http://vestnik.mrsu.ru
ISSN Print 0236-2910
ISSN Online 2313-0636

ИНФОРМАТИКА, ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА И УПРАВЛЕНИЕ / COMPUTER SCIENCE, COMPUTER ENGINEERING AND MANAGEMENT

УДК 577.33:004.4 DOI: 10.15507/0236-2910.027.201704.518-529

Нейросетевая молекула: решение обратной задачи биометрии через программную поддержку квантовой суперпозиции на выходах сети искусственных нейронов

В. И. Волчихин[1], **А. И. Иванов**[2*]
[1]*ФБГОУ ВО «Пензенский государственный университет» (г. Пенза, Россия)*
[2]*АО «Пензенский научно-исследовательский электротехнический институт» (г. Пенза, Россия)*
[*]*ivan@pniei.penza.ru*

Введение. Целью работы является многократное ускорение решения обратной задачи нейросетевой биометрии на обычном настольном компьютере.
Материалы и методы. Для ускорения вычислений искусственная нейронная сеть вводится в динамический режим «дрожания» состояний всех ее 256 выходных разрядов. При этом слишком большое число выходных состояний нейронной сети логарифмически свертывается путем перехода в пространство расстояний Хэмминга между кодом образа «Свой» и кодами образов «Чужой». Из базы образов «Чужой» выбирается 2,5 % наиболее похожих образов. В следующем поколении осуществляют восстановление 97,5 % отброшенных образов процедурами ГОСТ Р 52633.2-2010 путем скрещивания образов-родителей и получения от них образов-потомков.
Результаты исследования. За время порядка 10 мин удается осуществить 60 поколений направленого поиска решения обратной задачи, что дает возможность обращения матриц нейросетевых функционалов размерности 416 входов на 256 выходов с восстановлением до 97 % информации о неизвестных биометрических параметрах образа «Свой».
Обсуждение и заключения. Поддержка в течение 10 мин машинного времени 256-кубитной квантовой суперпозиции позволяет на обычном компьютере обойти актуальную бесконечность анализируемых состояний в 50^{50} (50 в степени 50) раз больше, чем мог бы сделать этот же компьютер, реализуя обычные вычисления. Увеличение длины поддерживаемой квантовой суперпозиции на 40 кубит эквивалентно увеличению тактовой частоты процессора приблизительно в 1 млрд раз. Именно по этой причине увеличение количества поддерживаемых кубит программным эмулятором квантовой суперпозиции более выгодно, чем создание более мощного процессора.

Ключевые слова: нейросетевой преобразователь биометрия-код, биометрические данные, большие размерности, программная поддержка квантовой суперпозиции, искусственные нейроны

Для цитирования: 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. 2017. Т. 27, № 4. С. 518–529. DOI: 10.15507/0236-2910.027.201704.518-529

Neural Network Molecule: a Solution of the Inverse Biometry Problem through Software Support of Quantum Superposition on Outputs of the Network of Artificial Neurons

V. I. Volchikhin[a], **A. I. Ivanov**[b*]
[a]*Penza State University (Penza, Russia)*
[b]*Penza Scientific Research Electrotechnical Institute (Penza, Russia)*
[*]*ivan@pniei.penza.ru*

Introduction. The aim of the study is to accelerate the solution of neural network biometrics inverse problem on an ordinary desktop computer.
Materials and Methods. To speed up the calculations, the artificial neural network is introduced into the dynamic mode of "jittering" of the states of all 256 output bits. At the same time, too many output states of the neural network are logarithmically folded by transitioning to the Hamming distance space between the code of the image "Own" and the codes of the images "Alien". From the database of images of "Alien" 2.5 % of the most similar images are selected. In the next generation, 97.5 % of the discarded images are restored with GOST R 52633.2-2010 procedures by crossing parent images and obtaining descendant images from them.
Results. Over a period of about 10 minutes, 60 generations of directed search for the solution of the inverse problem can be realized that allows inversing matrices of neural network functionals of dimension 416 inputs to 256 outputs with restoration of up to 97 % information on unknown biometric parameters of the image "Own".
Discussion and Conclusions. Supporting for 10 minutes of computer time the 256 qubit quantum superposition allows on a conventional computer to bypass the actual infinity of analyzed states in 50^{50} (50 to 50) times more than the same computer could process realizing the usual calculations. The increase in the length of the supported quantum superposition by 40 qubits is equivalent to increasing the processor clock speed by about a billion times. It is for this reason that it is more profitable to increase the number of quantum superpositions supported by the software emulator in comparison with the creation of a more powerful processor.

Keywords: neural network converter biometry-code, biometric data, large dimensions, software support of quantum superposition, artificial neurons

For citation: Volchikhin V. I., Ivanov A. I., Neural Network Molecule: a Solution of the Inverse Biometry Problem through Software Support of Quantum Superposition on Outputs of the Network of Artificial Neurons. *Vestnik Mordovskogo universiteta* = Mordovia University Bulletin. 2017: 27(4):518–529. DOI: 10.15507/0236-2910.027.201704.518-529

Введение

В 1980-е гг. Ю. Манин выдвинул идею создания квантовых, компьютеров, опирающихся на волновую математику квантовой механики уравнения Шредингера. Эта идея оказалась плодотворной, и математическая общественность за последующие 30 лет (1980–2010 гг.) создала под перспективную «квантовую» элементную базу ряд очень эффективных алгоритмов[1–2].

