УДК 004.067 DOI 10.18522/2311-3103-2024-2-17-25

Ю.А. Брюхомицкий

МОДЕЛЬ СИСТЕМЫ БИОМЕТРИЧЕСКОЙ ВЕРИФИКАЦИИ ПОЛЬЗОВАТЕЛЕЙ ИНФОРМАЦИОННЫХ СИСТЕМ

Предлагается гибридная модель системы текстонезависимой динамической верификации пользователей информационных систем, которая основана на комплексном использовании искусственных иммунных систем и искусственных нейронных сетей. Подлежащие верификации данные текстонезависимой динамической биометрии пользователей представлены, двумя последовательностями информационных единиц фиксированного размера векторов признаков, соответствующих образам двух классов – «свой» и «чужой». Такое представление ориентировано на массово-параллельную децентрализованную обработку данных, принятую в искусственных иммунных системах. Последующая верификация пользователей обоих классов реализуется с помощью вероятностной искусственной нейронной сети, которая в признаковом пространстве вычисляет плотности вероятности концентрации информационных единиц обоих классов. В дополнение к характеристикам плотности вероятности информационных единиц используются допустимые цены ошибок 1-го и 2-го рода для образов каждого класса. Итоговый результат биометрической верификации работающего пользователя контролируется на основании текущего сравнения совокупных статистических оценок плотности вероятности и допустимой цены ошибок образов каждого из двух классов. Предлагаемый подход к верификации личности работающего пользователя позволяет предложить общую схему этой процедуры для существенно различных модальностей динамической биометрии: голоса, рукописи и клавиатурного набора. Реализация такого подхода для биометрии конкретной модальности будет несколько отличаться, но общая схема верификации может быть сохранена. Преимуществами предлагаемого подхода являются: возможность текстонезависимого анализа динамической биометрии различной модальности, произвольного объема, содержания и языка; возможность принятия верификационного решения в непрерывном режиме в темпе поступления работы пользователя; в перспективе повышать точность работы системы верификации путем увеличения размерности нейронной сети; возможность использования истории анализа результатов верификации реальных пользователей для последующей более точной настройки системы. Относительным недостатком работы является необходимость программной реализации нейронной сети большой размерности. Однако в перспективе этот недостаток быстро нивелируется с повышением производительности средств вычислительной техники.

Текстонезависимая биометрическая верификация личности по динамическим биометрическим параметрам; искусственная иммунная система; вероятностная нейронная сеть; статистическая оценка плотности вероятности; цена ошибки классификации.

Yu.A. Bryuhomitsky

MODEL OF THE SYSTEM OF BIOMETRIC VERIFICATION OF INFORMATION SYSTEMS USERS

A hybrid model of the system of text-independent dynamic verification of users of information systems, which is based on the integrated use of artificial immune systems and artificial neural networks, is proposed. The verifiable data of text-independent dynamic user biometrics are represented by two sequences of information units of fixed-size feature vectors corresponding to the images of two classes – 'friend' and 'stranger'. This representation is oriented towards the massively parallel decentralized data processing adopted in artificial immune systems. The subsequent verification of the users of both classes is realized by a probabilistic artificial neural network, which computes the probability densities of the concentration of information units of both classes in the feature space. In addition to the probability density characteristics of the information units, the allowable 1st and 2nd kind error prices for images of each class are used. The final result of biometric verification of the working user is controlled based on the current comparison of the aggregate statistical estimates of the probability density and the acceptable price of errors of the images of each of the two classes. The proposed approach to verifying the identity of a working user allows to propose a general scheme of this procedure for significantly different modalities of dynamic biometrics: voice, handwriting, and keyboard typing. The implementation of such an approach for specific modality biometrics will be slightly different, but the general verification scheme can be maintained. The advantages of the proposed approach are: the possibility of text-independent analysis of dynamic biometry of different modality, arbitrary volume, content and language; possibility of making a

verification decision in continuous mode at the rate of user's work arrival; in the future to increase the accuracy of the verification system by increasing the dimensionality of the neural network; the possibility of using the history of analysis of verification results of real users for further more accurate tuning of the system. A relative disadvantage of the work is the necessity of program realization of a neural network of large dimensionality. However, in the future, this disadvantage will be quickly leveled with the increase of computing performance.

Text-independent biometric verification of identity by dynamic biometric parameters; artificial immune system; probabilistic neural network; statistical estimation of probability density of information units of two classes; price of classification errors.

Введение. Биометрическая идентификация личности в настоящее время получила широкое распространение. При этом большинство систем основано на распознавании личности по статическим биометрическим параметрам. При наличии многих преимуществ статической биометрии (удобство использования, компактность биометрических эталонов, относительная простота процедур регистрации и идентификации, возможность идентификации больших потоков людей), она имеет и ряд недостатков (открытость биометрических параметров, допускающая использование муляжей, высокая стоимость, негативное отношение некоторых слоев общества к сбору биометрических данных).

