УДК 004.93’1
doi:10.15217/issn1684-8853.2016.5.73

ЭКСПЕРИМЕНТАЛЬНАЯ ОЦЕНКА НАДЕЖНОСТИ ВЕРИФИКАЦИИ ПОДПИСИ СЕТЯМИ КВАДРАТИЧНЫХ ФОРМ, НЕЧЕТКИМИ ЭКСТРАКТОРАМИ И ПЕРСЕПТРОНАМИ

П. С. Ложников[а], *канд. техн. наук, доцент*
А. Е. Сулавко[а], *канд. техн. наук, старший преподаватель*
А. В. Еременко[б], *канд. техн. наук, доцент*
Д. А. Волков[а], *аспирант*
[а]*Омский государственный технический университет, Омск, РФ*
[б]*Омский университет путей сообщения, Омск, РФ*

Введение: *проблемы защиты информации с каждым годом становятся актуальней, поэтому требования к биометрическим системам ужесточаются. Цель работы: сравнить нечеткие экстракторы, нейросетевые преобразователи биометрия-код и сети квадратичных форм по надежности биометрической аутентификации на основе подписи субъекта.* ***Результаты:*** *проведен анализ научной литературы и серия вычислительных экспериментов на основе реальных биометрических данных. По результатам экспериментов нечеткие экстракторы значительно уступают другим системам по надежности аутентификации и длине ключа, сети Байеса — Пирсона — Хемминга показывают наилучший результат.* ***Практическая значимость:*** *полученные результаты будут интересны исследователям и разработчикам биометрических систем.*

Ключевые слова *— особенности воспроизведения подписи, биометрия, нечеткие экстракторы, искусственные нейронные сети, аутентификация.*

Введение

Проблемы защиты информации от несанкционированного доступа не теряют актуальности [1]. Одно из направлений по противодействию этому виду угроз — усовершенствование биометрических средств аутентификации. На данный момент идет «борьба за повышение» надежности биометрических систем с одновременным выполнением требований по защите биометрических эталонов субъектов, прописанных в ГОСТ Р 52633.0-2006 [4] (5.2, 5.3). Надежность определяется вероятностью ошибок 1-го и 2-го рода — ложного отказа в доступе «Своему» и ложного доступа «Чужого».

Статические образы (отпечатка пальца, сетчатки, радужки) не являются секретными, их можно скопировать, изготовив физический или цифровой муляж (для удаленной аутентификации). Поэтому усилия многих исследователей сконцентрированы на повышении надежности аутентификации по динамическим биометрическим признакам (особенностям воспроизведения рукописного или голосового образа и клавиатурного почерка). Для регистрации клавиатурного почерка можно разработать скрытый перехватчик на основе руткит-методик (обнаружить который крайне сложно [2]), голос может быть перехвачен посредством микрофона. В этом смысле лучше использовать параметры рукописных паролей. На настоящий момент динамические признаки дают более высокий процент ошибочных решений при аутентификации, чем статические. Но потенциал динамических образов значительно выше, так как они могут быть тайными (а их длина неограниченна [3]).

Существует несколько подходов к реализации методики принятия решений в биометрических системах с обеспечением защиты эталонных описаний образов субъектов [4]. Однако сопоставительные экспериментальные данные по их эффективности не нашли достаточного отражения в литературе. Настоящая работа посвящена актуальной научной проблеме: экспериментальной оценке надежности существующих методов биометрической аутентификации на основе особенностей воспроизведения рукописных образов с возможностью защиты биометрического эталона и некоторых вариантов модернизации данных методов.

Сравнение существующих подходов по данным научной литературы

Изначально сложилось два основных подхода к реализации связи «аутентификатор — субъект» с защитой биометрического эталона: нейросетевые преобразователи «биометрия-код» (НПБК) [4] и «нечеткие экстракторы» [5]. По определению, данному в монографии казахстанских и российских ученых [6], а также в ГОСТ Р 52633.0-2006 [4], «нейросетевой преобразователь “биометрия-код” — это заранее обученная искусственная нейронная сеть с большим числом входов и выходов,

преобразующая частично случайный вектор входных биометрических параметров "Свой" в однозначный код криптографического ключа (длинного пароля) и преобразующая любой иной случайный вектор входных данных в случайный выходной код». Таким образом, код доступа, получаемый из данных легального пользователя (выходной код «Свой»), должен быть фиксированным, а код из данных других субъектов (выходной код «Чужой» или все «Чужие») — случайной строкой бит. Основное отличие обозначенных методов от обычной биометрической аутентификации — это обезличивание эталонных описаний образов (отказ от необходимости хранить эталон либо хранение эталона в виде, не позволяющем восстановить исходные биометрические характеристики субъекта). Надежность системы аутентификации определяется вероятностью ошибок 1-го и 2-го рода — ложного отказа в доступе «Своему» и ложного доступа «Чужого».

Нейросетевые преобразователи «биометрия-код»

Сдерживающим фактором в применении нейронных сетей является сложный процесс их обучения. Малые нейронные сети быстро обучаются, но принимают низкокачественные решения. По мере увеличения размеров (количества слоев, нейронов и их входов) решения становятся более достоверными (на уровне людей-экспертов или лучше), но при этом растет сложность обучения нейросети, появляются проблемы «тупиков» и «зацикливания обучения», в результате этот процесс становится неприемлемо долгим либо неосуществимым [3, 7]. Для биометрии требуются сверхбыстрые алгоритмы обучения (выполняемые за несколько секунд на обычном персональном компьютере) [3]. Для данной цели не могут быть использованы итерационные алгоритмы, поскольку они теряют устойчивость при увеличении числа входов нейронов или при снижении качества биометрических данных [6]. Решение проблемы предложено в стандарте ГОСТ Р 52633.5-2011 [8]. Рекомендуется использовать прямое вычисление модулей весовых коэффициентов через математические ожидания и среднеквадратические отклонения биометрических параметров «Свой» и «Чужой». Благодаря этому процедуры обучения становятся рекордно быстрыми и устойчивыми [6]. Для обучения сети требуется не менее 21 образца данных «Свой» и 64 независимых образца данных «Чужой» (образцы от разных субъектов).

Другим сдерживающим фактором в использовании НПБК на практике является сложность тестирования их надежности [6]. Высоконадежные биометрические устройства с вероятностью ошибочных решений 10^{-12} и выше проще создать, чем доказательно проверить эту вероятность прямым численным экспериментом [6]. Для НПБК не годится упрощенная схема Бернулли [6], а для атак прямого подбора необходимы объемные базы данных биометрических признаков, собрать которые невозможно по причине нехватки населения Земли. Для тестирования предложены процедуры морфинга, определенные в ГОСТ Р 52633.2-2010, используя которые удается оценить «нано» и «пико» вероятности ошибок 2-го рода биометрической аутентификации на тестовых базах, состоящих из 10 000 естественных биометрических образов [6].

Особенностью НПБК является то, что для малых нейронных сетей слабые корреляционные связи между биометрическими параметрами слабо влияют на результирующую энтропию генерируемого кода, а для больших нейронных сетей ситуация становится обратной — из-за слабых корреляционных связей энтропия падает, что упрощает атаки перебора. Границей деления нейронных сетей на большие и малые являются 16 выходных разрядов [6].

Другой особенностью НПБК является процедура обогащения. Обогащение позволяет работать с «плохими биометрическими данными» и восстанавливать до 50 % ошибок исходных данных [9]. При высоком уровне первичного обогащения данных обыкновенные нейроны (персептроны) оказываются малоэффективными. Более эффективны искусственные нейроны с несколькими выходными дискретными состояниями [6]. Практика показала, что использование операции циклического сдвига при настройке формы нелинейного элемента нейрона не является оптимальной. Более качественные результаты получаются, если определенным участкам области значений сумматора нейрона (вне интервала «Свой») задавать выходные коды случайным образом. При таком способе усиливаются хеширующие свойства обученного нейрона по отношению к образам все «Чужие», нелинейные элементы с длительными монотонными участками хуже перемешивают данные [6]. В работе [7] предложено использовать трид-нейроны с двумя выходными состояниями, которые имеют два порога квантования. Использование трид-нейронов позволяет повысить длину генерируемого кода в два раза, а энтропию кодов — в полтора раза, если квантователь выходных значений не является монотонной дискретной функцией.

