BULLETIN OF NATIONAL ACADEMY OF SCIENCES
OF THE REPUBLIC OF KAZAKHSTAN
ISSN 1991-3494
Volume 6, Number 352 (2014), 7 – 15

MODIFICATIONS OF BERNOULLI TRIALS FOR A STATISTICAL DESCRIPTION OF NETWORKS OF ARTIFICIAL NEURAL WITH MULTILEVEL QUANTIZERS

B. S. Akhmetov[1], A. I. Ivanov[2], E. A. Malygina[3], D. N. Nadeev[2]

[1]Kazakh National Technical University named after K. I. Satpayev, Almaty, Kazakhstan;
[2]OAO "Penza Research Institute of Electrical Engineering", Penza, Russia;
[3]FGBOU VPO "Penza State University", Penza, Russia

Key words: scheme of Bernoulli trials, evaluation of the probability of dependent events, neural networks, neurons with multilevel quantizers, biometric data.

Abstract. Transition to the use of artificial neurons with quantizers with multiple levels, is technically beneficial, but already created standardized test methods are inoperable for them. Further modification of software implementation of the scheme of Bernoulli trials is proposed, which takes into account not only the dependence of the data, but also the set of states quantizers data. This opens up the possibility of creating a new test methods for neural network converters biometrics code with multilevel quantizers in artificial neurons. It is expected that for this class of converters it will be able to carry out effective testing of small test samples, since for them the Hamming distance distribution is close to normal.

УДК 519.7; 519.66; 612.087.1

МОДИФИКАЦИЯ СХЕМЫ ИСПЫТАНИЙ БЕРНУЛЛИ ДЛЯ СТАТИСТИЧЕСКОГО ОПИСАНИЯ СЕТЕЙ ИСКУССТВЕННЫХ НЕЙРОНОВ С МНОГОУРОВНЕВЫМИ КВАНТОВАТЕЛЯМИ*

Б. С. Ахметов[1], А. И. Иванов[2], Е. А. Малыгина[3], Д. Н. Надеев[2]

[1]Казахский национальный технический университет им. К. И. Сатпаева, Алматы, Казахстан;
[2]ОАО «Пензенский научно-исследовательский электротехнический институт», Пенза, Россия;
[3]ФГБОУ ВПО «Пензенский государственный университет», Пенза, Россия

Ключевые слова: схема испытаний Бернулли, оценка вероятности зависимых событий, нейронные сети, нейроны с многоуровневыми квантователями, биометрические данные.

Аннотация. Переход к использованию искусственных нейронов, имеющих квантователи с несколькими уровнями, технически выгоден, однако уже созданные стандартизованные методики тестирования оказываются для них неработоспособными. Предложена дополнительная модификация программной реализации схемы испытаний Бернулли, которая учитывает не только зависимость данных, но и множество состояний квантователей данных. Это открывает возможность создания новых методик тестирования нейросетевых преобразователей биометрия-код с многоуровневыми квантователями в искусственных нейронах. Ожидается, что и для этого класса преобразователей удастся осуществлять эффективное тестирование на малых тестовых выборках, так как и для них распределение расстояний Хэмминга оказывается близко к нормальному.

* Статья подготовлена в рамках выполнения проекта «Исследование вариантов реализации и разработка действующего лабораторного образца ON-LINE системы биометрического обезличивания электронных историй болезней для медицинского учреждения» в соответствии с Приказом Председателя Комитета науки МОН РК №17-нж от 08.04.2013 г.

В настоящее время в России и за рубежом активно идут работы по созданию преобразователей биометрии в код ключа доступа [1, 2]. Отечественные технологии строятся на использовании искусственных нейронных сетей, зарубежные технологии строятся на использовании так называемых «нечетких экстракторов» [3–6]. Независимо от использованной технологии идеальный преобразователь биометрия-код описывается классическим биномиальным законом (законом Бернулли). Если ключ на выходе преобразователя имеет длину – n и состоит только из нулей «0000…00», то угадывание h разрядов этого ключа происходит с вероятностью:

$$P(h, n, P_{"0"}) = \frac{n!}{h!\cdot(n-h)!}\cdot(P_{"0"})^{h}\cdot(1-P_{"0"})^{n-h}, \quad (1)$$

где $P_{"0"}$ – вероятность выпадения состояния «0» при поочередном угадывании разрядов кода ключа.

