УДК 004.93'1

А.Е. Сулавко, А.В. Еременко, С.С. Жумажанова, Е.В. Бурая

ГЕНЕРАЦИЯ КЛЮЧЕВЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ И ВЕРИФИКАЦИЯ СУБЪЕКТОВ НА ОСНОВЕ ДВУМЕРНОГО ИЗОБРАЖЕНИЯ ЛИЦА[1]

Сулавко Алексей Евгеньевич, *кандидат технических наук, окончил факультет «Информационно-управляющие системы» Сибирской государственной автомобильно-дорожной академии. Старший преподаватель Омского государственного технического университета. Имеет более 50 научных статей в области биометрии и распознавания образов в системах информационной и производственной безопасности. [e-mail: sulavich@mail.ru].*

Еременко Александр Валериевич, *кандидат технических наук, окончил факультет «Информационно-управляющие системы» СибАДИ. Инженер-проектировщик Омского государственного университета путей сообщения. Имеет более 35 научных статей в области биометрии и распознавания образов в системах информационной и производственной безопасности. [e-mail: nexus-@mail.ru].*

Жумажанова Самал Сагидулловна, *окончила факультет «Информационно-управляющие системы» СибАДИ. Аспирант ОмГТУ. Имеет 7 научных статей в области биометрии и распознавания образов в системах информационной и производственной безопасности. [e-mail: samal_shumashanova@mail.ru].*

Бурая Екатерина Викторовна, *окончила Уфимский государственный авиационный технический университет. Аспирант УГАТУ. Имеет 5 научных статей по биометрии. [e-mail: burka-777@yandex.ru].*

Аннотация

Рассматривается проблема защиты данных от неавторизованного доступа. Предлагается генерировать ключи-пароли на основе биометрических параметров лица для последующей аутентификации субъектов. Рассмотрены различные подходы к выработке битовых последовательностей из биометрических данных: нечеткий экстрактор, нейросетевой преобразователь биометрия-код на базе сети персептронов, обученной по ГОСТ Р 52633.5-2011, использование сетей нейронов на базе метрики Пирсона. Собрана база данных изображений лиц 70 субъектов. Сформировано пространство 46 признаков лица. Произведена оценка вероятностей ошибок верификации субъектов по параметрам лица на основе рассмотренных подходов. По данным эксперимента нечеткие экстракторы работают хуже нейросетевых преобразователей биометрия-код, сети персептронов уступают в надежности генерируемого ключа сетям функционалов Пирсона. Достигнуты следующие результаты по генерации ключевых последовательностей: нечеткие экстракторы: FRR=0,032, FAR=0,014 при длине ключа 42 бита; сети персептронов: FRR=0,014, FAR=0,029 при длине ключа 100 бит; Пирсона-Хемминга: FRR=0,0039, FAR=0,0022 при длине ключа 120 бит.

Ключевые слова: физиологические параметры лица, нечеткий экстрактор, искусственные нейронные сети, преобразователь биометрия-код, сети квадратичных форм.

GENERATION OF KEY SEQUENCES AND VERIFICATION OF SUBJECTS ON THE BASIS OF A TWO-DIMENSIONAL IMAGE OF THE FACE

Aleksei Evgenevich Sulavko, *Candidate of Engineering; graduated from the Faculty "Information Systems in Management" of Siberian State Automobile and Highway Academy; Senior Teacher at Omsk State Technical University; an author of more than 50 articles in the field of biometrics and image identification in information and industrial security systems. e-mail: sulavich@mail.ru.*

Aleksandr Valerevich Eremenko, *Candidate of Engineering; graduated from the Faculty "Information Systems in Management" of Siberian State Automobile and Highway Academy; Design Engineer at Omsk State Transport University; an author of more than 35 articles in the field of biometrics and image identification in information and industrial security systems. e-mail: nexus-@mail.ru.*

Samal Sagidullovna Zhumazhanova, *graduated from the Faculty "Information Systems in Management" of Siberian State Automobile and Highway Academy; Postgraduate Student at Omsk State Technical University; an author of 7*

1 Работа выполнена при финансовой поддержке РФФИ (грант № 15-07-09053) и Министерства образования и науки РФ, проект № 541 на 2016 год.

articles in the field of biometrics and image identification in information and industrial security systems. e-mail: samal_shumashanova@mail.ru.

Ekaterina Viktorovna Buraia, *graduated from Ufa State Aviation University; Postgraduate Student of Ufa State Aviation University; an author of 5 articles in the field of biometrics. e-mail: burka-777@yandex.ru.*

Abstract

The problem of data protection from unauthorized access was considered. Generation of keys-passwords based on biometric parameters of the face for authentication of subjects is proposed. The authors discuss various approaches to generation of bit sequences of biometric data such as a fuzzy extractor, neural networks biometrics-code converter on the basis of a perceptron network trained in accordance with GOST R 52633.5–2011, using neural networks based on the Pearson's metrics. The database of 70 subjects' faces was constructed. The space of 46 facial features was formed. Assessment of the probability of subjects verification errors in the facial parameters on the basis of these approaches was carried out. According to the results of the experiment, neural network converters work better than fuzzy extractors, perceptions are inferior in reliability of the generating key to Pearson networks. The following results in the generation of key sequences were obtained: fuzzy extractors: FRR = 0.032, FAR = 0.014 in case of 42 bit key length; perceptron networks: FRR = 0.014, FAR = 0.029 in case of 100 bit key length; Pearson-Hemming network: FRR = 0.0039, FAR = 0.0022 in case of 120 bit key length.

Key words: physiological parameters of the face, fuzzy extractor, artificial neural networks, biometrics-code converter, networks of quadratic forms.

Введение

На сегодняшний день киберпреступность беспокоит не только специалистов по информационной безопасности, но и высшее руководство организаций. Сумма мировых убытков от несанкционированных действий внешних и внутренних нарушителей информационной безопасности постоянно возрастает [1]. Имеющиеся оценки таких потерь впечатляют и по разным источникам составляют от 18–29 [2] до 375–575 [3] млрд. долларов США в год.