К сожалению, создание вычислительных элементов для квантовой математики уравнений Шредингера оказалось сложной задачей. На данный момент аппаратным путем удается воспроизвести квантовые алгоритмы на

[1] **Нильсон М., Чанг И.** Квантовые вычисления и квантовая информация. М. : Мир, 2006. 821 с.
[2] **Душкин Р. В.** Квантовые вычисления и функциональное программирование. ДМК-Пресс, 2015. 234 с.

несколько кубит. При этом время синхронизма (поддержания необходимой квантовой сцепленности) не превышает нескольких милисекунд. Появление в ближайшие несколько лет универсального квантового 256-кубитного компьютера представляется маловероятным.

Одним из направлений замещения отсутствующих квантовых вычислительных элементов является их имитационное моделирование на обычных компьютерах. Если усложнять задачу, увеличивая число электронов и протонов, то уже при 32 электронах потребуется использование супер-ЭВМ. В этом отношении уравнение Шредингера является крайне неудобным для эмулирования эффектов квантовой суперпозиции.

Обзор литературы

Гораздо более удобными оказываются другие уравнения, например, соответствующие хи-квадрат математической молекуле [1–3], корреляционной математической молекуле [4] или математической молекуле асимметрии распределения данных малой выборки [5]. Данные конструкции принципиально отличаются от молекулы водорода тем, что их уравнения просты для моделирования. Для достаточно точного моделирования молекулы водорода (уравнения Шредингера) на обычном компьютере необходимо программное обеспечение, состоящее из нескольких тысяч строк кода; для молекулы хи-квадрат с любым числом степеней свободы достаточно 5 строк кода на языке MathCAD[3]. Переход от приближенных вычислений пакетом из нескольких тысяч строк программного кода к точным вычислениям простыми программами кардинально меняет ситуацию. Моделирование даже малого числа кубит при их описании квантовой механикой уравнений Шредингера на обычном компьютере технически нецелесообразно из-за высокой сложности вычислений. При моделировании уравнения Шредингера наблюдается экспоненциальный рост вычислительной сложности с увеличением числа степеней свободы. Напротив, моделирование достаточно большого числа кубит простейших математических молекул оказывается рациональным, поскольку для этих конструкций рост вычислительной сложности прямо пропорционален росту числа степеней свободы (электронов или опытов).

Молекулу водорода H_2 можно рассматривать как некоторый не наблюдаемый внутренний генератор континуума возможных состояний электрона с не наблюдаемым внутренним квантователем его энергии. Например, квантователь может быть выполнен в виде планетарной модели атома с разрешенными орбитами, кратными некоторому целому числу фотонов [2–5]. В этом случае наблюдается не сама молекулу, а ее выходной спектр излучения. При этом, наблюдая положение спектральных линий на оси частот, можно очень точно оценить, присутствуют ли в той или иной пробе вещества молекулы водорода. На этом принципе строился спектральный анализ.

Материалы и методы

Конструкцию, аналогичную ранее созданным математическим молекулам, возможно создать для нейросетевого преобразователя биометрия-код, обученного по ГОСТ 52633.5[4]. Нейросетевой преобразователь следует рассматривать как некоторую нейросете-

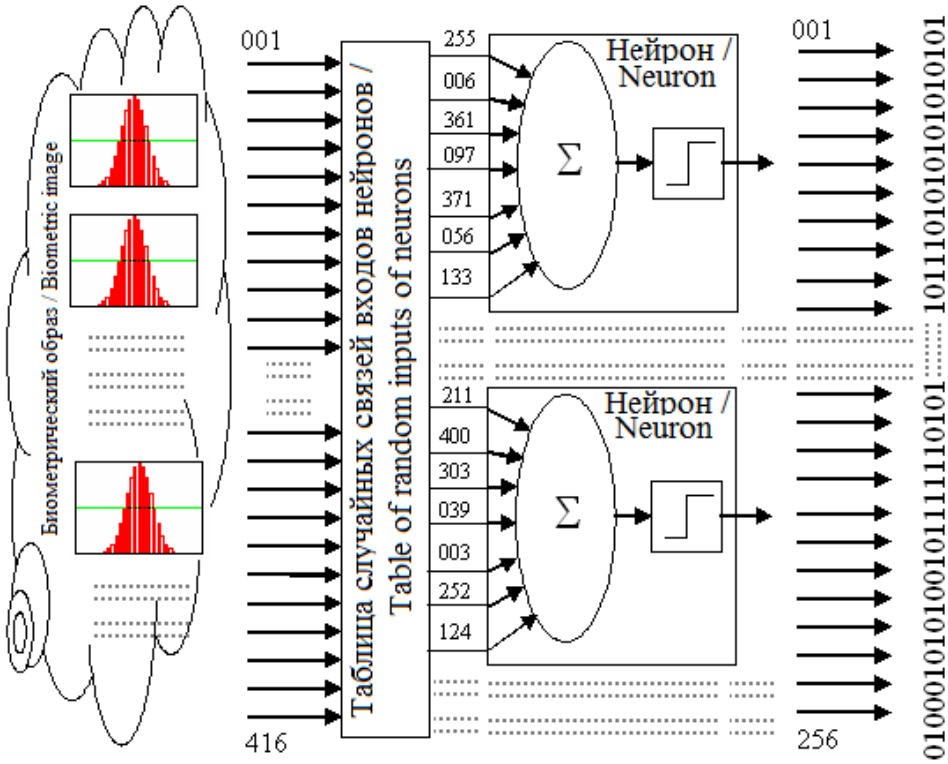
[3] **Иванов А. И.** Многомерная нейросетевая обработка биометрических данных с программным воспроизведением эффектов квантовой суперпозиции. Пенза : АО «ПНИЭИ», 2016. 133 с. URL: http://пниэи.рф/activity/science/BOOK16.pdf

[4] ГОСТ Р 52633.5-2011 «Защита информации. Техника защиты информации. Автоматическое обучение нейросетевых преобразователей биометрия-код доступа». URL: http://www.gostrf.com/normadata/1/4293797/4293797154.pdf

вую молекулу. Структура модели такой молекулы изображена на рис. 1.