Биномиальный закон (1) получен Бернулли подбрасыванием симметричной или асимметричной монеты. Если монета правильная (симметричная), то выпадение обоих ее сторон равновероятно. Другими словами, $P_{"0"} = P_{"1"} = 0{,}5$. Число испытаний (длину ключа) примем $n = 256$ (эта длина соответствует длине криптографического ключа, используемого отечественными стандартами на шифрование и формирование электронно-цифровой подписи).

Идеальный преобразователь биометрия-код, соответствующий классической схеме испытаний Бернулли программно моделируется блок-схемой, отображенной на рисунке 1. Для того, чтобы получить код длиной 256 бит используются 256 генераторов нормальных случайных данных ξi, далее непрерывные случайные данные квантуются.

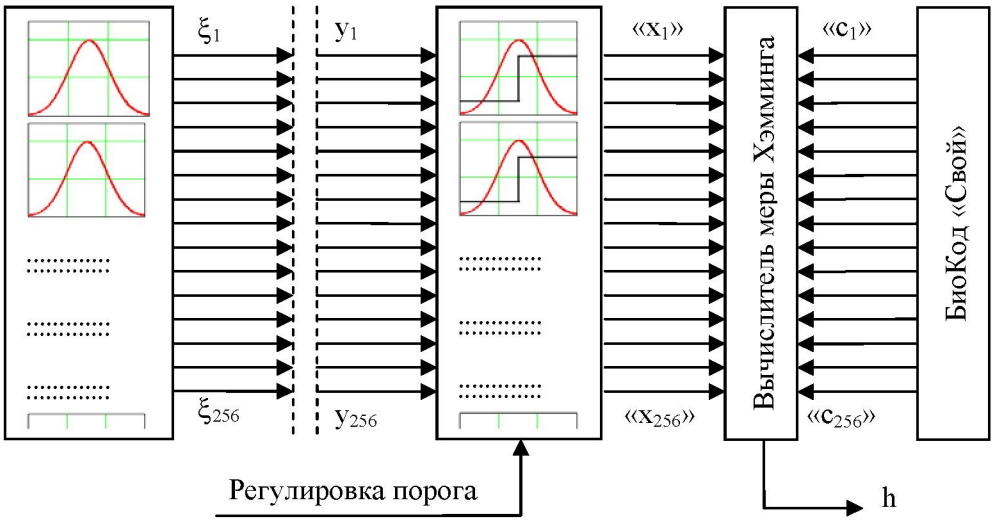

Рисунок 1 – Блок-схема программного эмулятора испытаний Бернулли

Все используемые генераторы и квантователи одинаковы, что эквивалентно подбрасыванию одной и той же монеты. Подсчет числа угаданных разрядов кода осуществляется через вычисление расстояния Хэмминга:

$$h = \sum_{i=1}^{256} "x_i" \oplus "c_i", \quad (2)$$

где $"x_i"$ – это i-тый разряд случайного кода, $"c_i"$ – это тот же разряд био-кода «Свой».

Для независимых кодов длиной 256 бит распределение расстояний Хэмминга оказывается нормальным (гистограмма расстояний Хэмминга, соответствует нормальному закону распределения значений). Для $P_{«0»} = 0.5$ математическое ожидание E(h) точно совпадает с половиной длины кода – 128, а среднеквадратическое отклонение составит $\sigma(h) = 8$. Наблюдается очень точное совпадение измеряемых параметров с параметрами классического биномиального закона (1).

Регулировка порога квантователей схемы испытаний Бернулли эквивалентно тому, что последовательно подбрасывается единственная не симметричная монета. При изменении порога срабатывания квантователей вероятность выпадения состояния «0» изменяется в пределах от 1 до 0, при этом математическое ожидание и среднеквадратическое отклонение расстояний Хэмминга продолжает точно соответствовать параметрам классического биномиального закона (1). Эти факты могут быть проверены (подтверждены) любым, кто программно воспроизведет схему испытаний Бернулли (рисунок 1).

Моделирование вектора равнокоррелированных данных. К сожалению, гипотеза независимости данных в биометрии вообще не применима. Реальные био-коды всегда имеют значительный уровень корреляции состояний разрядов. Российский базовый биометрический стандарт ГОСТ Р 52633.0-2006 [7] содержит прямое ограничение уровня остаточных корреляционных связей. Средний модуль коэффициентов парной корреляции нейросетевых преобразователей биометрия-код не должен превышать 0.15. Измерять зависимость между разрядами рекомендуется, подавая на вход преобразователя биометрия-код, случайно выбранный биометрический образ «Чужой».