Применяются также динамические системы биометрической идентификации личности, основанные на анализе индивидуальных особенностей хорошо заученных подсознательных движений человека. Такие системы используются преимущественно как средство аутентификации личности при входе в информационные системы (ИС). Практическое применение в настоящее время получили системы анализа голоса [1–3], рукописи [4–8] и клавиатурного почерка [9–13]. Преимущества этих систем: низкая стоимость, возможность сохранения образа личности в тайне и быстрой смены этого образа в случае его компрометации. Недостатки этих систем – сравнительно меньшая точность и зависимость результатов идентификации от психофизического состояния человека (испуг, стресс и т.п.). Вместе с тем этот недостаток в некоторых приложениях может эффективно использоваться для контроля психофизического состояния личности (допуск к работе, характеризующейся высокой ценой ошибки, выявление лжи и неправомерных действий со стороны пользователей (аналог полиграфа) и т.п.).

Особое место в динамических биометрических системах идентификации занимают т.н. текстонезависимые технологии, в которых вместо парольных слов и фраз используется личностные особенности воспроизведения произвольных текстов: голосом, рукописью, клавиатурным набором. В таких системах эталоны личностей строятся на основе достаточно больших образцов текста соответствующей модальности. При этом возникает ряд проблем, связанных с трудностью формирования, анализа и сопоставления эталонов с предъявляемыми образцами. Вместе с тем, эти проблемы уже возможно удовлетворительно решать в задачах информационной безопасности, связанных с текущим контролем работы пользователей в ИС. Примерами таких задач являются: непрерывная скрытная верификация работающих пользователей ИС; скрытное выявление инсайдеров, осуществляющих злонамеренные и неправомерные действия в ИС; выявление отклонений в психофизическом состоянии личности; аудит безопасности ИС на основе интерактивного взаимодействия администратора ИС с пользователями; выявление лжи (аналог полиграфа) и другие подобные задачи.

Постановка задачи. Биометрическая аутентификация личности может реализовываться в двух вариантах:

- путем предъявления личностью только биометрических признаков, которые последовательно сопоставляются со биометрическими эталонами всех пользователей ИС, зарегистрированных в биометрической базе данных ИС, с целью выявления признаков, схожих к предъявленным (аутентификация);
- путем предварительного предъявления личностью не биометрического идентификатора, позволяющего извлечь из биометрической базы данных ИС соответствующий ему биометрический эталон (если таковой имеется) с последующим сопоставлением его с предъявленным биометрическим признаком (верификация).

Данная работа ориентирована на систему верификации личности, получившую преимущественное распространение при использовании биометрических идентификаторов. Для этого предлагается использовать гибридную модель, сочетающую в себе две технологии искусственного интеллекта: искусственные иммунные системы (ИИС) – для представления образов текстонезависимой динамической биометрии) [14–20] и искусственные нейронные сети (ИНС) – для сопоставления и распознавания этих образов [21].

В текстонезависимой динамической биометрии данные представлены, по существу, сигналами (функциями времени), структура которых отражает индивидуальные особенности текущего воспроизведения личностью произвольных текстов различной модальности. Для распознавания таких сигналов предложено множество методов, которые обычно сводятся сначала к переводу их в статическое представление в частотной, или в частотно-временной областях. После чего задача распознавания решается уже в формате статического представления исходных сигналов.

В данной работе для верификации работающей в ИС личности предлагается альтернативный подход к распознаванию сигналов, который сводится к представлению их последовательностями информационных единиц фиксированного размера, в виде векторов признаков двух классов пользователей – «свой» и «чужой». Такое представление хорошо согласуется с массово-параллельной децентрализованной обработкой данных, принятой в ИИС.

На этапе верификации пользователей двух классов «свой» – «чужой» используется вероятностная нейронная сеть (PNN – Probabilistic Neural Network), являющаяся модификацией ИНС радиально-базисных функций (RBF) [22-24]. Применение сети PNN позволяет фиксировать плотность концентрации последовательностей информационных единиц обоих классов в признаковом пространстве. Результат верификации «свой» – «чужой» определяется путем сравнения статистических оценок плотности вероятности распределения образов каждого из двух классов. В дополнение к характеристикам плотности вероятности информационных единиц каждого класса предлагается также использовать цену ошибок, как допустимых ошибок 1-го и 2-го рода процедуры верификации.

