ЕВРАЗИЙСКОЕ НАУЧНОЕ ОБЪЕДИНЕНИЕ
EURASIAN SCIENTIFIC ASSOCIATION
www.esa-conference.ru

Биометрическая идентификация личности методами искусственного интеллекта

Брюхомицкий Юрий Анатольевич, кандидат технических наук, доцент
Южный Федеральный университет (г. Таганрог)

Введение. В современных системах безопасности все более прочное место занимают биометрические технологии идентификации личности, которые в наибольшей степени сочетают в себе высокую степень защиты, конфиденциальность, надежность и удобство использования. Особой разновидностью биометрических технологий является идентификация личности с помощью динамических биометрических характеристик личности (динамическая биометрия).

Динамические биометрические характеристики представлены подсознательными хорошо заученными человеком движениями, такими как походка, жестикуляция, мимика, голосовая артикуляция, рукопись и т. п. Эти движения реализуются в многомерном пространстве мышечных двигательных возможностей человека, что порождает колоссальную избыточность вариантов достижения цели. Постепенно в течение многих у каждого человека вырабатываются свои индивидуальные способы реализации большинства двигательных функций, которыми он затем успешно пользуется на протяжении всей жизни. При этом задача управления сложными двигательными функциями фактически переносится на подсознательный уровень, что приводит появлению устойчивых индивидуальных особенностей сложных движений (индивидуального двигательного почерка).

В настоящее время практическое применение получили динамические биометрические системы анализа голоса, рукописи и клавиатурного почерка. Динамическая биометрия используется преимущественно как средство аутентификации личности при входе в компьютерные и мобильные системы, а также для удаленной аутентификации. Процедура аутентификации сводится обычно к предъявлению условной (парольной) фразы, воспроизведенной голосом, рукописью на графическом планшете или клавиатуре.

Главным достоинством этих систем является низкая стоимость, обусловленная их реализацией преимущественно программными средствами. Другим важным достоинством динамической биометрии является возможность сохранения образа личности в тайне и быстрой его смены в случае компрометации, путем смены парольной фразы.

Недостатком динамической биометрии является меньшая, по сравнению со статической биометрией, точность идентификации и влияние на ее 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 разновидность динамической биометрии, когда процедура идентификации личности осуществляется без использования условной (парольной) фразы по любому тексту, воспроизводимому голосом, рукописью или на клавиатуре (текстонезависимая идентификация личности). В этом случае указанные недостатки динамической биометрии, или не имеют решающего значения, или, целенаправленно используются.

Круг задач, которые можно решать с применением текстонезависимой динамической биометрии:

- 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).

Техники идентификации личности при решении таких задач существенно отличаются от техник аутентификации по парольной фразе.

Общей особенностью динамической биометрии является представление исходных данных функциями времени (сигналами), структура которых собственно и содержит все необходимые для идентификации индивидуальные особенности личности. Известные подходы к решению задачи распознавания таких сигналов сводятся к двухэтапной процедуре. 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. На втором этапе уже в форматах статического представления решается собственно задача распознавания биометрических образов.

В математической постановке указанные задачи относятся к плохо-формализуемым. При их решении традиционными методами возникает ряд принципиальных проблем, в числе которых:

- трудности извлечения из произвольных образцов текста индивидуальных характеристик личности для создания биометрического эталона;
- необходимость создания, хранения и оперативного использования биометрических эталонов большой размерности;
- трудности сопоставления идентифицируемых образцов динамической биометрии с биометрическими эталонами.

Постановка задачи. Продуктивным подходом для решения плохо-формализуемых задач текстонезависимой динамической биометрии является использование обучаемых систем искусственного интеллекта – искусственных иммунных систем (ИИС) и искусственных нейронных сетей (ИНС). При этом ИИС предлагается использовать на стадии обучения динамической биометрической системы, а ИНС – на этапе распознавания (идентификации) личности.