Даже между данными случайных биометрических образов «Чужой» обнаруживаются существенные остаточные корреляционные связи. Однако, если био-коды «Чужой» зашифровать или осуществить их хеширование, то корреляционные связи исчезают, поток данных становится действительно «белым» шумом с независимыми и равновероятными состояниями всех разрядов. Гипотеза независимости разрядов био-кодов «Чужой» становится корректной только, если коды криптографически защищены. Во всех остальных случаях необходимо отказываться от гипотезы независимости и пытаться учесть корреляционные связи разрядов био-кодов «Чужой» [7–10].

Для того чтобы учесть существование реальных корреляционных связей между данными воспользуемся связывающей матрицей, имеющей одинаковые элементы вне единичной диагонали. Умножение на такую матрицу вектора случайных чисел приводит к появлению зависимых равно коррелированных данных:

$$\begin{bmatrix} 1 & a & \cdots & a \\ a & 1 & \cdots & a \\ \cdots & \cdots & \cdots & \cdots \\ a & a & \cdots & 1 \end{bmatrix} \times \begin{bmatrix} \xi_{1,i} \\ \xi_{2,i} \\ \cdots \\ \xi_{n,i} \end{bmatrix} = \begin{bmatrix} y_{1,i} \\ y_{2,i} \\ \cdots \\ y_{n,i} \end{bmatrix} \quad \Rightarrow \quad R = \begin{bmatrix} 1 & r & \cdots & r \\ r & 1 & \cdots & r \\ \cdots & \cdots & \cdots & \cdots \\ r & r & \cdots & 1 \end{bmatrix}. \qquad (3)$$

Номограмма, связывающая значение параметра коэффициентов корреляции между выходными данными, приведена на рисунке 2.

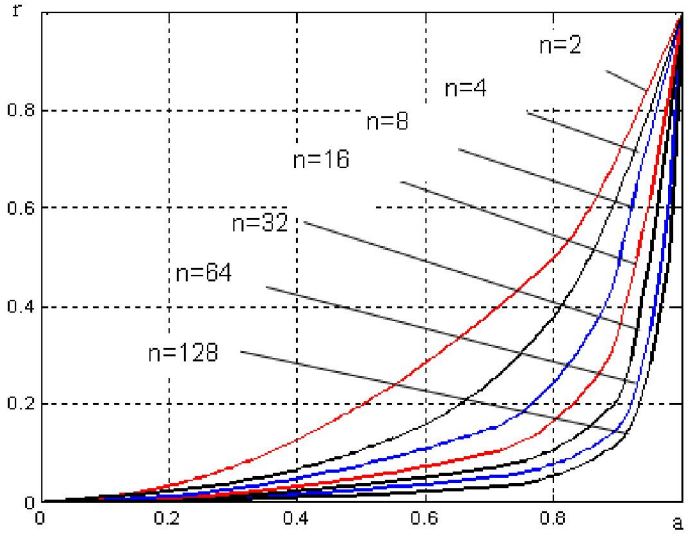

Рисунок 2 – Номограмма связи коэффициента равной коррелированности со значениями элементов связывающей матрицы

Опираясь на операцию умножения случайных данных на связывающую матрицу (3), можно построить блок введения корреляционных связей в данные.

Если этот блок включить в классическую схему испытаний Бернулли (между пунктирными линиями рисунка 1), то получим модифицированную схему испытаний Бернулли. Она будет соответствовать подбрасыванию одной монеты, однако получаемые выходные коды "$\overline{x}$" будут иметь зависимые состояния разрядов. Вместо кодов, соответствующих «белому шуму» мы получаем коды не являющиеся «белым шумом».

Если плавно изменять параметр регулировки в модифицированной схеме испытаний Бернулли, то заметим, как плотность распределения расстояний Хэмминга начнет эволюционировать. При этом при изменении коэффициента равной коррелированности в интервале от 0.0 до 0.37 плотность распределения $p(h, n = 256, P_{"0"} = 0.5, r)$ будет с инженерной точностью описываться нормальным законом распределения значений (см. рисунок 3). Именно на этот факт опирается стандарт ГОСТ Р 52633.3-2011 [11] при оценках малых вероятностей ошибок на тестовых выборках недостаточного объема, состоящих всего из 100 тестовых примеров «Чужой».

