УДК 004.93'1
doi:10.15217/issn1684-8853.2017.1.50

КОМПЛЕКСИРОВАНИЕ НЕЗАВИСИМЫХ БИОМЕТРИЧЕСКИХ ПРИЗНАКОВ ПРИ РАСПОЗНАВАНИИ СУБЪЕКТОВ НА ОСНОВЕ СЕТЕЙ КВАДРАТИЧНЫХ ФОРМ, ПЕРСЕПТРОНОВ И МЕРЫ ХИ-МОДУЛЬ

А. Е. Сулавко[а], *канд. техн. наук, старший преподаватель*
А. В. Еременко[б], *канд. техн. наук, доцент*
Е. В. Толкачева[б], *канд. техн. наук, доцент*
Р. В. Борисов[в], *аспирант*
[а]*Омский государственный технический университет, Омск, РФ*
[б]*Омский государственный университет путей сообщения, Омск, РФ*
[в]*Сибирская государственная автомобильно-дорожная академия, Омск, РФ*

Постановка проблемы: *статические биометрические образы не являются секретными и могут быть скопированы для изготовления физического или электронного муляжа незаметно для владельца, поэтому идет процесс поиска эффективных решений для аутентификации субъектов по динамическим биометрическим признакам.* ***Цель исследования:*** *разработать более надежные способы однофакторной и многофакторной биометрической аутентификации в пространстве малоинформативных признаков.* ***Результаты:*** *проведена серия вычислительных экспериментов на основе биометрических данных подписи, клавиатурного почерка, лица и голоса субъектов с использованием сетей персептронов, квадратичных форм и функционалов хи-модуль. Предложено адаптировать алгоритм обучения персептронов из ГОСТ Р 52633.5-2011 для настройки сетей квадратичных форм. Удалось достичь количества ошибок верификации образа субъекта по подписи около 1 %, клавиатурному почерку и подписи — 0,31 %, лицу — менее 0,5 %, лицу совместно с клавиатурным почерком — менее 0,1 %, а также трех- и четырехфакторной верификации образов субъектов порядка 0,54–0,01 %.* ***Практическая значимость:*** *методы двух- (без образов голоса), трех- и четырехфакторной верификации образов субъектов, рассмотренные в работе, можно использовать на практике при реализации контрольно-пропускной функции или удаленной аутентификации. Подделку признаков более двух видов образов на практике можно считать неосуществимой.*

Ключевые слова *— параметры подписи, клавиатурный почерк, характеристики голоса, физиологические особенности лица, биометрия, искусственные нейронные сети, квадратичные формы, алгоритмы распознавания образов.*

Введение

Мы переживаем период глобальной технологической революции. Происходит формирование новых инновационных рынков и их активное освоение: человеко-машинные коммуникации, новые методы получения энергии, беспилотные наземные и летательные аппараты и другие, среди которых одним из ключевых становится рынок информационной безопасности. В соответствии с Национальной технологической инициативой (НТИ) — долгосрочной комплексной программой по созданию условий для обеспечения лидерства российских компаний на новых высокотехнологичных рынках — важное место в мировом масштабе занимают защищенные компьютерные технологии и решения в области безопасности информационных и киберфизических систем. К основным проектам НТИ в сфере информационной безопасности относятся:

— мультимодальная биометрия для системы управления персональными данными;

— система биометрического контроля и аутентификации;

— национальная биометрическая платформа;

— биометрическая аутентификация и цифровая подпись в доверенной среде.

Важность биометрических технологий подтверждается тенденцией их широкомасштабного внедрения. По данным глобального исследования рынков информационной безопасности, проведенного PricewaterhouseCoopers, на октябрь 2016 года 57 % руководителей предприятий установили биометрические системы аутентификации для защиты корпоративных ресурсов [1].

Поиск новых эффективных методик биометрической аутентификации обусловлен недостатками разработанных решений: статически биометрические признаки (отпечатки пальца, сетчатки, радужки; геометрия руки) допускают возможность изготовления муляжа, не являются секретными и не позволяют реализовать процедуру скрытой идентификации субъекта. Поэтому усилия многих исследователей сконцентрированы на развитии других биометрических технологий, в частности на базе динамических признаков рукописных, голосовых образов, лица и клавиатурного почерка. Основной их недостаток заключается в более низкой надежности, которая определяется вероятностью ошибок

1-го и 2-го рода — ложного отказа в доступе «Своему» (FRR — False Reject Rate) и ложного доступа «Чужого» (FAR — False Acceptance Rate).

Цель проведенного в настоящей работе исследования — разработка более надежных способов однофакторной и многофакторной биометрической аутентификации в пространстве малоинформативных признаков.

Биометрические признаки

Перспективным направлением повышения надежности процедур биометрической аутентификации является комплексирование биометрических признаков, получаемых по независимым каналам. В работе рассматриваются следующие независимые группы признаков:

1) особенности воспроизведения и внешнего вида подписей;

2) физиологические особенности лица;

3) характеристики клавиатурного почерка;

4) параметры голоса диктора.

Для этой цели использовалась база следующих биометрических образцов, полученных от каждого из 60 испытуемых: не менее 50 образцов подписи (автографа), не менее 50 образцов парольной фразы «авторизация пользователя компьютерной системы», 10-минутная аудиозапись голоса при произношении произвольного текста (стихотворения, чтение новостных лент), видеозапись диалога с испытуемым длительностью 30–60 с. Образцы подвергались статистической обработке, в результате которой из каждого образца вычислялся вектор значений признаков, краткое описание которых приводится в табл. 1 и далее по тексту.

Особенности воспроизведения и внешнего вида подписей

Перед вычислением вектора значений признаков подпись нормируется по алгоритму на основе прямого и последующего обратного преобразования Фурье [2]. В качестве биометрических признаков решено использовать характеристики

■ ***Таблица 1***. Биометрические признаки субъектов

№	Краткое описание группы признаков	Количество
1.1	Нормированные по энергии амплитуды 16 самых низкочастотных гармоник функций давления $p(t)$ и скорости пера $v_{xy}(t)$	32
1.2	Коэффициенты корреляции между функциями $x(t)$, $y(t)$, $p(t)$	15
1.3	Расстояния между некоторыми точками подписи в трехмерном пространстве (точки выбираются равномерно с некоторым шагом, далее находятся расстояния между всеми парами этих точек, третье измерение — давление пера на планшет)	120
1.4	Значения функций $x(t)$, $y(t)$, $p(t)$ и $v_{xy}(t)$ в некоторых точках	64
1.5	Некоторые характеристики изображения подписи: отношение длины подписи к ее ширине, центр подписи, угол наклона подписи, угол наклона между центрами половин подписи	5
1.6	Коэффициенты вейвлет-преобразований Добеши по базису D6 функций $v_{xy}(t)$ и $p(t)$	134
2.1	Расстояния между глазами, правым (левым) глазом и центром лица, правым (левым) глазом и кончиком носа, правым (левым) глазом и центром рта, центром рта и лица, кончиком носа и центром рта, центром рта и кончиком носа (в пикселях, значения нормировались по длине диагонали области лица в кадре)	10
2.2	Площади глаз, носа, рта (в пикселях, значения нормировались по площади лица)	4
2.3	Коэффициенты корреляции яркости и цветовых составляющих пикселей (в соответствии с моделью RGB) между всеми парами следующих областей лица: глаз, носа, рта	24
2.4	Цветовые составляющие в модели RGB и яркость глаз и кожи	8
3.1	Временные задержки удержания клавиш	L
3.2	Временные задержки между нажатием клавиш	$L-1$
4.1	Характеристики интегральной частоты фрагментов речевого сигнала (нулевой форманты)	20
4.2	Характеристики интегральной частоты переходов речевого сигнала через огибающую энергии	20
4.3	Частотные характеристики уровня положительного давления	20
4.4	Частотные характеристики уровня отрицательного давления	20
4.5	Коэффициенты корреляции характеристик интегральной частоты сигнала и переходов речевого сигнала через огибающую энергии	20
4.6	Коэффициенты корреляции частотных характеристик уровня положительного и уровня отрицательного давления	20

