УДК 612.087.1; 519.7; 519.66

*В. И. Волчихин, А. И. Иванов, В. А. Фунтиков, Е. А. Малыгина*

# ПЕРСПЕКТИВЫ ИСПОЛЬЗОВАНИЯ ИСКУССТВЕННЫХ НЕЙРОННЫХ СЕТЕЙ С МНОГОУРОВНЕВЫМИ КВАНТОВАТЕЛЯМИ В ТЕХНОЛОГИИ БИОМЕТРИКО-НЕЙРОСЕТЕВОЙ АУТЕНТИФИКАЦИИ

**Аннотация**. *Актуальность и цели.* В настоящее время вопросы аутентификации личности с использованием биометрических данных становятся актуальными. Преимущество искусственных нейронных сетей большого размера над классическими кодами с обнаружением и исправлением ошибок обусловлено тем, что они в момент обучения способны учитывать реальные распределения многомерных вероятностей биометрических данных, тогда как все классические коды с обнаружением и исправлением ошибок строились в гипотезе равновероятного распределения ошибок. Целью данной работы является изменение парадигмы нейросетевой обработки; предложено от бинарных нейронов (персептронов) перейти к использованию нейронов с многоуровневыми квантователями. *Материалы и методы.* Сравнение проведено с использованием комплексного показателя качества кодов – энтропии (близости их к «белому шуму»). Для кодов длиной порядка 20 бит расчет энтропии может быть проведен по Шеннону. Для более длинных кодов ресурсов современных машин недостаточно. Предложено анализировать только начальный участок кодовых последовательностей возрастающей длины. Далее строится экстраполирующий полином и предсказывается ожидаемое значение энтропии длинных кодов. *Результаты*. Результирующее значение 256-мерной энтропии кодов нейросетевого преобразователя оказалось выше, чем 51-мерная энтропия кодов «нечеткого экстрактора». Выигрыш обусловлен увеличение длины биокода несмотря на то, что длинные коды имеют более высокий уровень корреляции их разрядов. Переход от бинарных нейронов к нейронам с многоуровневыми квантователями увеличивает выигрыш примерно в миллион раз. *Выводы*. При переходе от бинарных нейронов к троичным нейронам длина выходного кода увеличивается в два раза, а их энтропия увеличивается примерно в полтора раза. Выигрыш, связанный с ростом энтропии биокодов, растет с числом уровней квантования в каждом нейроне. При этом проблемы обучения нейронных сетей усиливаются. Необходимо модифицировать стандартный алгоритм обучения ГОСТ Р 52633.5–2011 под сети, состоящие из смеси обычных бинарных нейронов и троичных нейронов.

**Ключевые слова**: искусственные нейронные сети, преобразование биометрии в код, бинарные квантователи, многоуровневые квантователи, нейроны с большим числом квантовых состояний.

*V. I. Volchikhin, A. I. Ivanov, V. A. Funtikov, E. A. Malygina*

# PERSPECTIVES OF USING ARTIFICIAL NEURAL NETWORKS WITH MULTILAYER QUANTIZER IN TECHNOLOGY OF BIO-METRIC-NEURAL-NETWORK AUTHENTICANTION

**Abstract**. *Background.* At the present time the problems of personality authentication using biometric data are becoming topical. The advantage of artificial neural networks of large size over classical codes with error detection and correction lies in

the fact that in the moment of learning the networks are capable of taking into account real distributions of multidimensional probabilities of biometric data, whereas all the classical codes of error detection and correction are based on the hypothesis of probable distribution of errors. The article is aimed at changing the paradigm of neural network processing; the authors suggest to switch from binary neurons (perceptron) to using neurons with multilayer quantizers. *Materials and methods.* The comparison is conducted using a complex code quality index - entropy (proximity to "the white noise"). For codes of about 20 bits in length the entropy may be calculated according to Shannon. For longer codes the resources modern machines are insufficient. It is suggested to analyze only the initial part of the code sequence of the increasing length. After that it is necessary to build an extrapolating polynomial and predict the expected long code's entropy value. *Results.* The resulting value of 256 bit entropy of codes of the neural network converter turned to be higher than 51-vit entropy of codes of "the fuzzy extractor". The gain is conditioned by the length of the bio-code despite the fact that long codes have a higher level of correlation of their positions. The transition from binary neurons to neurons with multilevel quantizers increases the gain to up to million times. *Conclusions.* In the course of transition from binary neurons to ternary neurons the length of the output code increases two times, and their entropy increases appoximately 1,5 times. The gain relating to the increase of biocode entropy increases with the number of quantization levels in each neuron. At the same time the problems of neural network learning also become complicated. It is necessary to modify the standard algorithm of learning ГОСТ Р 52633.5–2011 for networks consisting of the combination of regular binary neurons and ternary neurons.