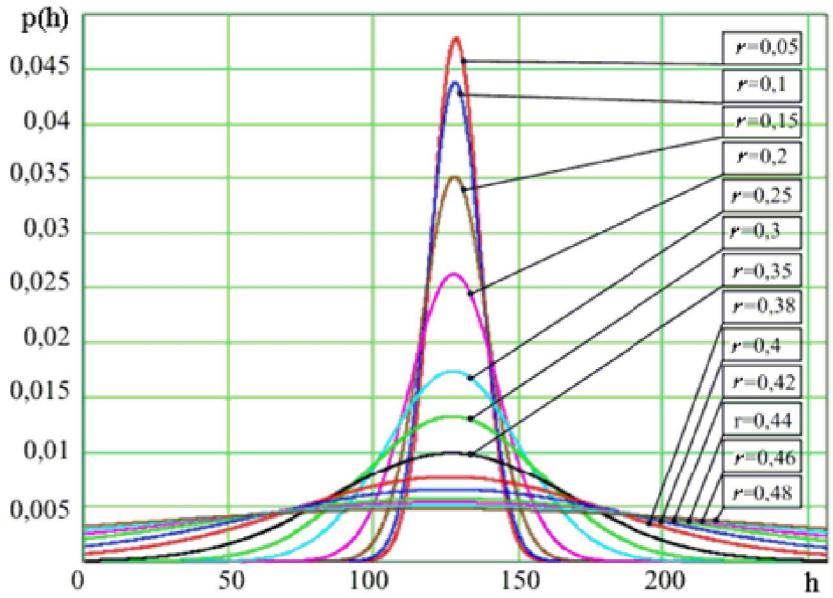

Рисунок 3 – Изменение плотности распределения значений расстояний Хэмминга для кодов с разным уровнем коррелированности разрядов

В интервале коэффициентов корреляции от 0.37 до 0.5 инженерная точность статистического описания зависимых кодов достигается использованием смеси двух источников случайных данных с нормальным и равномерным законом распределения значений. При $r = 0.5$ нормальная составляющая в смеси полностью вырождается. Для любых длин кодов распределение становится равномерным:

$$p(h, n, P_{"0"} = \frac{1}{2}, r = \frac{1}{2}) = \text{const} = \frac{1}{n+1}. \quad (4)$$

Практические преимущества модифицированной схемы испытаний Бернулли. Учет коррелированности состояний подбрасываемой монеты в модифицированной схеме испытаний Бернулли позволяет осуществлять быстрое тестирование нейросетевых преобразователей биометрия-код. Еще до испытания нейросетевого преобразователя биометрия-код априори видим, что распределение расстояний Хэмминга между кодами «Свой» и «Чужие» хорошо описывается нормальным законом распределения. Это означает, что для тестирования вероятности появления ошибок второго рода (ошибочное предоставление доступа «Чужому») необходимо оценить вероятность попадания значения расстояния Хэмминга в интервал от «0» до «1». Для этого достаточно вычислить по 100 примерам биометрических данных разных образов «Чужой» –

100 био-кодов. Далее следует найти для них E(h) и σ(h). Тогда вероятность ошибок второго рода составит:

$$P_2 \approx \frac{1}{\sigma(h)\cdot\sqrt{2\pi}}\cdot\int_0^1 \exp\left(\frac{(E(h)-u)^2}{2\cdot(\sigma(h))^2}\right)\cdot du\,. \qquad (5)$$

Провести сотню тестирований и вычислить, соответствующие, статистические моменты E(h) и σ(h) технически не сложно. Получается, что удается оценивать вероятности ошибок первого рода на уровне $P_2 = 0.000000001$, используя малую тестовую выборку, состоящую всего из 100 примеров. Эффект снижения размеров тестовой выборки примерно в миллион раз обусловлен тем, что имеется достоверная статистическая модель описания зависимых кодов «Чужой». Столь значительное сокращение затрат на тестирование является легитимным [12], только если речь идет о тестировании высоконадежных преобразователей биометрия-код построенных с использованием однослойных сетей бинарных искусственных нейронов. Каждый такой нейрон имеет в своем составе бинарный квантователь. Если бы стандарт ГОСТ Р 52633.3-2011 [8] отсутствовал, то возможность оценки вида (5) следовало бы регулярно доказывать, например, через проверку гипотезы нормальности по критерию χ^2, что неминуемо привело бы к увеличению размеров тестовой выборки в 3–5 раз.

