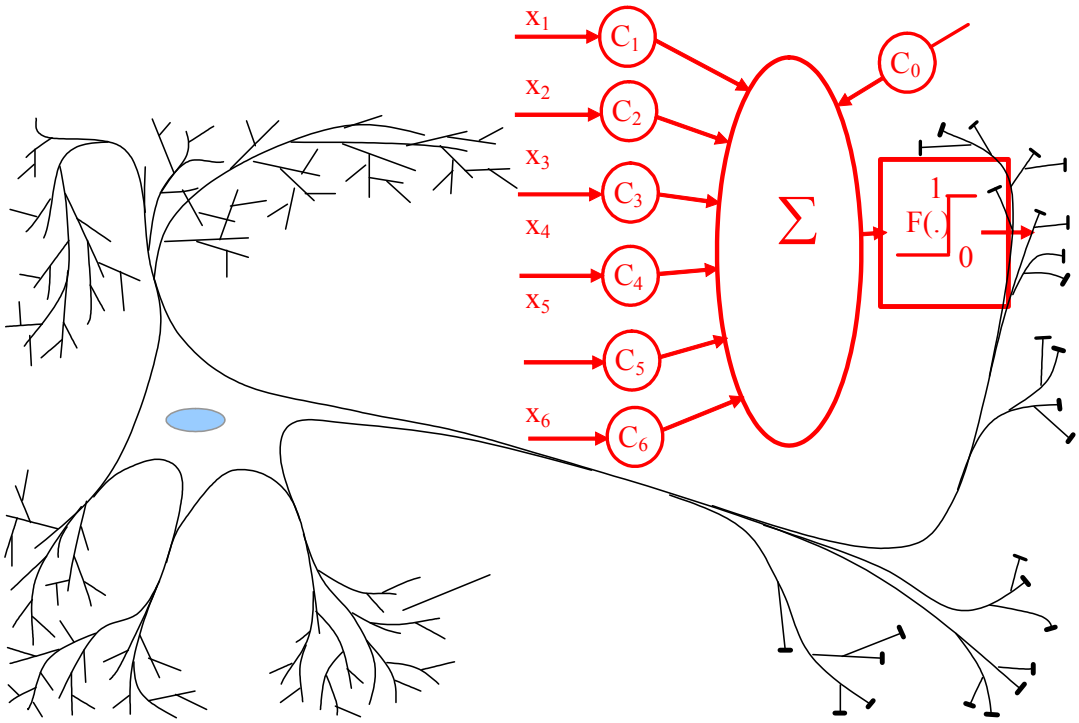
УДК: 519.24; 53; 57.017
И 18
ББК 32.818

Издательство АО «ПНИЭИ»,
электронный вариант учебного пособия размещен на сайте
http://пниэи.рф/activity/science/noc/BOOK18-2.pdf

Иванов Александр Иванович (Пенза)

ЧИСЛЕННАЯ ОЦЕНКА ПОКАЗАТЕЛЕЙ КВАНТОВОЙ СЦЕПЛЕННОСТИ ВЫХОДНЫХ КУБИТ НЕЙРОСЕТЕВОЙ МОЛЕКУЛЫ ПРЕОБРАЗОВАТЕЛЯ БИОМЕТРИИЧЕСКИХ ДАННЫХ

Учебное пособие



Пенза -2018

УДК: 519.24; 53; 57.017
И 18
ББК 32.818

Рецензенты:
Доктор техн. наук, проф. М.М. Бутаев - ученый секретарь НТС АО НПП «Рубин» 440000, Россия, г. Пенза, ул. Байдукова, 2

Доктор техн. наук, проф. С.И. Геращенко – заведующий кафедрой «Медицинская кибернетика и информатика» ФГБОУ ВО «Пензенский государственный университет» 440026, Россия, г. Пенза ул. Красная, 40.

Иванов А.И.
Численная оценка показателей квантовой сцепленности выходных кубит нейросетевой молекулы преобразователя биометрических данных. Учебное пособие. Пенза – 2018 г. Издательство АО «Пензенский научно-исследовательский электротехнический институт» (АО «ПНИЭИ») – 27 с. Свободный доступ http://пниэи.рф/activity/science/noc/BOOK18-2.pdf

Изложены теоретические и практические аспекты численной оценки показателей квантовой сцепленности выходных разрядов большой сети искусственных нейронов, заранее обученной распознавать биометрические данные. Нейроны такой сети специально переводятся в динамический режим за счет добавления к биометрическим данным небольшого нормального шума. При этом для образа «Свой» показатели сцепленности выходных разрядов нейронной сети остаются высокими. Иначе ведут себя данные для образов «Чужой», в этом случае вероятность состояний «0» и «1» в каждом разряде случайны, а соседние разряды оказываются слабо сцепленными.

Рассмотренные в пособии процедуры численной оценки показателей сцепленности иллюстрируются программными приложениями, написанными в среде инженерных расчетов MathCAD.

Учебное пособие рассчитано на студентов, аспирантов, преподавателей и научных работников, занимающихся прецизионной статистико-нейросетевой обработкой биометрических данных в режиме программной поддержки эффектов квантовой суперпозиции на выходах нейросетевой молекулы.

Оглавление

Введение …….. 4
1. Получение достоверных 416-ти мерных векторов биометрических параметров динамики воспроизведения рукописных образов …… 5
2. Обучение нейронов преобразователя биометрия-код ……. 6
3. Геометрическая интерпретация работы сети обученных нейронов …… 6
4. «Тряска» обученного нейрона на входных данных «Свой» ……. 7
5. Выявление слабых разрядов кода образа «Свой» ……. 8
6. Показатель стабильности выходных разрядов нейросетевой молекулы 9
7. Как сделать средний показатель стабильности образа «Свой» нулевым 11
8. Как сделать средний показатель стабильности образа «Чужой» нулевым …….. 11
9. Оценка значения показателя квантовой сцепленности данных внутри одного кубита нейросетевой молекулы через вычисление коэффициента автокорреляции …….. 12
10. Оценка значения показателя квантовой сцепленности пар кубит нейросетевой молекулы через вычисление коэффициента взаимной корреляции ……..……. 13
11. Вычисление вероятности ошибок второго рода нейросетевого преобразователя биометрия-код в пространстве расстояний Хэмминга …… 15
12. Оценка усредненной сцепленности 256 кубит нейросетевой молекулы через 256-мерную энтропию ее выходных состояний ……. 16
13. Симметризация корреляционных связей и их программное моделирование …… 17
14. Приближенная оценка 256-мерной энтропии по значениям расстояний Хэмминга для нейросети с одинаковой коррелированностью выходных состояний нейронов ……. 19
15. Переход от 256-ти мерной энтропии к легко вычисляемым корреляционным функционалам той же размерности ……. 19
16. Вычисление сверток Хэмминга по модулю 256 …….. 20
17. Многообразие функционалов, оценивающих уровень сцепленности групп выходных кубит нейросетевой молекулы …… 22

Заключение ……. 23
ЛИТЕРАТУРА …….. 24

ВВЕДЕНИЕ

Данное учебное пособие является продолжением темы нейросетевой обработки биометрических данных в режиме программной поддержки эффектов квантовой суперпозиции [1]. Если подмешать в биометрические данные шум, то нейронная сеть будет вести себя как «нейросетевая молекула» [2] с дискретным выходным спектром. Совершенно такая же ситуация возникает, если хи-квадрат критерий, математическое ожидание, стандартное отклонение, коэффициенты корреляции биометрических данных [3] вычисляются на малых выборках. Все функционалы для вычисления младших статистических моментов легко преобразуются в соответствующие «математические молекулы» с дискретным выходным спектром. К таким вычислениям оказываются применимы процедуры квантовой механики и квантовой нейродинамики. При воспроизведении этих математических конструкций программными средствами на языке MathCAD амплитуды вероятности дискретного спектра состояний волновой функции легко наблюдаемы.

Из теории квантовых вычислений следует, что для полноценного описания сложных объектов только амплитуд вероятности спектра состояний волновой функции недостаточно. Спектр амплитуд вероятностей должен быть дополнен показателями сцепленности кубит «нейросетевой молекулы» или иной похожей математической конструкции. В данном пособии я постарался, как можно более просто показать, что процедура вычисления показателей сцепленности кубит «нейросетевой молекулы» не является сложной задачей. Главное состоит в том, что любой желающий (студент, аспирант, преподаватель) может проверить описанные в данном учебном пособии процедуры. Для меня принципиально важно показать, что «квантовая нейродинамика» - это очень просто. Ее можно проверить своими руками. Это намного проще, чем «квантовой механика» с ее котами Шредингера. Моделирование уравнения Шредингера на обычном компьютере – является задачей экспоненциальной вычислительной сложности. Под эту задачу нужны огромные и дорогие СУПЕРкомпьютеры, которых нет у студентов и их преподавателей.

Совершенно иная ситуация возникает в «квантовой нейродинамике», уравнения нейронных сетей просты, их моделирование на обычных компьютерах имеет линейную вычислительную сложность. Приведенные в данном учебном пособии программы позволяют моделировать два, три кубита, однако их легко можно модифицировать под 256 кубит [4] и получить желаемый эффект ускорения вычислений или повышения точности (устойчивости) вычислений на малых выборках. Эффективность квантовых вычислений определяется числом воспроизводимых кубит и временем поддержки квантовой суперпозиции. Рассматриваемый в учебном пособии метод позволяет на обычном компьютере поддерживать как угодно долго квантовую суперпозицию сотен и/или тысяч кубит.

1. Получение достоверных 416-ти мерных векторов биометрических параметров динамики воспроизведения рукописных образов

При воспроизведении имитационных моделей крайне важно знать, какого вида законом распределения значений описываются биометрические параметры той или иной технологии. Для определения вида закона распределения значений необходимо получить достаточно большую выборку биометрических данных. Сегодня получить доступ через Интернет к достоверным биометрическим данным почти невозможно, производители коммерческой биометрии, как правило, не пускают пользователей к данным своих продуктов. Единственным исключением является сайт АО «Пензенский научно-исследовательский электротехнический институт», через который осуществляется доступ к свободно распространяемой среде моделирования «БиоНейроАвтограф» [5]. Для получения достоверных биометрических данных необходимо ввести 20 примеров рукописного образа, например, образа «Пенза», как это показано на рисунке 1.

