

16. *Bespalov D.A.* Parallel'naya realizatsiya algoritmov veyvlet-analiza na mnogoprotsessornykh klasterakh [Parallel implementation of algorithms for wavelet analysis on multiprocessor clusters], *Izvestiya vysshikh uchebnykh zavedeniy. Severo-Kavkazskiy region. Seriya: Tekhnicheskie nauki* [University News. North-Caucasian Region. Technical Sciences Series], 2007, No. 1, pp. 11-14.
17. *Bespalov D.A.* Veyvlet-fil'tratsiya signalov adaptivnymi porogami [Wavelet filtering of signals and adaptive thresholds], *Izvestiya vysshikh uchebnykh zavedeniy. Severo-Kavkazskiy region. Seriya: Tekhnicheskie nauki* [University News. North-Caucasian Region. Technical Sciences Series], 2007, No. 2, pp. 13-15.
18. *Veitch D. & Abry P.* A wavelet-based joint estimator of the parameters of long-range dependence, *IEEE Trans. Info. Theo.*, 1999, Vol. 45, pp. 878-897.
19. *Paladin G. & Vulpiani A.* Anomalous scaling laws in multifractal objects, *Phys. Rep.*, 1987, Vol. 156, pp. 147-225.
20. *Muzy J.-F., Bacry E. & Arneodo A.* Wavelets and multifractal formalism for singular signals: Application to turbulence data, *Phys. Rev. Lett.*, 1991, Vol. 67, pp. 3515-3518.

Статью рекомендовал к опубликованию д.т.н. Н.И. Витиска.

Беспалов Дмитрий Анатольевич – Южный федеральный университет; e-mail: bda82@mail.ru; 347928, г. Таганрог, ул. Чехова, 2, корп. «И»; тел.: 89604661762; кафедра вычислительной техники; доцент.

Bespalov Dmitry Anatolyevich – Southern Federal University; e-mail: bda82@mail.ru; 2, Chekhov street, build. "I", Taganrog, 347928, Russia; phone: +79604661762; the department of computer science; associate professor.

УДК 004.067

DOI 10.23683/2311-3103-2017-5-56-66

Ю.А. Брюхомицкий

ИММУНОЛОГИЧЕСКИЙ ПОДХОД К ИДЕНТИФИКАЦИИ ЛИЧНОСТИ ПО ДИНАМИЧЕСКИМ БИОМЕТРИЧЕСКИМ ПАРАМЕТРАМ

Предлагается обобщенный иммунологический подход к решению задачи – идентификации личности человека по его динамическим биометрическими характеристикам различной модальности: голосу, рукописи, клавиатурному набору. Подход ориентирован на идентификацию личности человека при воспроизведении им текстов произвольного объема и содержания. Решение поставленной задачи базируется на принципах построения и функционирования искусственных иммунных систем, с использованием векторного представления и обработки биометрических данных, хорошо согласующегося с числовым характером сигналов динамической биометрии. Особенностью подхода является представление сигналов динамической биометрии последовательностями информационных единиц фиксированного формата, с последующей их децентрализованной обработкой на основе иммунологической модели отщипывания отбора. Информационными единицами последовательностей являются синтаксически связанные фрагменты текста, несущие наиболее выраженные индивидуальные особенности личности. Последующий анализ и обработка фрагментов текста осуществляется в многомерном метрическом пространстве признаков. Распознавание образов динамической биометрии, представленных фрагментами текста, реализуется путем их сопоставления с распознающими элементами – детекторами. Сопоставление осуществляется по принципу негативной селекции. Рассмотрены возможные для использования две разновидности детекторов. Первые представлены в пространстве признаков многомерными векторами (простые детекторы), вторые – многомерными сферами (объемные детекторы). Предложены вычислительная процедура формирования объемных детекторов на стадии обучения и процедура сопоставления сигналов динамической биометрии с объемными детекторами на стадии идентификации. Предлагаемый подход в рамках иммунологического представления позволяет обобщить существенно различные применяемые методы идентификации личности по динамическим биометрическим параметрам разной

модальности – голоса, рукописи и клавиатурного набора. Отличием подхода является возможность текстонезависимого анализа текстов различной модальности, произвольного объема и содержания. Другим отличием является переход от интегральной оценки результатов анализа биометрических данных за фиксированный период времени к непрерывной оценке данных в темпе их поступления, с возможностью своевременного принятия правильного решения.

Текстонезависимая идентификация личности; динамическая биометрия; искусственные иммунные системы; векторное представление данных.

Yu.A. Bryukhomitsky

IMMUNOLOGICAL APPROACH TO PERSONALITY IDENTIFICATION BY DYNAMIC BIOMETRIC PARAMETERS

The generalized immunological approach of solving the problem of personality identification by its dynamic biometric characteristics of different modalities: voice, penscript, keyboard set, is offered. The approach is oriented to the personality identification while reproducing by the person of texts of arbitrary volume and content. The solution of this task is based on the principles of constructing and functioning of artificial immune systems, using vector representation and processing of biometric data, good conforming to the numerical character of the signals of dynamic biometry. A special feature of the approach is the presentation of signals of dynamic biometry by sequences of information units of fixed format, with their following decentralized processing based on the immunological model of negative selection. Informational units of sequences are syntactically related fragments of the text, carrying the most expressed individual characteristics of personality. The following analysis and processing of text fragments are carried out in the multidimensional metric space of attributes. Recognition of images of dynamic biometry, represented by text fragments, is realized by their comparison with recognizing elements - detectors. The comparison is carried out on the principle of negative selection. Two possible types of detectors are considered. The former are represented in the feature space by multidimensional vectors (simple detectors), the latter – by multidimensional spheres (volumetric detectors). A computational procedure for the formation of volumetric detectors at the learning stage and a procedure for comparing the signals of dynamic biometry with volumetric detectors at the identification stage are proposed. The proposed approach in the context of the immunological presentation allows us to generalize essentially different methods of identification of a person using the dynamic biometric parameters of different modalities - voice, penscript and keyboard set. The difference of approach is the possibility of text-independent analysis of texts of different modality, arbitrary volume and content. Another difference is the transition from an integrated evaluation of the results of the analysis of biometric data over a fixed period of time to a continuous evaluation of data at the rate of their receipt, with the possibility of timely making the right decision.