В практических приложениях ИИС в наибольшей степени используются две модели: отрицательного отбора и клональной селекции. Каждая из моделей имеет свои преимущества и недостатки в различных приложениях. Вы-

ЕВРАЗИЙСКОЕ НАУЧНОЕ ОБЪЕДИНЕНИЕ
EURASIAN SCIENTIFIC ASSOCIATION
www.esa-conference.ru

бор оптимальной модели ИИС для решения задач текстонезависимой динамической биометрии кроме того существенно зависит и от типа используемых биометрических признаков. В данной работе предлагаются решения инвариантные к типам биометрических признаков на основе модели отрицательного отбора [1-2].

Модель отрицательного отбора (МОО) приближенно воспроизводит способность иммунной системы обнаруживать неизвестные антигены, не реагируя на собственные клетки. В иммунной системе Т-лимфоциты (или Т-клетки) способны распознавать патогены, презентованные с помощью своих рецепторов на поверхности других клеток. В процессе генерации (Т-клеток) их рецепторы производятся посредством псевдослучайного процесса генетической перегруппировки, после чего подвергаются процессу цензуры, называемому отрицательным отбором. В этом процессе Т-клетки, которые реагируют против собственных антигенов организма, разрушаются. Оставшиеся зрелые Т-клетки циркулируют затем по всему организму, выполняя иммунологические функции и защищая организм от чужеродных антигенов.

Механизм отрицательного отбора воспроизводится в МОО на стадии обучения ИИС путем создания детекторов, соответствующих аномальному поведению исследуемого объекта. Для этого сначала случайным образом генерируются кандидаты в детекторы, которые становятся детекторами лишь в том случае, если они не реагируют ни на один из образцов «своих». Полученное таким образом множество детекторов в значительной степени описывает пространство предполагаемых «чужих» и образуют иммунную память системы. В процессе распознавания образец считается «чужим», если его распознает хотя бы один из существующих детекторов. Сопоставление кандидатов в детекторы с образцами «своих» на стадии обучения, как и последующее сопоставление образованных детекторов с неизвестными образцами на стадии распознавания осуществляется по принципу частичного совпадения.

Воспроизведение в ИИС межклеточных взаимодействий, свойственных иммунной системе, приводит к необходимости соответствующей структуризации информации и принципов ее обработки в прикладной задаче. Для использования ИИС в текстонезависимой динамической биометрии биометрические сигналы предлагается представлять последовательностями информационных единиц определенного формата, с последующей децентрализованной обработкой этих единиц на основе МОО. В целом такое представление в определенной степени имитирует массово-параллельную обработку информации на уровне клеток, наблюдаемую в иммунной системе.

В МОО используются два вида представления исходных данных – строковое и векторное. В общем случае, при формализации предлагаемого подхода сигналы динамической биометрии можно считать многомерными: $\boldsymbol{x}(t) = x_1(t), x_2(t), \dots, x_n(t)$, что создает предпочтение для использования их векторного представления.

Решение поставленной задачи. На этапе предварительной обработки сигнал $\boldsymbol{x}(t)$ масштабируется по амплитуде, из него исключаются длительные паузы, не обусловленные индивидуальными особенностями воспроизведения текста. В голосовой биометрии исключаются также неинформативные (с точки зрения распознавания) фонемы шипящих звуков. После указанных преобразований сигнал $\boldsymbol{x}(t)$ квантуется по времени $\boldsymbol{x}(t) \to \boldsymbol{x}(t_i) = \boldsymbol{x}_i, i = 1, 2, \dots$. При этом отсчеты сигнала $\boldsymbol{x}_i$ в ИИС рассматриваются как точки метрического пространства E^n, представленные векторами признаков $\boldsymbol{x_i} = x_{1i}, x_{2i}, \dots, x_{ni}$.

Содержательный смысл размерности n векторов признаков $\boldsymbol{x_i}$ определяется числом биометрических параметров, учитываемых в одном отсчете. Исследования в области динамической биометрии [3-4], показывают, что индивидуальные особенности личности в большей степени проявляются при воспроизведении синтаксически связанных фрагментов воспроизводимого текста. Использование этого феномена при анализе позволяет строить системы текстонезависимой биометрической идентификации личности с существенно более высокими характеристиками по точности.