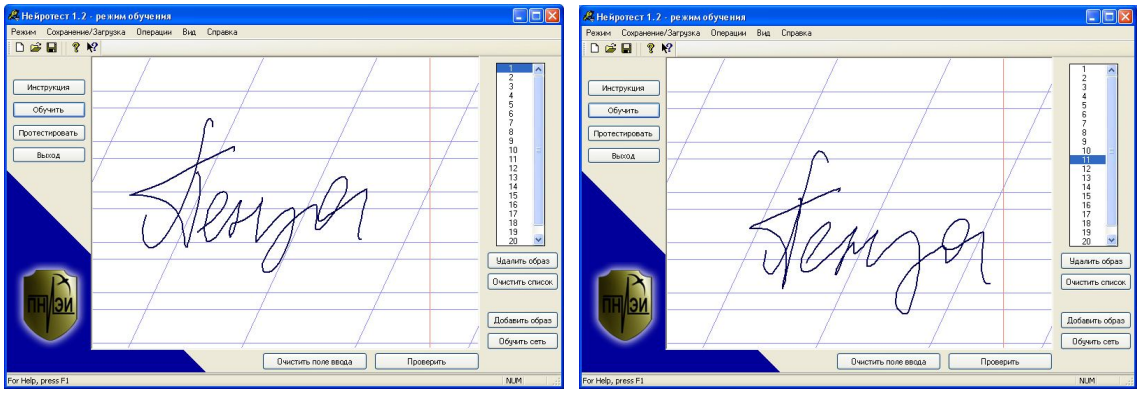


Рис. 1. Сбор биометрических данных «Свой» в среде моделирования «БиоНейроАвтограф» [6]

Среда моделирования позволяет сохранять данные и преобразовывать их в вектор из 416 биометрических параметров образа [6], запоминаемых в файле Data\params.txt. Из рисунка 1 видно, что одинаковые примеры рукописного образа *«Пенза»* существенно отличаются от друг друга, соответственно будут отличаться от друг друга и их вектора из 416 коэффициентов двухмерного преобразования Фурье колебаний пера по координатам Y(t) и X(t).

Еще больше между собой будут отличаться вектора биометрических параметров разных рукописных образов, как это показано на рисунке 2.

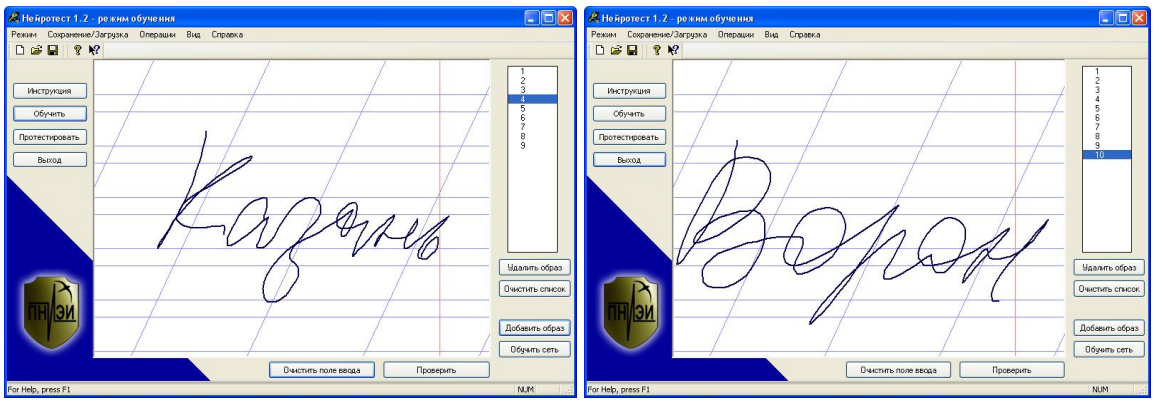


Рис. 2. Сбор биометрических данных «Чужой» в среде моделирования «БиоНейроАвтограф» [5]

Получение достоверных биометрических данных для моделирования нейродинамики является принципиально важным условием. Нельзя «брать данные с потолка», так как они с высокой вероятностью будут принадлежать физически не реализуемым нейродинамическим процессам. Только использование реальных данных всегда дает статистически устойчивые нейросетевые вычисления.

2. Обучение нейронов преобразователя биометрия-код

Существует огромное число численных методов обучения нейронов [7, 8], большинство из них являются итерационными или неустойчивыми. Применять такие методы следует с осторожностью, так как они могут дать вместо «хорошего» обучения «удовлетворительное». В биометрии это недопустимо. В связи с этим обучение нейросетевых преобразователей биометрия-код в России стандартизовано [9]. При формировании нейросети преобразователя входные связи каждого нейрона выбираются случайно. Весовые коэффициенты сумматора нейрона вычисляются через математическое ожидание и стандартное отклонение контролируемых биометрических параметров образа «Свой». Выходной квантователь нейронов всегда переключается в центре множества биометрических параметров ВСЕ «Чужие».

На рисунке 3 приведена программа, которая читает биометрические данные примеров рукописного образа «Пенза», формирует один нейрон и обучает его выдавать состояние «0» для примеров образа «Пенза».

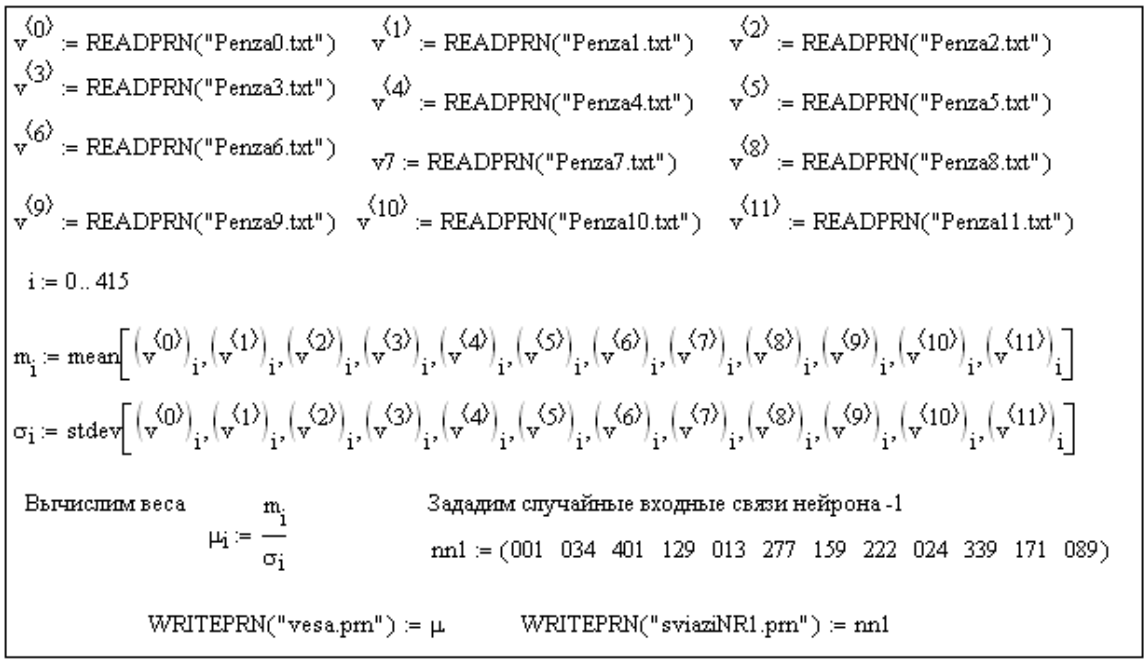


Рис. 3. Программа формирования связей нейрона и вычисления его весовых коэффициентов по 12 примерам рукописного образа *«Пенза»*

3. Геометрическая интерпретация работы сети обученных нейронов

Данные множества биометрических образов Все «Чужие» оказываются слабо коррелированны между собой. То есть, их можно представить 416-ти мерной гиперсферой. Отобразить гиперсферу столь высокой размерности на бумаге нельзя. Однако можно отобразить плоское сечение такой гиперсферы по двум параметрам. На рисунке 4 дано сечение 416-ти мерной гиперсферы по первому и 157 биометрическому параметру.

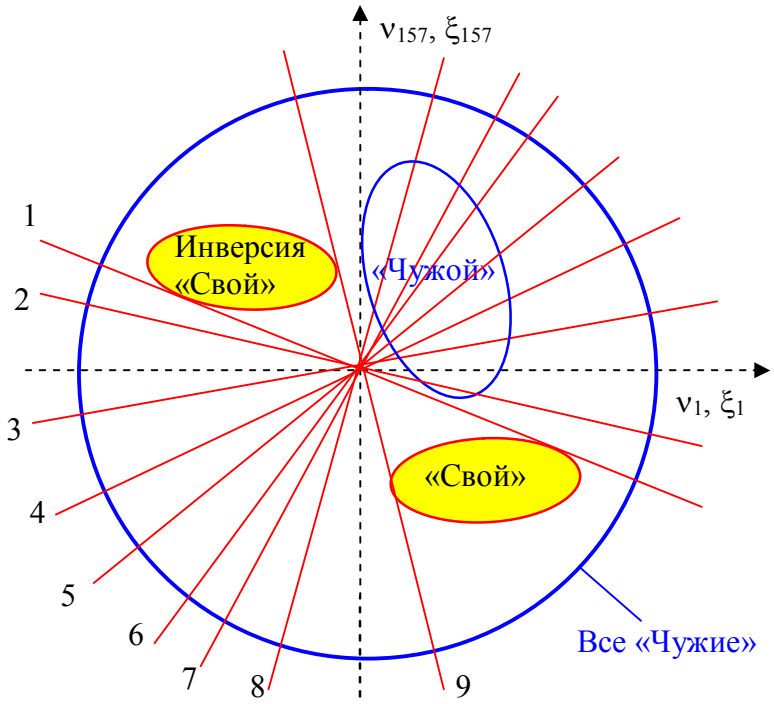


Рис. 4. Двухмерное сечение многомерной области все «Чужие»

Из рисунка 4 видно, что далеко не все нейроны преобразователя биометрии в код работают с этой парой биометрических параметров. Из 256 нейронов преобразователя «БиоНейроАвтограф» только 9 нейронов работают с этой парой биометрических параметров. При этом каждый из 9 нейронов делят окружность Все «Чужие» попалам. Свойством стандартизованного алгоритма обучения [9] является то, что ни одна разделяющая гиперплоскость 256 нейронов не пересекает гиперэллипс «Свой». При этом обязательно получается второй инверсный гиперэллипс «Свой», который так же не будет пересекаться гиперплоскостями всех 256 обученных нейронов.

Такое свойство приводит к тому, что внутри гипесферы образов Все «Чужие» будут существовать две гиперсферы распределения биометрических данных «Свой» и инверсия «Свой», дающих выходные коды с высокой стабильностью их разрядов. То есть примеры векторов биометрических параметров «Свой» $\bar{\nu}$ должны давать стабильный выходной код "$\bar{c}$" с почти нулевой энтропией $H("\bar{c}") \approx 0$. Небольшие изменения входных биометрических параметров $\Delta\bar{\nu}$ не приводят к изменению выходного кода "$\bar{c}$".

Если проинвертировать биометрические данные, то вектор $-\bar{\nu}$ будет давать стабильный инверсный выходной код "$\neg\bar{c}$" с почти нулевой энтропией $H("\neg\bar{c}") \approx 0$. Это происходит из-за того, что гиперсферы «Свой» и инверсия «Свой» не пересекаются гиперплоскастями всех 256 нейронов преобразователя биометрия-код.

Совершенно иная ситуация возникает для биометрических данных примеров образа «Чужой». Как видно из рисунка 4 гиперэллипс образа «Чужой» многократно пересекается проекциями разделяющих гиперплоскостей обученных нейронов. По этой причине даже незначительные изменения биометрических параметров $\Delta\bar{\xi}$ приводят к сильному изменению состояний выходного кода "$\bar{x}$" нейросетевого преобразователя. Возникает эффект хэширования (усиления) небольших изменений входных данных. Энтропия выходных кодов для примеров образа «Чужой» много выше почти нулевой энтропии примеров образа «Свой».