Text-independent personality identification; dynamic biometry; artificial immune systems; vector data representation.

Введение. Динамические системы биометрической идентификации личности (динамическая биометрия) основаны на анализе индивидуальных особенностей хорошо заученных подсознательных движений человека. Практическое применение в настоящее время получили системы анализа голоса [1–3], рукописи [4–8] и клавиатурного почерка [9–12]. Динамическая биометрия используется преимущественно как средство аутентификации личности при входе в компьютерные и мобильные системы, а также для удаленной (голосовой) аутентификации. Процедура аутентификации личности сводится к предъявлению парольной фразы, воспроизведенной голосом, рукописью на графическом планшете или набранной на клавиатуре.

Главным достоинством этих систем является низкая стоимость, обусловленная тем, что они могут быть построены исключительно программными средствами, или с использованием стандартных уже имеющихся на компьютере средств мультимедиа. Еще одним важным достоинством динамической биометрии является возможность сохранения образа личности в тайне и возможность быстрой смены этого образа за счет смены парольной фразы.

Недостатком динамической биометрии является меньшая, по сравнению со статической биометрией, точность идентификации и влияние на результат психофизического состояния личности (испуг, стресс, психотропные препараты и т.п.). Эти недостатки в значительной степени ограничивают практическое применение динамической биометрии.

Вместе с тем, существует другая, перспективная область применения динамической биометрии – текстонезависимая идентификация личности. В этой области указанные недостатки, или не имеют решающего значения, или, напротив, плодотворно используются. Круг задач, которые можно решать с помощью текстонезависимой динамической биометрии отличается от классической задачи аутентификации личности:

- ◆ верификация и идентификация личности (голосовая, рукописная и клавиатурная биометрия);
- ◆ непрерывная скрытная верификация пользователей компьютерных систем (клавиатурная биометрия);
- ◆ скрытное выявление инсайдеров – легальных пользователей компьютерных систем, совершающих неправомерные действия (клавиатурная биометрия);
- ◆ скрытное выявление психофизических отклонений состояния человека от нормативного (голосовая, рукописная и клавиатурная биометрия);
- ◆ контроль правдивости ответов на заданные вопросы («детектор лжи») (голосовая, рукописная и клавиатурная биометрия).

Процедура анализа входных биометрических данных в этом случае производится без использования парольной фразы, по любому тексту, воспроизводимому голосом, рукописью или на клавиатуре. Техники идентификации личности в таких системах существенно отличаются от техник, применяемых в системах биометрической аутентификации по парольной фразе.

В текстонезависимой динамической биометрии эталоны личности строятся на основе достаточно больших образцов текста соответствующей модальности (голос, рукопись, клавиатурный набор). При этом возникает ряд принципиальных проблем:

- ◆ необходимость хранения и использования биометрических эталонов большой размерности;
- ◆ трудности определения и извлечения из больших биометрических эталонов с произвольными образцами текста индивидуальных особенностей двигательных функций личности;
- ◆ трудности сопоставления идентифицируемых образцов динамической биометрии с эталонами;

Постановка задачи. Общей особенностью текстонезависимой динамической биометрии является представление исходных данных сигналами (функциями времени) структура которых содержит все необходимые для идентификации индивидуальные особенности личности. Решение задачи распознавания таких сигналов классическими методами осуществляется в два этапа. На первом этапе осуществляется преобразование сигналов в какое-либо статическое представление: в частотной области (разложения Фурье, Уолша, Хаара и др.); в частотно-временной области (вейвлет-преобразование); временной области (коэффициентами линейного цифрового фильтра) и др. Затем в формате статического представления решается собственно задача распознавания биометрических образов.

В данной работе предлагается иной подход к решению указанной задачи, базирующийся на принципах построения и функционирования искусственных иммунных систем (ИИС) [13–15], с векторным представлением иммунологических данных, хорошо согласующимся с числовым характером сигналов динамической биометрии.

Особенностью подхода является представление сигналов динамической биометрии в виде последовательности информационных единиц определенного формата, с последующей их децентрализованной обработкой на основе иммунологической модели отрицательного отбора [16, 17]. Информационные единицы при этом имитируют иммунокомпетентные клетки иммунной системы лимфоциты, которые отвечают за распознавание специфических «чужих», а также неизвестные, подлежащие распознаванию клетки, которые могут быть как «своими», так и «чужими» (антигенами). Такое представление имитирует массово-параллельную обработку информации на уровне клеток, наблюдаемую в иммунной системе.

Решение поставленной задачи. Воспроизведение произвольного текста средствами динамической биометрии любой модальности реализуется совокупностью заученных подсознательных движений, которые преобразуются в электрические сигналы (функции времени) с возможным добавлением шума (голосовые системы). В голосовой биометрии эти сигналы, как правило, одномерные, в рукописной биометрии – многомерные (мерность определяется числом учитываемых степеней свободы пера дигитайзера), в клавиатурной биометрии сигналы могут быть и одномерными и многомерными (зависит от выбранного метода представления параметров). В общем случае можно считать сигнал динамической биометрии многомерным: $\mathbf{x}(t) = x_1(t), x_2(t), \dots, x_n(t)$.