Модель молекулы имеет 416 разных нормальных континуумов контролируемых биометрических параметров (при использовании среды моделирования «БиоНейроАвтограф»[5]) и 256 дискретных выхода (каждый из выходов может иметь состояние «0» или «1»[4]). Молекула состоит из 256 нейронов, каждый из которых отвечает за состояние одного выходного разряда. Всего выходной код может иметь 2^{256} состояний. Статистика этих состояний зависит от того, какой биометрический образ использован: если 416-мерный континуум примера образа «Свой», то на выходах нейронной сети с высокой вероятностью появляется стабильный (практически детерминированный) код образа "$\bar{c}$". Другими словами, обученная на образе «Свой» нейросеть устраняет естественную энтропию данных биометрического образа практически до нуля:

$$H("\bar{c}") \approx 0{,}03 \text{ бит.} \qquad (1)$$



Р и с. 1. Модель нейросетевой молекулы, откликающейся спектром выходных состояний на предъявленный ей биометрический образ

F i g. 1. Model of a neural network molecule responding with spectrum of output states to the biometric image presented

Совершенно иная ситуация возникает при использовании примеров образа «Чужой». В этом случае исходная энтропия биометрических примеров усиливается, а на выходах нейронной сети появляются случайные выходные коды. Каждый пример образа «Чужой» будет давать свой выходной

[5] **Иванов А. И., Захаров О. С.** Среда моделирования «БиоНейроАвтограф» : программный продукт. URL: http://пниэи.рф/activity/science/noc.htm

код, а энтропия этих кодов оказывается намного больше нуля:

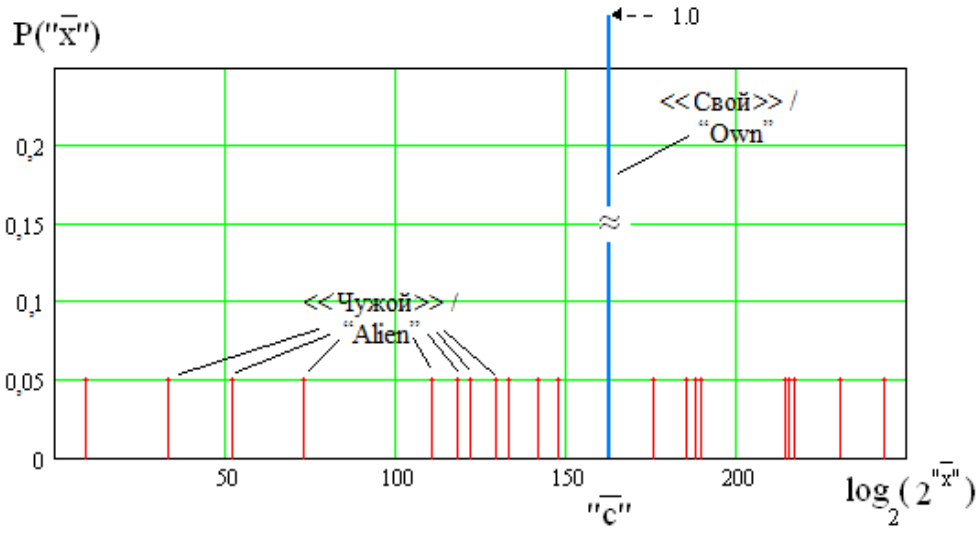
$$H("\bar{x}") \approx 27 >> 0,0 \text{ бит.} \qquad (2)$$

Это происходит несмотря на то, что собственная энтропия континуумов примеров образа «Свой» и «Чужой» сопоставимы:

$$H(\bar{v}) \approx H(\bar{\xi}) \text{ бит.} \qquad (3)$$

Выполнение свойств (1–3) обеспечивается процедурами автоматического обучения нейронной сети по ГОСТ Р 52633.5[6].

Если перейти к спектральному представлению выходных состояний нейросетевой молекулы, то для 21 примера образов «Свой» и «Чужой» мы получим вероятности появления спектральных линий, отображенные на рис. 2.



Р и с. 2. Вероятности появления спектральных линий нейросетевой молекулы при воздействии на нее 21 примером образа «Свой» и образа «Чужой»

F i g. 2. Probability of appearance of spectral lines of a neural network molecule upon exposure by 21 examples of the image of “Own” and the image of “Alien”

Из-за того что выходной код откликов образа «Чужой» случаен, на рис. 2 его спектральные линии имеют случайное положение и низкую интенсивность $P("\bar{x}") = 0,048$. Для образа «Свой» ситуация иная: все примеры дают один и тот же код, спектральная линия которого в 21 раз ярче спектральных линий кодов «Чужой».