4. «Тряска» обученного нейрона на входных данных «Свой»

То, что разряды выходных кодов примеров образа «Свой» стабильны, проверим на одном нейроне. Для этой цели используем пример рукописного образа «Пенза-20» не участвовавший в обучении нейрона. Подадим эти данные на входы нейрона, добавив к ним случайный шум. Такая проверка выполняется программой, приведенной на рисунке 5.

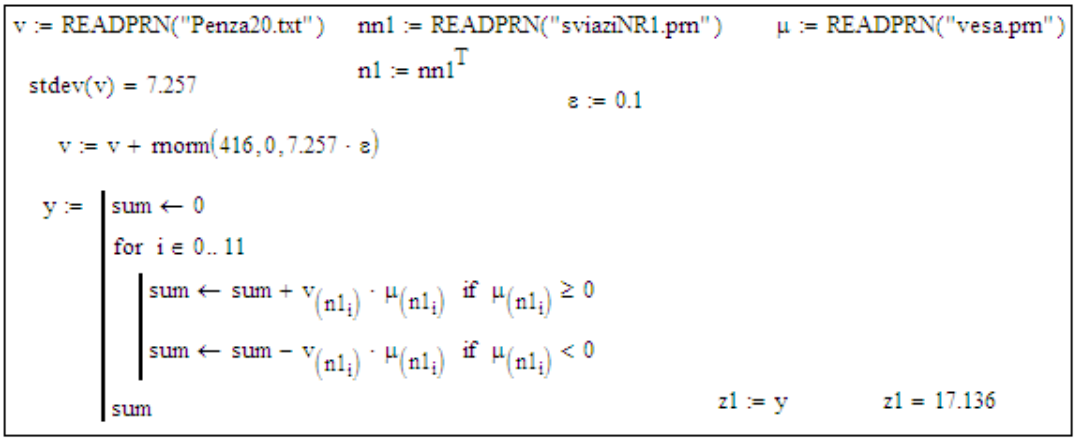


Рис. 5. Программная реализации просмотра окрестностей данных примера «Penza20» за счет их размывания белым шумом

Программа рисунка 5 вычисляет стандартное отклонение данных внутри одного примера. Далее программным генератором создается псевдослучайный белый шум с амплитудой в ε раз меньше собственного стандартного отклонения данных примера биометрического образа. На рисунке 6 даны распределения размытых данных при разных масштабах шума размывания.

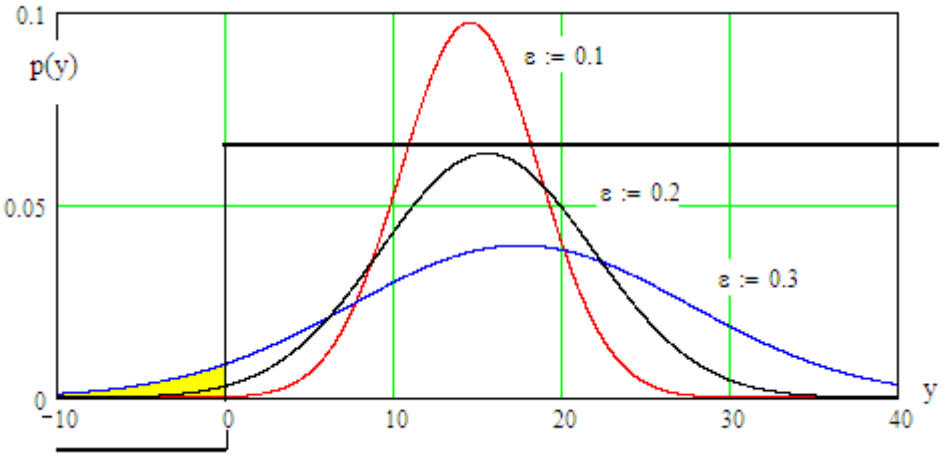


Рис. 6. Распределения по разному размытых шумом данных «Свой» на фоне функции квантования выходного сумматора нейрона

Из рисунка 6 видно, что малое размывание данных образа «Свой» ε=0.1 не влияет на выходное состояние обученного нейрона. Однако при большем размывающем шуме ε=0.2 и ε=0.3 на выходе нейрона кроме базового состояния «1» начинают возникать состояния «0». Чем выше амплитуда размывающего данные шума, тем чаще появляются состояния «0».

5. Выявление слабых разрядов кода образа «Свой»

Все примеры образа «Свой» должны размещаться внутри соответствующего гиперэллипса, как это показано на рисунке 7. Однако обучение нейрона выполнялось на малых выборках. По этой причине границы гиперэллипса установлены не точно и один пример образа «Свой» имеет нестабильные разряды даже при маленьком уровне размывающего шума.

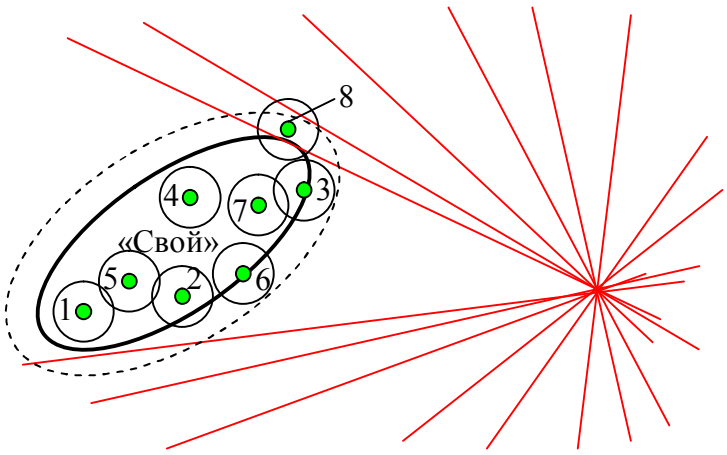


Рис. 7. Распределение примеров образа «Свой» с ошибочно вычисленными при обучении положением границы гиперэллипса

Получается, что воспользовавшись малым уровнем размывающего шума ε=0.1, мы можем обнаруживать «нестабильные» разряды кода «Свой» в которых могут появляться ошибки. Как правило, таких разрядов мало (не более 5%). Для каждого нейросетевого преобразователя биометрия-код такие «нестабильные» разряды могут быть заранее обнаружены и помечены. Знание положения таких разрядов позволяет экспоненциально сократить время корректировки ошибок кода «Свой» путем перебора возможных состояний нестабильных бит [10, 11] и безопасного сравнения хэшей проверяемых комбинаций с их эталоном.

Вторым важнейшим следствием является возможность упорядочивания примеров образ «Свой» по числу даваемых ими «нестабильных» разрядов и по уровню их нестабильности.

6. Показатель стабильности выходных разрядов нейросетевой молекулы

ГОСТ Р 52633.5 [4] вводит понятие показателя стабильности разрядов кода нейросетевой молекулы [2]:

$$w_i = 2 \cdot \left| 0.5 - P_i("0") \right| = 2 \cdot \left| 0.5 - P_i("1") \right| \quad (1),$$

где $P_i("0")$ - вероятность появления состояния «0» в i-том разряде, $P_i("1")$ - вероятность появления состояния «1» в i-том разряде.

Для примеров образа «Свой» и их инверсии все состояния 256 разрядов почти стабильны:

$$w_i(\bar{v}) = w_i(-\bar{v}) \approx 1 \quad (2).$$

Ситуация коренным образом меняется, когда обученной нейронной сети предъявляются данные образа «Чужой». В этом случае показатели стабильности значительно падают:

$$w_i(\bar{\xi}) = w_i(-\bar{\xi}) \approx 0.5 < 1 \quad (3).$$

Поддержка квантовой суперпозиции нейросетевой молекулы иллюстрируется рисунком 8.

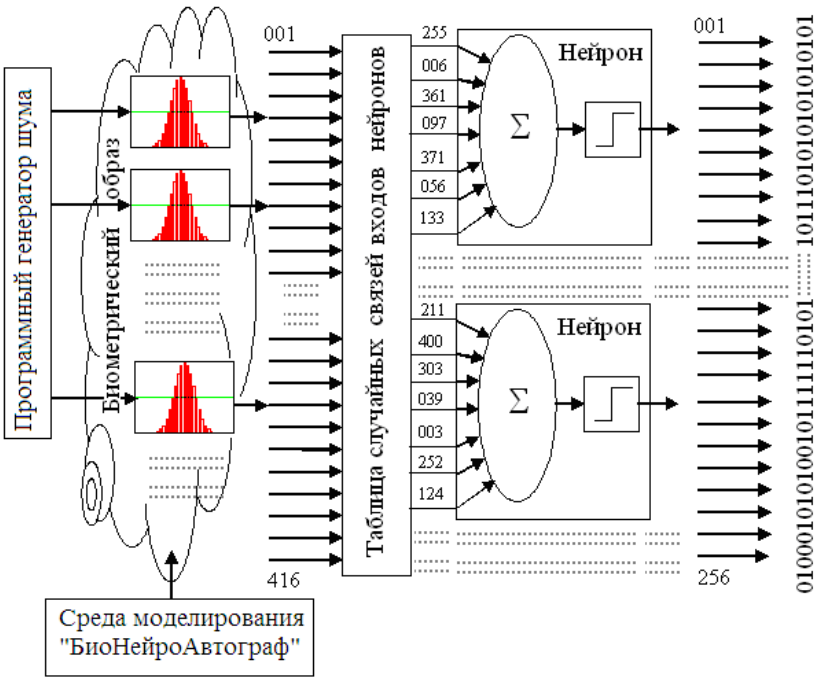


Рис. 8. Схема поддержания квантовой суперпозиции нейросетевой молекулы.

Обученная распознавать образ «Свой» нейросетевая молекула по разному реагирует на данные разных биометрических образов. Для образа «Свой» разряды выходного кода стабильны. При удалении от образа «Свой» стабильность разрядов кода падает. На рисунке 9 приведены гистограммы распределения показателей стабильности разрядов в зависимости от расстояний Хэмминга между кодами сравниваемых образов.