На этапе предварительной обработки сигнал $\mathbf{x}(t)$ оцифровывается $\mathbf{x}(t) \rightarrow \mathbf{x}(t_i) = \mathbf{x}(i)$, $i = 1, 2, \dots$, масштабировается (нормируются), из него исключаются длительные паузы, не обусловленные индивидуальными особенностями воспроизведения текста. В голосовой биометрии исключаются также неинформативные (с точки зрения распознавания) фонемы шипящих звуков.

Отсчеты сигнала $\mathbf{x}(i)$, $i = 1, 2, \dots$ можно рассматривать как точки метрического пространства E^n , представленные векторами признаков $\mathbf{x}_i = x_{1i}, x_{2i}, \dots, x_{ni}$, а сам сигнал $\mathbf{x}(i)$, – как последовательность $\mathbf{A}_{xi} = a_{x1}, a_{x2}, \dots$ элементов, представленных векторами признаков: $a_{xi} = \mathbf{x}_i$, $i = 1, 2, \dots$. В математическом смысле последовательность \mathbf{A}_{xi} «пробегают» конечное множество Ψ_x векторов признаков a_{xi} биометрии данной личности.

Содержательный смысл размерности n векторов признаков определяется числом учитываемых биометрических параметров в одном элементе a_{xi} последовательности \mathbf{A}_{xi} . Например, в голосовых системах n может соответствовать одному отсчету речевого сигнала. В рукописных системах n может соответствовать числу учитываемых в каждом отсчете степеней свободы колебаний пера [7, 8]. В клавиатурных системах n может соответствовать времени удержания клавиши или времени паузы [12].

При текстонезависимом анализе биометрических данных используются достаточно большие размеры произвольного текста, необходимые для получения приемлемого уровня точности идентификации. Поэтому анализ последовательности \mathbf{A}_{xi} векторов признаков a_{xi} в темпе $i = 1, 2, \dots$ их первичного цифрового представления приведет к чрезмерно высоким вычислительным затратам. Это обуславливает необходимость применения вторичного временного квантования сигналов $\mathbf{x}(i)$:

$$\mathbf{x}(i) \rightarrow \mathbf{x}(j), j = m \cdot i = 1, 2, \dots,$$

где i – исходный шаг квантования по времени; j – шаг вторичного квантования по времени; m – коэффициент вторичного квантования.

Шаг вторичного квантования j выбирается как компромисс между стремлением сохранить точность представления, достаточную для отражения индивидуальности автора, и допустимыми вычислительными затратами на обработку элементов a_{xj} последовательности \mathbf{A}_{xj} .

Исследования в области динамической биометрии, в частности, в клавиатурной [18–19], показывают, что индивидуальные особенности личности в наибольшей степени проявляются при воспроизведении не одиночных символов текста (в голосовой биометрии – фонем), а синтаксически связанных фрагментов текста (в голосовой биометрии речи). Использование этого феномена при анализе позволит строить системы текстонезависимой биометрической идентификации личности с существенно более высокими характеристиками точности.

Следуя указанному подходу к анализу, разобьем последовательность \mathbf{A}_{xi} на фрагменты одинакового размера по r отсчетов в каждом фрагменте.

Результатом будет новая последовательность $\mathbf{A}_{yk} = \mathbf{a}_{y1}, \mathbf{a}_{y2}, \dots, k = 1, 2, \dots$, каждый элемент \mathbf{a}_{yk} которой будет фрагментом исходной последовательности \mathbf{A}_{xi} , представленным совокупностью r векторов:

$$\begin{aligned} \mathbf{x}_{1j} &= x_{11}, x_{12}, \dots, x_{1n}; \\ \mathbf{x}_{2j} &= x_{21}, x_{22}, \dots, x_{2n}; \\ &\dots \dots \dots \dots \dots \dots \\ \mathbf{x}_{rj} &= x_{r1}, x_{r2}, \dots, x_{rn}. \end{aligned}$$

Векторы $\mathbf{x}_{1j}, \mathbf{x}_{2j}, \dots, \mathbf{x}_{rj}$ можно объединить в один-мерный вектор \mathbf{a}_{yk} , содержащий $s = n \times r$ компонентов:

$$\mathbf{a}_{yk} = \begin{bmatrix} a_{y11} & a_{y12} & \dots & a_{y1r} \\ a_{y21} & a_{y22} & \dots & a_{y2r} \\ \dots & \dots & \dots & \dots \\ a_{yn1} & a_{yn2} & \dots & a_{ynr} \end{bmatrix}, \quad p = 1, 2, \dots, n, \quad q = 1, 2, \dots, r, \quad k = 1, 2, \dots$$

В итоге, образы динамической биометрии будут представлены последовательностью \mathbf{A}_{yk} s -мерных векторов признаков \mathbf{a}_{yk} в пространстве признаков E^s .

Содержательный смысл параметра r в векторах признаков определяется числом учитываемых в одном фрагменте последовательных отсчетов последовательности \mathbf{A}_{yk} . Например, в голосовых системах r может соответствовать числу последовательных отсчетов речевого сигнала, приходящихся на один фрагмент, или числу коэффициентов частотного (или волнового) разложения сигнала на периоде одного фрагмента [1]. В рукописных системах r может соответствовать числу последовательных отсчетов колебаний пера в n степенях свободы, приходящихся на один фрагмент, или числу коэффициентов частотного разложения сигнала на периоде одного фрагмента [7, 8]. В клавиатурных системах r может соответствовать длине цепочки последовательно наступающих клавиатурных событий (удержаний клавиш и пауз между удержаниями) приходящихся на один фрагмент [18, 19].