Таким образом, достаточно просто отличить образ «Свой» от образа «Чужой» по спектру выходных состояний нейронной сети. Если спектр случаен и интенсивность линий примерно одинакова, то предъявлен образ «Чужой»; если спектр выходных состояний детерминирован – «Свой». Для принятия решения достаточно всего одного примера образа «Свой» или образа «Чужой», который при необходимости можно размножить до 20 или до 200 примеров путем введения в его дан-

[6] ГОСТ Р 52633.5-2011 «Защита информации. Техника защиты информации. Автоматическое обучение нейросетевых преобразователей биометрия-код доступа». URL: http://vsegost.com/Catalog/51/51407.shtml

ные «мутаций» и получения близких синтетических образов алгоритмами ГОСТ Р 52633.2[7].

Следует подчеркнуть, что подавая на вход нейронной сети размытые биометрические данные образа «Чужой», мы будем наблюдать нестабильность состояний каждого из 256 разрядов выходного кода. Исследуя коды, возможно вычислить для каждого i-го разряда вероятность появления состояния «0» и вероятность появления состояния «1», а также коэффициент корреляции между состояниями любой пары разрядов. Другими словами, каждый из «дрожащих» выходных разрядов выходного кода формально можно рассматривать как кубит, сцепленный с другими 256 кубитами. Следовательно, для 256-мерной сцепки кубит справедлива следующая формальная запись их квантовой суперпозиции[3]:

$$\left|\Psi(\bar{\xi})\right\rangle = \sum_{i=1}^{N} \beta_i \cdot \left|"x_1, x_2, ..., x_{256}"\right\rangle, \quad (4)$$

где $N = 2^{256}$.

Очевидно, что вычислить коэффициенты квантовой суперпозиции (4) технически невозможно из-за очень большого числа возможных состояний – N. Однако в рамках данной задачи нас мало волнуют все коэффициенты квантовой суперпозиции, кроме одного – β_c, который соответствует коду «Свой» – "$c_1, c_2, ... c_{256}$",. Только в случае совпадения кода «Чужой» и кода «Свой» запустится криптоалгоритм проверки и приведет к положительной биометрической аутентификации.

Если пользоваться традиционными алгоритмами перебора для оценки квадрата весового коэффициента β_c или вероятности ошибки второго рода P_2 ошибочного пропуска «Чужого», неизбежно столкновение со значительными техническими проблемами. Обойти эти трудности ГОСТ Р 52633.3[8] рекомендует через переход от обычных кодов в пространство расстояний Хэмминга между кодом «Свой» и кодами «Чужой»:

$$h = 256 - \sum_{i=1}^{256} ("c_i") \oplus ("x_i"). \quad (5)$$

Операция вычисления расстояний Хэмминга фактически является сверткой очень большого числа спектральных линий $N = 2^{256}$ до гораздо меньшего числа $n = \log_2(N) = 256$. Применение свертки Хэмминга – вынужденная мера, превращающая задачу огромной вычислительной сложности в обычную задачу.

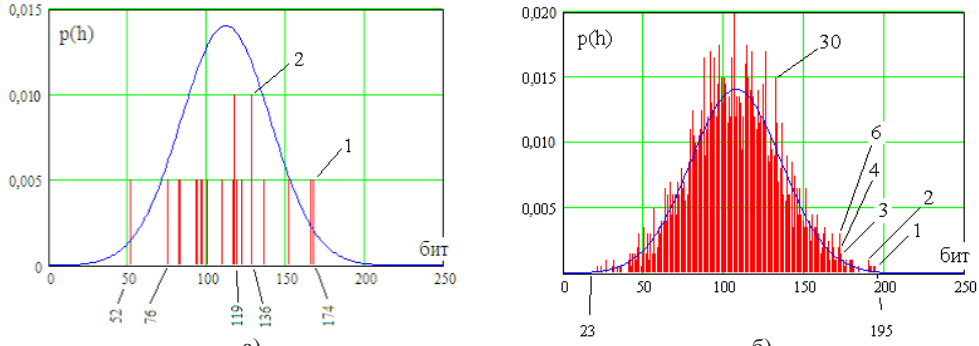
Одним из важных свойств свертки Хэмминга является нормализация распределений значений (рис. 3).

В численном эксперименте (Там же) всего наблюдаются 19 линий спектра, две из которых в 2 раза интенсивнее остальных 17 линий. Минимальное положение линии спектра – 52 бита, максимальное – 174 бита. По сути, это сильно прореженная гистограмма положения спектральных линий расстояний Хэмминга. У данной гистограммы 19 столбцов заполнены, а оставшиеся 174 – 50 – 19 = 105 столбцов – пусты.

Если из каждого из 21 примера образа «Чужой» вывести 99 близких примеров, то получится гистограмма распределения расстояний Хэмминга с гораздо более плотным заполнением столбцов. Как видно из рис. 3, б, гистограмма распределения значений расстояний Хэмминга уже не содержит пустых столбцов. В среднем каждый из столбцов гистограммы содержит порядка 15 опытов.

