СТАТЬЯ

УДК 004.67

ТЕКСТОНЕЗАВИСИМАЯ ВЕРИФИКАЦИЯ ЛИЧНОСТИ ПО ДИНАМИЧЕСКИМ БИОМЕТРИЧЕСКИМ ПАРАМЕТРАМ НА ОСНОВЕ НЕЙРОННОЙ СЕТИ КОХОНЕНА

Брюхомицкий Ю.А.

ФГАОУ ВО «Южный федеральный университет», Ростов-на-Дону, e-mail: info@sfedu.ru

В данной работе предлагается обобщенный подход к верификации личности по динамическим биометрическим параметрам разной модальности (клавиатурный почерк, рукопись, голос). Представление сигналов динамической биометрии личности осуществляется путем преобразования входных биометрических данных в однотипную последовательность информационных единиц, каждая из которых является ее текущим фрагментом, содержащим одинаковое количество позиций биометрического сигнала соответствующей модальности. Биометрическая последовательность, полученная для легитимной личности и являющаяся ее биометрическим эталоном, подвергается кластеризации на самообучающейся нейронной сети Кохонена большой размерности. Обученная нейронная сеть тестируется затем на биометрии легитимной личности, и производится статистический анализ результатов и получение необходимых числовых характеристик. В рабочем режиме через обученную сеть пропускается последовательность априори неизвестной личности того же размера, что и эталонная, и по результатам статистического анализа вычисляются аналогичные числовые характеристики. Принятие верификационного решения осуществляется, исходя из допустимой величины ошибки первого рода на основе пороговой величины невязки числовых характеристик для верифицируемой и легитимной личностей. Предлагаемый подход позволяет обобщить существенно различные методы верификации личности по динамическим биометрическим параметрам разной модальности. Его преимуществами являются: возможность текстонезависимого анализа динамической биометрии различной модальности, произвольного объема и содержания; принятие верификационного решения за фиксированное время, определяемое принятым размером эталона; возможность задания необходимой точности работы системы верификации путем изменения размерности нейронной сети. Недостатком является необходимость программной реализации нейронных сетей большой размерности. Однако, учитывая высокие темпы повышения производительности вычислительных средств, этот недостаток будет быстро нивелироваться.

Ключевые слова: динамические биометрические параметры, текстонезависимая верификация личности, кластеризация биометрической последовательности, нейронная сеть Кохонена, статистический анализ результатов обучения

TEXT-INDEPENDENT PERSONALITY VERIFICATION ON DYNAMIC BIOMETRIC PARAMETERS BASED ON THE KOHONEN NEURAL NETWORK

Bryukhomitskiy Yu.A.

Southern Federal University, Rostov-on-Don, e-mail: info@sfedu.ru

A generalized approach to verification of personality by dynamic biometric parameters of different modality (keyboard handwriting, penscript, voice) is proposed. Representation of dynamic personality biometric signals is carried out by converting the input biometric data into the same type sequence of information units, each of which is its current fragment containing the same number of positions of the biometric signal of corresponding modality. The biometric sequence obtained for a legitimate person and being its biometric standard is subjected to clustering on a Kohonen self-learning neural network of large dimension. The trained neural network is then tested on the biometrics of a legitimate person and a statistical analysis of the results is performed and the necessary numerical characteristics are obtained. In operating mode, a sequence of an a priori unknown person of the same size as the reference is passed through the trained network, and similar numerical characteristics are calculated from the results of statistical analysis. The verification decision is made based on the permissible error of the first kind on the basis of the threshold value of the discrepancy of numerical characteristics for verified and legitimate individuals. The proposed approach allows to summarize significantly different methods of verification of personality by dynamic biometric parameters of different modality. Its advantages are: the possibility of a text-independent analysis of dynamic biometrics of various modality, arbitrary volume and content; adoption of a verification decision for a fixed time determined by the accepted size of the standard; the ability to set the required accuracy of the verification system by changing the dimension of the neural network. The disadvantage is the need for software implementation of large-sized neural networks. However, taking into consideration the high rate of increase in computing productivity, this shortcoming will be quickly leveled.