**Key words**: artificial neural networks, transition of biometry into code, binary quantizers, multilevel quantizers, neurons with high number of quantum conditions.

## Введение

Все преобразователи биометрии в код делятся на «нечеткие экстракторы» [1–12] и нейросетевые преобразователи биометрии в код [13–17]. Основной вклад в развитие технологии «нечетких экстракторов» внесли исследователи США, Канады, стран Евросоюза и Южной Кореи. Нейросетевые преобразователи биометрия–код разрабатываются усилиями исследователей России, Белоруссии и Казахстана. Отличие между этими двумя технологиями только в положении квантователя непрерывных биометрических данных. В «нечетких экстракторах» квантователь преобразует в код «сырые» биометрические данные, а далее эти данные правятся самокорректирующимся кодом.

В нейросетевых преобразователях «сырые» биометрические данные первоначально обогащаются сумматорами искусственных нейронов, а далее уже обогащенные сигналы на выходах сумматоров квантуются выходным нелинейным элементом. Структурные схемы, отражающие положение квантователей в преобразователях биометрия–код, отображены на рис. 1.

В «нечетких экстракторах» может быть использован любой классический код, способный обнаруживать и исправлять ошибки. Обычно используются коды БЧХ (Боуза – Чоухуры – Хоквингема) примерно с 10-кратной избыточностью, способные править до 15 % ошибок. То есть при 512 контролируемых биометрических параметрах длина выходного кода «нечеткого экстрактора» составит 51 бит.

Нейронные сети осуществляют обогащение данных в непрерывной форме, и обычно для корректировки всех входных ошибок оказывается до-

статочно двукратной избыточности, т.е. 512 входных биопараметров нейронная сеть преобразует в 256 бит выходного кода практически без ошибок.

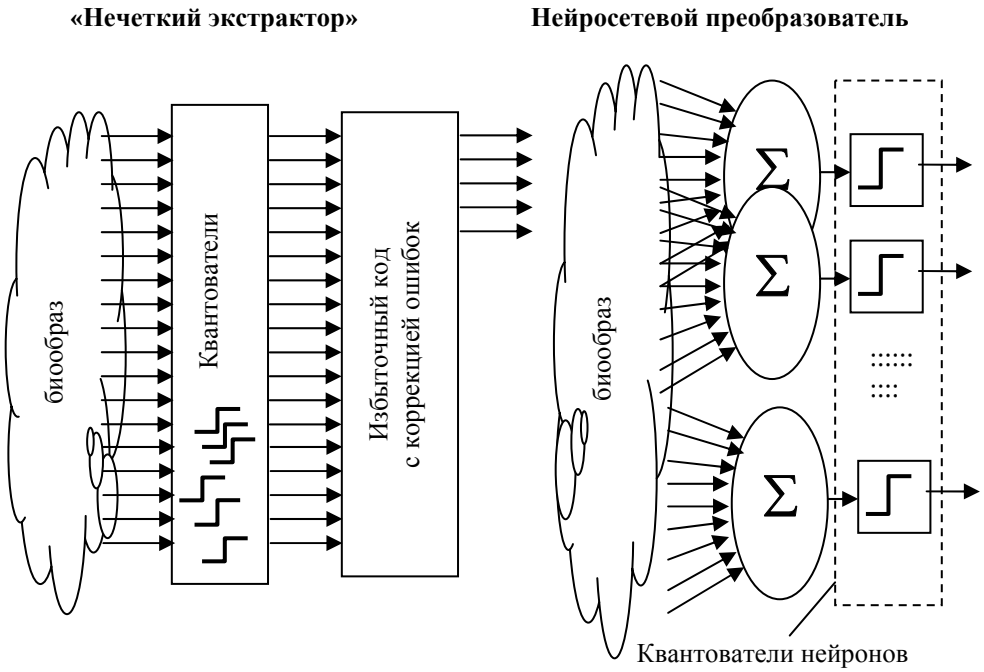



Рис. 1. «Нечеткие экстракторы» и нейросетевые преобразователи отличаются положением нелинейных элементов квантующих непрерывные данные в код с конечным числом состояний

С точки зрения получения биометрических свойств нейросетевые преобразователи биометрия–код всегда лучше «нечетких экстракторов». Это легко продемонстрировать на примере плохих биометрических данных, дающих ошибки в 50 % и более в разрядах биокода. Классические самокорректирующиеся коды не способны править более 50 % ошибок. Нейронные сети с этой проблемой справляются, если избыточность их становится хотя бы трехкратной (входов в три раза больше, чем выходов).