Решение поставленной задачи. Воспроизведение произвольного текста средствами динамической биометрии любой модальности реализуется совокупностью заученных подсознательных движений, которые преобразуются в электрические сигналы (функции времени). В динамической биометрии сигналы $\boldsymbol{x}(t)$ разной модальности имеют и различную мерность. В общем случае их следует рассматривать как многомерные:

$$\boldsymbol{x}(t) = x_1(t), x_2(t), \dots, x_n(t).$$

На этапе предварительной обработки сигналы $\boldsymbol{x}(t)$ оцифровываются $\boldsymbol{x}(t) \to \boldsymbol{x}(t_i)$, $i = 1, 2, \dots$, масштабируются. Далее из них исключаются длительные паузы, не обусловленные особенностями воспроизведения текста. В голосовой биометрии исключаются также неинформативные с точки зрения распознавания голоса фонемы шипящих звуков.

Отсчеты сигнала $\boldsymbol{x}(t_i)$, $i = 1, 2, \dots$ рассматриваются как точки метрического пространства E^n, представленные векторами признаков $\boldsymbol{x}(t_i) = x_1(t_i), x_2(t_i), \dots, x_n(t_i)$, а сам сигнал $\boldsymbol{x}(t_i)$, – как последовательность $\{\boldsymbol{x}(t_i)\}_{i=1}^{\infty}$ элементов, представленных векторами признаков: $\boldsymbol{x}(t_i)$.

Проведенные ранее исследования [11–13], показывают, что индивидуальные особенности динамической биометрии личности в большей степени проявляются не характером воспроизведения одиночных символов и фонем, а морфемно обусловленных последовательно идущими фрагментами текста. Для использования этого феномена последовательность$\{\boldsymbol{x}(t_i)\}_{i=1}^{\infty}$ расчленяется на фрагменты $\{\boldsymbol{x}(t_i)\}_{i=1}^{r}$ одинакового размера по *r* отсчетов в каждом фрагменте.

Результатом будет новая последовательность $\{\boldsymbol{y}(t_j)\}_{j=1}^{\infty}$, каждый элемент которой содержит *r* векторов $\boldsymbol{x}(t_i)$ исходной последовательности $\{\boldsymbol{x}(t_i)\}_{i=1}^{\infty}$:

$$\boldsymbol{y}(t_j)_{j=1}^{\infty} = \{\boldsymbol{x}(t_i)\}_{i=1}^{r}.$$

В реальной системе верификации последовательность $\{\boldsymbol{y}(t_j)\}_{j=1}^{\infty}$ ограничивается n элементами – $\{\boldsymbol{y}(t_j)\}_{j=1}^{n}$. При этом каждый вектор $\boldsymbol{y}(t_j)$ последовательности $\{\boldsymbol{y}(t_j)\}_{j=1}^{n}$ будет представлен s-мерным вектором, содержащим $s = n \times r$ компонент:

$$\boldsymbol{y}(t_j) = \begin{bmatrix} y_{11} & y_{12} & \cdots & y_{1r} \\ y_{21} & y_{22} & \cdots & y_{2r} \\ \cdots & \cdots & \cdots & \cdots \\ y_{n1} & y_{n2} & \cdots & y_{nr} \end{bmatrix}.$$

В итоге текстонезависимая динамическая биометрия личности будет представлена последовательностью $\{\boldsymbol{y}(t_j)\}_{j=1}^{n}$ s-мерных векторов признаков в метрическом пространстве E^n.

В связи с применением в данной работе комплексного использования аппарата ИИС и ИНС PNN представляется целесообразным использовать модель отрицательного отбора (МОО) ИИС [14–20].

Применение МОО ИИС для решения задачи верификации пользователей ИС по принципу «свой»-«чужой» предполагает вначале создание эталона $\boldsymbol{P}$ «своего» пользователя (в данном случае, в виде конечной последовательности $\boldsymbol{P} = \{\boldsymbol{y}(t_j)\}_{j=1}^{n}$), а затем совокупности m детекторов $\boldsymbol{D}$ в том же формате $\boldsymbol{D} = \{\boldsymbol{d}(t_j)\}_{j=1}^{m}$, которые должны отличаться от элементов последовательности $\boldsymbol{P} = \{\boldsymbol{y}(t_j)\}_{j=1}^{n}$ на некоторую заданную величину δ_0.

Соотношение числа элементов эталона $\boldsymbol{P}$ и числа детекторов $\boldsymbol{D}$ в общем случае зависит от задачи и вида применяемых детекторов. В данной работе, в связи с использованием ИНС PNN, для классификации «свой» – «чужой» предлагается использовать равное число элементов эталона $\boldsymbol{P}$ и числа детекторов $\boldsymbol{D}$, т. е. $n = m$.