Keywords: dynamic biometrics, text-independent verification of a person by, clustering of a biometric sequence, Kohonen neural network, statistical analysis of learning results

В защищенных информационных и мобильных системах процедура персонификации личности (идентификация и аутентификация) является первым обязательным рубежом защиты. Для реализации этой процедуры в настоящее время все большее внимание уделяется биометрическим методам, обладающим рядом неоспоримых преимуществ [1]. Особой разновидностью биометрических методов персонификации

личности является использование ее поведенческих (динамических) характеристик, представленных манерой подсознательного воспроизведения любого текста в трех модальностях: голосом [2–4], рукописью [5–7] или клавиатурным набором [8, 9]. Важным при этом является то, что произвольный текст может быть неограниченного объема и представлен на любом языке. По этой причине такая разновидность биометрии получила название текстонезависимой биометрии. Ее преимуществами является высокая защита от атак воспроизведения текста, сравнительно невысокие затраты на ее реализацию (преимущественно программную). Недостаток, – бóльшая продолжительность процедуры персонификации, обусловленная необходимостью сопоставления текстов с биометрическими эталонами большого объема. Кроме того, использование текстонезависимой биометрии связано с решением ряда проблем, связанных с оптимальным представлением эталонов образцов текста различной модальности, выбором необходимого объема образцов, своевременным определением момента принятия решения «свой – чужой» при персонификации личности.

Вместе с тем использование текстонезависимой биометрии не ограничивается исключительно задачами персонификации личности при входе в информационные и мобильные системы. Более перспективным направлением ее применения является скрытный мониторинг работы пользователей в уже ранее легально открытых ими информационных и мобильных системах. К таким задачам относятся, в частности [1]: скрытная непрерывная клавиатурная верификации работающих пользователей, исключающая их подмену в ранее легально открытых системах; скрытное выявление легальных пользователей (инсайдеров), осуществляющих неправомерные действия в системах, путем установления отклонений их клавиатурного почерка от нормы, вызванных незаконными действиями (психофизический эффект); открытое или скрытное выявление операторов, имеющих отклонение своего текущего психофизического состояния от нормы, актуальное в системах с большой ценой ошибки оператора; выявление личностей, поставляющих ложную информацию в вопрос-ответных процедурах (иная реализация детектора лжи) и другие задачи.

В текстонезависимой динамической биометрии образы личностей представлены периодическими сигналами. Традиционным подходом к решению задачи распознавания таких сигналов является предварительный перевод их в частотную область путем разложения в какой-либо ряд: Фурье, Уолша, Хаара и др. Коэффициенты разложений выступают в качестве контролируемых информационных параметров, и задача распознавания образов решается уже в формате статического представления [1].

В данной работе предлагается иной подход к распознаванию сигналов текстонезависимой динамической биометрии. Он заключается в первичном временном квантовании исходного сигнала и последующем его вторичном квантовании, позволяющем выделить группы соседних отсчетов сигнала первичного квантования одинакового размера. Выделенные группы представляются далее многомерными векторами в Евклидовом пространстве и трактуются как информационные единицы анализируемого биометрического сигнала. Такой подход имитирует принцип обработки данных в искусственных иммунных системах (ИИС) [10, 11]. Верификация динамической биометрии личности осуществляется далее путем кластеризации указанных многомерных векторов с помощью обученной нейронной сети Кохонена и последующего статистического анализа ее выходных данных.