[2], дополненные коэффициентами вейвлет-преобразования Добеши D6 (см. табл. 1), получаемыми при анализе подписей из нормированных по длительности функций скорости и давления пера на устройство ввода на уровнях разложения с 4-го по 6-й из работы [3]. В проведенных исследованиях [3] рассматривались различные базисы вейвлетов Добеши (от D4 до D10 [4]), при использовании вейвлета D6 получен достаточный по точности результат при приемлемой скорости преобразования. Основная доля мощности сигнала сосредоточена в коэффициентах, вычисляемых на уровнях разложения с 4-го по 6-й (частотный диапазон 1,5625÷12,5), так как они почти соответствуют диапазону частот колебаний руки подписанта (0,1÷10 Гц) [5] и, следовательно, являются информативными. Физический смысл коэффициентов вейвлет-преобразования, полученных в результате многомасштабного анализа, можно трактовать как характеристики гармоник сигнала, принадлежащих определенному частотному диапазону и возникающих в сигнале в определенный момент времени [3].

Физиологические особенности лица

В результате анализа видеозаписей с испытуемыми (длительность каждой записи составляла 30–60 с, частота 15–25 кадров в секунду, разрешение 480×360 пикселей, субъект обращен лицом к камере, расстояние до камеры 1–2 м, повороты головы не более 40 град) были получены изображения лиц (не менее 450 изображений на каждого субъекта). Далее каждое изображение преобразовывалось в вектор значений признаков, многие из которых использовались в работе [6] (площади глаз, носа, рта, расстояния между ними, коэффициенты корреляции между цветами пикселей в модели RGB для перечисленных выше участков), а также признаки, характеризующие цвет глаз и кожи в модели RGB (см. табл. 1). Для выделения признаков использовался метод Виолы — Джонса [7] и алгоритм обнаружения окружностей на основе преобразования Хафа [8].

Характеристики клавиатурного почерка

Методы распознавания по клавиатурному почерку основаны на том, что оператор запоминает удачные решения задачи набора текста на клавиатуре путем их многократных повторений [5, 9]. Программа управления мышцами откладывается в подсознательной сфере и реализуется автоматически [5, 9].

В настоящей работе вектор значений признаков клавиатурного почерка формировался непосредственно из регистрируемых временных задержек между нажатием клавиш и длительностей их удержания. Информативность парольной фразы в данном случае напрямую зависела от ее длины L, т. е. количества содержащихся в ней символов. При выборе парольной фразы и отборе испытуемых учитывались следующие принципы:

— признаки характеризуют оператора (т. е. информативны), если субъект имеет выработанный клавиатурный почерк;

— длинные парольные фразы сложно запомнить (велика вероятность ошибки при наборе фразы на клавиатуре).

По некоторым оценкам, время становления почерка работы с клавиатурой составляет около 6 месяцев [9] (желательно, чтобы скорость набора текста на клавиатуре была не менее 100 символов в минуту [9]), а парольная фраза должна содержать от 21 до 42 нажатий на клавиши [5].

Параметры голоса диктора

Из работы [10] следует, что, используя признаки, получаемые из фрагментов произвольной непрерывной речи, удалось добиться меньшей вероятности ошибок генерации ключевых последовательностей, чем из признаков, вычисляемых по фиксированным коротким фразам (или словам). Поэтому в данной работе применен подход к выделению признаков на основе анализа непрерывной речи.

Аудиозаписи голосов субъектов дискретизированы со следующими параметрами: размер аудиообразца 8 бит (256 уровней квантования), частота дискретизации $\upsilon_д$ 8000 Гц. Выбор значения первого параметра обусловлен стремлением минимизировать объем аудиообразца и субъективными оценками аудиентов, которыми распознавались записанные голоса: распознавание было однозначно удовлетворительным, не отличалось от записей аудиообразца размером 16 бит (65 536 уровней квантования). Второй параметр задавался исходя из диапазона частот, занимаемых речевым сигналом (до 4000 Гц), в соответствии с теоремой Котельникова о дискретизации сигнала: дискретное кодирование без потерь для непрерывного сигнала из диапазона до определенной частоты возможно при его дискретизации с удвоенной частотой. Каждая аудиозапись делилась на фрагменты Z_k, которые преобразовывались в векторы значений признаков. Помимо признаков из работы [10], описывающих нулевую форманту, вычислялись характеристики интегральной частоты переходов сигнала через огибающую энергии, частотные характеристики уровня положительного и отрицательного давления, коэффициенты корреляции характеристик интегральной частоты сигнала (нулевой форманты) и переходов речевого сигнала через огибающую энергии, а также частотные характеристики уровня положительного и отрицательного давления. Опишем данный процесс подробней.

Для вычисления векторов значений признаков исходный дискретный сигнал Y был разбит на интервалы Y_i по 0,025 с со сдвигом $\tau_{ОТ}$=0,0125 с. Значение 0,025 с объясняется частотой основного тона (ОТ), обусловленной частотой вибраций голосовых связок (80 Гц). Частота ОТ $\upsilon_{ОТ}$ является наименьшей значимой частотой спектра голосового сигнала min(ОТ). Длина интервала выбрана в два раза больше периода min(ОТ), чтобы в отдельный интервал поместился минимум один период ОТ. Длина сдвига была равной периоду min(ОТ) для более точной локализации во времени изменений обрабатываемого сигнала.

Для каждого сигнала Y_i вычислено количество переходов через нулевой уровень. Для этого от значений отсчетов Y_i был вычтен уровень квантования 128, соответствующий нахождению мембраны микрофона в спокойном состоянии, — сформирован сигнал Y_i^{128}, имеющий положительные и отрицательные значения, сумма которых на интервале близка к нулю (не равна строго, так как интервал не содержит точного количества периодов ОТ). Возможно отклонение суммы получаемых отсчетов Y_i^{128} от нуля из-за активного выходящего воздушного давления, отклоняющего мембрану микрофона от спокойного состояния (звуковые колебания записываются уже на напряженную мембрану). На этот случай сделана поправка: определено его среднее $Y_i^{ср}=\sum_{j=0}^{n}(Y_{ij}^{128})$, где $n=\tau_{ОТ}\upsilon_д$, которое затем было вычтено (если $Y_i^{ср}>0$) или добавлено (если $Y_i^{128}<0$) к значению каждого отсчета сигнала Y_i^{128}. Таким образом, получены центрированные сигналы Y_i^0. Каждому интервалу Y_i ставилось в соответствие количество переходов сигнала Y_i^0 через ноль — $T0(Y_i)$, вычисляемое по формуле

$$T0(Y_i)=\sum_{x=1}^{n}\left(y(x)=\begin{cases}1,\ Y_i^0(x-1)\cdot Y_i^0(x)<0\\0,\ Y_i^0(x-1)\cdot Y_i^0(x)\ge 0\end{cases}\right), \quad (1)$$

где $n=\tau_{ОТ}\upsilon_д$. Интервалы Y_i были сгруппированы в массивы, соответствующие фрагментам Z_k исходного 10-минутного сигнала. Каждому Z_k в соответствие ставится гистограмма относительных частот $G_k(T0(Y_i))$ значений $T0(Y_i)$, принадлежащих Z_k. Длительность Z_k подобрана исходя из влияния количества интервалов на сумму $\mathrm{Sum}(G_k(T0(Y_i)))$ квадратов разниц столбцов гистограмм в соответствии с правилом $\mathrm{Sum}(G_k(T0(Y_{i+1})))-\mathrm{Sum}(G_k(T0(Y_i)))<z$, где z — эмпирически определенный коэффициент. Чем выше длительность фрагмента речевого сигнала Z_k, тем точней вычислялись значения признаков. Однако длительная процедура записи голосового сообщения неудобна для практики, поэтому решено взять $z=0{,}03$, при этом длина фрагмента Z_k составляет 9–12 с. Совокупность значений столбцов $G_k(T0(Y_i))$ является признаком k-го голосового образца Z_k.

