ENGINEERING MATHEMATICS

MSC 62B01 **DOI: 10.14529/jcem170201**

SIMPLIFICATION OF STATISTICAL DESCRIPTION OF QUANTUM ENTANGLEMENT OF MULTIDIMENSIONAL BIOMETRIC DATA USING SYMMETRIZATION OF PAIRED CORRELATION MATRICES

A. I. Ivanov, Penza Scientific Research Electrotechnical Institute, Penza, Russian Federation, ivan@pniei.penza.ru**,**
A. V. Bezyayev, Penza branch FSUP HTS Atlas, Penza, Russian Federation, bezyayev_Alex@mail.ru**,**
A. I. Gazin, Lipetsk State Pedagogical P. Semenov-Tyan-Shansky University, Lipetsk, Russian Federation, yearn@bk.ru**.**

The aim of the paper is to simplify the description of quantum entanglement of multidimensional biometric data and data of another nature. We use a correlation symmetrization procedure based on conservation of quantum superposition entropy codes, supported on the outputs of neural networks converter of biometric data. We give a nomogram of parameter connection having the same correlation with the output entropy for codes with the length 2, 4, 8, 256 bits and the formula to convert the coordinate system, simplifying connection of entropy and quantum entanglement value of multidimensional data. We claim that synthesis of correct analytical models having high dimensions connecting quantum entanglement and quantum superposition is possible only for symmetrical mathematical constructions. Obtaining asymmetrical correct data is possible only by processing real biometric images of another nature.

Keywords: quantum superposition, quantum entanglement, neural network converter of biometric code, symmetrization of multidimensional correlative matrix, entropy.

1. Technology of Biometric Person Authentication Based on the Use of Large Artificial Neural Networks

Nowadays informatization of modern society is actively. People have to remember many passwords to their personal accounts. Meanwhile used passwords are short, because people are unable to remember long random digital sequences. The converters of biometrics into code allow to solve the problem of remembering long passwords. USA, Canada and the countries of the European Union use the so-called "fuzzy extractors" [1, 2, 3]. Russia [4] and Kasahstan [5] use neural network converters of type "biometric – access code".

Note that information security of citizens is very sensitive field of service. Therefore, a set of standards providing the possibility to certify corresponding hardware and software products, is created in Russia. In particular, the Standard SARS R 52633.5 [6], regulating the training of large artificial neural networks, is created.

If we use the standard SARS R 52633.5 [6], then we obtain large network of artificial neurons with a large number of inputs and outputs. An example of such network is given in Figure 1, where one of neurons from the network with 32 inputs and two tables is shown. The table of connections between the inputs of k-th neuron and inputs of neuron networks as a whole is shown in the left part of the figure. According to the standard, this table contains random addresses, obtained from software generator of pseudo-random numbers. The second table contains weight coefficients of neuron, obtained as a result of its training on several examples of the image "Friend"