Простейший способ создания детекторов $\boldsymbol{D}$ состоит из двух фаз. В первой фазе осуществляется случайная генерация кандидатов в детекторы $\dot{\boldsymbol{D}}$, равномерно распределенных в пространстве признаков E^n. Во второй фазе кандидаты в детекторы $\dot{\boldsymbol{D}}$ по координатам сопоставляются с векторами эталона $\boldsymbol{P}$ на основе меры близости Евклида:

$$\delta_{yd} = \sqrt{\sum\nolimits_{l=1}^{s} \left(y_{jl} - \dot{d}_{jl}\right)^2}.$$

Если $\delta_{yd} > \delta_0$, то кандидат $\dot{\boldsymbol{d}}_j$ в детекторы $\dot{\boldsymbol{D}}$ приобретает статус детектора $\boldsymbol{d}_j$, в противном случае он уничтожается. Таким образом формируется популяция заданного числа N_d детекторов $\boldsymbol{D}$.

В рабочем режиме производится верификация текстонезависимых биометрических данных работающей в ИС неизвестной личности, представленных двумя совокупностями данных (элементов эталона $\boldsymbol{P}$ и детекторов $\boldsymbol{D}$). Верификация указанных данных осуществляется на два класса «свой» – «чужой» с использованием модифицированной PNN-сети [21–24].

ИНС PNN представляет собой параллельную реализацию статистических методов Байеса и ориентирована исключительно на задачи классификации.

Верификацию биометрических данных работающей в ИС личности на два класса «свой» – «чужой» предлагается реализовать на основе формального правила:

- класс с более плотным распределением в области неизвестного образца, будет иметь преимущество перед другим классом;
- класс с более высокой ценой ошибки классификации будет иметь преимущество перед другим классом.

В ИНС PNN оценка плотности распределения образцов осуществляется методом Парцена (Parzen). Исходными данными для классификации являются две последовательности равной длины:

- $\{\boldsymbol{y}(t_j)\}_{j=1}^{n}$ – эталонная последовательность «своего»;

- $\{\boldsymbol{d}(t_j)\}_{j=1}^{n}$ – последовательность детекторов «чужого».

Для каждого элемента последовательностей $\{\boldsymbol{y}(t_j)\}_{j=1}^{n}$ и $\{\boldsymbol{d}(t_j)\}_{j=1}^{m}$ формируются упрощенные функция Гаусса, которые отличаются от классической отсутствием коэффициента $1/\sigma\sqrt{2\pi}$ перед экспонентой, что позволяет получить максимальное значение функции плотности вероятностей, равное единице:

$$\varphi(\boldsymbol{y}_j) = \exp\left(-\frac{\|\boldsymbol{y}-\boldsymbol{y}_j\|^2}{2\sigma^2}\right);\ \varphi(\boldsymbol{d}_j) = \exp\left(-\frac{\|\boldsymbol{d}-\boldsymbol{d}_j\|^2}{2\sigma^2}\right),$$

где σ – параметр, задающий ширину функции.

Функции плотностей распределения вероятностей элементов для каждого класса образуются путем суммирования функций Гаусса элементов последовательностей $\{\boldsymbol{y}(t_j)\}_{j=1}^{n}$ и $\{\boldsymbol{d}(t_j)\}_{j=1}^{m}$:

$$\varphi(\boldsymbol{Y}) = \sum_{i=1}^{L_k} \exp\left(-\frac{\|\boldsymbol{y}-\boldsymbol{y}_j\|^2}{2\sigma^2}\right);\quad \varphi(\boldsymbol{D}) = \sum_{i=1}^{L_k} \exp\left(-\frac{\|\boldsymbol{d}-\boldsymbol{d}_j\|^2}{2\sigma^2}\right),$$

где L_k – объем обучающей выборки каждого класса.

Структура ИНС PNN для решения задачи текстонезависимой верификации личности по динамическим биометрическим параметрам приведена на рис. 1.

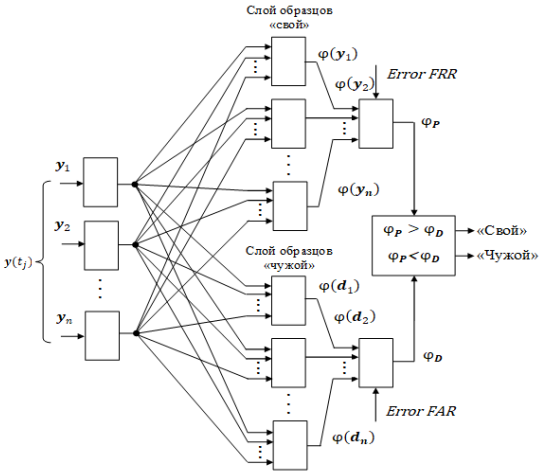

Рис. 1. PNN-сеть для решения задачи верификации личности

Входной слой и слой образцов образуют полно связную структуру. На входы сети последовательно поступают s-мерные векторы $\boldsymbol{y}_j$ последовательности $\boldsymbol{P} = \{\boldsymbol{y}_j\}_{j=1}^{n}$, биометрических данных неизвестной личности. Слой образцов представлен двумя группами нейронов «свой» и «чужой» по n нейронов в каждой группе. Веса обеих матриц связей слоя образцов определяются значениями компонент соответствующих s-мерных образцов входных векторов $\boldsymbol{y}_j$ и $\boldsymbol{d}_j$:

$$\boldsymbol{W}_{\boldsymbol{y}} = \begin{Vmatrix} y_{11} & y_{12} & \dots & y_{1n} \\ y_{21} & y_{22} & \dots & y_{2n} \\ \dots & \dots & \dots & \dots \\ y_{s1} & y_{s2} & \dots & y_{sn} \end{Vmatrix};\qquad \boldsymbol{W}_{\boldsymbol{d}} = \begin{Vmatrix} d_{11} & d_{12} & \dots & d_{1n} \\ d_{21} & d_{22} & \dots & d_{2n} \\ \dots & \dots & \dots & \dots \\ d_{s1} & d_{s2} & \dots & wd_{sn} \end{Vmatrix}.$$

Слой суммирования представлен двумя нейронами, каждый из которых суммирует плотность вероятности своей группы:

$$\varphi^{\boldsymbol{P}} = \varphi(\boldsymbol{y}_1), \varphi(\boldsymbol{y}_2), \dots \varphi(\boldsymbol{y}_n);\ \varphi^{\boldsymbol{D}} = \varphi(\boldsymbol{d}_1), \varphi(\boldsymbol{d}_2), \dots \varphi(\boldsymbol{d}_n).$$

Выходной нейрон выполняет функцию дискриминатора величины суммарной плотности вероятности $\varphi = \varphi^{\boldsymbol{P}} + \varphi^{\boldsymbol{D}}$ с учетом цены ошибок 1-го рода (FRR) и 2-го рода (FAR) и в итоге производит классификацию работающей личности:

$$\varphi = \begin{cases} \text{при } (\varphi_{\boldsymbol{P}} + \text{FRR}) > (\varphi_{\boldsymbol{D}} + \text{FAR}) - \text{«свой»}; \\ \text{при } (\varphi_{\boldsymbol{P}} + \text{FAR}) < (\varphi_{\boldsymbol{D}} + \text{FAR}) - \text{«чужой»}. \end{cases}$$

(мерности величин $\varphi_{\boldsymbol{P}}, \varphi_{\boldsymbol{D}}, FRR, FAR$) для конкретных задач верификации должны быть согласованы).

В ИНС PNN необходимо провести предварительную нормализацию входных векторов $\boldsymbol{y}_j$ и $\boldsymbol{d}_j$:

$$y_j^{\text{н}} = y_j \Big/ \sqrt{\textstyle\sum_{j=1}^{n} y_j^2}; \quad d_j^{\text{н}} = d_j \Big/ \sqrt{\textstyle\sum_{j=1}^{n} d_j^2}.$$

Такая операция превращает входные векторы $\boldsymbol{y}_j$ и $\boldsymbol{d}_j$ в векторы единичной длины $\boldsymbol{y}_j^{\text{н}}$ и $\boldsymbol{d}_j^{\text{н}}$ в пространстве E^n.

Исходя из соответствия метрик входных векторов $\boldsymbol{y}_j$, $\boldsymbol{d}_j$ и весов $\boldsymbol{W}_y$, нормализация производится и для весов $\boldsymbol{W}_y$

$$w_{ij}^{\text{н}} = w_{ij} \Big/ \sqrt{\textstyle\sum_{j=1}^{n} w_{ij}}.$$

С учетом нормализации и последующих преобразований плотности вероятностей для обеих последовательностей будут выглядеть так:

$$\varphi(\boldsymbol{y}_j) = \exp\left(\frac{1}{\sigma^2}\sum\nolimits_{j=1}^{n} y_j^{\text{н}} \cdot w_{ij}^{\text{н}} - 1\right); \; \varphi(\boldsymbol{d}_j) = \exp\left(\frac{1}{\sigma^2}\sum\nolimits_{j=1}^{n} d_j^{\text{н}} \cdot w_{ij}^{\text{н}} - 1\right)$$

Функции активности каждого нейрона слоя суммирования определяет значение плотностей вероятностей обоих классов $\varphi_{\boldsymbol{P}}$ и $\varphi_{\boldsymbol{D}}$:

$$\varphi_{\boldsymbol{P}} = \sum\nolimits_{j=1}^{n} \exp\left(\frac{1}{\sigma^2}\sum\nolimits_{j=1}^{n} y_j^{\text{н}} \cdot w_{ij}^{\text{н}} - 1\right);$$

$$\varphi_{\boldsymbol{D}} = \sum\nolimits_{j=1}^{n} \exp\left(\frac{1}{\sigma^2}\sum\nolimits_{j=1}^{n} d_j^{\text{н}} \cdot w_{ij}^{\text{н}} - 1\right).$$

В режиме верификации через обученную сеть PNN непрерывно по n текущих отсчетов $\boldsymbol{y}(t_j)$ пропускается входная биометрическая последовательность $\{\boldsymbol{y}(t_j)\}_{j=1}^{n}$ априори неизвестной личности.