Защита данных от несанкционированного доступа на уровне хранения обеспечивается их шифрованием. Современные методы шифрования надежны, если использовать стойкие ключи. Но проблема человеческого фактора усложняет использование длинных ключей шифрования. Аналогичным образом человеческому фактору подвержены средства аутентификации по паролю при осуществлении доступа к информационной системе. Не секрет, что длинный пароль создает существенные неудобства для работника организации, в результате частой является ситуация, когда субъект оставляет для себя подсказки на рабочем месте, которыми легко может воспользоваться нарушитель. Для защиты личных электронных кабинетов (учетных записей социальных сетей, электронной почты и т. д.) требования к генерации надежных паролей часто не выдерживаются. Наилучшим вариантом в сложившейся ситуации является привязка всех аутентификаторов к личности их владельцев. Такая привязка должна быть неотъемлемой от субъекта, надежной, без возможности ее фальсификации на практике. Неотъемлемыми от человека являются его биометрические признаки. Статические признаки – отпечатки пальцев, радужка дают возможность реализовать надежную привязку, однако позволяют злоумышленнику изготовить фальсификат. Динамические признаки – клавиатурный почерк, подпись, голос дают сравнительно высокий процент ошибочных решений [4, 5]. В рамках настоящей работы предлагается использовать двухмерные модели лица субъекта для реализации связи «человек-пароль».

Преобразователи биометрия-код

По определению, данному в ГОСТ Р 52633.0-2006 [6]: преобразователь биометрия-код преобразует вектор нечетких, неоднозначных биометрических параметров «Свой» в четкий однозначный код ключа (пароля) и откликается случайным выходным кодом на воздействие случайного входного вектора, не принадлежащего множеству образов «Свой». Под образами, не принадлежащими множеству «Свой», подразумевается образы «Чужой» (образ «Все чужие»). Соответственно образы «Свой» и «Чужой» – это векторы биометрических параметров (далее признаков), характеризующих легального пользователя и злоумышленника (просто неизвестного субъекта). Для получения вектора значений признаков (реализации) предварительно каждый исходный образ биометрических данных (изображение отпечатка пальцев, лица, речевой сигнал и т. д.) подвергается обработке, в результате которой из образца выделяется только необходимая информация. Далее реализации используются для обучения преобразователя биометрия-код и для генерации ключей.

Можно выделить три основных подхода к построению преобразователя биометрия-код:

1. «Нечеткий экстрактор» (Fuzzy Extractors) [7]. Данный подход основан на применении алгоритмов помехоустойчивого кодирования к «сырым» (не обогащенным) биометрическим данным для исправления ошибочных бит генерируемого ключа, возникающих вследствие невозможности абсолютно точного повторного воспроизведения биометрического образа. Нечеткие экстракторы развиваются в основном благодаря зарубежным научным коллективам. Известно несколько техник генерации ключа на базе аналогичного подхода с различными названиями: Fuzzy Vault («нечеткое хранилище») [8], Fuzzy Commitment [9] и т. д. Далее будем называть данные схемы генерации ключа нечетким экстрактором.

2. Нейросетевой преобразователь биометрия-код – однослойная или двухслойная сеть персептронов. Данный

подход является рекомендуемым в России, требования к таким преобразователям изложены в семействе отечественных стандартов ГОСТ Р 52633 (количество которых превышает число стандартов для «нечетких экстракторов [10]).

3. Сети иных функционалов. Основное отличие данного подхода от изложенного выше в том, что функционалом нейрона является не функция взвешенного суммирования, а иная мера близости входного образа к эталону. В зависимости от функционала могут быть сформированы сети квадратичных форм (Пирсона-Хемминга [11, 12], Евклида-Хемминга [11]) и другие (сети функционалов Хи-модуль [12] и др.) В зависимости от использующихся функционалов сети могут иметь различные конструктивные особенности и свойства.

Существуют требования к защите биометрических данных, описанные в ГОСТ Р 52633.0-2006 [6]. Поэтому независимо от выбранного подхода на практике должна существовать возможность представления и хранения эталонов субъектов в виде, не позволяющем восстановить их биометрические характеристики (значения признаков или образ).

Параметрами надежности преобразователей биометрия-код являются вероятности ошибок 1-го (FRR, false reject rate) и 2-го (FAR, false acceptance rate) рода. Ошибка 1-го рода происходит, когда на основе реализации «Свой» генерируется неверный ключ (нехарактерный для субъекта-владельца эталона), ошибка 2-го рода – когда на основе реализации «Чужой» генерируется верный ключ (характерный для субъекта-владельца эталона).

Особенности лиц субъектов. Формирование базы биометрических признаков

Подход к выделению признаков основан на методике вычисления биометрических параметров, используемой в работах [13, 14]. Сформирована база изображений лиц, полученных в результате анализа видеозаписей коротких диалогов с 70 испытуемыми (длительность каждой записи составляла 30–60 секунд, частота 15–25 кадров в секунду, разрешение 480x360 пикселей). Субъект большую часть времени был обращен лицом к камере (рис. 1), повороты головы составляли не более 30–40 градусов, расстояние до камеры 1–2 метра, площадь лица в кадре составляла не менее 35000 пикселей. Для каждого испытуемого получено не менее 450 изображений, каждое из которых преобразовывалось в вектор из 46 признаков:

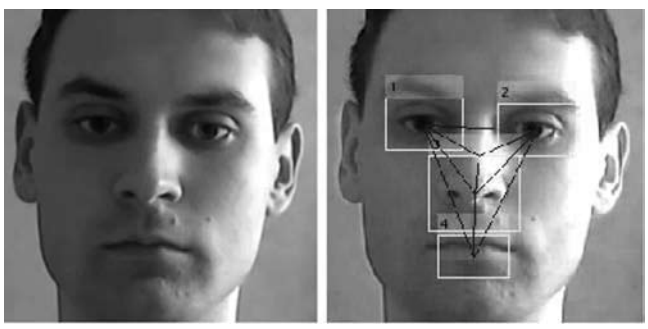

Рис. 1. Выделение области лица и областей глаз, рта, носа

- расстояния между следующими элементами: глаза, центр лица, кончик носа, центр рта (в пикселях, значения нормировались по длине диагонали области лица в кадре);
- площади глаз, носа, рта (в пикселях, значения нормировались по площади лица);
- коэффициенты корреляции яркости и цветовых составляющих пикселей (в соответствии с моделью RGB) между всеми парами элементов лица: глаз, носа, рта;
- величины, характеризующие цвет глаз и кожи.