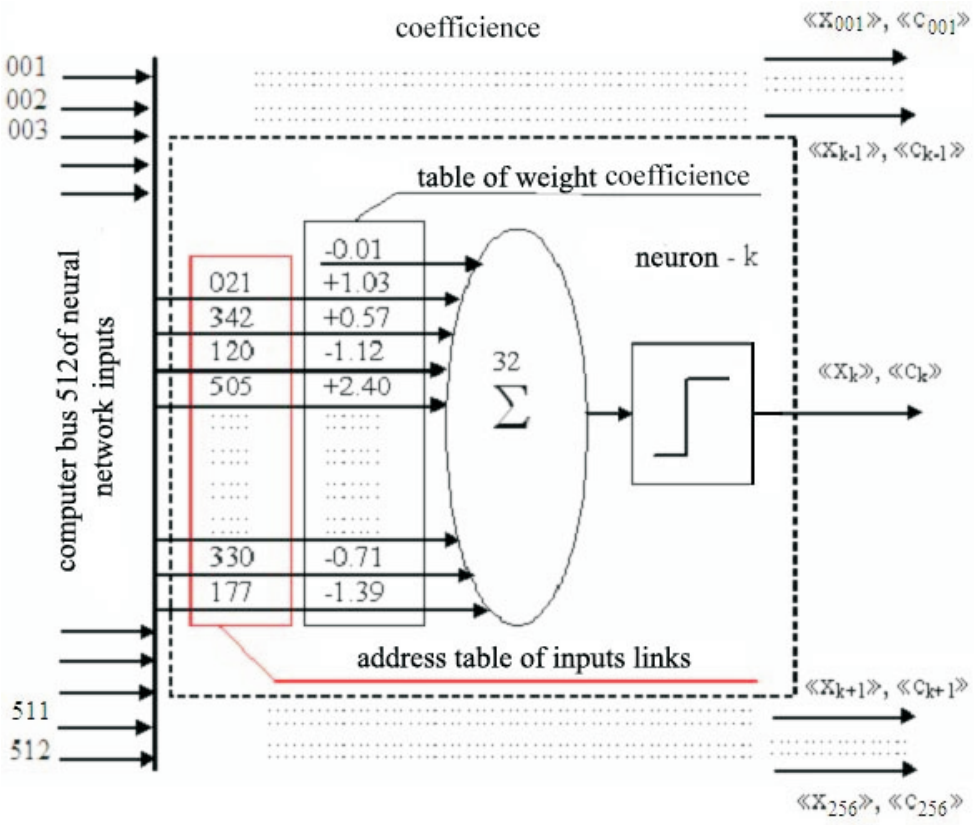

Fig. 1. Standard scheme of structure of neural networks converter having type "biometric –code"

Note that neural networks converter having type "biometric –code" behaves quite differently for the image "Friend" and the images "Foes". If the inputs are the data of the image "Friend" examples, then neural network converter reduces all instabilities of the image to the point of unique cryptographic key "$\bar{A}$". The entropy of the original continuous data of the biometric vector parameters is reduced to almost zero of entropy of the output code "Friend"

$$(\bar{\nu}) >> H(\text{"}\bar{A}\text{"}) \approx 0^1. \tag{1}$$

If vector $\bar{\xi}$ of biometric parameters of the image "Foe" examples is an input of the neural network converter having type "biometric–code", then their neural entropy

[1]The equation (1) contains both a vector of continuums and a vector of binary digits code. In order to distinguish these vectors, the vector of discrete states is marked with quotes, that is common notation for high level programming language.

increases:

$$(\bar{\nu}) \approx H(\bar{\xi}) < H(\text{"}\bar{x}\text{"}) >> 0. \tag{2}$$

For the data of the image "Foe", the neural network converter having type "biometric–code" performs a hash (blending, mixing) function of the data.

During training a neural network by the standard algorithm according to SARS R 52633.5 [6] such that all images have type "Foe the states having i-th bit of the output code "x_i" are equiprobable:

$$P_i(\text{"0"}) \approx P_i(\text{"1"}) \approx 0.5. \tag{3}$$

In addition, the bits of output codes for a single biometric image having type "Foe" and for different biometric images having type "Foe" are significantly correlated (dependent, entangled):

$$|r(\text{"}x_i\text{"},\text{"}x_j\text{"})| \neq 0.0. \tag{4}$$

Theoretically, for each state of 256-bite output code, the probability of its appearance is possible to find. As a result, a very long quantum superposition of spectrum of neural network output states can be built [7]:

$$|\Psi\rangle = \sum_{i=0}^{N} \sqrt{P_i} \cdot \left|000\underset{i}{...}01\right\rangle = \sum_{i=0}^{N} \sqrt{P_i} \cdot \left|\text{"}\underset{i}{\bar{x}}\text{"}\right\rangle \tag{5}$$

The length of quantum superposition is huge (N=2^{256}), however, practically all of its components are low-probability, i.e. $\sqrt{P_i} \approx 0.000001$ and less, with the exception of components close to the code "Friend" ("$\bar{A}$") and its inversion ("$\neg\bar{A}$").

Quantum superposition (5) is of interest mainly for theoretical purposes rather than for practice. This method of problem formalization is less suitable for practice, however it is important for theory, because the method allows to bridge the gap between neural network operations over images and quantum computers.

2. Problem of Statistical Description of High Dimensional Entanglement of Biometric Data

It should be emphasized that the simplest case is the situation when the output code bits are independent $|r(\text{"}x_i\text{"},\text{"}x_j\text{"})| = 0.0.$, and their states are equiprobable (3). In this case, the coefficients of all quantum superposition members (5) are the same:

$$\sqrt{P_i} = \left(\frac{1}{2}\right)^{\frac{n}{2}}, \tag{6}$$

where n is a number of qubit, corresponding to the quantum superposition, or a number of output neurons of biometric-code converter, performed according to scheme of Figure 1.