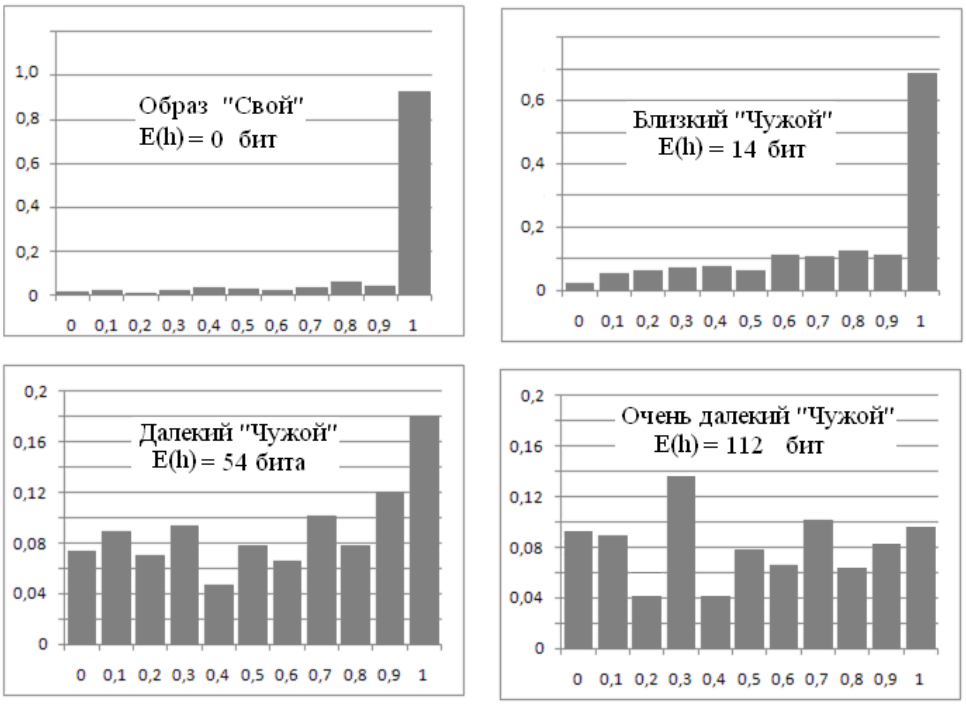


Рис. 9. Падение показателя стабильности разрядов кодов «Чужой» по мере удаления образа «Чужой» от образа «Свой»

Из рисунка 9 видно, что для образов почти «Свой» с математическим ожиданием близким к нулю разряды выходных кодов стабильны. По мере удаления образа «Чужой» от образа «Свой» по расстоянию Хэмминга растет нестабильность выходных разрядов нейросетевой молекулы. Для далеких образов с расстоянием Хэмминга h=128 (почти равномерное распределение в правой нижней части рисунка 9) средний показатель стабильности близок к 0.5.

7. Как сделать средний показатель стабильности образа «Свой» нулевым

Возникает вопрос о том, все ли варианты возможных распределений показателей стабильности отображены на рисунке 9. Переход от состояний полной стабильности всех разрядов $E(w)=1$ к состоянию половинной стабильности $E(w)=0.5$ может быть выполнен поиском далеких от образа «Свой» образов «Чужой». Для того, чтобы плавно понижать среднюю стабильность разрядов до нуля необходимо перемещать биометрический образ из его естественного положения в центр образов «Все Чужие» [12]. При этом возникает последовательность промежуточных биометрических образов с постепенно увеличивающимся уровнем центрирования биометрических параметров образа «Свой»:

$$\tilde{\nu}_i = \nu_i - E(\nu_i)\cdot\beta \qquad (4).$$

При изменении регулируемого параметра - β от 0 до 1 образ «Свой» из своего естественного положения попадает точно в центр образов «Все Чужие». В точке β=1 математическое ожидание коэффициентов стабильности становится почти нулевым $E(w)\approx 0$. На рисунке 10 приведена эволюция значений показателей стабильности при изменении регулируемого показателя - β.

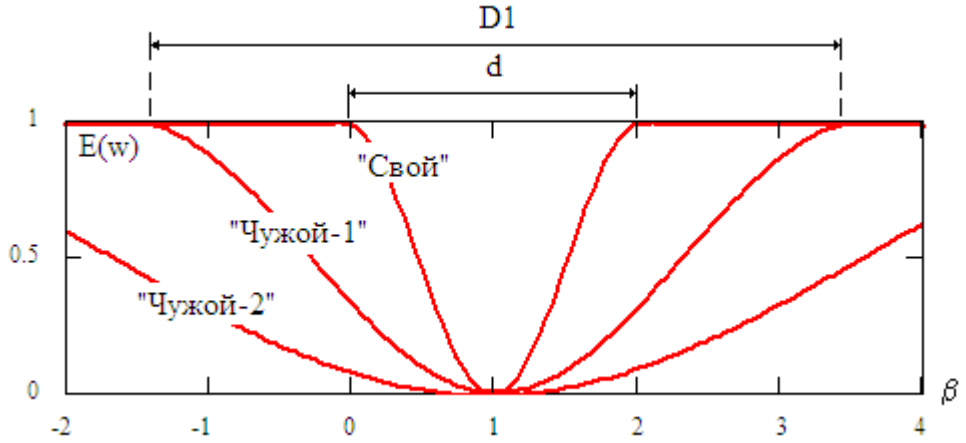


Рис. 10. Кривые изменения среднего показателя стабильности при изменении коэффициентов регулирования

Если увеличивать показатель β более 1, то мы будем наблюдать повышение показателя стабильности. В момент β=2 среднее значение показателей стабильности для выходных разрядов кода «Свой» принимает предельное значение $E(w)=1$. Дальнейший рост коэффициента регулирования - β не меняет ситуации.

8. Как сделать средний показатель стабильности образа «Чужой» нулевым

Тот же технический прием можно применить для биометрических данных образа «Чужой»:

$$\tilde{\xi}_i = \nu_i - E(\xi_i)\cdot\beta \qquad (5).$$

Результаты изменения регулируемого параметра отображены на рисунке 10. Из этого рисунка видно, что увеличение параметра регулирования приводит к уменьшению среднего значения показателей стабильности, далее происходит монотонный рост среднего значений показателей стабильности. Расстояния между правой и левой точками E(w)=1 краев оврага падения показателей стабильности следует рассматривать как наблюдаемый диаметр - D некоторого эллипса. Для каждого образа «Чужой» можно вычислить свое значение наблюдаемого диаметра - D. Все образы «Чужой» будут давать эллипс нормального распределение диаметров оврагов. Рассматривая их совместно для нескольких десятков образов «Чужой» можно вычислить взаимную коррелированность выходных образов нейросетевой молекулы, обученной распознавать образ «Свой». Эту ситуацию иллюстрирует рисунок 11.

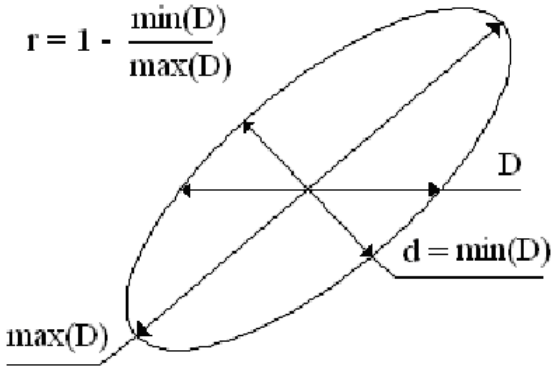


Рис. 11. Эллиптическая модель упорядочивания образов «Чужой» нейронной сетью, обученной узнавать образ свой.

Из теории известно, что отношение минимального диаметра эллипса распределения к его максимальному диаметру отражает коррелированность выходных данных образов «Чужой» на выходах нейронной сети, обученной распознавать данные образа «Свой». В конечном итоге мы получаем очень простые геометрические интерпретации, которые позволяют достаточно просто сравнивать между собой 416-ти мерные нейросетевые преобразователи биометрия-код, обученные распознавать разные биометрические образы. Кроме того, подобные интерпретации позволяют упорядочивать между собой (сопоставлять между собой) образы «Чужой», пользуясь как средством упорядочивания (сопоставления) нейронную сеть, ранее обученную распознавать образ «Свой». Появляется возможность синтеза адресов упорядочивания большого числа нейронных сетей опираясь на данные малого числа ранее обученных искусственных нейронных сетей.

Важнейшим статистическим показателем является уровень коррелированности всех образов «Чужой» в пространстве выходных кодов исследуемого нейросетевого преобразователя. Чем выше уровень коррелированности данных, тем уникальнее биометрический образ «Свой», на котором обучена тестируемая нейронная сеть.

9. Оценка значения показателя квантовой сцепленности данных внутри одного кубита нейросетевой молекулы через вычисление модуля коэффициента их автокорреляции

Показатель стабильности w_i выходных состояний каждого из разрядов нейросетевой молекулы зависит от того, с какой вероятностью меняются его состояния (1). Зная значение показателя стабильности легко ответить на вопрос, с какой вероятностью мы можем предсказать следующее состояние разряда по его

предыдущему состоянию. Показатель стабильности разряда есть не что иное, как свертка Хэмминга двух разрядов выходной последовательности состояний одного кубита или автокорреляционная функция этой бинарной последовательности:

$$w_i \approx E(1-("x_j"\oplus"x_{j+1}")) \approx \left|r("x_j","x_{j+1}")\right| \quad (6),$$

где j – номера состояний в обрабатываемой бинарной последовательности i-того кубита нейросетевой молекулы, r(.,.) – коэффициент автокорреляции.

Приведенное выше утверждение принципиально важно и к тому же легко проверяется численно. Программа проверки корректности вычисления показателя стабильности через усреднение парных сверток Хэмминга дана на рисунке 11.

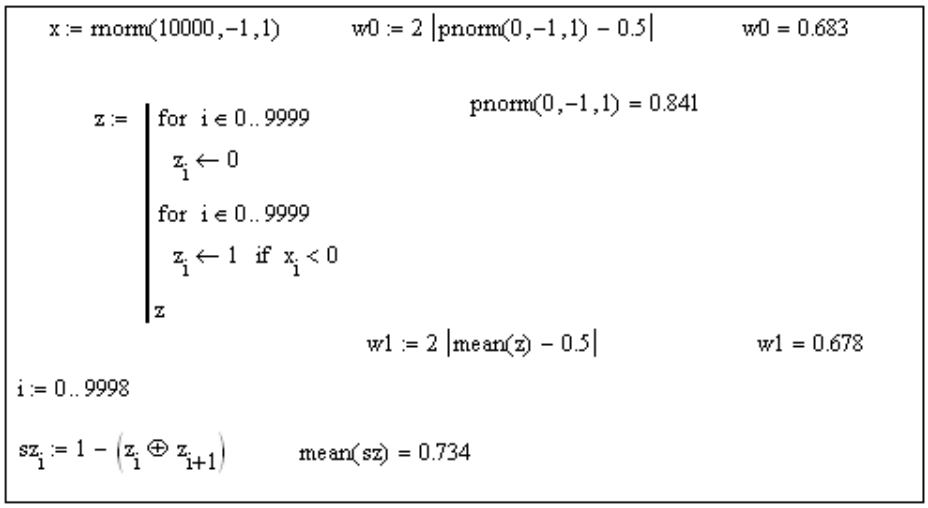


Рис. 11. Оценка показателя стабильности через усреднение пар разрядов кода, свернутых по Хэммингу

Операция усреднения парных сверток Хэмминга длинных последовательностей всегда приводит к нормализации распределения полученных данных. И сам контролируемый параметр – w и усредненная парная свертка Хэмминга описываются близкими нормальными распределениями данных, имеющими очень сильную корреляционную связь $r = 0.86$.

При подобных вычислениях присутствует мультипликативная методическая ошибка, которая исчезает в предельных точках w = 0 и w = 1. Эта ошибка составляет порядка 7% и при необходимости может быть скомпенсирована.