Все рассматриваемые признаки имеют распределение значений, достаточно близкое к нормальному, что проверялось критерием Хи-квадрат.

Для выделения лица (кожи), глаз, носа, рта применялся метод Виолы-Джонса [15], который является одним из лучших по соотношению показателей эффективность распознавания/скорость работы [16, 17].

В цветовой модели RGB цвет является интегральным показателем интенсивности красной (R), зелёной (G) и синей (B) составляющих пикселя. Цвета глаз и кожи – средние показатели составляющих совокупности пикселей на определенных областях, выделенных методом Виолы-Джонса. Цвет глаз – характеристика, определяемая пигментацией радужной оболочки. Алгоритм выделения радужки основан на преобразовании Хафа [18].

Вычисляемые признаки можно рассматривать как случайные величины, т. к. имеется погрешность их определения (связанная с условиями съемки и особенностями движений субъектов). Некоторые из указанных признаков являются очень информативными, т. к. функции плотностей вероятности их значений, характеризующих различных субъектов, имеют незначительные пересечения (рис. 2). Более 90% признаков имеют низкую взаимную корреляционную зависимость (коэффициент парной корреляции по модулю менее 0,3).

Генерация ключевых последовательностей нечеткими экстракторами

Нечеткий экстрактор фактически извлекает ключевую последовательность бит из битовой строки, которая формируется на этапе обучения из совокупности реализаций биометрических данных и генерируемого ключа. Ключ (пароль), представленный в виде битовой последовательности, кодируется помехоустойчивым кодом [19]. Сам ключ (пароль) создается до обучения, и методики его формирования в настоящей работе не рассматриваются. Для помехоустойчивого кодирования в нечетких экстракторах обычно используются классические самокорректирующие коды Адамара, Боуза-Чоудхури-Хоквингема (БЧХ-коды), Рида-Соломона (частный случай БЧХ) [20]. Кодируемый ключ далее объединяется с другой битовой последовательностью, получаемой в результате квантования эталонных биометрических данных. Биометрические данные не обогащаются (квантуются исходные значения признаков или их средние значения). На выходе получа-

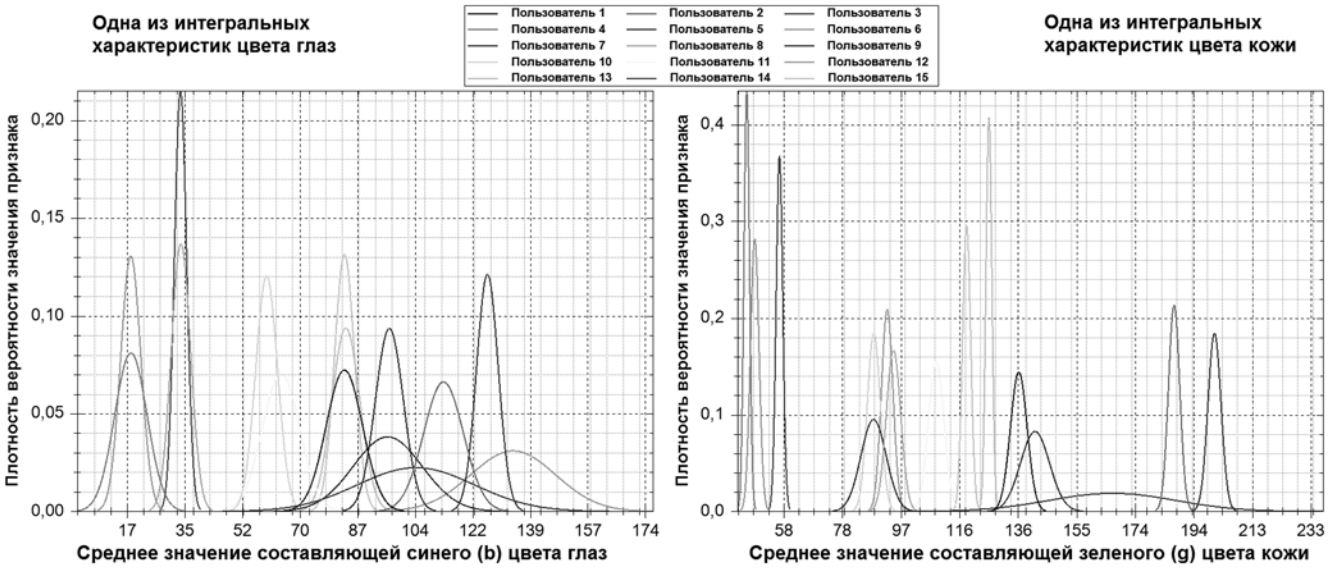

Рис. 2. Плотности распределения значений 2-х из наиболее информативных признаков, характеризующих 15 испытуемых

ется (открытая) строка, которую разрешается хранить в открытом виде, из нее нельзя восстановить ключ, т. к. на него наложена гамма в виде квантованных значений признаков [21, 22].