If we try to build the quantum superposition for real data having a real correlation matrix $[R]$, then the coefficients of quantum superposition ordered by the values of codes within the Dirak brackets $|0011....01\rangle$ have unpredictable (random) nature.

In order to avoid the chaos of random values of quantum superposition weight coefficients, we order the coefficients according to the power. In this case, we always obtain monotonously decreasing functions. Figure 2 shows examples of such functions.

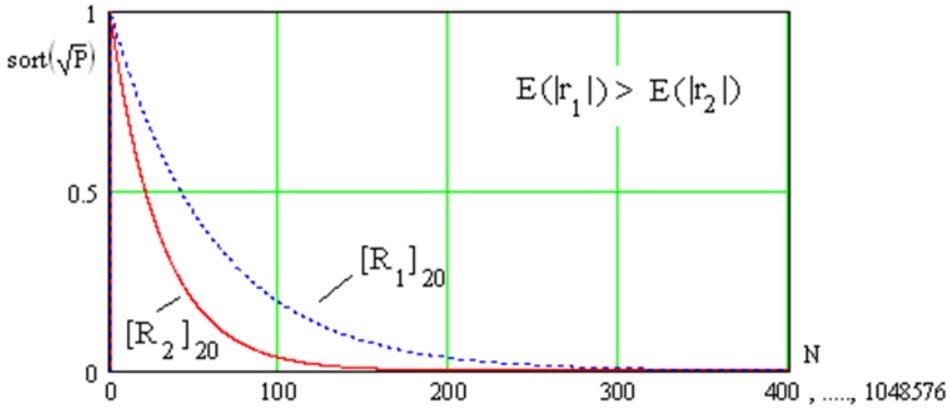

Fig. 2. Values of weight coefficients of quantum superposition for two different correlation matrices, based on real biometric data. The values are ordered according to their power

Figure 2 shows that for different biometric data we obtain different curves which demonstrate decreasing power of quantum superposition weight coefficients. For the first correlation matrix $[R_1]_{20}$ with 20×20 elements, more than 300 significant elements of quantum superposition should be taken into account. For data of the second correlation matrix $[R_2]_{20}$, quantum superposition with the same reliability should have approximately twice as less components.

The number of quantum superposition components taken into account depends on how large are correlation matrix modules lying out of the matrix diagonal. Formally, mathematical expectations of the correlation coefficients modules can be compared with each over even without taking into account coefficients 1 on diagonals of the correlation matrices. For correlation matrices with a large average of modules of its elements $(|r_1|) > (|r_2|)$, we should take into account more number of significant components of the quantum superposition.

On the whole, the proposed approach to calculate all elements of quantum superposition and to order the elements by their power is not constructive. For correlation matrix $[R]_{20}$ with 20×20 elements we should calculate 1 048 576 components of quantum superposition, which takes around 40 minutes of computer time when using the usual today computer. Calculation of the quantum superposition with the length of 256 qubit for real biometric data is technically impossible for the reasonable time interval.

However, for us, fundamentally important is the following. Based on the metric for average value of correlation coefficients modules, we can forecast the desired number of the quantum superposition components that gives statistical description of the research object with some reliability.

3. Symmetrization of Problem about Multidimensional Statistical Description of Neural Network Converter Having Type "Biometric-code".

It is known that symmetrization of multidimensional problems about identification of nonlinear dynamic objects is a very effective method to reduce computational

complexity [9, 10]. This statement has a rigorous proof with regard to identification procedures, based on the description of the object using the Volterra series [11, 12, 13].

Let us apply the method of calculation symmetrization to correlation matrices of real biometric data. In general, for a given matrix of correlation coefficients having general type, to reproduce the data by simulation modeling is rather difficult [14]. Therefore, the correlation matrix of real data should be replaced by a symmetric correlation matrix which is equivalent to it [9, 15].