Обобщение схемы испытаний Бернулли на сети искусственных нейронов с многоуровневыми квантователями. Анализ стойкости нейросетевых преобразователей биометрия-код к различным атакам (например, к атаке, описанной в работе [13]) показал, что технически выгодно использовать нейроны с квантователями, имеющими три и более выходных состояний. Переход от двоичных нейронов к троичным нейронам позволяет на выходе каждого нейрона иметь не один, а два бита ключа, что иллюстрируется рисунком 4.

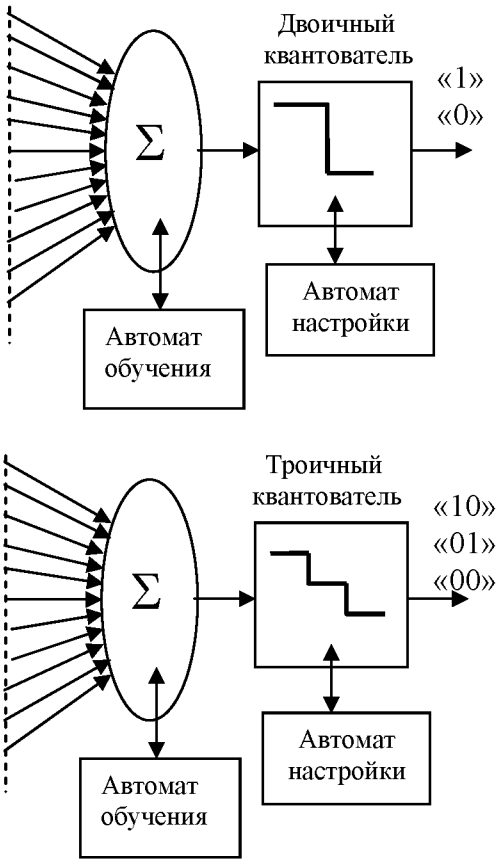

Рисунок 4 – Пример двоичного нейрона (левая часть рисунка) и троичного нейрона (правая часть рисунка)

Как следствие 21 нейрон преобразователя будут давать ключ длиной 42 бита. При этом в схеме испытаний достаточно применить только квантователь с двумя порогами срабатывания и по другой формуле вычислять расстояния Хэмминга:

$$h = \sum_{i=1}^{21} \begin{pmatrix} "x_i | x_{i+1}" \\ \oplus \quad \oplus \\ "c_i | c_{i+1}" \end{pmatrix}, \qquad (6)$$

где $"x_i|x_{i+1}"$ – конкатенация двоичных разрядов в пару, полученную на выходе i-го нейрона кода «Чужой», $"c_i|c_{i+1}"$ – конкатенация двоичных разрядов в пару, полученную на выходе i-го нейрона кода «Свой», $\oplus$ - операция поразрядного сложения по модулю два, $\sum(".|.")$ – операция сложения двухразрядных чисел в обычной двоичной арифметике (какой из разрядов бинарного кода является старшим значения не имеет).

Нейрон с троичным квантователем соответствует некоторому артефакту не зависимо или зависимо, подбрасываемому по схеме испытаний Бернулли (рисунок 1). Например, это может быть цилиндр, способный устойчиво находится в трех состояниях, опираясь на верхнее основание, нижнее основание или лежа на фрагменте боковой цилиндрической поверхности. Очевидно, что статистики состояний выходного кода длиной в 42 бита сильно зависят от симметрии подбрасываемого артефакта. Наиболее простой является статистика симметричного артефакта с тремя устойчивыми состояниями $P_{"00"}=1/3$, $P_{"01"}=1/3$, $P_{"10"}=1/3$. Оказалось, что статистики зависимых кодов хорошо описываются нормальным законом распределения значений. Соответствующие распределения для разных значений коррелированности, подбрасываемого артефакта приведены на рисунке 5.