[7] ГОСТ Р 52633.2-2010 «Защита информации. Техника защиты информации. Требования к формированию синтетических биометрических образов, предназначенных для тестирования средств высоконадежной биометрической аутентификации» URL: http://vsegost.com/Catalog/50/50123.shtml

[8] ГОСТ Р 52633.3-2011 «Защита информации. Техника защиты информации. Тестирование стойкости средств высоконадежной биометрической защиты к атакам подбора» URL: http://vsegost.com/Catalog/51/51416.shtml



Р и с. 3. Пример распределения значений спектральных линий расстояний Хэмминга для 21 (а) и 2 100 (б) примеров образа «Чужой»

F i g. 3. Example of the distribution of Hamming distance spectral values for 21 examples of the image “Alien” (a) and 2 100 examples of the same image (b)

Тот факт, что распределение расстояний Хэмминга для большого числа опытов является нормальным, позволяет достаточно просто вычислять вероятность ошибок второго рода через математическое ожидание – E(h) и стандартное отклонение – σ(h):

$$P_2(h=0) \approx$$

$$\approx \frac{1}{\sigma(h)\sqrt{2\pi}} \int_0^1 \exp\left\{\frac{-\left(E(h)-u\right)^2}{2\left(\sigma(h)\right)^2}\right\} \cdot du \approx \beta_C^2. \quad (6)$$

Очевидно, что по аналогии с (6) возможно вычислить вероятности появления 256 кодов «Чужой», отличающихся одним битом от кода «Свой»:

$$P\,(h=1) \approx \frac{1}{256 \cdot \sigma(h)\sqrt{2\pi}}$$

$$\int_1^2 \exp\left\{\frac{-\left(E(h)-u\right)^2}{2\left(\sigma(h)\right)^2}\right\} \cdot du \approx \beta_{C(h=1)}^2. \quad (7)$$

В пространстве расстояний Хэмминга наблюдается значительное упрощение вычислений. То, что технически невозможно сделать в обычном кодовом пространстве, легко вычисляется в логарифмически свернутом пространстве.

Известно, что один нейрон описывается статической нелинейной сверткой входных биометрических параметров:

$$\begin{cases} y = b + \sum_{i=1}^{k} a_i \cdot \xi_i, \\ z(y) = \text{"0"} \quad \text{при } y \le 0, \\ z(y) = \text{"1"} \quad \text{при } y > 0, \end{cases} \quad (8)$$

где k – число входов у нейрона; z(y) – квантователь с настройкой порога срабатывания b; ξ_i – один из обрабатываемых (свертываемых) биометрических параметров; a_i – весовой коэффициент нейрона, полученный в результате его обучения.

Формально уравнения (8) можно рассматривать как имитационную динамическую модель одного кубита, если входные биометрические параметры ξ_i постоянно изменяются и непрерывно подаются на входы нейрона.

Один кубит мало интересен для биометрии: ГОСТ Р 52633.5[6] ориентирован на обучение нейронной сети, обеспечивающей 256 кубит. Все эти биометрические кубиты оказываются сильно коррелированными (хорошо сце-

пленными)[3]. Именно это обстоятельство делает их эффективными при решении задач биометрической аутентификации. Переход от одного кубита к большому числу в 256 кубит принципиален.

Как показано на рис. 1, нейросеть преобразователя биометрия-код вместо одного нейрона будет иметь 256 нейронов, выход каждого из которых квантуется своим пороговым элементом. Нейросеть в целом может быть описана в матричной форме системой связанных между собой нелинейных сверток:

$$Z\{\overline{y}\} = Z\left\{\begin{bmatrix} a_{1,1} & a_{1,2} & a_{1,3} & :: & :: & :: & a_{1,416} \\ a_{2,1} & a_{2,2} & a_{2,3} & :: & :: & :: & a_{2,416} \\ :::: & :::: & :::: & :: & :: & :: & :::: \\ a_{256,1} & a_{256,2} & a_{256,3} & :: & :: & :: & a_{256,416} \end{bmatrix} \cdot \begin{bmatrix} \xi_1 \\ \xi_2 \\ \xi_3 \\ :::: \\ :::: \\ \xi_{415} \\ \xi_{416} \end{bmatrix} + \begin{bmatrix} b_1 \\ b_2 \\ ::::: \\ b_{256} \end{bmatrix}\right\} = \begin{bmatrix} "x_1" \\ "x_2" \\ ::::: \\ "x_{256}" \end{bmatrix}. \quad (9)$$

Поскольку нейросетевые преобразователи биометрия-код намного эффективнее «нечетких экстракторов» [6–9], ожидается их массовое использование в ближайшем будущем. Для полноты технологии нужно уметь не только обучать нейронные сети, но и уметь решать обратную задачу по извлечению знаний из параметров обученной нейронной сети.