Последовательность биометрических признаков \mathbf{A}_{yk} , ограниченная N_a элементами

$$\bar{\mathbf{A}}_{yk} = \mathbf{a}_{y1}, \mathbf{a}_{y2}, \dots, \mathbf{a}_{yN_a}, \quad k = 1, 2, \dots, N_a,$$

трактуются как биометрический эталон личности.

В отличие от классических методов распознавания образов, основанных на сопоставлении образов с эталоном, предлагается использовать иммунологическую модель отрицательного отбора, которая реализует децентрализованное распознавание образов, путем их сопоставления со специальными распознающими элементами – детекторами. Сопоставление осуществляется по принципу негативной селекции (срабатывание детектора свидетельствует о том, что предъявленный образ существенно отличается от эталона) [16–22].

Детекторы имитируют иммунокомпетентные клетки – лимфоциты, которые отвечают за распознавание специфических «чужих», т.е. не известных иммунной системе молекул (антигенов).

Популяция детекторов \mathbf{D} создается в метрике векторов \mathbf{a}_{yk} эталона $\bar{\mathbf{A}}_{yk}$:

$$\mathbf{D} = \{\mathbf{d}_i\} = \mathbf{d}_1, \mathbf{d}_2, \dots, \mathbf{d}_{N_d}, \quad i = 1, 2, \dots, N_d;$$

$$\mathbf{d}_i = \begin{bmatrix} d_{i11} & d_{i12} & \dots & d_{i1r} \\ d_{i21} & d_{i22} & \dots & d_{i2r} \\ \dots & \dots & \dots & \dots \\ d_{in2} & d_{in2} & \dots & d_{inr} \end{bmatrix}, \quad p = 1, 2, \dots, n, \quad q = 1, 2, \dots, r, \quad i = 1, 2, \dots, N_d.$$

Для распознавания «чужих» детекторы \mathbf{d}_i должны быть представлены векторами признаков, отличающимися от векторов признаков эталона \mathbf{a}_{yk} на некоторую заданную величину δ_0 .

Простейший способ создания детекторов \mathbf{d}_i популяции \mathbf{D} состоит из двух фаз. В первой фазе осуществляется случайная генерация кандидатов в детекторы $\hat{\mathbf{d}}_i$, равномерно распределенных в пространстве признаков E^s . Во второй фазе кандидаты $\hat{\mathbf{d}}_i$ сопоставляются с векторами \mathbf{a}_{yk} эталона $\bar{\mathbf{A}}_{yk}$ на основе меры близости Евклида:

$$\delta(\mathbf{a}_{yk}, \hat{\mathbf{d}}_i) = \sqrt{\sum_{l=1}^s (a_{ykl} - \hat{d}_{il})^2}$$

Если $\delta(\mathbf{a}_{yk}, \hat{\mathbf{d}}_i) > \delta_0$, то кандидат $\hat{\mathbf{d}}_i$ приобретает статус детектора \mathbf{d}_i , в противном случае кандидат $\hat{\mathbf{d}}_i$ уничтожается. По этой процедуре формируется популяция $\mathbf{D} = \{\mathbf{d}_i\} = \mathbf{d}_1, \mathbf{d}_2, \dots, \mathbf{d}_{N_d}$ из N_d детекторов. Останов процедуры может задаваться различными критериями, например: временем обучения; числом итераций; размером популяции; предельно допустимым числом неэффективных итераций, не добавляющих новых детекторов.

Приведенный метод создания популяции \mathbf{D} детекторов наиболее прост в реализации, но обладает существенным недостатком. Необходимое для качественного распознавания количество детекторов растет экспоненциально по мере увеличения размерности эталона $\bar{\mathbf{A}}_{yk}$. Этот недостаток можно устранить, используя другой тип детекторов, в котором представление детекторов в виде точек в пространстве признаков E^s заменяется их представлением в виде s -мерных сфер определенного радиуса. В литературе такие детекторы получили название V -детекторов (variable-sized detectors) [25–27].

V -детекторы, как и обычные, генерируются случайно как точки в пространстве признаков E^s , а затем, в отличие от обычных, трансформируются в s -мерные сферы, которые заполняют свободное от точек \mathbf{a}_{yk} эталона $\bar{\mathbf{A}}_{yk}$ пространство E^s . Принцип трансформации заключается в том, что радиус гиперсферы создаваемого V -детектора увеличивается до момента соприкосновения гиперсферы с какой-либо точкой эталона $\bar{\mathbf{A}}_{yk}$. Следствием такой процедуры создания V -детекторов будет следующее. Периферийные области пространства E^s , более удаленные от точек \mathbf{a}_{yk} эталона $\bar{\mathbf{A}}_{yk}$, будут заполняться сравнительно небольшим количеством V -детекторов больших радиусов. Напротив, области близкие к точкам \mathbf{a}_{yk} эталона $\bar{\mathbf{A}}_{yk}$ будут заполняться V -детекторами малых радиусов. В результате, свободное от точек \mathbf{a}_{yk} эталона $\bar{\mathbf{A}}_{yk}$ пространство E^s будет эффективно заполнено V -детекторами соответствующих радиусов. При этом потребное для распознавания количество V -детекторов при прочих равных условиях будет существенно меньшим чем обычных.

Принцип размещения V -детекторов в пространстве признаков E^2 иллюстрирует рис. 1.