Let us use m-generators of pseudorandom data and obtain the vector of independent states $\bar{\xi}$ by the generators. Then, these data can be entangle by multiplying this vector by the symmetric matrix:

$$\begin{bmatrix} 1 & 0 & \cdots\cdots\cdots & 0 \\ 0 & 1 & \cdots\cdots\cdots & 0 \\ \cdots\cdots & \cdots\cdots & \cdots\cdots\cdots & \cdots\cdots \\ 0 & 0 & \cdots\cdots\cdots & 1 \end{bmatrix} \times \begin{bmatrix} \xi_{1,i} \\ \xi_{2,i} \\ \cdots\cdots \\ \xi_{m,i} \end{bmatrix} = \begin{bmatrix} y_{1,i} \\ y_{2,i} \\ \cdots\cdots \\ y_{m,i} \end{bmatrix} \Rightarrow R_m = \begin{bmatrix} 1 & r & \cdots\cdots\cdots & r \\ r & 1 & \cdots\cdots\cdots & r \\ \cdots\cdots & \cdots\cdots & \cdots\cdots\cdots & \cdots\cdots \\ r & r & \cdots\cdots\cdots & 1 \end{bmatrix} \quad (7)$$

If all the entanglement matrix elements, that are outside the matrix diagonal, are the same, then all the elements of the correlation matrix of the output data are also the same. If all the entanglement matrix elements $a = 0.0$, then the correlation matrix elements are also zero, $r = 0.0$. In case when $a = 1$, the value of the coefficients with equal correlation is $r = 0.5$.

Usually, for biometric data, the average value of the correlation coefficients modules is less than 0.5. That is, by changing the entanglement parameter from 0 to 1, we always can obtain the desired value of the average module of correlation coefficient for the real data.

Next, entanglement continuum data with desired correlation connections should be compared with the predetermined quantization threshold. Therefore, we obtain a digitized flow of codes with dependent bits. Block diagram for the generator of flow of random codes with dependent (correlated or entangled) bits is shown in Figure 3.

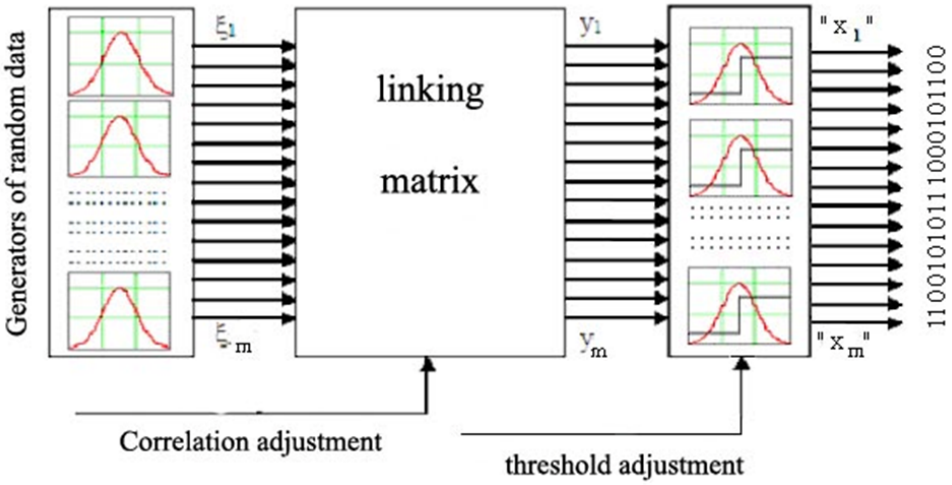

Fig. 3. Block diagram of numerical connection (entanglement) of continuum data, obtained by several pseudo-random software generators

The multidimensional generator constructed according to the block diagram in Figure 3 allows to set the desired ratio of probabilities that states "0"and "1"take place. To this end, the position of the quantization threshold for each output bit is changed. Therefore, we have technical possibility to simulate long random codes with dependent (entangled) bits. As a result, we can create a sufficient amount of codes with predetermined statistical characteristics and compute their entropy.

4. Connection Between the Entropies of Long Dependent Codes and a Coefficient Having Correlation Equal to Their Bits

Let the dimension of the entanglement matrices be 2, 4, 8...128, 256. Then, it is obvious that we obtain codes of different lengths with dependent bits. After calculating the corresponding entropy, we obtain a nomogram of functions of connection between the entropies and either the parameter of equal correlation $-r$ or the average module of coefficients correlation –E(|r|). Therefore, we obtain rather complicated system of functions [4], the low-order functions are given in Figure 4.