Результаты исследования

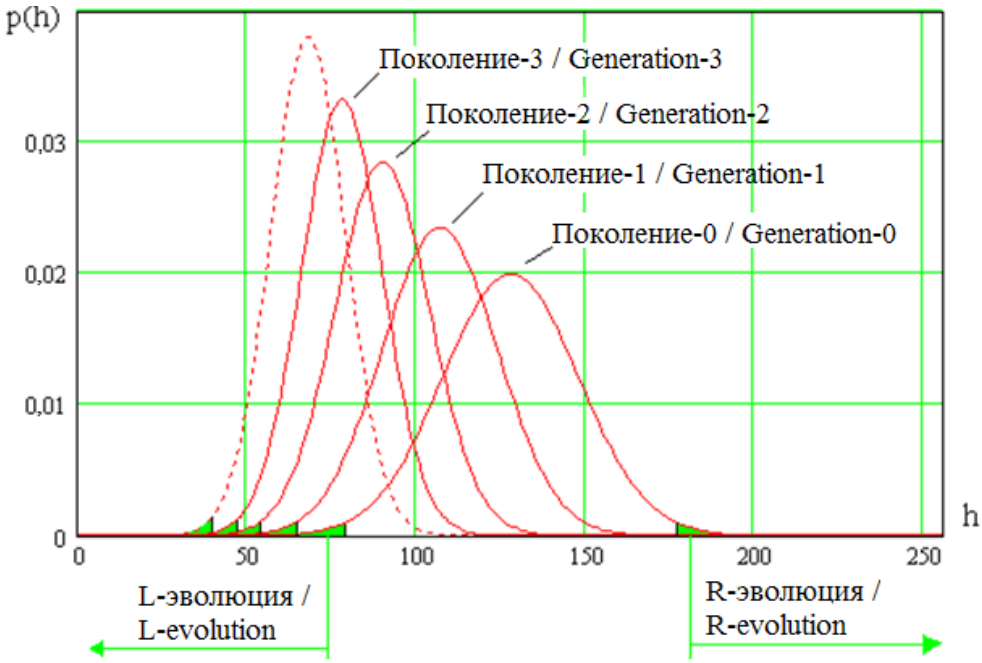
Одним из важных теоретических аспектов нейросетевой биометрии является наличие технической возможности обращения матриц нейросетевых функционалов очень большой размерности в ситуации, когда известен код «Свой». Если пользоваться линейной алгеброй и пытаться обращать корреляционные матрицы биометрических параметров, то для выборки из 21 примера задача оказывается плохо обусловленной. Для биометрии линейная алгебра позволяет обращать матрицы не выше 3–5-го порядка, в то время как реальные биометрические системы учитывают сотни и тысячи биометрических параметров.

При отказе от классических методов и использовании больших нейронных сетей, обученные по ГОСТ Р 52633.5[6] удается решить обратную задачу нейросетевой биометрии размерности 416 входов на 256 выходов.

Обращение матриц выполняется в пространстве расстояний Хэмминга с привлечением базы, состоящей из ~ 1 250 образов «Чужой», каждый из которых представлен 20 примерами. В данном случае база образов «Чужой» рассматривается как нулевое поколение. Подав эти образы на вход нейронной сети, получим распределение расстояний Хэмминга, отображенное в центральной части рис. 4.

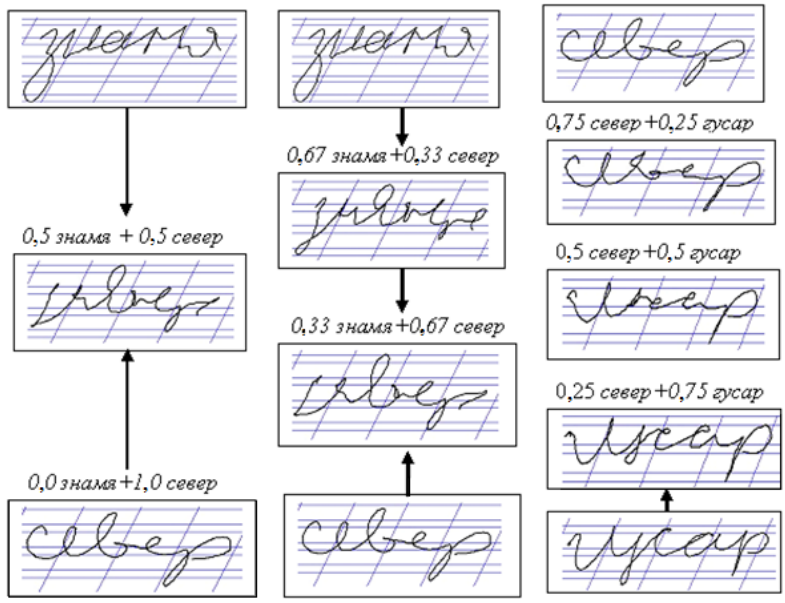
Очевидно, что образы «Чужой», наиболее похожие на образ «Свой», будут расположены в левой части распределения расстояний Хэмминга. Выберем 25 наиболее похожих образов «Чужой», что составит 2 % от исходной тестовой базы, исключив 98 % менее похожих образов.

Для того чтобы продолжить алгоритм, следует восстановить исходное количество биометрических образов. Для этой цели необходимо воспользоваться скрещиванием биометрических образов-родителей и получить от них образы-потомки путем морфинга. Примеры получения 1, 2, 3 образов-потомков от пар образов-родителей приведены на рис. 5.



Р и с. 4. Дрейф распределений расстояний Хэмминга в сторону образа «Свой» при использования генетического алгоритма подбора биометрических параметров в пяти поколениях

F i g. 4. The Hamming distance distributions drift toward the image of "Own" when using a genetic algorithm selection biometrics five generations



Р и с. 5. Скрещивание образов-родителей для получения 1, 2, 3 образов-потомков

F i g. 5. Crossing the parent images to obtain 1, 2, 3 descendant images

После того, как численность биометрических образов в поколении-1 восстановлена, можно снова найти 2 % наиболее похожих образов «Чужой» поколения-1. Как следует из рис. 4, эти образы будут иметь меньшее расстояние Хэмминга, чем образы предыдущего поколения.