На этапе генерации ключа производится обратная последовательность действий. Введенный образ преобразуется в реализацию значений признаков, которые квантуются (если признак не был зафиксирован на изображении, его битовое значение заполняется нулями) и «вычитаются» из открытой строки. К результату данной операции применяются соответствующие коды, исправляющие ошибки. В итоге будет получен исходный ключ либо неверная последовательность битов (если количество ошибочных бит в квантованных данных не превысит исправляющей способности кода) [21, 22].

В настоящей работе использовались способ квантования и методика ранжирования признаков по информативности (на этапе обучения) из работы [22]. Методика позволяет использовать для генерации ключа только те признаки субъекта, битовые значения которых наиболее стабильны, т. е. из биометрических данных удалялись наименее информативные участки. Проведен эксперимент с имеющейся базой изображений лиц по генерации ключей. Для создания открытых строк использовалось по 21 реализации данных лица от каждого субъекта (по аналогии с требованиями к обучению нейронных сетей по ГОСТ Р 52633.5-2011 [23]), остальные использовались для генерации ключа. Тестировалось 3 вида нечетких экстракторов: на основе кодов Рида-Соломона, БЧХ (для декодирования применялся алгоритм Питерсона-Горенстейна-Цирлера) или Адамара. По результатам эксперимента наивысшая скорость работы и наименьшие вероятности ошибок генерации ключа достигнуты с использованием кодов Адамара. Исключение нестабильных признаков снижает количество ошибок (рис. 3).

Наилучший достигнутый результат для нечетких экстракторов в рамках эксперимента (по минимуму FRR+FAR) был получен при количестве (наиболее информативных) признаков 32 и составил: FRR=0,032, FAR=0,014 с длиной генерируемого ключа 42 бита. Как можно видеть, длина

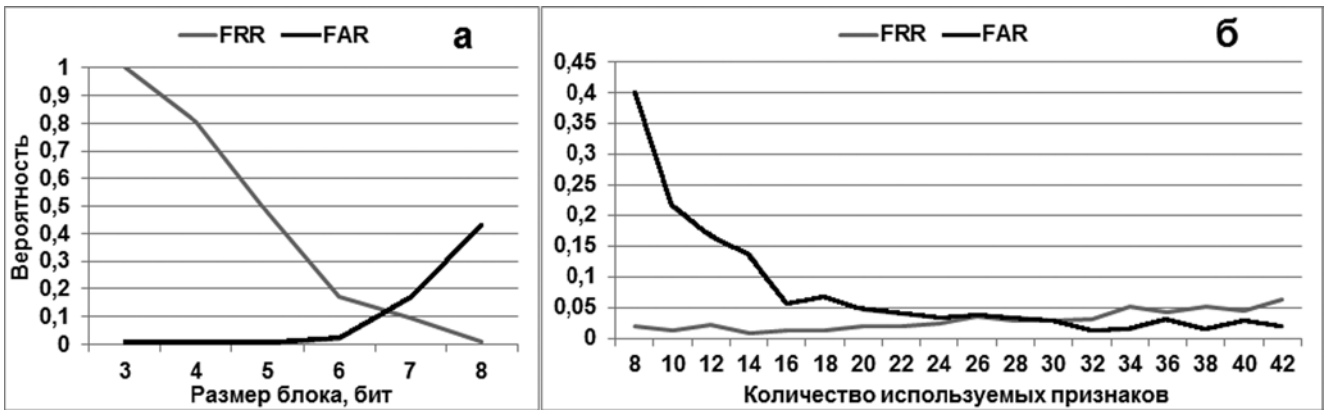

Рис. 3. Результаты генерации ключевых последовательностей нечетким экстрактором на базе кодов Адамара: а) с использованием 46 признаков; б) с различным количеством ранжированных по информативности признаков при размере блока 6 бит

ключевой последовательности невелика. Классические помехоустойчивые коды обладают большой избыточностью, которая возрастает с увеличением исправляющей способности (в кодах Адамара исправляющая способность зависит от размера блока, в кодах БЧХ – от других параметров), что уменьшает длину вырабатываемого ключа [10, 11, 24].

Генерация ключевых последовательностей сетями персептронов

В ГОСТ Р 52633.5-2011 [23] рекомендуется использовать однослойные или двухслойные сети персептронов. Первый слой обогащает входные биометрические данные посредством учета законов распределения значений признаков. Параметры законов распределения не хранятся в исходном виде, вместо них хранятся веса входов нейронов, каждый вход ассоциирован с определенным признаком. Второй слой играет роль кодов, исправляющих ошибки, но в отличие от нечетких экстракторов исправление ошибочных бит не влияет столь негативно на длину выходных кодов [10, 11]. Значение функционала нейрона любого слоя вычисляется по формуле (1) и далее сравнивается с нулем, от этого зависит бинарное выходное значение нейрона.

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

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 (порог срабатывания). Веса нейронов вычисляются детерминированно по формуле: $\mu_i = |E_ч(x_i) - E_c(x_i)| / \sigma_ч(x_i) \cdot \sigma_c(x_i)$, где $E_c(x_i)$ – математическое ожидание значений признака для образа «Свой», $\sigma_c(x_i)$ – среднеквадратичное отклонение значений признака для образа «Свой», $E_ч(x_i)$ и $\sigma_ч(x_i)$ – аналогичные показатели для образа «Чужой». Если признак не удалось зафиксировать на изображении лица, то соответствующие входы нейрона игнорируются. Однослойные сети нейронов с одним квантователем генерируют битовую строку с количеством бит, равным числу нейронов.

