А. И. Иванов, П. С. Ложников, А. Е. Сулавко, Оценка надежности верификации автографа на основе искусственных нейронных сетей, сетей многомерных функционалов Байеса и сетей квадратичных форм, *Компьютерная оптика*, 2017, том 41, выпуск 5, 765–774

DOI: 10.18287/2412-6179-2017-41-5-765-774

ОЦЕНКА НАДЕЖНОСТИ ВЕРИФИКАЦИИ АВТОГРАФА НА ОСНОВЕ ИСКУССТВЕННЫХ НЕЙРОННЫХ СЕТЕЙ, СЕТЕЙ МНОГОМЕРНЫХ ФУНКЦИОНАЛОВ БАЙЕСА И СЕТЕЙ КВАДРАТИЧНЫХ ФОРМ

А.И. Иванов[1], П.С. Ложников[2], А.Е. Сулавко[2]
[1]АО «Пензенский научно-исследовательский электротехнический институт», Пенза, Россия,
[2]ФГБОУ ВО «Омский государственный технический университет» (ОмГТУ), Омск, Россия

Аннотация

Осуществлено экспериментальное сравнение «широких» искусственных нейронных сетей из различных функционалов для верификации автографа подписанта. Собрана база автографов субъектов для проведения вычислительного эксперимента. Подтверждено, что повышение размерности решающих правил (функционалов) до определенного момента приводит к снижению вероятностей ошибок верификации подписи, увеличение количества нейронов сети уменьшает число ошибок, а также многомерный функционал Байеса работает тем лучше, чем выше корреляция между признаками и его размерность. Наилучший результат по верификации автографа получен с использованием сетей многомерных функционалов Байеса: вероятность ошибок 1-го и 2-го рода составила 0,0288 и 0,0232 соответственно.

Ключевые слова: нейронные сети, сети квадратичных форм, многомерные функционалы Байеса, особенности воспроизведения подписи, биометрические признаки.

Цитирование: **Иванов, А.И.** Оценка надежности верификации автографа на основе искусственных нейронных сетей, сетей многомерных функционалов Байеса и сетей квадратичных форм / А.И. Иванов, П.С. Ложников, А.Е. Сулавко // Компьютерная оптика. – 2017. – Т. 41, № 5. – С. 765-774. – DOI: 10.18287/2412-6179-2017-41-5-765-774.

Введение

На сегодняшний день подавляющее большинство офисных документов создается с помощью информационных технологий, для обеспечения аутентичности и целостности которых используется электронно-цифровая подпись (ЭЦП). Существенным недостатком классической ЭЦП является то, что она является отчуждаемой от своего владельца в отличие от традиционной подписи. Это обстоятельство является причиной множества компьютерных преступлений. По данным PricewaterhouseCoopers (PwC), число инцидентов, связанных с нарушением информационной безопасности, неуклонно растет [1]: в 2009 году PwC зафиксировано 3,4 млн. инцидентов, в 2010 – 9,4 млн., в 2011 – 22,7 млн., в 2012 – 24,9 млн., в 2013 – 28,9 млн., в 2014 – 42,8 млн., в 2015 – 59 млн. Оценки среднего ущерба от одного инцидента ИБ зависят от масштаба бизнеса и составляют от 0,41 до 5,9 млн. долларов США. Большая часть убытков обусловлена деятельностью собственных или бывших сотрудников компаний. На сегодняшний день наиболее опасный злоумышленник – это квалифицированный «инсайдер», получивший доступ к ЭЦП руководителя с помощью привилегий своего положения в компании. Чтобы устранить данный недостаток ЭЦП, предлагается перейти к концепции гибридного документооборота, сформулированной в [2]. Ключевым атрибутом гибридного документа является ЭЦП, при формировании которой используются биометрические данные ее владельца. В качестве биометрических характеристик (признаков) могут быть использованы параметры воспроизведения и внешнего вида рукописных образов. В настоящей работе проведена оценка эффективности различных преобразователей биометрия–код для решения задачи генерации ключевых последовательностей бит на основе особенностей автографа.

Общая концепция преобразователя биометрия–код

Основное отличие преобразователей биометрия–код (ПБК) от методов обычной биометрической аутентификации состоит в том, что каждый образец биометрических данных предварительно преобразуется в битовую (ключевую) последовательность, которую возможно использовать в целях аутентификации субъекта или криптографической защиты документов (в качестве кода доступа, ключа шифрования и т.д.). При этом эталон субъекта должен храниться в виде вспомогательной информации, не позволяющей восстановить из нее биометрические характеристики субъекта (рис. 1). Требования к защите биометрического эталона при разработке систем высоконадежной биометрической аутентификации прописаны в ГОСТ Р 52633.0-2006 [3] (пункты 5.2–5.3 стандарта). Если генерируется нехарактерный для субъекта код, происходит ошибка 1-го рода. За ошибку 2-го рода принимается ситуация, при которой коды, полученные из биометрических данных двух различных субъектов, совпадают. Вероятности ошибок 1-го (FRR, *false reject rate*) и 2-го (FAR, *false acceptance rate*) рода характеризуют надежность ПБК. При верификации кода решение принимается исходя из допустимого расстояния Хемминга H между генерируемым и верным кодами.

Биометрические признаки

Сформирована база данных автографов 65 субъектов, для ввода которых испытуемые пользовались графическим планшетом Wacom. Подпись состоит из функций положения пера на планшете $x(t)$, $y(t)$ и давления пера на планшет $p(t)$, где t – это время в дискретной форме. Операция преобразования образца и получения из него вектора значений признака (реализации) в

настоящей работе реализуется аналогично тому, как это выполнялось в работе [4]. Краткое описание признаков представлено в табл. 1. Общее количество признаков – 236. Предварительно, перед вычислением значений признаков, функции $x(t)$, $y(t)$ и $p(t)$ нормируются по длительности. Выполняется прямое разложение функций в ряд Фурье и последующее обратное преобразование, но с одинаковой длительностью, равной средней длине масштабируемых сигналов (размерность на выходе должна быть числом, кратным степени 2).