Преимущество искусственных нейронных сетей над классическими кодами с обнаружением и исправлением ошибок обусловлено тем, что они в момент обучения способны учитывать реальные распределения многомерных вероятностей биометрических данных, тогда как все классические коды с обнаружением и исправлением ошибок строились в гипотезе равновероятного распределения ошибок.

Практика показывает, что разряды выходных биокодов «Свой» имеют разную стабильность, т.е. гипотеза равновероятности ошибок в биометрии не работает. Под каждое конкретное распределение ошибок кодов «Свой» нужно синтезировать свой особый код, оптимально корректирующий ошибки, или применять нейросетевой обогатитель «сырых» биометрических данных, обучаемый по одному из известных алгоритмов [15].

## 2. Сравнительная оценка характеристик двух технологий через вычисление энтропии длинных зависимых кодов

Комплексным показателем качества кодов (близости их «белому шуму») является энтропия. Если имеется выборка из множества кодов со случайными состояниями разрядов «$x_i$», то можно последовательно начать вычисление среднего значения энтропии по одному разряду $E(H("x_i"))$, среднего значения энтропии по паре случайно выбранных разрядов $E(H("x_i, x_j"))$. Далее можно продолжить эту процедуру для троек, четверок, пятерок случайно выбранных разрядов. Если приходится иметь дело с «белым шумом», то энтропия будет линейно увеличиваться по мере увеличения числа учитываемых разрядов:

$$\begin{cases} E(H("x_i")) = 1, \\ E(H("x_i, x_j")) = 2, \\ \ldots \\ H("x_1, x_2, \ldots, x_n") = n. \end{cases} \quad (1)$$

Идеальных преобразователей биометрии в код со свойством (1) не существует. Реальное значение $n$-мерной энтропии всегда много меньше, чем энтропия $n$-мерного «белого шума»:

$$H("x_1, x_2, \ldots\ldots, x_n") < n\,. \quad (2)$$

Расчет энтропии по Шеннону технически выполним для кодов длиной порядка 20 бит, далее возможности обычных вычислительных машин в настоящее время не хватает. То есть на анализируемой кодовой последовательности следует оценивать только начальный участок последовательности возрастающих значений энтропии низкого порядка. Далее следует строить полином по полученным данным и предсказывать по нему ожидаемое значение энтропии длинных кодов. На рис. 2 приведены примеры использования полиномов 13 порядка для предсказания значений энтропии 51-битных кодов энтропии и 256-битных кодов.

Из данных рис. 2 видно, что кривая роста энтропии выходных кодов «нечетких экстракторов» находится ближе к идеальной линии роста энтропии кодов типа «белый шум». Коды на выходе «нечеткого экстрактора» менее коррелированны (менее зависимы), чем коды на выходе нейросетевого преобразователя биометрия–код. Тем не менее результирующее значение 256-мерной энтропии кодов нейросетевого преобразователя оказывается выше, чем 51-мерной энтропии кодов «нечеткого экстрактора». Этот факт является численным подтверждением преимуществ нейросетевых обогатителей данных в сравнении с классическими кодами, обнаруживающими и исправляющими ошибки.

## 3. Естественное ограничение числа нейронов сети преобразователя биометрия–код

Следует отметить, что увеличение длины выходного кода нейросетевых преобразователей за счет увеличения числа нейронов может приводить к со-

ответствующему росту энтропии только до некоторого предела. Технически можно сделать число выходов у нейронной сети как угодно большим, однако этот простой прием наращивания длины кода неэффективен. Каждый биометрический образ «Свой» имеет свою уникальную информативность. Если образ «Свой» нестабилен или близок к среднестатистическому, его информативность низка. И наоборот, биометрический образ «Свой» обладает высокой информативностью, если он стабилен и уникален. Существующие ограничения на длину выходного кода (числа нейронов сети) иллюстрируются рис. 3.