Следующие использованные признаки — переходы сигнала Y_i^0 через уровень среднего значения модуля уровня сигнала U, характеризующего уровень энергии сигнала. Для каждого Y_i^0 вычислено $U_i^p=\sum_{x=0}^{n}(|Y_i^0(x)|)$, где n — количество отсчетов интервала Y_i^0. Далее для каждого Y_i выполнялось преобразование

$$TU^p(Y_i)=$$
$$=\sum_{x=1}^{n}\left(y(x)=\begin{cases}1,\ (Y_i^0(x-1)-U_i^p)(Y_i^0(x)-U_i^p)<0\\0,\ (Y_i^0(x-1)-U_i^p)(Y_i^0(x)-U_i^p)\ge 0\end{cases}\right). \quad (2)$$

Каждому Z_k аналогичным образом ставилась в соответствие гистограмма относительных частот $G_k(TU^p(Y_i))$. Отдельно строились гистограммы $G_k(TU^m(Y_i))$ для переходов сигнала Y_i^0 через отрицательную функцию $U_i^m=-U_i^p$, а также гистограммы $G_k(TU^{pm}(Y_i))$ относительных частот переходов через $+U$ и $-U$, вычисляемых как $TU^{pm}(Y_i)=TU^p(Y_i)+TU^m(Y_i)$.

Количество столбцов гистограмм $G_k(T0(Y_i))$, $G_k(TU^p(Y_i))$, $G_k(TU^m(Y_i))$ и $G_k(TU^{pm}(Y_i))$ влияет на количество признаков, эмпирически было определено и решено использовать по 20 столбцов для каждой гистограммы. Множество значений столбцов гистограмм вместе с коэффициентами корреляции между функциями $T0(Y_i)$ и $TU^p(Y_i)$, а также $TU^{pm}(Y_i)$ и $TU^m(Y_i)$ принималось за вектор значений признаков, характеризующих образ диктора. При непопадании вычисляемых величин в интервал гистограммы, что происходит по причине недостаточной длины фрагмента (образца) Z_k, значение соответствующего признака игнорировалось (исключалось из вектора значений признаков), так как в данном случае приравнивать относительную частоту к нулю некорректно.

Подходы к формированию решений

В работе [2] проведено сравнение подходов к генерации ключей (кодов), используемых для аутентификации, на основе биометрических данных подписей. Установлено, что нечеткие экстракторы [11–13] существенно уступают искусственным нейронным сетям персептронов, квадратичных форм (сети Пирсона — Хемминга, Евклида — Хемминга) и функционалов, оценивающих близость к корреляционным связям образа (сеть Байеса — Пирсона — Хемминга) по надежности генерации ключа и другим параметрам. Поэтому в настоящей работе решено не применять технологии нечетких экстракторов и сконцентрировать усилия исключительно на сетях персептронов и иных функционалов.

В ГОСТ Р 52633.5-2011 [14] рекомендовано использовать однослойные или двухслойные сети персептронов. Первый слой необходим для обогащения входных биометрических данных. Параметры законов распределения признаков не хранятся в исходном виде, вместо них хранятся веса входов нейронов, каждый вход связан с определенным признаком. Второй слой обычно используется для корректировки ошибок [2, 14, 15] и в настоящем исследовании не применялся. Значение функционала нейрона вычислялось по формуле

$$y = \sum_{i=1}^{m} \mu_i v_i + \mu_0, \qquad (3)$$

где m — число входов; v_i — i-й вход нейрона; μ_i — весовой коэффициент i-го входа; μ_0 — нулевой вес, отвечающий за переключатель квантования (порог срабатывания), и далее сравнивалось с нулем. Каждый нейрон способен выдавать одно бинарное значение в зависимости от результата сравнения.

Веса нейронов считались детерминированно по формуле

$$\mu_i = |E_{\text{ч}}(x_i) - E_{\text{с}}(x_i)| \,/\, \sigma_{\text{ч}}(x_i)\sigma_{\text{с}}(x_i), \qquad (4)$$

где $E_{\text{ч}}(x_i)$ — математическое ожидание значений признака для образа «Чужой»; $\sigma_{\text{ч}}(x_i)$ — их среднеквадратическое отклонение; $E_{\text{с}}(x_i)$ и $\sigma_{\text{с}}(x_i)$ — аналогичные показатели для образа «Свой». Операции по обучению сети персептронов по ГОСТ Р 52633.5 [14] более подробно описаны в стандарте, а также в работах [2, 15].

Вместо второго слоя нейронов для исправления ошибочных битов в настоящей работе применялись специальные коды, исправляющие ошибки, предложенные для биометрии [16]. Они позволяют безопасно хранить синдромы ошибок в виде усеченной хеш-функции вместе с параметрами сети. Коды [16] можно использовать для учета неравномерного распределения единичных ошибок (в отличие от классических самокорректирующих кодов) и исправлять заданное количество бит, что удобней, чем использование второго слоя нейронов, и эффективнее классических кодов. В настоящей работе применялись однослойные сети с последующей корректировкой нестабильных битов кодами [16].

Другой способ распознавания субъектов может быть построен на использовании сетей квадратичных форм

$$y = (E(\overline{x}) - \overline{x})^{\mathrm{T}} \left[\mathbf{R}\right]^{-1} (E(\overline{x}) - \overline{x}), \qquad (5)$$

каждая из которых выдает бинарное значение. Здесь $E(\overline{x})$ — математическое ожидание вектора контролируемых биометрических параметров в нормированной системе координат; $[\mathbf{R}]^{-1}$ — корреляционная матрица контролируемых биометрических параметров. Обращать корреляционные матрицы $[\mathbf{R}]^{-1}$ высокой размерности не удается (это плохо обусловленная задача) [17, 18]. Поэтому приходится вместо квадратичных форм использовать сети персептронов. Без учета корреляционной зависимости признаков классическая квадратичная форма равна метрике Пирсона [2, 18], тем не менее при построении сетей из этих метрик удается получить более высокие результаты по сравнению с сетями персептронов в задаче верификации автографов [2]. Классическую квадратичную форму можно выразить через взвешенную меру Евклида

$$\varepsilon = \sqrt{\sum_{i=1}^{m} \mu_i (E(v_i) - v_i)^2}, \qquad (6)$$

где $E(v_i)$ — математическое ожидание (среднее значение) i-го входа нейрона.

Для настройки весов функционалов (6) могут использоваться аналогичные алгоритмы, применяемые для настройки нейронных сетей. Итерационные алгоритмы обучения нейронных сетей не подходят для биометрии [2, 17], так как они не устойчивы. Поэтому для настройки сетей мер (6) использовался абсолютно устойчивый детерминированный алгоритм обучения из ГОСТ Р 52633.5 [14]. Если μ_i является равным соответствующему коэффициенту обратной корреляционной матрицы $[\mathbf{R}]^{-1}$, деленному на среднеквадратическое отклонение $\sigma(v_i)$ i-го входа нейрона, то взвешенная мера Евклида станет равной классической квадратичной форме (5). При $\mu_i = 1$ взвешенная мера становится обычной евклидовой мерой. В любом случае взвешенная мера Евклида работает гораздо лучше, в чем можно убедиться из результатов проведенного эксперимента.

