать следующим образом:

$$\left|\psi(\nu)\right\rangle = \mu_0 \cdot \left|0\right\rangle + \mu_1 \cdot \left|1\right\rangle \qquad (61),$$

где $\left|...\right\rangle$ - скобки Дирака.

Очевидно, что сумма вероятностей выходных состояний нейрона единична:

$$P(|\psi(\nu)\rangle) = P(|0\rangle) + P(|1\rangle) = 1 = P("0") + P("1") = 1 \qquad (62).$$

При этом, вероятности состояний будут определяться через коэффициенты квантовой суперпозиции следующим образом:

$$P(|0\rangle) = P("0") = \frac{\mu_0}{\sqrt{\mu_0^2 + \mu_1^2}}, \qquad (63)$$

$$P(|1\rangle) = P("1") = \frac{\mu_1}{\sqrt{\mu_0^2 + \mu_1^2}} \qquad (64).$$

В случае использования входных данных образа «Свой» размытых слабым шумом, мы будем иметь одну из двух стабильных ситуаций:

$$\begin{cases} P(|0\rangle) = P("0") \approx 0.99, \\ P(|1\rangle) = P("1") \approx 0.01 \end{cases} \qquad (65) \quad \text{или} \quad \begin{cases} P(|0\rangle) = P("0") \approx 0.01, \\ P(|1\rangle) = P("1") \approx 0.99 \end{cases} \qquad (66).$$

Выходное состояние с высокой вероятностью будет нулевым (65) или единичным, (66) в зависимости от того, какое состояние разряда должен выдавать обученный нейрон.

Положение меняется, если на вход ИНС молекулы подать зашумленные данные примера образа «Чужой». Для функции квантовой суперпозиции $|\psi(\xi)\rangle$ соотношения (61), (62), (63), (64) остаются прежними. Изменяется только значения соотношений между вероятностями состояний:

$$P(|0\rangle) = P("0") \approx P(|1\rangle) = P("1") \approx 0.5 \qquad (67).$$

В теории квантовых вычислений симметричные состояния (67) играют особую роль и имеют особое обозначение:

$$|\psi(\xi)\rangle \approx \frac{1}{\sqrt{2}} \cdot |0\rangle + \frac{1}{\sqrt{2}} \cdot |1\rangle \approx |+\rangle \qquad (68).$$

В нейросетевой биометрии наличие квантовой суперпозиции $|\psi(\xi)\rangle \approx |+\rangle$ так же играет особую роль, более того, наличие такой квантовой суперпозиции для каждого выхода нейронной сети требует базовый национальный стандарт ГОСТ Р 52633.0 [80].

21.2. Наблюдение суперпозиции квантовых состояний двух и более бинарных нейронов (двух и более кубит)

Все, что написано выше характерно для любого из 256 выходов нейросетевого преобразователя биометрия-код, если же мы будем рассматривать любую пару выходных разрядов преобразователя, то мы получим квантовую суперпозицию пары кубит:

$$\begin{cases} |\psi(\nu)\rangle = \mu_{00}|00\rangle + \mu_{01}|01\rangle + \mu_{10}|10\rangle + \mu_{11}|11\rangle \\ |\psi(\xi)\rangle = \mu_{00}|00\rangle + \mu_{01}|01\rangle + \mu_{10}|10\rangle + \mu_{11}|11\rangle \end{cases} \qquad (69).$$

Вероятность появления каждого из двух кубит описывается по аналогии с соотношениями (54), (55):

$$\begin{cases} P(|00\rangle) = P("00") = \dfrac{\mu_{00}}{\sqrt{\mu_{00}^2+\mu_{01}^2+\mu_{10}^2+\mu_{11}^2}} \\ P(|01\rangle) = P("01") = \dfrac{\mu_{01}}{\sqrt{\mu_{00}^2+\mu_{01}^2+\mu_{10}^2+\mu_{11}^2}} \\ \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \end{cases} \qquad (70).$$

При этом, квантовая суперпозиция данных образа «Свой» является практически вырожденной, ее значение практически совпадает с заданными при обучении разрядами кода "$\overline{c}$". Например:

$$|\psi(\nu)\rangle \approx |00\rangle \quad \text{if} \quad \{\mu_{00} \approx 1, \mu_{01} \approx \mu_{10} \approx \mu_{11} \approx 0\} \qquad (71).$$

Для данных образов все «Чужие» характерна иная ситуация:

$$|\psi(\xi)\rangle \approx |++\rangle \quad \text{if} \quad \left\{\mu_{00} \approx \mu_{01} \approx \mu_{10} \approx \mu_{11} \approx \frac{1}{2}\right\} \qquad (72).$$

Получается, что квантовые суперпозиции выходных состояний двух нейронов достаточно просто описываются как для данных «Свой», так и для данных все «Чужие». Положение не меняется, если мы увеличим число нейронов в рассматриваемой группе.

В общем случае, когда мы будем рассматривать группу из m нейронов, мы получим почти детерминированное соотношение:

$$|\psi(\nu)\rangle \approx |10...1\rangle \quad \text{if} \quad \{\mu_{10..1} \approx 1, \text{а все иные } \mu \approx 0\} \qquad (73).$$

Для данных образов все «Чужие» сохранится равная вероятность всех кодовых состояний:

$$|\psi(\xi)\rangle \approx |++...+\rangle \quad \text{if} \quad \left\{\mu_{00...0} \approx \mu_{00...1} \approx \mu_{0...10} \approx .... \approx \mu_{11...1} \approx \frac{1}{\left(\sqrt{2}\right)^m}\right\} \qquad (74).$$

Важным обстоятельством является то, что весовые коэффициенты квантовой суперпозиции жестко связаны с вероятностью появления того или иного кодового состояния:

$$\begin{cases} |\psi(.)\rangle = \mu_{00...0}\cdot|00..0\rangle + \mu_{00...1}\cdot|00..1\rangle + ... + \mu_{11...1}\cdot|11..1\rangle \equiv \\ \equiv \sqrt{P(|00...0\rangle)}\cdot|00..0\rangle + \sqrt{P(|00...1\rangle)}\cdot|00..1\rangle + ... + \sqrt{P(|11...1\rangle)}\cdot|11..1\rangle \end{cases} \qquad (75).$$

Знание вероятности появления того или иного кодового состояния в квантовой суперпозиции, эквивалентно знанию весовых коэффициентов квантовой суперпозиции.

21.3. Наблюдение запутанности (коррелированности) состояний квантовой суперпозиции двух и более бинарных нейронов (двух и более кубит)

Кроме вероятностного описания суперпозиции квантовых состояний в биометрии широко используется корреляционное описание выходных кодовых состояний. Для двух разрядов выходного кода с номерами i, j корреляция может быть получена накоплением данных:

$$r(|x_i\rangle, |x_j\rangle) = \frac{1}{N}\left\{\sum_{k=1}^{N} |x_{i,k}\rangle \oplus |x_{j,k}\rangle\right\} - \frac{1}{N}\left\{\sum_{k=1}^{N} |x_{i,k}\rangle \oplus |\neg x_{j,k}\rangle\right\} \qquad (76).$$

По аналогии может быть вычислена корреляционная связь между разными парами разрядов кода, описываемого континуумом квантовых состояний:

$$r(|x_i, x_{i+1}\rangle, |x_j, x_{j+1}\rangle) = \frac{1}{N}\left\{\sum_{k=1}^{N}\left(|x_{i,k}\rangle \oplus |x_{j,k}\rangle\right)\oplus\left(|x_{i+1,k}\rangle \oplus |x_{j+1,k}\rangle\right)\right\} - \\ -\frac{1}{N}\left\{\sum_{k=1}^{N}\left(|x_{i,k}\rangle \oplus |\neg x_{j,k}\rangle\right)\oplus\left(|x_{i+1,k}\rangle \oplus |\neg x_{j+1,k}\rangle\right)\right\} \quad (77).$$

Данные континуумов квантовых состояний кардинально отличаются по показателям коррелированности разрядов. Для данных образов «Свой» модули коэффициентов парных и групповых корреляций оказываются близки к единице:

$$\left|r\left(|c_i\rangle, |c_j\rangle\right)\right| \approx \left|r\left(|c_i, c_{i+1}\rangle, |c_j, c_{j+1}\rangle\right)\right| \approx 1 \quad (78).$$

Очевидно, что усреднение данных по разным значениям индексов не меняет ситуацию:

$$E\left(\left|r\left(|c_i\rangle, |c_j\rangle\right)\right|\right) \approx E\left(\left|r\left(|c_i, c_{i+1}\rangle, |c_j, c_{j+1}\rangle\right)\right|\right) \approx 1 \quad (79).$$

Для биометрических данных все «Чужие» модули корреляционных связей значительно уменьшаются:

$$1 > \left|r\left(|x_i\rangle, |x_j\rangle\right)\right| \geq \left|r\left(|x_i, x_{i+1}\rangle, |x_j, x_{j+1}\rangle\right)\right| \quad (80).$$

Усреднение модулей коэффициентов корреляции соотношений не меняет:

$$1 > 0.3 \geq E\left(\left|r\left(|x_i\rangle, |x_j\rangle\right)\right|\right) \geq E\left(\left|r\left(|x_i, x_{i+1}\rangle, |x_j, x_{j+1}\rangle\right)\right| \geq 0\right) \quad (82).$$

Реальные биометрические данные не могут иметь нулевые корреляционные связи. На практике добиться нулевых корреляционных связей удается только шифрованием данных.

Запутанность (классическая коррелированность) разрядов квантовой суперпозиции выходных кодов присутствует как в самих биометрических образах все «Чужие», так и создается в нейронной сети преобразователя биометрия-код. В частности она возникает из-за того, что каждый нейрон имеет несколько одинаковых входов с другими нейронами.

Эта ситуация отображена на рисунке 46, где два нейрона используют один и тот же входной биометрический параметр №29 по нумерации входных биометрических данных.

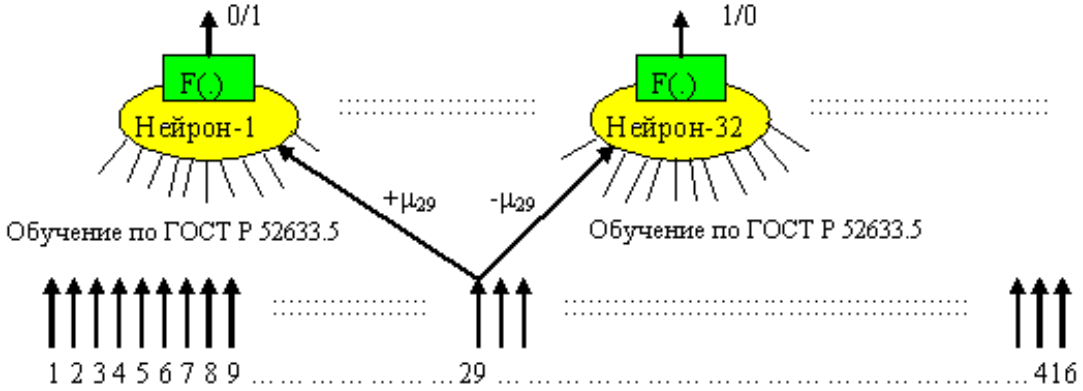


Рис. 46. Запутанность (коррелированность) выходных состояний нейронов, обусловленная общими входными связями нейронов

Как видно из рисунка 46 весовые коэффициенты нейрона №1 и нейрона № 32 одинаковы по модулю (они вычисляются по одному алгоритму ГОСТ Р 52633.5), но имеют разные знаки из-за программирования их на разные выходные кодовые состояния. Даже в том случае, если на входы нейронов будут поданы полностью независимые данные, данные нейронов №1 и №32, будут обязательно отрицательно коррелированны.

Запутанность или коррелированность разрядов квантовой суперпозиции Г.Б. Моршалко рассматривает как уязвимость, им была построена специализированная атака по уменьшению структурной неопределенности нейросетевых преобразователей биометрия-код [81].

21.4. Наблюдение энтропии суперпозиции квантовых состояний двух и более бинарных нейронов (двух и более кубит)

Очевидно, что высокий уровень корреляционных связей квантовых континуумов биометрических кодов приводит к практически нулевой энтропии для образа «Свой». Существенно большей оказывается энтропия квантовых континуумов кодов «Чужой» длиной - m. Без учета природы получения квантовых континуумов их энтропия вычисляется следующим образом:

$$H_m\left(\left|\psi(.)\right\rangle\right) = -\sum_{i=1}^{2^m} (\mu_i)^2 \cdot \log_2((\mu_i)^2) \qquad (82).$$

Формула (73) является аналогом формулы Шеннона, ею можно воспользоваться только для коротких квантовых континуумов. Для длинных последовательностей приходится использовать слишком много исходных данных. Можно снизить требования к размерам тестовой выборки и использовать относительно короткие последовательности длинной – k. В этом случае, энтропию для последовательностей с длиной кода-m можно оценить следующим образом:

$$H_m\left(\left|\psi(v)\right\rangle\right) \approx \frac{m}{m-k} \cdot E(H_k\left(\left|\psi(v)\right\rangle\right)) \qquad (83).$$

$$H_m\left(\left|\psi(\xi)\right\rangle\right) \approx \frac{m}{m-k} \cdot E(H_k\left(\left|\psi(\xi)\right\rangle\right) \qquad (84).$$

Показатель –k выбирается исходя из объема имеющихся данных. Соотношения (74), (75), фактически являются линейной интерполяцией более сложной зависимости. С ростом разницы между m и k ошибка приближения монотонно увеличивается, для ее компенсации требуется использование более сложных процедур предсказания [82, 83].

21.5. Наблюдение распределений расстояний Хэмминга суперпозиции квантовых состояний длинных кодов с зависимыми разрядами при разных температурах

В квантовой механике уравнений Шредингера [2] и в квантовой информатике [3], построенной на уравнениях Шредингера метрика расстояний Хэмминга не используется. Это связано с тем, что выходные состояния квантователя континуумов в микросистемах не удается наблюдать (наблюдается только производная состояний – спектр поглощения или излучения).

В этом отношении нейросетевые континуально-квантовые преобразования удачно дополняют уже созданные математические конструкции. Для нейросетевых преобразователей биометрия-код метрика расстояний Хэмминга между кодами «Свой» и кодами «Чужой» легко вычислима:

$$h = \sum_{i=1}^{m} \left|x_i\right\rangle \oplus \left|c_i\right\rangle \qquad (85).$$

Свертывание квантовой суперпозиции кодов $\left|\psi(\xi)\right\rangle$ с практически стабильным кодом $\left|\bar{c}\right\rangle$ (76) позволяет получить функцию вероятности появления разных значений расстояний Хэмминга - $P(h)$. От этой функции вероятности -

P(h) мы можем перейти к ее производной или к плотности вероятности распределения значений - p(h). В свою очередь, плотность вероятности распределения значений - p(h) играет важную роль в быстрых расчетах вероятности ошибок и энтропии квантовой суперпозиции длинных кодов нейросетевого преобразователя (см. рисунок 38 раздела 18).

Следует отметить, что появление таких конструкций, как функция вероятности расстояний Хэмминга - P(h) и плотность вероятности распределения значений - p(h), являются следствием квантовой суперпозиции наблюдаемых кодов на выходе нейросетевых преобразователей. Для статических преобразователей биометрия-код эти статистические характеристики не наблюдаемы. Однако если входных данных много (например, используются данные образов все «Чужие»), то построить функции P(h), p(h) удается. Так же удается построить эти функции, если одиночный пример биометрических данных размывается шумом (смотри рисунки 32, 33). Необходимо отметить, что вид функции вероятности и функции плотности распределения расстояний Хэмминга будет зависеть от положения центра и стандартного отклонения, используемых при тестировании биометрических данных. То есть, мы имеем дело с многомерными функциями $p(h, \overline{\sigma}(\zeta), \overline{E}(\zeta))$, где $\overline{\sigma}(\zeta)$ - вектор стандартных отклонений входного шума ИНС, $\overline{E}(\zeta)$ - вектор математических ожиданий входного шума ИНС.

Влияние параметров генератора шума на плотность распределения значений расстояний Хэмминга можно рассматривать как поведение некоторой искусственной молекулы, находящейся при разном значении температуры – T. В левой части рисунка 47 приведена блок-схема такой искусственной молекулы для данных «Свой».

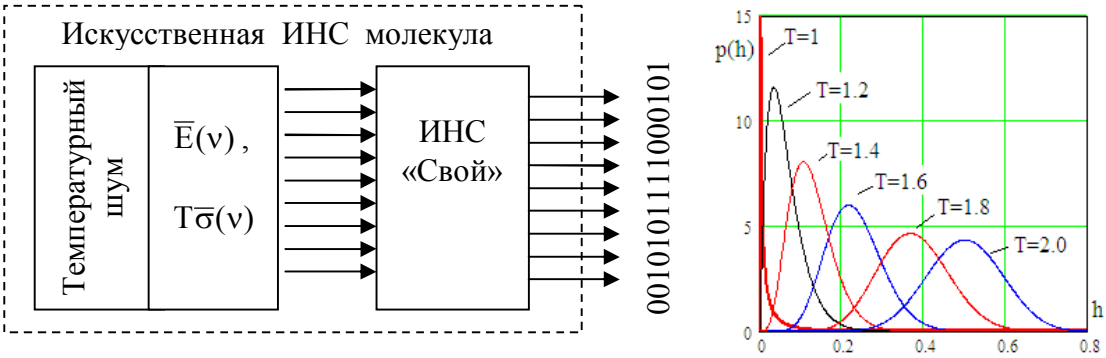


Рис. 47. Искусственная ИНС молекула, изменяющая состояния выходной квантовой суперпозиции с ростом температуры - T

При нулевой температуре T=0 такая искусственная молекула дает выходной код "$\overline{c}$", положение практически не меняется в интервале температур от 0 до 1 (до обычной температуры, когда стандартные отклонения данных «Свой» становятся обычными). При обычной температуре T=1 искусственная ИНС молекула начинает давать ошибки в выходном коде. По мере искусственного увеличения температуры до относительной величины 1.2, 1.4, … , 2.0, происходит увеличение нестабильных разрядов выходных состояний ИНС молекулы. Обычно стандартные отклонения данных биометрического образа «Свой» меньше в 2 -:- 3 раза в сравнении со стандартными отклонениями биометрических данных образов все «Чужие». То есть, при увеличении стандартной температуры в 2 раза, выходные данные ИНС молекулы становятся похожи на выходные данные кодов все «Чужие».

Выше рассмотрен только один пример искусственной ИНС молекулы. На практике их можно построить множество. Формально подобные конструкции могут быть построены для каждого из биометрических образов «Чужой-1», «Чужой-2», …. , «Чужой-N». При этом для каждой модели распределения расстояний Хэмминга оказываются похожи на те, что отображены в правой части рисунка 47. Отличаться они будут только их значениями температуры. В правой части рисунка 47 даны нормированные распределения значений расстояний Хэмминга для наибольших значений температуры. Для образов «Чужой-1», «Чужой-2», ….., «Чужой-N» (или все «Чужие») температуры для распределений правой части рисунка 46 должны составлять T= 0.1, 0.2, …., 1.0.

22. Принципиальные отличия компьютеров, построенных с использованием квантовой суперпозиции, воспроизводимой ИНС молекулами и молекулами Шредингера

Если подводить некоторые итоги, то основным отличием искусственных ИНС молекул от искусственных молекул Шредингера или полноценных квантовых вычислительных элементов, является простота создания квантовых суперпозиций. Из-за того, что используется ИНС молекула, а это уже макроуровень чтения и записи данных. На макроуровне мы без проблем наблюдаем квантовые состояния искусственной ИНС молекулы. Более того, к выходной квантовой суперпозиции ИНС молекулы, применимы обычные вычислительные элементы обычных компьютеров. Это принципиальное преимущество.

Вычислительные элементы, построенные на использовании искусственных молекул Шредингера, предположительно, могут порождать квантовые суперпозиции и работать с ними. Однако, их пока нет, они только создаются, работы по их созданию могут затянуться на десятки лет.

С другой стороны за относительную простоту создания квантовых суперпозиций и простоту работы с ними приходится расплачиваться искусственным оживлением статических ИНС молекул. Уравнение Шредингера трехмерно и развертывается во времени (оно относится к нелинейным дифференциальным уравнениям). Уравнение ИНС молекул многомерные статические, для того, что бы их заставить быть дифференциальными необходимо постоянно возбуждать ИНС молекулу источником температурного шума (рисунок 47) или замкнуть обратную связь при реализации генетических алгоритмов (рисунок 15, раздел 13).

Эффективность циклических континуально-квантовых вычислителей определяется количеством выполняемых циклов, которые можно реализовать с использованием континуальных функционалов и цифровых функционалов, задействованных внутри каждого цикла.

Линейные функционалы обычных нейронов являются далеко не единственными функционалами, способными обогащать данные в континуальной форме. В данной работе я попытался показать, что кроме линейных функционалов обычных нейронов и квадратичных функционалов радиально-базисных нейронов существуют нелинейные функционалы, построенные по аналогии с классическими статистическими критериями (раздел 15.4). Более того, могут быть использованы функционалы обогащения континуальных данных, построенных как аналог корреляционных функционалов Байеса (раздел 15.5). Необходимо уметь сравнивать множество функционалов обогащения континуальных данных по их мощности. Эта работа пока не выполнена, однако понятно, что ее нужно

выполнять. Понятно, что необходимо сравнивать эффективность континуальных функционалов по обеспечиваемой ими равновероятной ошибке (рисунки 29, 30).

Молекула ИНС, после обогащения континуальных данных, квантует их. Далее, мы имеет дело с кодами. Как показано в данной работе при обработке квантовой суперпозиции длинных кодов целесообразно использовать расстояния Хэмминга, вычисленные функционалами Хэмминга. Мощность этих функционалов растет пропорционально длине кодов, образующих квантовую суперпозицию. Кроме того, взвешивание расстояний Хэмминга показателями стабильности разрядов квантовой суперпозиции значительно усиливает мощность цифрового функционала. Получается, что по аналогии с континуальными функционалами, цифровых функционалов существует множество. Цифровые функционалы должны быть оптимизированы.

В целом, континуально-квантовые вычисления становятся эффективными, только если функционалы двух типов и квантователи между ними оказываются замкнутыми в циклическую структуру, отображенную на рисунке 48.

Очевидно, что функционалы обогащения континуальных данных описываются интегральными или дифференциальными уравнениями в пространстве входных континуальных состояний. Формально, замыкание петли обратной связи блок-схемы рисунка 48 по каждой из входных переменных должно приводить к появлению некоторых переходных процессов во времени. То есть, должны появляться дифференциальные или интегральные преобразования во времени. Теоретически блок-схема циклического применения ИНС молекулы должна приводить к появлению некоторого многомерного континуально-квантового уравнения, являющегося аналогом трехмерного дифференциального уравнения Шредингера. То, что континуально-квантовое уравнение молекулы ИНС не совпадает с уравнением Шредингера, является очевидным. Более того, можно утверждать, что континуально-квантовых уравнений ИНС молекул множество.

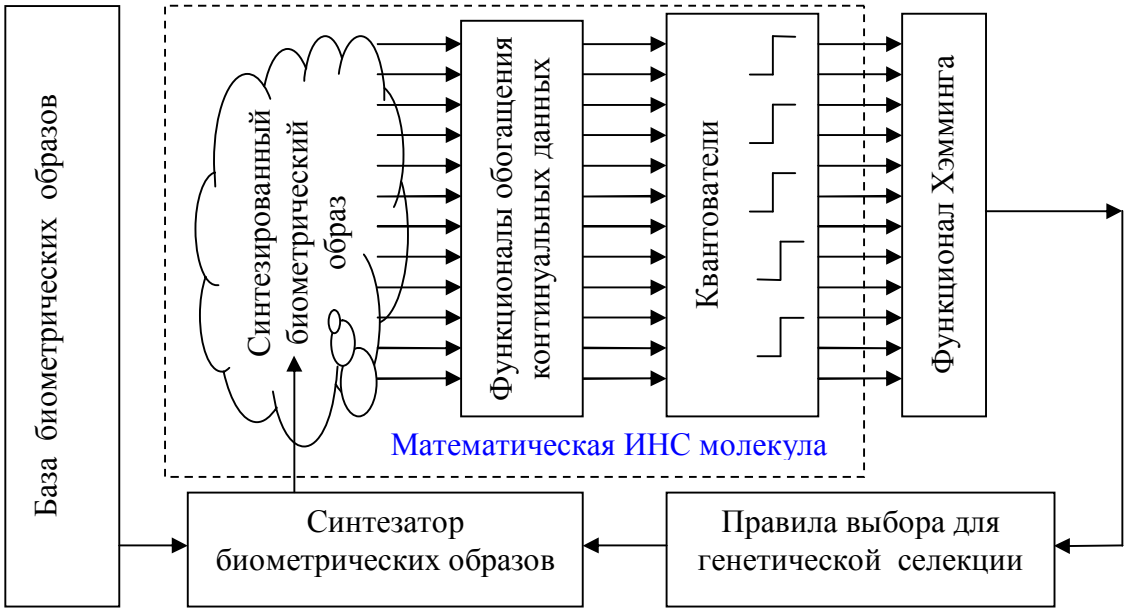


Рис. 48. Блок-схема циклического использования ИНС молекулы при решении обратной задачи биометрии

Для того, что бы получить новое уравнение, достаточно изменить параметры или способ построения континуальных функционалов. Новые уравнения будут получены, если изменить параметры квантователей. Новые

уравнения будут получены, если изменить правила генетической селекции или структуру вычисления функционала Хэмминга.

Следует отметить, что в теории квантовых вычислений созданной под вычислительные элементы Шредингера ветвь функционалов Хэмминга практически не используется [4, стр. 495]. Это связано с тем, что наблюдать квантовую суперпозицию в системах, описываемых уравнением Шредингера, практически невозможно. Для континуально-квантовых уравнений ИНС наблюдение квантовой суперпозиции не является проблемой и потому, ветвь использования функционалов Хэмминга и распределений расстояний Хэмминга будет активно развиваться.

В целом, континуально-квантовые уравнения ИНС преобразований должны дополнять уравнения Шредингера. Континуально-квантовые уравнения ИНС вычислителей должны занимать промежуточное положение между обычными компьютерами и полноценными квантовыми компьютерами. Видимо, континуально-квантовые вычислители, построенные на циклическом использовании ИНС молекулы, должны приближаться по своим показателям к полноценным квантовым компьютерами по их:

- быстродействию выполнения сложных вычислений;
- по способности корректировать шумы (ошибки в канале связи);
- по надежности распознавания образов;
- по возможности работы с выборками минимального объема;
- по возможности повышения устойчивости вычислений при решении обратных задач.

Все перечисленные выше направления совершенствования вычислительных процессов востребованы практикой и значительно различаются по механизмам их реализации. Сводить все к росту быстродействия вычислителей нельзя. Необходимо, при решении каждой из перечисленных выше задач, создавать свои специализированные вычислители.

23. Перспективы усиления мощности вычислителей, использующих квантовую суперпозицию, созданную на обычном компьютере

23.1. Перспектива перехода от использования бинарных нейронов к z-арным нейронам больших искусственных нейронных сетей

В настоящее время под искусственными нейронами обычно понимаются элементарные вычислители с несколькими входами, имеющие два выходных состояния «0» и «1». В случае перехода к нейронным сетям с большим числом нейронов, выходы нейронной сети (выходы ИНС молекулы) образуют легко наблюдаемую квантовую суперпозицию с некоторой запутанностью (коррелированностью) разрядов кода.