Помимо второго слоя нейронов, для корректировки ошибочных бит могут применяться специальные коды, исправляющие ошибки, предложенные в работе [25] специально для биометрии. Коды [25] не поглощают избыточностью генерируемый ключ и позволяют безопасно хранить синдромы ошибок отдельно от открытой строки в виде усеченной хеш-функции. В работе [26], посвященной нечетким экстракторам, показана связь эффективности коррекции ошибок с методами группирования бит с разной вероятностью единичной ошибки. Дело в том, что распределение ошибочных бит в квантованных нечетким экстрактором биометрических данных не является равномерным, однако классические коды подразумевают именно равномерное распределение ошибки. Коды из [25] позволяют учитывать неравномерное распределение единичных ошибок и исправлять заданное количество бит, что удобней, чем использование второго слоя нейронов и эффективнее классических кодов. В настоящей работе будет применяться однослойная нейронная сеть с последующей корректировкой нестабильных бит кодами из работы [25].

Для каждого из испытуемых сформирована сеть персептронов, для обучения которой в соответствии с ГОСТ Р 52633.5-2011 использовалось по 21 реализации его биометрических данных и по одной реализации от каждого из остальных субъектов (64 независимых образа «Все чужие»). Операции по настройке нейронной сети более подробно описаны в ГОСТ Р 52633.5-2011 [23] и работе [10]. Оптимальный результат (по всем параметрам превосходящий нечеткие экстракторы) для данного метода (рис. 4) получен при количестве нейронов 100 и входов нейронов 8: FRR=0,014, FAR=0,029 с длиной генерируемого ключа 100 бит.

Генерация ключевых последовательностей сетями Пирсона-Хемминга

Обогащение данных персептронами не является оптимальным. Помимо сетей персептронов возможно построение сетей нейронов на основе других функционалов. Целесообразность использования тех или иных функционалов определяется особенностью пространства признаков (в частности их взаимной корреляционной зави-

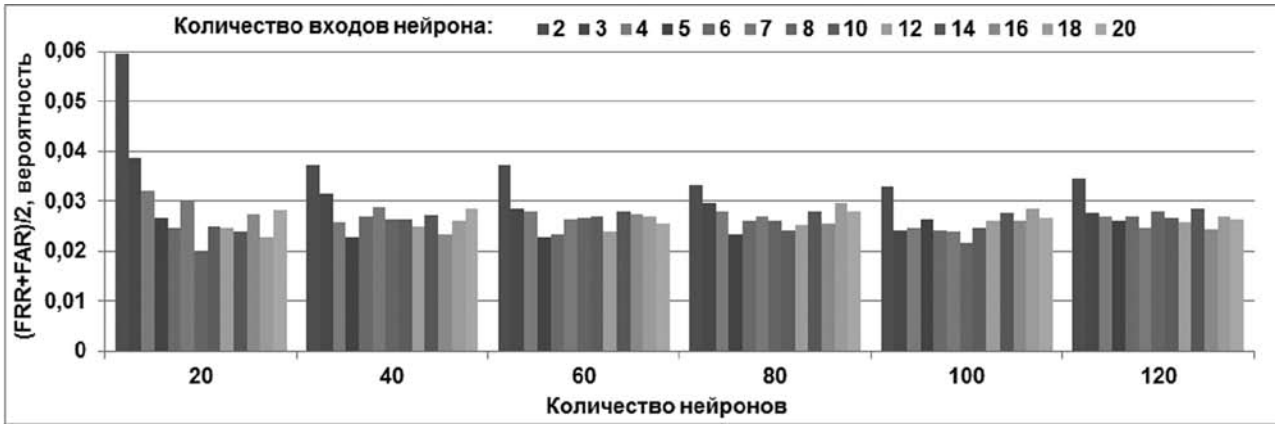

Рис. 4. Результаты генерации ключей сетями персептронов, обученных по ГОСТ Р 52633.5-2011 с корректировкой нестабильных бит специальными кодами [25]

симостью [12]). Применение в биометрии классических квадратичных форм, требующих обращения многомерных корреляционных матриц признаков, затруднительно по причине плохой обусловленности этой задачи [12]. При низкой корреляционной зависимости признаков допустимо игнорировать корреляционные связи и использовать сеть метрик Пирсона (2):

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

где v_i – i-й вход нейрона, $E(v_i)$ – математическое ожидание i-го входа нейрона, $\sigma(v_i)$ – среднеквадратичное отклонение i-го входа нейрона. Если в реализации признак отсутствует, то соответствующие входы игнорируются. Значение метрики (2) на выходе нейрона сравнивается с пороговым. Для каждого нейрона имеется свое оптимальное пороговое значение, которое подбирается эмпирически, исходя из произведения $\theta = \chi_{max} \cdot a_1$, где χ_{max} – это максимальное значение квадратичной формы при поступлении на вход обучающих примеров образа «свой», a_1 – стабилизирующий коэффициент, экспериментально подбираемый для каждого пространства признаков (по аналогии с [11]). При превышении порога нейрон выдает единицу («1») – иначе нуль («0»). Чтобы настроить сеть на верный ключ, значения выхода определенных нейронов инвертируются.

Особенностью сети Пирсона-Хемминга является необходимость хранения параметров законов распределения признаков, что противоречит требованиям защиты эталонов ГОСТ Р 52633.0-2006. Поэтому на практике можно использовать принцип защищенного нейросетевого контейнера [10]: создается гибридная сеть из персептронов и нейронов Пирсона, параметры нейронов Пирсона шифруются на верных выходах персептронов. В случае подачи на вход верного образа «Свой» выход потока персептронов формирует верную часть ключа, которая расшифровывает параметры нейронов Пирсона, которые в свою очередь формируют вторую часть итогового ключа. При подаче на вход сети образа «Чужой» персептроны выдают ошибочные биты, и параметры нейронов Пирсона расшифровываются неверно. Может использоваться более сложная схема с многократным шифрованием и большим количеством изолированных потоков персептронов, формирующая ключ из множества промежуточных частей. Итоговый ключ может дополнительно корректироваться вторым слоем нейронов из ГОСТ Р 52633.5-2011 или кодами из работы [25]. Все это имеет смысл, если вероятность ошибок генерации ключа гибридной сетью ниже, чем при использовании сети персептронов (нужно стремиться к вероятности, наблюдаемой у сетей Пирсона-Хемминга, см. рис. 5).