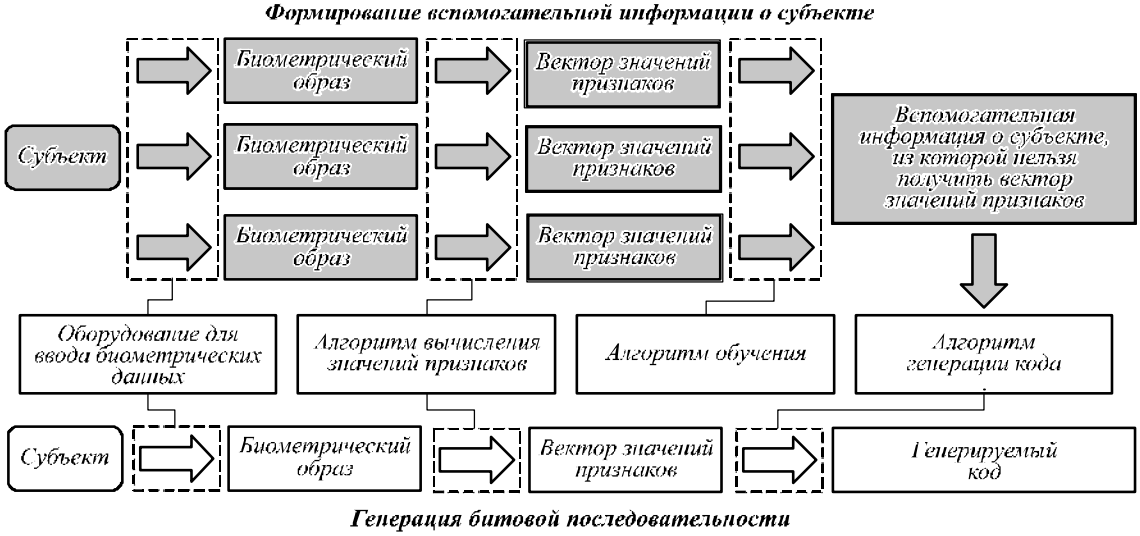

Рис. 1. Общая схема преобразователя биометрия–код

Табл. 1. Признаки, используемые для генерации кодов в настоящем исследовании

№	Краткое описание признаков	Количество признаков
1	Расстояния между 16 точками подписи, нормированные по длине подписи, в трехмерном пространстве (третье измерение – это давление $p(t)$). Точки выбираются равномерно, далее находятся расстояния между всеми различными парами этих точек [4].	120
2	Следующие характеристики статического изображения подписи: отношение длины подписи к её ширине, центр подписи, угол наклона подписи, угол наклона между центрами половин подписи [4].	5
3	Нормированные по энергии амплитуды первых 16 (наиболее низкочастотных) гармоник функции скорости перемещения пера на планшете $v_{xy}(t)$ и функции давления пера на планшет $p(t)$. Первые 16 гармоник содержат более 95% энергии сигналов $v_{xy}(t)$ и $p(t)$, что характерно для всех испытуемых [4].	32
4	Коэффициенты корреляции между всеми парами функций подписи $x(t)$, $y(t)$, $p(t)$ и их производными $x'(t)$, $y'(t)$, $p'(t)$ [4].	15
5.	Значения функций $x(t)$, $y(t)$ и $p(t)$, а также функции скорости перемещения пера на планшете $v_{xy}(t)$, которые выбираются равномерно (используется по 16 значений каждой функции) [4].	64

Модели преобразователей биометрия–код

Изначально сложилось 2 основных подхода к реализации преобразователей биометрия–код: «нечеткий экстрактор» [5] и нейросетевой (НПБК). Первый основан на квантовании «сырых», необогащенных значений признаков и применении к ним алгоритмов помехоустойчивого кодирования для исправления ошибок, возникающих вследствие невозможности точного повторного воспроизведения биометрического образа. По результатам исследований и экспериментального сравнения данных подходов установлено, что нечеткие экстракторы на основе классических самокорректирующихся кодов существенно уступают нейронным сетям в надежности генерации ключевых последовательностей, а также обладают множеством недостатков [4, 6–7]. Поэтому в настоящем исследовании «нечеткие экстракторы» не рассматриваются в качестве варианта решения поставленной задачи.

Второй подход основан на идее использования искусственных нейронных сетей. На данный момент эта идея доведена до эффективных практических решений. Сеть искусственных нейронов обогащает реализации, после чего эти данные квантуются на выходе сети. Корпорацией Google и рядом иных производителей используются так называемые «глубокие» нейронные сети Галушкина–Хинтона. Предложил многослойные нейронные сети и алгоритм их обучения в 1974 году А.И. Галушкин [8]. Джефри Хинтон [9] усовершенствовал алгоритм обучения, применив машины Больцмана для обучения нижних слов нейронов. Попытки использования «глубоких» нейронных сетей к решению задачи идентификации личности человека по динамике воспроизведения автографа не дают желаемого эффекта [10], так как у «глубоких» нейронных сетей существует ряд принципиальных недостатков:

– алгоритм обучения (переобучения) «глубоких» нейронных сетей «обратным распространением ошибки» имеет экспоненциальную вычислительную сложность, его нельзя реализовать на планшетном компьютере, оторванном от обучающих серверов корпорации Google (что неприемлемо в приложениях биометрический аутентификации);
– указанный алгоритм обучения (переобучения) «глубоких» нейронных сетей требует наличия огромной базы (порядка 100 000 и более) обучающих примеров;
– современные «глубокие» нейронные сети имеют до 100 слоев нейронов, что является избыточным по теоремам Колмогорова [11];
– пользователи «глубоких» нейронных сетей не могут быть уверены в надежности их работы, так как для них отсутствуют методы быстрого тестирования вероятностей ошибок первого и второго рода (по этой причине разработчикам этой технологии приходится придумывать другие критерии оценки надежности сетей);
– обучение глубоких нейронных сетей не может быть полностью автоматизировано и всегда ведется под контролем человека, что нежелательно в ответственных приложениях информационной безопасности.

В настоящем исследовании принято решение отказаться от использования «глубоких» нейронных сетей в рамках поставленных задач, так как этот путь требует огромных затрат вычислительных ресурсов и опасен для пользователей (нельзя компрометировать биометрические данные субъекта, оправляя их на удаленный сервер). Далее в статье рассматриваются «широкие» нейронные сети и их модификации, использование которых в приложениях биометрической аутентификации является рекомендуемым подходом в России. Данный подход хорошо стандартизован (гораздо лучше, чем «нечеткие экстракторы», семейство ГОСТ Р 52633 насчитывает 8 стандартов, описывающих требования к процедурам быстрого обучения, тестирования НПБК и интерфейсы взаимодействия с ними). Дополнительным преимуществом подхода является отсутствие привязки к огромной базе подписей, коллективно созданной для обучения и тестирования нейронных сетей.

В ГОСТ Р 52633.5-2011 [12] описан первый не итерационный абсолютно устойчивый алгоритм обучения сети персептронов, разработанный для биометрии. В соответствии с ГОСТ Р 52633.5-2011 [12] рекомендуется использовать однослойные или двухслойные нейронные сети, большее количество слоев считается избыточным [6]. Первый слой обогащает биометрические данные, второй слой играет роль кодов, исправляющих ошибки [12]. Сравнение сетей различных функционалов целесообразно производить без использования второго слоя, в настоящей работе будут применяться только однослойные сети. Разница между свёрточными сетями (сетями глубокого обучения Галушкина–Хинтона) и «широкой» нейронной сетью, обученной по ГОСТ Р 52633.5, иллюстрируется на рис. 2.