По требованиям ГОСТ Р 52633.0-2006 [4] при поступлении на вход НПБК образца данных «Чужой» вероятности значений «0» и «1» разрядов выходного кода должны быть равными (допускается разница в количестве различных значений разрядов не более 10 %). Для того чтобы поднять качество хеширования, могут быть использованы различные механизмы размножения ошибок, например, сложение по модулю 2 части выходного кода «Свой» от изолированного потока

нейронов и записанных в дискретной форме параметров обученной нейронной сети остальных нейронов (весовых коэффициентов нейронов и номеров связей между нейронами) [6]. Шифрование параметров нейронов на выходах других нейронов также предлагается использовать при запуске в недоверенной среде для защиты таблиц нейросетевых функционалов от анализа в целях восстановления эталона субъекта [6, 10]. Данный принцип защиты называется защищенным нейросетевым (биометрическим) контейнером [10]. Размер ключа выбирается по конструктивным особенностям и возможностям нейронной сети. Данная схема уязвима к атаке Г. Б. Маршалко, которая строится на наблюдении большого числа выходов у незащищенных нейронов [10]. Чтобы снизить эффективность таких атак на биометрию, следует отказаться от создания одного длинного ключа и использовать множество ключей увеличивающейся длины [6]. Тем не менее сегодня защищенные нейросетевые контейнеры являются наиболее эффективным средством хранения оцифрованной биометрии [10].

Нужно отметить, что длина эффективного кода (аутентификатора) зависит от количества информативных признаков, простое увеличение количества нейронов не ведет к аналогичному росту эффективного кода, так как энтропия генерируемого кода не соответствует его длине [10]. Вместе с тем для того чтобы снизить вероятность ошибок 2-го рода до уровня парольной защиты (~10^{-8}), необходимо использовать достаточно большое число выходов у НПБК.

Для обучения НПБК необходимо, чтобы биометрические данные имели закон распределения, близкий к нормальному, для контроля за этим используется критерий Пирсона, а также его модификации [11, 12].

Достоинством биометрических сетей является то, что биометрический шаблон человека не хранится более в памяти компьютера, вместо него хранятся весовые коэффициенты между нейронами (не существует эффективного способа восстановления параметров распределения биометрических признаков из данных нейросетевого биометрического контейнера) [1]. Защитные свойства усиливаются при использовании защищенных нейросетевых контейнеров. Обогащение данных нейронами является сильной стороной технологии по сравнению с квантованием «сырых» биометрических данных.

Нечеткие экстракторы

Данный подход активно развивается за рубежом и основан на использовании кодов, исправляющих ошибки, применяемых к «сырым», не обогащенным биометрическим данным для корректировки нестабильных бит генерируемого ключа. Известны схожие версии изложения данного подхода (многие из которых упоминаются и описываются в работах [13–16]): Fuzzy Vault («нечеткое хранилище») [17], Fuzzy Commitment [18] и т. д. Некоторые из них обладают бóльшим числом недостатков, чем классический «нечеткий экстрактор» (Fuzzy Extractor), который является общей схемой выработки ключевой последовательности, построенной на использовании классических самокорректирующих кодов. Далее объединим все указанные и аналогичные схемы общим названием — нечеткий экстрактор.

К принципиальным недостаткам нечетких экстракторов относятся:

1. Высокая избыточность классических самокорректирующих кодов, из-за которой длина генерируемого ключа оказывается низкой. К примеру, не существует кодов, способных исправлять 50 % ошибок, так как такие коды имеют огромную избыточность и пренебрежимо малую информационную часть [6, 10].

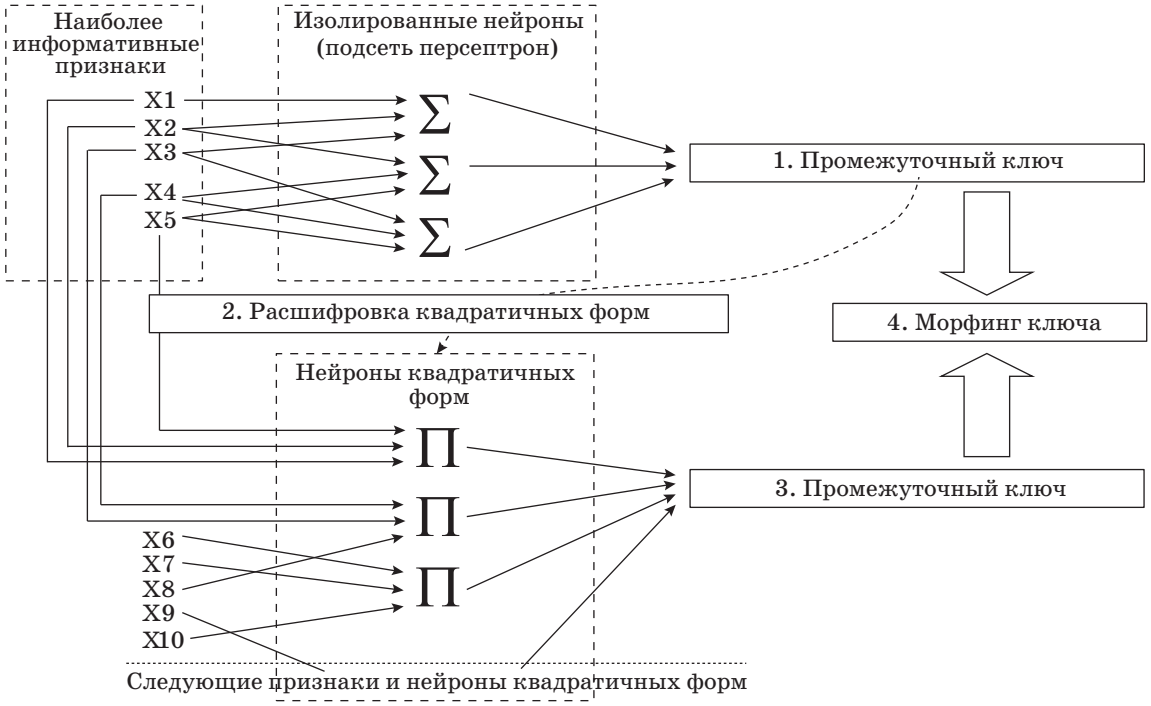
2. Уязвимости нечетких экстракторов [19], позволяющие ускорить перебор значений биометрических параметров в целях фальсификации ключа доступа. Считается, что наложение на биометрические данные гаммы в виде строки бит является надежной защитой для обеих составляющих только в случае равновероятной единичной ошибки в битовом представлении вектора биометрических признаков, чего на практике не наблюдается [19].

3. Нечеткие экстракторы квантуют «сырые» биометрические данные и не учитывают параметры распределения значений признаков, в результате они должны давать более высокий процент ошибок по сравнению с НПБК, которые в свою очередь располагают этими данными, кодируя их весовыми коэффициентами нейронов [6, 10, 19].

Для решения первой проблемы в работе [9] предложены коды, разработанные специально для биометрии. Они позволяют хранить синдромы ошибок отдельно от открытой строки в виде усеченной хеш-функции (последние 3 бита), поэтому извлекаемый из открытой строки ключ доступа будет длинней. В работе [20] показана связь эффективности коррекции ошибок с методами группирования битов с разной вероятностью единичной ошибки. Несмотря на предпринятые в данном направлении усилия, единого подхода для решения этого вопроса до сих пор не выработано. Поэтому вторая проблема экстракторов не считается решенной в полной мере. Третья проблема фактически не решается.

Сети квадратичных форм и модификация персептронов

В качестве альтернативы нейронным сетям по ГОСТ Р 52633.5-2011 [8] предлагается использовать сети квадратичных форм [21, 22] либо мо-



■ ***Рис. 1.*** Схема выработки ключа (аутентификатора) с использованием гибридной нейронной сети и принципа защищенного нейросетевого контейнера

дификации персептронов данного стандарта [7, 22], к которым относятся сети трид-нейронов [7] и нейроны с четной функцией двухстороннего квантования [22] (вместо нечетной ступенчатой квантующей функции). Функция [22] имеет два порога (правый и левый компаратор), при попадании в заданный интервал нейрон выдает значение, на которое настроен, в противном случае — обратное ему значение.