В настоящей работе сравнение подходов проводилось без использования принципа защищенного нейросетевого контейнера. Сети квадратичных форм решено реализовать с одним слоем нейронов с последующей корректировкой кодами из [25]. Проведен эксперимент с имеющейся базой реализаций. Сформированы сети Пирсона-Хемминга, для обучения которых использовалось по 21 реализации «Свой». Наилучший результат для данного метода (по минимуму FRR+FAR) получен при количестве нейронов 120 и входов нейронов 10: FRR= 0,0039, FAR=0,0022 с длиной генерируемого ключа 120 бит, что многократно превышает результаты, достигнутые на базе нечетких экстракторов и сетей персептронов.

Заключение

К основным выводам данной работы можно отнести следующее:

1. Наиболее информативными признаками из рассмотренных в настоящей работе являются параметры цвета глаз и кожи.

2. Нечеткие экстракторы работают хуже нейросетевых преобразователей биометрия-код даже в случае наличия информативных признаков.

3. Сети персептронов значительно уступают в надежности генерируемого ключа сетям Пирсона-Хемминга.

Достигнуты следующие результаты по генерации ключевых последовательностей на основе параметров лица субъектов (с последующей верификацией субъектов):

1. На основе нечетких экстракторов с использованием

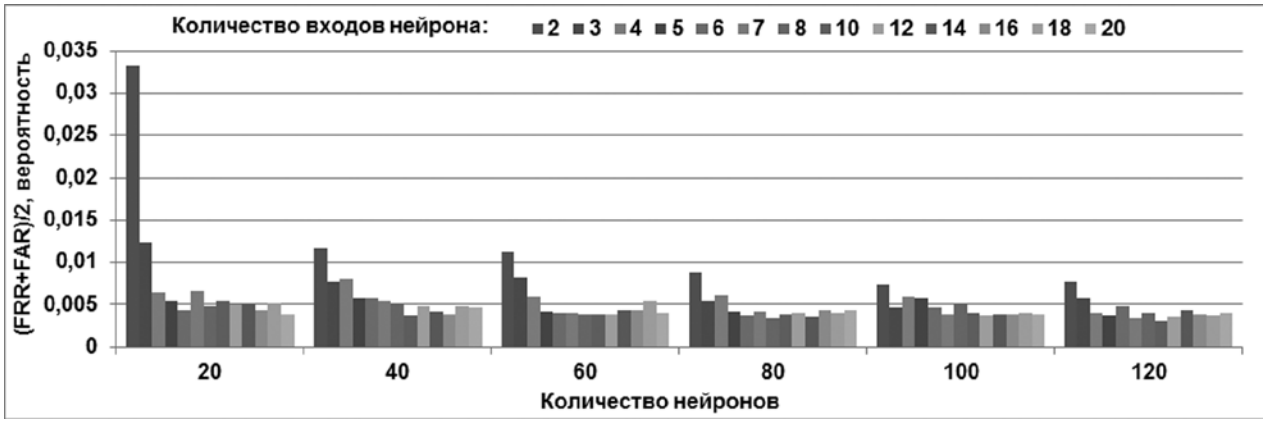

Рис. 5. Результаты генерации ключей сетями Пирсона-Хемминга с корректировкой нестабильных бит специальными кодами [25]

процедуры ранжирования признаков по информативности и кодов Адамара при размере блока 6 бит: FRR=0,032, FAR=0,014 при длине генерируемого ключа 42 бита.

2. На основе сетей персептронов, обученных по ГОСТ Р52633.5-2011, с количеством нейронов 100 и числом входов нейронов 8: FRR=0,014, FAR=0,029 при длине генерируемого ключа 100 бит.

3. На основе сетей Пирсона-Хемминга с количеством нейронов 120 и числом входов нейронов 10: FRR=0,0039, FAR=0,0022 при длине генерируемого ключа 120 бит.

На практике целесообразно создавать гибридные сети из персептронов и функционалов Пирсона, шифруя параметры нейронов Пирсона на выходах персептронов. Нужно провести ряд вычислительных экспериментов для построения эмпирической модели, иллюстрирующей эффективность использования принципа защищенного нейросетевого контейнера.

СПИСОК ЛИТЕРАТУРЫ

1. The Global State of Information Security® Survey 2016. PricewaterhouseCoopers. – URL: http://www.pwc.com/gx/en/issues/cyber-security/information-security-survey/download.html (дата обращения: 27.06.2016).

2. Center for Strategic and international Studies, Net Losses: Estimating the Global Cost of Cybercrime, June 2014.

3. Утечки конфиденциальной информации в России и в мире. Итоги 2016 года. Zecurion Analytics. – URL: http://www.zecurion.ru/upload/iblock/1e5/ Zecurion_Data_Leaks_2016_full.pdf (дата обращения: 06.07.2016).

4. Еременко А.В., Сулавко А.Е., Волков Д.А. Современное состояние и пути модернизации преобразователей биометрия-код // Информационные технологии – 2016. – № 3. – С. 203–210.

5. Технологии скрытой биометрической идентификации пользователей компьютерных систем / В.И. Васильев, П.С. Ложников, А.Е. Сулавко, А.В. Еременко // Вопросы защиты информации. – 2015. – № 3. – С. 37–47.

6. ГОСТ Р 52633.0-2006. Защита информации. Техника защиты информации. Требования к средствам высоконадежной биометрической аутентификации. – М. : Стандартинформ, 2006. – 24 с.

7. Dodis Y., L. Reyzin and A. Smith Fuzzy Extractors: How to Generate Strong Keys from Biometrics and Other Noisy, Data April 13, In EUROCRYPT, 2004, pp. 523–540.