В биометрических приложениях важна такая характеристика, как энтропия квантовой суперпозиции выходных состояний. В разделе 10 (рисунок 12) было показано, что неограниченно увеличивать число нейронов преобразователя биометрия-код нельзя. С некоторого момента, рост коррелированности разрядов кода из-за перекрытия входных данных нейронов (раздел 23.3., рисунок 46), не дает увеличиваться энтропии выходных кодов.

Выходом из создавшегося положения является увеличение энтропии выходных состояний ИНС за счет увеличения числа состояний выходных квантователей нейронов [84, 85, 86]. На рисунке 49 приведены нейроны с двоичным и троичным квантователем.

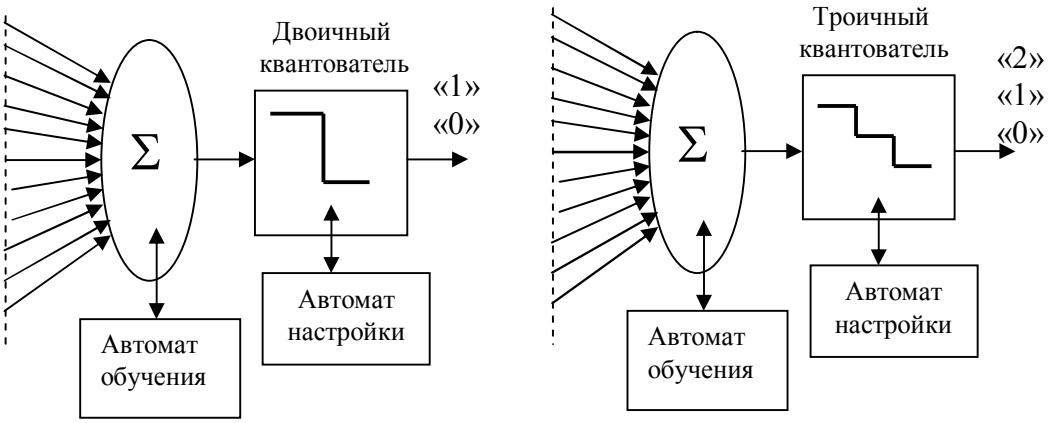


Рис. 49. Переход от бинарных нейронов к нейронам с троичными выходными состояниями

Очевидно, что этот переход должен привести к некоторому росту энтропии без увеличения числа нейронов. Практика применения нейронов с многоуровневым квантованием показывает, что прирост энтропии (снижение коррелированности) состояний разрядов оказывается ощутимым и может составить до одной трети. Естественно, что при этом усложняется процедура настройки функционалов обогащения входных континуальных данных нейрона, а так же усложняется процедура настройки порогов квантователя.

Теоретически, рост энтропии должен увеличиваться с ростом числа выходных состояний квантователей нейронов. На рисунке 49 приведен нейрон с квантователем, имеющем 4 выходных состояния. При этом, изменение состояний квантователя не обязательно должно быть монотонным по отношению к входным данным. Как показано на рисунке 45, соседние состояния квантователя могут быть заданы случайной таблицей, что так же должно приводить к росту энтропии квантовой суперпозиции.

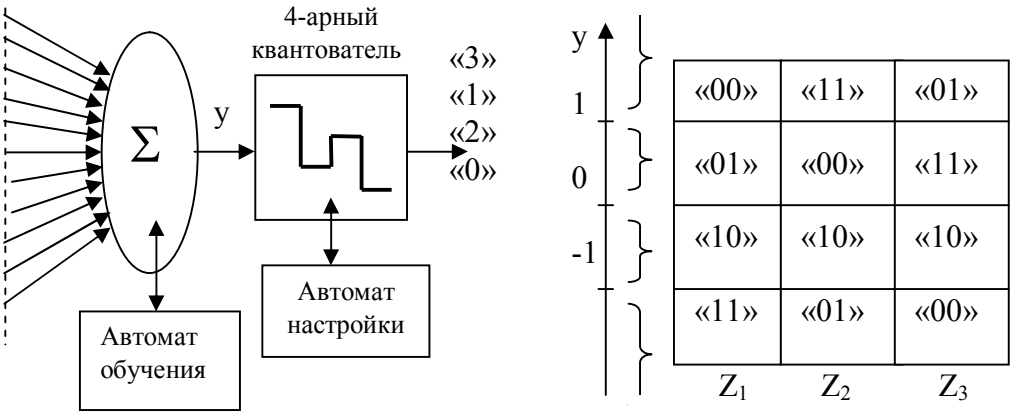


Рис. 50. Использование квантователя с четырьмя состояниями, входные значения которых заданы таблицей

Примечание. Если вернуться в раздел 20, то там речь идет о гистограмме с 6 столбцами (с 6 интервалами) – это эквивалентно наличию внутри функционала хи-квадрат квантователя с 6 выходными состояниями. По сути дела, ожидаемый рост мощности хи-квадрат критерия есть не что иное, как то же самое обогащение данных с учетом дискретности выходных состояний обогащающего функционала.

В данном разделе все это перенесено на обычные нейроны с линейными функционалами обогащения данных.

23.2. Перспектива усиления мощности нейронных сетей за счет создания новых алгоритмов обучения, учитывающих корреляционные связи пар биометрических параметров

При решении задачи на обычных вычислительных машинах, не имеет значения в какой вычислительной системе (с каким основанием) производятся расчеты. Мы всегда можем перейти от двоичной системе в 10-тичную систему или 16-тиричную систему. При континуально-квантовых нейростетевых вычислениях положение меняется коренным образом. При переходе к использованию нейронов со сложными квантователями, растет длина выходного кода, растет энтропия выходного кода, растет размер словаря образов, потенциально распознаваемых системой нейронных сетей.

Получается, что на тех же исходных данных при переходе к использованию более сложных z-арных нейронов, мы получаем решения с более высоким качеством, чем для обычных двоичных нейронов. При этом платить за это потребуется только усложнением алгоритма обучения искусственных нейронной. Естественно, что стандартный алгоритм обучения ГОСТ Р 52633.5 должен быть модифицирован под новую систему исчисления.

Новый и более эффективный алгоритм обучения и новая система нейросетевых вычислений неразрывно связаны между собой, что иллюстрирует рисунок 51.

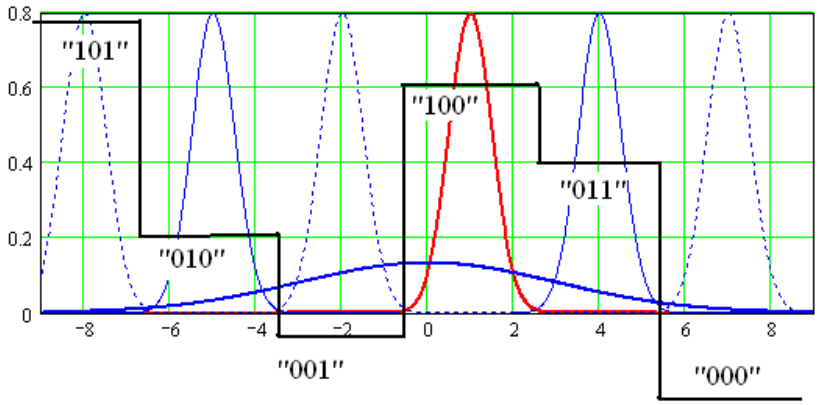


Рис. 51. Необходимость сжатия данных распределения образа «Свой» при использовании нейроном квантователя с шестью уровнями

Как видно из рисунка 51 расстояние между соседними порогами квантования должно составлять примерно шесть стандартных отклонений данных образа «Свой» - $6\sigma(y_\nu)$. Еще одним ограничением является то, что квантование должно выполняться внутри интервала шести стандартных отклонений образов все «Чужие». Получается, что в ситуации, отображенной на рисунке 51, когда один нейрон дает три выходных бита «000», нейросетевые вычисления не могут выполняться в 8-ми ричной системе исчисления. Только шесть квантователей нейрона попадают в интервал - $6\sigma(y_\xi)$, что соответствует 6-ти ричной системе нейросетевых вычислений.

Получается, что первоначально мы должны осуществить операцию обогащения данных, а уже позднее осуществить выбор параметров квантователя.

При обучении обогащающих данные функционалов необходимо использовать математические ожидания биометрических параметров, их стандартные отклонения и их коэффициенты корреляции.

Если использовать нормирование по стандартному отклонению данные, то по их знаку коэффициента корреляции можно определить знак суммирования. Если корреляция положительна, то контролируемые параметры следует вычитать. В зависимости от корреляции происходит усиление сжатия данных «Свой», как это показано на рисунке 52.

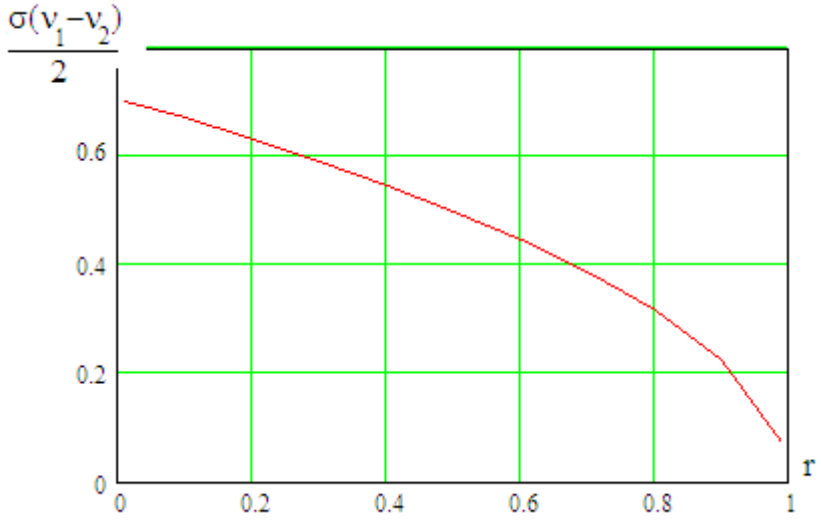


Рис. 52. Сжатие распределения коррелированных данных «Свой» сумматором с двумя входами

В случае обнаружения отрицательной корреляции для усиления сжатия данных «Свой» необходимо их складывать. Получается, что для усиления качества биометрических данных, достаточно выбирать их нормированные пары с близкими математическими ожиданиями и отрицательной коррелированностью. Или должны использоваться положительно коррелированные данные с близкими по модулю, но с разными знаками математических ожиданий. Подобные вычислительные алгоритмы, как и алгоритм ГОСТ Р 52633.5, имеют линейную вычислительную сложность.

Очевидно, что эта новая линейка алгоритмов оказывается чувствительной к ошибкам определения знака коэффициентов корреляции на малых обучающих выборках. Для устранения ошибок приходится использовать специальные корректирующие данные алгоритмы [46, 47, 48].

23.3. Перспектива перехода к многомерной регуляризации решений систем линейных уравнений

В разделе 13 данной работы было показано, что в пространстве расстояний Хэмминга (в 256-ти кубитном пространстве квантовой суперпозиции) удается решать обратную биометрическую задачу для матриц нейросетевых преобразований размерности 416x256. Для линейной алгебры это фантастически большая размерность. Если ориентироваться на обычные преобразования линейной алгебры, то при условии наблюдения биометрических данных с относительной ошибкой порядка 10%, задача обращения линейных матриц (решения систем линейных уравнений) становится плохо обусловленной уже для квадратных матриц 4, 5 порядка. В связи с этим печальным обстоятельством в литературе [87, 88, 89], обычно рекомендуют осуществить регуляризации,

увеличить число примеров в выборке исходных данных или понизить размерность задачи, убрав из уравнений малоинформативные параметры.

Для нас наибольший интерес представляет регуляризация, осуществляемая по Тихонову [82]. В соответствии с регуляризацией по Тихонову, к неустойчивой матрице с большим числом обусловленности необходимо добавить небольшой стабилизатор:

$$\widetilde{A}_0 = A + \alpha_0 \cdot [\![1]\!] \qquad (86),$$

где α_0 - малый коэффициент регуляризации, обеспечивающий минимум ошибки; $[\![1]\!]$ - единичная матрица с единичными элементами на диагонали.

В силу того, что единичная матрица абсолютно стабильна ($cond[\![1]\!]=1$), число обусловленности матрицы (86) всегда меньше, чем число обусловленности исходной матрицы – А.

Обратим внимание на то, что уравнение регуляризации (86) не является единственным. На самом деле мы имеем множество подобных уравнений с разными матричными стабилизаторами и разными параметрами стабилизации:

$$\widetilde{A}_i = A + \alpha_i \cdot [\pm 1] \qquad (87).$$

Любая единичная матрица единичными коэффициентами на диагонали любого знака (любого сочетания знаков) всегда является абсолютно устойчивой $cond[\pm 1]=1$. То есть, для матрицы 256х256 мы будем иметь 2^{256} возможных вариантов решения задачи регуляризации. Получается, что задача регуляризации по Тихонову только в первом приближении является простой – одномерной. На самом деле она является сложной – многомерной.

Предположительно решать задачу регуляризации или корректного обращения матриц необходимо по принципу, похожему на принцип, изложенный в разделе 13. Поясним это с использованием одной из геометрических трактовок числа обусловленности, приведенной на рисунке 53.

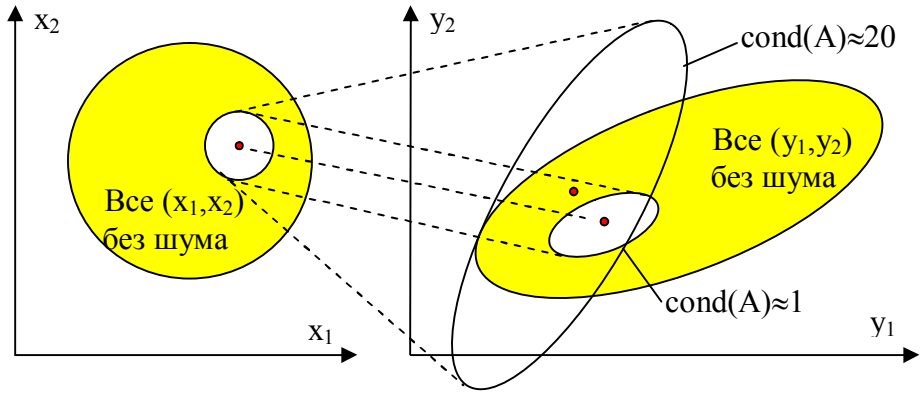


Рис. 53. Эллипсы распределения данных при плохой и хорошей обусловленности решаемой задачи

Независимо от качества матрицы преобразования – А, ее умножение на нормированный вектор независимых случайных данных $\bar{x}$ всегда приводит к появлению зависимых выходных данных - $\bar{y}$. На рисунке 53 эта ситуация отображена кругом и эллипсом, обозначенным заливкой. Если задача хорошо обусловлена ($cond(A)\approx 1$), то любой пример вектора входных данных (x_1, x_2) в левой части рисунка, размытый случайным шумом, дает эллипс сопоставимой площади в правой части рисунка «все (y_1, y_2)». При этом, размывающий данные шум не усиливается.

Ситуация меняется, если задача оказывается плохо обусловленной. В этом случае размывающий входные данные шум усиливается. Для $cond(A) \approx 20$ происходит примерно 20-ти кратное усиление шумов, размывающих каждый пример входных данных. Как видно из правой части рисунка 53, усиленная в 20 раз мощность шума входных данных оказывается сопоставима с мощностью эллипса данных «все (y_1, y_2) без шума». Пересечение эллипса «$cond(A) \approx 20$» и эллипса «все (y_1, y_2) без шума» дает правдоподобные решения. Области эллипса «$cond(A) \approx 20$», находящиеся вне эллипса «все (y_1, y_2) без шума», соответствуют не правдоподобным решениям задачи.

В рамках рассмотренной выше геометрической интерпретации задача регуляризации сводится к поиску некоторой стабилизирующей матрицы ΔA и вектора смещения математических ожиданий – Δa, уменьшающих область неправдоподобных решений для заданного уровня размывающих данные шумов $\Delta\bar{x}$.

Для того, что бы технически решить поставленную задачу необходимо построить квадратичную нейронную сеть, дающую состояния «0000….0000» для выходных данных «все (y_1, y_2, …, y_N) без шума». Очевидно, что для квантовой суперпозиции этих данных энтропия будет нулевой. Однако, как только входные данные «все (x_1, x_2, …, x_N)» будут подаваться с шумом 0.3(σ(x_1), (σ(x_2), …,(σ(x_N)), энтропия квантовой суперпозиции перестает быть нулевой.

При этом, многомерная регуляризация сводится к итерационному подбору параметров стабилизирующей матрицы - A и вектора смещения математических ожиданий – Δa, снижающих энтропию выходных кодов квадратичных нейронных сетей многомерного наблюдения данных. Алгоритм снижения энтропии, видимо, должен быть генетическим, подобным алгоритму раздела 13. Предположительно, задача обращения матриц нейросетевых функционалов раздела 13 и задача регуляризации обращения матриц линейной алгебры, будут иметь сопоставимую вычислительную сложность.

В этом случае, задача многомерной регуляризации решения систем линейных уравнений (обращения линейных матриц) технически разрешимы для размерностей в десятки и даже сотни параметров. Все это становится возможным из-за того, что мы переходим к работе с квантовыми суперпозициями в десятки и сотни кубит. Мы выполняем операции с множеством состояний квантовой суперпозиции при вычислении функционалов Хэмминга и других математических операций, выполняемых далее над функционалами Хэмминга.

23.4. Перспектива перехода к многомерному контролю параметров «белого» шума

Следует подчеркнуть, что интерес к квантовым вычислителям подогревается их возможностью применения к решению обратных криптографических задач [4, 90]. В частности, значительно повысился интерес к квантовым вычислениям, после создания квантового алгоритма поиска простых чисел (алгоритм Шора создан в 1994 году). В 2001 году работоспособность алгоритма Питера Шора была подтверждена группой специалистов из IBM, разложившей число 15 на множители 3 и 5 с использованием квантовой суперпозиции длиной в 7 кубит. Этот 7-ми кубитный рекорд сохраняется по настоящее время, однако, здесь важен сам факт подтверждения работоспособности квантовых вычислителей для решения тех или иных криптографических задач.

Криптография хорошо финансируется все, что с ней связано, может получить финансовую поддержку. В этом плане любые приложения квантовой

суперпозиции, ориентированные на тот или иной аспект криптографии, заслуживают внимания.

Попытаемся упростить ситуацию, будем рассматривать криптографию, как науку о сокрытии дискретных зависимых данных, путем их преобразования в «абсолютно» независимые данные – «белый шум» с максимально возможным значением энтропии. В этом случае криптоаналитику нельзя будет за что-то зацепиться. Получается, что качество криптографии зависит от качества обеспечиваемого ею «белого шума». То есть, необходим контроль того, на сколько та или иная цифровая последовательность использованная в криптографических преобразованиях или полученная с помощью криптографических преобразований, близка по своим свойствам к «белому шуму».

Для определенности рассмотрим задачу синтеза [91, 92] псевдослучайной последовательности для ее использования, например, в качестве ключа для симметричного шифрования. Очевидно, что после получения псевдослучайной последовательности нужно убедиться в ее качестве, воспользовавшись каким либо из известных тестов [93, 94]. К сожалению, все известные тесты низкоразмерны и будут давать противоречивые результаты. Однако, опираясь на использование квантовой суперпозиции, мы можем достаточно просто поднять размерность теста до длины ключа и тем самым, снять противоречия между результатами множества низкоразмерных тестов.

В случае идеального «белого шума» каждый бит является независимым и, состояния «0» или «1» для каждого i-того разряда являются равновероятными $P(«0_i»)=P(«1_i»)=0.5$.

Вероятность угадывания k бит из общего числа n-бит описывается биномиальным законом распределения значений:

$$P(k) = \frac{n!}{k!(n-k)!}(P("0"))^k \cdot (1-P("0"))^{n-k} \qquad (88).$$

С наибольшей вероятностью угадывается ровно половина разрядов k= n/2. Это означает, что случайно выбранное число длиной 256 бит при вычислении расстояний Хэмминга с другими случайно-выбранными числами из последовательности «белый шум», будет давать математическое ожидание расстояний Хэмминга E(h)=256/2=128 бит.

Из статистической теории [35, 38] так же известно, что стандартное отклонение функции вероятности (88) или расстояний Хэмминга определяется по следующей формуле:

$$\sigma^2(h) = n \cdot P("0") \cdot (1-P("0")) \qquad (89).$$

То есть, стандартное отклонение распределения расстояний Хэмминга для кода длиной 256 бит при белом шуме должно составлять 8 бит = $\sqrt{256/4}$. При этом, распределение расстояний Хэмминга p(h) – должно быть нормальным.

Получается, что высокоразмерный контроль близости псевдослучайной последовательности диной n к «белому шуму» может быть осуществлен сразу по трем условиям:

$$\begin{cases} E(h) = \dfrac{n}{2} \pm \Delta_E, \\ \sigma(h) = \sqrt{n/4} \pm \Delta_\sigma, \\ p(h) = \dfrac{1}{\sqrt{n\pi/2}} \cdot exp\left\{\dfrac{-(n/2-h)^2}{2n}\right\} \pm \Delta(h) \end{cases} \qquad (90).$$

Каждое из условий (81) должно выполняться с точностью до некоторой заданной величины. Допустимые отклонения определяются исходя из конечных размеров используемых тестовых данных.

Нарушение любого из условий (90) должно давать криптоаналитикам данные о возможности снижения вычислительных ресурсов при решении обратной криптографической задачи.

Еще одним важным моментом является то, что вычисление расстояний Хэмминга по своей сути является поразрядной сверткой двух кодов одинаковой длины. Проверка качества генератора m-последовательностей приводит нас к операции вычисления автосвертки разрядов кода на тот же код с циклическим сдвигом:

$$h_j = \sum_{i=1}^{256} ("x_i") \oplus ("x_{i+j}") \quad \text{при} \quad j = 1, 2, ..., 256 \qquad (91)$$

Для того, что бы вычислить автосвертку 256 разрядов по формуле (91), необходимо иметь код генератора m-последовательности длинной 512 бит.

Можно выполнить свертку разрядов числа самих на себя с некоторым циклическим сдвигом кода на – j разрядов:

$$h_j = \sum_{i=1}^{256} ("x_i") \oplus ("x_{(i+j) \bmod (256)}") \quad \text{при} \quad j = 1, 2, ..., 256 \qquad (92).$$

Для вычисления собственного расстояния Хэмминга (83) в двукратном увеличении длины кода m-последовательности, уже нет необходимости. Автосвертки Хэмминга вида (92) хорошо себя зарекомендовали при оценке высокоразмерной энтропии длинных кодов русскоязычного текста [82, 83].

23.5. Перспектива синтеза и обучения нейросетевых наблюдателей (оракулов) высокой размерности при решении задачи факторизации

Перспектива применения квантовых вычислителей для решения задач криптографии (например, через реализацию алгоритма Шора [4]) послужила мощным стимулом развития этой предметной области. В связи с этим, необходимо попытаться построить для циклических континуально - квантовых вычислителей некоторый аналог алгоритма Шора, опирающийся на нейросетевые технологии воспроизведения нужной квантовой суперпозиции.

Сегодня считается, что поиск произведения простых чисел является вычислительно сложной задачей [90]. Из теории известно, что перебор делителей имеет вычислительную сложность $O(\sqrt{n} \cdot \log^2 n)$. При больших значениях n, приходится проверять очень много чисел, именно по этой причине алгоритм считается вычислительно сложным. Однако такая оценка касается только одномерных наблюдателей без памяти, которые видят только последний остаток и забывают о нем, если он не равен нулю.

Очевидно, что для создания квантовой суперпозиции потребуется поднять размерность наблюдателя (наблюдатель или оракул должен уметь учитывать множество остатков от деления исследуемого числа на перебор близких чисел). В этом контексте может быть использован портрет факторизуемого числа, построенный в виде остатков, полученных в разных системах счисления. На рисунке 54 приведен такой портрет числа n= 2233369, полученный в 2016 году Д.Н. Надеевым. На рисунке остатки менее чем 0.1, даны белым цветом, все остальные остатки даны черным цветом.

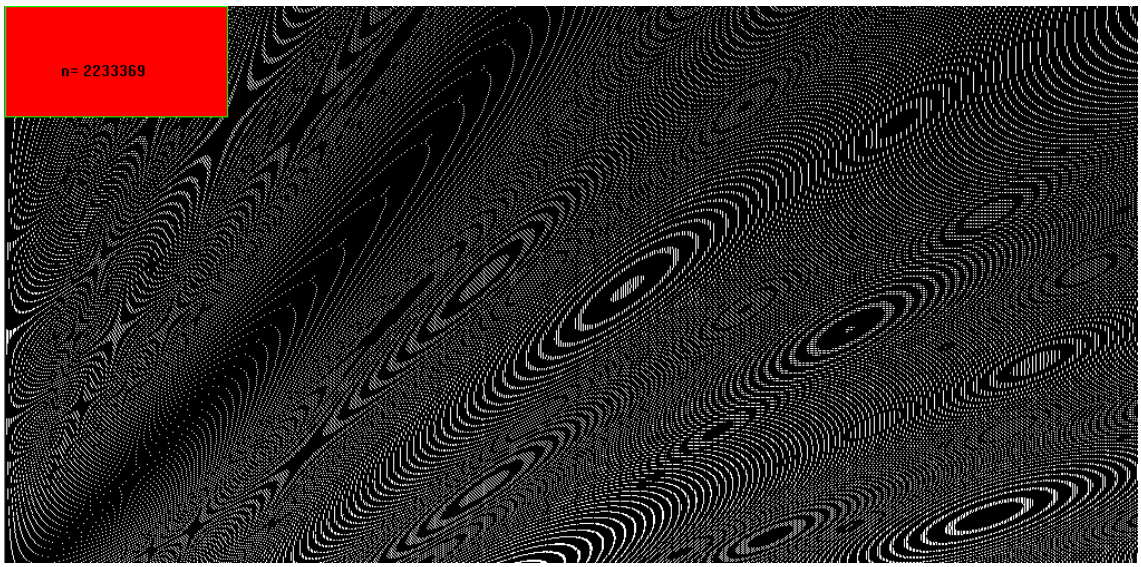


Рис. 54. Двухмерный портрет факторизуемого числа 2233369, полученный из остатков деления этого числа в разных системах счисления с основаниями 10.00, 9.98, 9. 96, ..., 5.12

В правой части рисунка 50 мы видим несколько эллиптических структур, каждая из которых имеет явный центр и кольца вокруг него. Изменение числа приводит к изменению его портрета, что отображено на рисунке 55.