Практика показывает, что после 50–60 поколений рассмотренный выше генетический алгоритм позволяет извлекать из параметров обученной нейронной сети до 97 % биометрических параметров образа «Свой». Обычно эта процедура занимает порядка 10 мин машинного времени для обычного настольного компьютера. Итогом решения задачи является получение распределения параметров образа, очень близкого к образу «Свой».

Обсуждение и заключения

Корректное решение даже 16-мерной обратной задачи биометрии в рамках линейной алгебры не представляется возможным. Переход к использованию 416-мерных искусственных нейронных сетей позволяет решать обратную задачу биометрии в случае рассмотрения статистики расстояний Хэмминга 256 выходных кубит. При этом поддержка 256-кубитной квантовой суперпозиции (4) выполняется за счет подключения шума «мутаций» к биометрическим данным и направленного синтеза по ГОСТ Р 52633.2 образов-потомков из образов-родителей. Тестируемая нейронная сеть должна находиться в динамическом режиме для того, чтобы состояния разрядов выходного кода менялись.

Очевидны преимущества использования 256-кубитной квантовой суперпозиции. В каждом поколении в 50 раз снижается размер просматриваемого поля состояний, т. е. отличие в сокращении просматриваемого поля состояний составляет 50^{50} раз. Это эквивалентно огромному росту вычислительных возможностей компьютера, на котором осуществляется численный эксперимент.

Следует подчеркнуть, что описанный выше результат достижим только в рамках нейродинамики нейросетевых молекул. Применение квантовой механики обычных молекул повлекло бы использование жидкого гелия или моделирование уравнения Шредингера при 416 степенях свободы. Отметим, что современные вычислительные машины не способны решать 416-мерные задачи экспоненциальной вычислительной сложности.

ГОСТ Р 52633.3 является первым в мировой практике стандартом, который построен на поддержке эффектов квантовой суперпозиции при тестировании искусственных нейронных сетей в динамическом режиме. Это стало возможным только потому, что моделирование многомерных уравнений, соответствующих уравнению (9) нейросетевой молекулы, имеет линейную вычислительную сложность. Операции, технически невозможные для реальных молекул и уравнений Шредингера, легко реализуются для простых виртуальных математических молекул[3] [2–5].

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Дискретный характер закона распределения хи-квадрат критерия для малых тестовых выборок / Б. Б. Ахметов [и др.] // Вестник Национальной академии наук Республики Казахстан. 2015. № 1. С. 17–25. URL: http://nblib.library.kz/elib/library.kz/jurnal/%D0%92%D0%B5%D1%81%D1%2%D0%BD%D0%B8%D0%BA%2001_2015/Akhmetova0115.pdf

2. Циклические континуально-квантовые вычисления: усиление мощности хи-квадрат критерия на малых выборках / В. П. Кулагин [и др.] // Аналитика. 2016. Т. 30, № 5. С. 22–29. URL: http://www.j-analytics.ru/journal/article/5679

3. Перспективы создания циклической континуально-квантовой хи-квадрат машины для проверки статистических гипотез на малых выборках биометрических данных и данных иной природы / В. И. Волчихин [и др.] // Известия высших учебных заведений. Поволжский регион. Технические науки. 2017. № 1. С. 3–7. URL: http://izvuz_tn.pnzgu.ru/files/izvuz_tn.pnzgu.ru/1117.pdf

4. Квантовая суперпозиция дискретного спектра состояний математической молекулы корреляции для малых выборок биометрических данных / В. И. Волчихин [и др.] // Вестник Мордовского университета. 2017. Т. 27, № 2. С. 230–243. URL: http://vestnik.mrsu.ru/content/pdf/17-2/07.pdf

5. Использование эффектов квантовой суперпозиции при регуляризации вычислений стандартного отклонения на малых выборках биометрических данных / В. И. Волчихин [и др.] // Измерение. Мониторинг. Управление. Контроль. 2017. № 1. С. 57–63. URL: http://imuk.pnzgu.ru/files/imuk.pnzgu.ru/08117.pdf

6. **Juels A., Wattenberg M.** A fuzzy commitment scheme // Proc. ACM Conf. Computer and Communications Security. 2013. Sep. P. 28–36 URL: http://www.arijuels.com/wp-content/uploads/2013/09/JW99.pdf

7. **Dodis Y., Reyzin L., Smith A.** Fuzzy extractors: how to generate strong keys from biometrics and other noisy // Eurocrypt. 2004. P. 523–540. URL: https://eprint.iacr.org/2003/235.pdf

8. **Hao F., Anderson R., Daugman J.** Crypto with biometrics effectively // IEEE Transactions on Computers. 2006. Vol. 55, no. 9. DOI: 10.1.1.727.4334

9. **Ушмаев О. В., Кузнецов В. В.** Алгоритмы защищенной верификации на основе бинарного представления топологии отпечатка пальцев // Информатика и ее применения. 2012. № 6 (1). С. 132–140. URL: http://www.ipiran.ru/journal/issues/2012_06_01

10. **Чморра А. Л.** Маскировка ключа с помощью биометрии // Проблемы передачи информации. 2011. № 2 (47). С. 128–143. http://www.mathnet.ru/links/82a00f759a28c473971e712adecd76c4/ppi2049.pdf

Поступила 06.09.2017; принята к публикации 16.10.2017; опубликована онлайн 19.12.2017

Об авторах:

Волчихин Владимир Иванович, президент ФГБОУ ВО «Пензенский государственный университет» (440000, Россия, г. Пенза, ул. Красная, д. 40), доктор технических наук, профессор, **ORCID: http://orcid.org/0000-0002-9986-531X**, vvi@pnzgu.ru

Иванов Александр Иванович, начальник лаборатории биометрических и нейросетевых технологий, АО «Пензенский научно-исследовательский электротехнический институт» (440026, Россия, г. Пенза, ул. Советская, д. 9), доктор технических наук, доцент, **ORCID: http://orcid.org/0000-0002-3854-2660**, ivan@pniei.penza.ru

Вклад соавторов:

В. И. Волчихин: научное руководство модернизацией квантово-механической вычислительной парадигмы; А. И. Иванов: нейросетевые преобразования биометрия-код, тестирования больших искусственных нейронных сетей.