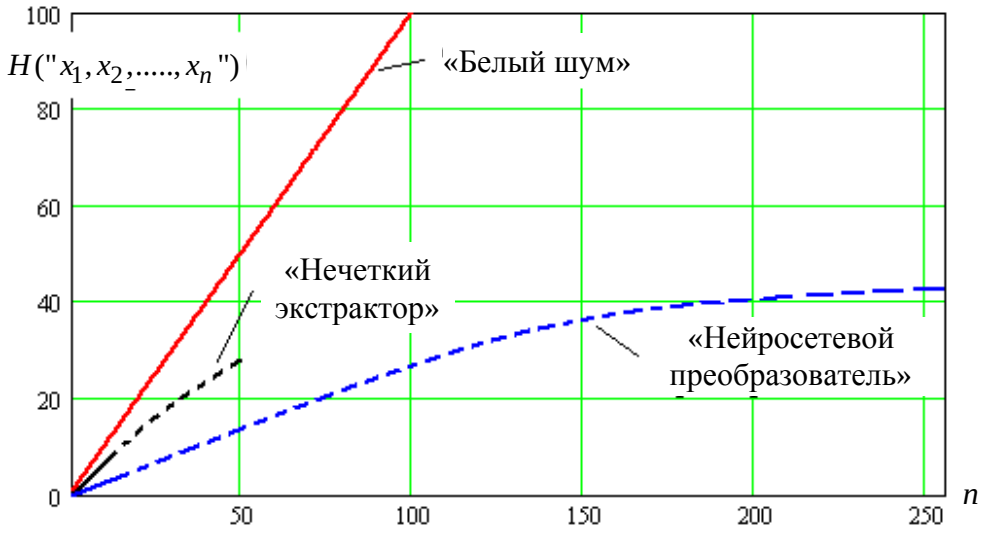



Рис. 2. Прогнозирование значений энтропии длинных кодов

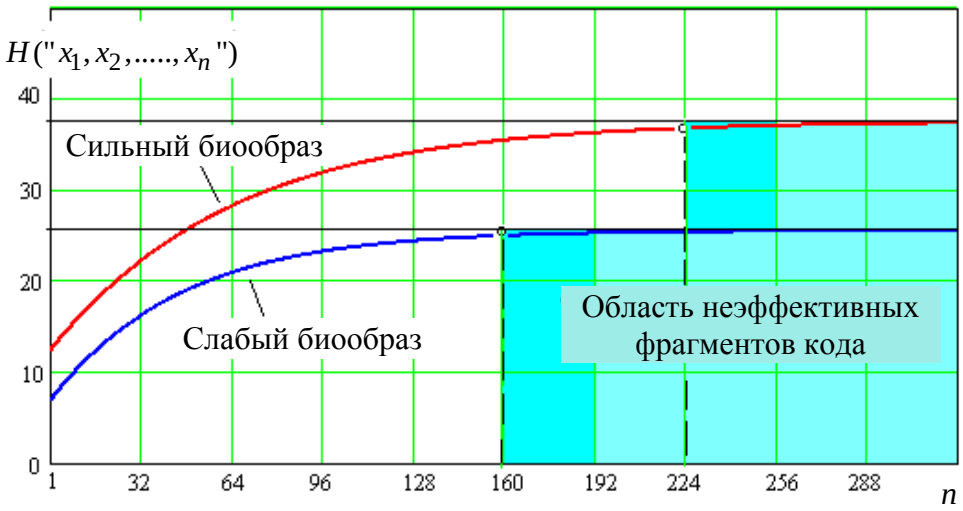



Рис. 3. Рост энтропии выходного биокода нейросети как функция от его длины

Из данных рис. 3 видно, что часть разрядов выходного биокода является лишней, учет этих разрядов не увеличивает энтропию кода. Это происходит из-за существенных корреляционных связей между решениями, принимае-

мыми искусственными нейронами. Из-за этого эффекта слишком сильно увеличивать число нейронов в выходном слое нейронной сети нецелесообразно.

Для слабого биометрического образа (он нестабилен или имеет низкую уникальность) искусственная нейронная сеть могла бы иметь 160 выходов. Для более сильного (более информативного) биометрического образа оптимальным будет код ключа 224 бита. Если нейросетевой преобразователь биометрия–код будет иметь 256 выходов, то часть разрядов и в первом, и во втором случае оказывается избыточной.

### 4. Биометрические параметры с нулевым математическим ожиданием

Маленькие нейронные сети (с малым числом входов и выходов, с малым числом внутренних связей) хорошо учатся, но никому не нужны из-за того, что их решения оказываются много хуже решений, принимаемых людьми. Большие нейронные сети могут принимать решения, сопоставимые с качеством решений, принимаемых людьми – экспертами. Сверхбольшие искусственные нейронные сети способны принимать решения более высокого качества, чем решения людей. Казалось бы, нужно увеличивать размерность искусственного интеллекта, однако при этом большие и сверхбольшие искусственные нейронные сети перестают обучаться. Так, корпорация Google, для того чтобы организовать поиск картинок, вынуждена для их классификации использовать большие нейронные сети, которые должны предварительно обучаться на 20 000 примерах распознаваемого образа. Обучение ведется методом обратного распространения ошибок, модифицированным Дж. Хинтоном в 2007 г. При этом отмечаем, что процесс обучения длится в течение нескольких суток с привлечением большого числа мощных серверов корпорации Google.