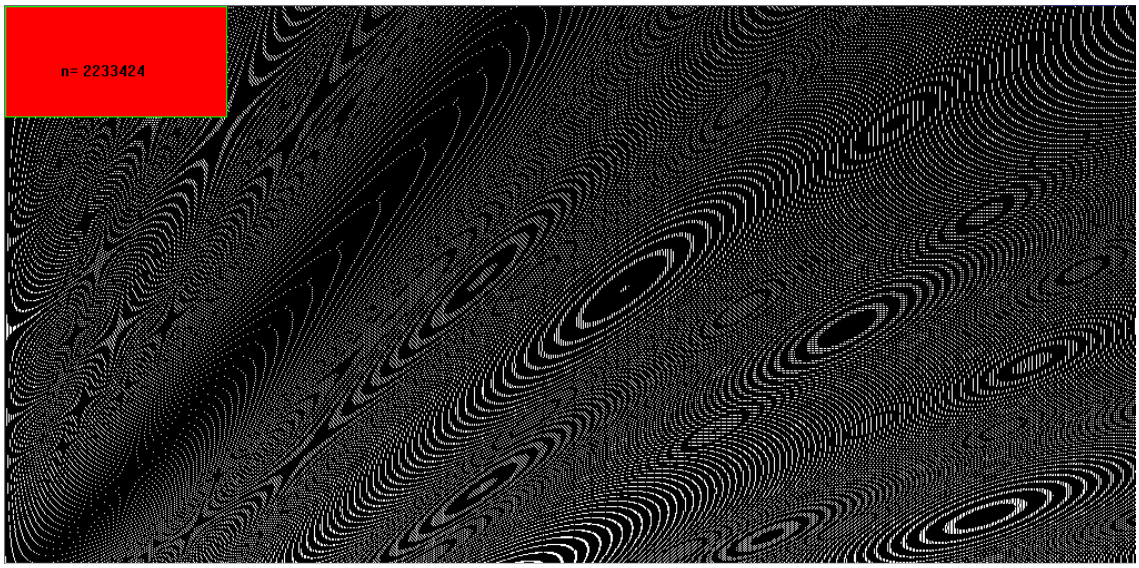


Рис. 55. Двухмерный портрет факторизуемого числа 2233424, полученный из остатков деления этого числа в разных системах счисления с основаниями 10.00, 9.98, 9. 96, ..., 5.12

Наблюдатель-человек легко выделяет в двухмерных портретах разных чисел одинаковые эллиптические структуры, имеющие разные фазы и разные периоды своих состояний. Формально можно утверждать, что каждую из эллиптических структур портретов чисел можно рассматривать как некоторого оракула, отвечающего за наблюдение одной из периодических составляющих исследуемых остатков. Остатки, получаемые при переборе делителей, ведут себя «непредсказуемо» только потому, что они описываются большим числом гармонических составляющих с разной фазой и периодом. Если мы смотрим одну

строку портрета (остатки в одной из систем счисления), увидеть эллиптические структуры гармонических оракулов мы не можем. Оракулы становятся наблюдаемы, только при переходе к двухмерным портретам факторизуемых чисел.

Портреты чисел, приведенные на рисунках 54 и 55, являются прекрасной иллюстрацией эффективности повышения размерности наблюдателя (оракула). То, что для одномерных наблюдателей является хаосом, для наблюдателей более высокой размерности является порядком. Чем выше размерность наблюдателя, тем выше его потенциальная возможность устранения хаоса.

Предположительно, учет данных одного эллиптического оракула (его периода и фазы) должен привести к ускорению перебора примерно на один кубит. В рисунках просматривается порядка 20 эллиптических структур, то есть, мы можем создать 40 мерный наблюдатель (40 мерный оракул), многократно ускоряющий обычный одномерный направленный перебор.

Опираясь на опыт использования нейронных сетей в биометрии, следует ожидать, что 40 мерный нейросетевой оракул будет давать предсказания, точность которых будет обеспечивать ускорение вычислений примерно до 20 кубит. Если такой ускоритель будет использоваться совместно с самым мощным на данный момент вычислителем Таньхэ-2 (240 МегоВатт потребления), то Китайскся народная республика вместо одной суперЭВМ, получит эквивалент в виде 2^{20}=1048576 виртуальных вычислительных машин такой же мощности. Вместо одной суперЭВМ появляется миллион виртуальных суперЭВМ при сохранении потребления одной вычислительной машины.

Этот пример показывает то, на сколько важно развивать технологию вычислений, построенных на использовании квантовой суперпозиции и квантовой запутанности, порождаемых искусственными нейронными сетями. Эти технологии не могут дать универсальных вычислителей, которые предполагается получить на новой элементной базе [4]. Однако, их можно строить уже сегодня, не дожидаясь будущих технологических прорывов квантовой микроэлектроники. Аналоговые вычислительные машины не могут быть универсальными, циклические аналого-цифровые машины (континуально-квантовые вычислители) так же не могут быть универсальными. Под каждую значимую задачу придется создавать (обучать) свой нейросетевой преобразователь образ-код, порождающий необходимую квантовую суперпозицию и квантовую запутанность.

ЗАКЛЮЧЕНИЕ

Континуально-квантовые вычислители, примеры которых приведены в этой работе, оказываются весьма и весьма эффективными. Я попытался это показать на примерах задач:

- извлечения знаний из искусственной нейронной сети (раздел 13 стр. 25);
- повышения уровня подавления шумов (раздел 18, стр. 50);
- повышения мощности хи-квадрат критерия для малых выборок (раздел 20, стр. 56);
- усиления мощности процедур регуляризации при решении систем линейных уравнений (раздел 23.3 стр. 73);
- снижения требований к размеру тестовой выборки при контроле параметров «белого шума» (раздел 23.4, стр. 75).

Это далеко не весь перечень задач, где формирование квантовой суперпозиции и ее использование окажутся эффективными. С очень высокой вероятностью, дальнейшие исследования в этом направления позволят расширить список приложений, где квантовая суперпозиция окажется эффективной.

Надеюсь, что аргументы, приведенный мной будут достаточно убедительны и научно-техническая общественность проявит к этой тематике интерес.

Когда я писал эту работу, технические преимущества применения квантовой суперпозиции для меня были главными. Философия и математика оставались в стороне, однако, математические и философские аспекты проблемы могут оказаться куда важнее уже достигнутых технических преимуществ.

С философских позиций меня всегда интересовал вопрос: почему мы умнее существующих компьютеров? Сегодняшние компьютеры имеют огромную память и огромное быстродействие (тактовую частоту в 10 000 000 000 Гц). Человеческий компьютер (мозг) работает с тактовой частотой всего 100 Гц), и тем не менее, мы пока умнее компьютеров.

Казалось бы, что ответ прост. Компьютер решает одномерные задачи, а мы решаем 10 000 мерные задачи. В грубом приближении это эквивалентно повышению тактовой частоты нашего естественного компьютера (мозга) до величины 1 000 000 Гц. Эта тактовая частота все равно оказывается в 10 000 раз меньше, чем у современных компьютеров. То есть, простым распараллеливанием вычислений объяснить интеллектуальные возможности людей нельзя, у людей есть еще какой-то механизм, ускоряющий вычисления.

Я взялся за эту книгу в надежде аргументировано показать, что большие нейронные сети в динамическом режиме (включена обратная связь или данные входного примера размываются встроенным генератором шума) порождают полноценную квантовую суперпозицию 256 кубит и более. Если мы начинаем работать блоками квантовой суперпозиции в 256 бит, возникают огромные ускорения вычислений или другие положительные эффекты. По сути дела мы разумны, мы высоко интеллектуальны потому, что распознаем образы высокой размерности и умеем для них формировать индивидуальную квантовую суперпозицию (индивидуальную квантовую запутанность). При обучении распознаванию образов, при упорядочивании образов, при быстром поиске образов, при корректировке ошибок, мы всегда использовали и используем вычисления, построенные на операциях с многомерными квантовыми суперпозициями.

Математика только сейчас выходит на понимание сверхвысокой эффективности квантовой суперпозиции [4]. Юрий Манин в 1980 году оказался провидцем, указав перспективу движения в сторону создания квантовых компьютеров. Однако, с позиций сегодняшнего дня я бы изменил акценты. Квантовые компьютеры на новой элементной базе – это не главное. Мы вполне можем использовать уже имеющиеся у нас компьютеры. Куда важнее полноценная математика создания и использования квантовых суперпозиций. То, что сегодня описано как квантовые вычисления [4], ориентировано только на известные решения уравнения Шредингера, и порождаемые ими квантовые суперпозиции (квантовые запутанности).

Одной из основных целей данной книги было показать, что систем, порождающих квантовые суперпозиции, множество. Уравнения Шредингера – это не более чем удобный для математики частный случай систем. Нейронные сети это еще один способ формирования и применения квантовых суперпозиций. Любой способ создания той или иной квантовой суперпозиции может быть использован для создания некоторого специализированного вычислителя под некоторую задачу.

Принципиально важным является то, что порождаемые нейронными сетями квантовые суперпозиции оказываются пригодны для выполнения операций в пространстве функционалов расстояний Хэмминга. Для квантовых суперпозиций, порождаемых решениями уравнений Шредингера, эти операции

невыполнимы. По этой причине функционалы Хэмминга пока не нашли применения в традиционных квантовых вычислениях [4]. Видимо, квантовые суперпозиции, порождаемые нейронными сетями, и квантовые суперпозиции, порождаемые уравнением Шредингера, дополняют друг друга. Со временим функционалы Хэмминга должны занять достойное место среди операций над квантовыми суперпозициями и квантовыми запутанностями.

ЛИТЕРАТУРА:

1. Милантьев В.П. История возникновения квантовой механики и развитие представлений об атоме. М.: Книжный дом Либерком. 2014 г., 248 с.
2. Саскинд Л., Фридман А. Квантовая механика. Теоретический минимум. СПб.: Питер, 2016 г., 400 с.
3. Брайн К. Квантовая теория. М. Рипол-классик, 215, 160 с.
4. Нильсон М., Чанг И. Квантовые вычисления и квантовая информация. М.: Мир. 2006 г. 821 с.
5. Ramírez-Ruiz J., Pfeiffer C., Nolazco-Flores J. Cryptographic Keys Generation Using FingerCodes. //Advances in Artificial Intelligence - IBERAMIA-SBIA 2006 (LNCS 4140), p. 178-187, 2006
6. Monrose F., Reiter M., Li Q., Wetzel S. Cryptographic key generation from voice. //Proc. IEEE Symp. on Security and Privacy, pp. 202-213, 2001.
7. Hao F., Anderson R., Daugman J. Crypto with Biometrics Effectively //IEEE TRANSACTIONS ON COMPUTERS, VOL. 55, NO. 9, SEPTEMBER, Page(s):1073 – 1074, 2006.
8. Dodis Y., Reyzin L., Smith A. Fuzzy Extractors: How to Generate Strong Keys from Biometrics and Other Noisy // Proc. EUROCRYPT, April 13, pages 523-540, 2004.
9. Иванов А.И., Захаров О.С. Среда моделирования «БиоНейроАвтограф». Программный продукт создан лабораторией биометрических и нейросетевых технологий, размещен с 2009 г. на сайте АО «ПНИЭИ» http://пниэи.рф/activity/science/noc.htm для свободного использования университетами России, Белоруссии, Казахстана.
10. Язов Ю.К. и др. Нейросетевая защита персональных биометрических данных. //Ю.К.Язов (редактор и автор), соавторы: В.И. Волчихин, А.И. Иванов, В.А. Фунтиков, И.Г. Назаров // М.: Радиотехника, 2012 г. 157 с. IBSN 978-5-88070-044-8
11. ГОСТ Р 52633.5-2011 «Защита информации. Техника защиты информации. Автоматическое обучение нейросетевых преобразователей биометрия-код доступа»
12. Иванов А.И. Нечеткие экстракторы: проблема использования в биометрии и криптографии. // Первая миля. № 1, 2015 г. с. 40-47.
13. Иванов А.И. Сопоставительный анализ показателей конкурирующих технологий биометрико-криптографической аутентификации личности. «Защита информации. ИНСАЙД» № 3 2014 г., с. 32-39.
14. ГОСТ Р ИСО/МЭК 19794-4 2014 Информационные технологии. Биометрия. Форматы обмена биометрическими данными. Часть 4. Данные изображения отпечатка пальца.
15. ГОСТ Р ИСО/МЭК 19794-5 2006 Автоматическая идентификация. Идентификация биометрическая. Форматы обмена биометрическими данными. Часть 5. Данные изображения лица.

16. ГОСТ Р ИСО/МЭК 19794-6 2006 Автоматическая идентификация. Идентификация биометрическая. Форматы обмена биометрическими данными. Часть 6. Данные изображения радужной оболочки.
17. ГОСТ Р ИСО/МЭК 19794-7 2006 Автоматическая идентификация. Идентификация биометрическая. Форматы обмена биометрическими данными. Часть 7. Данные динамики подписи.
18. ГОСТ Р ИСО/МЭК 19794-9 2009 Автоматическая идентификация. Идентификация биометрическая. Форматы обмена биометрическими данными. Часть 9. Данные изображения сосудистого русла.
19. ГОСТ Р ИСО/МЭК 19794-10 2010 Автоматическая идентификация. Идентификация биометрическая. Форматы обмена биометрическими данными. Часть 10. Данные контура кисти руки.
20. ГОСТ Р ИСО/МЭК 19794-14 2013 Информационные технологии. Биометрия. Форматы обмена биометрическими данными. Часть 14. Данные о ДНК.
21. Саймон Хайкин. Нейронные сети: полный курс. М.: «Вильямс», 2006. — С. 1104.
22. ГОСТ Р 52633.3-2011 «Защита информации. Техника защиты информации. Тестирование стойкости средств высоконадежной биометрической защиты к атакам подбора».
23. Захаров О.С., Хозин Ю.В., Иванов А.И., Капитуров Н.В. Оценка технических ограничений, накладываемых на размерность выходных кодов нейросетевых преобразователей рукописных паролей «Вопросы защиты информации» 2008 № 3. с.27-31.
24. Ахметов Б.С., Иванов А.И., Фунтиков В.А., Малыгин А.Ю. Основы биометрической идентификации личности. Учебное пособие. КазНТУ им. К.И. Сатпаева, Алматы, 2014 г., 151 с. ISBN 978-601-228-689-2
25. Волчихин В.И., Ахметов Б.Б., Иванов А.И. Быстрый алгоритм симметризации корреляционных связей биометрических данных высокой размерности. Известия высших учебных заведений. Поволжский регион. Технические науки. – Пенза: ПГУ, №1, 2016 с. 3-7.
26. ГОСТ Р 52633.1-2009 «Защита информации. Техника защиты информации. Требования к формированию баз естественных биометрических образов, предназначенных для тестирования средств высоконадежной биометрической аутентификации»
27. ГОСТ Р 52633.2-2010 «Защита информации. Техника защиты информации. Требования к формированию синтетических биометрических образов, предназначенных для тестирования средств высоконадежной биометрической аутентификации»
28. Иванов А.И., Качалин С.А.. Обратная задача: обращение матриц нейросетевых функционалов в условиях информации только о связях и весах нейронов. Сборник научных статей «Десятой Всероссийской научно-технической конференции: Современные охранные технологии и средства обеспечения комплексной безопасности объектов» 7-9 октября, 2014 г. Пенза-Заречный. Изд-во ПГУ-2014 г. стр. 128-133.
29. Ахметов Б.С., Иванов А.И., Безяев А.В., Качалин С.В. Оценка вычислительной сложности обращения матриц нейросетевых функционалов. Доклады национальной академии наук республики Казахстан. 2014, №5, с. 49-61.
30. Галушкин А.И., Цыпкин Я.З. Нейронные сети: история развития. М. Радиотехника, 2001 г., 840 с.
31. Шалыгин А.С., Палагин Ю.И. Прикладные методы статистического моделирования. Л.: Машиностроение, 1986 г. – 320 с.

32. Малыгин А.Ю., Волчихин В.И., Иванов А.И., Фунтиков В.А. Быстрые алгоритмы тестирования нейросетевых механизмов биометрико-криптографической защиты информации /Пенза-2006 г., Издательство Пензенского государственного университета., 161 с.
33. Ахметов Б.С., Волчихин В.И., Иванов А.И., Малыгин А.Ю. Алгоритмы тестирования биометрико-нейросетевых механизмов защиты информации Казахстан, Алматы, КазНТУ им. Сатпаева, 2013 г.- 152 с. ISBN 978-101-228-586-4, http://portal.kazntu.kz/files/publicate/2014-01-04-11940.pdf
34. Ахметов Б.Б., Иванов А.И. Многомерные статистики существенно зависимых биометрических данных, порождаемые нейросетевыми эмуляторами квадратичных форм. Казахстан, Алматы, 2016 г., 56 с.
35. Кобзарь А.И. Прикладная математическая статистика. Для инженеров и научных работников. М.: ФИЗМАТЛИТ, 2006 г., 816 с.
36. Р 50.1.037-2002 Рекомендации по стандартизации. Прикладная статистика. Правила проверки согласия опытного распределения с теоретическим. Часть I. Критерии типа $\chi 2$. Госстандарт России. Москва-2001 г., 140 с.
37. Абезгауз Г.Г., Тронь А.П., Копенкин Ю.Н., Коровина И.А. Справочник по вероятностным расчетами. М.: Воениздат, 1970 г., 536 с.
38. Бронштейн И.Н., Семендяев К.А. Справочник по математике для инженеров и учащихся вузов. М.: «Наука», 1980, 974 с.
39. Иванов А.И. Биометрическая идентификация личности по динамике подсознательных движений. //Монография. Пенза. Изд-во ПГУ, 2000 г., 178 с.
40. Иванов А.И. Нейросетевые алгоритмы биометрической идентификации личности. Книга 15, серии «Нейрокомпьютеры и их применение» М.: Радиотехника 2004 г., 144 с.
41. Стюарт Рассел, Питер Норвиг. Искусственный интеллект. Современный подход. Москва-С.Перербург-Киев 2006 г. 1407 с.
42. Иванов А.И., Ложников П.С., Серикова Ю.И. Понижение размера обучающей выборки симметризацией корреляционных связей биометрических данных «Кибернетика и системный анализ», Том 52 с. №3 май-июнь, 2016 с. 49-56
43. Иванов А.И., Ложников П.С., Качайкин Е.И. Идентификация подлинности рукописных автографов сетями Байеса-Хэмминга и сетями квадратичных форм. «Вопросы защиты информации» №2 2015 г., с. 28-34
44. Иванов А.И., Ложников П.С., Качайкин Е.И., Сулавко А.Е. Биометрическая идентификация рукописных образов с использованием корреляционного аналога правила Байеса. «Вопросы защиты информации» №3 2015 г., с. 48-54.
45. Волчихин В.И., Иванов А.И., Серикова Ю.И. Компенсация методических погрешностей вычисления стандартных отклонений и коэффициентов корреляции, возникающих из-за малого объема выборок. Известия высших учебных заведений. Поволжский регион. Технические науки. – Пенза: ПГУ, №1, 2016 с. 45-49
46. Кулагин В.П., Иванов А.И., Серикова Ю.И. Корректировка методических и случайных составляющих погрешностей вычисления коэффициентов корреляции, возникающих на малых выборках биометрических данных // Информационные технологии. Москва, №9 Том. 22 -2016 г. с.705-710.
47. Иванов А.И., Серикова Ю.И. Номограммы оценки погрешности, коэффициентов корреляции, вычисленных на малых выборках биометрических данных. // Вопросы радиоэлектроники, № 2, 2015, с 123-130.

48. Волчихин В.И., Ахметов Б.Б., Иванов А.И., Серикова Ю.И. Фрактально-корреляционный функционал, используемый при поиске пар слабо зависимых биометрических данных в малых выборках. //Известия высших учебных заведений. Поволжский регион. Технические науки. – Пенза: ПГУ, 2016 − №3. − С 38-40.
49. Петерс Э. Хаос и порядок на рынках капитала. Новый аналитический взгляд на циклы, цены и изменчивость рынка. М.: Мир, 2000, 333 с.
50. Гильмутдинов А.Х. Фракталы и дробные операторы. Казань, Из-во Фэн Академии наук РТ, 2010 г., 488 с. ISBN 978-5-9690-0123-4.
51. Шредер М. Фракталы, хаос, степенные законы. Миниатюры из бесконечного рая. Ижевск. НИЦ «Регулярная и хаотическая динамика» 2005 г., 528 с. ISBN 5-93972-041-2.
52. Grassberger P., Procaccia I. Measuring the strangeness of strange attractors /Physica D, 1983/ - V.9, pp 188-208.
53. Перфилов К.А. Критерий среднего геометрического, используемый для проверки достоверности статистических гипотез распределения биометрических данных. Труды научно-технической конференции кластера пензенских предприятий, обеспечивающих безопасность информационных технологий. Том 9, Пенза-2014, с. 92-93 (http://www.pniei.penza.ru/RV-conf/T9/C92).
54. Перфилов К.А., Иванов А.И., Проценко Е.Д. Расширение многообразия статистических критериев, используемых при проверке гипотез распределения значений биометрических данных. // «Европейский союз ученых» № 13, 2015 г., часть 5, с. 9-12.
55. Иванов А.И., Перфилов К.А., Малыгина Е.А. Многомерный статистический анализ качества биометрических данных на предельно малых выборках с использованием критериев среднего геометрического, вычисленного для анализируемых функций вероятности // Измерение. Мониторинг. Управление. Контроль. Пенза. №2 (16) 2016, с. 155-164.
56. Иванов А.И., Перфилов К.А. Оценка соотношения мощностей семейства статистических критериев «среднего геометрического» на малых выборках биометрических данных. // Тезисы доклада, Одиннадцатая Всероссийская конференция «Современные охранные технологии и средства обеспечения комплексной безопасности объектов» 4-6 октября г. Заречный Пензенской области.
57. Иванов А.И., Малыгина Е.А., Перфилов П.А., Вятчанин С.Е. Сравнение мощности критерия среднего геометрического и Крамера-фон Мезиса на малях выборках биометрических данных. // Модели, системы, сети в экономике, технике, природе и обществе. №2 2016, с 155-158.
58. Иванов А. И., Газин А.И., Вятчанин С.Е., Перфилов К.А. Сравнение мощности хи-квадрат критерия и критерия Крамера-фон Мезиса для малых тестовых выборок биометрических данных «Надежность и качество сложных систем» №2, 2016 с. 67-73.
59. Серикова. Н.И. Эффект снижения размера тестовой выборки за счет перехода к многомерному статистическому анализу биометрических данных/ В.И. Волчихин, А.И. Иванов, Н.И. Серикова, Ю.В. Фунтикова // Известия высших учебных заведений. Поволжский регион. Технические науки. – Пенза: ПГУ, 2015 − №1. − С. 50 – 59
60. Серикова Н.И., Иванов А.И., Серикова Ю.И. Оценка правдоподобия гипотезы о нормальном распределении по критерию Джини для числа степеней свободы, кратного числу опытов //Вопросы радиоэлектроники. 2015. № 1 (1). С. 85-94.

61. Серикова. Н.И., Иванов А.И., Качалин С.В. Биометрическая статистика: сглаживание гистограмм, построенных на малой обучающей выборке. /Вестник СибГАУ 2014 № 3(55) с.146-150
62. Безяев А.В. Нейросетевой преобразователь в самокорректирующийся код, совершенно не обладающий избыточностью «Нейрокомпьютеры: разработка, применение» №3, 2012 с. 52-55
63. Безяев А.В., Иванов А.И., Фунтикова Ю.В. Оптимизация структуры самокорректирующегося био-кода, хранящего синдромы ошибок в виде фрагментов хеш-функций. «Вестник Уральского федерального округа. Безопасность в информационной сфере» 2014 г. № 3*(13)* с. 4-14.
64. Андреев Д.Ю., Иванов А.И., Захаров О.С., Хозин Ю.В. Модификация меры Хемминга через взвешивание мерой стабильности выходных данных нейросетевых преобразователей биометрия-код. «Нейрокомпьютеры: разработка, применение» №6, 2009 с. 49 – 52
65. Андреев Д.Ю. Оценка эффективности применения обычной и взвешанной метрики Хэмминга при упорядочивании баз естественных биометрических образов «Нейрокомпьютеры: разработка, применение» №3, 2012 с. 31-34
66. Елфимов А.В. Оценка эффективности восстановления рукописных образов человеко-машинным комплексом при высоких уровнях зашумления изображений. Труды научно-технической конференции кластера пензенских предприятий, обеспечивающих безопасность информационных технологий. Том 9, Пенза-2014, с 51-55, http://пниэи.рф/activity/science/BIT/T-9-p51.pdf.
67. Р.Морелос-Сарагоса Искусство помехоустойчивого кодирования М.: Техносфера, 2007 г., 320 с.
68. Питерсон У., Уэлдон Э. Коды, исправляющие ошибки /монография, под ред. Добрушиной Р.Л., Самойленко С.И. /-М.: МИР, 1976 г., 364 с.
69. Куликов С.В., Секретов М.В., Захаров О.С., Иванов А.И., Майоров А.В. Учет «тяжелых» хвостов ненормального закона распределения биометрических параметров все «Чужие» при настройке нелинейного элемента нейрона с несколькими дискретными состояниями «Нейрокомпьютеры: разработка, применение» №3, 2012 с. 56-59.
70. . Ахметов Б.Б., Иванов А.И., Перфилов К.А, Фунтикова Ю.В., Алибиева Ж.М. Эффект от параллельного статистического анализ биометрических данных двумя критериями Пирсона // Доклады Национальной академии наук Республики Казахстан.. – Алматы, 2015. № 2. С.18-25.
71. Иванов А.И., Ложников П.С., Качайкин Е.И. Идентификация подлинности рукописных автографов сетями Байеса-Хэмминга и сетями квадратичных форм. «Вопросы защиты информации» №2 2015 г., с. 28-34.
72. Качайкин Е.И., Иванов А.И. Идентификация авторства рукописных образов с использованием нейросетевого эмулятора квадратичных форм высокой размерности. «Вопросы кибербезопасности» № 4(12) 2015 с. 42-47.
73. Качайкин Е.И., Иванов А.И., Безяев А.В., Перфилов К.А. Оценка достоверности нейросетевой автоматизированной экспертизы рукописного почерка. «Вопросы кибербезопасности» № 2(10) 2015 с. 43-48.
74. Серикова. Н.И., Иванов А.И., Качалин С.В. Биометрическая статистика: сглаживание гистограмм, построенных на малой обучающей выборке. /Вестник СибГАУ 2014 № 3(55) с.146-150
75. Серикова, Н.И. Оценка правдоподобия гипотезы о нормальном распределении по критерию Джини для сглаженных гистограмм, построенных на малых тестовых выборках /Н.И. Серикова, А.И. Иванов,

Ю.И. Серикова //Вопросы радиоэлектроники – М.: ЦНИИ «Электроника», сер. СОИУ, 2015, вып. 1, с. 85 – 94.
76. Ахметов Б.С., Иванов А.И., Серикова Н.И., Фунтикова Ю.В. Алгоритм искусственного повышения числа степеней свободы при анализе биометрических данных по критерию согласия хи-квадрат. Вестник национальной академии наук республики Казахстан. №5, 2014 г. с. 28-:-34.
77. Ахметов Б.Б., Иванов А.И., Серикова Н.И., Фунтикова Ю.В. Дискретный характер закона распределения хи-квадрат критерия для малых тестовых выборок // Вестник Национальной академии наук Республики Казахстан. – Алматы, 2015. № 1. С. 17-25.
78. B. Akhmetov, A. Ivanov, A. Gilmutdinov, A. Bezyaev, Y. Funtikova. //The Family of Chi-Square Molecules Pearson: Software-Continuum Quantum Accelerators of High-Dimensional Calculations // 15th International Conference on Control, Automation and Systems (ICCAS 2015) to be held on October 13-16, 2015 in BEXCO, Busan, Korea (TP03 - Signals and Intelligent Systems, report № TP03-78 , october-15).
79. Кулагин В., Иванов А., Газин А., Ахметов Б. Циклические континуально-квантовые вычисления: усиление мощности хи-квадрат критерия на малых выборках. /Аналитика № 5, 2016 (30), с. 22-29.
80. ГОСТ Р 52633.0-2006 «Защита информации. Техника защиты информации. Требования к средствам высоконадежной биометрической аутентификации».
81. Marshalko G. B. On the security of a neural network-based biometric authentication scheme //Математические вопросы криптографии, 2014, том 5:2, 87–98.
82. Иванов А.И., Фунтиков В.А., Майоров А.В., Надеев Д.Н. Моделирование кодовых последовательностей с энтропией естественных и искусственных биометрических языков. Инфокоммуникационные технологии Том 8, № 4, 2010 г., с. 75-79, http://ikt.psuti.ru.
83. Малыгина Е.А., Иванов А.И., Язов Ю.К., Надеев Д.Н. Прогнозирование значений энтропии длинных кодовых последовательностей, порождаемых естественными и искусственными языками «Инфокоммуникационные технологии» том 12, № 2 2014, с.12-15.
84. Иванов А.И. Биометрическая идентификация личности по динамике подсознательных движений. //Монография. Пенза. Изд-во ПГУ, 2000 г., 178 с.
85. Волчихин В.И., Иванов А.И., Фунтиков В.А., Малыгина Е.А. Перспективы использования искусственных нейронных сетей с многоуровневыми квантователями в технологии биометрико-нейросетевой аутентификации // Известия высших учебных заведений. Поволжский регион. Технические науки. 2013, №4(28) С. 88 – 99.
86. Иванов А.И., Малыгина Е.А. Биометрическая аутентификация личности: обращение матриц нейросетевых функционалов в пространстве метрики Хемминга // Вопросы защиты информации. №1, 2015 г. с.23-29.
87. Тихонов А.Н., Арсенин В.Я. Методы решения некорректных задач. М.: Наука, 1979, 248 с.
88. Форсайт Дж., Молер К. Численное решение систем линейных алгебраических уравнений . М.: Мир, 1969 г.
89. Райс Дж. Матричные вычисления и математическое обеспечение. – М.: Мир, 1984 г. 412 с.
90. Иванов А.И. Квантовые компьютеры: прошлое, настоящее, будущее. // "Защита информации. INSAID" № 2 2015 г. с. с. 29-32.