Основное отличие сети квадратичных форм заключается в строении искусственного нейрона. Классический нейрон и нейрон стандарта ГОСТ Р 52633.5-2011 [8] состоит из сумматора и линейной (нелинейной) пороговой функции на выходе нейрона, которая трансформирует полученную сумму обработанных параметров от каждого синапса (входа нейрона) в бинарное значение «0» или «1» [3, 6, 10]. Нейрон квадратичной формы может быть основан на метрике Евклида, Пирсона, Махаланобиса и др. [3]. К преимуществам квадратичных форм можно отнести отсутствие необходимости обучения на образцах «Чужой» и возможность нелинейного разделения собственных областей эталонов в пространстве признаков [3] (персептрон осуществляет линейное разделение). Очевидным недостатком является необходимость хранения параметров законов распределения признаков.

Проблема хранения эталона субъекта может быть решена по принципу защищенного нейросетевого контейнера [6, 10]. В настоящей работе для этого предлагается построить гибридную сеть из обычных (или модифицированных) нейронов и нейронов квадратичных форм. Параметры нейронов квадратичных форм шифруются на выходах изолированных нейронов подсети персептронов. Этот принцип иллюстрируется на рис. 1. Необходимо подготовить такие изолированные нейроны, на входы которых будут подаваться значения наиболее информативных признаков. При верной выдаче фрагмента ключа изолированными нейронами параметры нейронов квадратичных форм будут расшифрованы правильно. В результате будет формироваться оставшаяся часть ключа. В противном случае сеть должна генерировать случайный шум, так как расшифрованные значения весовых коэффициентов будут некорректны (либо не будут соответствовать эталону субъекта). Можно определить несколько потоков изолированных нейронов, чтобы шифровать данные многократно, каждый раз осуществляя морфинг нового промежуточного ключа на основе предыдущего и генерируемого очередным потоком, что усилит защиту весовых коэффициентов [6, 10]. Однако данный вопрос выходит за рамки задач, поставленных в статье.

Достоинства и недостатки существующих подходов

Требования к нейросетевым преобразователям «биометрия-код» изложены в семействе отечественных стандартов ГОСТ Р 52633, число которых существенно превышает число за-

■ ***Таблица 1***. Преимущества и недостатки преобразователей «биометрия-код»

Подход	Преимущества	Недостатки
Персептроны ГОСТ Р 52633.5-2011 и их модификации	1. Обогащает данные 2. Хорошо стандартизован 3. Маскирует биометрический эталон 4. Возможность создания защищенного нейросетевого контейнера [10]	Требуется обучать сеть на образцах данных «Чужой» (других субъектов)
Нечеткий экстрактор	1. Не требуется обучать сеть на образцах данных «Чужой» (образцах других субъектов) 2. Простота реализации на практике	1. Не учитывает параметры распределения признаков 2. Помехоустойчивые коды крайне избыточны, длина ключа оказывается низкой 3. Возможно ускорить перебор биометрических данных для фальсификации ключа [19]
Сети квадратичных форм	1. Не требуется обучать сеть на образцах данных «Чужой» 2. Обогащает данные 3. Возможность создания защищенного нейросетевого контейнера [10]	Возникает необходимость хранить параметры распределения значений признаков

рубежных аналогичных стандартов для нечетких экстракторов (ISO/IEC 24745:2011, ISO/IEC 24761:2009, ISO/IEC 19792:2009) [6], т. е. данный подход лучше стандартизован. Но каждый из рассмотренных подходов обладает как преимуществами, так и недостатками (табл. 1).

Экспериментальное сравнение существующих подходов

Для сравнения описанных подходов допустимо использовать любой рукописный образ. Личный автограф не является секретным, но очевидно является наиболее стабильным рукописным образом. Поэтому для проведения опытов решено использовать подпись. В эксперименте участвовало 65 субъектов.

Используемое пространство признаков

Для ввода подписей в настоящем исследовании испытуемые пользовались графическим планшетом фирмы Wacom. Подпись состоит из функций положения пера на планшете $x(t)$, $y(t)$ и давления пера на планшет $p(t)$, где t — время в дискретной форме. Будем обозначать значения этих функций через x_i, y_i, p_i. Необходимо определить признаки — величины, характеризующие владельца подписи. Далее использовались признаки из работ [23, 24].

Образцы подписи отличаются по продолжительности (количеству отсчетов). Первоначально необходимо привести их к единой продолжительности, выполнив операцию нормирования, состоящую из следующих этапов:

1) исключаются все отчеты с нулевым давлением в начале и конце подписи;

2) производится одномерное преобразование Фурье для $x(t)$, $y(t)$ и $p(t)$;

3) производится обратное преобразование Фурье для указанных функций с учетом того, что размерность на выходе должна соответствовать числу, которое является ближайшим меньшим кратным степени 2.

Часть пространства признаков формировалась посредством построения матрицы расстояний между отчетами подписи. Элементы r_{ij} (расстояние между i-й и j-й координатами) матрицы в 3-мерном пространстве (давление — третье измерение) вычисляются по формуле

$$r_{ij} = \sqrt{(x_i - x_j)^2 + (y_i - y_j)^2 + (p_i - p_j)^2}. \qquad (1)$$

Аналогичным образом вычисляется матрица расстояний в 2-мерном пространстве (без учета давления).

Поскольку при расчете получается слишком много элементов, что требует слишком высоких вычислительных ресурсов, то необходимо производить вычисления расстояний с некоторым шагом. Далее производится нормирование полученной матрицы по длине подписи: $r'_{ij} = r_{ij}/r_{12} + r_{23} + \ldots + r_{(n-1)n}$. Нормированные элементы r'_{ij} полученной матрицы являются биометрическими признаками.

Вычисляются некоторые признаки, характеризующие внешний вид подписи:

1) отношение длины подписи к ее ширине;

2) центр подписи, описываемый координатами C_X, C_Y, C_P;

3) угол наклона подписи. Под углом подписи понимается косинус среднего угла наклона ломаной траектории подписи к оси абсцисс:

$$\theta = \frac{1}{N-1}\sum_{i=1}^{N}\frac{x_{i+1} - x_i}{\sqrt{(x_{i+1} - x_i)^2 + (y_{i+1} - y_i)^2}};$$

4) угол наклона между центрами половин подписи. После того как был найден центр подписи, разобьем множество $(X, Y, Z) = \{(x_i, y_i, p_i)\}$ на два подмножества $L = \{(x_i, y_i, p_i) | x_i \le C_X\ C_X\}$ и $R = \{(x_i, y_i, p_i) | x_i > C_X\}$ и найдем центры этих подмножеств:

$$C_{X_L} = \frac{1}{|L|}\sum_{x_i \in L}^{N} x_i,\ C_{Y_L} = \frac{1}{|L|}\sum_{y_i \in L}^{N} y_i,$$

$$C_{P_L} = \frac{1}{|L|}\sum_{p_i \in L}^{N} p_i;$$

$$C_{X_R} = \frac{1}{|R|}\sum_{x_i \in R}^{N} x_i,\ C_{Y_R} = \frac{1}{|R|}\sum_{y_i \in R}^{N} y_i,$$

$$C_{P_R} = \frac{1}{|R|}\sum_{p_i \in R}^{N} p_i.$$

Следующая категория признаков основана на использовании преобразования Фурье. Функции, которые подвергаются разложению по формуле (2): $p(t)$ на планшет и функция скорости пера на планшете $v(t)$, значения которой вычисляются по формуле (3). При использовании $v(t)$ исчезает зависимость от того, под каким углом расположен планшет относительно руки подписанта. Можно воспользоваться быстрым или обычным дискретным преобразованием Фурье. В отличие от дискретного, которое имеет сложность порядка $O(N^2)$, быстрое преобразование Фурье имеет сложность $O(N\log_2 N)$.