Очевидно, что технологии Google неприменимы для биометрии. Большие нейронные сети преобразователей биометрия–код должны учиться на 20 примерах образа «Свой» за время порядка 1 с на обычной вычислительной машине. Затем данные, использованные при обучении, должны быть удалены. Таковы требования информационной безопасности и национального стандарта ГОСТ Р 52633.0–2006 «Защита информации. Техника защиты информации. Требования к средствам высоконадежной биометрической аутентификации».

Для того чтобы удовлетворить столь жестким требованиям в Пензенском государственном университете и Пензенском научно-исследовательском электротехническом институте в 2002 г. [14] были созданы специальные алгоритмы быстрого обучения больших искусственных нейронных сетей, которые позднее легли в основу национального стандарта ГОСТ Р 52633.5–2011 «Защита информации. Техника защиты информации. Автоматическое обучение нейросетевых преобразователей биометрия–код доступа». Именно благодаря наличию нового стандартизованного алгоритма автоматического обучения удается поднять эффективную длину ключа до 43 бит для некоторого биометрического образа, в сравнении с 28 битами, полученными «нечетким экстрактором» для того же биометрического образа (см. рис. 2).

Можно говорить о том, что в основу национального стандарта ГОСТ Р 52633.5–2011 положен наиболее эффективный алгоритм обучения из всех существующих на сегодня алгоритмов обучения сетей искусственных бинарных нейронов (персептронов). Однако нет предела совершенствованию технологии, и это хорошо понимает коллектив исследователей, создавший алго-

ритм ГОСТ Р 52633.5–2011 с рекордными показателями скорости обучения и рекордными показателями устойчивости процесса обучения.

Одним из серьезных недостатков ГОСТ Р 52633.5–2011 является то, что он ориентирован только на обучение сетей из бинарных нейронов (персептронов). К сожалению, бинарные нейроны оказались неспособны эффективно обогащать биометрические данные с нулевым и близким к нулевому математическим ожиданием. Если у *i*-го биометрического параметра $\nu_i$ образа «Свой» и у *i*-х биометрических параметров $\xi_i$ образов «Все Чужие» математические ожидания близки

$$E(\nu_i) \approx E(\xi_i), \qquad (3)$$

то весовые коэффициенты у связей таких данных оказываются нулевые. Более того, проведенные исследования показали, что выполнить жесткие требования информационной безопасности и снять ограничения вида (3) невозможно, если оставаться в парадигме использования бинарных нейронов (персептронов).

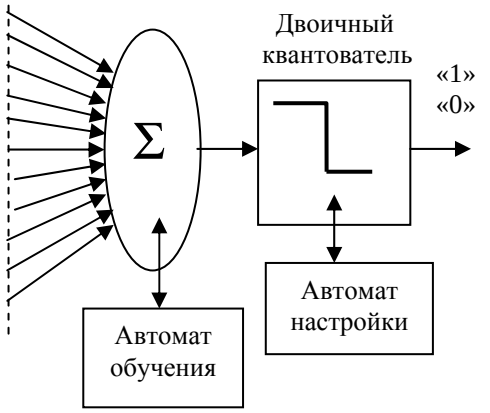
## 5. Новая парадигма использования нейронов с многоуровневыми квантователями

В обычных двоичных нейронах на выходе сумматора подключен бинарный квантователь с одним порогом сравнения. У троичных нейронов на выходе сумматора подключен квантователь с двумя порогами сравнения и тремя выходными состояниями, как это показано на рис. 4.

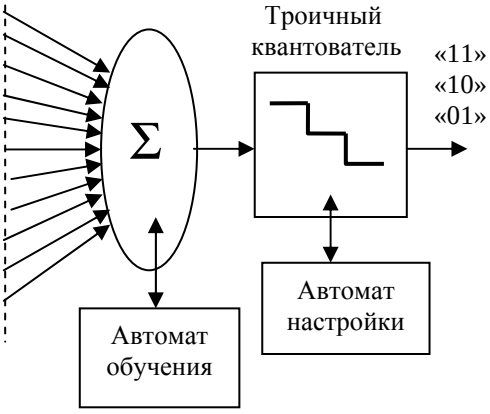
Как правило, выполнение примитивных арифметико-логических операций на современных компьютерах может выполняться в любой системе счисления. Выполнение обычной арифметики в двоичной, троичной, четверичной и т.д. системах счисления не дает какого-либо выигрыша (нет преимуществ). Совершенно не так получается при нейросетевых континуально-квантовых преобразованиях. При переходе к использованию трит-нейронов проблема данных с нулевым математическим ожиданием решается. На рис. 5 приведены варианты выполнения троичных квантователей, позволяющих с выхода каждого из трит-нейронов получать 2 разряда биокода.