Чтобы адаптировать алгоритм обучения ГОСТ Р 52633.5 [14] для настройки весовых коэффициентов сетей Евклида — Хемминга, перейдем к схожей мере, которая дает аналогичные результаты, но ее пороговое значение сложней балансировать:

$$\varepsilon^2 = \sum_{i=1}^{m} \mu_i (E(v_i) - v_i)^2. \qquad (7)$$

Выполнив замену квадрата отклонений признака от его математического ожидания на ξ, перейдем к классическому персептрону

$$\varepsilon^2 = \sum_{i=1}^{m} \mu_i \xi_i + \mu_0, \qquad (8)$$

где $\xi_i = (E(v_i) - v_i)^2$; μ_0 — переключатель квантования.

Классический персептрон можно обучить по ГОСТ Р 52633.5, вычислив весовые коэффициенты в соответствии с формулой

$$\mu_i = |E_{ч}(\xi_i) - E_{с}(\xi_i)| / \sigma_{ч}(\xi_i)\sigma_{с}(\xi_i), \quad (9)$$

где $E_{ч}(\xi_i)$ — математическое ожидание квадрата отклонений значений признака от его математического ожидания для образа «Чужой»; $\sigma_{ч}(\xi_i)$ — среднеквадратическое отклонение данных величин для образа «Чужой»; $E_{с}(\xi_i)$ и $\sigma_{с}(\xi_i)$ — аналогичные показатели для образа «Свой».

Выбор метода распознавания образов зависит от корреляционной зависимости между признаками, значения которых поступают на входы функционалов. Метрика Пирсона лучше работает с признаками, взаимная корреляционная зависимость которых незначительна (модуль коэффициента корреляции менее 0,3 [19]). Для персептронов коэффициент корреляции между признаками не должен превышать 0,7 [17], так как в противном случае эффект накопления ошибок будет многократно усиливаться. В работе [20] показано, что на малых выборках биометрических данных погрешность оценки корреляции между признаками очень значительна. На практике нельзя требовать от пользователя вводить слишком много обучающих примеров (более 30–40) для настройки биометрической системы, так как это сделает процедуру обучения неприемлемо долгой (по требованиям ГОСТ Р 52633.5 [14] для обучения персептронов достаточно 21 образца данных «Свой», при таком количестве наблюдаются погрешности при вычислении коэффициентов корреляции ±0,65 [20]). Поэтому подобрать признаки, коэффициент корреляции между которыми не превысит критических значений для определенного функционала, часто не удается и приходится использовать все признаки.

Результаты верификации образов сетями персептронов, Евклида — Хемминга и сетями квадратичных форм (8) (взвешенных мер Евклида — Хемминга с обучением по ГОСТ Р 52633.5) решено также сравнить с получаемыми сетью метрик хи-модуль [18]:

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

которая ведет себя схожим образом с мерой Пирсона [18], но при отсутствии признака в векторе значений проявляются существенные различия. Нейроны на основе функционалов (3) и (8) имеют нулевые пороговые значения, для нейронов на базе мер Евклида и хи-модуль оптимальные пороговые значения настраиваются эмпирически, исходя из откликов на обучающие примеры «Свой» при обучении и откликов на образы «Чужой» в процессе проведения последующего вычислительного эксперимента (по аналогии с [2]). Независимо от функционала если во входном векторе отсутствуют какие-либо признаки (этому подвержены используемые в настоящем исследовании параметры голоса), то соответствующие входы нейрона игнорируются.

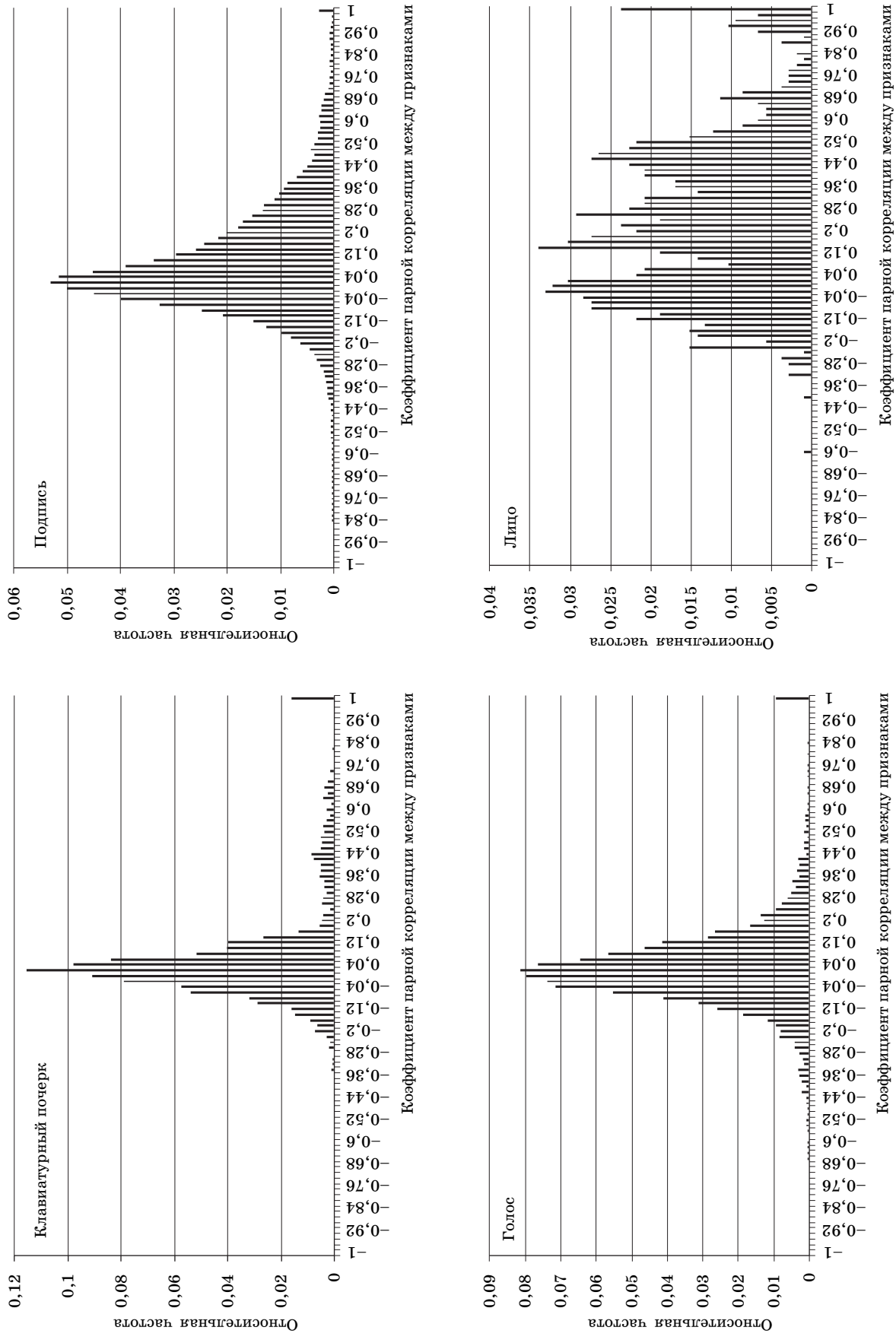
Экспериментальное сравнение рассматриваемых подходов при построении однофакторных и многофакторных биометрических систем

Проведен вычислительный эксперимент на основе имеющейся базы биометрических образов с использованием сетей персептронов, Евклида — Хемминга, Евклида — Хемминга с обучением по ГОСТ Р 52633.5 и хи-модуль-сетей. Для формирования эталонов использовалось по 21 образу каждого субъекта (и по одному образу всех субъектов в качестве данных «Чужой» для обучения персептронов). Остальные образы использовались для распознавания (генерации ключей). Вероятности ошибок 1-го и 2-го рода подсчитывались в следующем виде: $FRR = er_1/ex_1$, $FAR = er_2/ex_2$, где er — количество ошибок соответствующего рода; ex — количество опытов для выявления ошибки соответствующего рода. Проведена оценка взаимной корреляционной зависимости используемых признаков, исходя из которой различные сети могут работать по-разному (рис. 1 и 2). Конечный результат зависит также от количества и информативности признаков, которая определяется схожестью распределений значений признаков для одного субъекта и их различием для разных субъектов.