$$X_k = \sum_{i=0}^{N-1} x_i e^{\frac{-j2\pi ki}{N}}, \qquad (2)$$

где X_k — k-я гармоника в комплексной форме $\mathrm{Re}_k + j\mathrm{Im}_k$; x_i — i-е значение функции; N — количество отсчетов в дискретном сигнале. Исходный дискретный сигнал представляется в виде суммы функций:

$$f(t_i) = \sum_{k=0}^{N-1}\left[\frac{\mathrm{Re}_k}{N}\cos\left(\frac{2\pi k t_i}{T}\right) - \frac{\mathrm{Im}_k}{N}\sin\left(\frac{2\pi k t_i}{T}\right)\right] =$$

$$= \sum_{k=0}^{N-1} A_k \cos\left(2\pi t_n / T_k + \varphi_k\right) =$$

$$= \sum_{k=0}^{N-1} A_k \cos\left(2\pi t_i v_k + \varphi_k\right) = \sum_{k=0}^{N-1} G_k(t_i),$$

$$v_i = \sqrt{(x_{i+1} - x_i)^2 + (y_{i+1} - y_i)^2}. \qquad (3)$$

Далее будем функцию $G_k(t) = A_k \cos\frac{2\pi t_n}{T_k + \varphi_k}$ называть k-й гармоникой. Амплитуды вычисляются в соответствии с формулой

$$A_k = \frac{1}{N}\sqrt{\mathrm{Re}_k^2 + \mathrm{Im}_k^2}. \qquad (4)$$

Далее производится расчет энергии функции по формуле

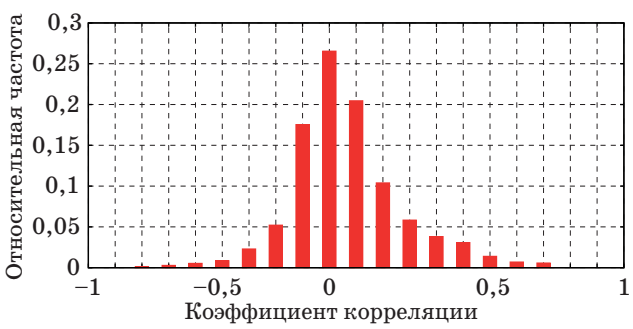
$$E_p = \int_{-\infty}^{\infty} A^2(t)\mathrm{d}t. \qquad (5)$$

На следующем шаге производится деление амплитуды каждой гармоники на значение энергии сигнала. Эта операция называется нормированием амплитуд по энергии и осуществляется в целях приведения различных реализаций подписи к одному масштабу. Решено использовать 16 нормированных амплитуд первых наиболее низкочастотных гармоник функции давления и функции скорости пера на планшете в качестве признаков по аналогии с работой [23].

Помимо описанных характеристик признаками в настоящей работе являются коэффициенты парной корреляции между функциями $x(t)$, $y(t)$ и $p(t)$ (и их производными). Установлено, что данные коэффициенты корреляции для каждого рукописного образа подписи субъекта близки по значениям и более существенно различаются для рукописных образов подписей различных субъектов [25]. Все указанные признаки имеют распределение значений, близкое к нормальному, что проверялось критерием хи-квадрат Пирсона. Общее число признаков 236. На рис. 2 представлена гистограмма относительных частот коэффициентов парной корреляции между сечениями признаков, полученных при статистической обработке всех имеющихся на момент проведения эксперимента подписей.

Модель нечеткого экстрактора

Для выработки ключа-аутентификатора нечетким экстрактором необходимы биометрические данные и дополнительная информация, хранящаяся на общедоступном сервере (носителе), из которой нельзя восстановить эталон (не существует простого способа это сделать). Данная информация называется открытой строкой. Сначала генерируется случайная равномерно распределенная битовая последовательность,

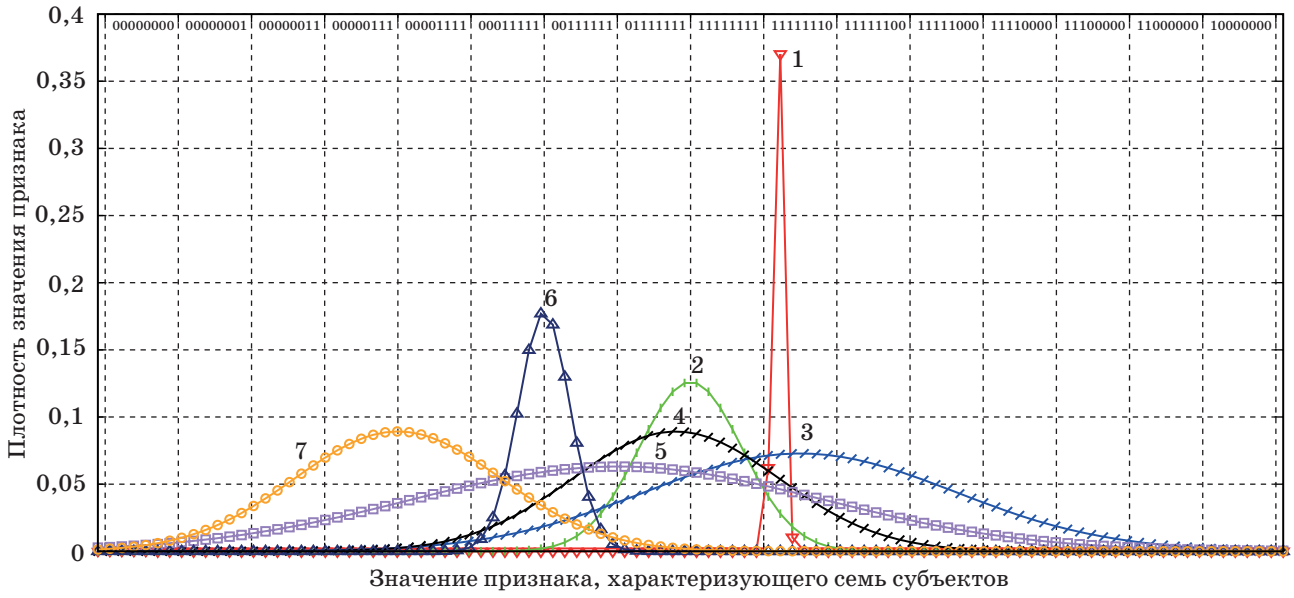


■ ***Рис. 2.*** Распределение коэффициентов парной корреляции между признаками по всем реализациям подписей всех испытуемых

которая является ключом. Далее осуществляется помехоустойчивое кодирование ключа доступа (к битовой последовательности добавляются синдромы ошибок помехоустойчивых кодов). На полученную избыточную строку накладывается гамма в виде битового представления эталонных биометрических данных (обычно берется вектор средних значений признаков). На выходе получается открытая строка, которую можно хранить на общедоступном сервере [5]. Для получения ключа субъект вводит новую реализацию признаков, которая «вычитается» от открытой строки, к результату этой операции применяются корректирующие коды (Адамара, Хемминга, Рида — Соломона и др.) [26]. Если расстояние Хемминга между введенным вектором признаков и эталонным вектором (который накладывался на избыточную строку) не превышает исправляющей способности кода, то после декодирования будет восстановлен исходный ключ доступа, в противном случае ключ будет другой. Длина ключа будет тем меньше, чем больше исправляющая способность кода.

В настоящем исследовании решено сравнить экстракторы на базе кодов Адамара и Рида — Соломона. Эквидистантные коды Адамара, обладая большим кодовым расстоянием, позволяют исправить и большое количество ошибок, зависящее от размера блока. Достоинством кодов Адамара является сравнительно высокая скорость работы. Коды БХЧ (Боуза — Чоудхури — Хоквингема) — это широкий класс циклических кодов, которые отличаются возможностью установки определенных корректирующих свойств. Широко используемым подмножеством кодов БЧХ являются коды Рида — Соломона. Это такие коды БЧХ, у которых мультипликативный порядок алфавита символов кодового слова делится на длину кода. Согласно теореме о границе Рейгера, коды Рида — Соломона являются оптимальными с точки зрения соотношения длины пакета и возможности исправления ошибок — используя $2t$ дополнительных проверочных символов исправляется t ошибок (и менее) [26]. Код Рида — Соломона является одним из наиболее мощных кодов, исправляющих групповые ошибки [26].