Размерность сигналов текстонезависимой динамической биометрии зависит от модальности. В голосовых системах сигналы одномерные, в рукописных онлайновых системах мерность определяется числом квазинепрерывных характеристик взаимного положения пера и графического планшета (обычно от двух до восьми степеней свободы), в клавиатурных системах мерность определяется способом представления исходных данных. Поэтому в общем случае сигналы текстонезависимой динамической биометрии следует считать многомерными: $\boldsymbol{x}(t) = x_1(t), x_2(t), \ldots, x_n(t)$. Далее на этапе предварительной обработки они оцифровываются $\boldsymbol{x}(t) \to \boldsymbol{x}(t_i) = \boldsymbol{x}(t_i) = x_1(t_i)$, $x_2(t_i) \ldots, x_n(t_i)$, $i = 1, 2, \ldots$ и приводятся к единому масштабу по всем компонентам. В реальном масштабе времени текст может содержать длительные паузы, не обусловленные индивидуальным характером его воспроизведения данной личностью, поэтому такие паузы исключаются из анализа. При голосовом воспроизведении текста из него исключатся также неинформативные фонемы шипящих звуков.

Сигнал $\boldsymbol{x}(t_i)$, $i = 1, 2, \ldots$ рассматривается далее как последовательность $\{\boldsymbol{x}_i\}_{i=1}^{\infty} = \boldsymbol{x}_1, \boldsymbol{x}_2, \ldots$ элементов, представленных векторами признаков: $\boldsymbol{x}_i$.

В динамической биометрии выявлен принципиально важный феномен, который заключается в том, что личностные особенности воспроизведения определенного текста наблюдаются в большей степени не в одиночных символах, а в группах последовательно расположенных символов, несущих индивидуальную морфологическую окраску слов. Это позволяет существенно повысить точность биометрической верификации личности [1].

Для воспроизведения указанного феномена последовательность $\{\boldsymbol{x}_i\}_{i=1}^{\infty}$ расчленяется на фрагменты одинакового размера по r отсчетов в каждом фрагменте $\{\boldsymbol{x}_i\}_{i=1}^{r}$. Каждый фрагмент $\{\boldsymbol{x}_i\}_{i=1}^{r}$ трактуется далее как элемент новой последовательности $\{\boldsymbol{y}_j\}_{j=1}^{\infty}$, содержащий r векторов $\boldsymbol{x}_i$ исходной последовательности $\{\boldsymbol{x}_i\}_{i=1i}^{\infty}$

$$\{\boldsymbol{y}_j\}_{j=1}^{\infty} = \boldsymbol{y}_1, \boldsymbol{y}_2, \ldots, \boldsymbol{y}_j = \{\boldsymbol{x}_i\}_{i=1}^{r},$$
$$i = 1,2,\ldots,r, j = 1,2,\ldots .$$

Для использования указанного феномена последовательность $\{\boldsymbol{x}_i\}_{i=1}^{\infty}$ расчленяется на фрагменты $\{\boldsymbol{x}_i\}_{i=1}^{r}$ одинакового размера по r отсчетов в каждом фрагменте. Результатом будет новая последовательность $\{\boldsymbol{y}_j\}_{j=1}^{\infty} = \boldsymbol{y}_1, \boldsymbol{y}_2, \ldots, j = 1,2,\ldots$, каждый элемент $\boldsymbol{y}_j$ которой содержит r векторов $\boldsymbol{x}_i$ исходной последовательности $\{\boldsymbol{x}_i\}_{i=1i}^{\infty}$:

$$\{\boldsymbol{y}_j\}_{j=1}^{\infty} = \boldsymbol{y}_1, \boldsymbol{y}_2, \ldots, \boldsymbol{y}_j = \{\boldsymbol{x}_i\}_{i=1}^{r},$$
$$i = 1,2,\ldots,r, j = 1,2,\ldots .$$

При этом элементы $\boldsymbol{y}_j$ представляют собой s-мерные вектора $\boldsymbol{y}_j$, содержащие $s = n \times r$ компонент:

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

Последовательность $\{\boldsymbol{y}_j\}_{j=1}^{N_y}$, ограниченная N_y элементами, представляет биометрический эталон личности.

В итоге общее распределение динамических биометрических данных личности будет представлено множеством кластеров $\{\boldsymbol{y}_j\}_{j=1}^{N_y}$ s-мерных векторов $\boldsymbol{y}_j$, в пространстве признаков E^s. При этом каждый кластер будет содержать фрагменты биометрии, специфичные по воспроизведению данной личностью.