91. Дональд Э. Кнут. Глава 3. Случайные числа // Искусство программирования— 3-е изд. — М.: Вильямс, 2000. — Т. 2. Получисленные алгоритмы. — 832 с. — ISBN 5-8459-0081-6.
92. Recommendation for Random Number Generation Using Deterministic Random Bit Generators NIST SP 800-90.
93. Иванов М.А., Чугунков И. В. Глава 4. Методика оценки качества генераторов ПСП // Теория, применение и оценка качества генераторов псевдослучайных последовательностей. — М.: КУДИЦ-ОБРАЗ, 2003. — 240 с. — ISBN 5-93378-056-1
94. A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications NIST SP 800-22
95. Боос В. Лекции по математике. Т 10. Перебор и эффективные алгоритмы. М.: Издательство URSS, 2014 г., 216 с.

СВЕДЕНИЯ ОБ АВТОРЕ:

Иванов Александр Иванович, начальник лаборатории биометрических и нейросетевых технологий (ЛБНТ) АО «ПНИЭИ», 440000, г. Пенза, ул. Советская, 9, телефон: (8412) 59-33-10, e-mail: ivan@pniei.penza.ru. Диссертацию доктора технических наук защитил в 2002 г. по специальности 05.13.01 - Системный анализ, управление и обработка данных. Диплом доцента по специальности 05.13.01 получен в 2009 г.

В период с 2008 г. по 2013 г. являлся экспертом без права голоса от России в двух международных комитетах ISO/IEC JTC1 SC37 (Биометрия) и ISO/IEC JTC1 SC27 (Техника защиты информации) в связи с тем, что был научным руководителем ряда НИР (Исполнитель - АО «ПНИЭИ», Заказчик - ФСТЭК России) по разработке пакета отечественных стандартов: ГОСТ Р52633.0-2006, ГОСТ Р 52633.1-2009, ГОСТ Р 52633.2-2010, ГОСТ Р 52633.3-2011, ГОСТ Р 52633.4-2012, ГОСТ Р 52633.5-2011, ГОСТ Р 52633.6-2013, ГОСТ Р 52633.7-20xx.

Примеры приложений обработки данных, использующие при вычислениях эффекты квантовой суперпозиции, воспроизведенные программными средствами среды инженерных расчетов MathCAD

Приложение №1

Вычисление значений спектральных составляющих выходных состояний хи-квадрат критерия (8 опытов, 4 столбца гистограммы) для нормального распределения значений средствами среды моделирования MathCAD

$i := 0..99999$

$xn8^{\langle i \rangle} := sort(rnorm(8,0,1))$

Создание выборки

$$xn8n^{\langle i \rangle} := \frac{xn8^{\langle i \rangle} - mean\left(xn8^{\langle i \rangle}\right)}{stdev\left(xn8^{\langle i \rangle}\right)}$$

Вычисление значения хи-квадрат

$$xi2_i := 8\left[\sum_{j=0}^{3} \frac{\left(\frac{hist\left(int, xn8n^{\langle i \rangle}\right)_j}{8} - P_j\right)^2}{P_j}\right]$$

$$hist\left(int, xn8n^{\langle 0 \rangle}\right) = \begin{pmatrix} 1 \\ 2 \\ 4 \\ 1 \end{pmatrix}$$

Гистограмма

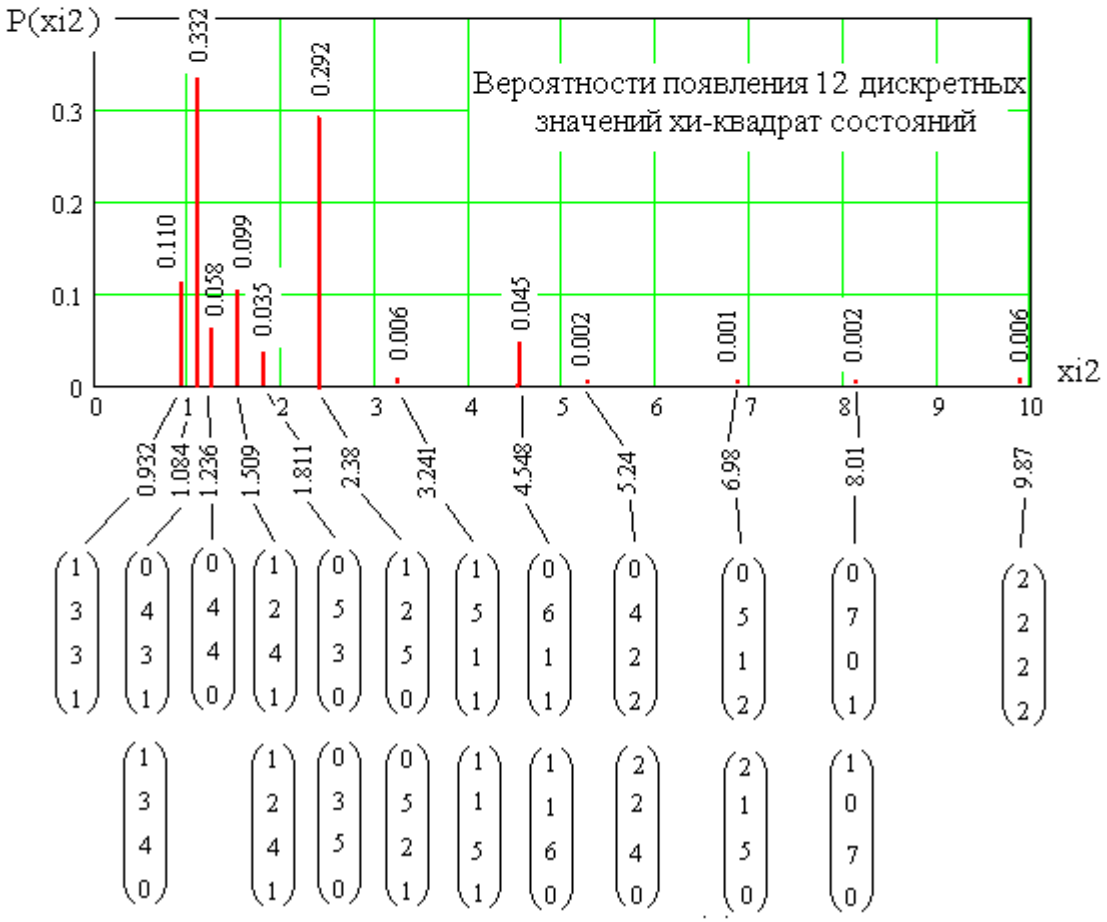
$$int := \begin{pmatrix} -3.1 \\ -1.5 \\ 0 \\ 1.5 \\ 3.1 \end{pmatrix}$$

Интервалы гистограммы

$$P := \begin{pmatrix} 0.067 \\ 0.433 \\ 0.433 \\ 0.067 \end{pmatrix}$$

Ожидаемые вероятности

$WRITEPRN("xi2.txt") := xi2$



Варианты различного размещения данных в 4-х интервалах гистограммы

Приложение №2 Переход от спектральных составляющих хи-квадрат квантователя (8 опытов, 4 столбца, нормальный закон) к параметрам эквивалентной квантовой суперпозиции средствами среды моделирования MathCAD

Переход из десятиченой в двоичную систему для симметричной гистограммы

$$P\begin{pmatrix}1\\3\\3\\1\end{pmatrix} = P\begin{pmatrix}001\\011\\011\\001\end{pmatrix} = 0.932 = P(\text{" 001 011 011 001"})$$

12 кубит первая линия

Гистограмы с дополняющей друг друга асимметрией

2 линия

$$P\begin{pmatrix}0\\4\\3\\1\end{pmatrix} = P\begin{pmatrix}000\\100\\011\\001\end{pmatrix} = P\begin{pmatrix}1\\3\\4\\0\end{pmatrix} = P\begin{pmatrix}001\\011\\100\\000\end{pmatrix} = 0.542$$

3 линия

$$P\begin{pmatrix}0\\4\\4\\0\end{pmatrix} = 0.618$$

4 линия

$$P\begin{pmatrix}1\\2\\4\\1\end{pmatrix} = P\begin{pmatrix}1\\4\\2\\1\end{pmatrix} = 0.045$$

5 линия

$$P\begin{pmatrix}0\\5\\3\\0\end{pmatrix} = P\begin{pmatrix}0\\3\\5\\0\end{pmatrix} = 0.018$$

6 линия

$$P\begin{pmatrix}1\\2\\5\\0\end{pmatrix} = P\begin{pmatrix}0\\5\\2\\1\end{pmatrix} = 0.146$$

7 линия

$$P\begin{pmatrix}1\\5\\1\\1\end{pmatrix} = P\begin{pmatrix}1\\1\\5\\1\end{pmatrix} = 0.0015$$

8 линия

$$P\begin{pmatrix}0\\6\\1\\1\end{pmatrix} = P\begin{pmatrix}1\\1\\6\\0\end{pmatrix} = 0.023$$

9 линия

$$P\begin{pmatrix}0\\4\\2\\2\end{pmatrix} = P\begin{pmatrix}2\\2\\4\\0\end{pmatrix} = 0.001$$

10 линия

$$P\begin{pmatrix}0\\5\\1\\2\end{pmatrix} = P\begin{pmatrix}2\\1\\5\\0\end{pmatrix} = 0.0005$$

11 линия

$$P\begin{pmatrix}0\\7\\0\\1\end{pmatrix} = P\begin{pmatrix}1\\0\\7\\0\end{pmatrix} = 0.001$$

12 линия

$$P\begin{pmatrix}2\\2\\2\\2\end{pmatrix} = 0.006$$

Итоговая квантовая суперпозиция

$$|\Psi\rangle = \sqrt{0.932}\cdot|001\,011\,011\,001\rangle + \sqrt{\frac{0.542}{2}}\cdot|000\,100\,011\,001\rangle + \sqrt{\frac{0.542}{2}}\cdot|001\,011\,100\,001\rangle +$$

$$+\sqrt{0.618}\cdot|000\,100\,100\,000\rangle + \sqrt{\frac{0.045}{2}}\cdot|001\,010\,100\,001\rangle + \sqrt{\frac{0.045}{2}}\cdot|001\,100\,010\,001\rangle +$$

$$+\sqrt{\frac{0.018}{2}}\cdot|000\,101\,011\,000\rangle + \sqrt{\frac{0.018}{2}}\cdot|000\,011\,101\,000\rangle + \ldots +$$

$$+ \ldots + \sqrt{0.006}\cdot|010\,010\,010\,010\rangle$$

Приложение №3 Пересчет всех линий хи-квадрат спектра в последовательность расстояний Хэмминга по отношению к коду первой линии спектра

$$h\left(\begin{pmatrix}1\\3\\3\\1\end{pmatrix},\begin{pmatrix}0\\4\\3\\1\end{pmatrix}\right)=h\left(\begin{pmatrix}1\\3\\3\\1\end{pmatrix},\begin{pmatrix}1\\3\\4\\0\end{pmatrix}\right)=4 \text{ бита}$$ до 2 линии

$$h\left(\begin{pmatrix}1\\3\\3\\1\end{pmatrix},\begin{pmatrix}0\\4\\4\\0\end{pmatrix}\right)=8 \text{ бит}$$ До 3 линии

$$h\left(\begin{pmatrix}1\\3\\3\\1\end{pmatrix},\begin{pmatrix}1\\2\\4\\1\end{pmatrix}\right)=h\left(\begin{pmatrix}1\\3\\3\\1\end{pmatrix},\begin{pmatrix}1\\2\\4\\1\end{pmatrix}\right)=4 \text{ бита}$$ До 4 линии

$$h\left(\begin{pmatrix}1\\3\\3\\1\end{pmatrix},\begin{pmatrix}0\\5\\3\\0\end{pmatrix}\right)=h\left(\begin{pmatrix}1\\3\\3\\1\end{pmatrix},\begin{pmatrix}0\\3\\5\\0\end{pmatrix}\right)=4 \text{ бита}$$ До 5 линии

$$h\left(\begin{pmatrix}1\\3\\3\\1\end{pmatrix},\begin{pmatrix}1\\2\\5\\0\end{pmatrix}\right)=h\left(\begin{pmatrix}1\\3\\3\\1\end{pmatrix},\begin{pmatrix}0\\5\\2\\1\end{pmatrix}\right)=4 \text{ бита}$$ До 6 линии

$$h\left(\begin{pmatrix}1\\3\\3\\1\end{pmatrix},\begin{pmatrix}1\\5\\1\\1\end{pmatrix}\right)=h\left(\begin{pmatrix}1\\3\\3\\1\end{pmatrix},\begin{pmatrix}1\\1\\5\\1\end{pmatrix}\right)=3 \text{ бита}$$ До 7 линии

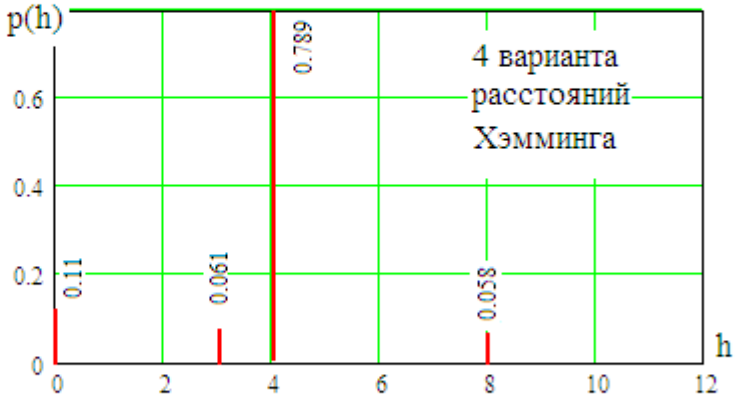
$$h\left(\begin{pmatrix}1\\3\\3\\1\end{pmatrix},\begin{pmatrix}0\\6\\1\\1\end{pmatrix}\right)=h\left(\begin{pmatrix}1\\3\\3\\1\end{pmatrix},\begin{pmatrix}1\\1\\6\\0\end{pmatrix}\right)=3 \text{ бита}$$ До 8 линии

$$h\left(\begin{pmatrix}1\\3\\3\\1\end{pmatrix},\begin{pmatrix}0\\4\\2\\2\end{pmatrix}\right)=h\left(\begin{pmatrix}1\\3\\3\\1\end{pmatrix},\begin{pmatrix}2\\2\\4\\0\end{pmatrix}\right)=4 \text{ бита}$$ До 9 линии

$$h\left(\begin{pmatrix}1\\3\\3\\1\end{pmatrix},\begin{pmatrix}0\\5\\1\\2\end{pmatrix}\right)=h\left(\begin{pmatrix}1\\3\\3\\1\end{pmatrix},\begin{pmatrix}2\\1\\5\\0\end{pmatrix}\right)=4 \text{ бита}$$ До 10 линии

$$h\left(\begin{pmatrix}1\\3\\3\\1\end{pmatrix},\begin{pmatrix}0\\7\\0\\1\end{pmatrix}\right)=h\left(\begin{pmatrix}1\\3\\3\\1\end{pmatrix},\begin{pmatrix}1\\0\\7\\0\end{pmatrix}\right)=3 \text{ бита}$$ До 11 линии

$$h\left(\begin{pmatrix}1\\3\\3\\1\end{pmatrix},\begin{pmatrix}2\\2\\2\\2\end{pmatrix}\right)=4 \text{ бита}$$ До 12 линии



Вероятности появления расстояний Хэмминга

Приложение № 4 Пересчет всех линий хи-квадрат спектра в последовательность расстояний Хэмминга по отношению к коду второй линии спектра

$$h\left(\begin{pmatrix}1\\3\\4\\0\end{pmatrix},\begin{pmatrix}1\\3\\3\\1\end{pmatrix}\right)=h\left(\begin{pmatrix}0\\4\\3\\1\end{pmatrix},\begin{pmatrix}1\\3\\3\\1\end{pmatrix}\right)=4\text{ бита}$$ до 1 линии

$$h\left(\begin{pmatrix}0\\4\\3\\1\end{pmatrix},\begin{pmatrix}0\\4\\4\\0\end{pmatrix}\right)=h\left(\begin{pmatrix}1\\3\\4\\0\end{pmatrix},\begin{pmatrix}0\\4\\4\\0\end{pmatrix}\right)=2\text{ бита}$$ До 3 линии

$$h\left(\begin{pmatrix}1\\3\\4\\0\end{pmatrix},\begin{pmatrix}1\\2\\4\\1\end{pmatrix}\right)=2\text{ бита}$$ До 4 линии

$$h\left(\begin{pmatrix}0\\4\\3\\1\end{pmatrix},\begin{pmatrix}1\\2\\4\\1\end{pmatrix}\right)=6\text{ бит}$$ До 4 линии

$$h\left(\begin{pmatrix}1\\3\\4\\0\end{pmatrix},\begin{pmatrix}0\\5\\3\\0\end{pmatrix}\right)=h\left(\begin{pmatrix}0\\4\\3\\1\end{pmatrix},\begin{pmatrix}0\\3\\5\\0\end{pmatrix}\right)=6\text{ бит}$$ До 5 линии

$$h\left(\begin{pmatrix}1\\3\\4\\0\end{pmatrix},\begin{pmatrix}1\\2\\5\\0\end{pmatrix}\right)=h\left(\begin{pmatrix}0\\4\\3\\1\end{pmatrix},\begin{pmatrix}0\\5\\2\\1\end{pmatrix}\right)=2\text{ бита}$$ До 6 линии

$$h\left(\begin{pmatrix}1\\3\\4\\0\end{pmatrix},\begin{pmatrix}1\\5\\1\\1\end{pmatrix}\right)=h\left(\begin{pmatrix}0\\4\\3\\1\end{pmatrix},\begin{pmatrix}1\\1\\5\\1\end{pmatrix}\right)=5\text{ бит}$$ До 7 линии

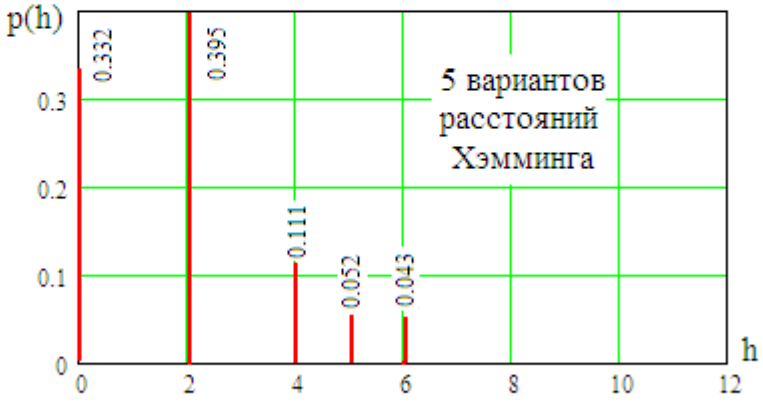
$$h\left(\begin{pmatrix}1\\3\\4\\0\end{pmatrix},\begin{pmatrix}0\\6\\1\\1\end{pmatrix}\right)=h\left(\begin{pmatrix}0\\4\\3\\1\end{pmatrix},\begin{pmatrix}1\\1\\6\\0\end{pmatrix}\right)=5\text{ бит}$$ До 8 линии

$$h\left(\begin{pmatrix}1\\3\\4\\0\end{pmatrix},\begin{pmatrix}0\\4\\2\\2\end{pmatrix}\right)=h\left(\begin{pmatrix}0\\4\\3\\1\end{pmatrix},\begin{pmatrix}2\\2\\4\\0\end{pmatrix}\right)=5\text{ бит}$$ До 9 линии

$$h\left(\begin{pmatrix}1\\3\\4\\0\end{pmatrix},\begin{pmatrix}0\\5\\1\\2\end{pmatrix}\right)=h\left(\begin{pmatrix}0\\4\\3\\1\end{pmatrix},\begin{pmatrix}2\\1\\5\\0\end{pmatrix}\right)=6\text{ бит}$$ До 10 линии

$$h\left(\begin{pmatrix}1\\3\\4\\0\end{pmatrix},\begin{pmatrix}0\\7\\0\\1\end{pmatrix}\right)=h\left(\begin{pmatrix}0\\4\\3\\1\end{pmatrix},\begin{pmatrix}1\\0\\7\\0\end{pmatrix}\right)=4\text{ бита}$$ До 11 линии

$$h\left(\begin{pmatrix}1\\3\\4\\0\end{pmatrix},\begin{pmatrix}2\\2\\2\\2\end{pmatrix}\right)=6\text{ бит}$$ До 12 линии



Вероятности появления расстояний Хэмминга

Приложение №5 Синтез данных с одинаковой коррелированностью для связывающей матрицы 7x7 средствами среды моделирования MathCAD

$a := 0.2071$ $i := 0..99999$

$x^{\langle i \rangle} := rnorm(7, 0, 1)$

$y^{\langle i \rangle} := A \cdot x^{\langle i \rangle}$

$$A := \begin{pmatrix} 1 & a & a & a & a & a & a \\ a & 1 & a & a & a & a & a \\ a & a & 1 & a & a & a & a \\ a & a & a & 1 & a & a & a \\ a & a & a & a & 1 & a & a \\ a & a & a & a & a & 1 & a \\ a & a & a & a & a & a & 1 \end{pmatrix}$$

$x0_i := (y^{\langle i \rangle})_0$ $x2_i := (y^{\langle i \rangle})_2$ $x4_i := (y^{\langle i \rangle})_4$ $x6_i := (y^{\langle i \rangle})_6$

$x1_i := (y^{\langle i \rangle})_1$ $x3_i := (y^{\langle i \rangle})_3$ $x5_i := (y^{\langle i \rangle})_5$

corr(x0,x1) = 0.498

corr(x0,x2) = 0.501 corr(x1,x2) = 0.502

corr(x0,x3) = 0.496 corr(x1,x3) = 0.497 corr(x2,x3) = 0.5

corr(x0,x4) = 0.499 corr(x1,x4) = 0.5 corr(x2,x4) = 0.5 corr(x3,x4) = 0.499

corr(x0,x5) = 0.5 corr(x1,x5) = 0.501 corr(x2,x5) = 0.501 corr(x3,x5) = 0.499 corr(x4,x5) = 0.5

corr(x0,x6) = 0.498 corr(x1,x6) = 0.502 corr(x2,x6) = 0.498 corr(x3,x6) = 0.498 corr(x4,x6) = 0.501

corr(x5,x6) = 0.499

Таблица зависимости коэффициентов равной коррелированности от параметра-а для симметричной связывающей матрицы 7x7

$$\begin{pmatrix} a \\ r \end{pmatrix} = \begin{pmatrix} 0.00487 & 0.0445 & 0.0844 & 0.1236 & 0.1653 & 0.2071 & 0.2555 & 0.3111 & 0.3861 & 0.5005 & 0.7877 \\ 0.01 & 0.1 & 0.2 & 0.3 & 0.4 & 0.5 & 0.6 & 0.7 & 0.8 & 0.9 & 0.99 \end{pmatrix}$$

Приложение № 6

Синтез данных с одинаковыми по модулю коэффициентами парных корреляций для связывающей матрицы 9х9 средствами среды моделирования MathCAD

$a := 0.2905$

$i := 0..99999$

$$A := \begin{pmatrix} 1 & -a & a & -a & a & -a & a & -a & a \\ -a & 1 & -a & a & -a & a & -a & a & -a \\ a & -a & 1 & -a & a & -a & a & -a & a \\ -a & a & -a & 1 & -a & a & -a & a & -a \\ a & -a & a & -a & 1 & -a & a & -a & a \\ -a & a & -a & a & -a & 1 & -a & a & -a \\ a & -a & a & -a & a & -a & 1 & -a & a \\ -a & a & -a & a & -a & a & -a & 1 & -a \\ a & -a & a & -a & a & -a & a & -a & 1 \end{pmatrix}$$

$x^{\langle i \rangle} := rnorm(9,0,1)$

$y^{\langle i \rangle} := A \cdot x^{\langle i \rangle}$

$x0_i := (y^{\langle i \rangle})_0$ $x1_i := (y^{\langle i \rangle})_1$ $x2_i := (y^{\langle i \rangle})_2$ $x3_i := (y^{\langle i \rangle})_3$ $x4_i := (y^{\langle i \rangle})_4$

$x5_i := (y^{\langle i \rangle})_5$ $x6_i := (y^{\langle i \rangle})_6$ $x7_i := (y^{\langle i \rangle})_7$ $x8_i := (y^{\langle i \rangle})_8$

$corr(x0,x1) = -0.698$

$corr(x0,x2) = 0.702$ $corr(x1,x2) = -0.701$

$corr(x0,x3) = -0.7$ $corr(x1,x3) = 0.7$ $corr(x2,x3) = -0.701$

$corr(x0,x4) = 0.699$ $corr(x1,x4) = -0.699$ $corr(x2,x4) = 0.7$ $corr(x3,x4) = -0.698$

$corr(x0,x5) = -0.7$ $corr(x1,x5) = 0.699$ $corr(x2,x5) = -0.702$ $corr(x3,x5) = 0.701$ $corr(x4,x5) = -0.701$

$corr(x0,x6) = 0.7$ $corr(x1,x6) = -0.699$ $corr(x2,x6) = 0.703$ $corr(x3,x6) = -0.699$ $corr(x4,x6) = 0.698$

$corr(x0,x7) = -0.7$ $corr(x1,x7) = 0.7$ $corr(x2,x7) = -0.702$ $corr(x3,x7) = 0.701$ $corr(x4,x7) = -0.699$

$corr(x0,x8) = 0.702$ $corr(x1,x8) = -0.7$ $corr(x2,x8) = 0.701$ $corr(x3,x8) = -0.7$ $corr(x4,x8) = 0.7$

$corr(x5,x6) = -0.701$

$corr(x5,x7) = 0.701$ $corr(x6,x7) = -0.702$

$corr(x5,x8) = -0.702$ $corr(x6,x8) = 0.699$ $corr(x7,x8) = 0.699$

Таблица зависимости модулей коэффициентов равной коррелированности от регулируемого ппараметра - а для симметричной связывающей матрицы 9х9

$$\begin{pmatrix} a \\ r \end{pmatrix} = \begin{pmatrix} 0.00462 & 0.0442 & 0.0816 & 0.1175 & 0.1545 & 0.1943 & 0.2375 & 0.2905 & 0.3610 & 0.4730 & 0.7651 \\ 0.01 & 0.1 & 0.2 & 0.3 & 0.4 & 0.5 & 0.6 & 0.7 & 0.8 & 0.9 & 0.99 \end{pmatrix}$$

Приложение № 7 Получение достоверных биометрических данных в среде моделирования "БиоНейроАвтограф" для выполнения последующих корректных вычислений с использованием квантовой суперпозиции

П7.1. Запуск среды моделирования "БиоНейроАвтограф"

Следует отметить, что задавать корректно биометрические данные достаточно сложно. Если пользоваться некоторым программным генератором данных, то всегда возникает вопрос о том, на сколько эти данные корректны. Для того, что бы снять вопрос о корректности получаемых биометрических данных была создана среда моделирования «БиоНейроАвтограф», на данный момент это единственный общедоступный инструмент для получения корректных биометрических данных как в русскоязычном сегменте Интернет, так и англоязычном сегменте Интернет. К сожалению, фирмы разработчики биометрических продуктов отказываются предоставлять открытый доступ к содержанию своих технических решений. То, что данные в среде моделирования «БиоНейроАвтограф» корректны каждый может убедиться самостоятельно, выполнив ряд лабораторных работ размещенных на сейте ОА «ПНИЭИ». То, что биометрические данные этого продукта общедоступны обеспечивается их открытым хранением в директории DATA среде моделирования «БиоНейроАвтограф», где в процессе работы сохраняются файлы:

- 3sigma.txt (содержит информацию о факте попадания биометрических данных каждого из 416 параметров в его допустимый интервал ±3σ);
- mean.txt (содержит запись среднего значения каждого из 416 контролируемых биометрич6еских параметров);
- mera.txt (содержит меры Хэмминга между кодом «trainKey» и кодом «trainKey», полученные при инициализации режима «проверить»);
- params.txt (содержит 416 биометрических параметров, учитываемых нейронной сетью);
- stdev.txt (содержит 416 стандартных отклонения биометрических параметров, учитываемых нейронной сетью);
- testKeys.txt (содержит данные о коде длинной 256 бит, полученном на выходах нейронной сети при предыдущих проверках);
- trainKey.txt (содержит данные о коде длинной 256 бит, использованном при обучении искусственной нейронной сети);
- weights.txt (содержит данные о 24 весах 256 нейронеов преобразователя биометрия-код, полученных в результате последнего обучения).