Для реализации указанного феномена разобьем квантованный сигнал $\boldsymbol{x}_i$ на фрагменты по r отсчетов в каждом фрагменте. Результатом будет последовательность $\mathbf{A}_{xj} = \boldsymbol{a}_{x1}, \boldsymbol{a}_{x2}, \dots, j = 1, 2, \dots$, каждый элемент $\boldsymbol{a}_{xj}$ которой будет представлен -мерным вектором $\boldsymbol{a}_{xk}$, содержащим $s = n \times r$ компонент.

В итоге, образы динамической биометрии будут представлены последовательностью $\mathbf{A}_{xj}$ s-мерных векторов признаков $\boldsymbol{a}_{xj}$ в пространстве E^s. В конкретных приложениях распределение векторов признаков будет сосредоточено в ограниченном рабочим подпространстве E_w^s пространства E^s, т.е. $E_w^s \subset E^s$.

Последовательность биометрических признаков $\mathbf{A}_{xj}$ одной личности, ограниченную N_a элементами $\overline{\mathbf{A}}_{xj} = \boldsymbol{a}_{x1}, \boldsymbol{a}_{x2}, \dots, \boldsymbol{a}_{xN_a}, j = 1, 2, \dots N_a$, будем трактовать как биометрический эталон этой личности.

В соответствии с используемой МОО следующим шагом является – создание на основе биометрического эталона личности распознающих элементов – детекторов, предназначенных для негативной селекции входных сигналов на этапе распознавания.

Множество детекторов $\mathbf{D}$ создается в метрике векторов $\boldsymbol{a}_{xj}$ эталона $\overline{\mathbf{A}}_{xj}$:

$$\mathbf{D} = \{\boldsymbol{d}_k\} = \boldsymbol{d}_1, \boldsymbol{d}_2, \dots, \boldsymbol{d}_{N_d}, k = 1, 2, \dots N_d;$$

$$\boldsymbol{d}_k = \begin{bmatrix} d_{k11} & d_{k12} \dots & d_{k1r} \\ d_{k21} & d_{k22} \dots & d_{k2r} \\ \dots & \dots \dots & \dots \\ d_{kn2} & d_{kn2} \dots & d_{knr} \end{bmatrix}, k = 1, 2, \dots N_d.$$

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

Простейший способ создания детекторов $\boldsymbol{d}_k$ популяции $\mathbf{D}$ состоит из двух фаз. В первой фазе осуществляется случайная генерация кандидатов в детекторы $\dot{\boldsymbol{d}}_k$, равномерно распределенных в пространстве признаков E^s. Во второй фазе кандидаты в детекторы $\dot{\boldsymbol{d}}_k$ сопоставляются с векторами $\boldsymbol{a}_{xj}$ эталона $\overline{\mathbf{A}}_{xj}$ на основе какой-либо меры близости. Для образов динамической биометрии, представленных последовательностями $\mathbf{A}_{xj}$ s-мерных векторов признаков $\boldsymbol{a}_{xj}$ в пространстве E^s, наиболее уместным является использование меры близости Евклида: $\rho(\boldsymbol{a}_{xj}, \dot{\boldsymbol{d}}_k) = \sqrt{\sum_{l=1}^{s}(a_{xjl} - \dot{d}_{kl})^2}$

Если результат сравнения $\rho(\boldsymbol{a}_{xj}, \dot{\boldsymbol{d}}_k) > \rho_0$, то кандидат в детекторы $\dot{\boldsymbol{d}}_k$ приобретает статус детектора $\boldsymbol{d}_k$, в противном случае он уничтожается. Результатом этой процедуры будет множество из N_d детекторов: $\mathbf{D} =$

ЕВРАЗИЙСКОЕ НАУЧНОЕ ОБЪЕДИНЕНИЕ
EURASIAN SCIENTIFIC ASSOCIATION
www.esa-conference.ru

$\{\boldsymbol{d}_k\} = \boldsymbol{d_1}, \boldsymbol{d_2}, \ldots, \boldsymbol{d}_{N_d}$. Останов процедуры может задаваться различными критериями: временем обучения, числом итераций, размером популяции, предельно допустимым числом неэффективных итераций, не добавляющих новых детекторов.