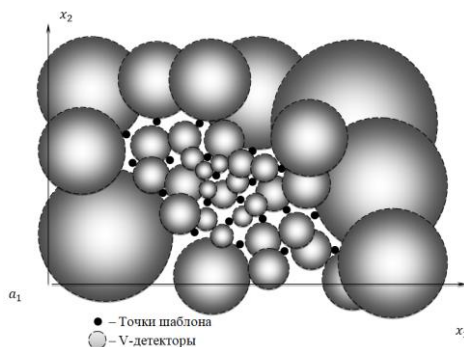


Рис. 1. Принцип размещения V-детекторов в двумерном пространстве

Предлагается следующая процедура формирования V-детекторов.

1. В пространстве E^S случайно, с равномерным законом распределения, генерируется кандидат в V-детекторы $\dot{\mathbf{d}}_l = (d_1, d_2, \dots, d_s)$.

2. Проверяется, попадает ли кандидат в V-детекторы $\dot{\mathbf{d}}_l$ в гиперсферы n_d ранее созданных V-детекторов $\mathbf{d}_1, \mathbf{d}_2, \dots, \mathbf{d}_{n_d}$. Для этого последовательно решаются неравенства:

$$\sum_{v=1}^s (\dot{d}_{lv} - d_{lv})^2 \leq R_l^2, \quad i = 1, 2, \dots, n_d,$$

где

$$R_l^2 = \sum_{v=1}^s (d_{lv} - d_{lv0})^2.$$

Если неравенство выполняется, то переход на шаг 1 иначе переход на следующий шаг.

3. Вычисляются расстояния Евклида между кандидатом в V-детекторы $\dot{\mathbf{d}}_l$ и всеми $k = 1, 2, \dots, N_a$ элементами $\mathbf{a}_{y1}, \mathbf{a}_{y2}, \dots, \mathbf{a}_{yN_a}$ шаблона $\bar{\mathbf{A}}_{yk}$:

$$E(\dot{\mathbf{d}}_l, \mathbf{a}_{yk}) = \sqrt{\sum_{v=1}^s (\dot{d}_{lv} - a_{ykv})^2}, \quad k = 1, 2, \dots, N_a.$$

4. Из вычисленных на шаге 3 расстояний $E(\dot{\mathbf{d}}_l, \mathbf{a}_{yk})$ выбирается минимальное $E_{min}(\dot{\mathbf{d}}_l, \mathbf{a}_{yk}) = \min_k E(\dot{\mathbf{d}}_l, \mathbf{a}_{yk})$, которое определяет радиус гиперсферы создаваемого детектора \mathbf{d}_l ,

$$E_{min}(\dot{\mathbf{d}}_l, \mathbf{a}_{yk}) = R_{i+1} = \sqrt{\sum_{j=1}^s [d_{(i+1)j} - d_{(i+1)0}]^2}. \quad (1)$$

5. Полученный на шаге 4 радиус R_{i+1} увеличивается на величину ΔR , соответствующую возможной ошибке первого рода формирования эталона $\bar{\mathbf{A}}_{yk}$: $R_{i+1}^* = R_{i+1} + \Delta R$.

6. Параметры гиперсферы (1) присваиваются созданному V-детектору \mathbf{d}_{i+1} популяции $\mathbf{D} = \{\mathbf{d}_i\}$.

7. Проверяется, создано ли достаточное число N_d V-детекторов в популяции $\mathbf{D} = \{\mathbf{d}_i\}$: если да, то конец процедуры, иначе переход на шаг 1.

Следует заметить, что шаг 2 алгоритма, предусматривающий проверку попадания вновь образуемого V-детектора в гиперсферы ранее созданных V-детекторов, не является обязательными. При наличии такой проверки, процедура создания V-детекторов будет иметь большую вычислительную трудоемкость. Однако, за счет уменьшения зон пересечения гиперсфер V-детекторов, их общее количество N_d будет меньшим, что приведет к сокращению вычислительной трудоемкости самой процеду-

ры анализа. При отсутствии проверки вычислительная трудоемкость процедуры создания V-детекторов сократится, но их количество N_d увеличится, что, в свою очередь, приведет к увеличению вычислительной трудоемкости процедуры анализа.

Учитывая то обстоятельство, что процедура создания V-детекторов является составной частью фазы обучения, которая проводится существенно реже, чем фаза распознавания, конечная эффективность системы анализа при наличии шага 2 алгоритма будет выше.

Пример размещения детекторов на рис. 1 соответствует варианту отсутствия шага 2 алгоритма.

Создание популяции $\mathbf{D} = \{\mathbf{d}_i\}$ детекторов завершает фазу обучения ИИС.

В фазе распознавания элементы \mathbf{a}_{yk} анализируемой последовательности \mathbf{A}_{yk} сопоставляется с детекторами \mathbf{d}_i популяции $\mathbf{D} = \{\mathbf{d}_i\}$.

При использовании обычных детекторов \mathbf{d}_i используется мера близости Евклида между векторами \mathbf{a}_{yk} и \mathbf{d}_i :

$$\delta(\mathbf{a}_{yk}, \mathbf{d}_i) = \sqrt{\sum_{v=1}^s (a_{ykv} - d_{iv})^2}.$$

Критический уровень близости $\delta(\mathbf{a}_{yk}, \mathbf{d}_i) = \delta_0$ определяет границу для принятия системой решения «свой/чужой» и задается, исходя из допустимых ошибок первого и второго рода.

Если для некоторой пары \mathbf{a}_{yl} и \mathbf{d}_m $\delta(\mathbf{a}_{yl}, \mathbf{d}_m) < \delta_0$, то считается, что элемент \mathbf{a}_{yl} анализируемой последовательности \mathbf{A}_{yk} отсутствует в шаблоне $\bar{\mathbf{A}}_{yk}$ и потому принадлежит «чужому».