Для получения среду моделирования зайдите на страницу http://пниэи.рф/activity/science/noc.htm, скачайте архив bioneuroautograph.zip. Распакуйте архив и запустите находящийся в папке файл БиоНейроАвтограф.exe. При этом появится основная экранная форма с фотографией административного здания АО "ПНИЭИ" г. Пенза, улица Советская, 9.

П7.2. Как задать пароль доступа или криптографический ключ

Среда моделирования "БиоНейроАвтограф" предназначена для нейросетевого связывания рукописного пароля с обычным паролём доступа (набираемым на клавиатуре) или криптографическим ключом. Пароль доступа может быть изменён по усмотрению студента. Для того чтобы задать или

изменить пароль необходимо выбрать пункт меню "Режим", подпункт "Задать пароль" в левом верхнем углу основного диалогового окна (рис. П7.1). Или одновременно нажать комбинацию клавиш "Ctrl+P".

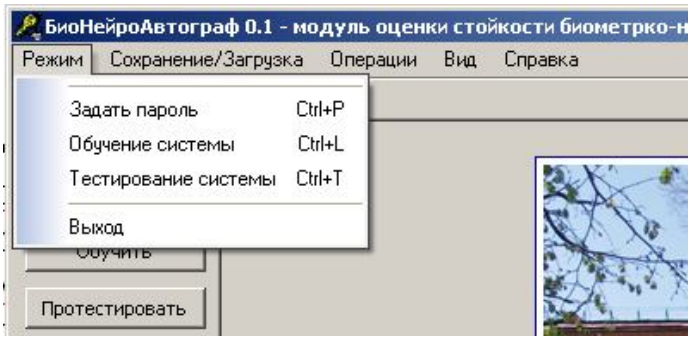


Рис. П7.1. Выбор пункта меню "Задать пароль".

При этом появится окно создания пользовательского пароля с двумя полями ввода (рис. П7.2). В верхнем поле введите имя пользователя (свой логин), в нижнем введите свой пароль, состоящий, например, из 32-х символов "a" в латинской кодировке.

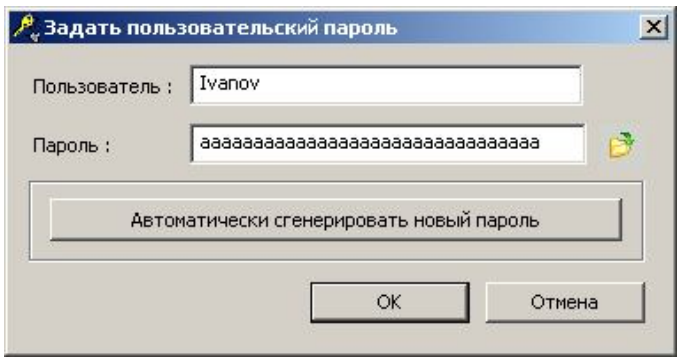


Рис. П7.2. Диалоговое окно создания пароля

Для создания длинного случайного пароля нажмите кнопку "Автоматически сгенерировать новый пароль". Сгенерированный 32-х символьный пароль при обучении преобразуется в обучающий ключ длиной 256 бит (32 случайных символа в 8 битной кодировке). Сохранение введённого имени пользователя и пароля происходит после нажатия кнопки "OK". В случае успешного сохранения данных можно приступать к обучению нейронной сети.

П7.3. Как обучить нейронную сеть

Обучение нейронной сети осуществляется в режиме обучения (рис. П7.3), который вызывается с помощь нажатия кнопки "Обучить" основного меню, либо выбором пункта меню "Режим", подпункт "Обучение системы", либо одновременным нажатием комбинации клавиш "Ctrl+L".

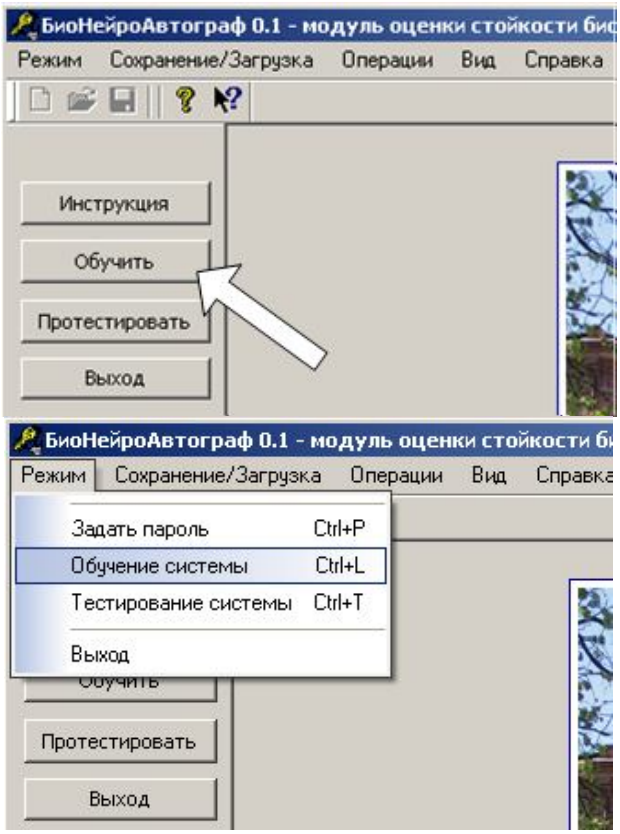


Рис. П7.3. Вызов режима обучения

Для того чтобы обучить нейронную сеть необходимо ввести несколько обучающих примеров той или иной рукописной буквы или рукописного слова. Если пользоваться манипулятором "мышь", то лучше вводить примеры отдельных букв, либо короткие слова, т.к. писать с помощью "мышки" достаточно сложно. Если имеется графический планшет, то для обучения необходимо вводить рукописное слово, состоящее из трех и более букв. При выборе обучающего символа или слова необходимо знать, что чем длиннее вводимое слово и чем выше стабильность его написания, тем выше стойкость обученной сети к атакам подбора. Так как с помощью манипулятора "мышь" вводить длинные стабильные слова невозможно, то качество обучения будет низким, а вероятности появления ошибок первого и второго рода высокими.

После входа в режим обучения введите с помощью манипулятора "мышь" или графического планшета несколько примеров выбранного для обучения рукописного слова или рукописной буквы.

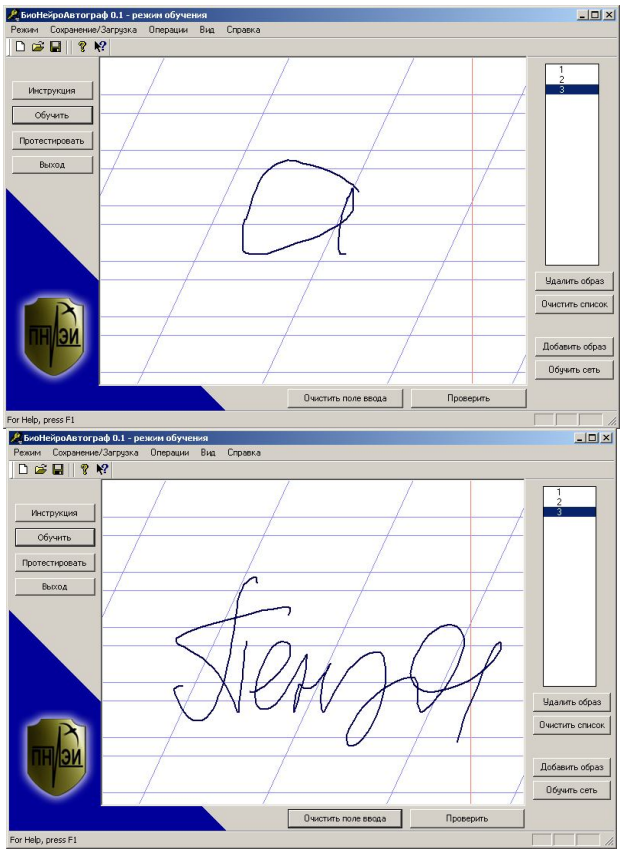


Рис. П7.4. Диалоговое окно обучения нейронной сети

После каждого ввода примера обучающего слова, необходимо добавить введённый пример в список обучающих примеров (список в правом верхнем углу диалогового окна обучения). Добавление примера осуществляется нажатием кнопки "Добавить образ" в правом нижнем углу диалогового окна.

Все ранее введенные примеры могут быть просмотрены щелчком манипулятора "мышь" по соответствующему номеру примера в списке обучающих примеров. Если добавленный в список пример неудачен (например, дрогнула рука), то его можно удалить. Для этого необходимо выбрать неудачный пример в списке обучающих примеров и нажать кнопку "Удалить образ". Чтобы удалить все обучающие примеры из списка нажмите кнопку "Очистить список".

Удаление текущего введённого рукописного образа и очистка поля ввода осуществляется с помощью кнопки "Очистить поле ввода".

После добавления в список обучающих примеров трёх или более примеров рукописного образа, запустите процесс обучения нейронной сети, нажав кнопку "Обучить сеть". Обучение сети из 256 нейронов длится менее одной секунды. По окончанию обучения появляется окно с результатами обучения (рис. П7.5), содержащее информацию о предполагаемой стабильности введенных биометрических примеров, вероятности узнавания образа "Свой" и ожидаемой стойкости системы к атакам подбора обучающего рукописного слова-пароля, т.е. вероятность пропуска образа "Чужой".

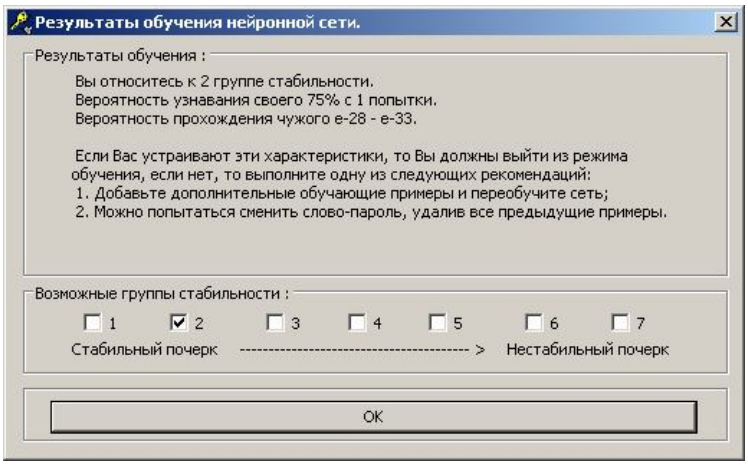


Рис. П7.5. Окно с результатами обучения

Можно попытаться изменить качество обучения, увеличивая или уменьшая число примеров обучения. Более точную оценку качества обучения можно дать только после тестирование искусственной нейронной сети. Доверие к результатам обучения, отображаемым в окне с результатами обучения, низкое, так как эти данные рассчитывались по обучающей выборке.

П7.4. Как проверить обученную нейронную сеть

Для того чтобы получить достоверную оценку качества обучения необходимо в поле ввода рукописных образов ввести пример рукописного образа "Свой" и нажать кнопку "Проверить". При этом вычисляются параметры введенного рукописного образа, они подаются на входы искусственной нейронной сети, вычисляется выходной код и выводится окно с результатами сравнения полученного выходного кода с обучающим кодом (рис. П7.6).

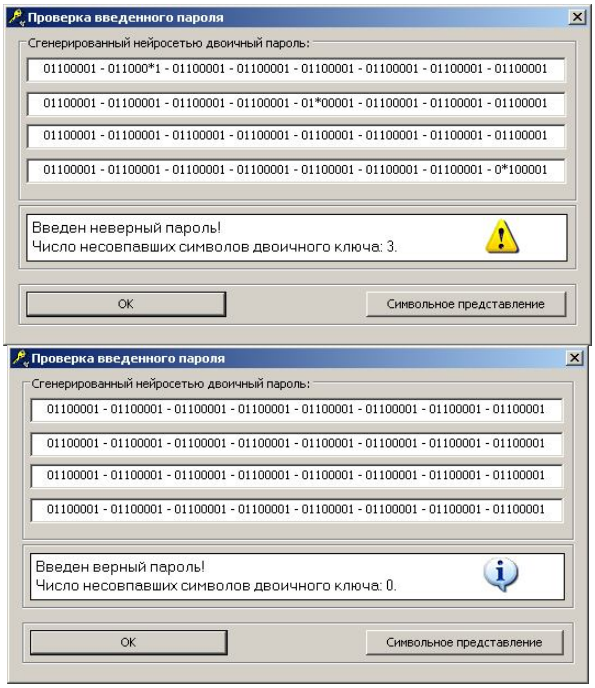


Рис. П7.6. Окно вывода полученного кода на примерах образа "Свой"

Сеть хорошо узнаёт образ "Свой", если мера Хемминга на тестовых примерах равно нулю (все разряды полученного кода совпадают с заданным при обучении кодом "Свой"). Если несколько бит кодов не совпадают, то обучение

нужно продолжить, добавив в обучающую выборку дополнительные примеры рукописного образа "Свой". Хорошо обученная нейронная сеть должна с высокой вероятностью узнавать образ "Свой".

Для проверки способности нейронной сети отказывать в доступе образам "Чужой" необходимо воспроизвести случайное рукописное слово (букву). При этом появляется случайный код, совпадающий с кодом "Свой" в случайных разрядах. В окне вывода полученного кода совпавшие разряды отображаются верными состояниями "0" и "1", а несовпавшие разряды отображаются символом "*" (рис. П7.7).

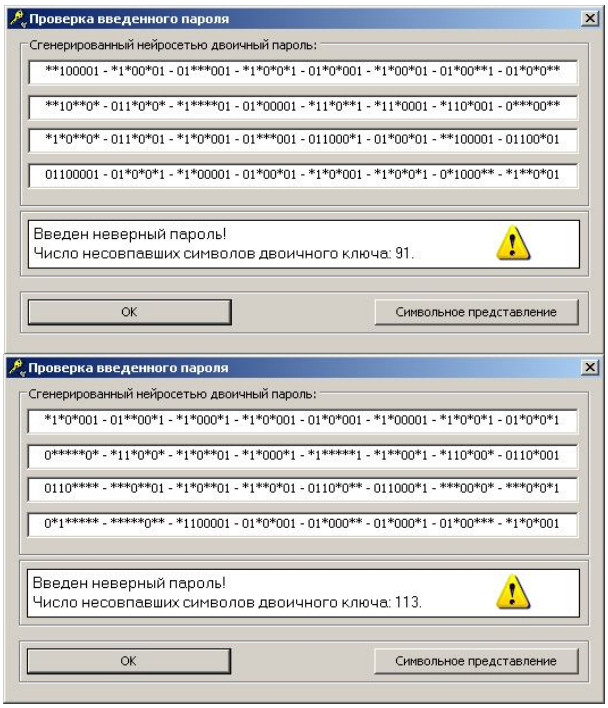


Рис. П7.7 Окно вывода полученного кода на примерах образа "Чужой"

Даже в том случае, когда воспроизводится один и тот же случайный рукописный образ "Чужой" выходные коды нейросети должны быть случайными (отличающиеся состояния должны располагаться в разных разрядах кодов).

Стойкость обученной нейронной сети тем выше, чем ближе число отличающихся разрядов кода к величине 128. Так как для действительно случайных состояниях выходного кода "Чужой" с наибольшей вероятностью угадывает примерно половину из 256 разрядов кода.

П.5. Как сохранить и загрузить биометрические образы

Для того чтобы надёжно тестировать качество работы обученного преобразователя биометрия-код нужно создавать специальные базы тестовых образов "Свой" и "Чужой" по требованиям ГОСТ Р 52633.1-2009. Средство моделирования большой нейронной сети "БиоНейроАвтограф" имеет встроенные средства, позволяющие собирать базы биометрических образов.

Сохранение обучающей выборки примеров "Свой" осуществляется путём выбора пункта меню "Сохранение/Загрузка", подпункта "Сохранить образы на диск", либо одновременным нажатием комбинации клавиш "Ctrl+S" (рис. П7.8).

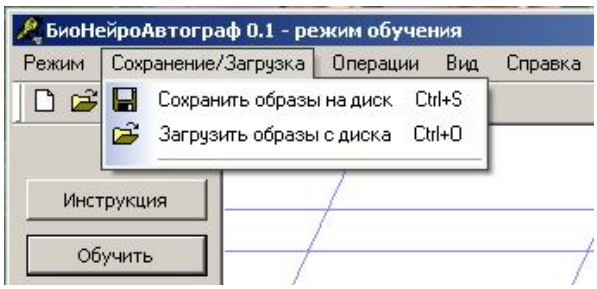


Рис. П7.8. Пункт меню сохранения и загрузки образов

Далее в открывшемся диалоговом окне укажите каталог, в котором будет сохранён файл, и задайте имя файла (по-умолчанию задано имя "MyImages.dat"). Рекомендуется примеры, на которых производилось обучение, сохранять с именем "Обучение__.dat", а примеры для тестирования обозначать именами "Тестирование_СВОЙ_.dat" или "Тестирование_ЧУЖИЕ_.dat".

После успешного сохранения можно удалить все обучающие примеры.

Сохранённые ранее примеры рукописных образов всегда можно загрузить и повторно обучить нейронную сеть. Загрузка рукописных образов осуществляется путём выбора пункта меню "Сохранение/Загрузка", подпункта "Загрузить образы с диска", либо одновременным нажатием комбинации клавиш "Ctrl+O" (рис. П7.8).

В появившемся диалоговом окне выберите требуемый файл с образами и нажмите кнопку "Открыть", загруженные примеры автоматически добавляются в список обучающих примеров.

Режим сохранения и загрузки рукописных образов крайне важен для формирования больших баз биометрических образов. У людей существует порог "комфортности" требований к ним со стороны биометрических автоматов. Мы легко пишем подряд десяток рукописных слов, однако требование воспроизвести подряд 20 одинаковых слов уже воспринимается людьми как некоторое обременение. Требование воспроизвести своею рукой 200 одинаковых слов людьми воспринимается как существенное обременение (нужно написать страницу рукописного текста). В связи с этим сохранение образов и обмен базами "все Чужие" – это мера, позволяющая существенно снизить трудоемкость лабораторных работ.

Следует иметь в виду, что режим "Сохранение/Загрузка" есть только у учебных средств моделирования искусственных нейронных сетей. Реальные средства биометрико-нейросетевой аутентификации должны уничтожать данные обучения и тестирования по требованиям ГОСТ Р 52633.0-2006.

П.6. Специальные режимы работы

П.6.1. Режим, воспроизводящий биометрическую аутентификацию

Среда моделирования "БиоНейроАвтограф" ориентирована на студентов занимающихся изучением применения нейросетевого искусственного интеллекта к приложениям защиты информации. В связи с этим в этой среде реализован режим, имитирующий меню программного средства биометрической аутентификации. Попасть в этот режим можно через основное меню, нажав кнопку "Протестировать", либо выбрав пункт меню "Режим", подпункт "Тестирование системы", либо одновременным нажатием комбинации клавиш "Ctrl+T". Главное диалоговое окно тестирования работы нейронной сети в режиме аутентификации пользователей представлено на рисунке П7.9.

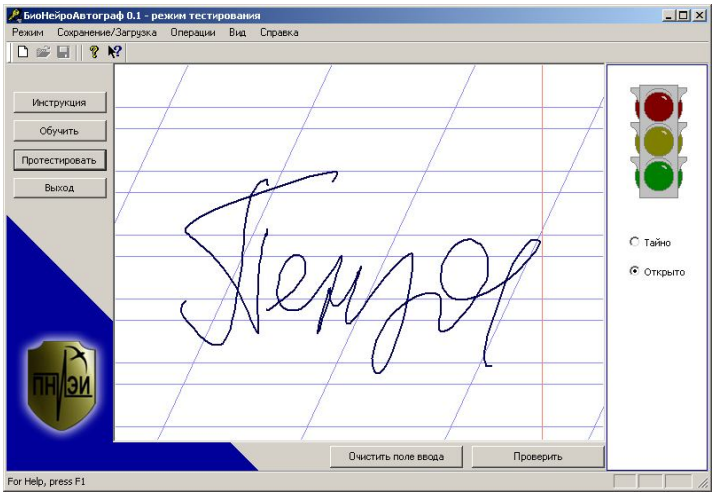


Рис. П7.9. Диалоговое окно режима тестирования

В правом верхнем углу диалогового окна расположен светофор с тремя состояниями: красный, жёлтый и зелёный. В случае положительного результата аутентификации загорается зелёный свет светофора. Если введённый биометрический образ близок к эталонному образу "Свой", загорается жёлтый свет светофора. Если введённый биометрический образ далек от эталонного образа "Свой", загорается красный свет. Светофор помогает пользователю "Свой" ориентироваться в текущем состоянии протокола биометрико-криптографической аутентификации. Индикатор состояния, выполненный в форме светофора безопасен, так как выполнен в соответствии с требованиями ГОСТ Р 52633.6.

Особенно важен светофор в режиме "Тайно", когда пользователь аутентифицируется по рукописному слову-паролю, которое не отображается на экране видеомонитора. Режим "Тайно" применяется пользователем в ситуации присутствия рядом с ним посторонних лиц. Режим "Открыто" применяется пользователем, когда он один, и никто не может подсмотреть его тайный рукописный пароль.

Основное отличие режима аутентификации от режимов обучения и тестирования состоит в том, что в этом режиме ключ "Свой" неизвестен, следовательно невозможно вычислить количество отличающихся бит ключа и показать их позиции. Так как в режиме аутентификации сравниваются не ключи/пароли, а хеш-код полученного ключа с хеш-кодом эталонного, то отображается только сигнал светофора и выводится сообщение с результатами проверки введённого пароля.

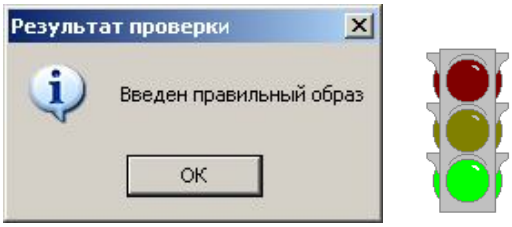


Рис. П7.10. Аутентификация пройдена

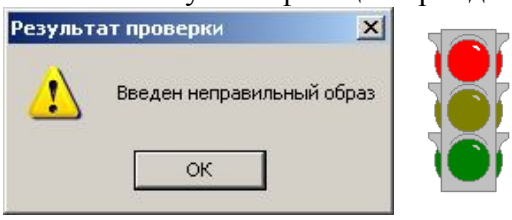


Рис. П7.11. Аутентификация не пройдена

Жёлтый сигнал светофора выдаётся вместе с сообщением "Введен неправильный образ".

П.6.2. Режим автоматического тестирования на базе тестовых образов

В случае, когда тестовая база создана заранее, можно воспользоваться специальным режимом тестирования на образах из базы. Для этого необходимо выбрать пункт меню "Операции", подпункт "Тестировать на тестовых образах" (рис. П7.12).

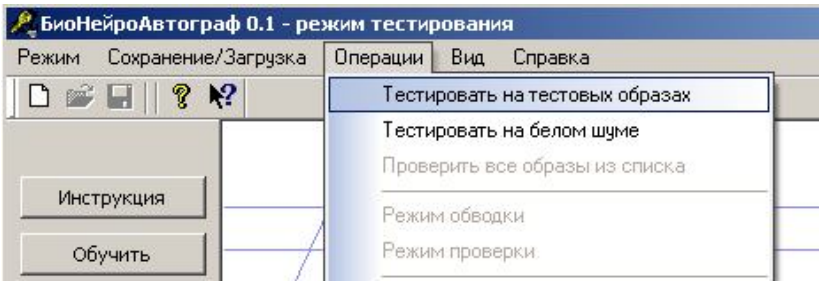


Рис. П7.12. Запуск тестирования на реальных образах

В результате появляется диалоговое окно выбора каталога, в котором хранятся файлы с тестовыми рукописными образами. После выбора нужного файла и нажатия кнопки "Открыть" запускается процесс тестирования обученной нейронной сети на выбранных образах. После завершения процесса тестирования выводится окно с результатами проверки (рис. П7.13).

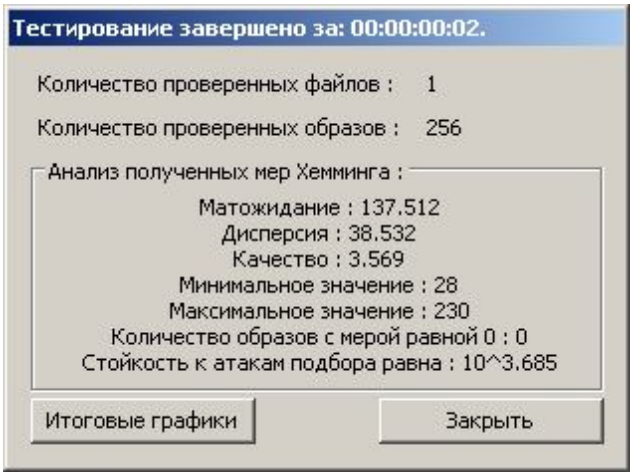


Рис. П7.13. Окно с результатами тестирования

Окно результатов содержит информацию о количестве использовавшихся во время тестирования примеров реальных рукописных образов, математическое ожидание, среднеквадратическое отклонение, качество, минимальное и максимальное значение полученных мер Хемминга. Также отображается количество "взломов" системы (количество образов с нулевой мерой) и вычисленная на тестовой базе стойкость к атакам подбора. Все вычисляемые во время тестирования меры Хемминга записываются в файл Data/<Имя_пользователя>/mera.txt. Каталог Data находится рядом с запускаемым файлом БиоНейроАвтограф.exe. После каждого тестирования происходит перезаписывание данных в файле mera.txt.