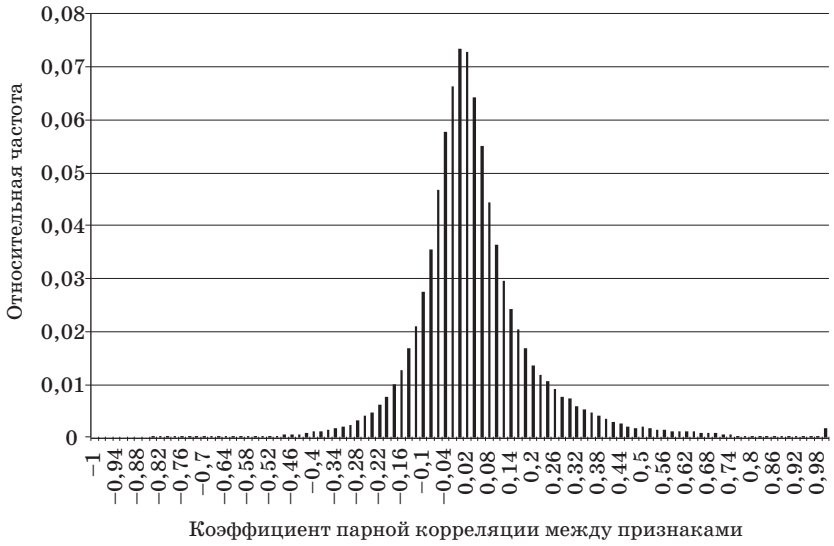
Результаты эксперимента представлены на рис. 3–6 и в табл. 2.

Отметим, что при увеличении числа нейронов сети N можно повышать надежность верификации, пока нейроны допускают различные ошибки (если их выходы не слишком коррелированы). При этом увеличивается длина генерируемого сетью ключа. Повышать длину ключа имеет смысл, пока его энтропия не перестанет возрастать [15].

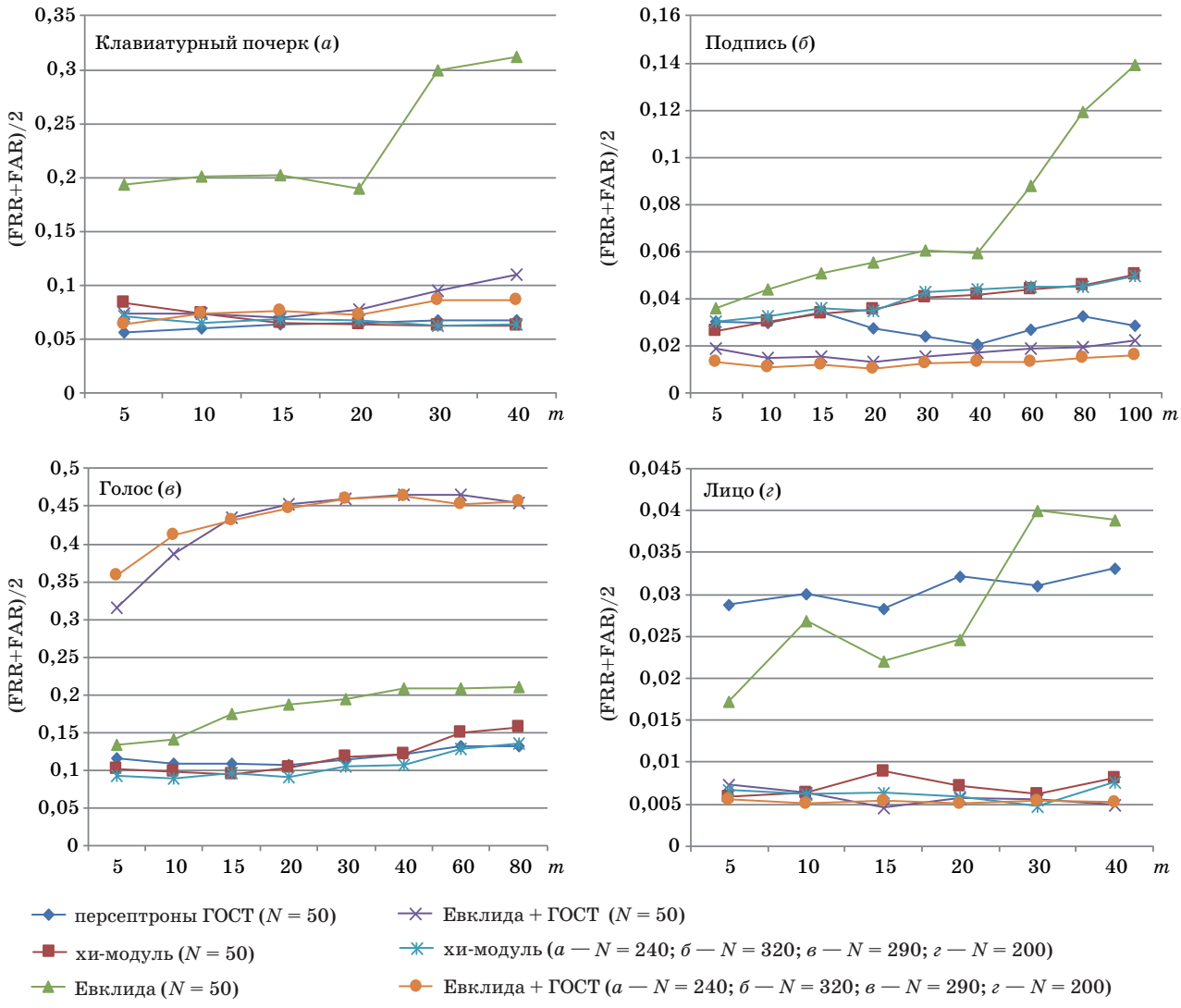
Из рис. 3 видно, что вероятности ошибок верификации сетями квадратичных форм были значительны ($>0,3$) для случая, когда на входы сети поступали признаки речи. Это обусловлено отсутствием некоторых голосовых признаков в векторе их значений. Сети персептронов и метрик хи-модуль ведут себя иным образом. Для персептрона (3) отсутствие признака эквивалентно поступлению его нулевого значения. Величина ошибки метрик (6) и (10) меньше в $(E(v_i) - v_i)/\sigma_{с}(v_i)$ раз. Вследствие чего зарегистрированы существенно более низкие вероятности ошибок распознавания