При использовании традиционного подхода на основе МОО создание множества детекторов $\mathbf{D} = \{\boldsymbol{d}_k\}$ завершает фазу обучения ИИС. Далее, в фазе распознавания (идентификации) личности, элементы $\boldsymbol{a}_{xj}$ анализируемой последовательности $\mathbf{A}_{xj}$ сопоставляется с детекторами $\boldsymbol{d}_k$ из множества $\mathbf{D} = \{\boldsymbol{d}_k\}$ с использованием той же меры близости Евклида между векторами $\boldsymbol{a}_{xj}$ и $\boldsymbol{d}_k$.

Критический уровень близости $\rho(\boldsymbol{a}_{xj}, \boldsymbol{d}_k) = \rho_0$ определяет границу для принятия системой решения «свой/чужой» и задается, исходя из допустимых ошибок первого и второго рода. Если для некоторой пары $\boldsymbol{a}_{xl}$ и $\boldsymbol{d}_m$ $\rho(\boldsymbol{a}_{xl}, \boldsymbol{d}_m) < \rho_0$, то считается, что элемент $\boldsymbol{a}_{xl}$ анализируемой последовательности $\mathbf{A}_{xj}$ с погрешностью δ_0 принадлежит «чужому».

Программная реализация распознавания по указанной схеме сопровождается существенными затратами вычислительных ресурсов на массовые операции сопоставления элементов биометрических данных с большим числом детекторов, что неизбежно приводит к увеличению времени анализа. Вместе с тем, время отклика является одной из важнейших характеристик биометрической системы идентификации. Поэтому, с целью улучшения этой характеристики, фазу распознавания предлагается реализовать на основе ИНС. Для этого предлагается частично изменить описанную процедуру обучения и полностью – процедуру распознавания биометрической системы.

Известные попытки использования ИНС для классификации биометрических данных наталкиваются на специфическую проблему построения обучающей выборки. В традиционной постановке обучение ИНС на распознавание образцов двух классов («своих» и «чужих») осуществляется на основе обучающего множества $\Psi = \Psi_с \cup \Psi_ч$, объединяющего подмножества образцов «своих» $\Psi_с$ и образцов «чужих» $\Psi_ч$. При этом формирование подмножества $\Psi_с$ обычно не вызывает трудностей, поскольку в него могут быть включены «живые» образцы реальных «своих». Проблема возникает при формировании подмножества $\Psi_ч$. Использование для $\Psi_ч$ «живых» образцов личностей, заведомо не относящихся к «своим», не решает проблему, поскольку вынужденно ограниченное число образцов подмножества $\Psi_ч$ не дает полной картины области распределения произвольных «чужих». Как следствие, ИНС при обучении не может построить достаточно точные разделяющие границы между кластерами $\Psi_с$ и $\Psi_ч$, что приводит к ошибкам классификации. Предложены методы [5, 6], частично решающие эту проблему, но и при их использовании точность нейросетевой классификации биометрических данных не всегда оказывается удовлетворительной.

Использование иммунологического подхода для представления биометрических данных приводит к тому, что в фазе обучения ИИС создаваемое множество детекторов $\mathbf{D} = \{\boldsymbol{d}_k\}$ фактически имитирует подмножество «чужих» $\Psi_ч$. Это автоматически решает указанную проблему обучения на «чужих» при использовании ИНС. При этом в фазе обучения ИНС биометрический эталон личности, представленный последовательностью векторов $\bar{\mathbf{A}}_{xj} = \{\boldsymbol{a}_{xj}\}$, выступает в качестве обучающего подмножества образцов «своего» $\Psi_с$, а множество детекторов $\mathbf{D} = \{\boldsymbol{d}_k\}$ – в качестве обучающего подмножества образцов «чужих» $\Psi_ч$. После обучения ИНС может осуществлять классификацию элементов $\boldsymbol{a}_{xj}$ входной последовательности $\mathbf{A}_{xj}$ по принципу «свой»/»чужой» непосредственно в темпе их поступления. Основные вычислительные и временные затраты в этом случае будут преимущественно сосредоточены в фазе обучения системы. При этом число детекторов множества $\mathbf{D} = \{\boldsymbol{d}_k\}$, необходимое для качественного распознавания биометрических сигналов, также не будет оказывать существенного влияния на общее быстродействие системы.