На эффективность нечеткого экстрактора влияет способ предварительного квантования «сырых» биометрических данных. В рамках эксперимента решено дискретизировать значения признака в соответствии с преобразованием $y = f(x)$, где x — значение признака, а y принадлежит множеству {0, 1, 3, 7, 15, 31, 63, 127, 255, 254, 252, 248, 240, 224, 192, 128}. Значения y представляются в двоичном виде. Суть операции преобразования иллюстрирует рис. 3. Данное преобразование существенно уменьшает количество единичных ошибок на этапе квантования, что сказывается на вероятностях ошибок 1-го и 2-го рода (они также снижаются). Кроме того, возрастает длина генерируемого ключа. Однако энтропия квантованных данных сильно падает, что, конечно, отрицательно сказывается на защитных свойствах экстрактора (ключ и биометрию субъекта более нельзя считать надежно защищенной, если ее хранить в открытой строке). Также этот способ требует знания границ области значений признаков, т. е. экстрактор нужно обучить на образцах данных «Чужой», следовательно, одно из преимуществ экстрактора исчезает (см. табл. 1). Но даже при таком способе квантования нечеткий экстрактор работает хуже нейронных сетей,



■ ***Рис. 3.*** Квантование «сырых» биометрических данных

как можно убедиться далее. Более «честным» способом квантования является квантование данных, предложенное в работах [23, 27]. Но при таком способе в описанном пространстве признаков и при увеличении количества испытуемых до 65 (в работах [23, 27] оценки ошибок носили предварительный характер, надежность оценивалась на малых выборках и малом количестве испытуемых — 12–14) ошибки выработки ключа оказываются значительны (сумма ошибок 1-го и 2-го рода превышает 0,5). В настоящем исследовании предлагается модификация нечеткого экстрактора с оценкой стабильности битового представления признаков по формуле [8, 19]

$$\omega_i = 2 \cdot |0{,}5 - P_{0,i}| = 2 \cdot |0{,}5 - P_{1,i}|, \qquad (6)$$

где $P_{0,i}$ — вероятность (относительная частота) появления нуля в i-м разряде кода; $P_{1,i}$ — вероятность (относительная частота) появления единицы в i-м разряде кода.

Для каждого субъекта выбирается определенное количество признаков, для которых произведения вычисляемых по формуле (6) величин будет наивысшим.

При использовании описанной модификации нужно хранить дополнительную информацию о номерах стабильных признаков. Для усиления защитных свойств экстрактора данную информацию целесообразно держать в секрете, т. е. требуется отдельный сервер или носитель. Реализацию такого экстрактора нельзя назвать простой, т. е. этим нивелируется одно из преимуществ подхода (см. табл. 1). Но вероятность ошибок при этом снижается.

Модель нейронной сети

В ГОСТ Р 52633.5-2011 [8] рекомендуется использовать однослойные или двухслойные нейронные сети (сети с большим количеством слоев являются избыточными, и для их применения необходимо специальное обоснование [6]). Первый слой осуществляет обогащение данных, второй играет роль кодов, исправляющих ошибки [8]. Алгоритм из ГОСТ Р 52633.5-2011 служит для послойного обучения сети нейронов: сначала осуществляется обучение первого слоя, далее эти же обучающие данные подаются на вход второго слоя сети, и вычисляются весовые коэффициенты нейронов второго слоя. Модули весов нейронов вычисляются детерминированно по нижеприведенным формулам (7) и (8) [8]

$$\mu_i = |E_{\text{ч}}(x_i) - E_{\text{с}}(x_i)|/\sigma_{\text{ч}}(x_i) \cdot \sigma_{\text{с}}(x_i), \qquad (7)$$

где $E_{\text{с}}(x_i)$ — математическое ожидание (среднее значение) значений признака для образа «Свой»; $\sigma_{\text{с}}(x_i)$ — среднеквадратичное отклонение значений признака для образа «Свой»; $E_{\text{ч}}(x_i)$ и $\sigma_{\text{ч}}(x_i)$ — аналогичные показатели для образа «Чужой». Знак весового коэффициента при условии, что нейрон должен выдавать единицу («1»), выбирается исходя из правила: «+», если $E_{\text{ч}}(x_i) < E_{\text{с}}(x_i)$, иначе «–». Если нейрон должен выдавать ноль («0»), знаки весовых коэффициентов инвертируются:

$$\mu_i = a_2\omega_i/E(\omega_i), \qquad (8)$$

где a_2 — стабилизирующий коэффициент для нейронов второго слоя, экспериментально подбираемый для каждой задачи выработки ключа; ω_i — показатель стабильности i-го разряда выходного кода нейронов первого слоя, вычисляемый по формуле (6) [8, 19]; $E(\omega_i)$ — математическое ожидание (среднее значение) показателей стабильности разрядов выходного кода нейронов первого слоя.

Алгоритм обучения позволяет настроить сеть на выдачу заданного ключа и случайной битовой последовательности при поступлении образа неизвестного пользователя.

При использовании второго слоя необходимо перейти от промежуточных кодов «0» и «1» к эквивалентным «–1» и «1». Число входов нейронов второго слоя рекомендуется выбирать от 0,2 до 0,8 от числа нейронов первого слоя. Рекомендации по выбору количества нейронов первого и второго слоя аналогичные и описаны в стандарте [8]. Связи нейронов первого слоя с нейронами второго слоя задаются случайно. Обработчики признаков связывают с нейронами первого слоя сначала последовательно, а при превышении номера нейрона над числом признаков — случайно. Далее осуществляется корректировка знаков весовых коэффициентов, которая носит эмпирический характер, с целью добиться желаемой вероятности ошибок аутентификации [8]. Выход сумматора нейрона любого слоя на этапе принятия решений определяется по формуле

$$y = \sum_{i=1}^{m} \mu_i v_i + \mu_0, \qquad (9)$$

где v_i — i-й вход нейрона; m — число входов; μ_i — весовой коэффициент i-го входа; μ_0 — нулевой вес, отвечающий за переключатель квантования нейрона.

Модели сетей квадратичных форм

В настоящей работе проверяется три модели сетей квадратичных форм на основе соответствующих мер близости: Пирсона, Байеса — Пирсона и Евклида. Метрика Пирсона заключается в получении интегральной оценки близости (расстояния) входного образца к эталону образа по формуле

$$\chi = \sum_{i=1}^{m} \frac{(E(v_i) - v_i)^2}{\sigma(v_i)^2}, \qquad (10)$$

где v_i — i-й вход нейрона; $E(v_i)$ — математическое ожидание (среднее значение) i-го входа нейрона; $\sigma(v_i)$ — среднеквадратичное отклонение i-го входа нейрона.

Данная метрика не учитывает корреляционных связей между признаками образа, поэтому с ростом корреляционных связей ее мощность падает [21]. В этом случае рекомендуется пользоваться метрикой Байеса — Пирсона [21], рассчитываемой по формуле

$$\chi = \sum_{j=1}^{m}\sum_{i=1}^{m}\left|\frac{|E(v_i)-v_i|}{\sigma(v_i)} - \frac{|E(v_j)-v_j|}{\sigma(v_j)}\right|. \qquad (11)$$

Метрика Байеса — Пирсона [21] не содержит в явной форме вычислительных операций с коэффициентами корреляции, однако коэффициенты многомерной корреляции биометрических данных сильно влияют на нее [21]. Таким образом, данная метрика позволяет определять близость образца не только к эталону образа, но и близость к эталону корреляционных связей образа. Следовательно, эта метрика должна лучше работать в пространстве сильно коррелирующих признаков, чем метрика Пирсона.

Последней рассматриваемой квадратичной формой является метрика Евклида, вычисляемая по формуле

$$\varepsilon = \sqrt{\sum_{i=1}^{m}\left(E(v_i)-v_i\right)^2}. \qquad (12)$$

Данная метрика является более слабой, так как не учитывает среднеквадратичное отклонение биометрического параметра.

Сеть квадратичных форм можно реализовать с одним слоем нейронов или двумя слоями нейронов. Первый слой состоит из нейронов, рассчитывающих выход по одной из указанных выше формул, от этого зависит тип сети: Пирсона — Хемминга, Байеса — Пирсона — Хемминга, Евклида — Хемминга (могут существовать и другие виды нейронов на базе иных квадратичных форм), либо это гибридная сеть, если она состоит из различных типов нейронов (такой вариант в рамках статьи не рассматривается). Полученное значение далее сравнивается с пороговым. Для каждого нейрона имеется свое оптимальное пороговое значение, которое подбирается эмпирически, исходя из произведения $\theta = \chi_{max} a_1$, где χ_{max} — максимальное значение квадратичной формы при поступлении на вход обучающих примеров образа «Свой»; a_1 — стабилизирующий коэффициент, экспериментально подбираемый для каждого пространства признаков. Далее при превышении порога нейрон выдает единицу («1»), иначе ноль («0»). При необходимости настройки на нужный выходной ключ нейрон можно перепрограммировать, инвертировав данные выходные значения. Флаг инверсии будет также являться параметром нейрона наряду с параметрами распределения признаков. Ввиду того, что нейрон сравнивает вычисляемую величину с пороговым значением и на выходе выдает бинарное значение, квадратичные формы называют не только по имени метрики, но и по имени Хемминга.