ПРИМЕЧАНИЕ. В каталоге Data также хранятся весовые коэффициенты обученной нейронной сети в файле weights.txt; а в файле coefs.txt хранятся

коэффициенты двухмерного преобразования Фурье последнего поданного на нейронную сеть примера биометрического образа.

П7.6.3. Режим автоматического тестирования на "белом шуме"

Если нет корректно собранной базы биометрических образов, то тестирование может быть выполнено на данных, получаемых от генератора случайного шума, т.е. тестирование на искусственно синтезированных образах. Для запуска тестирования на белом шуме необходимо выбрать пункт меню "Операции", подпункт "Тестировать на белом шуме" (рис. П7.14).

Рис. П7.14. Запуск тестирования на синтезированных образах

Тест запускается автоматически. Тестирование обученной нейронной сети осуществляется на 1 000 сгенерированных примерах рукописных образов. После завершения процесса тестирования выводится окно с результатами проверки (рис. П7.15).

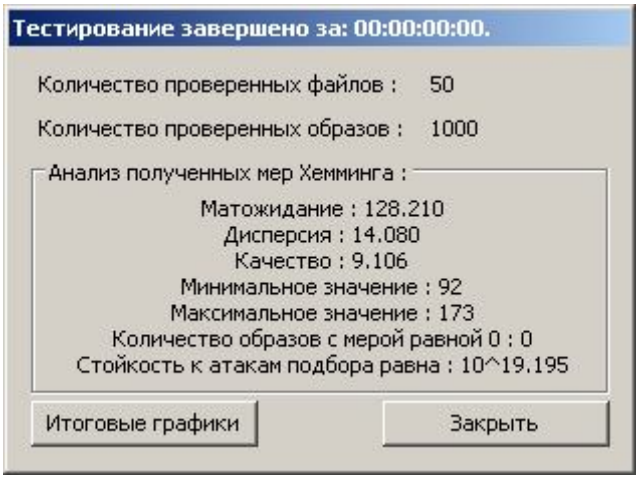


Рис. П7.15. Окно с результатами тестирования

Окно результатов содержит информацию о количестве использовавшихся во время тестирования примеров реальных рукописных образов, математическое ожидание, среднеквадратическое отклонение, качество, минимальное и максимальное значение полученных мер Хемминга. Также отображается количество "взломов" системы (количество образов с нулевой мерой) и вычисленная на тестовой базе стойкость к атакам подбора. Все вычисляемые во время тестирования меры Хемминга записываются в файл Data/<Имя_пользователя>/mera.txt. Каталог Data находится рядом с запускаемым файлом БиоНейроАвтограф.exe. После каждого тестирования происходит перезаписывание данных в файле mera.txt.

П.6.4. Режим проверки примеров из списка образов

Быстрая проверка всех примеров из списка обучающих примеров осуществляется выбором подпункта "Проверить все образы из списка" пункта меню "Операции". При этом все примеры из списка последовательно подаются на обученную нейронную сеть, вычисляется выходной код и сравнивается с эталонным. На экран выводится отчёт об общем количестве проверенных примеров и количестве примеров, распознанных как "Свой" и "Чужой". Данный режим подходит для быстрой оценки качества обучения нейронной сети. Позволяет увидеть, все ли обучающие примеры правильно распознаются как "Свой". Если есть тестовые примеры образа "Свой", то можно увидеть какова ошибка первого рода, т.е. какой процент примеров правильно распознан как "Свой" и неправильно отнесён в группу "Чужой".

Также в режиме обучения можно активировать режим быстрой проверки примеров из списка обучающих примеров. Для активации режима проверки необходимо выбрать пункт меню "Операции", подпункт "Режим проверки" (рис. П7.16). Деактивация осуществляется аналогично.

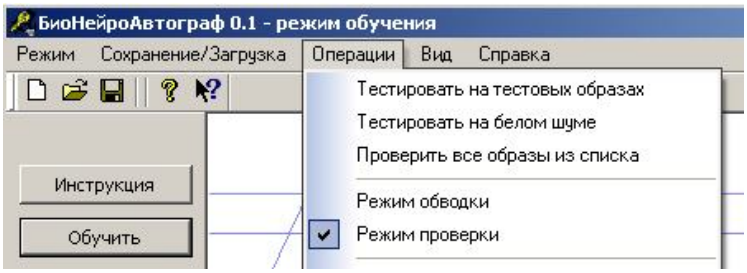


Рис. П7.16. Активация режима проверки

После активации в левом нижнем углу поля ввода рукописных образов появится красная надпись "Включён режим проверки". Теперь, если выбрать пример из списка, он будет автоматически подаваться на обученную нейронную сеть, вычисляться выходной код и сравниваться с эталонным, полученная мера Хемминга будет выводится в верхнем левом углу поля ввода.

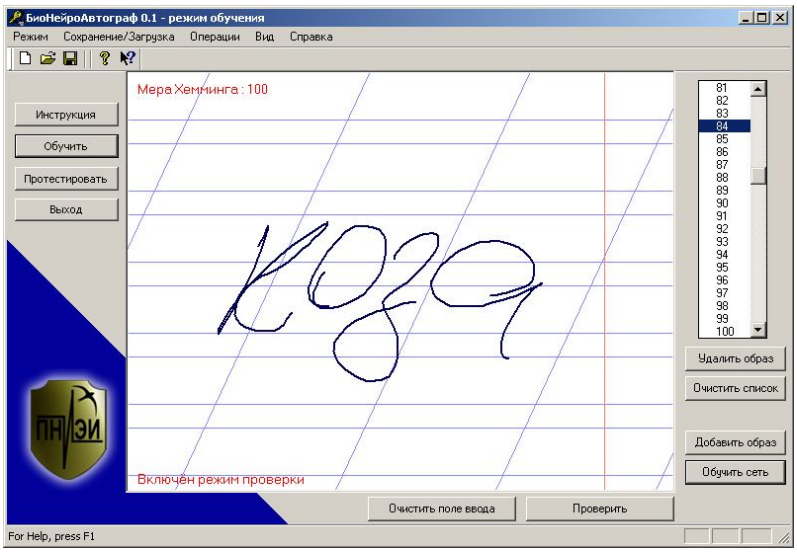


Рис. П7.17. Вычисление меры Хемминга образов в режиме проверки

Данный режим позволяет быстро вычислить меры Хемминга на всех примерах из списка, увидеть близкие и далёкие к обучающему примеру и оценить качество обучения нейронной сети.

П7.7. Завершение работы

Окончание работы среды моделирования "БиоНейроАвтограф" осуществляется нажатием крестика в верхнем правом углу главного диалогового окна. При этом появляется диалоговое окно с предложение завершить или продолжить работу (рис. П7.19).

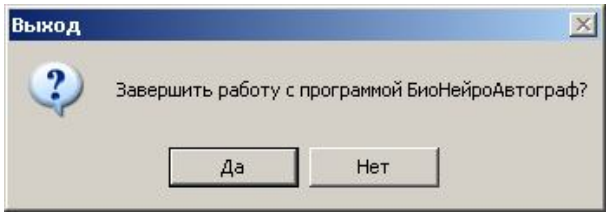


Рис. П7.19. Выход из программы

Для окончания работы необходимо нажать кнопку "Да".

Перед завершение работы необходимо сохранить обучающие примеры (если это необходимо). Все несохранённые данные после завершения работы приложения автоматически удаляются.

Приложение № 8 Оценка вероятности ошибок второго рода, обученного нейросетевого преобразователя рукописного пароля "Пенза" в код доступа длинной 256 бит (32 случайных символа)

h := (81 102 88 61 100 177 79 41 111 58 74 44 27 119 97 143 58 26 48 87 140 37 98 68 125 81

Расстояния Хэмминга 77 125 131 77 60 118)

mean(h) = 86.19 stdev(h) = 35.92

$$P2 := \frac{1}{35.92\sqrt{2\pi}} \cdot \int_{0}^{1} e^{\left[\frac{-(86.19-u)^2}{2\cdot 35.92^2}\right]} du$$

P2 = 0.00065 Оценка снизу

$$P2 := \frac{1}{35.92\sqrt{2\pi}} \cdot \int_{-100}^{1} e^{\left[\frac{-(86.19-u)^2}{2\cdot 35.92^2}\right]} du$$

P2 = 0.00885 Оценка сверху

Приложение № 9 Оценка достоверности гипотезы нормальности закона распределения значений расстояний Хэмминга для образов "Чужие" для выборки из 32 примеров

$h := (81\ \ 102\ \ 88\ \ 61\ \ 100\ \ 177\ \ 79\ \ 41\ \ 111\ \ 58\ \ 74\ \ 44\ \ 27\ \ 119\ \ 97\ \ 143\ \ 58\ \ 26\ \ 48\ \ 87\ \ 140\ \ 37\ \ 98\ \ 68\ \ 125\ \ 81$

Расстояния Хэмминга $77\ \ 125\ \ 131\ \ 77\ \ 60\ \ 118)$

$mean(h) = 86.19$ $stdev(h) = 35.92$ $min(h) = 26$

$max(h) = 177$

$i := 0..5$

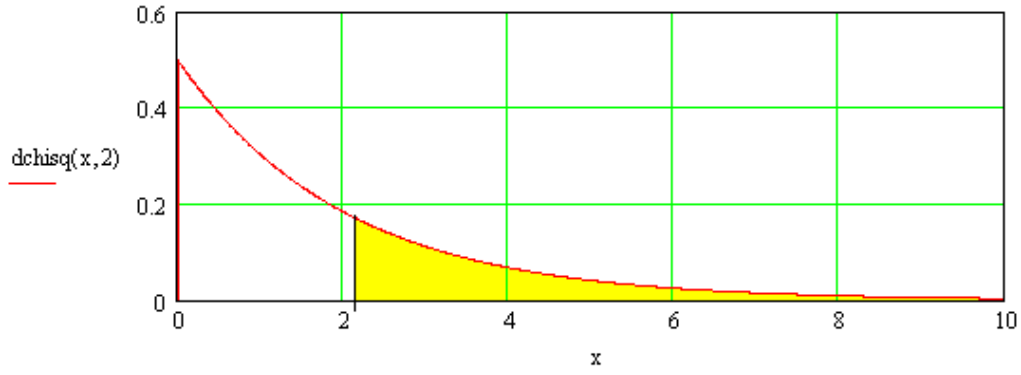
$int_i := 25 + 31 \cdot i$ $int = \begin{pmatrix} 25 \\ 56 \\ 87 \\ 118 \\ 149 \\ 180 \end{pmatrix}$ $hist(int, h) = \begin{pmatrix} 6 \\ 11 \\ 7 \\ 7 \\ 1 \end{pmatrix}$

$i := 0..4$

$$P_i := \frac{1}{35.92\sqrt{2\pi}} \cdot \int_{int_i}^{int_{i+1}} e^{\left[\frac{-(86.19-u)^2}{2\cdot 35.92^2}\right]} du \qquad P = \begin{pmatrix} 0.156 \\ 0.309 \\ 0.303 \\ 0.148 \\ 0.036 \end{pmatrix}$$

$$xi2 := 32\left[\sum_{i=0}^{4} \frac{\left(\frac{hist(int,h)_i}{32} - P_i\right)^2}{P_i}\right] \qquad xi2 = 2.19$$

$x := 0, 0.01..10$ $1 - pchisq(2.19, 2) = 0.335$ $pchisq(2.19, 2) = 0.665$



Вывод: для тестовой выборки из 32 примеров доверительная вероятность оценок приложения №8 составляет 0.665 , если пользоваться стандартными рекомендациями [36]

Приложение № 10 Необходимость корректировки таблиц доверительной вероятности критерия хи-квадрат на малых выборках

$i := 0..99999$

$xn32^{\langle i \rangle} := sort(rnorm(32,0,1))$

$m_i := mean(xn32^{\langle i \rangle})$

$s_i := stdev(xn32^{\langle i \rangle})$

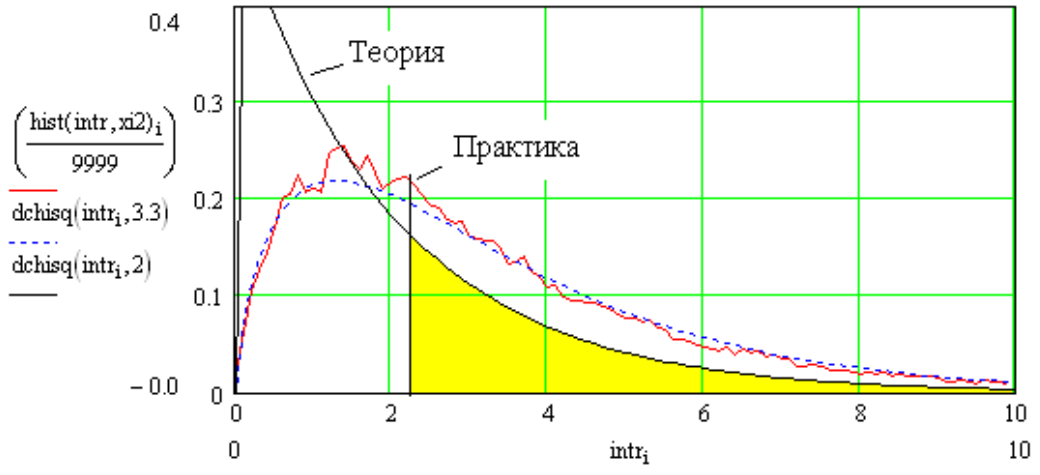
$$int_i := \begin{bmatrix} (xn32^{\langle i \rangle})_0 \\ (xn32^{\langle i \rangle})_0 + \frac{[(xn32^{\langle i \rangle})_{31} - (xn32^{\langle i \rangle})_0] \cdot 1}{5} \\ (xn32^{\langle i \rangle})_0 + \frac{[(xn32^{\langle i \rangle})_{31} - (xn32^{\langle i \rangle})_0] \cdot 2}{5} \\ (xn32^{\langle i \rangle})_0 + \frac{[(xn32^{\langle i \rangle})_{31} - (xn32^{\langle i \rangle})_0] \cdot 3}{5} \\ (xn32^{\langle i \rangle})_0 + \frac{[(xn32^{\langle i \rangle})_{31} - (xn32^{\langle i \rangle})_0] \cdot 4}{5} \\ (xn32^{\langle i \rangle})_{31} \end{bmatrix}$$

$$P^{\langle i \rangle} := \begin{bmatrix} pnorm[(int_i)_1, m_i, s_i] - pnorm[(int_i)_0, m_i, s_i] \\ pnorm[(int_i)_2, m_i, s_i] - pnorm[(int_i)_1, m_i, s_i] \\ pnorm[(int_i)_3, m_i, s_i] - pnorm[(int_i)_2, m_i, s_i] \\ pnorm[(int_i)_4, m_i, s_i] - pnorm[(int_i)_3, m_i, s_i] \\ pnorm[(int_i)_5, m_i, s_i] - pnorm[(int_i)_4, m_i, s_i] \end{bmatrix}$$

$$xi2_i := 32 \left[\sum_{j=0}^{4} \frac{\left[\frac{hist(int_i, xn32^{\langle i \rangle})_j}{32} - (P^{\langle i \rangle})_j \right]^2}{(P^{\langle i \rangle})_j} \right]$$

$i := 0..100$

$intr_i := 0 + 0.1 \cdot i$



Вывод. Доверительная вероятность для малых выборок, оцениваемая по стандартным рекомендациям Р 50.1.037-2002 [36] дает заниженные значения

Приложение № 11 Наблюдение дискретных компонент спектра хи-квадарт критерия для малой тестовой выборки из 32 примеров

$i := 0..99999$

$xn32^{\langle i \rangle} := sort(rnorm(32,0,1))$

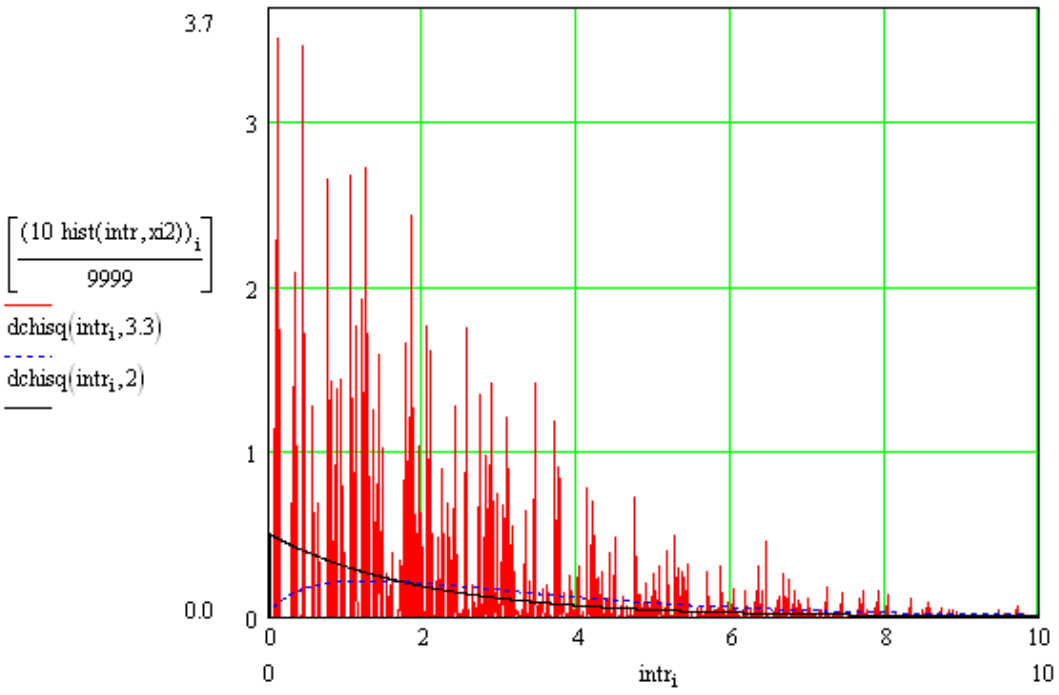
$xn32n^{\langle i \rangle} := \frac{xn32^{\langle i \rangle} - mean\left(xn32^{\langle i \rangle}\right)}{stdev\left(xn32^{\langle i \rangle}\right)}$

$$int := \begin{pmatrix} -3.3 \\ -1.8 \\ -0.6 \\ 0.6 \\ 1.8 \\ 3.3 \end{pmatrix} \qquad P := \begin{bmatrix} pnorm\left[\left(int_1\right),0,1\right] - pnorm\left[\left(int_0\right),0,1\right] \\ pnorm\left[\left(int_2\right),0,1\right] - pnorm\left[\left(int_1\right),0,1\right] \\ pnorm\left[\left(int_3\right),0,1\right] - pnorm\left[\left(int_2\right),0,1\right] \\ pnorm\left[\left(int_4\right),0,1\right] - pnorm\left[\left(int_3\right),0,1\right] \\ pnorm\left[\left(int_5\right),0,1\right] - pnorm\left[\left(int_4\right),0,1\right] \end{bmatrix}$$

$$xi2_i := 32\left[\sum_{j=0}^{4} \frac{\left(\frac{hist\left(int, xn32n^{\langle i \rangle}\right)_j}{32} - P_j\right)^2}{P_j}\right]$$

$i := 0..1000$

$intr_i := 0 + 0.01 \cdot i$



Приложение № 12 Наблюдение распределений ошибок вычисления математического ожидания, возникающих из-за ограниченного объема тестовой выборки

$i := 0..999999$

$x5^{\langle i \rangle} := rnorm(5,0,1)$ $m5_i := mean\left(x5^{\langle i \rangle}\right)$ $mean(m5) = 0.0002674$ $stdev(m5) = 0.447$

$x7^{\langle i \rangle} := rnorm(7,0,1)$ $m7_i := mean\left(x7^{\langle i \rangle}\right)$ $mean(m7) = -0.0002414$ $stdev(m7) = 0.378$

$x9^{\langle i \rangle} := rnorm(9,0,1)$ $m9_i := mean\left(x9^{\langle i \rangle}\right)$ $mean(m9) = 0.000238$ $stdev(m9) = 0.333$

$x11^{\langle i \rangle} := rnorm(11,0,1)$ $m11_i := mean\left(x11^{\langle i \rangle}\right)$ $mean(m11) = 0.0000297$ $stdev(m11) = 0.302$

$x16^{\langle i \rangle} := rnorm(16,0,1)$ $m16_i := mean\left(x16^{\langle i \rangle}\right)$ $mean(m16) = -0.0001541$ $stdev(m16) = 0.25$

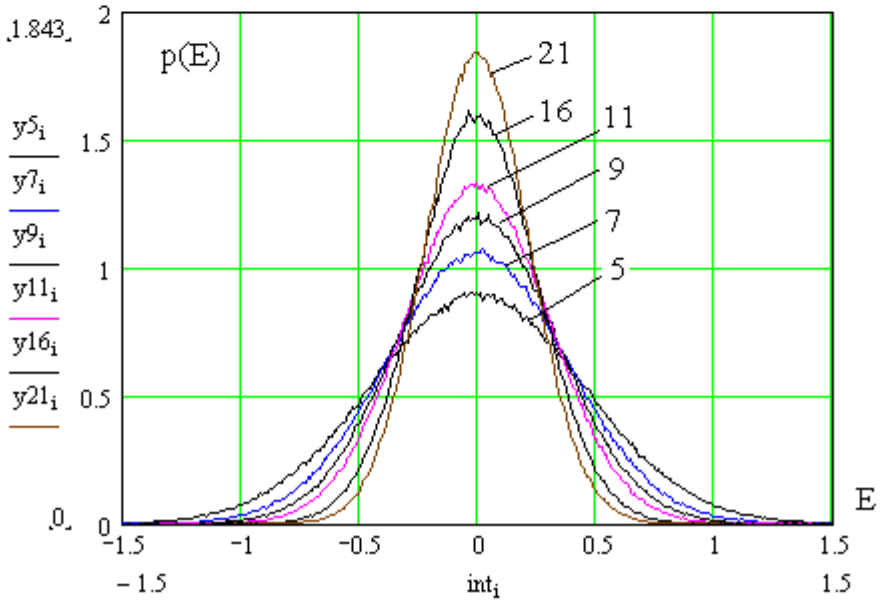
$x21^{\langle i \rangle} := rnorm(21,0,1)$ $m21_i := mean\left(x21^{\langle i \rangle}\right)$ $mean(m21) = 0.0002555$ $stdev(m21) = 0.218$

$i := 0..4000$

$int_i := -2 + 0.01 \cdot i$

$$y5 := \frac{hist(int, m5)}{9999} \qquad y7 := \frac{hist(int, m7)}{9999} \qquad y9 := \frac{hist(int, m9)}{9999}$$

$$y11 := \frac{hist(int, m11)}{9999} \qquad y16 := \frac{hist(int, m16)}{9999} \qquad y21 := \frac{hist(int, m21)}{9999}$$



Приложение № 13 Наблюдение плотностей распределения значений оценок стандартных отклонений для тестовых выборок разного объема

$i := 0 .. 999999$

$x5^{\langle i \rangle} := rnorm(5, 0, 1)$ $s5_i := stdev(x5^{\langle i \rangle})$ mean(s5) = 0.8409147

$x7^{\langle i \rangle} := rnorm(7, 0, 1)$ $s7_i := stdev(x7^{\langle i \rangle})$ mean(s7) = 0.8882948

$x9^{\langle i \rangle} := rnorm(9, 0, 1)$ $s9_i := stdev(x9^{\langle i \rangle})$ mean(s9) = 0.9139702

$x11^{\langle i \rangle} := rnorm(11, 0, 1)$ $s11_i := stdev(x11^{\langle i \rangle})$ mean(s11) = 0.9300257

$x16^{\langle i \rangle} := rnorm(16, 0, 1)$ $s16_i := stdev(x16^{\langle i \rangle})$ mean(s16) = 0.9523007

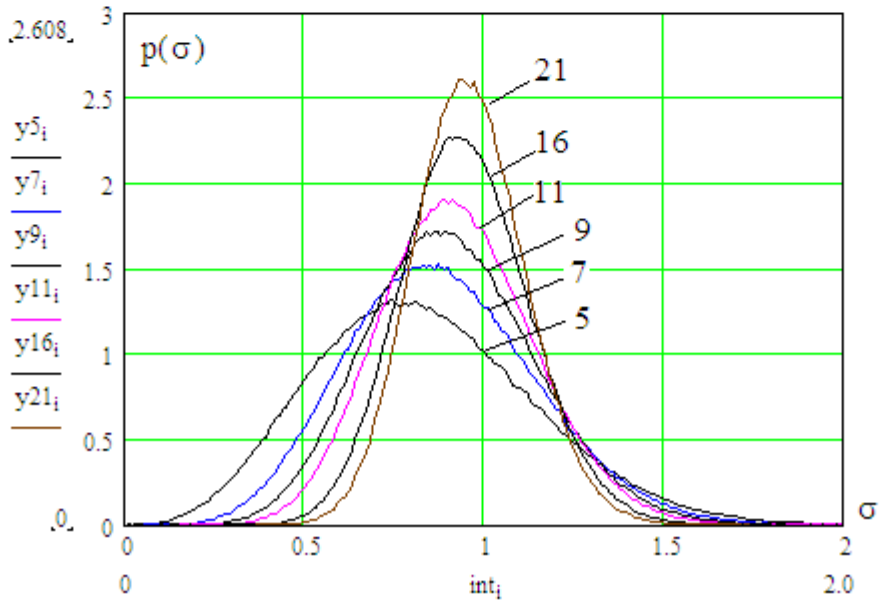
$x21^{\langle i \rangle} := rnorm(21, 0, 1)$ $s21_i := stdev(x21^{\langle i \rangle})$ mean(s21) = 0.963622

$i := 0 .. 4000$

$int_i := 0 + 0.01 \cdot i$

$y5 := \frac{hist(int, s5)}{9999}$ $y7 := \frac{hist(int, s7)}{9999}$ $y9 := \frac{hist(int, s9)}{9999}$

$y11 := \frac{hist(int, s11)}{9999}$ $y16 := \frac{hist(int, s16)}{9999}$ $y21 := \frac{hist(int, s21)}{9999}$



Приложение № 14

Компенсация методической погрешности оценки стандартного отклонения на малых тестовых выборках

$i := 0 .. 999999$

$x5^{\langle i \rangle} := rnorm(5, 0, 1)$ $\quad s5_i := \left(1.003 + \frac{1}{5}\right) \cdot stdev\left(x5^{\langle i \rangle}\right) - 0.011$ $\quad mean(s5) = 1.0001457$

$x7^{\langle i \rangle} := rnorm(7, 0, 1)$ $\quad s7_i := \left(1.003 + \frac{1}{7}\right) \cdot stdev\left(x7^{\langle i \rangle}\right) - 0.011$ $\quad mean(s7) = 1.0067774$

$x9^{\langle i \rangle} := rnorm(9, 0, 1)$ $\quad s9_i := \left(1.003 + \frac{1}{9}\right) \cdot stdev\left(x9^{\langle i \rangle}\right) - 0.011$ $\quad mean(s9) = 1.0068651$