Режим верификации предполагает возможность сопоставления предъявленного образца биометрии априори легитимной личности соответствующему ей биометрическому эталону $\mathbf{P} = \{\boldsymbol{y}_{Pj}\}_{j=1}^{N_y}$. По результатам сопоставления принимается верификационное решение «свой – чужой». Анализ минимаксных значений $\boldsymbol{y}_{Pj}$ по координатам s позволяет сузить потенциальное пространство признаков E^s в рабочее пространство E_p^s.

Обучение системы осуществляется на основе самоорганизующейся нейронной сети Кохонена (или какой-либо последующей ее модификации) [12–14]. Цель обучения – кластеризация пространства признаков E_p^s для эталона $\mathbf{P} = \{\boldsymbol{y}_{Pj}\}_{j=1}^{N_y}$. Результатом кластеризации будет совокупность кластеров $k = 1, 2, \ldots, l$. Число кластеров l выбирается из эмпирических соображений, связанных с приемлемой точностью и вычислительной сложностью воспроизведения сети.

Простейший вариант схемы нейронной сети Кохонена для решения поставленной задачи приведен на рисунке.

Нейроны сети Кохонена реализуют операцию взвешенного суммирования:

$$z_k = b_k + \sum_{i=1}^{s} w_{ik} \cdot y_j, \; i = 1,2,\ldots,s, \; k = 1,2,\ldots,l,$$

где y_j компоненты входного вектора $\boldsymbol{y}_j$; z_k – выходы нейронов; b_k – пороги нейронов; w_{ik} – веса нейронов.

Выходные сигналы нейронов подвергаются конкуренции по правилу «победитель получает всё». Для этого выходные сигналы нейронов сравниваются и максимальный из них обращается в 1, остальные обращаются в 0. Если максимум возникает одновременно на выходах нескольких нейронов, то все эти выходные сигналы также обращаются в 1.

Счетчики на выходах блока конкуренции служат для подсчета единиц на выходах сети при предъявлении входной последовательности $\{\boldsymbol{y}_j\}_{j=1}^{N_y}$.

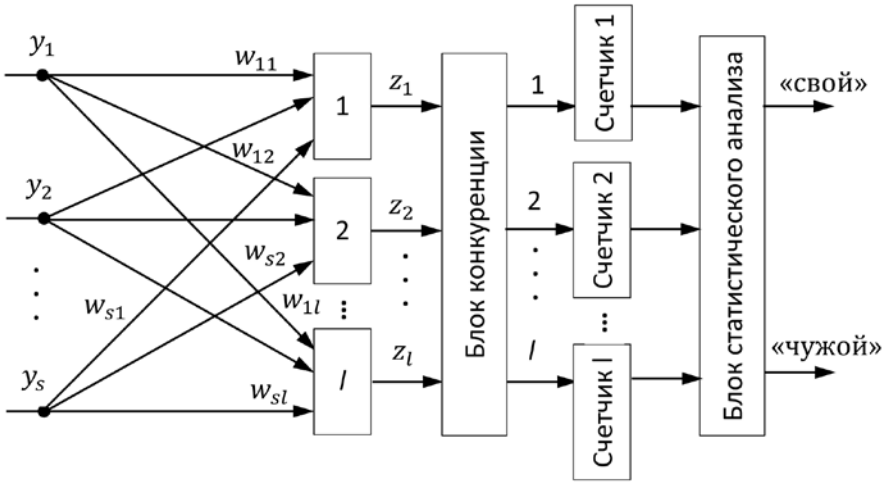

Схема нейронной сети Кохонена

Нейрон становится победителем в конкуренции, если для него выполняется соотношение

$$d\left(\boldsymbol{y}, \boldsymbol{w}_j\right) = \min_{1<k\le l} d\left(\boldsymbol{y}, \boldsymbol{w}_k\right),$$