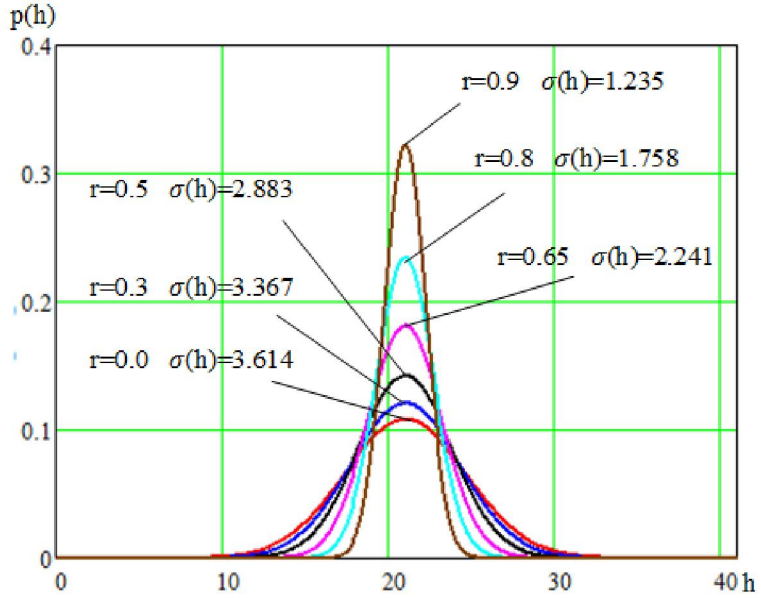

Рисунок 5 – Статистики распределений расстояний Хэмминга для модифицированной схемы испытаний Бернулли для симметричного артефакта с тремя устойчивыми состояниями и 21 испытания (E(h) = 21)

Следует подчеркнуть, что троичные нейроны ведут себя совершенно иначе, чем двоичные нейроны. У двоичных нейронов хеширующие свойства слабо выражены. В связи с этим повышение уровня коррелированности биометрических данных приводит к очевидному ослаблению преобразователя биометрия-код, состоящего из бинарных нейронов (рисунок 3).

У троичных нейронов хеширующие свойства выражены явно. И это тем сильнее заметно, чем более коррелированные сигналы подаются на входы сети из трит-нейронов. Именно из-за этого

эффекта происходит сжатие распределения расстояний Хэмминга образов « Чужой» (рисунок 5). В пределе r→1 нормальное распределение вырождается в две дельта функции:

$$\begin{cases} p(E(h)=21)=\dfrac{2}{3} \\ p(h=0)=\dfrac{1}{3} \end{cases}, \tag{7}$$

Очевидно, что метаморфоза преобразования нормального закона распределения значений в две дельта функции не может быть осуществлена линейным преобразованием. Эта метаморфоза описывается достаточно сложной нелинейной функцией.

Из-за наличия эффективного хеширования данных на уровне каждого трит-нейрона возникает иллюзия усиления стойкости нейросетевого преобразователя биометрия-код по мере роста коррелированности входных данных. Метрика расстояний Хэмминга для трит-нейронов не может быть использована для сокращения объемов тестовой выборки через вычисления вида (5). Для синтеза процедур быстрого тестирования преобразователей биометрия-код с сетью третичных нейронов необходимо переходить в иное метрическое пространство и наблюдать другие статистики. Российский стандарт [7] не применим, так как он требует перед тестированием отключить механизмы хеширования данных (механизмы перемешивания разрядов био-кода). Если есть, какой либо другой механизм размножения ошибок, его так же следует отключить. Отключить механизм хеширования в трит-нейронах технически невозможно (это новое свойство троичных квантователей, отсутствующее у двоичных квантователей).

Совершенно те же самые выводы можно сделать для всех иных артефактов с более чем тремя устойчивыми состояниями. Четыре устойчивых состояния соответствуют пирамидке с треугольными сторонами и треугольным основанием, которая должна подбрасываться во время испытаний по модифицированной схеме Бернулли. Для нейронов с пятью уровневыми квантователями геометрическую аналогию придумать достаточно сложно. Зато для нейронов с шестью устойчивыми состояниями модифицированную схему испытаний можно реализовать подбрасыванием кубика (игральной кости).

Для игральной кости (6-атных нейронов) расстояния Хэмминга вычисляется уже по тройкам соседних бинарных разрядов 63 битного выходного кода, образуемого 21 испытанием:

$$h=\sum_{i=1}^{21}\begin{pmatrix} "x_i\vert & x_{i+1}\vert & x_{i+2}" \\ \oplus & \oplus & \oplus \\ "c_i\vert & c_{i+1}\vert & c_{i+2}" \end{pmatrix}. \tag{8}$$

Все Т-арные нейроны с симметричными квантователями по (Т-1)-му порогу будут иметь нормальные распределения расстояний Хэмминга похожие на распределения, представленные на рисунке 5. Если же Т-арные нейроны утрачивают симметричность нормальные законы распределения смещаются в право или в лево от центра интервала [0; max(h)].