Очевидно, что при полностью коррелированных данных, соответствующий выходной кубит нейросетевой молекулы полностью вырождается (данные становятся полностью детерминированными, предсказуемыми). По мере снижения предсказуемости данных вычислительный потенциал воспроизводимого кубита растет, однако этот потенциал не может быть слишком высоким. Потенциал воспроизводимого кубита должен соответствовать конкретной решаемой задаче.

10. Оценка значения показателя квантовой сцепленности пар кубит нейросетевой молекулы через вычисление коэффициента взаимной корреляции

Один кубит, даже имеющий высокий вычислительный потенциал, бесполезен. Эффект повышения скорости вычисления или эффект снижения требований к точности исходных данных достигается, только когда кубит вычислителя становится достаточно много и они между собой верно сцеплены под конкретные условия решаемой задачи. В связи с этим возникает необходимость

контроля показателя квантовой сцепленности пар выходных кубит нейросетевой молекулы. Схема оценки высокого уровня сцепленности выходных данных образа «Свой» приведена на рисунке 12.

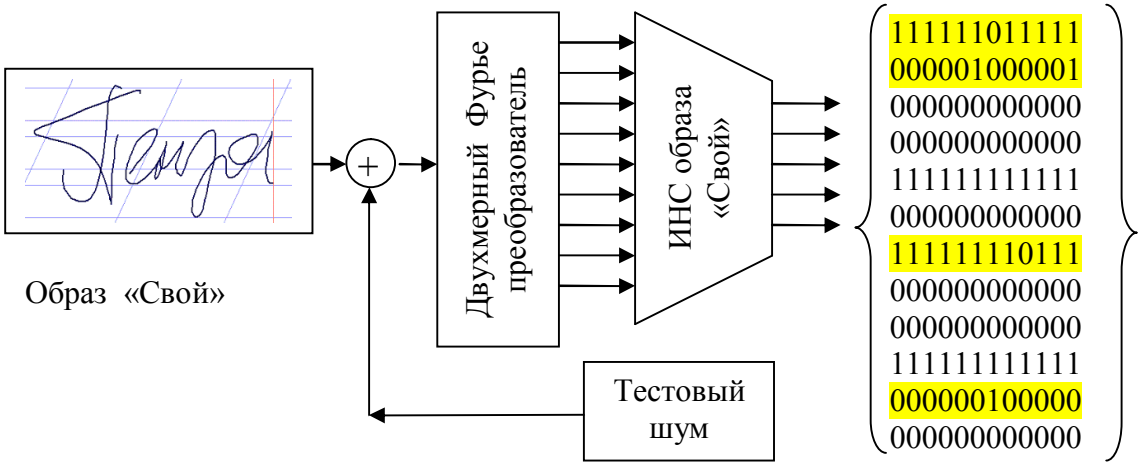


Рис. 12. Отклик обученной нейронной сети на известный ей образ «Свой», размытый тестовым шумом

Подобная схема поддержки квантовой суперпозиции интересна, когда требуется обеспечить высокий уровень доступности, например, за счет корректировки ошибок [10, 11]. Глядя на выходные коды нейросети, легко выявить нестабильные биты, они помечены заливкой. Когда оценивается стойкость нейросетевого преобразователя к атакам подбора, используется схема тестирования, приведенная на рисунке 13.

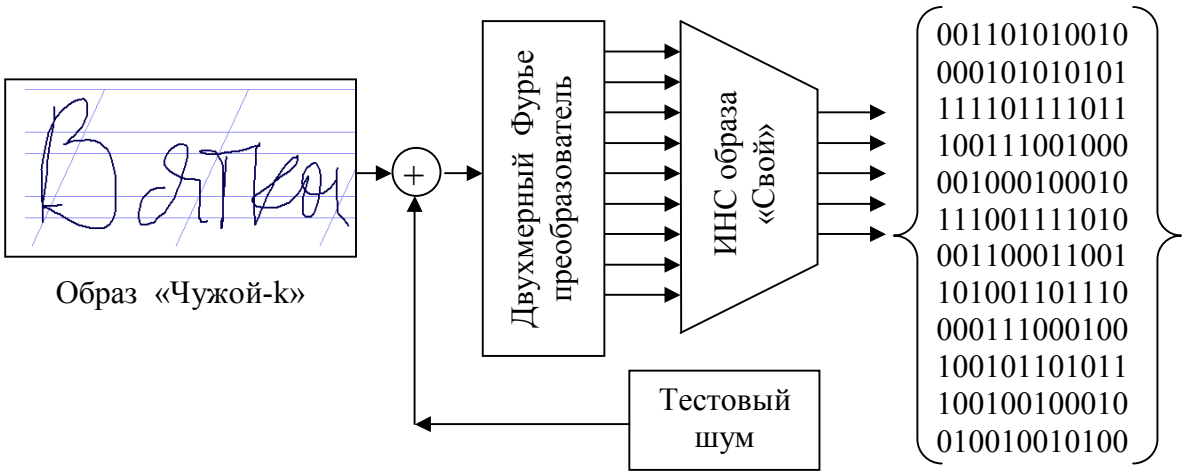


Рис. 13. Отклик искусственной нейронной сети на неизвестный ей образ «Чужой», размытый тестовым шумом

Для схемы тестирования рисунка 12 стабильность каждого разряда выходного кода высока $w_i \approx 1$, что эквивалентно сильному уровню коррелированности пар выходных разрядов нейросетевой молекулы $|r_{i,j}| \approx 1$. Иная ситуация возникает при тестировании нейросетевой молекулы по схеме, изображенной на рисунке 13, где показатель стабильности выходных разрядов нейросетевой молекулы падает до уровня $w_i \approx 0{,}5$. В этом случае задача контроля уровня коррелированности пар выходных разрядов (парной сцепленности кубит) становится актуальной. На рисунке 14 приведена программа имитационного

моделирования состояний нейрона при его возбуждении разными входными данными образа «Чужой».

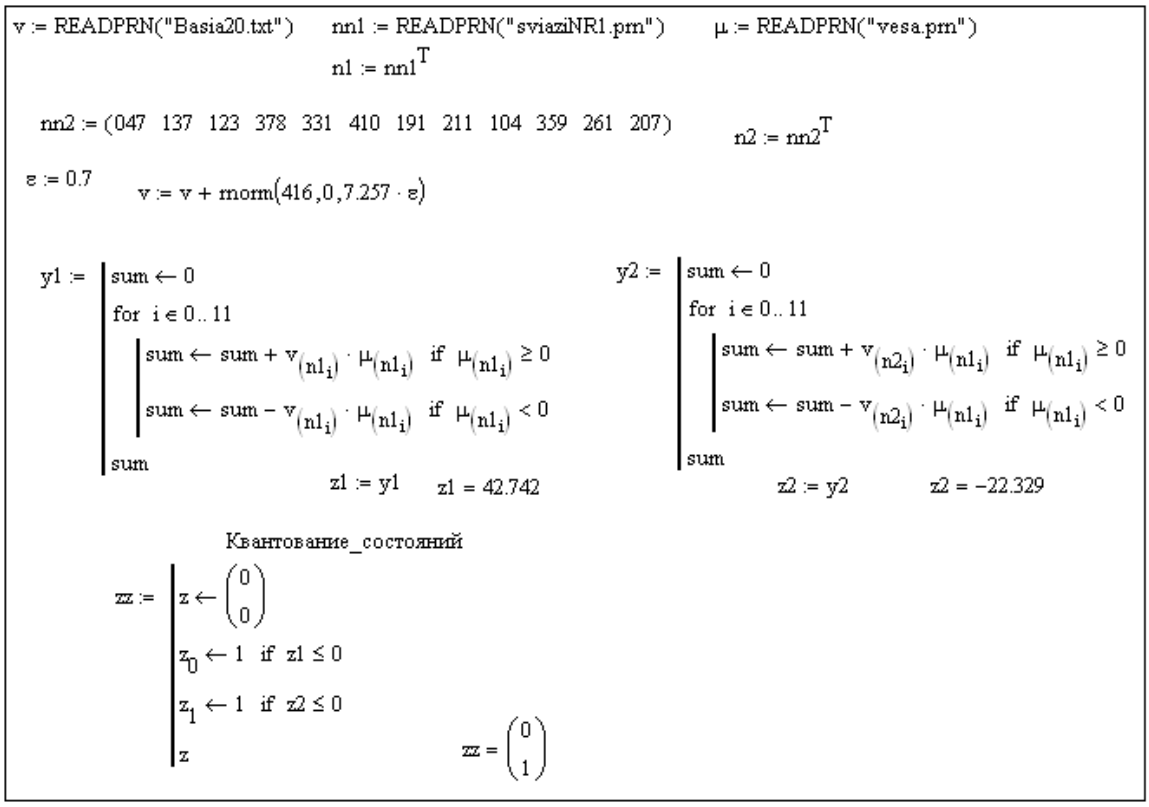


Рис. 14. Получение двух выходных состояний нейрона, при подаче на его входы разных данных образа «Чужой»

Из рисунка 14 видно, что при возбуждении нейрона разными входными данными его состояния меняются. Нет принципиальной разницы между возбуждением одного нейрона разными данными образа «Чужой» и двух нейронов по разному обученных. Из-за случайности выбора связей и случайного характера случайно, выбранного образа «Чужой» результат в среднем получается такой же. Выбор одного нейрона вместо двух обусловлен желанием уменьшить размер программы рисунка 14. Многократный запуск этой программы и запоминание результатов ее работы позволяет получить конкретные данные, условно отображенные на рисунке 13, и вычислить по ним коэффициент корреляции двух бинарных векторов. Для данных образа «Basia20.txt» уровень коррелированности составляет $r \approx 0{,}319$, что хорошо отражает реальную ситуацию и согласуется с другими численными экспериментами.

11. Вычисление вероятности ошибок второго рода для нейросетевого преобразователя биометрия-код в пространстве расстояний Хэмминга

Каждый нейрон нейросетевой молекулы смотрит на предъявленный биометрический образ со своего ракурса в пространстве своей размерности. Чем больше нейронов в нейросетевом преобразователе, тем надежнее он способен отличать образ «Свой» от образа «Чужой» или образов «Все Чужие». При использовании нейронной сети из 256 нейронов среды моделирования «БиоНейроАвтограф» вероятность появления ошибок второго рода (пропуск образа «Чужой» как образа «Свой») мала. Для оценки вероятности ошибок второго рода обычными методами требуется создавать тестовые базы биометрических

образов очень большого размера. Обойти проблему сбора больших баз биометрических образов удается в том случае, когда мы переходим из пространства обычных кодов в 2^{256} состояний в более компактное пространство расстояний Хэмминга:

$$h = 256 - \sum_{i=1}^{256} "c_i" \oplus "x_i" \qquad (7),$$

где $"c_i"$ - разряд кода «Свой»; $"x_i"$ - разряд кода «Чужой».

В новом пространстве расстояний Хэмминга будет существовать только (256+1)=257 состояний, что приводит к существенному снижению требований к объему тестовой выборки. Упрощение вычислений связано с тем, что свертка Хэмминга (7) является хорошим нормализатором (при ее вычислении осуществляется суммирование 256 слагаемых). Это свойство использовано стандартом ГОСТ Р 52633.3 [13], который рекомендует выполнять тестирование по схеме, приведенной на рисунке 15.