При переходе от бинарных нейронов к троичным прогнозируемая длина выходного кода увеличивается в два раза, а длина эффективного кода увеличивается примерно в полтора раза. То есть, переходя от бинарных нейронов, дающих энтропию кодов 43 бита, к троичным нейронам, увеличивается энтропия кодов примерно до 64 бит. Выигрыш составляет 21 бит, или $10^6$ раз по значению вероятности ошибок второго рода. Выигрыш в миллион раз по значению вероятности ошибок дорогого стоит, он возникает не на пустом месте. Оказывается, трит-нейроны могут выполнять то, что в принципе не способны делать обычные нейроны (персептроны). В частности, трит-нейроны оказались способны эффективно выполнять функцию хэширования данных, если использовать немонотонные квантователи (правый нижний и левый верхний углы рис. 5).

Если же использовать монотонные квантователи (правый верхний угол и нижний левый угол), то хэширующие свойства трит-нейронов значительно ослабевают.




***а***)




***б***)

Рис. 4. Двоичный нейрон (***а***) и троичный нейрон (***б***)

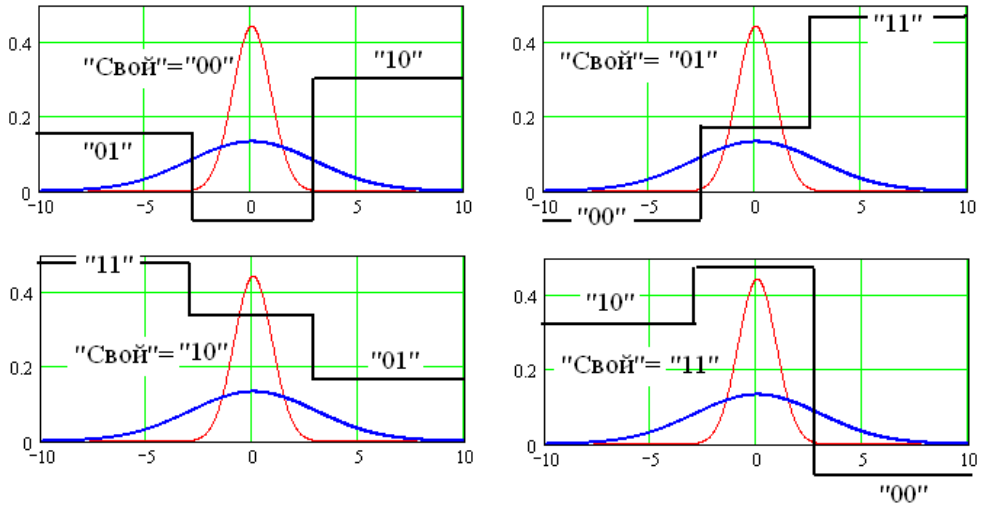



Рис. 5. Примеры использования разных вариантов троичных квантователей

**Заключение**

Следует отметить, что выигрыш, связанный с ростом энтропии биокодов, растет с усложнением квантователей. Чем больше уровней квантования обеспечивает квантователь, тем выше энтропия выходных биокодов и тем сложнее обучать такие нейроны. Поэтому в настоящее время начата работа по модификации алгоритмов обучения ГОСТ Р 52633.5–2011 под сети, состоящие из смеси обычных нейронов и трит-нейронов.