Для всех Т-арных нейронов в пределе r→1 происходит метаморфоза вырождения нормального распределения в две дельта функции:

$$\begin{cases} p(E(h))=\dfrac{T-1}{T} \\ p(h=0)=\dfrac{1}{T} \end{cases}. \tag{9}$$

Выводы. Бернулли предложил свою схему испытаний и вывел на ее основе биномиальный закон распределения значений вероятности почти 300 лет назад. Этот закон оказался вполне применим для статистического описания криптографических протоколов аутентификации, которые дают действительно независимые кодовые последовательности («белый шум»). Больше нет практических приложений, для которых гипотеза «белого шума» корректна. Для всех остальных практических приложений и, в том числе, для приложений нейросетевой биометрии нельзя пренебрегать коррелированностью исходных данных. Особенно это относится к методикам оценки вероятностей ошибок первого и второго рода средств биометрической аутентификации. Для

биометрии учет влияния коррелированности данных обязателен. Попытки применить для биометрических данных гипотезу «белого шума» приводят к фантастически «хорошим» результатам статистических оценок, противоречащим здравому смыслу и практическим наблюдениям.

Описанная в данной работе модификация схемы испытаний Бернулли позволяет учитывать взаимное влияние внутренних корреляционных связей объекта исследования. Появляется возможность корректного оценивания вероятности появления достаточно больших цепочек зависимых (коррелированных) событий. Такую оценку нельзя выполнить аналитически, пользуясь некоторой формулой (аналогом формулы (1) для зависимых данных). Однако, опираясь на модифицированную схему испытаний Бернулли, не трудно получить кривые функций распределения значений зависимых событий для любого числа порогов у искусственных нейронов преобразователей биометрия-код с любым числом выходов.

ЛИТЕРАТУРА

[1] Язов Ю.К., Волчихин В.И., Иванов А.И., Фунтиков В.А., Назаров И.Г. Нейросетевая защита персональных биометрических данных. – М.: Радиотехника, 2012. – 157 с.

[2] Ахметов Б.С., Волчихин В.И., Иванов А.И., Малыгин А.Ю. Алгоритмы тестирования биометрико-нейросетевых механизмов защиты информации. –Алматы: Изд-во КазНТУ им. Сатпаева, 2013. – 152 с. Режим доступа: http://portal.kaznu.kz/files/publicate/2014-01-04-11940.pdf

[3] Feng Hao, Ross Anderson, John Daugman. Crypto with Biometrics Effectively // IEEE Transactions on computers. – 2006. – Vol. 55, N 9.

[4] Y. Dodis, L. Reyzin, A. Smith Fuzzy Extractors: How to Generate Strong Keys from Biometrics and Other Noisy, Data April 13 // In EUROCRYPT. – 2004. – P. 523-540.

[5] 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.

[6] Чморра А.Л. Маскировка ключа с помощью биометрии // Проблемы передачи информаци. – 2011. – № 2(47). – С. 128-143.

[7] ГОСТ Р 52633.0-2006 «Защита информации. Техника защиты информации. Требования к средствам высоконадежной биометрической аутентификации».

[8] Ivanov A., Funtikov V., Akhmetov B., Malygin A., Urnev I. Statistical Description of Output States of the Neural Network "Biometrics-code" Transformers // Progress in Electromagnetics Research Symposium "PIERS 2012 Moscow – Progress in Electromagnetics Research Symposium, Proceedings". – 2012. – С. 62-66.

[9] Сериков А.В., Урнев И.В., Иванов А.И. Учет корреляционных связей при тестировании средств биометрико-нейросетевой аутентификации личности // Радиопромышленность. – 2011. – № 4. – С. 44-49.

[10] Ахметов Б.С., Надеев Д.Н., Урнев И.В., Сериков И.В. Аппроксимация биномиального зависимого закона композициями нормального, равномерного, арксинусного распределений значений // Нейрокомпьютеры: разработка, применение. – 2012. – № 3. – С. 17-21.

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

[12] 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.

[13] Маршалко Г.Б. Вопросы оценки стойкости нейросетевой системы биометрической аутентификации // Мат-лы конф. «РусКрипто-2013», 29 марта, г. Москва. – Режим доступа: http://www.ruscrypto.ru/netcat_files/File/ruscrypto.2013.051.zip

REFERENCES

[1] Yazov J.K., Volchikhin V.I., Ivanov A.I., Funtikov V.A. Nazarov I.G. Neural protection of personal biometric data. M.: Radio engineering, 2012. 157 p.