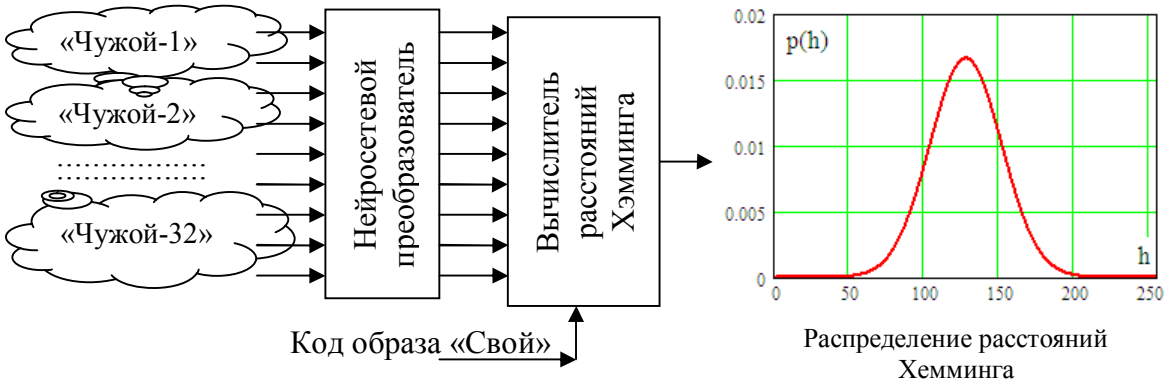


Рис. 15. Оценка вероятности ошибок второго рода, обученного нейросетевого преобразователя

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) расстояний Хэминга и стандартное отклонение - σ(h) расстояний Хэмминга. Располагая этими данными, мы можем приближенно определить вероятность ошибок второго рода по следующей формуле:

$$P_2 \approx \frac{1}{\sigma(h)\sqrt{2\pi}} \int_{-\infty}^{1} \exp\left\{\frac{-(E(h)-u)^2}{2(\sigma(h))^2}\right\} \cdot du \qquad (8).$$

Вероятность полного совпадения кода «Свой» и кода «Чужой» h=0 оценивается как вероятность попадания в интервал от -∞ до 1 непрерывного нормального распределения (8), что является избыточным. То есть оценка (8) является оценкой сверху вероятности ошибок второго рода.

12. Оценка усредненной сцепленности 256 кубит нейросетевой молекулы через 256-мерную энтропию ее выходных состояний

Если бы кубиты на выходах нейросетевой молекулы были бы идеальными (отсуствовала корреляция между парами кубит, тройками кубит, четверками кубит и так далее), то распределение расстояний Хэмминга было бы нормальным и имело бы математическое ожидание 128 бит, а стандартное отклонение 8 бит. Это следует из биномиального закона распределения для 256 степеней свободы и равновероятного выпадения состояний «0» и «1». Условие равновероятного

состояния выпадения состояний «0» и «1» хорошо выполняется из-за того, что нейросетевой преобразователь обучался по ГОСТ Р 52633.5 [9].

В случае E(h)=128, σ(h)=8 полностью случайные коды нейросетевой молекулы можно было бы использовать как криптографические ключи длиной 256 бит. То есть энтропия каждого разряда такого ключа 1 бит, а так как разряды независимы, то общая энтропия ключа должна составить 256 бит. При этом вероятность угадывания кода ключа с первой попытки должна быть 2^{-256}.

В нашем случае мы имеем вероятность второго рода (угадывания биометрического образа с первой попытки) много выше $P_2 \approx 2^{-25}$, что соответствует длине ключа в 25 бит и такой же его энтропии в 25 бит.

Последнее означает, что 256-ти мерная энтропия выходных кодов нейросетевого преобразователя может быть вычислена по следующей простой формуле:

$$H("x_1, x_2, ..., x_{256}") = -\log_2(P_2) \approx 25 \qquad (9).$$

Из-за того, что между разрядами выходных кодов присутствуют корреляционные связи $r_{i,j} \approx 0.319$, эквивалентный ключ оказывается примерно в 10 раз короче, чем идеальный ключ, получаемый от 256 полностью независимых генераторов.

Для нас важно так же то, что квантовые компьютеры «будущего» с «новой» элементной базой, охлаждаемой жидким гелием [14, 15], ориентируются на то, что их аппаратные кубиты будут близки к идеальным. В рамках квантовой механики создать близкие к идеальным кубиты так же сложно как и в рамках нейродинамики. Скорее всего, для каждого типа математических задач и их аппаратной поддержки существует свой предел (асимптота улучшения идеальности среднего кубита и средней сцепленности между кубитами).

В нашем случае поддержания в динамике нейросетевых молекул число реальных кубит будет всегда примерно в 10 раз меньше, чем число выходов нейросетевого преобразователя биометрия-код. Усложнение конструкций нейронов [16, 17] приводят к росту числа идеальных эквивалентных кубит нейросетевой молекулы при том же числе ее выходов.

13. Симметризация корреляционных связей и их программное моделирование

Когда корреляционные связи в исходных данных отсутствуют, то для их моделирования достаточно использовать несколько независимых программных генераторов. Для воспроизведения этой ситуации можно воспользоваться короткой программой, приведенной на рисунке 16.

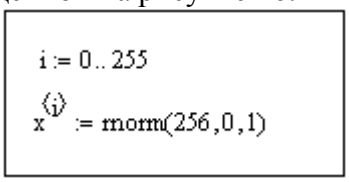


Рис. 16. Программа создания 256 независимых векторов псевдослучайных чисел

Для того чтобы сделать случайные данные одинаково зависимыми, можно воспользоваться симметричной связывающей матрицей. Пример соответствующей программы приведен на рисунке 17.

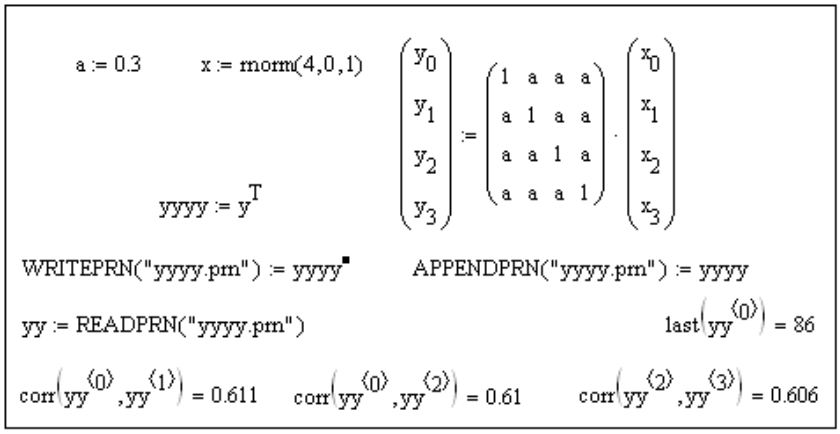


Рис. 17. Программа, использующая связывающую данные симметричную матрицу для получения четырех векторов одинаково коррелированных данных

Работа программы, отображенной на рисунке 17, не нуждается в пояснениях, однако ей нельзя пользоваться, когда для моделирования применяются стандартные средства MathCAD, MathLAB, STATISTICA. Из-за необходимости работать с симметричными матрицами большой размерности быстро кончается оперативная память компьютера, вычисления становятся очень медленными или вообще не выполняются.

При моделировании векторов зависимых данных следует применять простой технический прием, отраженный в программе, приведенной на рисунке 18.

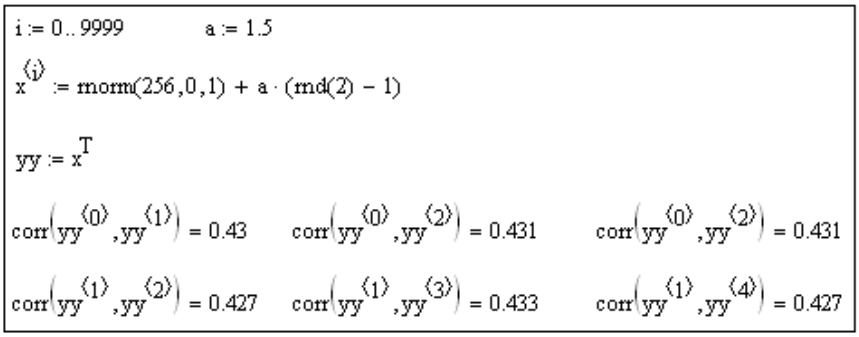


Рис. 18. Программное обеспечение, создающее 1000 векторов-столбцов из 256 случайных одинаково коррелированных данных

Из рисунка 18 видно, что вычисленные по выборке в 10 000 опытов коэффициенты одинаковой коррелированности различаются во втором и третьем знаках. Более точным получается результат после усреднения по 100 коэффициентам равной коррелированности. В таблице №1

Таблица № 1. Связь регулируемого параметра и коэффициентов одинаковой коррелированности для вектора из 256 зависимых отсчетов

n	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
a	0	0.3	0.5	0.8	1	1.1	1.3	1.5	2	3	4	5	6	7	8	9
r	0	0.03	0.075	0.172	0.251	0.288	0.357	0.429	0.574	0.748	0.842	0.893	0.924	0.942	0.955	0.964

Изменение длины вектора связываемых данных приводит к необходимости вычисления другой таблицы связи.

14. Приближенная оценка 256-мерной энтропии по значениям расстояний Хэмминга для нейросети с одинаковой коррелированностью выходных состояний нейронов

Предположим, что данные на выходах 256 нейронов оказались одинаково коррелированными. В этом случае, изменяя только один параметр, мы можем отследить связь изменения значения 256-мерной энтропии выходных кодов со значением равной коррелированности исходных данных.

Для этой цели необходимо выполнить квантование 256-ти мерных векторов зависимых данных. Далее следует принять код ключа «Свой» состоящим только из нулей "$\bar{c}$"="00000.....00000". Тогда подсчет нескольких значений расстояний Хэмминга упрощается до простого подсчета единичных разрядов в коде. Программа для вычисления вектора из 50 расстояний Хэмминга для зависимых данных приведена на рисунке 19.