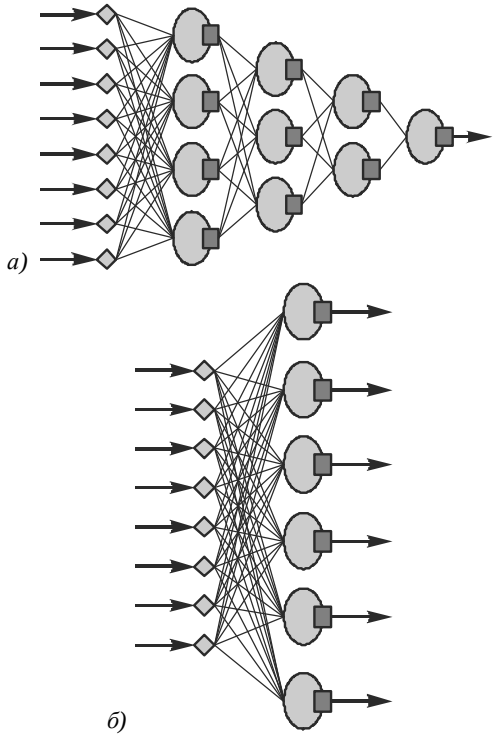

Рис. 2. Два типа архитектуры нейронных сетей: «глубокие» и «широкие» нейронные сети: глубокая сеть нейронов Галушкина–Хинтона (а) и широкая сеть нейронов по ГОСТ Р 52633.5-2011 (б)

Согласно ГОСТ Р 52633.5-2011 для обучения персептронов требуется не менее 21 реализации образа «Свой» и 64 независимых реализации образа «Чужой». Для каждого субъекта требуется создавать отдельную сеть нейронов. Операции по настройке сети описаны в стандарте [12], а также их можно найти в работах [4, 6–7]. Отметим лишь, что модули весов нейронов первого слоя вычисляются по формуле (1), а выход сумматора нейрона на этапе верификации определяется по формуле (2).

$$\mu_j = |M_ч\langle a_j\rangle - M_c\langle a_j\rangle| \,/\, \sigma_ч\langle a_j\rangle \cdot \sigma_c\langle a_j\rangle, \qquad (1)$$

где $M_c\langle a_j\rangle$ – математическое ожидание значений j-го признака образа «Свой», $\sigma_c\langle a_j\rangle$ – среднеквадратичное отклонение значений j-го признака образа «Свой», $M_ч\langle a_j\rangle$ и $\sigma_ч\langle a_j\rangle$ – аналогичные показатели образа «Чужой». Если нейрон настроен на выдачу единицы при поступлении реализации образа «Свой», то знак весового коэффициента выбирается исходя из правила: «+» при $M_ч\langle a_j\rangle < M_c\langle a_j\rangle$, иначе «–». Если нейрон настроен на нуль, знаки инвертируются.

$$y_i = \sum_{j=1}^{m} \mu_j \cdot a_j + \mu_0, \qquad (2)$$

где a_j – значение j-го входа i-го нейрона, ассоциированного с одним из признаков, m – число входов нейрона, μ_j – весовой коэффициент j-го входа i-го нейрона, μ_0 – нулевой вес, отвечающий за переключатель квантователя нейрона (пороговое значение).

Помимо сетей персептронов, для генерации кода можно использовать сеть иных функционалов, в частности, квадратичных форм (3). Классическая квадратичная форма предполагает обращение корреляционных (ковариационных) матриц (размерность матрицы равна количеству признаков). В биометрических приложениях обращение этих матриц затруднительно, если их размерность оказывается высокой [13–14]. В этом случае возникает эффект, называемый «проклятием размерности» [13–14]. Поэтому возможно использовать сети малоразмерных квадратичных форм (3) или высокоразмерных квадратичных форм, не учитывающих корреляционные связи, например, сеть из функционалов Пирсона (4) [13–15]. Метрика Пирсона (4) не учитывает корреляцию между признаками, с усилением корреляционной зависимости ее мощность снижается [15]. Альтернативным вариантом является мера Байеса–Пирсона (5) [15], которая зависит от многомерной корреляции между признаками. Механизм влияния корреляционных связей на метрику (5) поясняется в работе [15].

$$y(\overline{a}) = (\mathrm{M}\langle \overline{a} \rangle - \overline{a})^T \cdot [R]^{-1} \cdot (\mathrm{M}(\overline{a}) - \overline{a}), \qquad (3)$$

где $\overline{a}$ – вектор значений признаков с единичными стандартными отклонениями, $\mathrm{M}\langle a_j \rangle$ – математическое ожидание нормированных значений соответствующих признаков.

$$y_i = \sum_{j=1}^{m} \frac{(\mathrm{M}\langle a_j \rangle - a_j)^2}{\sigma\langle a_j \rangle^2}, \qquad (4)$$

$$y_i = \sum_{j=1}^{m} \sum_{k=1}^{m} \left| \frac{|\mathrm{M}\langle a_k \rangle - a_k|}{\sigma\langle a_k \rangle} - \frac{|\mathrm{M}\langle a_j \rangle - a_j|}{\sigma\langle a_j \rangle} \right|, \qquad (5)$$

где a_j – значение j-го входа i-го нейрона, ассоциированного с одним из признаков, $\mathrm{M}\langle a_j \rangle$ – математическое ожидание значений j-го входа i-го нейрона, $\sigma\langle a_j \rangle$ – среднеквадратичное отклонение значений j-го входа i-го нейрона, m – количество входов нейрона.

В работах [14, 16] предложено использовать сеть многомерных функционалов Байеса (6) [16], которые так же, как мера Байеса–Пирсона, ориентированы на нахождение близости входного образа не только к эталону, но и к корреляционным связям образа между признаками. В теории m-мерный вычислительный элемент Байеса (6) работает лучше при повышении размерности m и значений модулей коэффициентов его равной коррелированности [16].

$$y_{k,j} = \sum_{i=1}^{m} \left| \frac{|\mathrm{M}\langle a_k \rangle - a_{k,j}|}{\sigma\langle a_k \rangle} - \frac{|\mathrm{M}\langle a_i \rangle - a_{i,j}|}{\sigma\langle a_i \rangle} \right|, \qquad (6)$$

где $a_{i,j}$ – значение i-го признака (входа нейрона) с высоким значением модуля корреляции $|r_{i,k}|$ по отношению к k-му биометрическому признаку $a_{k,j} (i \neq k)$, j – номер биометрического образца образа «Свой», для которого вычисляется функционал, $\mathrm{M}\langle a_i \rangle$ и $\sigma\langle a_i \rangle$ – математическое ожидание и среднеквадратичное отклонение i-го признака (входа нейрона). При функциональной зависимости признаков ($|r| = 1$) значение метрики (6) всегда имеет нулевое значение. При уменьшении $|r|$ значения функционала (6) и их стандартное отклонение возрастают.