$x11^{\langle i \rangle} := rnorm(11, 0, 1)$ $\quad s11_i := \left(1.003 + \frac{1}{11}\right) \cdot stdev\left(x11^{\langle i \rangle}\right) - 0.011$ $\quad mean(s11) = 1.0066092$

$x16^{\langle i \rangle} := rnorm(16, 0, 1)$ $\quad s16_i := \left(1.003 + \frac{1}{16}\right) \cdot stdev\left(x16^{\langle i \rangle}\right) - 0.011$ $\quad mean(s16) = 1.0035652$

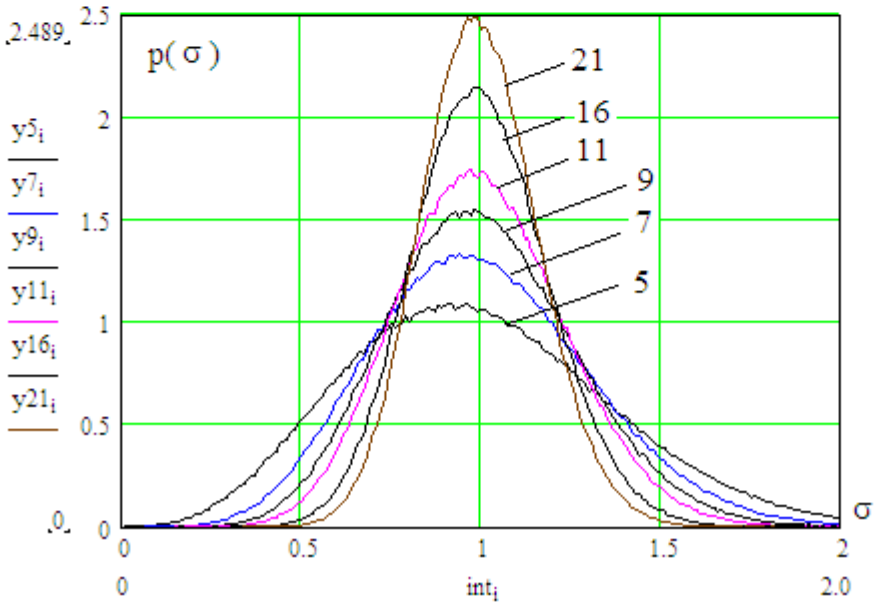
$x21^{\langle i \rangle} := rnorm(21, 0, 1)$ $\quad s21_i := \left(1.003 + \frac{1}{21}\right) \cdot stdev\left(x21^{\langle i \rangle}\right) - 0.011$ $\quad mean(s21) = 1.0011916$

$i := 0 .. 4000$

$int_i := 0 + 0.01 \cdot i$

$y5 := \frac{hist(int, s5)}{9999}$ $\quad y7 := \frac{hist(int, s7)}{9999}$ $\quad y9 := \frac{hist(int, s9)}{9999}$

$y11 := \frac{hist(int, s11)}{9999}$ $\quad y16 := \frac{hist(int, s16)}{9999}$ $\quad y21 := \frac{hist(int, s21)}{9999}$



Приложение № 15 Наблюдение распределений ошибок вычисления коэффициентов корреляции для выборки из 16 опытов

$i := 0..99999$ $x0^{\langle i \rangle} := rnorm(16, 0, 1)$ $x1^{\langle i \rangle} := rnorm(16, 0, 1)$

$a := 100$ $y^{\langle i \rangle} := \frac{x0^{\langle i \rangle} + a \cdot x1^{\langle i \rangle}}{\sqrt{1 + a^2}}$ $r00_i := corr\left(x0^{\langle i \rangle}, y^{\langle i \rangle}\right)$ $mean(r00) = 0.00934$

$a := 9.5$ $y^{\langle i \rangle} := \frac{x0^{\langle i \rangle} + a \cdot x1^{\langle i \rangle}}{\sqrt{1 + a^2}}$ $r01_i := corr\left(x0^{\langle i \rangle}, y^{\langle i \rangle}\right)$ $mean(r01) = 0.10084$

$a := 3.07$ $y^{\langle i \rangle} := \frac{x0^{\langle i \rangle} + a \cdot x1^{\langle i \rangle}}{\sqrt{1 + a^2}}$ $r03_i := corr\left(x0^{\langle i \rangle}, y^{\langle i \rangle}\right)$ $mean(r03) = 0.3$

$a := 1.67$ $y^{\langle i \rangle} := \frac{x0^{\langle i \rangle} + a \cdot x1^{\langle i \rangle}}{\sqrt{1 + a^2}}$ $r05_i := corr\left(x0^{\langle i \rangle}, y^{\langle i \rangle}\right)$ $mean(r05) = 0.5$

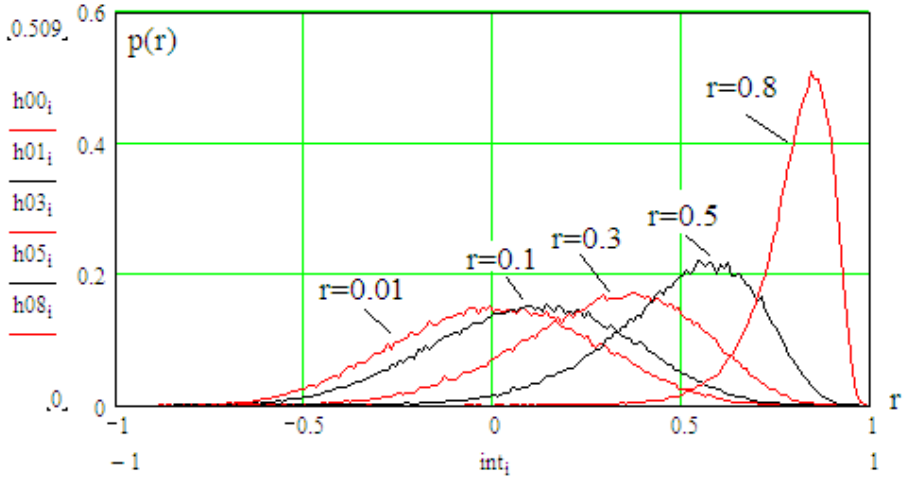
$a := 0.72$ $y^{\langle i \rangle} := \frac{x0^{\langle i \rangle} + a \cdot x1^{\langle i \rangle}}{\sqrt{1 + a^2}}$ $r08_i := corr\left(x0^{\langle i \rangle}, y^{\langle i \rangle}\right)$ $mean(r08) = 0.801$

$i := 0..200$

$int_i := -1 + 0.01 \cdot i$

$h00 := \frac{hist(int, r00)}{9999}$ $h01 := \frac{hist(int, r01)}{9999}$ $h03 := \frac{hist(int, r03)}{9999}$ $h05 := \frac{hist(int, r05)}{9999}$

$h08 := \frac{hist(int, r08)}{9999}$



Приложение № 16 Корректировка вычисления коэффициентов корреляции для слабо зависимых данных при объеме выборки в 16 опытов

$n := 16 \qquad d16 := 9.51 \qquad b16 := 3.40$

$x := rnorm(n,0,1) \qquad y := rnorm(n,0,1) \qquad corr(x,y) = -4.183 \times 10^{-3}$

$xn := \frac{x - min(x)}{max(x) - min(x)} \qquad yn := \frac{y - min(y)}{max(y) - min(y)} \qquad corr(xn,yn) = -4.183 \times 10^{-3}$

$R^{\langle 0 \rangle} := xn \qquad R^{\langle 1 \rangle} := yn \qquad RT := R^{T}$

$SRT0 := rsort(RT,0) \qquad SRT1 := rsort(RT,1)$

$sR0 := SRT0^{T} \qquad sR1 := SRT1^{T}$

$$D0 := \sum_{i=0}^{n-2} \left| \left(sR0^{\langle 1 \rangle}\right)_i - \left(sR0^{\langle 1 \rangle}\right)_{i+1} \right| \qquad D1 := \sum_{i=0}^{n-2} \left| \left(sR1^{\langle 0 \rangle}\right)_i - \left(sR1^{\langle 0 \rangle}\right)_{i+1} \right|$$

$r := corr(x,y) \qquad rf := \sqrt[3]{1 - \frac{D0 + D1}{d16}} \qquad DD := (r \;\; rf)$

$WRITEPRN("DD16\_r00.prn") := DD$ $\qquad APPENDPRN("DD16\_r00.prn") := DD$

$FR := READPRN("DD16\_r00.prn") \qquad corr\left(FR^{\langle 0 \rangle}, FR^{\langle 1 \rangle}\right) = -0.228 \qquad last\left(FR^{\langle 0 \rangle}\right) = 36$

$$kr := \left(1 - \frac{1}{b16}\right) \cdot FR^{\langle 0 \rangle} + \frac{FR^{\langle 1 \rangle}}{b16}$$

$mean\left(FR^{\langle 0 \rangle}\right) = -0.018834 \qquad stdev\left(FR^{\langle 0 \rangle}\right) = 0.207$

$mean(kr) = -0.043 \qquad stdev(kr) = 0.172$

Случайная ошибка снизилась в $\frac{stdev\left(FR^{\langle 0 \rangle}\right)}{stdev(kr)} = 1.203$ раз

Приложение № 17 Обучение нейрона с линейным функционалом обогощения входных данных алгоритмом близким к ГОСТ Р 52633.5

$n := 9$ при 9 входах (15 примеров образа "Свой" s1, ..., s15)

$v^{\langle 0 \rangle} := READPRN("s1.txt")$ $v^{\langle 1 \rangle} := READPRN("s2.txt")$ $v^{\langle 2 \rangle} := READPRN("s3.txt")$

$v^{\langle 3 \rangle} := READPRN("s4.txt")$ $v^{\langle 4 \rangle} := READPRN("s5.txt")$ $v^{\langle 5 \rangle} := READPRN("s6.txt")$

$v^{\langle 6 \rangle} := READPRN("s7.txt")$ $v^{\langle 7 \rangle} := READPRN("s8.txt")$ $v^{\langle 8 \rangle} := READPRN("s9.txt")$

$v^{\langle 9 \rangle} := READPRN("s10.txt")$ $v^{\langle 10 \rangle} := READPRN("s11.txt")$ $v^{\langle 11 \rangle} := READPRN("s12.txt")$

$v^{\langle 12 \rangle} := READPRN("s13.txt")$ $v^{\langle 13 \rangle} := READPRN("s14.txt")$ $v^{\langle 14 \rangle} := READPRN("s15.txt")$

$V := v^T$ $WRITEPRN("V.prn") := V$

Веса сумматора нейрона - 0

$$mu0 := \left| \begin{array}{l} \text{for } i \in 0..n-1 \\ \quad mu_i \leftarrow \dfrac{1}{stdev\left(V^{\langle i \rangle}\right)} \text{ if } mean\left(V^{\langle i \rangle}\right) \geq 0 \\ \quad mu_i \leftarrow \dfrac{-1}{stdev\left(V^{\langle i \rangle}\right)} \text{ if } mean\left(V^{\langle i \rangle}\right) < 0 \\ mu \end{array} \right.$$

Отклики сумматора нейрона - 0

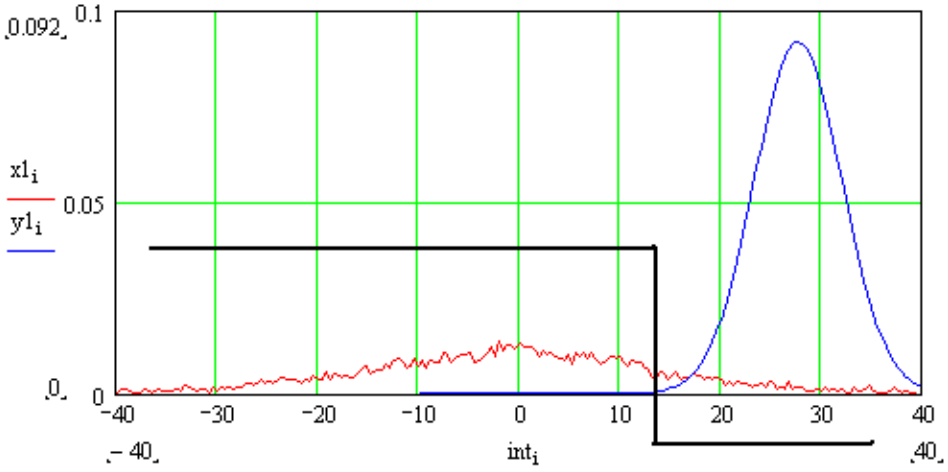
$$y(k) := \left| \begin{array}{l} \text{for } j \in 0..14 \\ \quad y_j \leftarrow \sum_{i=0}^{n-1} mu0_i \cdot \left(V^{\langle i+k \rangle}\right)_j \\ y \end{array} \right.$$

Порог срабатывания нейрона - 0

$k0 := mean(y(0)) - 3 \cdot stdev(y(0))$ $k0 = 14.607$

$k := 0..(416 - n)$ $Y^{\langle k \rangle} := y(k)$

$i := 0..200$ $int_i := -40 + 0.4 \cdot i$ $x1 := \dfrac{hist(int, Y)}{6240 - 9 \cdot 15}$ $y1_i := dnorm\left(int_i, mean(y(0)), stdev(y(0))\right)$

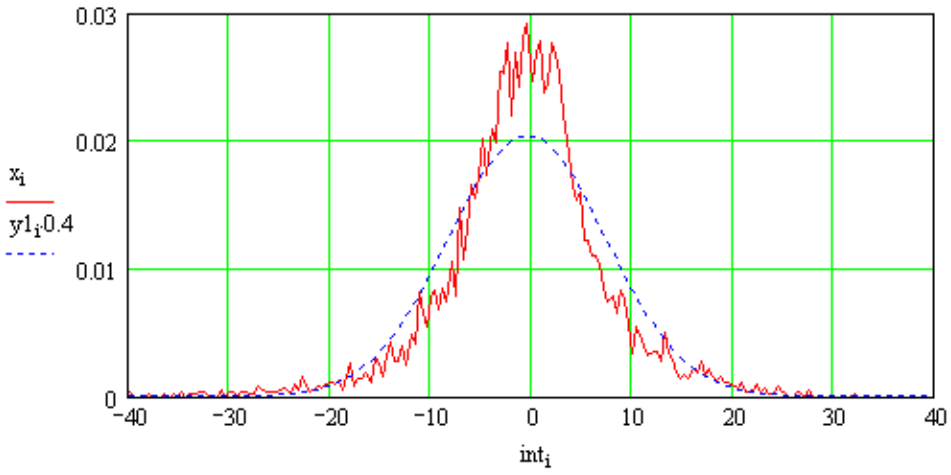


Приложение № 18 Учет "тяжелых" хвостов распеделения биометрических данных рукописного образа

$V := READPRN("V.prn")$

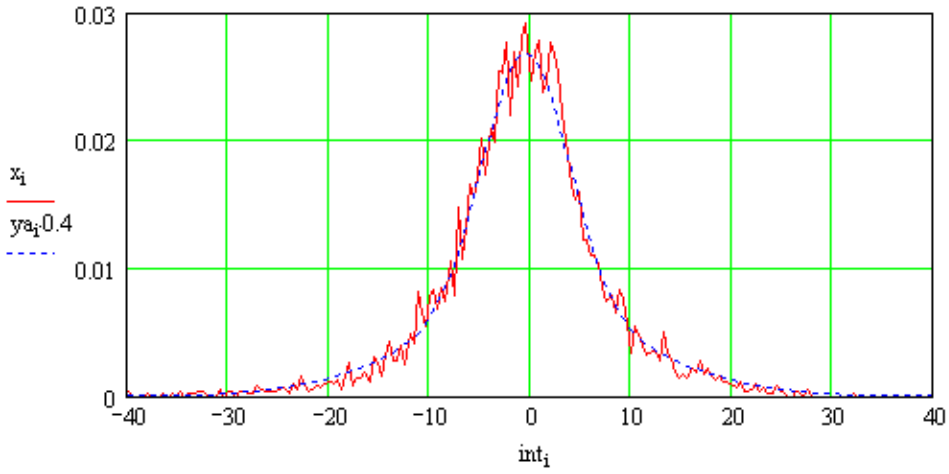
$i := 0..200$

$int_i := -40 + 0.4 \cdot i$ $\qquad x := \frac{hist(int, V)}{6240}$ $\qquad y1_i := dnorm(int_i, mean(V), stdev(V))$



Приближение распределения данных смесью двух нормальных законов

$ya_i := 0.45 \cdot dnorm(int_i, mean(V), 1.45 \cdot stdev(V)) + 0.55 \cdot dnorm(int_i, mean(V), 0.55 \cdot stdev(V))$



Приложение № 19 Наблюдение распределения коэффициентов корреляции реальных биометрических данных рукописного образа

$V := READPRN("V.prn")$

$i := 1..415 \quad r_{i-1} := corr\left(V^{\langle 0 \rangle}, V^{\langle i \rangle}\right) \quad last(r) = 414$

$i := 414..414 + 413 \quad r_{i-1} := corr\left(V^{\langle 1 \rangle}, V^{\langle i-414 \rangle}\right) \quad last(r) = 826$

$i := 826..826 + 412 \quad r_{i-1} := corr\left(V^{\langle 2 \rangle}, V^{\langle i-826 \rangle}\right) \quad last(r) = 1238$

$i := 1238..1238 + 411 \quad r_{i-1} := corr\left(V^{\langle 3 \rangle}, V^{\langle i-1238 \rangle}\right) \quad last(r) = 1649$

$i := 1649..1649 + 410 \quad r_{i-1} := corr\left(V^{\langle 4 \rangle}, V^{\langle i-1649 \rangle}\right) \quad last(r) = 2059$

$i := 2059..2059 + 409 \quad r_{i-1} := corr\left(V^{\langle 5 \rangle}, V^{\langle i-2059 \rangle}\right) \quad last(r) = 2468$

$i := 2468..2468 + 408 \quad r_{i-1} := corr\left(V^{\langle 6 \rangle}, V^{\langle i-2468 \rangle}\right) \quad last(r) = 2876$

$i := 2876..2876 + 407 \quad r_{i-1} := corr\left(V^{\langle 7 \rangle}, V^{\langle i-2876 \rangle}\right) \quad last(r) = 3283$

$i := 3283..3283 + 406 \quad r_{i-1} := corr\left(V^{\langle 8 \rangle}, V^{\langle i-3283 \rangle}\right) \quad last(r) = 3689$

$i := 3689..3689 + 405 \quad r_{i-1} := corr\left(V^{\langle 9 \rangle}, V^{\langle i-3689 \rangle}\right) \quad last(r) = 4094$

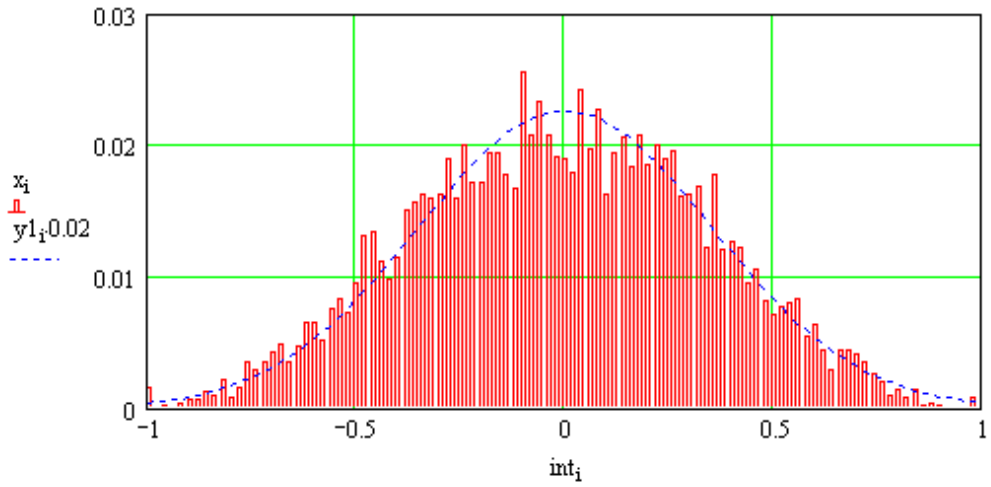
$i := 4094..4094 + 404 \quad r_{i-1} := corr\left(V^{\langle 10 \rangle}, V^{\langle i-4094 \rangle}\right) \quad last(r) = 4498$

$i := 4498..4498 + 403 \quad r_{i-1} := corr\left(V^{\langle 11 \rangle}, V^{\langle i-4498 \rangle}\right) \quad last(r) = 4900$

$i := 0..100$

$WRITEPRN("r.prn") := r$

$int_i := -1 + 0.02 \cdot i \qquad x := \frac{hist(int, r)}{last(r)} \qquad y1_i := dnorm\left(int_i, mean(r), stdev(r)\right)$

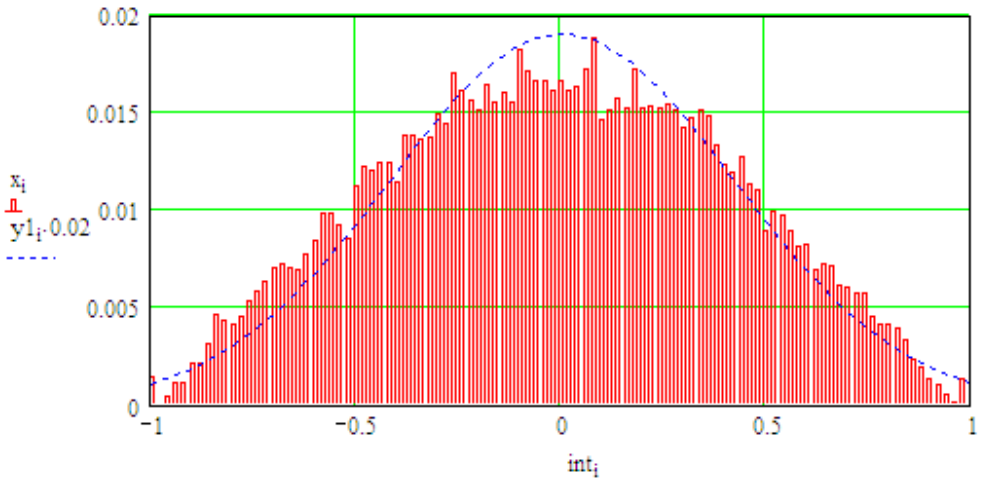


Приложение № 20 Учет плоской вершины распределения коэффициентов парной корреляции параметров биометрического образа

WRITEPRN("r.prn") := r last(r) = 32041

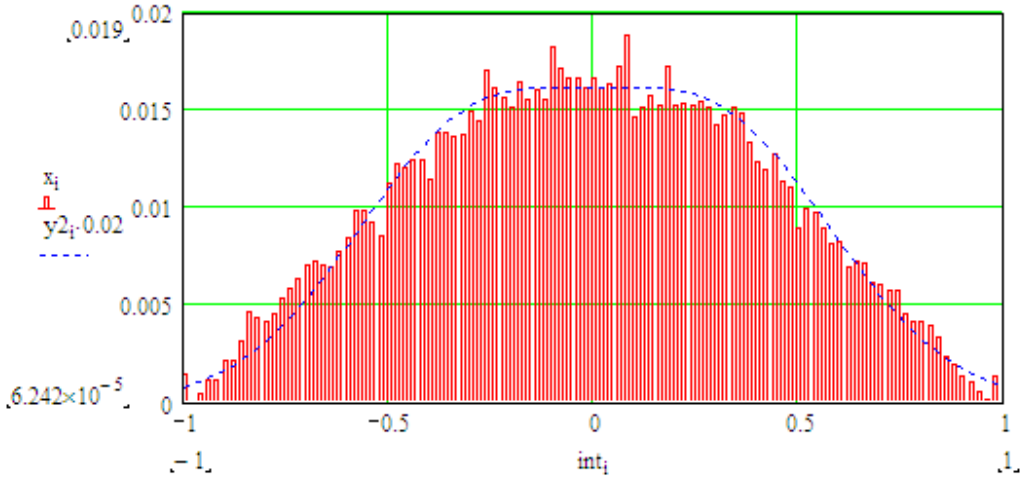
$i := 0..100$

$int_i := -1 + 0.02 \cdot i$ $x := \frac{hist(int, r)}{last(r)}$ $y1_i := dnorm(int_i, mean(r), stdev(r))$



$a := 0.3$

$y2_i := 0.5 \cdot dnorm[int_i, mean(r) - a, (1 - a) \cdot stdev(r)] + 0.5 \cdot dnorm[int_i, mean(r) + a, (1 - a) \cdot stdev(r)]$



Приложение № 21 Обучение нейронов по ГОСТ Р 52633.5 при использовании линейных функционалов обогащения с 9 входами

$n := 9$

$V := READPRN("V.prn")$

Вычисление весовых коэффициентов нейронов

$$mu(k) := \begin{| mu \leftarrow \frac{1}{stdev(V^{\langle k \rangle})} \text{ if } mean(V^{\langle k \rangle}) \geq 0 \\ mu \leftarrow \frac{-1}{stdev(V^{\langle k \rangle})} \text{ if } mean(V^{\langle k \rangle}) < 0 \\ mu \end{|}$$

$i := 0..255$

$MU_i := mu(i)$

$WRITEPRN("MU.prn") := MU$

Вычисление откликов нейронов на примеры "Свой"

$$yn(k,m) := \begin{| y \leftarrow \sum_{i=0}^{n-1} \left[MU_{i+m} \cdot \left(V^{\langle i+m \rangle} \right)_k \right] \\ y \end{|}$$

$c := last(V^{\langle 0 \rangle})$ $i := 0..c$

$YN_i := yn(i,0)$ $YN_{i+c} := yn(i,1)$ $YN_{i+2c} := yn(i,2)$ $YN_{i+3c} := yn(i,3)$ $YN_{i+4c} := yn(i,4)$

$YN_{i+5c} := yn(i,5)$ $YN_{i+6c} := yn(i,6)$ $YN_{i+7c} := yn(i,7)$ $YN_{i+8c} := yn(i,8)$ $YN_{i+9c} := yn(i,9)$

$YN_{i+10c} := yn(i,10)$ $YN_{i+10c} := yn(i,10)$ $YN_{i+11c} := yn(i,11)$ $YN_{i+12c} := yn(i,12)$ $YN_{i+13c} := yn(i,13)$

$YN_{i+14c} := yn(i,14)$ $YN_{i+15c} := yn(i,15)$ $YN_{i+16c} := yn(i,16)$ $YN_{i+17c} := yn(i,17)$ $YN_{i+18c} := yn(i,18)$

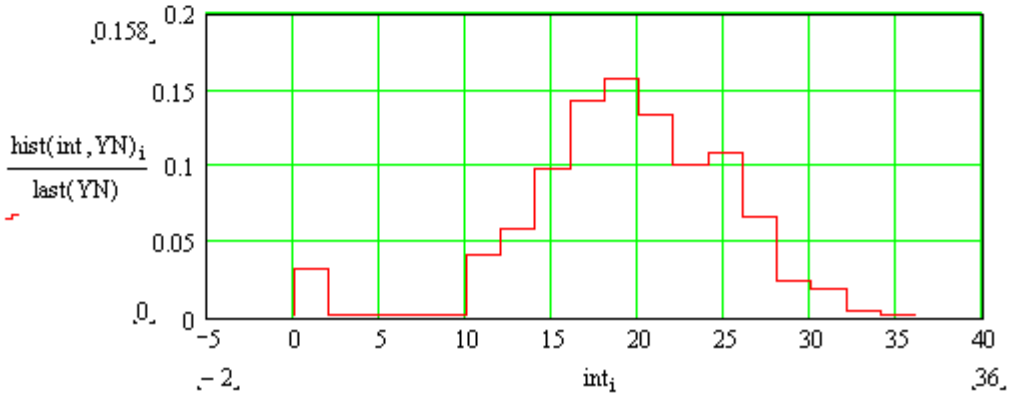
$YN_{i+18c} := yn(i,19)$ $YN_{i+20c} := yn(i,20)$ $YN_{i+21c} := yn(i,21)$ $YN_{i+22c} := yn(i,22)$ $YN_{i+23c} := yn(i,23)$