8. Juels A., Sudan M. A Fuzzy Vault Scheme // IEEE International Symposium on Information Theory, 2002.

9. Juels A., Wattenberg M. A Fuzzy Commitment Scheme // Proc. ACM Conf. Computer and Communications Security, 1999, pp. 28–36.

10. 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 «ИздательствоLEM», 2014. – 144 с.

11. Экспериментальная оценка надежности верификации подписи сетями квадратичных форм, нечеткими экстракторами и персептронами / П.С. Ложников, А.Е. Сулавко, А.В. Еременко, Д.А. Волков // Информационно-управляющие системы. – 2016. – № 5. – С. 73–85.

12. Биометрическая идентификация рукописных образов с использованием корреляционного аналога правила Байеса / А.И. Иванов, П.С. Ложников, Е.И. Качайкин, А.Е. Сулавко // Вопросы защиты информации. – 2015. – № 3. – С. 48–54.

13. Vasilyev V.I., Sulavko A.E., Eremenko A.V., Zhumazhanova S.S. Identification potential capacity of typical hardware for the purpose of hidden recognition of computer network users // X International IEEE Scientific and Technical Conference «Dynamics of Systems, Mechanisms and Machines» (Dynamics), 15-17 November, 2016, Omsk, Russia. – URL: http://ieeexplore.ieee.org/abstract/document/7819106/?part=1 (дата обращения: 07.02.2017).

14. Оценка идентификационных возможностей биометрических признаков от стандартного периферийного оборудования / В.И. Васильев, П.С. Ложников, А.Е. Сулавко, С.С. Жумажанова // Вопросы защиты информации. – 2016. – № 1. – С. 12–20.

15. Viola P. and M. Jones. Rapid object detection using a boosted cascade of simple features. Computer Vision and Pattern Recognition, 2001. CVPR 2001. Proceedings of the 2001 IEEE Computer Society Conference on. pp I, 511, I, 518 vol.1. 2001.

16. Cho, H. & Hwang, SY. J. High-performance on-road vehicle detection with non-biased cascade classifier by weight-balanced training // EURASIP Journal on Image and Video Processing, (2015) 2015: 16. doi:10.1186/s13640-015-0074-5.

17. Srinivasa, K.G. & Gosukonda, S. Continuous multimodal user authentication: coupling hard and soft biometrics with support vector machines to attenuate noise // CSI Transactions on ICT, June 2014, Volume 2, Issue 2, pp. 129–140. doi:10.1007/s40012-014-0054-4.

18. P. V. C. Hough, A method and means for recognizing complex patterns, U. S. Patent No.3.069.654, (1962).

19. Robert H Morelos-Zaragoza. The art of error correcting coding. John Wiley & Sons, 2006. – 320 p.

20. Соловьева Ф.И. Введение в теорию кодирования : учеб. пособие / Новосиб. гос. ун-т. – Новосибирск, 2006. – 127 с.

21. Еременко А.В., Сулавко А.Е. Исследование алгоритма генерации криптографических ключей из биометрической информации пользователей компьютерных систем // Информационные технологии. – 2013. – № 11. – С. 47–51.

22. Сулавко А.Е., Еременко А.В., Борисов Р.В. Генерация криптографических ключей на основе голосовых сообщений // Прикладная информатика. – 2016. – № 5. – С. 76–89.

23. ГОСТ Р52633.5-2011. Защита информации. Техника защиты информации. Автоматическое обучение нейросетевых преобразователей биометрия-код доступа. – М. : Стандартинформ, 2011. – 20 с.

24. 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. – 2014. – № 2 (12). – С. 16–23.

25. 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.

26. 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 Conference, IEEE. 2008. – pp. 130–139.

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: 27.06.2016).

2. Net Losses: Estimating the Global Cost of Cybercrime, *Center for Strategic and International Studies,* June 2014.

3. Utechki konfidentsialnoi informatsii v Rossii i v mire. Itogi 2016 goda [Leakage of Confidential Information in Russia and Arround the Globe]. *Zecurion Analytics*. Available at: http://www.zecurion.ru/upload/iblock/1e5/ Zecurion_Data_Leaks_2016_full.pdf (accessed: 06.07.2016).

4. Eremenko A.V., Sulavko A.E., Volkov D.A. Sovremennoe sostoianie i puti modernizatsii preobrazovatelei biometriia-kod [Current State and Ways to Modernize Converters Biometrics to Code]. *Informatsionnye tekhnologii* [Information Technologies], 2016, no. 3, pp. 203–210.

5. Vasiliev V.I., Lozhnikov P.S., Sulavko A.E., Eremenko A.V. Tekhnologii skrytoi biometricheskoi identifikatsii polzovatelei kompiuternykh system [Hidden Biometric Identification Technologies of Users of Computer Systems]. *Voprosy zashchity informatsii* [Issues on Information Protection], 2015, no. 3, pp. 37–47.

6. GOST R 52633.0-2006. Zashchita informatsii. Tekhnika zashchity informatsii. Trebovaniya k sredstvam vysokonadezhnoy biometricheskoy autentifikatsii [Information Protection. Information Protection Technology. Requirements to the Means of High-Reliability Biometric Authentication]. Moscow, Standartinform Publ., 2006. 24 p.

7. Dodis Y., L. Reyzin and A. Smith. Fuzzy Extractors: How to Generate Strong Keys from Biometrics and Other Noisy Data. , *In EUROCRYPT*, April 13, 2004, pp. 523–540.

8. Juels A., Sudan M. A Fuzzy Vault Scheme. *IEEE International Symposium on Information Theory,* 2002.

9. Juels A., Wattenberg M. A Fuzzy Commitment Scheme. *Proc. ACM Conf. Computer and Communications Security*. 1999, pp. 28–36.