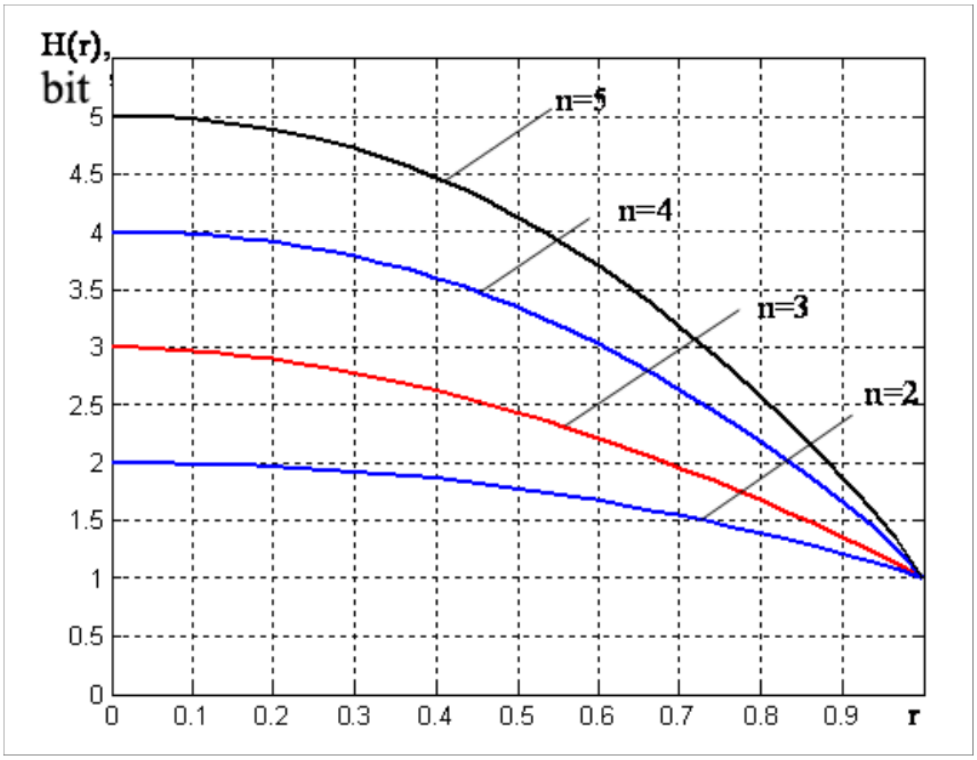

Fig. 4. Connection between the entropies and a coefficient of equal correlation for different values of dimension (a code length is n)

Figure 4 shows that variation range of entropy increases, when the dimension growth increases. This clear and almost linear effect is of no particular interest. Much more interesting are the derivatives of these processes, which are convenient to observe in the system of the following correlation functionals:

$$R(q) = \left(1 - \frac{(" x_1,\ x_2,\ \ldots\ , x_q")}{q}\right) \tag{8}$$

After such transformations, we obtain nomogram of functions given in Figure 5.

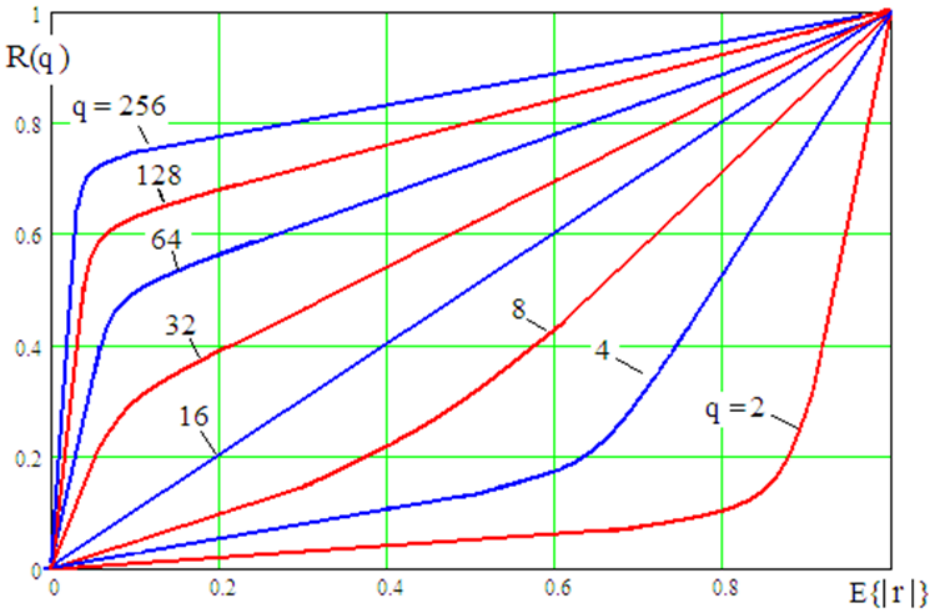

Fig. 5. Nomogram of connection between the generalized coefficient of multidimensional correlation and the coefficients of equal correlation of symmetric correlation matrix