Все авторы прочитали и одобрили окончательный вариант рукописи.

REFERENCES

1. Akhmetov B. B., et al. [The discrete nature of the chi-square distribution of the criterion for small test samples]. *Vestnik Natsionalnoy akademii nauk Respubliki Kazakhstan* = Bulletin of the National Academy of Sciences of the Republic of Kazakhstan. 2015; 1:17–25. Available at: http://nblib.library.kz/elib/library.kz/jurnal/%D0%92%D0%B5%D1%81%D1%2%D0%BD%D0%B8%D0%BA%2001_2015/Akhmetova0115.pdf (In Russ.)

2. Kulagin V., Ivanov A., Gazin A., Akhmetov B. [Cyclic continuum-quantum computing: strengthening the chi-square power of a criterion on small samples]. *Analitika* = Analitics. 2016; 30(5):22–29. Available at: http://www.j-analytics.ru/journal/article/5679 (In Russ.)

3. Volchikhin V. I., Ivanov A. I., Pashchenko D. V., Akhmetov B. B., Vyatchanin S. Ye. The prospect of creation of a cyclic continual-quantum chi-squared machine for checking statistical hypetheses on small test samples of bioetric and other types of data. *Izvestiya vysshikh uchebnykh zavedeniy. Povolzhskiy region. Tekhnicheskiye nauki* = Proceedings of Higher Educational Institutions. Volga region. Engineering. 2017; 1:3–7. Available at: http://izvuz_tn.pnzgu.ru/files/izvuz_tn.pnzgu.ru/1117.pdf (In Russ.)

4. Volchikhin V. I., Ivanov A. I., Serikov A. V., Serikova Yu. I. Quantum superposition of the discrete spectrum of states of a mathematical correlation molecule status for small samples of biometric data. *Vestnik Mordovskogo universiteta* = Mordovia University Bulletin. 2017; 27(2):230–243. Available at: http://vestnik.mrsu.ru/content/pdf/17-2/07.pdf (In Russ.)

5. Volchikhin V. I., Ivanov A. I., Serikov A. V., Serikov Y. I. Using the effects of quantum superposition of the regularization of the standard deviation calculation on small samples of biometric data. *Izmereniye. Monitoring. Upravleniye. Kontrol* = Measurement. Monitoring. Menagement. Control. 2017; 1:57–63. Available at: http://imuk.pnzgu.ru/files/imuk.pnzgu.ru/08117.pdf (In Russ.)

6. Juels A., Wattenberg M. A fuzzy commitment scheme. Proc. ACM Conf. Computer and Communications Security. 2013; 9:28–36. Available at: http://www.arijuels.com/wp-content/uploads/2013/09/JW99.pdf

7. Dodis Y., Reyzin L., Smith A. Fuzzy extractors: how to generate strong keys from biometrics and other noisy. Eurocrypt. 2004; 523–540. Available at: https://eprint.iacr.org/2003/235.pdf

8. Hao F., Anderson R., Daugman J. Crypto with biometrics effectively. IEEE Transactions on Computers. 2006; 55(9). DOI: 10.1.1.727.4334

9. Ushmayev O. V., Kuznetsov V. V. Protected verification algorithms based on binary representation of fingerprint topology. *Informatika i ee primeneniya* = Informatics and its applications. 2012; 6(1):132–140. Available at: http://www.ipiran.ru/journal/issues/2012_06_01 (In Russ.)

10. Chmorra A. L. Masking a key using biometrics. *Problemy peredachi informatsii* = Problems of Information Transfer. 2011; 2(47):128–143. Available at: http://www.mathnet.ru/links/82a00f759a28c473971e712adecd76c4/ppi2049.pdf (In Russ.)

Submitted 06.09.2017; revised 16.10.2017; published online 19.12.2017

About the authors:

Vladimir I. Volchikhin, President of Penza State University (40 Krasnaya St., Penza 444000, Russia), Dr.Sci. (Engineering), Professor, **ORCID: http://orcid.org/0000-0002-9986-531X**, vvi@pnzgu.ru

Alexander I. Ivanov, Head of Biometric and Neuronal Nets Technology Laboratory, Penza Scientific Research Electrotechnical Institute (9 Sovetskaya St., Penza 440026, Russia) Dr.Sci. (Engineering), Associate Professor, **ORCID: http://orcid.org/0000-0002-3854-2660**, ivan@pniei.penza.ru

Contribution of the co-authors:

V. I. Volchikhin: scientific management of modernization of the quantum mechanical computational paradigm; A. I. Ivanov: neural network biometry-code conversion, testing of large artificial neural networks.

All authors have read and approved the final version of the manuscript.