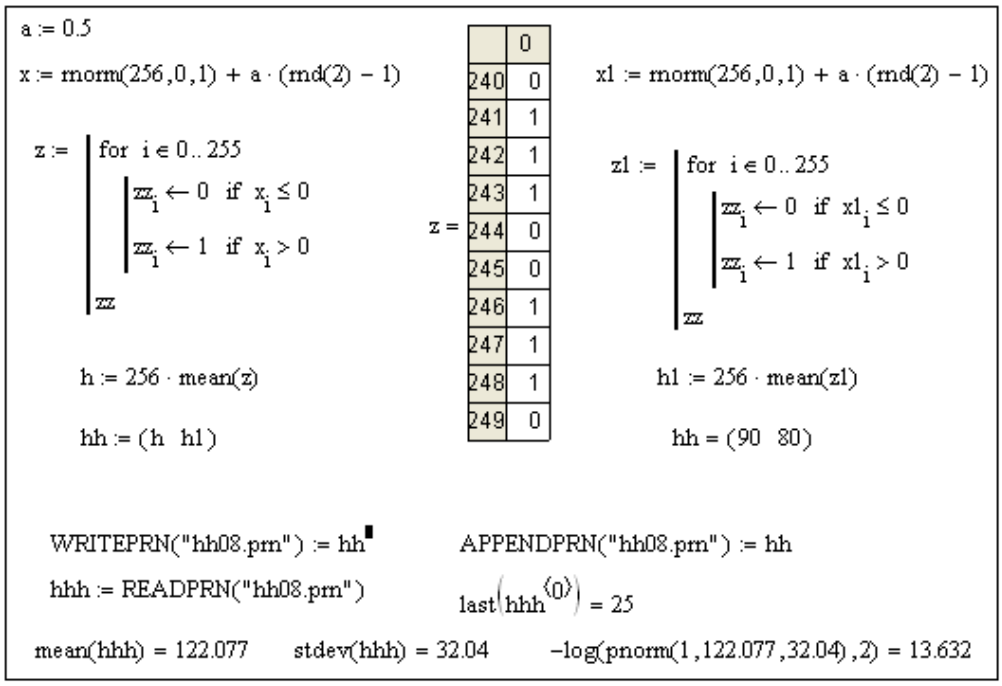


Рис. 19. Вычисление энтропии зависимых кодов по 50 значениям расстояний Хэмминга

Из рисунка 19 видно, что уже при небольших значениях коррелированности, наблюдается существенное снижение энтропии с 256 бит до 13.632 бит. Так же следует иметь в виду, что оценка энтропии в пространстве расстояний Хэмминга является оценкой снизу. Реальная энтропия всегда оказывается выше той, что дает программа рисунка 19.

15. Переход от 256-ти мерной энтропии к легко вычисляемым корреляционным функционалам той же размерности

Выше мы оценили через переход в пространство расстояний Хэмминга 256-мерную энтропию, опираясь на симметризацию корреляционных связей. При симметризации мы воспользовались показателем равной коррелированности, который в первом приближении можно вычислить, усредняя модули всех коэффициентов корреляцонной матрицы 256x256:

$$E_{256}(|r|)=\frac{1}{256^2-256}\left\{\left(\sum_{i=1}^{256}\sum_{j=1}^{256}|r_{i,j}|\right)-256\right\} \qquad (10).$$

Естественно, что при вычислениях усреднения по матрицам высокой размерности приходится привлекать существенные вычислительные ресурсы из-за квадратичной вычислительной сложности, решаемой задачи. В этом отношении вычисление 256-ти мерной энтропии является гораздо более экономичной процедурой, так как она имеет линейную вычислительную сложность и выполнима на малой выборке из 50 примеров (смотри программу рисунка 19).

В связи с этим возникает желание создать более эффективный в вычислительном отношении корреляционный функционал столь же высокой размерности [1]:

$$R_{256}(|r|)=\left\{1-\frac{H("x_1,x_2,....,x_{256}")}{256}\right\} \qquad (11).$$

В ситуации, когда корреляционные связи на выходах нейронов полностью отсутствуют, корреляционный функционал становится нулевым. При предельной корреляционной связанности выходных данных нейронов корреляционный функционал (11) становится единичным. Знак у корреляционных функционалов этого типа всегда положителен.

Очевидно, что размерность корреляционных функционалов (11) может быть любой.

16. Вычисление сверток Хэмминга по модулю 256

Переход в пространство расстояний Хэмминга дает возможность оценивать энтропию длинных паролей. При этом энтропию можно вычислять как в пространстве обычных расстояний Хэмминга, так и в пространстве сверток Хэмминга по модулю 256 [1, 18] (смотри программу рисунка 20).

T := "book is intended" ETOL := str2vec(T) last(ETOL) = 15

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 private keys are used "fuzzy
extractors". "

TXT := str2vec(TTT) last(TXT) = 365

i := 0..(365 − 15)

$$h256_i := \sum_{j=0}^{15} |TXT_{j+i} - ETOL_j|$$

$h256^T =$

	0	1	2	3	4	5	6	7	8	9
0	220	387	445	461	405	397	377	231	405	375

mean(h256) = 399.806 stdev(h256) = 98.965

−log(pnorm(1,399.806,98.965),2) = 15.129 $\frac{15.129}{16} = 0.946$

Рис. 20. Программа расчета энтропии осмысленного длинного пароля на английском языке в пространстве сверток Хэмминга по модулю 256

Целесообразность перехода к сверткам Хэмминга по модулю 256 обусловлена тем, что кодировка текстов на русском и английском языке осуществляется в стандарте ASCII (8 бит кода на один знак текста). Получается, что несущие смысл знаки текста должны сравниваться друг с другом в метрике 256 состояний (число состояний 8 бит кода). При переходе к использованию нейронов с несколькими выходными состояниями [16, 17] так же придется применять свертки Хэмминга по модулю, точно совпадающему с числом состояний у квантователей каждого из нейронов. Так как разные нейроны преобразователя биометрия-код могут иметь квантователи с разным числом состояний, то видимо придется использовать свертки Хэмминга с изменяющимся модулем по мере перехода вдоль анализируемой кодовой последовательности.

17. Многообразие функционалов, оценивающих уровень сцепленности групп выходных кубит нейросетевой молекулы

Когда мы рассматриваем одиночный кубит, то для его описания достаточно только вероятности появления одного из его состояний, например, $P(\text{"0"})$. Вторая использованная нами статистическая характеристика - показатель стабильности состояний - w (1) избыточна, так как она легко получается из первой статистической характеристики.

Ситуация меняется, когда приходится описывать показатели сцепленности групп кубит на выходе нейросетевой молекулы. Во первых, в одну группу кубиты могут объединяться по разному. Самый простой вариант, когда в одну группу объединяются кубиты рядом расположенных нейронов. Этот способ объединения отображен в левой части рисунка 21.

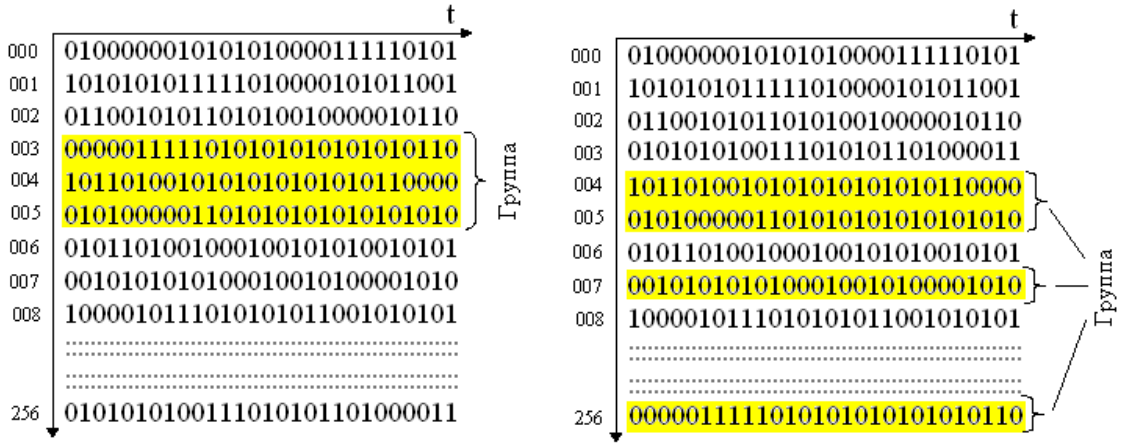


Рис. 21. Разные способы объединения кубит в одну группу

Вполне реальна иная ситуация, когда объединяемые в одну группу кубиты имеют случайные номера нейронов. Способ объединения кубит нейронов в одну группу должен быть задан заранее. Очевидно так же, что каждая группа выходов нейронов должна характеризоваться числом ее членов – m. Определившись с размером группы и ее составом, мы всегда можем вычислить вероятности появления состояния ноль в каждом из кубит $\{P_0(\text{«0»}), P_1(\text{«0»}), \ldots, P_m(\text{«0»})\}$. Этот вектор статистических данных всегда может быть сведен к двум его интегральным характеристикам таким, как математическое ожидание $E\{P_i(\text{«0»})\}$ и стандартное отклонение $\sigma\{P_i(\text{«0»})\}$ по группе.

Как еще один вариант группового описания сцепленности группы кубит может быть использован вектор показателей стабильности $\{w_0, w_1, \ldots, w_m\}$ и их младшие статистические моменты $E_m(w_i)$ и $\sigma_m(w_i)$.

Почти эквивалентом показателей стабильности являются показатели автокорреляции состояний соседних разрядов $\{r_0, r_1, \ldots, r_m\}$ и их младшие статистические моменты $E_m(r_i)$ и $\sigma_m(r_i)$.

Кроме того, взаимное статистическое влияние кубит друг на друга в группе может достаточно эффективно описываться через вычисление корреляционной матрицы. Обобщение матрицы парных коэффициентов корреляции должно выполняться через вычисление младших статистических моментов модулей ее элементов $E_m\left(\left|r_{i,j}\right|\right)$ и $\sigma_m\left(\left|r_{i,j}\right|\right)$.

Еще одним направлением создания эффективных функционалов для контроля сцепленности кубит в группе является вектор сверток Хэмминга по модулю два $\{h_0, h_1, \ldots, h_m\}$ и их младших статистических моментов $E_m(h_i)$, $\sigma_m\left(\left|h_i\right|\right)$. Однако такие же вектора могут быть получены и для сверток Хэмминга по любому иному модулю. Модуль зависит от особенностей реализации нейросетевой молекулы.

Следует отметить, что пара интегральных биометрических статистик $E_m(h_i)$ и $\sigma_m\left(\left|h_i\right|\right)$ дает возможность перейти к вычислению вектора значений m-мерной энтропии биометрических образов «Чужой» - $\{H_{0,m}, H_{1,m}, \ldots, H_{k,m}\}$, эти данные являются обобщенными показателями сцепленности кубит при воздействии на нейросетевую молекулу разными образами «Чужой». Естественно, что над вектором значений энтропии мы можем выполнить операции по вычислению младших статистических моментов $E_m\left(H_{i,m}\right)$, $\sigma_m\left(\left|H_{i,m}\right|\right)$.

Тот факт, что в пространстве сверток Хэмминга оценка m-мерной энтропии имеет почти линейную вычислительную сложность, позволяет перейти к достаточно просто вычисляемым корреляционным функционалам высокой размерности $\{R_{0,m}, R_{1,m}, \ldots, R_{k,m}\}$ и их младшим статистическим моментам $E_m\left(R_{i,m}\right)$, $\sigma_m\left(\left|R_{i,m}\right|\right)$.

Следует отметить, что все перечисленное выше показатели сцепленности кубит нейросетевой молекулы дополняют друг друга, но не исчерпывают. Вычислительные машины, ориентированные на работу с образами (ОВМ), могут иметь разную специализацию и разное представление образов. Так информация об образах может быть представлена k обученными нейронными сетями и/или примерами образов «Свой-k».