Figure 5 shows that correlation functionals form two groups of straight lines. The lower group is formed by straight lines passing through the point {0,0}. The upper group is formed by straight lines passing through the point {1,1}. One of the lines belongs to both groups and corresponds n=16.

As a result, we obtain rather simple way to describe multidimensional quantum entanglement from 2 to 256 bits of the quantum superposition code for output states of artificial neural network. If we try to describe the bits entanglement (correlation of bits) using asymmetric correlation matrix, then we face an ill-posed problem of enormous computational complexity. Considered symmetrization of the correlation matrix simultaneously reduces the dimension of computing and makes them sustainable.

Nomogram in Figure 5 is constructed for the neural network converters of biometric data into code. The neural networks are trained by the standard algorithm [6] and therefore have equal probability values of states "0" and "1" for all bits (3). In general case, this condition can be changed by setting different thresholds for quantization of data in the scheme of synthesis of equally correlated data (Figure 3). All thresholds can be moved so as the condition of equal asymmetry of bits is hold.

$$P_i(\text{"0"}) = \beta \cdot P_i(\text{"1"}) \tag{9}$$

This leads to deformation of the histogram in Figure 5. However, the new histogram still has a clearly expressed structure, formed by two groups of straight lines, passing through two different points collecting straight lines.

Conclusion

In this paper, we tried to show that the description of quantum entanglement and the corresponding quantum superposition is a technically difficult problem. However, this problem becomes almost one-dimensional and its calculations become technically feasible, if the correlation connections are symmetrized by replacing arbitrary correlation data with equivalent data with symmetric correlation matrix.

This method was already successfully tested on calculations of the predicted probabilities for errors of the first and the second kind for neural network converters of biometric code. However, symmetrization of the data is a tool with much greater opportunities.

In order to program a quantum computer to solve a particular problem, we need to take reliable baseline data (e.g., biometrics data) such that both the quantum superposition and the quantum entanglement, which are typical for the problem, are already included in the data. To this end, we need at least to train the neural network converter having type "biometric–code" and to use the converter to support both quantum superposition and quantum entanglement (7).

The second way for correct connection of the observed quantum superposition and quantum entanglement is a symmetrization of the correlation connections. The symmetrization of correlation connections and similar quantization of data (9) makes problem about multidimensional description correct and low-dimensional (almost one-dimensional).

References

1. Dodis Y., Reyzin L., Smith A. Fuzzy Extractors: How to Generate Strong Keys from Biometrics and Other Noisy Data. *International Conference on the Theory and Applications of Cryptographic Techniques EUROCRYPT 2004: Advances in Cryptology (LNCS 3027)*. 2004, pp. 523–540. doi: 10.1007/978-3-540-24676-3_31
2. Monrose F., Reiter M., Li Q., Wetzel S. Cryptographic Key Generation from Voice. *Proc. IEEE Symp. on Security and Privacy*. 2001, pp. 202–213. doi: 10.1109/SECPRI.2001.924299
3. Ramirez-Ruiz J., Pfeiffer C., Nolazco-Flores J. Cryptographic Keys Generation Using FingerCodes. *Advances in Artificial Intelligence – IBERAMIA-SBIA 2006 (LNCS 4140)*. 2006, pp. 178–187. doi: 10.1007/11874850_22
4. Volochihin V.I., Ivanov A. I., Funtikov V. A., Nazarov I.G., Yazov Y.K. *Neural Network Protection of Personal Biometric Data*. Moscow, Radiotecnika Publ., 2012. (in Russian)
5. Ahmetov B.S., Ivanov A.I., Funtikov V.A., Bezyayev A. V., Malygina E. A. *Technology of Using Large Neural Networks for Converting Fuzzy Biometric Data in Key Code Access*. Almaty, Publisher LEM, 2014. (in Russian)
   Available at: http://portal.kazntu.kz/files/publicate/2015-10-18-11940_7.pdf (accessed on 20 June 2017)
6. SARS0 P 52633.5-2011 "*Information Protection. Technology of Information Protection. Automatic teaching of neural networks to biometrics access code*". (in Russian)