$YN_{i+24c} := yn(i,24)$ $YN_{i+25c} := yn(i,25)$ $YN_{i+26c} := yn(i,26)$ $YN_{i+27c} := yn(i,27)$ $YN_{i+28c} := yn(i,28)$

$i := 0..20$

$int_i := -2 + 2 \cdot i$

Распределение данных примеров "Свой"



Приложение № 22 Наблюдение распределения данных образов "Чужие" на выходах сумматоров, ранее обученных нейронов

$n := 9$

$Hv := READPRN("Hv.prn")$

$MU := READPRN("MU.prn")$

Вычисление откликов нейронов на примеры образов "Чужие"

$$yn(k,m) := \left| y \leftarrow \sum_{i=0}^{n-1} \left[MU_{i+m} \cdot \left(Hv^{\langle i+m \rangle} \right)_k \right] \right| \; y$$

$c := last\left(Hv^{\langle 0 \rangle}\right)$ $i := 0..c$

$YN_i := yn(i,0)$ $YN_{i+c} := yn(i,1)$ $YN_{i+2c} := yn(i,2)$ $YN_{i+3c} := yn(i,3)$ $YN_{i+4c} := yn(i,4)$

$YN_{i+5c} := yn(i,5)$ $YN_{i+6c} := yn(i,6)$ $YN_{i+7c} := yn(i,7)$ $YN_{i+8c} := yn(i,8)$ $YN_{i+9c} := yn(i,9)$

$YN_{i+10c} := yn(i,10)$ $YN_{i+10c} := yn(i,10)$ $YN_{i+11c} := yn(i,11)$ $YN_{i+12c} := yn(i,12)$ $YN_{i+13c} := yn(i,13)$

$YN_{i+14c} := yn(i,14)$ $YN_{i+15c} := yn(i,15)$ $YN_{i+16c} := yn(i,16)$ $YN_{i+17c} := yn(i,17)$ $YN_{i+18c} := yn(i,18)$

$YN_{i+18c} := yn(i,19)$ $YN_{i+20c} := yn(i,20)$ $YN_{i+21c} := yn(i,21)$ $YN_{i+22c} := yn(i,22)$ $YN_{i+23c} := yn(i,23)$

$YN_{i+24c} := yn(i,24)$ $YN_{i+25c} := yn(i,25)$ $YN_{i+26c} := yn(i,26)$ $YN_{i+27c} := yn(i,27)$ $YN_{i+28c} := yn(i,28)$

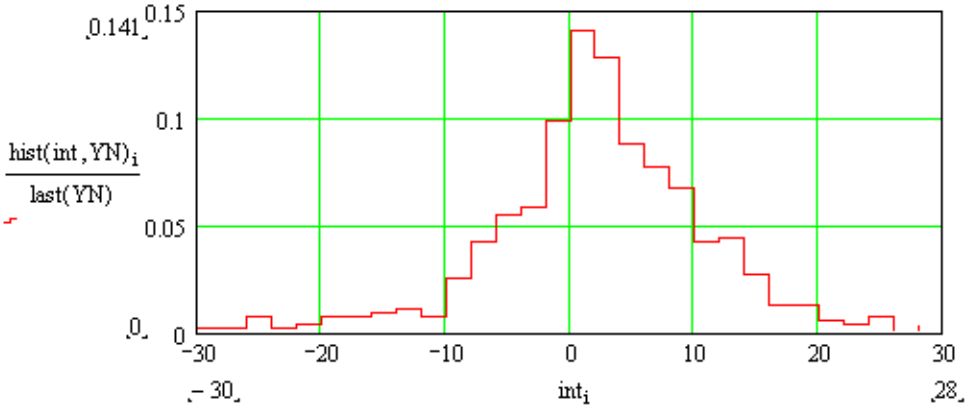
$YN_{i+29c} := yn(i,29)$ $YN_{i+30c} := yn(i,30)$ $YN_{i+31c} := yn(i,31)$ $YN_{i+32c} := yn(i,32)$ $YN_{i+33c} := yn(i,33)$

$YN_{i+34c} := yn(i,34)$ $YN_{i+35c} := yn(i,35)$ $YN_{i+36c} := yn(i,36)$ $YN_{i+37c} := yn(i,37)$ $YN_{i+38c} := yn(i,38)$

$i := 0..30$

$int_i := -30 + 2 \cdot i$

Гистограмма распределения данных образов "Чужие"



Приложение № 23 Отображение квантовой суперпозиции в пространство расстояний Хэмминга между кодом "Свой" и кодами 32 образов "Чужой"

$n := 9$

$Hv := READPRN("Hv.prn")$

$MU := READPRN("MU.prn")$

Отклики нейрон-m на образ "Чужой-k"

$$zn(k,m) := \begin{| y \leftarrow \sum_{i=0}^{n-1} \left[MU_{i+m} \cdot \left(Hv^{\langle i+m \rangle} \right)_k \right] \\ z \leftarrow 0 \ \text{if} \ y \geq 0 \\ z \leftarrow 1 \ \text{if} \ y > 0 \\ z$$

Матрица откликов нейронов

$HH := matrix\left(last\left(Hv^{\langle 0 \rangle}\right) + 1, 128, zn\right)$

Вектор расстояний Хэмминга

$m := 0..last\left(Hv^{\langle 0 \rangle}\right)$

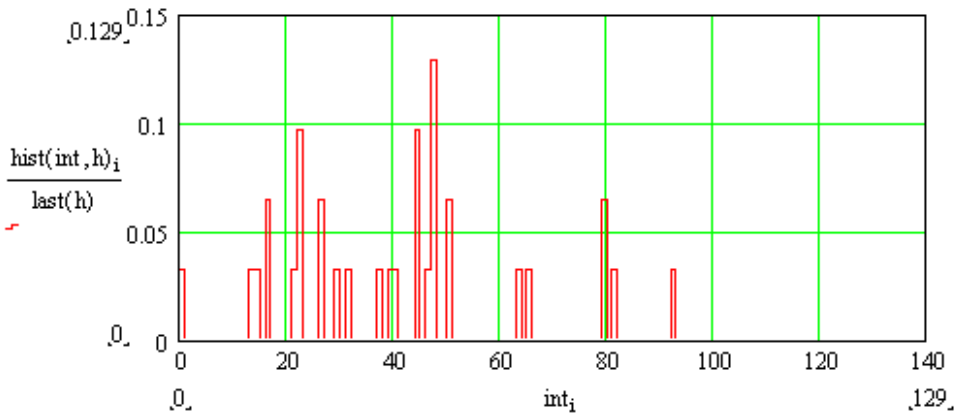
$$h_m := 128 - \sum_{i=0}^{127} HH_{m,i}$$

$h =$

	0
0	39
1	65
2	21
3	29
4	44
5	92
6	46
7	22
8	79
9	14
10	13
11	50
12	26
13	40
14	63
15	16

$i := 0..130$

$int_i := 0 + 1 \cdot i$



Приложение № 24 Наблюдение стабильности выходных состояний 64 нейронов на данных одного примера образа "Свой"

$V := READPRN("V.prn")$ $MU := READPRN("MU.prn")$

$shym := 0.3 \cdot stdev(V)$ $stdev(V) = 7.739$

$Y := V^{T}$

$k := 0..32$

$v^{\langle k \rangle} := rnorm(416, 0, shym) + Y^{\langle 0 \rangle}$

Номер варианта шума

Номер нейрона

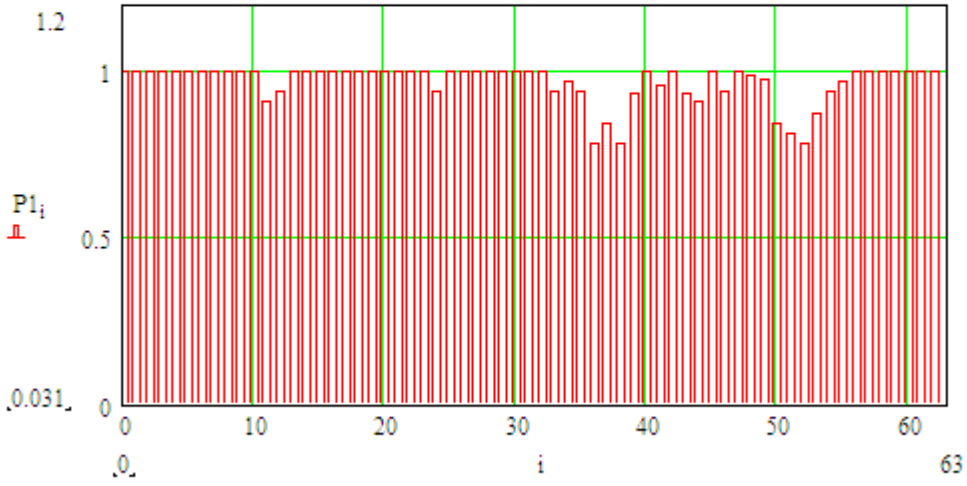
$$yn(k,m) := \left| \begin{array}{l} y \leftarrow \sum_{i=0}^{n-1} \left[MU_{i+m} \cdot \left(v^{\langle k \rangle} \right)_{i+m} \right] \\ z \leftarrow 1 \text{ if } y \geq 0 \\ z \leftarrow 0 \text{ if } y < 0 \\ z \end{array} \right.$$

$YZ := matrix(32, 64, yn)$

$i := 0..63$

$P1_i := mean\left(YZ^{\langle i \rangle}\right)$

Вероятность появления состояния "1" на выходах нейронов



Приложение №25 Наблюдение стабильности выходных состояний 64 нейронов на данных одного примера образа "Чужой"

$n := 9$

$Hv := READPRN("Hv.prn")$ $MU := READPRN("MU.prn")$

$shym := 0.3 \cdot stdev(Hv)$ $stdev(Hv) = 7.671$

$Y := Hv^{T}$

$k := 0..32$

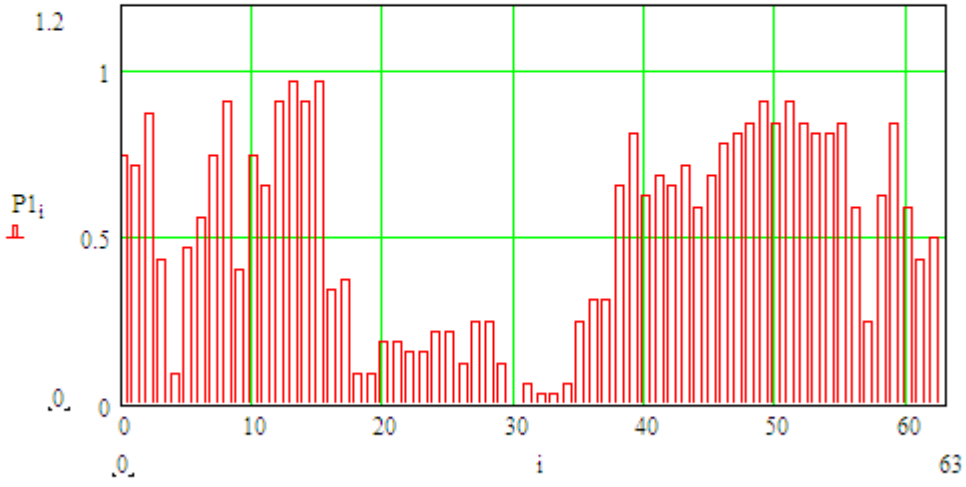
$v^{\langle k \rangle} := rnorm(416, 0, shym) + Y^{\langle 1 \rangle}$

$$yn(k,m) := \left| \begin{array}{l} y \leftarrow \sum_{i=0}^{n-1} \left[MU_{i+m} \cdot \left(v^{\langle k \rangle} \right)_{i+m} \right] \\ z \leftarrow 1 \text{ if } y \geq 0 \\ z \leftarrow 0 \text{ if } y < 0 \\ z \end{array} \right.$$

$YZ := matrix(32, 64, yn)$

$i := 0..63$

$P1_i := mean\left(YZ^{\langle i \rangle} \right)$



Приложение № 26 Наблюдение расстояний Хэмминга для "белого" шума с длиной кода 128 бит (16 случайных кодов букв)

$$D2B(x) := \left| \begin{array}{l} \text{for } i \in 0..7 \\ \quad V_i \leftarrow \text{mod}(x,2) \\ \quad x \leftarrow \text{floor}\left(\frac{x}{2}\right) \\ V \end{array} \right.$$

$$GB(n) := \left| \begin{array}{l} \text{for } i \in 0..n-1 \\ \quad V_i \leftarrow \text{rnd}(255) \\ \quad V_i \leftarrow \text{floor}(V_i) \\ V \end{array} \right.$$

$ETOL := GB(16)$

$ISL := GB(360)$

$$ISI(ISL,k) := \left| \begin{array}{l} \text{for } i \in 0..15 \\ \quad V_i \leftarrow ISL_{i+k} \\ V \end{array} \right.$$

$$HHH(ETOL,IS) := \left| \begin{array}{l} h \leftarrow 0 \\ \text{for } j \in 0..15 \\ \quad E1_j \leftarrow D2B(ETOL_j) \\ \quad E2_j \leftarrow D2B(IS_j) \\ \quad h \leftarrow h + \sum_{i=0}^{7} \left[(E1_j)_i \oplus (E2_j)_i \right] \\ h \end{array} \right.$$

$i := 0..(360-16)$

$IIS^{\langle i \rangle} := ISI(ISL,i)$

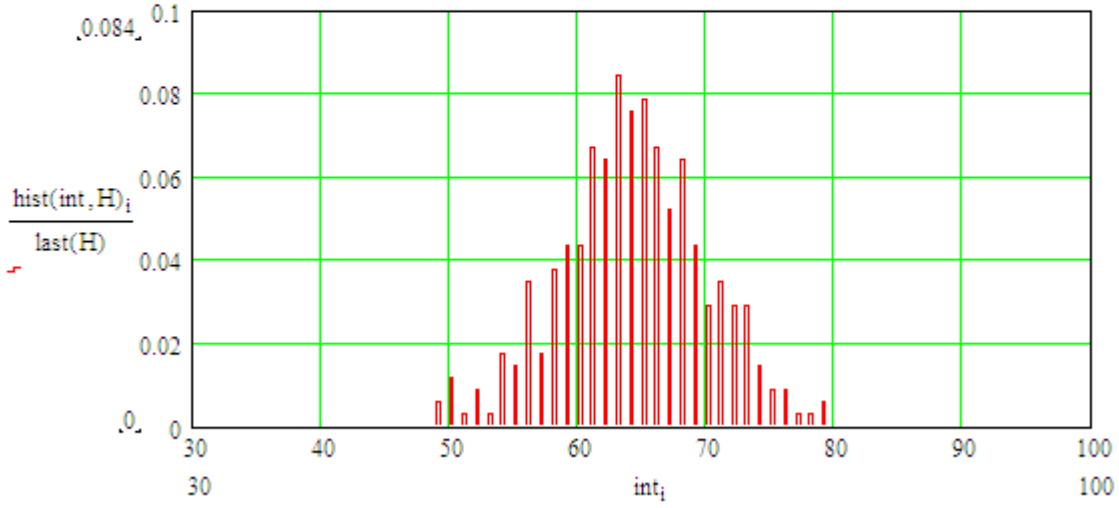
$H_i := HHH(ETOL, IIS^{\langle i \rangle})$

mean(H) = 64.104 stdev(H) = 5.632

$i := 0..512$

$int_i := 0.25 \cdot i$

Распределение расстояний Хэмминга для "белого" шума



Приложение № 27 Наблюдение расстояний Хэмминга для текста на английском с длиной кода 128 бит (16 букв осмысленного текста)

T := "book is intended" ETOL := str2vec(T)

TTT := "This monograph is considering the problem of the use of large artificial neural networks to protect the secret of biometric images of man and his personal cryptographic keys. About Digital Democracy can speak only when ordinary people personal data protected. In the U.S. and the EU to protect the personal biometrics and priyate keys are used "fuzzy extractors"

ISL := str2vec(TTT) last(ISL) = 365

ISI(ISL, k) :=
for i ∈ 0.. 15
  $V_i \leftarrow ISL_{i+k}$
V

GB(n) :=
for i ∈ 0.. n − 1
  $V_i \leftarrow rnd(255)$
  $V_i \leftarrow floor(V_i)$
V

HHH(ETOL, IS) :=
h ← 0
for j ∈ 0.. 15
  $E1_j \leftarrow D2B(ETOL_j)$
  $E2_j \leftarrow D2B(IS_j)$
  $h \leftarrow h + \sum_{i=0}^{7} \left[(E1_j)_i \oplus (E2_j)_i \right]$
h

i := 0.. (365 − 16)

$IIS^{\langle i \rangle} := ISI(ISL, i)$

$H_i := HHH(ETOL, IIS^{\langle i \rangle})$

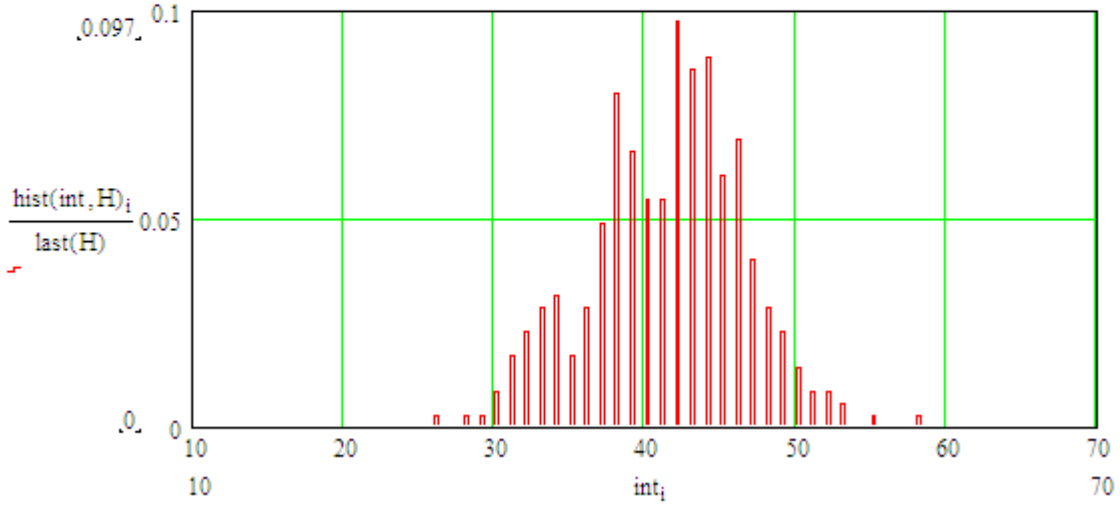
mean(H) = 41.306

stdev(H) = 5.102

i := 0.. 512

$int_i := 0.25 \cdot i$

Распределение расстояний Хэмминга для текста на английском



Приложение № 28 Наблюдение расстояний Хэмминга по модулю 8 на английском тексте для квантовой суперпозиции 128 кубит

T := "book is intended" ETOL := str2vec(T)

TTT := "This monograph is considering the problem of the use of large artificial neural networks to protect the secret of biometric images of man and his personal cryptographic keys. About Digital Democracy can speak only when ordinary people personal data protected. In the U.S. and the EU to protect the personal biometrics and priyate keys are used "fuzzy extractors"

ISL := str2vec(TTT) last(ISL) = 365

ISI(ISL, k) := for i ∈ 0..15 $V_i \leftarrow ISL_{i+k}$; V

GB(n) := for i ∈ 0..n − 1 $V_i \leftarrow rnd(255)$; $V_i \leftarrow floor(V_i)$; V

HH8(ETOL, IS) := h ← 0 ; for j ∈ 0..15 $h \leftarrow h + |ETOL_j - IS_j|$; h

i := 0..(365 − 16)

$IIS^{\langle i \rangle}$:= ISI(ISL, i)

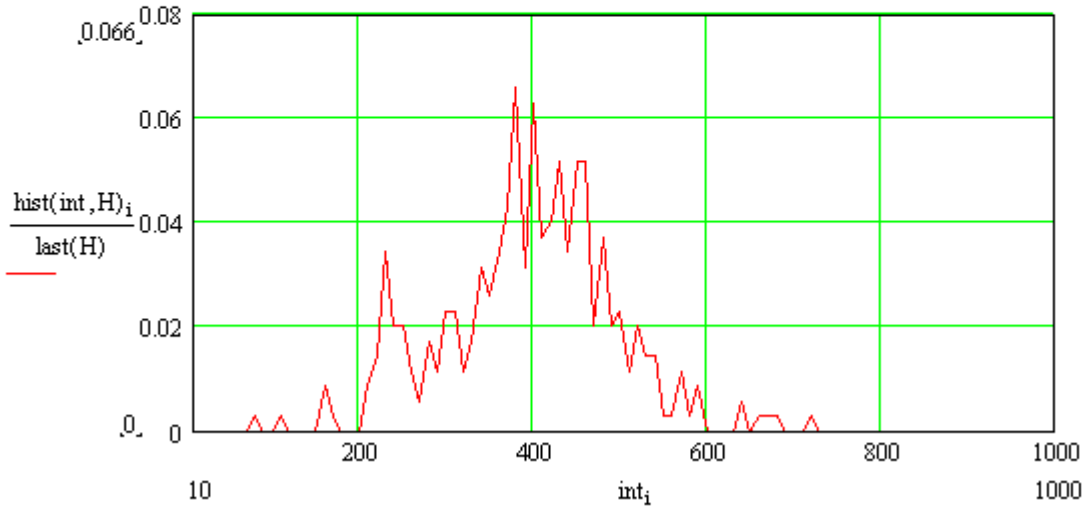
$H_i := HH8(ETOL, IIS^{\langle i \rangle})$

mean(H) = 399.24 stdev(H) = 98.537

i := 0..150

$int_i := 10 \cdot i$

Распределение расстояний Хэмминга для текста на английском



Термины и определения

Биометрический образ «Свой» - многомерный континуум входных биометрических данных, обычно представленный примерно 20 примерами векторов из нескольких сотен, контролируемых биометрических параметров. Биометрический образ попадает в категорию «Свой», если нейронная сеть преобразователя биометрия-код дает выходной код близкий к коду использованному при ее обучении.

Биометрический образ «Чужой» - многомерный континуум входных биометрических данных обычно представленный примерно 20 примерами векторов из нескольких сотен, контролируемых биометрических параметров. Биометрический образ попадает в категорию «Чужой», если нейросетевой преобразователь биометрия-код заранее не обучен на этом образе.

Извлечение знаний из обученной нейронной сети – итерационная процедура направленного извлечения знаний из обученной нейронной сети о выходном коде биометрического образа «Свой» и о контролируемых биометрических параметрах образа «Свой». Поиск осуществляется путем направленного подбора образов с минимальной энтропией выходных состояний кодов нейронной сети (квантовой суперпозиции выходных кодов). После селекции образов с минимальной энтропией, осуществляют восстановления численность образов в следующем поколении через их морфинг скрещивание по правилам ГОСТ Р 52633.2-2010. Обычно задача решается с использованием базы в 10 000 образов «Чужой», каждый из которых представлен 20 примерами.

Квантовая суперпозиция – множество выходных кодов обученного нейросетевого преобразователя, например, наблюдаемая при воздействии на его входы примером образа «Свой» в сумме с шумом сканирования многомерной окрестности. Каждый бит квантовой суперпозиции нестабилен, имеет некоторую вероятность появления состояния «0» и некоторую вероятность появления в нем состояния «1».

Квантовая запутанность – наличие корреляционных связей между разрядами выходного кода выходной квантовой суперпозиции нейросетевого преобразователя биометрия-код.

Квантовый ускоритель для извлечения знаний из нейронной сети – программная реализация циклического вычислителя многократно осуществляющего вычисления в области многомерных континуумов и в дискретной области их отображений, например, построенная с использованием направленного поиска минимума многомерной энтропии. Величина ускорения определяется как показатель сужения пространства перебора в степени числа осуществленных циклов направленного подбора. Например, если генетическая селекция оставляет 2% образов «Чужой» с минимальной энтропией кодов квантовой суперпозиции, то каждый цикл континнумы и их код дает 50-ти кратное ускорение. Если циклов 50, то мы получим ускорение 50^{50} за счет направленного поиска по критерию минимума многомерной энтропии.

Квантовый усилитель мощности хи-квадрат критерия - программная реализация хи-квадрат критерия Присона, построенная на наблюдении дискретного спектра его состояний для малых выборок, обеспечивающая

многократное снижение объема выборки при тех же доверительных вероятностях (при том же уровне вероятности ошибок первого и второго рода). Усилитель мощности может быть циклическим и ациклическим. Ациклический усилитель строится путем сглаживания столбцов гистограммы (уменьшения шумов квантования) и обеспечивает коэффициент усиления до 30 раз. Циклический усилитель работает перебирая множество возможных подвыборок из исходной большой выборки. Например, усилитель может анализировать все возможные подвыборки по 16 опытов, получаемые из полной выборки в 21 опыт (всего возможно C_{21}^{16} = 20 346 сочетаний). Обработка нескольких тысяч состояний, предположительно, может дать эффект квантового усиления до 3 000 раз.

Кубит – один разряд выходного кода нейронной сети (выход одного нейрона), меняющий свое состояние при воздействии на входы обученной нейронной сети. Один кубит описывается вероятностью появления состояний «0» и вероятностью появления состояния «1».

Нейросетевой преобразователь биометрия-код – нейронная сеть, обученная преобразовывать примеры образа «Свой» в код ключа доступа, например, длиной 256 бит при минимальном (близком к нулю) значении энтропии этой квантовой суперпозиции. При предъявлении примеров образа «Чужой» выходной код случаен, его разряды нестабильны, квантовая суперпозиция выходного кода имеет высокое значение энтропии.

Расстояние Хэмминга – расстояние между одним из кодов квантовой суперпозиции и кодом «Свой», получаемое подсчетом числа не совпадающих разрядов, или расстояние между центром кодов образа «Чужой» и одним из этих кодов.

Пространство расстояний Хэмминга – множество расстояний Хэмминга, например, полученное вычислением квантовой суперпозиции кодов «Чужой» с кодом «Свой».

Пример биометрического образа - пример вектора наблюдаемых биометрических параметров, принадлежащих некоторому биометрическому образу. Возможно множество примеров одного биометрического образа, образующих многомерный континуум.

Монография

Иванова Александра Ивановича

Многомерная нейросетевая обработка биометрических данных с программным воспроизведением эффектов квантовой суперпозиции. Пенза – 2016 г. Издательство АО «Пензенский научно-исследовательский электротехнический институт» (ОА «ПНИЭИ») – 133 с., открытый доступ http://пниэи.рф/activity/science/BOOK16.pdf

Подписано к печати 18.11.2016 г. Формат 60x80 1/16 Усл. печ. л. 7.81.
Тираж 300 экз.

Издательство АО «ПНИЭИ», 44000, г. Пенза, ул. Советская, 9

Отпечатано ФГОУ ВПО ПГУ
Заказ № ___ от _____
440026, г. Пенза, ул. Красная, 44.