При формировании сети функционалов (4) и (5) обработчики признаков соединялись с нейронами случайным образом. Количество нейронов N и входов m задавалось как параметр и изменялось в процессе вычислительного эксперимента. Сеть многомерных функционалов Байеса (6) формировалась иным образом. Изначально вычислялись коэффициенты парной корреляции r между всеми сечениями (совокупностями значений) всех признаков (рис. 3) обучающей выборки. Признаки соединялись с входами нейронов исходя из модуля равной коррелированности, под которой подразумевается, что разница $|r|$ для признаков не превышает τ (значение τ задавалось как параметр). Сначала формируется K_1 нейронов для первого признака, потом K_2 для второго и так далее. С первым из K_1 нейронов соединяются первый признак и признаки, которые имеют модуль коэффициента корреляции с ним в интервале $[1; 1-\tau]$, если их число не менее двух (минимальная размерность). Далее производится поиск признаков, имеющих модуль коэффициента корреляции с первым признаком в интервале $[1-\tau; 1-2\cdot\tau]$, процедура повторяется многократно, пока $1-l\cdot\tau > \phi$, где ϕ – максимальный модуль корреляции учитываемых признаков, l – номер итерации поиска признаков с равной корреляцией. Аналогичным образом формируются по K_j нейронов на признак, с каждым из которых связан j-й признак и i-е признаки, если $1-(l-1)\cdot\tau < |r_{i,j}| < 1-l\cdot\tau$. Общее количество нейронов сети равно сумме коэффициентов K_j, т.е. число нейронов для каждой сети (для каждого из испытуемых) не является фиксированным, как и количество входов нейронов.

Независимо от типа нейрона, значение на выходе его функционала сравнивается с пороговым. Для каждого нейрона существует оптимальный порог срабатывания, который вычисляется (кроме персептронов) исходя из произведения $\theta = y_{max} \cdot h$, где y_{max} – это максимальное значение функционала при поступлении на вход обучающих реализаций образа «Свой», h – стабилизирующий коэффициент, экспериментально подбираемый для каждого пространства признаков по минимальной сумме вероятностей ошибок 1-го и 2-го рода. Если порог превышен, нейрон выдает единицу («1»), иначе нуль («0»). Настройка сети на нужный выходной код производится инвертированием выходных значений отдельных нейронов. Название искусственной нейронной сети зависит от метрики, которая лежит в ее основе: Пирсона–Хемминга (4), Байеса–Пирсона-Хемминга (5), Байеса–Хемминга (6).

Особенностью функционалов (4), (5), (6) является необходимость хранения параметров распределения признаков. Недостаток устраняется путем создания гибридной сети с изолированным потоком персептронов (2), на выходах которых будут шифроваться параметры нейронов иных функционалов по принципу защищенного нейросетевого контейнера [4].

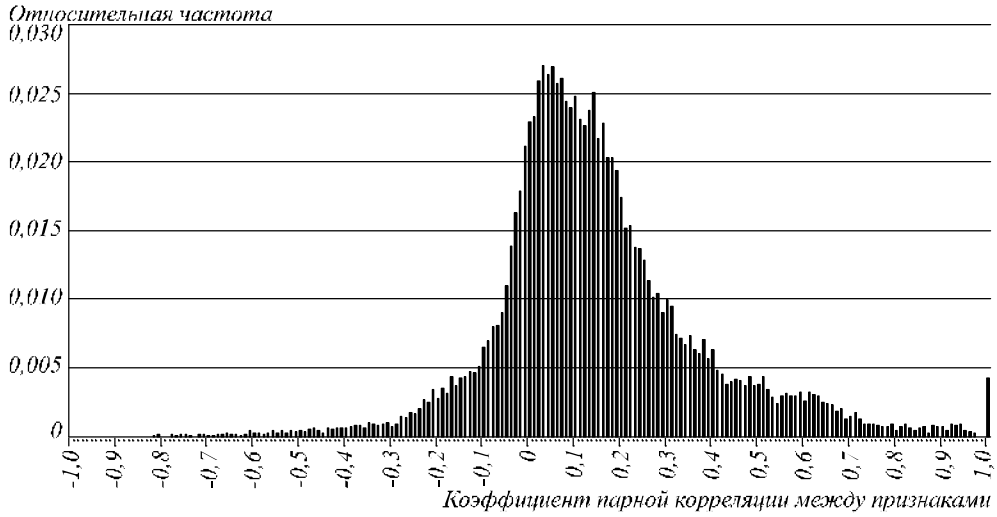

Рис. 3. Корреляционная зависимость 236 признаков подписей для 65 испытуемых (вычисление коэффициентов корреляции выполнялось в отдельности для каждого субъекта)

Результаты по генерации кодов и их анализ

Проведен вычислительный эксперимент. Подписи были преобразованы в реализации. Для обучения использовалось по 21 реализации образа «Свой» (а также по 1 реализации каждого образа для обучения персептронов на данных «Чужой»). Далее проводились серии опытов по верификации субъектов сетями персептронов, Байеса–Пирсона–Хемминга, Пирсона–Хемминга и Байеса–Хемминга. В процессе эксперимента изменялись значения параметров N, m, τ и ϕ. Подсчитывалось общее число ошибок 1-го и 2-го рода, FRR и FAR вычислялись как отношения количества ошибок соответствующего рода к числу проведенных опытов с использованием соответственно реализаций «Свой» и «Чужой». Рис. 4 демонстрирует графики вероятностей ошибки верификации любого рода испытуемых при оптимальных значениях порога (определяется по минимуму FRR+FAR в каждой серии испытаний).