7. Ivanov A.I. *Multifunctional Neural Network Processing of Biometric Data with Software Playback Effects of Quantum Superposition*. Penza, Publisher PNIAI, 2016. (in Russian) Available at: http://пниэи.рф/activity/science/BOOK16.pdf (accessed on 20 June 2017)
8. Nielsen M., Chuang I. *Quantum Computation and Quantum Information*. Cambridge University Press, 2010.
9. Ivanov A.I. *Nejrosetevye tehnologii biometricheskoj autentifikacii pol'zovatelej otkrytyh sistem* [*Neural Networks Technology for Biometric Authentification of Open System Users*]. ScD (Techn) Work. Penza, 2002. (in Russian)
10. Eykhoff P. *System identification: parameter and state estimation*. John Wiley and Sons Ltd., 1974.
11. Ivanov A.I. Two Methods of Hammersteine Orthogonal Model Identification with the Possibility of Convergence Defect Estimation. *Engineering Simulation*, 1999, vol. 16, pp. 553–560.
12. Ivanov A.I. Simple Numerical Method of SeparableVolterra Kernels Symmetrization. *Engineering Simulation*, 1999, vol. 16, pp. 411–416.
13. Ivanov A.I. Synthesis of Nonlinear Dynamic Wiener – Hammerstein Models by Input-Output Memory Redistribution. *Automation and Remote Control*, 1997, no. 11, pp. 21–32. (in Russian)
14. Shalygin A.S., Palagin Yu.I. *Applied Methods of Statistical Modeling*. Leningrad, Mashinostroenie Publ., 1986. (in Russian)
15. Ivanov A.I. *Biometric Identification of a Person by Dynamics of Subconscious Movements*. Penza, University press PSU, 2000. (in Russian)

Alexander I. Ivanov, DSc (Techn), Associate Professor, Laboratory of Biometric and Neural Network Technologies, Penza Scientific Research Electrotechnical Institute (Penza, Russian Federation), ivan@pniei.penza.ru

Alexander V. Bezyayev, PhD (Techn), Leading Specialist of Penza branch FSUP HTS "Atlas" (Penza, Russian Federation), bezyayev_Alex@mail.ru

Alexei I. Gazin, PhD (Techn), Department of Informatics, information technology and information security, Lipetsk State Pedagogical P. Semenov-Tyan-Shansky University (Lipetsk, Russian Federation,), yearn@bk.ru

Received May 7, 2015

УДК 519.2, 612.087, 621.319.7 DOI: 10.14529/jcem170201

УПРОЩЕНИЕ СТАТИСТИЧЕСКОГО ОПИСАНИЯ КВАНТОВОЙ СЦЕПЛЕННОСТИ МНОГОМЕРНЫХ БИОМЕТРИЧЕСКИХ ДАННЫХ ЗА СЧЕТ ИСПОЛЬЗОВАНИЯ СИММЕТРИЗАЦИИ МАТРИЦ ПАРНЫХ КОРРЕЛЯЦИОННЫХ СВЯЗЕЙ

А. И. Иванов, А. В. Безяев, А. И. Газин

Целью работы является упрощение описания квантовой сцепленности многомерных биометрических данных и данных иной природы. Материалы и методы. Используется процедура симметризации корреляционных связей, построенная исходя из условия сохранения энтропии кодов квантовой суперпозиции, поддерживаемой на выходах нейросетевого преобразователя биометрических данных. Результаты. Дана номограмма связи параметра равной коррелированности с выходной энтропией длякодов длинной 2, 4, 8,. . . ., 256 бит. Приведена формула преобразования системы координат, упрощающая связь энтропии и показателя квантовой сцепленности многомерных данных. Выводы. Утверждается, что синтез корректных аналитических моделей высоких размерностей связывающих квантовую сцепленность и квантовую суперпозицию возможен только для симметричных математических конструкций. Получить асимметричные корректные данные можно только обработкой реальных биометрических образов или образов иной природы.