***Список литературы***


1. **Juels, A.** A Fuzzy Commitment Scheme / A. Juels, M. Wattenberg // Proc. ACM Conf. Computer and Communications Security, 1999. – P. 28–36
2. **Monrose, F.** Cryptographic key generation from voice / F. Monrose, M. Reiter, Q. Li, S. Wetzel // In Proc. IEEE Symp. on Security and Privacy, 2001.
3. **Juels, A.** A Fuzzy Vault Scheme / A. Juels, M. Sudan // IEEE International Symposium on Information Theory, 2002.
4. **Dodis, Y.** Fuzzy Extractors: How to Generate Strong Keys from Biometrics and Other Noisy / Y. Dodis, L. Reyzin, A. Smith // In EUROCRYPT, Data April 13, 2004. – P. 523–540.
5. **Yang, S.** Automatic Secure Fingerprint Verification System Based on Fuzzy Vault Scheme / S. Yang, I. Verbauwhede // Proc. IEEE ICASSP, 2005. – P. 609–612.
6. **Cauchie, S.** From features extraction to strong security in mobile environment: A new hybrid system / S. Cauchie, T. Brouard, H. Cardot // On the Move to Meaningful Internet Systems 2006: OTM 2006 Workshops, Springer, 2006. – P. 489–498,
7. **Ramírez-Ruiz, J.** Cryptographic Keys Generation Using FingerCodes / J. Ramírez-Ruiz, C. Pfeiffer, J. Nolazco-Flores // Advances in Artificial Intelligence – IBERAMIA-SBIA, 2006. – P. 178–187.
8. **Arakala, A.** Fuzzy Extractors for Minutiae-Based Fingerprint Authentication / A. Arakala, J. Jeffers, K. J. Horadam // Advances in Biometrics (LNCS 4642), Springer, 2007. – P. 760–769.
9. **Lee, Y. J.** Biometric Key Binding: Fuzzy Vault Based on Iris Images / Y. J. Lee, K. Bae, S. J. Lee, K. R. Park, J. Kim // Proceedings of 2nd International Conference on Biometrics. – Seoul, South Korea, 2007, August. – P. 800–808.
10. **Nandakumar, K.** Fingerprint-Based Fuzzy Vault: Implementation and Performance / K. Nandakumar, A. K. Jain, S. Pankanti // IEEE Transactions on Information Forensics and Security, 2007. – Vol. 2(4). – P. 744–757.
11. **Balakirsky, V. B.** Constructing Passwords from Biometrical Data / V. B. Balakirsky, A. R. Ghazaryan, A. J. Han Vinck // Advances in Biometrics (LNCS 5558), Springer, 2009. – P. 889–898.
12. **Kanade, S.** Multi-Biometrics Based Cryptographic Key Regeneration Scheme / S. Kanade, D. Petrovska-Delacretaz, B. Dorizzi // Proceedings of the 3rd IEEE international conference on Biometrics: Theory, applications and systems, 2009. – P. 333–339.
13. **Иванов, А. И.** Биометрическая идентификация личности по динамике подсознательных движений : моногр. / А. И. Иванов. – Пенза : Изд-во ПензГУ, 2000. – 156 с.
14. **Волчихин, В. И.** Быстрые алгоритмы обучения нейросетевых механизмов биометрико-криптографической защиты информации. : моногр. / В. И. Волчихин, А. И. Иванов, В. А. Фунтиков. – Пенза : Изд-во ПензГУ, 2005. – 273 с.
15. **Язов, Ю. К.** Нейросетевая защита персональных биометрических данных / Ю. К. Язов, В. И. Волчихин, А. И. Иванов, В. А. Фунтиков, И. Г. Назаров ; ред. Ю. К. Язов. – М. : Радиотехника, 2012. – 157 с.

16. **Ахметов, Б. С.** Алгоритмы тестирования биометрико-нейросетевых механизмов защиты информации : моногр. / Б. С. Ахметов, В. И. Волчихин, А. И. Иванов, А. Ю. Малыгин. – Алматы, Республика Казахстан : Изд-во КазНТУ им. Сатпаева, 2013. – 152 с.
17. **Akhmetov, B.** Biometric Technology in Securing the Internet Using Large Neural Network Technology / B. Akhmetov, A. Doszhanova, A. Ivanov, T. Kartbaev and A. Malygin // World Academy of Science, Engineering and Technology. Singapore. – 2013, July. – Issue 79. – P. 129–138.