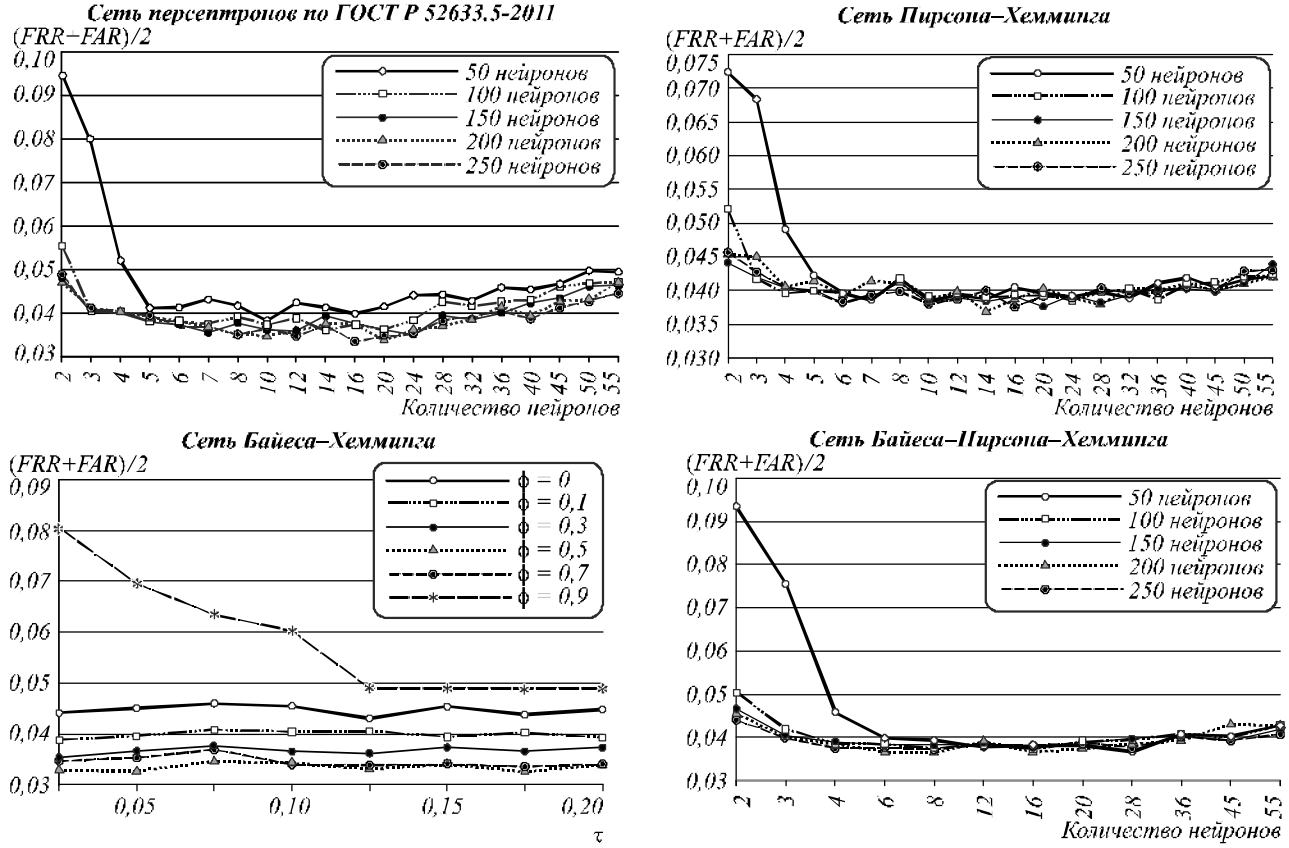

Рис. 4. Вероятности ошибок верификации 65 испытуемых (при пороге H = 0)

При использовании только «плохих», сильно коррелирующих признаков ($0{,}5 \le \phi < 0{,}9$) вероятность ошибки генерации сетями Байеса–Хемминга (рис. 4) ниже, чем в случае, если использовать также признаки со слабой корреляцией ($\phi < 0{,}5$). Это подтверждает тезис о том, что многомерный функционал Байеса работает тем лучше, чем выше корреляция между признаками (при работе с «хорошими» признаками функционал с большей вероятностью выдает неверный бит кода). Число признаков с высокой корреляцией невелико (рис. 3), поэтому при $\phi = 0{,}9$ размерность сети низкая и ошибок много, но при увеличении значения τ их количество интенсивно снижается. В остальных случаях этот параметр влияет на вероятность ошибок незначительно. С ростом значения τ интервал равной корреляции расширяется, т.е. в один функционал попадают признаки со все более различной взаимной корреляцией. Одновременно с этим размерность функционалов m повышается. Это не противоречит тезису о том, что многомерный функционал Байеса повышает работоспособность при увеличении размерности, если признаки равно коррелированы, т.е. снижение вероятности может не происходить по причине неравной корреляции. Однако при $\phi = 0{,}9$ почти все признаки коррелируют одинаково, т.к. τ не может превысить 0,1 (при $\phi = 0{,}9$, $\tau > 0{,}1$ ничего не меняется, рис. 4).

Из рис. 4 видно, что повышение размерности функционалов снижает вероятность ошибок до определенного момента – участка насыщения. Увеличение N не влияет существенным образом на вероятность ошибки, если не корректировать коды, генерируемые сетью. Корректировка ключевой последовательности может быть осуществлена вторым слоем нейронов, реализованным по ГОСТ Р 52633.5-2011 [12], или методом помехоустойчивого кодирования, предложенным в [17] и разработанным специально для биометрии. Второй вариант предпочтительнее, т.к. позволяет скорректировать фиксированное количество бит кода.

Рис. 5 иллюстрирует следующее: если повысить пороговое значение расстояния Хемминга H от генерируемого до верного кода, то можно получить выигрыш по сумме FRR+FAR. Как раз это и позволяет сделать метод помехоустойчивого кодирования из [17] без необходимости в хранении эталонного (верного) кода, на который настраивается сеть, для вычисления H. После анализа результатов эксперимента были найдены оптимальные пороговые значения H, при которых сумма ошибок 1-го и 2-го рода была минимальной. Уменьшение ошибок может достигаться, пока корреляция выходных значений нейронов невысока. В этом отношении разные сети имеют отличия (рис. 6). Наиболее показательными являются результаты верификации сетями Байеса–Хемминга, даже с учетом, что при $\phi = 0{,}9$ вероятность ошибки не меняется (рис. 4 и 7).

Полученные результаты (табл. 2) могут быть улучшены при добавлении множества менее информативных признаков (коэффициенты корреляции между коэффициентами одно-, двух- и трехмерного ряда Фурье, вейвлет-преобразований, двумерные и трехмерные амплитуды гармоник суперпозиций функций $x(t)$ $y(t)$, $p(t)$). Рассмотренная система из 236 признаков имеет максимум по r (при $r \approx 0{,}0$, рис. 3). В интервал [0; 0,3] попадает около 50 % признаков, их следует анализировать сетями Пирсона–Хэмминга, более 30 % признаков имеют модуль корреляции в интервале [0,3; 0,7], их следует обрабатывать персептронами, обученными по ГОСТ Р 52633.5. Порядка 30 % признаков с $|r| > 0{,}5$ нужно обрабатывать сетями многомерных функционалов Байеса–Хэмминга. Создав гибридную сеть, можно снизить FRR и FAR.

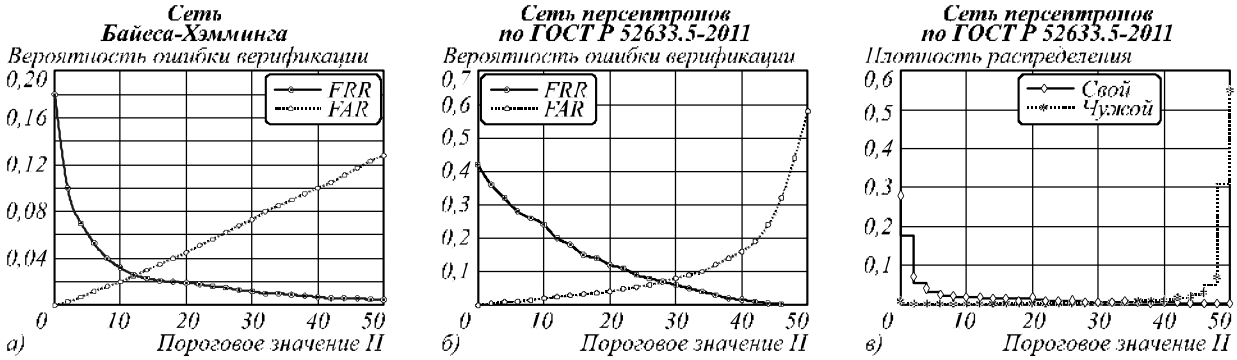

Рис. 5. Влияние H на FRR и FAR (а, б), распределение H от получаемого до верного кода (в)