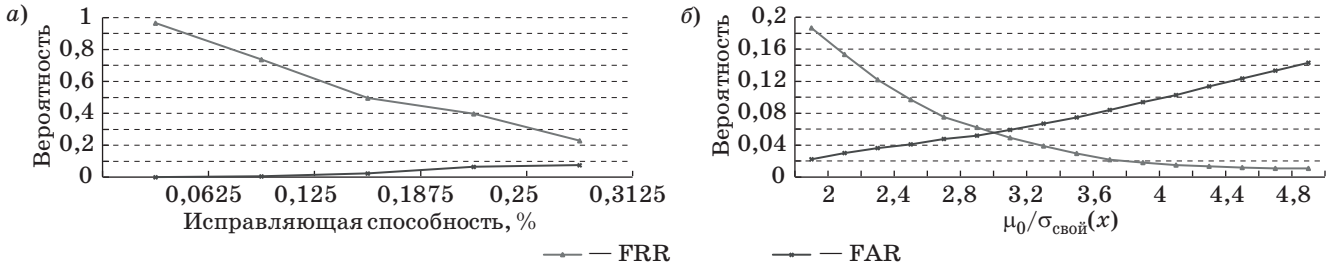
Второй слой нейронной сети можно полностью скопировать из стандарта ГОСТ Р 52633.5-2011 [8]. Второй слой играет роль кодов, исправляющих ошибки, его можно применить к любой нейросети, будь то сеть квадратичных форм, персептрон или его модификация. В качестве альтернативы второго слоя можно применить схемы [13] восстановления ошибочных бит ключа. В рамках данной работы второй слой квадратичных форм не рассматривается.

Результаты проведенного эксперимента

Проведено натурное моделирование (вычислительный эксперимент с реальными биометрическими данными субъектов, как при натурном, только информация подавалась на вход алгоритмов в автоматическом режиме). Каждым испытуемым было введено не менее 50 образцов подписи. Часть этих данных использовалась для обучения, остальные — для экспериментальной оценки надежности аутентификации (выработки ключа доступа). Количество образцов обучающей выборки решено сделать идентичным для нейронных сетей, сетей квадратичных форм и нечетких экстракторов: 21 реализация образа «Свой» и 64 реализации образа «Чужой» для персептронов (по одной реализации на каждого другого испытуемого). Вероятности ошибок 1-го и 2-го рода подсчитывались следующим образом: $FRR = er_1/ex_1$, $FAR = er_2/ex_2$, где er — количество ошибок соответствующего рода, ex — количество опытов для выявления ошибки соответствующего рода. Также подсчитывалась сумма ошибок 1-го и 2-го рода *ErrorRate* (ER) как площадь пересечения функций плотностей вероятности расстояний Хемминга от генерируемых кодов реализациями образов «Свой» до ожидаемого (идеального) кода и от генерируемых кодов реализациями образов «Чужой». Указанные плотности аппроксимировались нормальным законом распределения для кодов «Чужой» и бета-распределением для кодов «Свой» [6, 10]. Оптимальным размером блока для кодов Адамара является 6 бит, так как при этом значении достигается наименьший процент ошибок. Коды Рида — Соломона целесообразно использовать с максимально возможной исправляющей способностью (рис. 4, *а*, *б*). Тестирование нейронных сетей

будет проводиться без построения защищенного нейросетевого контейнера. Данное требование формулировалось в работах [4, 6] по отношению к стандартизованным персептронам. Лучшие результаты (по наименьшей сумме FFR и FAR) проведенного натурного моделирования приведены в табл. 2.

Получаемая длина ключа завышена (энтропия вырабатываемого кода не соответствует его длине), в особенности у экстракторов, так как используемый способ квантования дает низкую энтропию биокода, при иной методике квантования показатели FRR, FAR и ER для нечетких экстракторов становятся в разы выше.



■ ***Рис. 4.*** Вероятности ошибок выработки ключа нечетким экстрактором на основе кодов Рида — Соломона (*а*) и нейронной сетью по ГОСТ Р52633.5-2011 с одним слоем (*б*) при использовании 236 признаков

■ ***Таблица 2.*** Основные результаты эксперимента

Сравнение НПБК с нечеткими экстракторами				
Способ, количество признаков	FRR	FAR	ER	Длина ключа, бит
Экстрактор (коды Адамара), 228	0,148	0,05	0,075	304
Экстрактор (коды Рида — Соломона), 236	0,228	0,076	0,308	360
Экстрактор (коды Рида — Соломона), 90	0,191	0,033	0,21	150
НПБК (1 слой), 236	0,029	0,074	0,068	236
НПБК (2 слоя), 236	0,045	0,051	0,056	236
Сравнение НПБК с сетями квадратичных форм				
Способ (236 признаков)	FRR	FAR	ER	Число входов нейрона
Сеть Пирсона — Хемминга	0,044	0,046	0,057	59
Сеть Байеса — Пирсона — Хемминга	0,045	0,039	0,056	59
Сеть Евклида — Хемминга	0,097	0,118	0,302	59
Персептрон ГОСТ Р 52633.52011	0,028	0,076	0,067	59
Персептрон (2 компаратора)	0,029	0,077	0,064	59
Персептрон (третичное квантование)	0,033	0,079	0,068	59
Сеть Пирсона — Хемминга	0,041	0,054	0,058	118
Сеть Байеса — Пирсона — Хемминга	0,045	0,051	0,060	118
Сеть Евклида — Хемминга	0,084	0,155	0,314	118
Персептрон ГОСТ Р 52633.5-2011	0,029	0,074	0,068	118
Персептрон (2 компаратора)	0,027	0,077	0,064	118
Персептрон (третичное квантование)	0,035	0,080	0,068	118
Сеть Пирсона — Хемминга	0,032	0,066	0,059	177
Сеть Байеса — Пирсона — Хемминга	0,036	0,064	0,062	177
Сеть Евклида — Хемминга	0,066	0,211	0,320	177
Персептрон ГОСТ Р 52633.5-2011	0,02	0,1	0,067	177
Персептрон (2 компаратора)	0,017	0,109	0,066	177
Персептрон (третичное квантование)	0,021	0,11	0,068	177

Заключение

По результатам проведенного эксперимента нечеткие экстракторы уступают в надежности аутентификации нейросетевым преобразователям «биометрия-код», выполненным по ГОСТ Р 52633.5-2011. Защитные свойства нечетких экстракторов также хуже и имеют большее число недостатков. Этот вывод подтверждается данными из научной литературы. По данным экспериментальных оценок сети квадратичных форм Пирсона — Хемминга и Байеса — Пирсона — Хемминга превосходят персептроны из ГОСТ Р 52633.5-2011 по надежности выработки ключа доступа. Сеть Евклида — Хемминга работает значительно хуже других сетей квадратичных форм. Замена нечетной ступенчатой квантующей функции персептрона из ГОСТ Р 52633.5-2011 на четную функцию двухстороннего ограничения не дала заметного повышения эффективности работы. Аналогичные результаты получены и при использовании трид-нейронов. Сеть Пирсона — Хемминга при увеличении входов нейронов работает лучше сети Байеса — Пирсона — Хемминга, однако при уменьшении количества входов сеть Байеса — Пирсона — Хемминга становится более эффективной, чем сеть Пирсона — Хемминга. Наилучший результат в рамках эксперимента получен на основе сети Байеса — Пирсона — Хемминга с 59 входами каждого нейрона при 236 признаках, вероятности ошибок составили: FRR = 0,045, FAR = 0,039, сумма ошибок 1-го и 2-го рода была наименьшей — 0,084.

Работа выполнена при финансовой поддержке РФФИ (грант № 16-07-01204).