### *References*

1. Juels A. A, Wattenberg M. *Proc. ACM Conf. Computer and Communications Security*, 1999, pp. 28–36
2. Monrose F., Reiter M., Li Q., Wetzel S. *In Proc. IEEE Symp. on Security and Privacy*, 2001.
3. Juels A. A, Sudan M. *IEEE International Symposi-um on Information Theory*, 2002.
4. Dodis Y., Reyzin L., Smith A. *In EUROCRYPT*, Data April 13, 2004, pp. 523–540.
5. Yang S., Verbauwhede I. *Proc. IEEE ICASSP*, 2005, pp. 609–612.
6. Cauchie S., Brouard T., Cardot H. *On the Move to Meaningful Internet Systems 2006: OTM 2006 Workshops, Springer*, 2006, pp. 489–498,
7. Ramírez-Ruiz J., Pfeiffer C., Nolazco-Flores J. *Advances in Artificial Intelligence – IBERAMIA-SBIA*, 2006, pp. 178–187.
8. Arakala A., Jeffers J., Horadam K. J. *Advances in Biometrics (LNCS 4642), Springer*, 2007, pp. 760–769.
9. Lee Y. J., Bae K., Lee S. J., Park K. R., Kim J. *Proceedings of 2nd International Conference on Biometrics, Seoul, South Korea, August*, 2007, pp. 800–808.
10. Nandakumar K., Jain A. K., Pankanti S. *IEEE Transactions on Information Forensics and Security*, 2007, vol. 2(4), pp. 744–757.
11. Balakirsky V. B., Ghazaryan A. R., A. J. Han Vinck *Advances in Biometrics (LNCS 5558), Springer*, 2009, pp. 889–898.
12. Kanade S., Petrovska-Delacretaz D., Dorizzi B. *Proceedings of the 3rd IEEE interna-tional conference on Biometrics: Theory, applications and systems*, 2009, pp. 333–339.
13. Ivanov A. I. *Biometricheskaya identifikatsiya lichnosti po dinamike podsoznatel'nykh dvizheniy: monogr.* [Biometric identification of personality by dynamics of subconscious movements: monograph]. Penza: Izd-vo PenzGU, 2000, 156 p.
14. Volchikhin V. I., Ivanov A. I., Funtikov V. A. *Bystrye algoritmy obucheniya neyrosetevykh mekhanizmov biometriko-kriptograficheskoy zashchity informatsii: monogr*. [Fast algorithms of learning of neural network mechanisms in biometric-cryptographic data security: monograph]. Penza: Izd-vo PenzGU, 2005, 273 p.
15. Yazov Yu. K., Volchikhin V. I., Ivanov A. I., Funtikov V. A., Nazarov I. G. *Neyrosetevaya zashchita personal'nykh biometricheskikh dannykh* [Neural network security of personal biometric data]. Moscow: Radiotekhnika, 2012, 157 p.
16. Akhmetov B. S., Volchikhin V. I., Ivanov A. I., Malygin A. Yu. *Algoritmy testirovaniya biometriko-neyrosetevykh mekhanizmov zashchity informatsii: monogr*. [Testing algorithms of biometric-neural-network mechanisms of information security: monograph]. Almaty, Respublika Kazakhstan: Izd-vo KazNTU im. Satpaeva, 2013, 152 p.
17. Akhmetov B., Doszhanova A., Ivanov A., Kartbaev T. and Malygin A. *World Academy of Science, Engineering and Technology*. Singapore. 2013, July, issue 79, pp. 129–138.

***Волчихин Владимир Иванович***
доктор технических наук, профессор, президент Пензенского государственного университета (Россия, г. Пенза, ул. Красная, 40)

E-mail: president@pnzgu.ru

***Volchikhin Vladimir Ivanovich***
Doctor of engineering sciences, professor, president of Penza State University (40 Krasnaya street, Penza, Russia)

***Иванов Александр Иванович***
доктор технических наук, доцент, начальник лаборатории биометрических и нейросетевых технологий, Пензенский научно-исследовательский электротехнический институт (Россия, г. Пенза, ул. Советская, 9)

E-mail: ivan_pniei@penza.ru

***Ivanov Aleksandr Ivanovich***
Doctor of engineering sciences, associate professor, head of the laboratory of biometric and neural network technologies, Penza Research Institute of Electrical Engineering (9 Sovetskaya street, Penza, Russia)

***Фунтиков Вячеслав Александрович***
кандидат технических наук, генеральный директор Пензенского научно-исследовательского электротехнического института (Россия, г. Пенза, ул. Советская, 9)

E-mail: pniei@penza.ru

***Funtikov Vyacheslav Aleksandrovich***
Candidate of engineering sciences, general director of Penza Research Institute of Electrical Engineering (9 Sovetskaya street, Penza, Russia)

***Малыгина Елена Александровна***
аспирант, Пензенский государственный университет (Россия, г. Пенза, ул. Красная, 40)

E-mail: mal890@yandex.ru

***Malygina Elena Aleksandrovna***
Postgraduate student, Penza State University (40 Krasnaya street, Penza, Russia)

УДК 612.087.1; 519.7; 519.66

**Волчихин, В. И.**

**Перспективы использования искусственных нейронных сетей с многоуровневыми квантователями в технологии биометрико-нейросетевой аутентификации** / В. И. Волчихин, А. И. Иванов, В. А. Фунтиков, Е. А. Малыгина // Известия высших учебных заведений. Поволжский регион. Технические науки. – 2013. – № 4 (28). – С. 86–96.