Табл. 2. Наилучшие полученные параметры надежности верификации субъектов (ΔEr – коэффициент снижения суммы вероятностей ошибок FRR+FAR)

Тип сети	FRR, $H=0$	FAR, $H=0$	Параметры сети, $H=0$	FRR, $H>0$	FAR, $H>0$	Параметры сети, $H>0$	Среднее ΔEr, %
Байеса–Пирсона–Хемминга	0,0421	0,0308	$m=8$; $N=200$	0,0407	0,029	$m=4$; $N=250$	2,08 %
Пирсона–Хемминга	0,0317	0,0421	$m=14$; $N=200$	0,0236	0,0459	$m=5$; $N=50$	3,59 %
НПБК ГОСТ Р 52633.5-2011	0,0307	0,0361	$m=16$; $N=250$	0,0307	0,0361	$m=16$; $N=250$	0,6 %
Байеса–Хемминга	0,034	0,0312	$\tau=0{,}05$; $\phi=0{,}5$	0,0288	0,0232	$\tau=0{,}05$; $\phi=0{,}5$	12,38 %

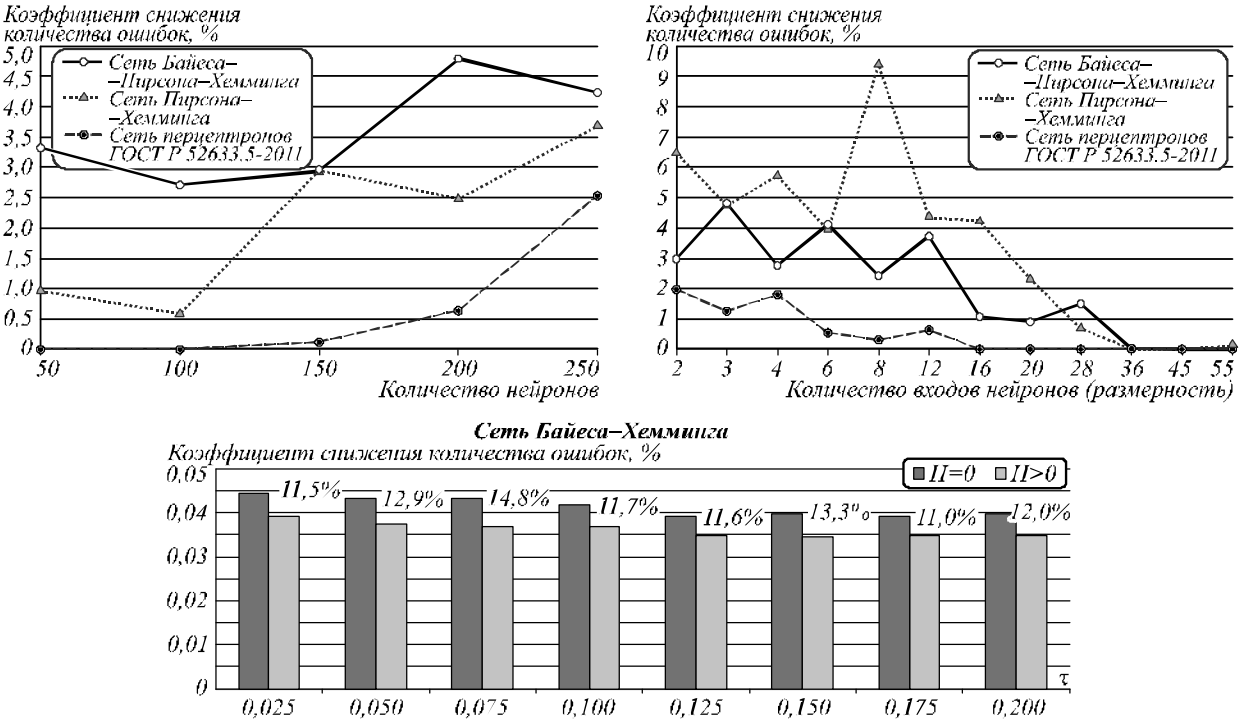

Рис. 6. Снижение вероятностей ошибок верификации с повышением порогового значения H