ИНС PNN по итоговым значениям плотности вероятности и ошибок первого и второго рода $\varphi_{\boldsymbol{P}}$ и $\varphi_{\boldsymbol{D}}$ обоих классов определяет принадлежность входной последовательности $\boldsymbol{y}(t_j)$ к одному из двух возможных классов «свой» или «чужой».

Принятие верификационного решения, осуществляется, исходя из соотношения совокупной оценки плотностей вероятности $\varphi_{\boldsymbol{P}}$ и $\varphi_{\boldsymbol{D}}$ с учетом ошибок 1-го и 2-го рода:

$$\boldsymbol{y}(t_j) \equiv \begin{cases} \text{"свой", если } \varphi_{\boldsymbol{P}} > \varphi_{\boldsymbol{D}}; \\ \text{"чужой", если } \varphi_{\boldsymbol{P}} \le \varphi_{\boldsymbol{D}}. \end{cases}$$

Принятие решения «свой» – «чужой» осуществляется в непрерывном режиме в темпе поступлении входной последовательности текстонезависимой биометрии $\{\boldsymbol{y}(t_j)\}_{j=1}^{n}$ априори неизвестной личности.

Заключение. Предлагаемый подход к верификации личности работающего оператора ИС позволяет предложить общую схему этой процедуры для существенно различных модальностей динамической биометрии: голоса, рукописи и клавиатурного набора. Реализация такого подхода для биометрии конкретной модальности может отличаться, но общая схема верификации будет сохранена.

Преимуществами предлагаемого подхода являются:

- возможность текстонезависимого анализа динамической биометрии различной модальности, произвольного объема, содержания и языка;
- возможность принятия верификационного решения в непрерывном режиме в темпе поступления входной последовательности текстонезависимой биометрии различной модальности априори неизвестной личности;
- перспектива, вследствие развития информационных технологий, повышения точности работы системы верификации путем увеличения размерности слоя образцов PNN-сети.
- возможность использования истории анализа результатов верификации реальных пользователей для последующей более точной настройки ИНС PNN в части оптимального соотношения примеров «своего», «чужого» и выбора цены ошибок 1-го и 2-го рода.

Относительным недостатком предлагаемого подхода в текущее время является необходимость реализации нейронной сети PNN большой размерности. В перспективе же развития электронных и программных технологий ИС этот недостаток будет быстро нивелироваться.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *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.
2. *Campbell W., Assaleh K., Broun C.* Speaker recognition with polynomial classifiers // IEEE Trans. Speech Audio Process. – 2002. – Vol. 10, No. 4. – P. 205-212.
3. *Брюхомицкий Ю.А.* Иммунологическая модель текстонезависимой голосовой идентификации личности // Известия ЮФУ. Технические науки. – 2022. – № 2 (226). – С. 6-13.
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. *Брюхомицкий Ю.А., Абрамов Е.С.* Верификация рукописных текстов с использованием иммунологических и нейросетевых технологий // Вопросы защиты информации. – М.: Научные и информационные издания ФГУП «НТЦ оборонного комплекса «КОМПАС». – С. 31-37.
8. *Брюхомицкий Ю.А.* Иммунологичекий метод верификации рукописи с использованием векторного представления данных // Известия ЮФУ. Технические науки. – 2016. – № 9 (182). – С. 50-57.
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. *Брюхомицкий Ю.А.* Клавиатурный мониторинг на основе иммунологического клонирования // Безопасность информационных технологий. – 2016. – № 4 (40). – С. 5-11.
12. *Брюхомицкий Ю.А.* Иммунологический метод клавиатурного мониторинга // Вестник Брестского государственного технического университета. Физика, математика, информатика. – 2016. – № 5 (101). – С. 28-32.
13. *Брюхомицкий Ю.А.* Цепочный метод клавиатурного мониторинга // Известия ЮФУ. Технические науки. – 2009. – № 11. – С. 135-145.
14. *Dasgupta D.* Artificial Immune Systems and Their Applications, Ed. – Springer-Verlag, 1999.
15. *De Castro L.N., Timmis J.I.* Artificial Immune Systems: A New Computational Intelligence Approach, London: Springer-Verlag, 2000. – 357 p.
16. *Hofmeyr S. and Forrest S.* Architecture for an Artificial Immune System // Evolutionary Computation. – 2000. – 8 (4). – P. 443-473.
17. *Specht D.F.* Probabilistic neural networks // Neural Networks. – 1990. – No. 3. – P. 109-118.
18. *Чернышев Ю.О., Венцов Н.Н., Григорьев Г.В.* Искусственные иммунные системы: обзор и современное состояние // Программные продукты и системы. – 2014. – № 4. – С. 136-142.