10. Akhmetov B.S., Ivanov A.I., Funtikov V.A., Beziaev A.V., Malygina E.A. *Tekhnologiia ispolzovaniia bolshikh neironnykh setei dlia preobrazovaniia nechetkikh biometricheskikh dannykh v kod kliucha dostupa. Monografiia* [Big Neural Network Technology for the Transformation of Fuzzy Biometric Data to the Access Key Code]. Almaty, TOO "IzdatelstvoLEM" Publ., 2014. 144 p.

11. P.S. Lozhnikov, A.E. Sulavko, A.V. Eremenko, D.A. Volkov Eksperimentalnaia otsenka nadezhnosti verifikatsii podpisi setiami kvadratichnykh form, nechetkimi ekstraktorami i perseptronami [Experimental Evaluation of Reliability of Signature Verification by Quadratic Form Networks, Fuzzy Extractors and Perceptrons]. *Informatsionno-upravliaiushchie sistemy* [Information Control Systems], 2016, no. 5, pp. 73–85.

12. Ivanov A.I., Lozhnikov P.S., Kachaykin E.I., Sulavko A.E. Biometricheskaia identifikatsiia rukopisnykh obrazov s ispolzovaniem korreliatsionnogo analoga pravila Bayesa [Biometric Identification of Handwritten Images Via Correlation Analog of Bayes" Rule]. *Voprosy zashchity informatsii* [Issues on Information Protection], 2015, no. 3, pp. 48–54.

13. Vasilyev V.I., Sulavko A.E., Eremenko A.V., Zhumazhanova S.S. Identification Potential Capacity of Typical Hardware for the Purpose of Hidden Recognition of Computer Network Users. *X International IEEE Scientific and Technical Conference "Dynamics of Systems, Mechanisms and Machines" (Dynamics),* 15–17 November, 2016, Omsk, Russia. Available at: http://ieeexplore.ieee.org/abstract/document/7819106/?part=1 (accessed: 07.02.2017).

14. VasilevV.I., Lozhnikov P.S., Sulavko A.E., Zhumazhanova S.S. Otsenka identifikatsionnykh vozmozhnostei biometricheskikh priznakov ot standartnogo periferiinogo oborudovaniia [Identification Possibilities Assessment of Biometric Features from Standard Peripheral Equipment]. *Voprosy zashchity informatsii* [Issues on Information Protection], 2016, no. 1, pp. 12–20.

15. Viola P. and M. Jones. Rapid Object Detection Using a Boosted Cascade of Simple Features. Computer Vision and Pattern Recognition, 2001. CVPR 2001. *Proceedings of the 2001 IEEE Computer Society Conference*. 2001, vol. 1, pp I, 511, I, 518.

16. Cho, H. and Hwang, SY. J. High-performance On-road Vehicle Detection with Non-biased Cascade Classifier by Weight-balanced Training. *EURASIP Journal on Image and Video Processing,* (2015) 2015: 16. doi:10.1186/s13640-015-0074-5.

17. Srinivasa, K.G. and Gosukonda, S. Continuous Multimodal User Authentication: Coupling Hard and Soft Biometrics with Support Vector Machines to Attenuate Noise. *CSI Transactions on ICT*, June 2014, Vol. 2, Iss. 2, pp 129–140. doi:10.1007/s40012-014-0054-4.

18. Hough P. V. C. A *Method and Means for Recognizing Complex Patterns,* U. S. Patent No.3.069.654, (1962).

19. Robert H Morelos-Zaragoza. The *Art of Error Correcting Coding*. John Wiley & Sons Publ., 2006. 320 p.

20. Soloveva F.I. *Vvedenie v teoriiu kodirovaniia. Ucheb. Posobie* [Introduction to the Coding Theory. Textbook]. Novosibirsk, Novosibirsk State University Publ., 2006. 127 s.

21. Eremenko A.V., Sulavko A.E. Issledovanie algoritma generatsii kriptograficheskikh kliuchei iz biometricheskoi

informatsii polzovatelei kompiuternykh system [Analysis of Algorithms for Cryptography Key Generation Based on User-Specific Biometric Information of Computer Systems Users]. *Informatsionnye tekhnologii* [Information Technologies], 2013, no. 11, pp. 47–51.

22. Sulavko A.E., Eremenko A.V., Borisov R.V. Generatsiia kriptograficheskikh kliuchei na osnove golosovykh soobshchenii [Generation of Key Sequences Based on Voice Messages]. *Prikladnaia informatika* [Applied Informatics], 2016, no. 5, pp. 76–89.

23. *GOST R 52633.5-2011. Zashchita informatsii. Tekhnika zashchity informatsii. Avtomaticheskoe obuchenie neirosetevykh preobrazovatelei biometriia-kod dostupa* [Information Protection. Information Protection Technology. The Neural Net Biometry-Code Convertor Automatic Training]. Moscow, Standartinform Publ., 2011. 20 p.

24. Ivanov A.I., Somkin S.A., Andreev D.Iu., Malygina E.A. O mnogoobrazii metrik, pozvoliaiushchikh nabliudat realnye statistiki raspredeleniia biometricheskikh dannykh "nechetkikh ekstraktorov" pri ikh zashchite nalozheniem gammy [Diversity Metrics to Watch Actual Biometric Data Distribution Statistics "Fuzzy Extractors" in their Protection of a Range]. *Vestnik UrFO. Bezopasnost v informatsionnoi sfere* [Ural Federal Region Newsletter. Information Security], 2014, no. 2 (12), pp. 16–23.

25. Beziaev A.V., Ivanov A.I., Funtikova Iu.V. Optimizatsia struktury samokorrektiruiushchegosia biokoda, khraniashchego sindromy oshibok v vide fragmentov khesh-funktsii [Optimization of the Structure Self-Correcting Bio-Code, Storing Syndromes Error as Fragments Hash-Functions]. *Vestnik UrFO. Bezopasnost v informatsionnoi sfere* [Ural Federal Region Newsletter. Information Security], 2014, no. 3 (13), pp. 4–13.

26. 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 Conference, IEEE*. 2008, pp. 130–139.