где j – номер нейрона-победителя; $d(\boldsymbol{y}, \boldsymbol{w}_j)$ – расстояние между векторами $\boldsymbol{y}$ и $\boldsymbol{w}$ в метрике Евклида

$$d\left(\boldsymbol{y}, \boldsymbol{w}_i\right) = \boldsymbol{y} - \boldsymbol{w}_i = \sqrt{\sum_{j=1}^{s}(y_j - w_{jk})^2}.$$

Корректировка весов «выигравшего» нейрона осуществляется по правилу Кохонена

$$\boldsymbol{w}_j^{(t+1)} = \boldsymbol{w}_j^{(t)} + \eta_j^{(t)}\left[\boldsymbol{y} - \boldsymbol{w}_j^{(t)}\right],$$

где $\eta_j^{(t)}$ – коэффициент скорости обучения j-нейрона в t-цикле обучения.

Нейронная сеть обучается путем поочередной подачи на ее входы элементов эталонной последовательности $\mathbf{P} = \left\{\boldsymbol{y}_{Rpj}\right\}_{j=1}^{N_y}$. После обучения пространство E_p^s будет расчленено на кластеры, представляющие собой s-мерные многогранники Вороного – Дирихле, стороны которых являются фрагментами секущих пространство E_p^s гиперплоскостей. Центры кластеров представлены векторами, соответствующими столбцам весовой матрицы сети.

За один цикл обучения, соответствующий предъявлению всех N_y единиц входных данных **P**, на каждом из $k = 1, 2, \ldots, l$ выходах сети будет появляться n_{kP} единиц. Величины n_{kP} можно считать случайными величинами, зависящими от структуры входной последовательности $\left\{\boldsymbol{y}_{Pj}\right\}_{j=1}^{N_y}$. Таким образом, общая картина возбуждений сети будет представлена системой случайных величин n_{kP}.

Длительность обучения в системе определяется одним циклом прогона последовательности $\mathbf{P} = \left\{\boldsymbol{y}_{Pj}\right\}_{j=1}^{N_y}$.

После обучения нейронная сеть подвергается тестированию, чтобы зафиксировать конечный результат кластеризации пространства E_p^s, необходимый для последующего статистического анализа.

При тестировании через обученную сеть пропускается последовательность эталона **P** и по каждому k-выходу сети подсчитывается количество единиц n_{kP}. Далее рассчитывается вероятность появления образов в каждом кластере для эталонной последовательности $\mathbf{P} = \left\{\boldsymbol{y}_{Pj}\right\}_{j=1}^{N_y}$:

$$p_{kP} = \frac{n_{kP}}{N_y}.$$

Математическое ожидание количества единиц в k-кластере сети будет равно

$$m_{Pk} = \sum_{j=1}^{N_y} n_{kPj} \cdot p_{kP}.$$

Математическое ожидание m_P всей картины возбуждений сети для эталона **P** будет равно сумме математических ожиданий количества единиц в каждом k-кластере:

$$m_P = m_{P1} + m_{P2} + \ldots + m_{Pk} = \sum_{k=1}^{l} m_{Pk}.$$

Полученный результат m_P трактуется как статистическая оценка всей картины кластеризации пространства E_p^s для эталона **P**. На этом этап тестирования сети заканчивается, и она готова для верификации биометрических данных.

В рабочем режиме через обученную сеть пропускается последовательность априори неизвестной личности **X** того же размера, что и эталонная – $\left\{ \boldsymbol{y}_{Xj} \right\}_{j=1}^{N_y}$ и делается оценка математического ожидания m_x картины кластеризации пространства E_p^s на основе рассчитанных ранее вероятностей появления выходных образов в каждом кластере для эталона **P**:

$$m_{Xk} = \sum_{j=1}^{N_y} n_{kXj} \cdot p_{kP};$$

$$m_X = m_{X1} + m_{X2} + \ldots + m_{Xk} = \sum_{k=1}^{l} m_{Xk}.$$

Картина кластеризации пространства E_p^s, представленная суммарным математическим ожиданием m_X будет характеризовать биометрию личности **X**. Если анализируемая биометрия принадлежит легальной личности, то m_X будет близка к величине m_P. Для любой другой личности **X** она будет существенно отличаться от m_P.