19. *Зайцев С.А., Субботин С.А.* Обобщенная модель искусственной иммунной системы // Proceedings. – Berlin–Heidelberg: Springer-Verlag, 2003. – Ser. LNCS 2723. – P. 195-206.
20. *Литвиненко В.И., Дидык А.А., Захарченко Ю.А*. Компьютерная система для решения задач классификации на основе модифицированных иммунных алгоритмов // Автоматика. Автоматизация. Электротехнические комплексы и системы. – 2008. – № 2 (22).
21. Нейронные сети: полный курс. – 2-е изд.: пер. с англ. – М.: Издательский дом «Вильямс», 2006. – 1104 с.
22. *Spech D.F.* Probailistic neural networks // Neural Networks. – 1990. – No. 3. – P. 109-118.
23. *Каллан Р.* Основные концепции нейронных сетей. – М.: Вильямс, 2001. – 291 с.
24. *Брюхомицкий Ю.А.* Верификация динамических биометрических параметров личности на основе вероятностной нейронной сети // Известия ЮФУ. Технические науки. – 2020. – № 5 (215). – С. 52-60.

REFERENCES

1. *Matveev Yu.N.* Tekhnologii biometricheskoy identifikatsii lichnosti po golosu i drugim modal'nostyam [Technologies for biometric personal identification by voice and other modalities], *Vestnik MGTU im. N.E. Baumana. Seriya «Priborostroenie»* [Bulletin of MSTU im. N.E. Bauman. Series "Instrument making"], 2012, No. 2, pp. 46-61.
2. *Campbell W., Assaleh K., Broun C.* Speaker recognition with polynomial classifiers, *IEEE Trans. Speech Audio Process,* 2002, Vol. 10, No. 4, pp. 205-212.
3. *Bryukhomitskiy Yu.A.* Immunologicheskaya model' tekstonezavisimoy golosovoy identifikatsii lichnosti [Immunological model of text-independent voice identification of a person], *Izvestiya YuFU. Tekhnicheskie nauki* [Izvestiya SFedU. Engineering Sciences], 2022, No. 2 (226), pp. 6-13.
4. *Anisimova E.S.* Identifikatsiya onlayn-podpisi s pomoshch'yu okonnogo preobrazovaniya Fur'e i radial'nogo bazisa [Identification of an online signature using a windowed Fourier transform and a 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. *Bryukhomitskiy Yu.A., Abramov E.S.* Verifikatsiya rukopisnykh tekstov s ispol'zovaniem immunologicheskikh i neyrosetevykh tekhnologiy [Verification of handwritten texts using immunological and neural network technologies], *Voprosy zashchity informatsii* [Issues of information protection]. Modcow: Nauchnye i informatsionnye izdaniya FGUP «NTTS oboronnogo kompleksa «KOMPAS», pp. 31-37.
8. *Bryukhomitskiy Yu.A.* Immunologichekiy metod verifikatsii rukopisi s ispol'zovaniem vektornogo predstavleniya dannykh [Immunological method of manuscript verification using vector representation of data], *Izvestiya YuFU. Tekhnicheskie nauki* [Izvestiya SFedU. Engineering Sciences], 2016, No. 9 (182), pp. 50-57.
9. *Maznichenko N.I. Gvozdenko M.V.* Analiz vozmozhnostey sistem avtomaticheskoy identifikatsii klaviaturnogo pocherka [Analysis of the capabilities of systems for automatic identification of keyboard handwriting], *Vestnik Natsional'nogo tekhnicheskogo universiteta «Khar'kovskiy politekhnicheskiy institut». Seriya «Informatika i modelirovanie»* [Bulletin of the National Technical University “Kharkiv Polytechnic Institute”. Series “Informatics and Modeling”], 2008, Issue № 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 for reconstructing dynamic systems in biometric identification systems based on keyboard handwriting], *Infokommunikatsionnye tekhnologii* [Infocommunication technologies], 2008, Vol. 6, No. 1, pp. 51-53.
11. *Bryukhomitskiy Yu.A.* Klaviaturnyy monitoring na osnove immunologicheskogo klonirovaniya [Keyboard monitoring based on immunological cloning], *Bezopasnost' informatsionnykh tekhnologiy* [Information technology security], 2016, No. 4 (40), pp. 5-11.
12. *Bryukhomitskiy Yu.A.* Immunologicheskiy metod klaviaturnogo monitoringa [Immunological method of keyboard monitoring], *Vestnik Brestskogo gosudarstvennogo tekhnicheskogo universiteta. Fizika, matematika, informatika* [Bulletin of Brest State Technical University. Physics, mathematics, computer science], 2016, No. 5 (101), pp. 28-32.