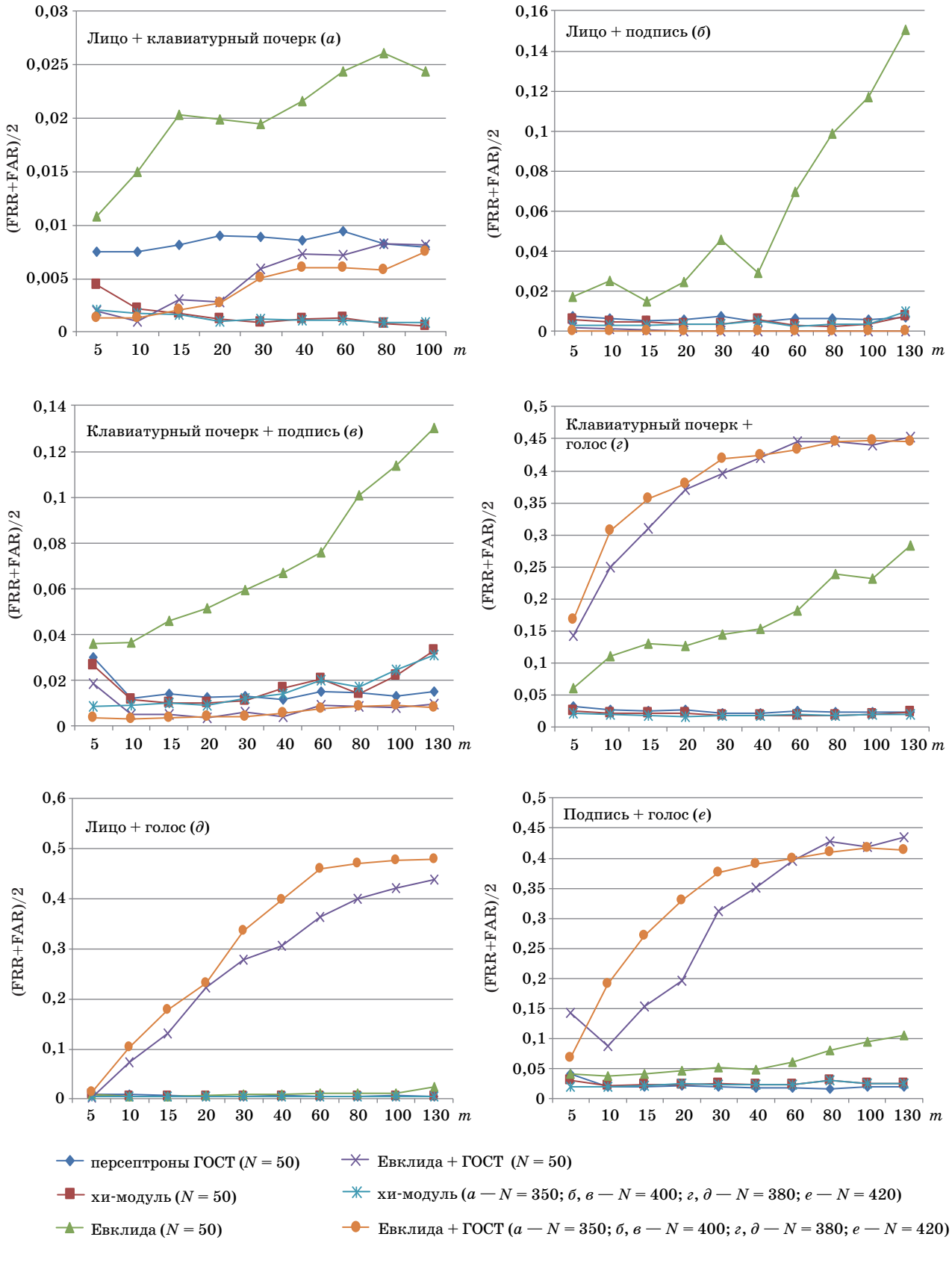
■ *Рис. 1.* Взаимная корреляционная зависимость признаков



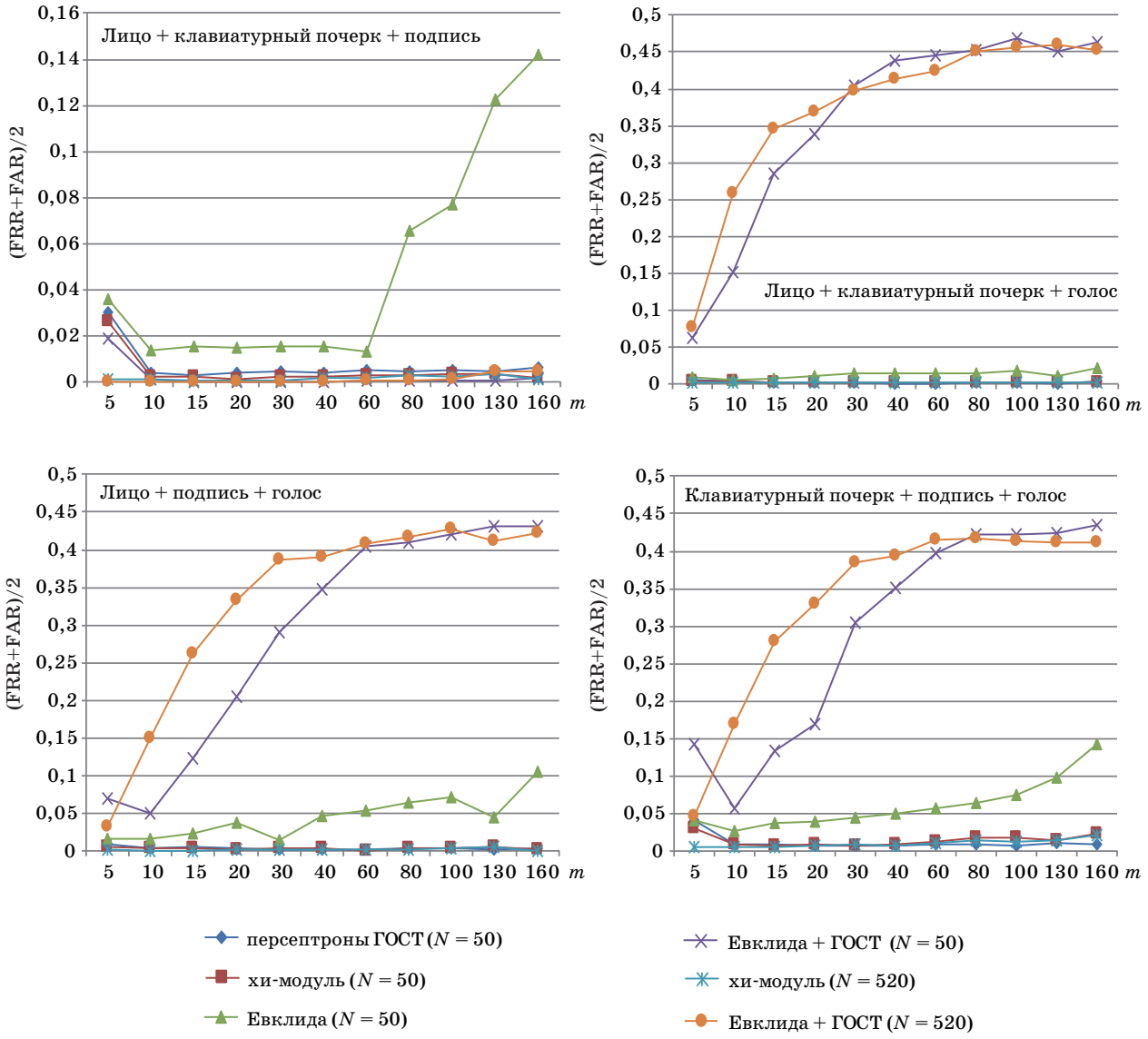
■ ***Рис. 2.*** Взаимная корреляционная зависимость всех рассмотренных признаков при их совместном использовании (комплексировании)



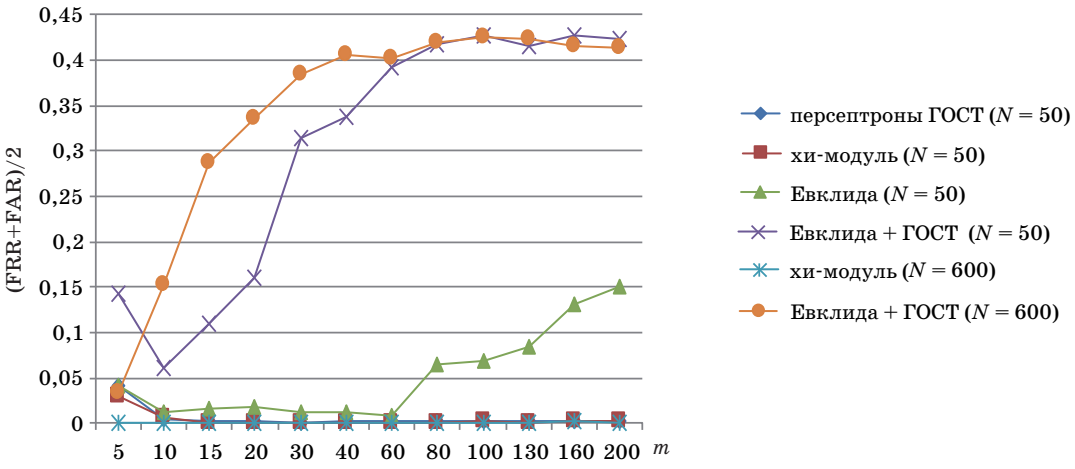
■ ***Рис. 3.*** Результаты распознавания субъектов однофакторными системами