[2] Akhmetov B.S., Volchikhin V.I., Ivanov A.I., Maligin A.Y. Biometrics-testing algorithms neural network information protection mechanisms. Almaty Univ. KazNTU. Satpaev, 2013. 152 p. Mode of access: http://portal.kaznu.kz/files/publicate/2014-01-04-11940.pdf

[3] Feng Hao, Ross Anderson, John Daugman. Crypto with Biometrics Effectively. IEEE Transactions on computers. 2006. Vol. 55, N 9.

[4] Dodis Y., Reyzin L., Smith A. Fuzzy Extractors: How to Generate Strong Keys from Biometrics and Other Noisy, Data April 13. In EUROCRYPT. 2004. P. 523-540.

[5] Ushmaev OV, Kuznetsov VV Secure verification algorithms based on the binary representation of the topology of a fingerprint. Informatics and Applications. 2012. N 6 (1). P. 132-140.

[6] Chmorra A.L. Masking key using biometrics. Problems of Information Transmission. 2011. N 2(47). P. 128-143.

[7] GOST R 52633.0-2006 "Information Security. Security technique. Requirements for a highly reliable means of biometric authentication".

[8] Ivanov A., Funtikov V., Akhmetov B., Malygin A., Urnev I. Statistical Description of Output States of the Neural Network "Biometrics-code" Transformers. Progress in Electromagnetics Research Symposium "PIERS 2012 Moscow – Progress in Electromagnetics Research Symposium, Proceedings". 2012. S. 62-66.

[9] Serikov A.V., Urnev I.V., Ivanov A.I. Accounting for correlations in testing means biometrics-neural network identity authentication // Radio industry. 2011. N 4. S. 44-49.

[10] Akhmetov B.S., Nadeev D.N., Urnev I.V., Serikov I.V. Approximation of the binomial law dependent compositions of normal, uniform, arksinusnogo distributions of values. Neurocomputers: development and application. 2012. N 3. S. 17-21.

[11] GOST R 52633.3-2011 "Information Security. Security technique. Testing resistance means highly reliable biometric security to attack the selection".

[12] Volchikhin V.I., Ivanov A.I., Funtikov V.A., Malygina E.A. Prospects for the use of artificial neural networks with multi-level quantizers in biometrics technology, neural network authentication. News of higher educational institutions. Volga region. Engineering science. 2013. N 4(28). S. 88-99.

[13] Marshalko G.B. Questions to estimate the resistance of the neural network system of biometric authentication // Proceedings of the conference "RusCrypto 2013", 29 March, Moscow. Mode of access: http://www.ruscrypto.ru/netcat_files/File/ruscrypto.2013.051.zip

КӨПДЕҢГЕЙЛІ КВАНТТАУШЫЛАРЫ БАР ЖАСАНДЫ НЕЙРОНДАР ЖЕЛІСІН СТАТИСТИКАЛЫҚ СИПАТТАУ ҮШІН БЕРНУЛЛИНІҢ СЫНАҒЫНЫҢ СҰЛБАСЫН ЖАҢАРТУ

Б. С. Ахметов[1], А. И. Иванов[2], Е. А. Малыгина[3], Д. Н. Надеев[2]

[1]Қ. И. Сәтбаев атындағы Қазақ ұлттық техникалық университеті, Алматы, Қазақстан;
[2] "Пенза электротехникалық ғылыми-зерттеу институты" ААҚ, Пенза, Ресей;
[3] "Пенза мемлекеттік университеті" ФМББМ ЖКБ, Пенза, Ресей

Тірек сөздер: Бернулли сынақ сұлбасы, тәуелді оқиғалардың мүмкіндігін бағалау, нейрондық желілер, көпдеңгейлі кванттаушылары бар нейрондар, биометрикалық мәліметтер.

Аннотация. Мәліметтерді кванттау күйінің жиыны және мәліметтер тәуелділігін есепке алып Бернулли сынағының сұлбасын іске асыру бағдарламасын жаңартудың қосымшасы ұсынылады. Бұл жасанды нейрондарда көпдеңгейлі кванттаушылары бар биометрия-кодты нейрожелілік түрлендіргіштерді сынаудың жаңа тәсілін жасаудың мүмкіндіктерін ашады.

Поступила 23.10.2014 г.