При использовании V-детекторов сопоставление реализуется путем проверки попадания векторов \mathbf{a}_{yk} в гиперсферы V-детекторов популяции $\mathbf{D} = \{\mathbf{d}_i\}$, что соответствует поочередному решению неравенств

$$\sum_{v=1}^s (a_{ykv} - d_{iv})^2 \leq R_i^2, \quad k = 1, 2, \dots, N_a, \quad i = 1, 2, \dots, N_d.$$

Удовлетворение неравенства для любой пары векторов \mathbf{a}_{yl} и \mathbf{d}_m свидетельствует о том, что элемент \mathbf{a}_{yl} анализируемой последовательности \mathbf{A}_{yk} отсутствует в шаблоне $\bar{\mathbf{A}}_{yk}$ и потому принадлежит «чужому».

Большие размеры анализируемых текстов и большое число детекторов, а также наличие существенных вариаций динамических биометрических параметров определяют целесообразность применения статистического подхода при формировании системой распознавания итогового решения.

При сопоставлении анализируемого текста с детекторами контролируется частота f срабатываний детекторов, которая приближенно отражает статистическую вероятность принадлежности анализируемого текста «чужому»:

$$\hat{P}^ч \approx f = \frac{n_d^+}{n_d},$$

где n_d^+ – число срабатываний детекторов в проведенных операциях сопоставления; n_d – общее число проведенных операций сопоставления.

Принятие решения о принадлежности анализируемой последовательности \mathbf{A} «чужому» считается обоснованным, при превышении частоты f заданного порогового значения f_{Π} :

$$\mathbf{A} \equiv \begin{cases} \mathbf{A}^c, & \text{если } f < f_{\Pi}; \\ \mathbf{A}^ч, & \text{если } f \geq f_{\Pi}, \end{cases}$$

где \mathbf{A} – анализируемая последовательность векторов признаков; \mathbf{A}^c – последовательность векторов признаков «свой»; $\mathbf{A}^ч$ – последовательность векторов признаков «чужой».

Заключение. Предлагаемый подход в рамках иммунологического представления позволяет обобщить существенно различные применяемые методы идентификации личности по динамическим биометрическим параметрам разной модальности – голоса, рукописи и клавиатурного набора. Отличием подхода является возможность текстонезависимого анализа текстов различной модальности, произвольного объема и содержания. Другим отличием является переход от интегральной оценки результатов анализа биометрических данных за фиксированный период времени к непрерывной оценке данных в темпе их поступления, с возможностью своевременного принятия правильного решения. В работе представлены также варианты иммунологического решения задачи распознавания данных динамической биометрии с использованием обычных детекторов и детекторов с измеряемой геометрией.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Ахмад Х.М., Жирков В.Ф.* Введение в цифровую обработку речевых сигналов. – Владимир: Изд-во Владим. гос. ун-та, 2007. – 192 с.
2. *Матвеев Ю.Н.* Технологии биометрической идентификации личности по голосу и другим модальностям // Вестник МГТУ им. Н.Э. Баумана. Серия Приборостроение. – 2012. – № 2. – С. 46-61.
3. *Campbell W., Assaleh K., Broun C.* Speaker recognition with polynomial classifiers // IEEE Trans. Speech Audio Process. – 2002. – Vol. 10, No. 4. – P. 205-212.
4. *Анисимова Э.С.* Идентификация онлайн-подписи с помощью оконного преобразования Фурье и радиального базиса // Компьютерные исследования и моделирование. – 2014. – Т. 6, № 3. – С. 357-364.
5. *Jain A.K., Friederike D.G., Connel S.D.* On-line signature verification // Pattern Recognition. – 2002. – Vol. 35 (12). – P. 2963-2972.
6. *Plamondon R., Srihari S.* On-line and Off-line Handwriting Recognition: A Comprehensive Survey // IEEE Trans. PAMI. – 2000. – Vol. 22 (1). – P. 63-84.
7. *Иванов А.И.* Биометрическая идентификация личности по динамике подсознательных движений: монография. – Пенза: Изд-во Пенз. гос. ун-та, 2000. – 188 с.
8. *Брюхомицкий Ю.А., Казарин М.Н.* Система аутентификации личности по почерку // Сборник трудов научно-практической конференции с международным участием «Информационная безопасность». – Таганрог: Изд-во ТРТУ, 2002. – С. 22-29.
9. *Мазниченко Н.И., Гвозденко М.В.* Анализ возможностей систем автоматической идентификации клавиатурного почерка // Вестник Национального технического университета «Харьковский политехнический институт». Серия Информатика и моделирование. – 2008. – Вып. № 24. – С. 77-82.
10. *Скубицкий А.В.* Анализ применимости метода реконструкции динамических систем в системах биометрической идентификации по клавиатурному почерку // Инфокоммуникационные технологии. – 2008. – Т. 6, № 1. – С. 51-53.
11. *Чалая Л.Э.* Модель идентификации пользователей по клавиатурному почерку // Искусственный интеллект. – 2004. – № 4. – С. 811-817.
12. *Брюхомицкий Ю.А., Казарин М.Н.* Метод биометрической идентификации пользователя по клавиатурному почерку на основе разложения Хаара и меры близости Хэмминга // Известия ТРТУ. – 2003. – № 4 (33). – С. 141-149.
13. *Dasgupta D.* Artificial Immune Systems and Their Applications. Ed., Springer-Verlag, 1999.
14. *De Castro L.N., Timmis J.I.* Artificial Immune Systems: A New Computational Intelligence Approach. – London: Springer-Verlag, 2000. – 357 p.
15. Искусственные иммунные системы и их применение / под ред. Д. Дасгупты; пер. с англ. А.А. Романюхи. – М.: Физматлит, 2006. – 344 с.
16. *Dasgupta D., Forrest S.* Tool breakage detection in milling operations using a negative-selection algorithm // Technical report CS95-5, Department of computer science, University of New Mexico, 1995.
17. *Forrest S., Perelson A.S., Allen L., Cherukuri R.* Self-nonsel self discrimination in a computer // In: Proc. of Ieee symposium on research in security, Oakland, CA, 16-18 May 1994. – P. 202-212.
18. *Брюхомицкий Ю.А.* Иммунологический подход к организации клавиатурного мониторинга // Известия ЮФУ. Технические науки. – 2014. – № 2 (151). – С. 33-41.