■ ***Рис. 4.*** Результаты распознавания субъектов двухфакторными системами



■ ***Рис. 5.*** Результаты распознавания субъектов трехфакторными системами



■ ***Рис. 6.*** Результаты распознавания субъектов четырехфакторными системами

■ ***Таблица 2***. Наилучшие показатели ошибок генерации и длины кодов

Признаки	Тип сети	FRR	FAR	Длина кода, бит
Клавиатурный почерк	хи-модуль	0,055	0,0694	240
Подпись	Евклида + ГОСТ	0,0126	0,0083	320
Голос	хи-модуль	0,118	0,062	290
Лицо	хи-модуль	0,0033	0,0061	200
Лицо + клавиатурный почерк	хи-модуль	≈0	0,0018	350
Лицо + подпись	Евклида + ГОСТ	≈0	≈0	400
Клавиатурный почерк + подпись	Евклида + ГОСТ	0,0057	0,0005	400
Клавиатурный почерк + голос	хи-модуль	0,0184	0,0155	380
Лицо + голос	хи-модуль	0,0057	0,0029	380
Подпись + голос	хи-модуль	0,023	0,0189	420
Лицо + клавиатурный почерк + подпись	Евклида + ГОСТ	≈0	≈0	520
Лицо + клавиатурный почерк + голос	хи-модуль	0,0034	0,0006	520
Лицо + подпись + голос	хи-модуль	0,0023	0,0004	520
Клавиатурный почерк + голос + подпись	хи-модуль	0,0057	0,0051	520
Все признаки	хи-модуль	≈0	0,0005	600

(генерации ключа) сетями этих метрик. Однако в большинстве других случаев (без использования признаков голоса) сеть взвешенных мер Евклида показала наилучшие результаты.

Положительный эффект от комплексирования независимых групп признаков (см. рис. 4–6) заключается не только в увеличении их количества, но и в появлении большого числа новых пар параметров с низкой корреляцией (см. рис. 2). Последнее сказалось на улучшении работы всех сетей, особенно квадратичных форм.

Заключение

Применение адаптированного алгоритма обучения сетей персептронов, описанного в ГОСТ Р52633.5-2011 [14], по отношению к сетям квадратичных форм (взвешенных мер Евклида) позволило получить высокие результаты в ряде задач биометрической аутентификации. В частности, удалось достичь вероятностей ошибочных решений по верификации образов субъекта в пространстве признаков подписи около 1 %, клавиатурного почерка и подписи — 0,31 %, признаков лица и подписи — с процентом ошибочных решений, близким к нулю. Использование сетей хи-модуль также позволило получить очень высокий результат во многих случаях: при распознавании субъектов по лицу зарегистрирован процент ошибок менее 0,5 %, лицу совместно с клавиатурным почерком — менее 0,1 % ошибок, лицу, подписи и голосу — около 0,13 %. Полученные результаты превосходят аналоги [21, 22]. Исходя из результатов, можно заключить: методы двух- (без образов голоса), трех- и четырехфакторной верификации образов субъектов, рассмотренные в работе (на основе сетей хи-модуль и сетей квадратичных форм, обученных по адаптированному алгоритму из ГОСТ Р 52633.5), можно использовать на практике при реализации контрольно-пропускной функции или удаленной аутентификации. Однако для этого требуется обеспечить защиту биометрических эталонов (этого требует ГОСТ Р 52633.0-2006 [23]). Подделать все признаки на практике крайне затруднительно, изготовление муляжа более двух видов образов одновременно можно считать неосуществимым. Пространство признаков голоса субъектов требует дополнительной проработки, так как в рассмотренном в работе виде не дает желаемого результата.

Работа выполнена при финансовой поддержке РФФИ (грант № 15-07-09053).

Литература

1. Moving Forward with Cybersecurity and Privacy. http://www.pwc.ru/ru/riskassurance/publications/assets/gsiss-report_2017_eng.pdf (дата обращения: 11.12.2016).
2. **Ложников П. С.** и др. 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. doi:10.15217/issn1684-8853.2016.5.73
3. **Lozhnikov P. S.,** et al. Methods of Generating Key Sequences based on Parameters of Handwritten Passwords and Signatures / P. S. Lozhnikov, A. E. Su-

lavko, A. V. Eremenko, D. A. Volkov // Information. 2016. N 7. P. 59. doi:10.3390/info7040059
4. **Daubechies I.** Ten Lectures on Wavelets. — Philadelphia: S.I.A.M., 1992. — 357 p.
5. **Иванов А. И.** Биометрическая идентификация личности по динамике подсознательных движений. — Пенза: Изд-во Пенз. гос. ун-та, 2000. — 188 с.
6. **Васильев В. И.** и др. 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.
7. **Viola P. and Jones M.** Rapid Object Detection Using a Boosted Cascade of Simple Features//Computer Vision and Pattern Recognition CVPR: Proc. of the 2001 IEEE Computer Society Conf. 2001. Vol. 1. P. 511–518.
8. **Hough P. V. C.** A Method and Means for Recognizing Complex Patterns. Patent U. S., no. 3.069.654, 1962.
9. **Ворона В. А., Тихонов В. А.** Системы контроля и управления доступом. — М.: Горячая линия-Телеком, 2010. — 272 с.
10. **Сулавко А. Е., Еременко А. В., Борисов Р. В.** Генерация криптографических ключей на основе голосовых сообщений // Прикладная информатика. 2016. № 5. С. 76–89.
11. **Dodis Y., Reyzin L.** A. Smith Fuzzy Extractors: How to Generate Strong Keys from Biometrics and Other Noisy // EUROCRYPT. April 2004. P. 523–540.
12. **Juels A., Sudan M.** A Fuzzy Vault Scheme // IEEE International Symposium on Information Theory. 2002. P. 408–425.
13. **Juels A., Wattenberg M.** A Fuzzy Commitment Scheme // Proc. ACM Conf. Computer and Communications Security. 1999. P. 28–36.
14. ГОСТ Р 52633.5-2011. Защита информации. Техника защиты информации. Автоматическое обучение нейросетевых преобразователей биометрия-код доступа. — М.: Стандартинформ, 2011. — 20 с.
15. **Ахметов Б. С.** и др. 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: Издательство LEM, 2014. — 144 с.
16. **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. С. 4–13.
17. **Иванов А. И.** Нейросетевые алгоритмы биометрической идентификации личности. — М.: Радиотехника, 2004. — 144 с.
18. **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.
19. **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.
20. **Иванов А. И., Ложников П. С., Серикова Ю. И.** Снижение размеров достаточной для обучения выборки за счет симметризации корреляционных связей биометрических данных // Кибернетика и системный анализ. 2016. № 3. С. 49–56.
21. **Еременко А. В., Сулавко А. Е., Волков Д. А.** Современное состояние и пути модернизации преобразователей биометрия-код // Информационные технологии. 2016. № 3. С. 203–210.
22. **Васильев В. И.** и др. 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.
23. ГОСТ Р 52633.0-2006. Защита информации. Техника защиты информации. Требования к средствам высоконадежной биометрической аутентификации. — М.: Стандартинформ, 2006. — 24 с.