Литература

1. The Global State of Information Security® Survey 2016. PricewaterhouseCoopers. http://www.pwc.com/gx/en/issues/cyber-security/information-security-survey/download.html (дата обращения: 27.06.2016).
2. **Хогланд Г.** Руткиты: внедрение в ядро Windows. — СПб.: Питер, 2007. — 285 с.
3. **Иванов А. И.** Нейросетевые алгоритмы биометрической идентификации личности / под ред. А. И. Галушкина. –– М.: Радиотехника, 2004. — 144 с. — (Научная серия «Нейрокомпьютеры и их применение». № 15).
4. ГОСТ Р 52633.0-2006. Защита информации. Техника защиты информации. Требования к средствам высоконадежной биометрической аутентификации. — М.: Стандартинформ, 2006. — 24 с.
5. **Dodis Y., Reyzin L., Smith A.** Fuzzy Extractors: How to Generate Strong Keys from Biometrics and Other Noisy// EUROCRYPT. April 13, 2004. P. 523–540.
6. **Ахметов Б. С.** и др. Технология использования больших нейронных сетей для преобразования нечетких биометрических данных в код ключа доступа / Б. С. Ахметов, А. И. Иванов, В. А. Фунтиков, А. В. Безяев, Е. А. Малыгина: монография. — Алматы: Издательство LEM, 2014. — 144 с.
7. **Волчихин В. И.** и др. 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 // Изв. высших учебных заведений. Поволжский регион. 2013. № 4(28). С. 86–96.
8. ГОСТ Р52633.5-2011. Защита информации. Техника защиты информации. Автоматическое обучение нейросетевых преобразователей биометрия-код доступа. — М.: Стандартинформ, 2011. — 20 с.
9. **Безяев А. В., Иванов А. И., Фунтикова Ю. В.** Оптимизация структуры самокорректирующегося биокода, хранящего синдромы ошибок в виде фрагментов хеш-функций // Вестник УрФО. Безопасность в информационной сфере. 2014. № 3(13). С. 4–13.
10. **Иванов А. И.** Нейросетевая защита конфиденциальных биометрических образов гражданина и его личных криптографических ключей: монография. —Пенза: ПНИЭИ, 2014. — 57 с.
11. **Ахметов Б. С., Иванов А. И., Серикова Н. И.** Алгоритм искусственного повышения числа степеней свободы при анализе биометрических данных по критерию согласия хи-квадрат // Вестник Национальной академии наук Республики Казахстан. 2014. № 5. С. 28.
12. **Иванов А. И.** и др. Сравнение мощности хи-квадрат критерия и критерия Крамера — фон Мизеса для малых тестовых выборок биометрических данных/ А. И. Иванов, А. И. Газин, С. Е. Вятчанин, К. А. Перфилов // Надежность и качество сложных систем. 2016. № 2(14). С. 21–28.
13. **Васильев В. И.** Интеллектуальные системы защиты информации: учеб. пособие. 2-е изд., испр. и доп. — М.: Машиностроение, 2012. — 199 с.
14. **Busch C.** Biometrics and Security / NIS Net – Winter School FINSE. April 27, 2010. http://www.nisnet, no/filer/Finse 10/Biometrics_and_ Security_ Busch.pdf (дата обращения: 27.06.2016).
15. **Cavoukian A., Stoianov A.** Biometric Encryption Chapter from the Encyclopedia of Biometrics. http://www.ipc.on.ca/images/Resours/bio-encrypt-chp.pdf (дата обращения: 27.06.2016).
16. **Куликова О. В.** Биометрические криптографические системы и их применение. http://www.pvti.ru/data/file/bit/bit_3_2009_10.pdf (дата обращения: 27.06.2016).
17. **Juels A., Sudan M.** A Fuzzy Vault Scheme // Designs, Codes and Cryptography. February 2006. Vol. 38. Iss. 2. P. 237–257. doi:10.1007/s10623-005-6343-z

18. **Juels A., Wattenberg M.** A Fuzzy Commitment Scheme // Proc. ACM Conf. Computer and Communications Security. 1999. P. 28–36.
19. **Иванов А. И.** и др. О многообразии метрик, позволяющих наблюдать реальные статистики распределения биометрических данных «нечетких экстракторов» при их защите наложением гаммы / А. И. Иванов, С. А. Сомкин, Д. Ю. Андреев, Е. А. Малыгина // Вестник УрФО. Безопасность в информационной сфере. № 2(12). 2014. С. 16–23.
20. **Scotti F.,** et al. Privacy-aware Biometrics: Design and Implementation of a Multimodal Verification System / F. Scotti, S. Cimato, M. Gamassi, V. Piuri, R. Sassi // 2008 Annual Computer Security Applications Conf. IEEE. 2008. P. 130–139.
21. **Ложников П. С.** и др. 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.
22. **Иванов А. И., Ложников П. С., Качайкин Е. И.** Идентификация подлинности рукописных автографов сетями Байеса — Хэмминга и сетями квадратичных форм // Вопросы защиты информации. 2015. № 2. С. 28–34.
23. **Lozhnikov P. S., Sulavko A. E., Volkov D. A.** Application of Noise Tolerant Code to Biometric Data to Verify the Authenticity of Transmitting Information // Control and Communications (SIBCON), Omsk, Russia, May 21–23, 2015. P. 1–3. doi:10.1109/SIBCON.2015.7147126
24. **Еременко А. В.** и др. Генерация криптографических ключей на основе подписей пользователей компьютерных систем/ А. В. Еременко, Майков В. Б., Ступко К. О., Мироненко О. Е. // Аппроксимация логических моделей, алгоритмов и задач — АЛМАЗ'2: материалы Второй Междунар. конф., Омск, 27–30 апреля 2015 г. С. 23–27.
25. **Еременко А. В.** Повышение надежности идентификации пользователей компьютерных систем по динамике написания паролей: автореф. дис. ... канд. техн. наук. — Омск: СибАДИ, 2011. — 20 с.
26. **Robert H. Morelos-Zaragoza.** The Art of Error Correcting Coding. — John Wiley & Sons, 2006. — 320 p.
27. **Еременко А. В., Сулавко А. Е.** Способ двухфакторной аутентификации пользователей компьютерных систем на удаленном сервере с использованием клавиатурного почерка // Прикладная информатика. 2015. № 6. С. 48–59.

UDC 004.93'1
doi:10.15217/issn1684-8853.2016.5.73

Experimental Evaluation of Reliability of Signature Verification by Quadratic Form Networks, Fuzzy Extractors and Perceptrons

Lozhnikov P. S.[a], PhD, Tech, Associate Professor
Sulavko A. E.[a], PhD, Tech, Senior Lecturer
Eremenko A. V.[b], PhD, Tech, Associate Professor
Volkov D. A.[a], Post-Graduate Student
[a]Omsk State Technical University, 11, Mira Ave., 644050, Omsk, Russian Federation
[b]Omsk Transport University, 35, Karl Marx Ave., 644046, Omsk, Russian Federation

Purpose: The problems of information security become more and more pressing, therefore the demands to biometric systems become tougher. Our objective is to compare fuzzy extractors, neural network biometry-code converters and networks of quadratic forms by their authentication reliability, on the base of signature features. **Results:** We have analyzed the literature and conducted a series of numerical experiments based on real biometric data. The main result of the experiments is that fuzzy extractors are significantly inferior to the other system by their authentication reliability and the key length. The best performance was provided by Bayesian–Pearson networks. **Practical relevance:** The results will be of interest to researchers and developers of biometric systems.

Keywords — Signature Reproduction Features, Biometrics, Fuzzy Extractors, Artificial Neural Networks, Authentication.