19. Брюхомицкий Ю.А. Анализ рукописного текста методами иммунокомпьютинга // Информационное противодействие угрозам терроризма. – 2015. – № 24. – С. 36-43.
20. Брюхомицкий Ю.А. Иммунологический метод идентификации личности по рукописи // Известия ЮФУ. Технические науки. – 2015. – № 5 (166). – С. 174-183.
21. Брюхомицкий Ю.А. Иммунологический метод верификации рукописи с использованием векторного представления данных // Известия ЮФУ. Технические науки. – 2016. – № 9 (182). – С. 50-57.
22. Брюхомицкий Ю.А. Клавиатурный мониторинг на основе иммунологического клонирования // Безопасность информационных технологий. – 2016. – № 4 (40). – С. 5-11.
23. Брюхомицкий Ю.А. Клавиатурная идентификация личности. Lambert Academic Publishing, Saarbrücken, Germany, 2012. – 140 с. – ISBN 978-3-8484-1119-1.
24. Брюхомицкий Ю.А. Цепочный метод клавиатурного мониторинга // Известия ЮФУ. Технические науки. – 2009. – № 11 (100). – С. 135-145.
25. Ji Z., Dasgupta D. Real-valued negative selection algorithm with variable-sized detectors // Genetic and Evolutionary Computation (GECCO 2004): Proceedings. – Berlin–Heidelberg: Springer-Verlag, 2004. – Ser. LNCS 3102. – Part I. – P. 287-298.
26. Ji Z., Dasgupta D. Revisiting negative selection algorithm // Evolutionary Computation. – 2007. – Vol. 15, No. 2 (Summer). – P. 223-251.
27. Ji Z., Dasgupta D. V-Detector: An Efficient Negative Selection Algorithm with «Probably Adequate» Detector Coverage // Information Sciences. – 2009. – Vol. 179. – P. 1390-1406.

REFERENCES

1. Akhmad Kh.M., Zhirkov V.F. Vvedenie v tsifrovuyu obrabotku rechevykh signalov [Introduction to digital processing of speech signals]. Vladimir: Izd-vo Vladim. gos. un-ta, 2007, 192 p.
2. Matveev Yu.N. Tekhnologii biometricheskoy identifikatsii lichnosti po golosu i drugim modal'nostyam [The technology of biometric identification by voice and other modalities], *Vestnik MGTU im. N.E. Baumana. Seriya Priborostroenie* [Herald of the Bauman Moscow State Technical University. Series Instrument Engineering], 2012, No. 2, pp. 46-61.
3. Campbell W., Assaleh K., Broun C. Speaker recognition with polynomial classifiers, *IEEE Trans. Speech Audio Process*, 2002, Vol. 10, No. 4, pp. 205-212.
4. Anisimova E.S. Identifikatsiya onlayn-podpisi s pomoshch'yu okonnogo preobrazovaniya Fur'e i radial'nogo bazisa [Identification of online signatures using the windowed Fourier transform and radial basis], *Komp'yuternye issledovaniya i modelirovanie* [Computer research and modeling], 2014, Vol. 6, No. 3, pp. 357-364.
5. Jain A.K., Friederike D.G., Connel S.D. On-line signature verification, *Pattern Recognition*, 2002, Vol. 35 (12), pp. 2963-2972.
6. Plamondon R., Srihari S. On-line and Off-line Handwriting Recognition: A Comprehensive Survey, *IEEE Trans. PAMI*, 2000, Vol. 22 (1), pp. 63-84.
7. Ivanov A.I. Biometricheskaya identifikatsiya lichnosti po dinamike podsoznatel'nykh dvizheniy: monografiya [Biometric personal identification by dynamics of subconscious movements: monograph]. Penza: Izd-vo Penz. gos. un-ta, 2000, 188 p.
8. Bryukhomitskiy Yu.A., Kazarin M.N. Sistema autentifikatsii lichnosti po pocherku [System, person authentication by handwriting], *Sbornik trudov nauchno-prakticheskoy konferentsii s mezhdunarodnym uchastiem «Informatsionnaya bezopasnost'»* [Proceedings of scientific-practical conference with international participation "Information security"]. Taganrog: Izd-vo TRTU, 2002, pp. 22-29.
9. Maznichenko N.I. Gvozdenko M.V. Analiz vozmozhnostey sistem avtomaticheskoy identifikatsii klaviaturnogo pocherka [The analysis of possibilities of automatic identification systems keyboard handwriting], *Vestnik Natsional'nogo tekhnicheskogo universiteta «Khar'kovskiy politekhnicheskii institut». Seriya Informatika i modelirovanie* [Bulletin of National technical University "Kharkiv Polytechnic Institute". Series Informatics and modeling], 2008, Issue No. 24, pp. 77-82.
10. Skubitskiy A.V. Analiz primenimosti metoda rekonstruktsii dinamicheskikh sistem v sistemakh biometricheskoy identifikatsii po klaviaturnomu pocherku [Analysis of the applicability of the method of reconstruction of dynamical systems in systems of biometric identification by handwriting keyboard], *Infokommunikatsionnye tekhnologii* [Infocommunication technologies], 2008, Vol. 6, No. 1, pp. 51-53.