Ключевые слова: квантовая суперпозиция, квантовая сцепленность, нейросетевой преобразователь биометрия-код, симметризация многомерных корреляционных матриц, энтропия.

Литература

1. Dodis, Y. Fuzzy extractors: how to generate strong keys from biometrics and other noisy data / Y. Dodis, L. Reyzin, A. Smith // International Conference on the Theory and Applications of Cryptographic Techniques EUROCRYPT 2004: Advances in Cryptology. – 2004. – P. 523–540.
2. Monrose, F. Cryptographic key generation from voice / F. Monrose, M. Reiter, Q. Li, S. Wetzel // Proc. IEEE Symp. on Security and Privacy. – 2001. – P. 202–213.
3. Ramirez-Ruiz, J. Cryptographic keys generation using FingerCodes / J. Ramirez-Ruiz, C. Pfeiffer, J. Nolazco-Flores // Advances in Artificial Intelligence – IBERAMIA-SBIA 2006 (LNCS 4140). – 2006. – P. 178–187.
4. Волчихин, В.И. Нейросетевая защита персональных биометрических данных / В.И. Волчихин, А.И. Иванов, И.Г. Назаров, В.А. Фунтиков, Ю.К. Язов. – М.: Радиотехника, 2012.
5. Ахметов, Б.С. Технология использования больших нейронных сетей для преобразования нечетких биометрических данных в код ключа доступа / Б.С. Ахметов, А.И. Иванов, В.А. Фунтиков, А.В. Безяев, Е.А. Малыгина. – Алматы: Издательство LEM, 2014. Доступ: http://portal.kazntu.kz/files/publicate/2015-10-18-11940_7.pdf (запрос 20 июня 2017)
6. ГОСТ Р 52633.5-2011 «Защита информации. Техника защиты информации. Автоматическое обучение нейросетевых преобразователей биометрия – код доступа».

7. Иванов, А.И. Многомерная нейросетевая обработка биометрических данных с программным воспроизведением эффектов квантовой суперпозиции / А.И. Иванов. – Пенза: Изд-во ПНИЭИ, 2016. Доступ: http://пниэи.рф/activity/science/BOOK16.pdf (запрос 20 июня 2017)
8. Нильсон, М. Квантовые вычисления и квантовая информация / М. Нильсон, И. Чанг. – М.: Мир, 2006.
9. Иванов, А.И. Нейросетевые технологии биометрической аутентификации пользователей открытых систем: автореферат дис. на соискание ученой степени доктора тех. наук / А.И. Иванов. – Пенза, 2002.
10. Эйкхофф, П. Основы идентификации систем управления / П. Эйкхофф. – М.: Мир. 1975.
11. Ivanov, A.I. Two methods of hammersteine orthogonal model identification with the possibility of convergence defect estimation / A.I. Ivanov // Engineering Simulation. – 1999. – V. 16. – P. 553–560.
12. Ivanov, A.I. Simple numerical method of separabel Volterra Kernels symmetrization / A.I. Ivanov // Engineering Simulation. – 1999. – V. 16. – P. 411–416.
13. Иванов, А.И. Синтез нелинейных динамических моделей Винера-Гаммерштейна перераспределением памяти между входом и выходом / А.И. Иванов // Автоматика и телемеханика. – 1997. – № 11. – С. 21–32.
14. Шалыгин, А.С. Прикладные методы статистического моделирования / А.С. Шалыгин, Ю.И. Палагин. – Л.: Машиностроение, 1986.
15. Иванов, А.И. Биометрическая идентификация личности по динамике подсознательных движений / А.И. Иванов. – Пенза: Изд-во ПГУ, 2000.

Иванов Александр Иванович, доктор технических наук, доцент, лаборатория биометрических и нейросетевых технологий, Пензенский научно-исследовательский электротехнический институт (г. Пенза, Российская Федерация), ivan@pniei.penza.ru

Безяев Александр Викторович, кандидат технических наук, ведущий специалист Пензенского филиала ФГУП НТЦ "Атлас" (г. Пенза, Российская Федерация), Bezyaev_Alex@mail.ru

Газин Алексей Иванович, кандидат технических наук, кафедра Информатики, информационных технологий и защиты информации, Липецкий государственный педагогический университет (г. Липецк, Российская Федерация), yearn@bk.ru

Поступила в редакцию 7 мая 2015 г.