UDC 004.93′1
doi:10.15217/issn1684-8853.2017.1.50

Complexation of Independent Biometric Features in People Recognition with Quadratic Forms, Perceptrons and Functional Hee-module

Sulavko A. E.[a], PhD, Tech., Senior Lecturer, sulavich@mail.ru
Eremenko A. V.[b], PhD, Tech., Associate Professor, nexus-@mail.ru
Tolkacheva E. V.[b], PhD, Tech., Associate Professor, tolkacheva_ev@mail.ru
Borisov R. V.[c], Post-Graduate Student, brv1986@yandex.ru
[a]Omsk State Technical University, 11, Mira Pr., 644050, Omsk, Russian Federation
[b]Omsk State Transport University, 35, Karl Marx Pr., 644046, Omsk, Russian Federation
[c]Siberian State Automobile and Highway Academy, 5, Mira Pr., Omsk, 644080, Russian Federation

Introduction: Static biometric features are not a secret and can be falsified, so the search for effective methods of authenticating people by their dynamic biometric characteristics is a very important problem. **Purpose:** The aim is to develop more reliable methods for one- and multi-factor biometric authentication using uninformative features. **Results:** A series of numerical experiments were

conducted on the basis of biometric data of a signature, keyboard handwriting, faces and voices of people using perceptrons networks, quadratic forms and functional Hee-module. An error level for the user verification by handwriting dynamics is about 1%, an error for the user verification by keyboard signature and handwriting dynamics is about 0.31%, face image gives an error level less than 0.5%, face and keyboard signature gives an error level less than 0.1%, using 3- and 4-factor verification gives 0,54–0,01% error level. **Practical relevance:** Methods of two- (without voice features), three- and four-factor user verification discussed in the paper can be used in practice for the implementation of a remote authentication function. Forging features of more than two kinds of images can be considered practically impossible.

Keywords — Parameters of Signature, Keyboard Signature, Voice Characteristics, Personal Physiological Characteristics, Biometrics, Artificial Neural Network, Quadratic Forms, Pattern Recognition Algorithms.

References

1. Moving Forward with Cybersecurity and Privacy. Available at: http://www.pwc.ru/ru/riskassurance/publications/assets/gsiss-report_2017_eng.pdf (accessed 11 December 2016).
2. Lozhnikov P. S., Sulavko A. E., Eremenko A. V., Volkov D. A. Experimental Evaluation of Reliability of Signature Verification by Quadratic Form Networks, Fuzzy Extractors and Perceptrons. *Informatsionno-upravliaiushchie sistemy* [Information and Control Systems], 2016, no. 5, pp. 73–85 (In Russian). doi:10.15217/issn1684-8853.2016.5.73
3. Lozhnikov P. S., Sulavko A. E., Eremenko A. V., Volkov D. A. Methods of Generating Key Sequences based on Parameters of Handwritten Passwords and Signatures. *Information*, 2016, no. 7, p. 59. doi:10.3390/info7040059
4. Daubechies I. *Ten Lectures on Wavelets*. Philadelphia, S.I.A.M., 1992. 357 p.
5. Ivanov A. I. *Biometricheskaia identifikatsiia lichnosti po dinamike podsoznatel'nykh dvizhenii* [Biometric Identification of the Person on the Dynamics of Subconscious Movements]. Penza, Penzenskii gosudarstvennyi universitet Publ., 2000. 188 p. (In Russian).
6. Vasil'ev V. I., Lozhnikov P. S., Sulavko A. E., Zhumazhanova S. S. Evaluation of Identification Capability of Biometric Features from a Standard Peripheral Equipment. *Voprosy zashchity informatsii*, 2016, no. 1, pp. 12–20 (In Russian).
7. Viola P. and Jones M. Rapid Object Detection using a Boosted Cascade of Simple Features. *Proc. of the 2001 IEEE Computer Society Conf. "Computer Vision and Pattern Recognition", CVPR*, 2001, vol. 1, pp. 511–518.
8. Hough P. V. C. A Method and Means for Recognizing Complex Patterns. Patent U. S., no. 3.069.654, 1962.
9. Vorona V. A., Tikhonov V. A. *Sistemy kontrolia i upravleniia dostupom* [Access Control Systems]. Moscow, Goriachaia liniia-Telekom Publ., 2010. 272 p. (In Russian).
10. Sulavko A. E., Eremenko A. V., Borisov R. V. Cryptographic Keys Generated on the Basis of Voice Messages. *Prikladnaia informatika*, 2016, no. 5, pp. 76–89 (In Russian).
11. Dodis Y., Reyzin L. A. Smith Fuzzy Extractors: How to Generate Strong Keys from Biometrics and Other Noisy. *EUROCRYPT*, April 2004, pp. 523–540.
12. Juels A., Sudan M. A Fuzzy Vault Scheme. *IEEE Intern. Symp. on Information Theory*, 2002, pp. 408–425.
13. Juels A., Wattenberg M. A Fuzzy Commitment Scheme. *Proc. ACM Conf. Computer and Communications Security*, 1999, pp. 28–36.
14. 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).
15. Akhmetov B. S., Ivanov A. I., Funtikov V. A., Beziaev A. V., Malygina E. A. *Tekhnologiia ispol'zovaniia bol'shikh neironnykh setei dlia preobrazovaniia nechetkikh biometricheskikh dannykh v kod kliucha dostupa* [Technology is the Use of Large Neural Networks for Fuzzy Transformation of Biometric Data in the Access Code Key]. Almaty, Izdatel'stvo LEM Publ., 2014. 144 p. (In Russian).
16. Beziaev A. V., Ivanov A. I., Funtikova Iu. V. Optimization of the Structure of Bio-Self-Correcting Code Storing Error Syndromes as Fragments Hash Functions. *Vestnik UrFO. Bezopasnost' v informatsionnoi sfere*, 2014, no. 3, pp. 4–13 (In Russian).
17. Ivanov A. I. *Neirosetevye algoritmy biometricheskoi identifikatsii lichnosti* [Neural Network Algorithms for Biometric Identification]. Moscow, Radiotekhnika Publ., 2004. 144 p. (In Russian).
18. Lozhnikov P. S., Ivanov A. I., Kachaikin E. I., Sulavko A. E. Biometric Identification of Manuscript Images Using Analog Correlation Bayes Rule. *Voprosy zashchity informatsii*, 2015, no. 3, pp. 48–54 (In Russian).
19. Ivanov A. I., Lozhnikov P. S., Kachaikin E. I. Identification of the Authenticity of the Manuscript Autographs Networks Bayesian Networks and Hamming Quadratic Forms. *Voprosy zashchity informatsii*, 2015, no. 2, pp. 28–34 (In Russian).
20. Ivanov A. I., Lozhnikov P. S., Serikova Iu. I. Reducing the Size of the Sample Sufficient for Training by Symmetrization Correlations Biometric Data. *Kibernetika i sistemnyi analiz*, 2016, no. 3, pp. 49–56 (In Russian).
21. Eremenko A. V., Sulavko A. E., Volkov D. A. Current Status and the Modernization Converters Biometrics-Code. *Informatsionnye tekhnologii*, 2016, no. 3, pp. 203–210 (In Russian).
22. Vasil'ev V. I., Lozhnikov P. S., Sulavko A. E., Eremenko A. V. Technology Hidden Biometric Identification of Users of Computer Systems. *Voprosy zashchity informatsii*, 2015, no. 3, pp. 37–47 (In Russian).
23. State Standard R 52633.0-2006. Data Protection. Information Protection Technique. Requirements for Highly Reliable Means of Biometric Authentication. Moscow, Standartinform Publ., 2006. 24 p. (In Russian).