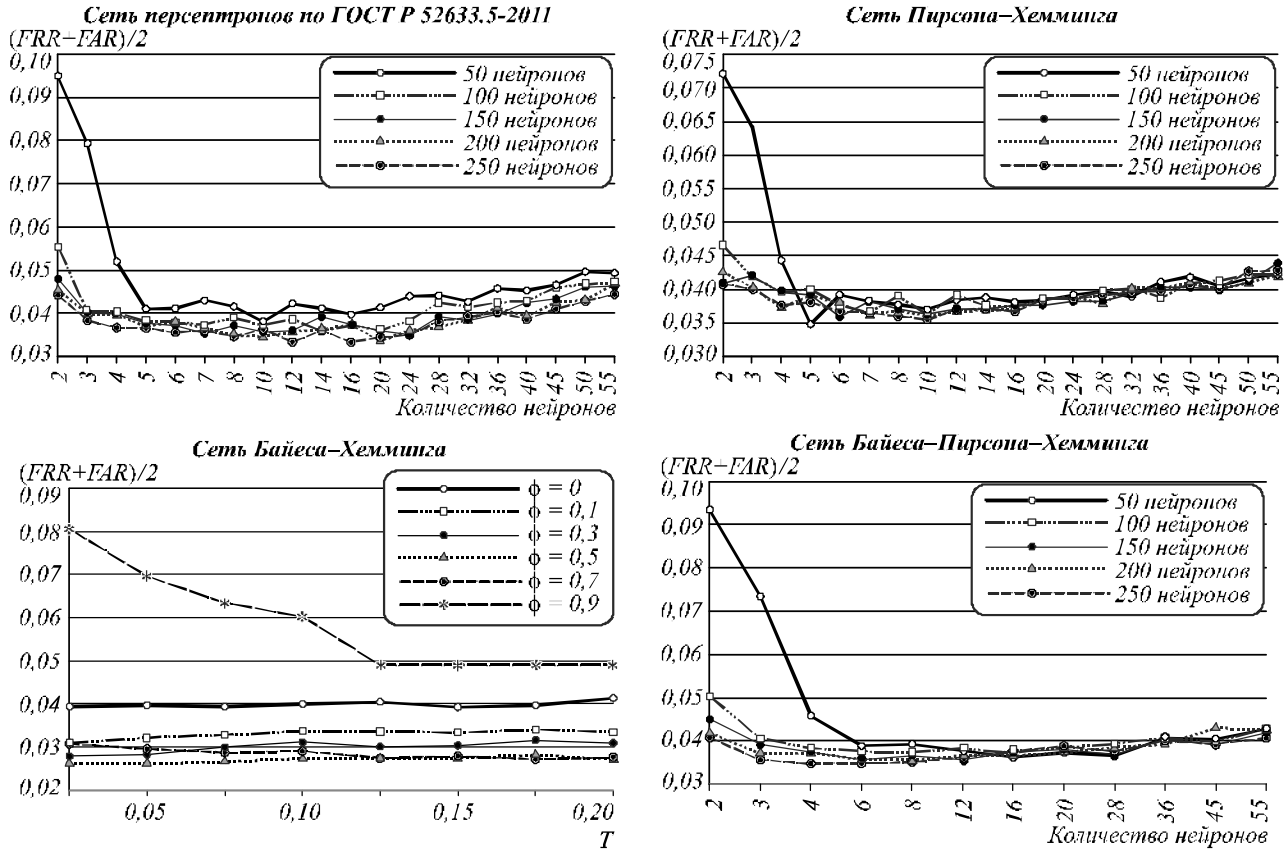

Рис. 7. Вероятности ошибок верификации 65 испытуемых (при пороге H>0)

Заключение

Сформулируем ключевые выводы. В процессе работы экспериментально подтверждено, что многомерный функционал Байеса работает тем лучше, чем выше коэффициент равной коррелированности признаков и выше его размерность. Повышение размерности функционалов позволяет снизить вероятность ошибок до попадания на участок насыщения, дальнейшее повышение размерности не дает преимуществ. Сформировав сеть из нескольких решающих

правил с близкими вероятностями ошибок и объединив их результаты, удается получить существенный выигрыш в показателях интегральной ошибки распознавания субъектов. Наивысшим потенциалом по снижению ошибок таким способом обладает сеть Байеса–Хемминга, наименьшим – сеть персептронов (12,38 %). При генерации кода на основе биометрических данных аналогичного эффекта можно добиться корректировкой нескольких неверных бит на выходе первого слоя сети нейронов [17]. Увеличение количества решающих правил целесообразно проводить, пока правила ошибаются по-разному, т.е. не полностью коррелированы. Наилучший результат был получен сетью Байеса–Хемминга: FRR = 0,0288; FAR = 0,0232.

Благодарности

Работа частично выполнена (анализ недостатков глубоких искусственных нейронных сетей) при финансовой поддержке Министерства образования и науки РФ в рамках базовой части государственного задания в сфере научной деятельности (проект № 2.9314.2017/БЧ).

Экспериментальная часть работы выполнена при финансовой поддержке РФФИ (грант № 16-07-01204).

Литература

1. The Global State of Information Security® Survey 2016. PricewaterhouseCoopers [Electronical Resource]. – URL: http://www.pwc.com/gx/en/issues/cyber-security/information-security-survey/download.html (request date 27.06.2016).
2. **Иванов, А.И.** Технология формирования гибридных документов / А.И. Иванов, П.С. Ложников, А.Е. Самотуга // Кибернетика и системный анализ. – 2014. – Т. 50, № 6. – С. 152-156.
3. ГОСТ Р 52633.0-2006. Защита информации. Техника защиты информации. Требования к средствам высоконадёжной биометрической аутентификации. – М.: Стандартинформ, 2006. – 24 с.
4. **Ложников, П.С.** Экспериментальная оценка надёжности верификации подписи сетями квадратичных форм, нечёткими экстракторами и персептронами / П.С. Ложников, А.Е. Сулавко, А.В. Ерёменко, Д.А. Волков // Информационно-управляющие системы. – 2016. – № 5(84). – С. 73-85. – DOI: 10.15217/issn1684-8853.2016.5.73.
5. **Dodis, Y.** Fuzzy extractors: How to generate strong keys from biometrics and other noisy / Y. Dodis, L. Reyzin, A. Smith // International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT 2004). – 2004. – С. 523-540. – DOI: 10.1007/978-3-540-24676-3_31.
6. **Ахметов, Б.С.** Технология использования больших нейронных сетей для преобразования нечетких биометрических данных в код ключа доступа: Монография / Б.С. Ахметов, А.И. Иванов, В.А. Фунтиков, А.В. Безяев, Е.А. Малыгина. – Алматы: ТОО «Издательство LEM», 2014. – 144 с.
7. **Иванов, А.И.** Нейросетевая защита конфиденциальных биометрических образов гражданина и его личных криптографических ключей. Монография / А.И. Иванов. – Пенза: ПНИЭИ, 2014. – 57 с.
8. **Галушкин, А.И.** Синтез многослойных систем распознавания образов / А.И. Галушкин. – М.: «Энергия», 1974. – 368 с.
9. **Hinton, G.E.** Training products of experts by minimizing contrastive divergence. Neural Computation. – 2002. – Vol. 14, Issue 8. – P. 1771-1800. – DOI: 10.1162/089976602760128018.
10. **Hafemann, L.G.** Writer-independent feature learning for offline signature verification using deep convolutional neural networks / L.G. Hafemann, R. Sabourin, L.S. Oliveira // 2016 International Joint Conference on Neural Networks (IJCNN). – 2016. – P. 2576-2583. – DOI: 10.1109/IJCNN.2016.7727521.
11. **Колмогоров, А.Н.** О представлении непрерывных функций нескольких переменных в виде суперпозиции непрерывных функций одного переменного / А.Н. Колмогоров // Доклады АН СССР. – 1957.– Т. 114, № 5. – С. 953-956.
12. ГОСТ Р 52633.5-2011. Защита информации. Техника защиты информации. Автоматическое обучение нейросетевых преобразователей биометрия-код доступа. – М.: Стандартинформ, 2011. – 20 с.
13. **Иванов, А.И.** Нейросетевые алгоритмы биометрической идентификации личности / А.И. Иванов. – Серия: Нейрокомпьютеры и их применение. – Вып. 15. – М.: Радиотехника, 2004.– 144 с. – ISBN: 978-5-93108-048-2.
14. **Иванов, А.И.** Идентификация подлинности рукописных автографов сетями Байеса-Хэмминга и сетями квадратичных форм / А.И. Иванов, П.С. Ложников, Е.И. Качайкин // Вопросы защиты информации. – 2015. – № 2. – С. 28-34.
15. **Ложников, П.С.** Биометрическая идентификация рукописных образов с использованием корреляционного аналога правила Байеса / П.С. Ложников, А.И. Иванов, Е.И. Качайкин, А.Е. Сулавко // Вопросы защиты информации. – 2015. – № 3.– С. 48-54.
16. **Иванов, А.И.** Снижение размеров достаточной для обучения выборки за счёт симметризации корреляционных связей биометрических данных / А.И. Иванов, П.С. Ложников, Ю.И. Серикова // Кибернетика и системный анализ. – 2016. – Т. 52, № 3. – С. 49-56.
17. **Безяев, А.В.** Оптимизация структуры самокорректирующегося био-кода, хранящего синдромы ошибок в виде фрагментов хеш-функций / А.В. Безяев, А.И. Иванов, Ю.В. Фунтикова // Вестник УрФО. Безопасность в информационной сфере. – 2014. – № 3(13). – С. 4-13.