Большие размеры анализируемых текстов, а также наличие существенных вариаций динамических биометрических параметров определяют целесообразность применения статистического подхода для принятия системой распознавания итогового решения. При таком подходе текущие реакции ИНС при распознавании элементов последовательности $\mathbf{A}_{xj}$ обобщаются в статистическую вероятность $\hat{P}^{ч}$ принадлежности анализируемого текста «чужому», которая в свою очередь аппроксимирует частоту f текущего отношения числа реакций на «чужого» в общем числе реакций ИНС: $\hat{P}^{ч} \approx f = n_d^+ / n_d$, где:

n_d^+ – число реакций ИНС, соответствующих обнаружению «чужого»;

n_d – общее число зафиксированных реакций ИНС.

Решение о принадлежности анализируемой последовательности $\mathbf{A}_{xj}$ «своему» выносится в том случае, если частота f будет ниже заданного порогового уровня $f_п$. В противном случае выносится решение, согласно которому последовательность $\mathbf{A}_{xj}$ принадлежит «чужому» $\mathbf{A}^{ч}$:

$$\mathbf{A}_{xj} \equiv \begin{cases} \mathbf{A}^{с}, \text{если } f < f_п; \\ \mathbf{A}^{ч}, \text{если } f \geq f_п. \end{cases}$$

Заключение. В работе предлагается комплексный подход к построению системы текстонезависимого анализа данных динамической биометрии средствами искусственного интеллекта. Предложенный подход сочетает иммунологическое представление динамических биометрических данных, принятое в ИИС, и метод их распознавания, основанный на использовании ИНС. Это позволяет методически обобщить и эффективно реализовать текстонезависимую идентификацию личности по динамическим биометрическим параметрам разной модальности – голоса, рукописи и клавиатурного набора средствами искусственного интеллекта. Предложенный подход позволяет вести непрерывный контроль динамических биометрических данных в темпе их поступления, с возможностью своевременного принятия правильного аутентификационного решения.

Литература:

1. Dasgupta D., Forrest S. Novelty detection in time series data using ideas from immunology // In: ISC A 5th international conference on intelligent systems, Reno, Nevada, June 19-21, 1996.

2. Брюхомицкий Ю.А. Мониторинг информационных процессов методами искусственных иммунных систем // Известия ЮФУ. Технические науки. Тематический выпуск «Информационная безопасность». – Таганрог: Изд-во ТТИ ЮФУ, 2012. – №12. – С. 82-90.

3. Брюхомицкий Ю.А. Иммунологический подход к организации клавиатурного мониторинга // Известия ЮФУ. Технические науки. Тематический выпуск «Информационная безопасность». – Таганрог: Изд-во ИТА ЮФУ, 2014. – №2 (151). – С. 33-41.

4. Брюхомицкий Ю.А. Анализ рукописного текста методами иммунокомпьютинга // Информационное противодействие угрозам терроризма. – 2015. №24. – С. 36-43. / Материалы XIV Международной научно-практической конференции «Информационная безопасность». – Таганрог: Изд-во ЮФУ, 2015. 3.

5. Брюхомицкий, Ю. А. Метод обучения нейросетевых биометрических систем на основе построения аппроксимированных областей // Известия ТРТУ. – 2003. – № 4(33). – С. 155–159.

6. Брюхомицкий, Ю. А. Метод обучения нейросетевых биометрических систем на основе копирования областей // Перспективные информационные технологии и интеллектуальные системы. – 2003. – №3 (15). – С. 17–23.