13. *Bryukhomitskiy Yu.A.* Tsepochnyy metod klaviaturnogo monitoringa [Chain method of keyboard monitoring], *Izvestiya YuFU. Tekhnicheskie nauki* [Izvestiya SFedU. Engineering Sciences], 2009, No. 11, pp. 135-145.
14. *Dasgupta D.* Artificial Immune Systems and Their Applications, Ed. Springer-Verlag, 1999.
15. *De Castro L.N., Timmis J.I.* Artificial Immune Systems: A New Computational Intelligence Approach, London: Springer-Verlag, 2000, 357 p.
16. *Hofmeyr S. and Forrest S.* Architecture for an Artificial Immune System, *Evolutionary Computation,* 2000, 8 (4), pp. 443-473.
17. *Specht D.F.* Probabilistic neural networks, *Neural Networks,* 1990, No. 3, pp. 109-118.
18. *Chernyshev Yu.O., Ventsov N.N., Grigor'ev G.V*. Iskusstvennye immunnye sistemy: obzor i sovremennoe sostoyanie [Artificial immune systems: review and current state], *Programmnye produkty i sistemy* [Software products and systems], 2014, No. 4, pp. 136-142.
19. *Zaytsev S.A., Subbotin S.A.* Obobshchennaya model' iskusstvennoy immunnoy sistemy [Generalized model of an artificial immune system], *Proceedings*. Berlin–Heidelberg: Springer-Verlag, 2003. Ser. LNCS 2723, pp. 195-206.
20. *Litvinenko V.I., Didyk A.A., Zakharchenko Yu.A.* Komp'yuternaya sistema dlya resheniya zadach klassifikatsii na osnove modifitsirovannykh immunnykh algoritmov [Computer system for solving classification problems based on modified immune algorithms], *Avtomatika. Avtomatizatsiya. Elektrotekhnicheskie kompleksy i sistemy* [Automation. Automation. Electrical complexes and systems], 2008, No. 2 (22).
21. Neyronnye seti: polnyy kurs [Neural networks: a complete course]. 2nd ed.: transl. from engl. Moscow: Izdatel'skiy dom «Vil'yams», 2006, 1104 p.
22. *Spech D.F.* Probailistic neural networks, *Neural Networks,* 1990, No. 3, pp. 109-118.
23. *Kallan R.* Osnovnye kontseptsii neyronnykh setey [Basic concepts of neural networks]. Moscow: Vil'yams, 2001, 291 p.
24. *Bryukhomitskiy Yu.A.* Verifikatsiya dinamicheskikh biometricheskikh parametrov lichnosti na osnove veroyatnostnoy neyronnoy seti [Verification of dynamic biometric personality parameters based on a probabilistic neural network], *Izvestiya YuFU. Tekhnicheskie nauki* [Izvestiya SFedU. Engineering Sciences], 2020, No. 5 (215), pp. 52-60.

Статью рекомендовал к опубликованию д.т.н., профессор К.Е. Румянцев.

Брюхомицкий Юрий Анатольевич – Южный федеральный университет; e-mail: bryuhomitskiy@sfedu.ru; г. Таганрог, Россия; тел.: 88634371905; кафедра безопасности информационных технологий; с.н.с.; доцент.

Bryuhomitsky Yuriy Anatoly – Southern Federal University; e-mail: bryuhomitskiy@sfedu.ru; Taganrog, Russia; phone: +78634371905; the department of security in data processing technologies; senior researcher; associate professor.

УДК 004.93 DOI 10.18522/2311-3103-2024-2-25-31

А.Н. Бакуменко, В.А. Деркачев, В.В. Бахчевников, В.Т. Лобач

МОДЕЛЬ АЛГОРИТМА ПОТОКОВОЙ МАРКИРОВКИ ШИРОКОФОРМАТНОГО ИЗОБРАЖЕНИЯ

В настоящей статье предложен алгоритм обработки широкоформатного изображения для применения в системах, работающих в режиме реального масштаба времени с высокоскоростным потоком видеоданных. Вопрос предварительной обработки изображения, его кластеризации, сегментации и маркировки имеет особую важность для систем обработки видеопотока высокого разрешения в режиме реального времени. Кроме того, при реализации таких алгоритмов остро стоит вопрос минимизации затрат вычислительных ресурсов программируемых логических интегральных схем (ПЛИС), на которых происходит непосредственное развертывание алгоритмов потоковой обработки изображений. Минимальное потребление ресурсов обеспечивают однопроходные алгоритмы маркировки, в которых отсутствует необходимость буферизации изображения, что имеет особую важность при обработки широкоформатного изображения высокого разрешения. Однако, при реализации одиночного прохода изображения через систему обработки может происходить создание множества дополнительных маркеров подлежащих дальнейшему объединению, особенно при анализе изображения с большим разрешением. Созданные дополнитель-