Сведения об авторах

Иванов Александр Иванович (Пенза, Россия) – доктор технических наук, начальник лаборатории биометрических и нейросетевых технологий АО «Пензенский научно-исследовательский электротехнический институт». E-mail: *ivan@pniei.penza.ru* .

Ложников Павел Сергеевич (Омск, Россия) – кандидат технических наук, заведующий кафедрой комплексной защиты информации ФГБОУ ВО ОмГТУ. E-mail: *lozhnikov@gmail.com* .

Сулавко Алексей Евгеньевич (Омск, Россия) – кандидат технических наук, старший преподаватель кафедры комплексной защиты информации ФГБОУ ВО. E-mail: *sulavich@mail.ru* .

Поступила в редакцию 29 мая 2017 г. Окончательный вариант – 21 августа 2017 г.

EVALUATION OF SIGNATURE VERIFICATION RELIABILITY BASED ON ARTIFICIAL NEURAL NETWORKS, BAYESIAN MULTIVARIATE FUNCTIONAL AND QUADRATIC FORMS

A.I. Ivanov[1], P.S. Lozhnikov[2] , A.E. Sulavko[2]
[1] Penza Scientific and Research Electrotechnical Institute, Penza, Russia,
[2] Omsk State Technical University, Omsk, Russia

Abstract

An experimental comparison of various functional neural networks for signature verification is performed. A signature database for the realization of the computing experiment is built. It is confirmed that up to a certain point, the increase of the decision rule dimension reduces the probability of signature verification error, with an increase in the number of neurons in the network reducing the number of errors. A higher-dimension multi-dimensional Bayes functional with stronger inter-feature correlation is found to perform better. The best result for the signature verification is obtained using networks of Bayesian multidimensional functional, with false acceptance rate of $FRR = 0.0288$ and false rejection rate of $FAR = 0.0232$.

Keywords: neural networks, network of quadratic forms, multi-dimensional Bayes functional, signature reproduction peculiarities, biometric features.

Citation: Ivanov AI, Lozhnikov PS, Sulavko AE. Evaluation of signature verification reliability based on artificial neural networks, Bayesian multivariate functional and quadratic forms. Computer Optics 2017; 41(5): 765-774. DOI: 10.18287/2412-6179-2017-41-5-765-774.

Acknowledgements: The work was partially funded (in the part of analysis of the shortcomings of deep artificial neural networks) by the Ministry of Education and Science of the Russian Federation under the state research contract (project No. 2.9314.2017/BC). The experimental part of the work was funded by the Russian Foundation for Basic Research (grant No. 16-07-01204).

References

[1] The Global State of Information Security® Survey 2016. PricewaterhouseCoopers. Source: ⟨http://www.pwc.com/gx/en/issues/cyber-security/information-security-survey/download. html⟩.

[2] Ivanov AI, Lozhnikov PS, Samotuga AE. A technology to form hybrid documents [In Russian]. Cybernetics and Systems Analysis 2014; 50(6): 152-156.

[3] GOST R 52633.0-2006. Information protection. Information protection technology. Requirements to the means of high-reliability biometric authentication [In Russian]. Moscow: "Standartinform" Publisher; 2006.

[4] Lozhnikov PS, Sulavko AE, Eremenko AV, Volkov DA. Experimental evaluation of reliability of signature verification by quadratic form networks, fuzzy extractors and perceptrons [In Russian]. Information and Control Systems 2016, 5(84): 73-85. DOI: 10.15217/issn1684-8853.2016.5.73.

[5] Dodis Y, Reyzin L, Smith A. Fuzzy extractors: How to generate strong keys from biometrics and other noisy. EUROCRYPT 2004: 523-540. DOI: 10.1007/978-3-540-24676-3_31.

[6] Ahmetov BS, Ivanov AI, Funtikov VA, Bezjaev AV, Malygina EA. Technology of large neural networks usage for fuzzy biometric data conversion to access key codes: monograph. Almaty, Kazakhstan: "LEM" Publisher; 2014.

[7] Ivanov AI. Neural network protection of confidential biometric data and private cryptographic keys: A monograph [In Russian]. Penza: "PNIEI" Publisher; 2014.

[8] Galushkin AI. Synthesis of multi-level systems for pattern recognition [In Russian]. Moscow: "Energija" Publisher; 1974.

[9] Hinton GE. Training products of experts by minimizing contrastive divergence. Neural Comput 2002; 14(8): 1771-1800. DOI: 10.1162/089976602760128018.

[10] Hafemann LG, Sabourin R, Oliveira LS. Writer-independent feature learning for offline signature verification using deep convolutional neural networks. IJCNN 2016: 2576-2583. DOI: 10.1109/IJCNN.2016.77275212016.

[11] Kolmogorov AN. On the representation of a multivariate continuous function as a superposition of monovariate continuous functions [In Russian]. Doklady Akademii Nauk SSSR 1957; 114(5): 953-956.

[12] GOST R 52633.5-2011. Information protection. Information protection technology. The neural net biometry-code converter automatic training [In Russian]. Moscow: "Standartinform" Publisher; 2011.

[13] Ivanov A.I. Neural network algorithms for biometric personal identification [In Russian]. Moscow: "Radiotehnika" Publisher; 2004. ISBN: 978-5-93108-048-2.

[14] Ivanov AI, Lozhnikov PS, Kachajkin EI. Verification of authenticity for handwritten signatures using Bayesian-Hamming networks and quadric form networks. Information Security Questions 2015; 2: 28-34.

[15] Lozhnikov PS, Ivanov AI, Kachajkin EI, Sulavko AE. Biometric identification of handwritten images via correlation analog of Bayes' rule [In Russian]. Information Security Questions 2015; 3: 48-54.

[16] Ivanov AI, Lozhnikov PS, Serikova JuI. Reducing the size of training-sufficient sampling due to symmetrization of correlation relationships of biometric data [In Russian]. Cybernetics and Systems Analysis 2016; 52(3): 49-56.

[17] Bezev AV, Ivanov AI, Funtikova JuV. Optimization of the structure self-correcting bio-code, storing syndromes error as fragments hash-functions [In Russian]. UrFR Newsletter. Information Security 2014; 3(13): 4-13.

Authors' information

Alexander I. Ivanov Doctor of Technical Sciences, Head of Biometric and Neural Network Technologies laboratory of Penza Scientific and Research Electrotechnical Institute E-mail: *ivan@pniei.penza.ru* .

Pavel S. Lozhnikov Candidate of Technical Sciences, Head of Comprehensive Information Protection department of Omsk State Technical University. E-mail: *lozhnikov@gmail.com* .

Alexey E. Sulavko Candidate of Technical Sciences, Senior Lecturer, of Complex Information Protection department of Omsk State Technical University E-mail: *sulavich@mail.ru* .

Received May 29, 2017. The final version – August 21, 2017.