Для принятия верификационного решения, исходя из допустимой величины ошибки первого рода (недопуск «своего»), устанавливается пороговая величина невязки $\Delta_T = m_R - m_X$, на основании которой неизвестную личность **X** следует признать «своим» $\mathbf{X}^{\text{С}}$ или «чужим» $\mathbf{X}^{\text{Ч}}$:

$$\mathbf{X} \equiv \begin{cases} \mathbf{X}^{\text{С}}, \text{ если } \Delta < \Delta_T; \\ \mathbf{X}^{\text{Ч}}, \text{ если } \Delta \geq \Delta_T. \end{cases}$$

Заключение

Однотипное представление сигналов динамической биометрии разной модальности позволило предложить общий подход к реализации процедуры верификации личности на основе сочетания принципов представления данных, характерных для в ИИС и принципов их кластеризации в самоорганизующихся нейронных сетях. Перспектива применения такого подхода определяется стремительным ростом производительности вычислительных средств, открывающим возможность эффективно применять ИИС и самоорганизующиеся нейронные сети больших размерностей для решения таких сложных задач.

Список литературы

1. Брюхомицкий Ю.А. Биометрические технологии идентификации личности: учебное пособие. Южный федеральный университет. Ростов-на-Дону – Таганрог: Издательство Южного федерального университета, 2017. 263 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. Капустин А.И., Симончик К.К. Система верификации дикторов по голосу на основе использования CFP-SVM подхода // DSPA-2010. Тр. 12-й Межд. конф. «Цифровая обработка сигналов и ее применение». М., 2010. Т. 1. С. 207–210.

4. Pekhovsky T., Lokhanova A. Variational Bayesian Model Selection for GMM–Speaker Verification Using Universal Background Model. INTERSPEECH-2011. Proc. 12th Annual Conf. Florence, 2011. P. 2705–2708.

5. 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.

6. Лапина Т.И., Епишев Н.Н., Лапин Д.В. Способ биометрической аутентификации пользователя в компьютизированных системах контроля доступа // Труды СПИИРАН. 2013. Вып. 4 (27). С. 189–197.

7. Дорошенко Ю., Костюченко Е.Ю. Система аутентификации на основе динамики рукописной подписи // Доклады ТУСУРа. 2014. № 2 (32). С. 219–223.

8. Брюхомицкий Ю.А. Клавиатурная идентификация личности. Lambert Academic Publishing, Saarbrűcken, Germany, 2012. 140 с.

9. Брюхомицкий Ю.А. Клавиатурная идентификация и мониторинг пользователей компьютерных систем // Актуальные аспекты информационной безопасности: монография: глава 5. С. 310–407. Таганрог: Изд-во ТТИ ЮФУ, 2011. 448 с.

10. Брюхомицкий Ю.А. Искусственные иммунные системы в информационной безопасности: учебное пособие. Южный федеральный университет. Ростов-на-Дону – Таганрог: Издательство Южного федерального университета, 2020. 147 с.

11. Чернышев Ю.О., Григорьев Г.В., Венцов Н.Н. Искусственные иммунные системы: обзор и современное состояние // Программные продукты и системы 2014. № 4 (108). С. 136–141.

12. Нейронные сети Кохонена // NEURONUS.com. [Электронный ресурс]. URL: https://neuronus.com/theory/nn/955-nejronnye-seti-kokhonena.html (дата обращения: 04.05.2021).

13. Манжула В.Г., Федяшов Д.С. Нейронные сети Кохонена и нечеткие нейронные сети в интеллектуальном анализе данных // Фундаментальные исследования. 2011. № 4. С. 108–115.

14. Козлов А.А. Моделирование нейронных сетей Кохонена на графических процессорах // Молодой ученый. 2016. № 28 (132). С. 22–26.