References

1. *The Global State of Information Security® Survey 2016. PricewaterhouseCoopers.* Available at: http://www.pwc.com/gx/en/issues/cyber-security/information-security-survey/download.html (accessed 27 June 2016).
2. Hogland G. *Rutkity: vnedrenie v iadro Windows* [Rootkits: Subverting the Windows Kernel]. Saint-Petersburg, Piter Publ., 2007. 285 p. (In Russian).
3. Ivanov A. I. *Neirosetevye algoritmy biometricheskoi identifikatsii lichnosti* (Nauchnaia seriia "Neirokomp'iutery i ikh primenenie", no. 15) [Neural Network Algorithms for Biometric Identification (Science Series "Neurocomputers and their Application", no. 15]. A. I. Galushkin ed. Moscow, Radiotekhnika Publ., 2004. 144 p. (In Russian).
4. State Standard R52633.0-2006. Data Protection. Information Protection Technique. Requirements for Highly Reliable Means of Biometric Authentication. Moscow, Standartinform Publ., 2006. 24 p. (In Russian).
5. Dodis Y., Reyzin L., Smith A. Fuzzy Extractors: How to Generate Strong Keys from Biometrics and Other Noisy. *EUROCRYPT*, April 2004, pp. 523–540.
6. Ahmetov B. S., Ivanov A. I., Funtikov V. A., Bezjaev A. V., Malygina E. A. *Tekhnologiia ispol'zovaniia bol'shikh neironnykh setei dlia preobrazovaniia nechetkikh biometricheskikh dannykh v kod kliucha dostupa* [Technology of Using Large Neural Networks for Fuzzy Transformation of Biometric Data in the Access Code Key].

Almaty, Izdatel'stvo LEM Publ., 2014. 144 p. (In Russian).
7. Volchihin V. I., Ivanov A. I., Funtikov V. A., Malygina E. A. Prospects of Using Artificial Neural Networks with Multi-Level Quantizers Technology in Biometrics-Neural Network Authentication. *Izvestiia vysshikh uchebnykh zavedenii. Povolzhskii region*, 2013, no. 4(28), pp. 86–96 (In Russian).
8. State Standard R 52633.5-2011. Data Protection. Information Protection Technique. Automatic Learning Neural Network Converters Biometry-Code Access. Moscow, Standartinform Publ., 2011. 20 p. (In Russian).
9. Bezjaev A. V., Ivanov A. I., Funtikova Ju. V. Optimization of the Structure of Bio-Self-Correcting Code Storing Error Syndromes as Fragments of Hash Functions. *Vestnik UrFO. Bezopasnost' v informatsionnoi sfere*, 2014, no. 3(13), pp. 4–13 (In Russian).
10. Ivanov A. I. *Neirosetevaia zashchita konfidentsial'nykh biometricheskikh obrazov grazhdanina i ego lichnykh kriptograficheskikh kliuchei* [Neural Protection of Sensitive Biometric Images of the Citizen and his Personal Cryptographic Keys]. Penza, PNIEI Publ., 2014. 57 p. (In Russian).
11. Ahmetov B. B., Ivanov A. I., Serikova N. I. The Algorithm is an Artificial Increase in the Number of Degrees of Freedom in the Analysis of the Biometric Data on the Criterion of the Consent of The Chi-Square. *Vestnik Natsional'noi akademii nauk Respubliki Kazakhstan*, 2014, no. 5, pp. 28 (In Russian).
12. Ivanov A. I., Gazin A. I., Perfilov K. A., Vyatchanin S. E. Noise Elimination of Quantization Biometric Data While Using Multivariate Test Cramer – Von Mizes in Small Samples. *Nadezhnost' i kachestvo slozhnykh system*, 2016, no. 2(14), pp. 21–28 (In Russian).
13. Vasil'ev V. I. *Intellektual'nye sistemy zashchity informatsii* [Intelligent Information Security Systems]. Moscow, Mashinostroenie Publ., 2012. 199 p. (In Russian).
14. Busch C. Biometrics and Security. *NISNet – FINSE Winter School*, April 27, 2010. Available at: http://www.nisnet, no/filer/Finse 10/Biometrics_and_ Security_ Busch:pdf (accessed 26 June 2016).
15. Cavoukian A., Stoianov A. *Biometric Encryption Chapter from the Encyclopedia of Biometrics*. Available at: http://www.ipc.on.ca/images/Resours/bio-encrypt-chp.pdf (accessed 26 June 2016).
16. Kulikova O. V. *Biometricheskie kriptograficheskie sistemy i ikh primenenie* [Biometric Cryptographic Systems and their Applications]. Available at: http://www. pvti.ru/ data/file/bit/bit_3_2009_10.pdf (accessed 26 June 2016).
17. Juels A., Sudan M. A Fuzzy Vault Scheme. *Designs, Codes and Cryptography*, February 2006, vol. 38, iss. 2, pp. 237–257. doi: 10.1007/s10623-005-6343-z
18. Juels A., Wattenberg M. A Fuzzy Commitment Scheme. *Proc. ACM Conf. Computer and Communications Security*, 1999, pp. 28–36.
19. Ivanov A. I., Somkin S. A., Andreev D. Ju., Malygina E. A. The Variety of Metrics that Allow to Observe the Real Statistical Distribution of Biometric Data "Fuzzy Extractors" under the Protection of their Scale Overlay. *Vestnik UrFO. Bezopasnost' v informatsionnoi sfere*, 2014, no. 2(12), pp. 16–23 (In Russian).
20. Scotti F., Cimato S., Gamassi M., Piuri V., Sassi R. Privacy-aware Biometrics: Design and Implementation of a Multimodal Verification System. *2008 Annual Computer Security Applications Conf.*, IEEE, 2008, pp. 130–139.
21. Lozhnikov P. S., Ivanov A. I., Kachaykin E. I., Sulavko A. E. Biometric Identification of Manuscript Images Using Analog Correlation Bayes Rule. *Voprosy zashchity informatsii* [Issues of Protection of Information], 2015, no. 3, pp. 48–54 (In Russian).
22. Ivanov A. I., Lozhnikov P. S., Kachaykin E. I. Identification of the Authenticity of Handwritten Autographs Bayesian-Hamming Networks and Quadratic Forms Networks. *Voprosy zashchity informatsii* [Issues of Protection of Information], 2015, no. 2, pp. 28–34 (In Russian).
23. Lozhnikov P. S., Sulavko A. E., Volkov D. A. Application of Noise Tolerant Code to Biometric Data to Verify the Authenticity of Transmitting Information. *Control and Communications (SIBCON)*, Omsk, Russia, May 21–23, 2015, pp. 1–3. doi:10.1109/SIBCON.2015.7147126
24. Eremenko A. V., Majkov V. B., Stupko K. O., Mironenko O. E. The Generation of Cryptographic Keys Based on the Signatures of Computer System Users. *Materialy Vtoroi Mezhdunarodnoi konferentsii "Approksimatsiia logicheskikh modelei, algoritmov i zadach – ALMAZ'2* [Proc. of the Second Intern. Conf. "Approximation of Logic Models, Algorithms and Tasks"], Omsk, April 27–30, 2015, pp. 23–27 (In Russian).
25. Eremenko A. V. *Povyshenie nadezhnosti identifikatsii pol'zovatelei komp'iuternykh sistem po dinamike napisaniia parolei*. Dis. kand. tehn. nauk [Improving the Reliability of Computer Systems Users Identification by the Dynamics of Writing Passwords. PhD tech. sci. diss.]. Omsk, SibADI Publ., 2011. 20 p. (In Russian).
26. Robert H. Morelos-Zaragoza. *The Art of Error Correcting Coding*. John Wiley & Sons, 2006. 320 p.
27. Eremenko A. V., Sulavko A. E. A Method of Two-Factor Authentication of Computer Systems Users on a Remote Server by Using Keyboard Handwriting. *Prikladnaia informatika* [Applied Informatics], 2015, no. 6, pp. 48–59 (In Russian).

УВАЖАЕМЫЕ АВТОРЫ!

Научные базы данных, включая SCOPUS и Web of Science, обрабатывают данные автоматически. С одной стороны, это ускоряет процесс обработки данных, с другой — различия в транслитерации ФИО, неточные данные о месте работы, области научного знания и т. д. приводят к тому, что в базах оказывается несколько авторских страниц для одного и того же человека. В результате для всех по отдельности считаются индексы цитирования, снижая рейтинг ученого.

Для идентификации авторов в сетях Thomson Reuters проводит регистрацию с присвоением уникального индекса (ID) для каждого из авторов научных публикаций.

Процедура получения ID бесплатна и очень проста: входите на страницу http://www.researcherid.com, слева под надписью «New to ResearcherID?» нажимаете на синюю кнопку «Join Now It's Free» и заполняете короткую анкету. По указанному электронному адресу получаете сообщение с предложением по ссылке заполнить полную регистрационную форму на ORCID. Получаете ID.