Например, в 2010 году в лаборатории биометрических и нейросетевых технологий АО «ПНИЭИ» была реализована ОВМ для решения обратной задачи нейросетевой биометрии. По условиям этой задачи нужно было восстановить код образа «Свой» и распределения его биометрических параметров, имея базу из 10 000 образов «Чужой». Под решение этой задачи была написана специализированная ОВМ [2], работающая с одной нейронной сетью «Свой» и миллиардами биометрических образов, синтезированных по ГОСТ Р 52633.2 [19] из исходной базы в 10 000 образов «Чужой». По сути дела специализированная ОВМ осуществляет направленный синтез биометрических образов, двигаясь в сторону образа «Свой» и инверсии образа «Свой». При этом параллельно вычислялись две свертки Хэмминга:

$$\begin{cases} h = 256 - \sum_{i=1}^{256} "c_i" \oplus "x_i" \\ h_{\neg} = 256 - \sum_{i=1}^{256} "c_i" \oplus "\neg x_i" = 256 - \sum_{i=1}^{256} "\neg c_i" \oplus "x_i" \end{cases} \quad (12).$$

Необходимость вычисления двух сверток Хэмминга для прямых и инверсных кодов порождается особенностями решаемой задачи. Более того, оказалось, что взвешенные показателями стабильность разрядов кода свертки Хэмминга имеют большую мощность [20, 21]:

$$\begin{cases} h_w = 256 - \sum_{i=1}^{256} w_i(\xi) \cdot ("c_i" \oplus "x_i") \\ h_{\neg w} = 256 - \sum_{i=1}^{256} w_i(\xi) \cdot ("\neg c_i" \oplus "x_i") = 256 - \sum_{i=1}^{256} w_i(\xi) \cdot ("c_i" \oplus "\neg x_i") \end{cases} \quad (13).$$

Рост мощности показателей сцепленности (13) по сравнению с показателями сцепленности (12) обусловлен тем, что ослабляется влияние нестабильных кубит на конечный результат оценки. Численно рост мощности показателей проявляется через снижение числа поколений направленного синтеза биометрических образов при работе ОВМ для достижения заданного уровня похожести образов.

Приведенный выше пример интересен тем, что позволяет легко перейти от подчеркивания влияния стабильных разрядов кода (вырожденных кубит) к их подавлению. Для этого достаточно выполнить следующие вычисления:

$$\begin{cases} h_w = 256 - \sum_{i=1}^{256} (1 - w_i(\xi)) \cdot ("c_i" \oplus "x_i") \\ h_{\neg w} = 256 - \sum_{i=1}^{256} (1 - w_i(\xi)) \cdot ("\neg c_i" \oplus "x_i") = 256 - \sum_{i=1}^{256} (1 - w_i(\xi)) \cdot ("c_i" \oplus "\neg x_i") \end{cases} \quad (14).$$

Преобразование (14) подчеркивает влияние полноценных кубит нейросетевой молекулы на результат оценки их сцепленности, подавляя влияние стабильных разрядов кода. Мы наблюдаем то, что один из перечисленных ранее показателей сцепленности может быть использован как весовая функция при вычислении другого показателя.

Заключение

Классическая теория «квантовой механики» сложна для понимания, применения, преподавания. Динамическое уравнение Шредингера является крайне неудобным объектом для моделирования на обычном компьютере. Для воспроизведения динамического уравнения Шредингера на обычном компьютере требуются пакеты программ, состоящие из сотен тысяч сток кода. Эта задача имеет экспоненциальную вычислительную сложность. Существует даже теорема о том, что на обычном компьютере кубиты уравнения Шредингера воспроизводить нет смысла.

Совершенно иная ситуация возникает, когда мы используем статическое уравнение обычной нейронной сети. Перейти в нейродинамику не сложно, достаточно размазать статические данные белым шумом. Для воспроизведения режима поддержки нейродинамики достаточно самостоятельно написанных программ в 10 строк. Даже столь простые программы позволяют наблюдать квантовые эффекты нейродинамики, когда нейронная сеть имеет десятки и сотни выходных разрядов. Каждый из сотен этих разрядов оказывается сцеплен с соседями и «дрожит», его можно рассматривать как кубит.

У таких программных конструкций нет ограничений по числу воспроизводимых кубит и по времени поддержания их в режиме квантовой суперпозиции [1]. Это означает, что можно создавать полноценные квантовые компьютеры на обычных компьютерах без их охлаждения жидким гелием. Более того мы с Вами оказываемся умными только потому, что в наших головах уже реализована нейродинамика, непрерывно поддерживающая квантовую суперпозицию сотен и тысяч кубит. Это позволяет нашим головам быть

супервычислителями даже при тактовой частоте работы с образами всего в 10 Герц. Мы осуществляем супервычисления, потому что уже поддержка квантовой супервозиции в 40 полноценных кубит позволяет нам догнать обычные компьютеры с тактовой частотой в 10 гигоГерц. Реализация в наших головах квантовой суперпозиции под 60 полноценных кубит никогда не позволит «камням» современных процессоров с обычной математикой догнать нас по уровню интеллекта. У искусственного интеллекта появляется шанс догнать людей по уровню их разумности только, если удастся реализовать на обычных компьютерах образные вычисления с достаточно большим числом эквивалентных полноценных кубит.

В данном учебном пособии описаны несколько показателей, позволяющих оценивать уровень сцепленности кубит, порождаемых нейродинамикой. То, что единого показателя нет, не является трагедией. При решении практических задач приходится использовать несколько показателей сцепленности, одни показатели могут бы заменены на другие. Могут так же быть использованы их комбинации.

ЛИТЕРАТУРА:

1. *Иванов А.И.* Многомерная нейросетевая обработка биометрических данных с программным воспроизведением эффектов квантовой суперпозиции. Издательство АО «ПНИЭИ», Пенза-2016 г., 133 с. Свободный доступ http://пниэи.рф/activity/science/BOOK16.pdf

2. *Волчихин В.И., Иванов А.И.* Нейросетевая молекула: решение обратной задачи биометрии через программную поддержку квантовой суперпозиции на выходах сети искусственных нейронов. //Вестник Мордовского университета. Т27. №4, 2017, с 518-523.

3. *Иванов А.И.* Простейшие оракулы, обученные корректировать ошибки вычисления младших статистических моментов на малых выборках биометрических данных. Учебное пособие. Издательство АО «Пензенский научно-исследовательский электротехнический институт», 2018 г., 35 с. http://пниэи.рф/activity/science/noc/BOOK18.pdf

4. ГОСТ Р 52633.5-2011 «Защита информации. Техника защиты информации. Автоматическое обучение нейросетевых преобразователей биометрия-код доступа».

5. *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/bioneuroautugraph.zip для свободного использования университетами России, Белоруссии, Казахстана.

6. *Иванов А.И.* Автоматическое обучение больших искусственных нейронных сетей в биометрических приложениях. Учебное пособие по курсу лабораторных работ. Пенза-2013 г. 30 с. http://пниэи.рф/activity/science/noc/tm_IvanovAI.pdf

7. *Саймон Хайкин.* Нейронные сети: полный курс. М.: «Вильямс», 2006. — С. 1104.

8. *Галушкин А.И., Цыпкин Я.З.* Нейронные сети: история развития. М. Радиотехника, 2001 г., 840 с.

9. ГОСТ Р 52633.5-2011 «Защита информации. Техника защиты информации. Автоматическое обучение нейросетевых преобразователей биометрия-код доступа».

10. *Иванов А.И., Безяев А.В., Елфимов А.В., Вятчанин С.Е.* Корректное квантово-континуальное преобразование данных, многократно ускоряющее оценку

вероятности ошибок биометрической аутентификации личности /«Специальная техника» 2017 г. № 1 с. 48-51.

11. *Волчихин В.И., Иванов А.И., Безяев А.В., Елфимов А.В., Юнин А.П.* Оценка эффекта ускорения вычислений, обусловленного поддержкой квантовой суперпозиции при корректировке выходных состояний нейросетевого преобразователя биометрии в код //«Известия высших учебных заведений. Поволжский регион. Технические науки. № 1, 2017 с. 43-55.

12. *Иванов А.И., Безяев А.В., Куприянов Е.Н.* Нейросетевая молекула: спектр показателей стабильности состояний выходных кубит нейросетевого преобразователя биометрия-код. // XXIII Международный симпозиум «Надежность и качество 2018». Том. 2., 15-18 мая 2018., с. 287-290.

13. ГОСТ Р 52633.3-2011 «Защита информации. Техника защиты информации. Тестирование стойкости средств высоконадежной биометрической защиты к атакам подбора».

14. *Нильсон М., Чанг И.* Квантовые вычисления и квантовая информация. М.: Мир. 2006 г. 821 с.

15. *Душкин Р.* Квантовые вычисления и функциональное программирование. М.: ДМК, 2015 г. 232 с. IBSN 978-5-97060-275-1

16. *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

17. *Волчихин В.И., Иванов А.И., Вятчанин С.Е., Малыгина Е.А. А*бсолютно устойчивый алгоритм автоматического обучения сетей вероятностных нейронов «Крамера - фон Мизеса» на малых выборках биометрических данных / Известия высших учебных заведений. Поволжский регион. Технические науки. 2017. № 2 (42). С. 55-65.

18. *Юнин А.П., Корнеев О.В.* Оценка энтропии легко запоминаемых, длинных паролей со смыслом в ASCII кодировке для русского и английского языков. // Труды научно-технической конференции кластера пензенских предприятий, обеспечивающих БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ. Том 10, Пенза-2016, с. 40-42 (http://пниэи.рф/activity/science/BIT/T10-p40.pdf)

19. ГОСТ Р 52633.2-2010 «Защита информации. Техника защиты информации. Требования к формированию синтетических биометрических образов, предназначенных для тестирования средств высоконадежной биометрической аутентификации»

20. *Иванов А.И., Сомкин С.А., Андреев Д.Ю., Малыгина Е.А.* О многообразии метрик, позволяющих наблюдать реальные статистики распределения биометрических данных «нечетких экстракторов» при их защите наложением гаммы. //Вестник Уральского федерального округа. Безопасность в информационной сфере. 2014 г. № *2(12)* с. 16-23.

21. *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

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 52633.7-20хх.

В период с 2017 г. по 2018 г. являлся руководителем разработки технической спецификации ТК26 (Криптографическая защита информации) «Защита нейросетевых биометрических контейнеров с использованием криптографических алгоритмов».

Учебное пособие.

Иванов Александр Иванович

Численная оценка показателей квантовой сцепленности выходных кубит нейросетевой молекулы преобразователя биометрических данных. Пенза – 2018 г. Издательство АО «Пензенский научно-исследовательский электротехнический институт» (АО «ПНИЭИ») – 27 с. http://пниэи.рф/activity/science/noc/BOOK18-2.pdf

Подписано к печати 27.04.2018 формат 60x80 1/16 Усл. печ. л. 0,97
Тираж 300 экз.

Издательство АО «ПНИЭИ», 440000, г. Пенза, ул. Советская, 9

Отпечатано с готового оригинал-макета в Издательстве ФБГОУ ВО «ПГУ»
440026, г. Пенза, ул. Красная, 44