11. *Chalaya L.E.* Model' identifikatsii pol'zovateley po klaviaturnomu pocherku [Model identification of users at the keyboard handwriting], *Iskusstvennyy intellect* [Artificial intelligence], 2004, No. 4, pp. 811-817.
12. *Bryukhomitskiy Yu.A., Kazarin M.N.* Metod biometricheskoy identifikatsii pol'zovatelya po klaviaturnomu pocherku na osnove razlozheniya Khaara i mery blizosti Khemminga [The method of biometric identification of the user at the keyboard handwriting based on the decomposition of the Haar and proximity measure of the Hamming], *Izvestiya TRTU* [Izvestiya TSURE], 2003, No. 4 (33), pp. 141-149.
13. *Dasgupta D.* Artificial Immune Systems and Their Applications. Ed., Springer-Verlag, 1999.
14. *De Castro L.N., Timmis J.I.* Artificial Immune Systems: A New Computational Intelligence Approach. London: Springer-Verlag, 2000, 357 p.
15. *Iskusstvennye immunnye sistemy i ikh primeneniye* [Artificial immune systems and their applications], ed. by D. Dasgupty: the translation from english A.A. Romanyukhi. Moscow: Fizmatlit, 2006, 344 p.
16. *Dasgupta D., Forrest S.* Tool breakage detection in milling operations using a negative-selection algorithm, *Technical report CS95-5, Department of computer science, University of New Mexico, 1995.*
17. *Forrest S., Perelson A.S., Allen L., Cherukuri R.* Self-nonsel self discrimination in a computer, *In: Proc. of Ieee symposium on research in security, Oakland, CA, 16-18 May 1994*, pp. 202-212.
18. *Bryukhomitskiy Yu.A.* Immunologicheskii podkhod k organizatsii klaviaturnogo monitoringa [The immunologic approach to keyboard monitoring organization], *Izvestiya YuFU. Tekhnicheskie nauki* [Izvestiya SFedU. Engineering Sciences], 2014, No. 2 (151), pp. 33-41.
19. *Bryukhomitskiy Yu.A.* Analiz rukopisnogo teksta metodami immunokomp'yutinga [Analysis of handwriting methods immunocomputing], *Informatsionnoe protivodeystvie ugrozam terrorizma* [Information counteraction to the terrorism threats], 2015, No. 24, pp. 36-43.
20. *Bryukhomitskiy Yu.A.* Immunologicheskii metod identifikatsii lichnosti po rukopisi [Immunotechnique metod of penscript analysis], *Izvestiya YuFU. Tekhnicheskie nauki* [Izvestiya SFedU. Engineering Sciences], 2015, No. 5 (166), pp. 174-183.
21. *Bryukhomitskiy Yu.A.* Immunologicheskii metod verifikatsii rukopisi s ispol'zovaniem vektornogo predstavleniya dannykh [The immunological method of penscript verification using vector representation of data], *Izvestiya YuFU. Tekhnicheskie nauki* [Izvestiya SFedU. Engineering Sciences], 2016, No. 9 (182), pp. 50-57.
22. *Bryukhomitskiy Yu.A.* Klaviaturnyy monitoring na osnove immunologicheskogo klonirovaniya [Keyboard monitoring based on immunological cloning], *Bezopasnost' informatsionnykh tekhnologiy* [Safety of information technology], 2016, No. 4 (40), pp. 5-11.
23. *Bryukhomitskiy Yu.A.* Klaviaturnaya identifikatsiya lichnosti [Keyboard identification]. Lambert Academic Publishing, Saarbrücken, Germany, 2012, 140 p. ISBN 978-3-8484-1119-1.
24. *Bryukhomitskiy Yu.A.* Tsepochnyy metod klaviaturnogo monitoringa [Chain method of keyboard monitoring], *Izvestiya YuFU. Tekhnicheskie nauki* [Izvestiya SFedU. Engineering Sciences], 2009, No. 11 (100), pp. 135-145.
25. *Ji Z., Dasgupta D.* Real-valued negative selection algorithm with variable-sized detectors // Genetic and Evolutionary Computation (GECCO 2004): Proceedings. Berlin–Heidelberg: Springer-Verlag, 2004. Ser. LNCS 3102, Part I, pp. 287-298.
26. *Ji Z., Dasgupta D.* Revisiting negative selection algorithm, *Evolutionary Computation*, 2007, Vol. 15, No. 2 (Summer), pp. 223-251.
27. *Ji Z., Dasgupta D.* V-Detector: An Efficient Negative Selection Algorithm with «Probably Adequate» Detector Coverage, *Information Sciences*, 2009, Vol. 179, pp. 1390-1406.

Статью рекомендовал к опубликованию к.т.н. М.Ю. Руденко.

Брюхомицкий Юрий Анатольевич – Южный федеральный университет; e-mail: bya@tgn.sfedu.ru; 347928, г. Таганрог, ул. Чехова, 2; тел.: 88634371905; кафедра безопасности информационных технологий; старший научный сотрудник; доцент.

Bryukhomitskiy Yuriy Anatoly – Southern Federal University; e-mail: bya@tgn.sfedu.ru; 2, Chekhov street, Taganrog, 347928, Russia; phone: +78634371905; the department of security in data processing technologies; Senior researcher; Associate professor.