УНИВЕРСИТЕТ ИТМО
НАУЧНО-ТЕХНИЧЕСКИЙ ВЕСТНИК ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ, МЕХАНИКИ И ОПТИКИ
июль–август 2017 Том 17 № 4 ISSN 2226-1494 http://ntv.ifmo.ru/
SCIENTIFIC AND TECHNICAL JOURNAL OF INFORMATION TECHNOLOGIES, MECHANICS AND OPTICS
July–August 2017 Vol. 17 No 4 ISSN 2226-1494 http://ntv.ifmo.ru/en

УДК 004.93

ИССЛЕДОВАНИЕ ПРИМЕНИМОСТИ ИСКУССТВЕННЫХ НЕЙРОННЫХ СЕТЕЙ ДЛЯ ВЕРИФИКАЦИИ ПОЛЬЗОВАТЕЛЕЙ ПО ДИНАМИКЕ ПОЧЕРКА

Д.И. Дикий[a], В.Д. Артемьева[b]

[a] Университет ИТМО, Санкт-Петербург, 197101, Российская Федерация
[b] Балтийский федеральный университет имени И. Канта, Калининград, 236016, Российская Федерация
Адрес для переписки: Dimandikiy@mail.ru

Информация о статье
Поступила в редакцию 17.04.17, принята к печати 07.06.17
doi: 10.17586/2226-1494-2017-17-4-677-684
Язык статьи – русский

Ссылка для цитирования: Дикий Д.И., Артемьева В.Д. Исследование применимости искусственных нейронных сетей для верификации пользователей по динамике почерка // Научно-технический вестник информационных технологий, механики и оптики. 2017. Т. 17. № 4. С. 677–684. doi: 10.17586/2226-1494-2017-17-4-677-684

Аннотация
Рассмотрены особенности применения искусственных нейронных сетей для решения задачи верификации пользователей информационных систем по динамике их рукописного почерка. Задача актуальна в связи с развитием облачных вычислений и методов машинного обучения, которые все чаще применяются для распознавания образов. На основании обзора наиболее известных методов цифровой предобработки данных пользователей предложено применение искусственных нейронных сетей для верификации пользователей по динамике их почерка. На примере дискретного преобразования Фурье проведен эксперимент с различными структурами и алгоритмами обучения искусственных нейронных сетей. Исследование выполнено на основе базы данных SVC 2004 международного чемпионата по биометрической аутентификации. При этом из базы данных заимствованы декартовы координаты траектории и временные отсечки. Показано, что искусственные нейронные сети способны решить поставленную задачу верификации, но с увеличением образцов, предъявляемых при обучении, растет вероятность успешного прохождения верификации как у легальных пользователей, так и злоумышленников. Для повышения эффективности работы искусственных нейронных сетей предложено применение метода корреляционного анализа данных, поступающих на вход нейронной сети. Предложенный подход позволил достичь ошибки первого рода (FRR) 12,6% и ошибки второго рода (FAR) 2,26%. При этом пока нерешенной остается задача различения легального пользователя и злоумышленника, знающего, как выглядит подпись или пароль. Решение проблемы авторы видят в использовании дополнительных параметров динамики почерка (давление, угол наклона).

Ключевые слова
динамика почерка, аутентификация, искусственная нейронная сеть, ошибки первого рода, ошибки второго рода, корреляционный анализ, генетический алгоритм, алгоритм обратного распространения ошибки

RESEARCH OF ARTIFICIAL NEURAL NETWORK APPLICABILITY FOR USER`S ONLINE HANDWRITTEN SIGNATURE VERIFICATION

D.I. Dikiy[a], V.D. Artemeva[b]

[a] ITMO University, Saint Petersburg, 197101, Russian Federation
[b] Immanuel Kant Baltic Federal University, Kaliningrad, 236016, Russian Federation
Corresponding author: Dimandikiy@mail.ru

Article info
Received 17.04.17, accepted 07.06.17
doi: 10.17586/2226-1494-2017-17-4-677-684
Article in Russian

For citation: Dikiy D.I., Artemeva V.D. Research of artificial neural network applicability for user`s online handwritten signature verification. *Scientific and Technical Journal of Information Technologies, Mechanics and Optics*, 2017, vol. 17, no. 4, pp. 677–684 (in Russian). doi: 10.17586/2226-1494-2017-17-4-677-684

Abstract
The paper considers features of artificial neural networks (ANN) application for online user`s verification by handwriting dynamics. This problem is urgent due to the development of cloud computing and machine learning, that even more often are used for pattern recognition. The review of the most widespread methods of digital user`s data pre-processing shows the relevance of ANN usage for verification. On the example of discrete Fourier transformation we made the experiments with different ANN structures and training algorithms. For these purposes we used the database of Signature Verification

Competition (SVC) 2004. Cartesian coordinates and time parameters of trajectories have been taken from the database. The results of research show that artificial neural networks are able to solve that task, but at the same time with increasing the number of samples for study, success probability for legal users and malefactors also increases. For increasing of ANN performance we suggest the application of correlation analysis method for research data. It helps to increase the efficiency of artificial neural network. The false acceptance rate, or FAR, is about 2.26% and the false recognition rate, or FRR, is 12.6% with the use of correlation analysis method. At the same time, the task of distinguishing between a legal user and a malefactor, knowing how the signature or the password looks, is unsolved so far. In our opinion, the problem solution lies in the usage of additional parameters of handwriting dynamics (pressure, angle of inclination) for analysis.

Keywords
handwriting dynamics, authentication, artificial neural network, FRR, FAR, correlation analysis, genetic algorithm, back propagation algorithm

Введение

В настоящее время вопросы информационной безопасности затрагивают жизнь почти каждого человека, который каким-либо образом взаимодействует с информационными системами (ИС). С развитием инфотелекоммуникационных сетей все большую популярность набирают распределенные ИС с предоставлением удаленного доступа пользователям. Согласно п 9.4.3. ГОСТ Р ИСО/МЭК 17799[1], внешние соединения с ИС обеспечивают возможность неавторизованного доступа к информации. По этой причине при доступе удаленных пользователей они должны пройти операцию аутентификации. Исходя из оценки риска, важно определить необходимый уровень защиты для выбора метода аутентификации. Например, при предоставлении услуг дистанционного банковского обслуживания широко распространен метод двухфакторной аутентификации с помощью постоянного и краткосрочного пароля, высылаемого на мобильный номер пользователя. Однако такой метод подвержен атакам на протоколы SS7 [1]. В связи с этим актуальным становится развитие технологий на основе биометрических методов аутентификации с использованием облачных вычислений [2].

Все биометрические признаки человека делятся на статические [3] и динамические [4]. Самым известным примером аутентификации по статическому признаку человека является метод, основанный на уникальности рисунка папиллярных узоров пальцев. Однако существенным недостатком статических методов является ограниченное количество информации, которое может предоставить пользователь при регистрации в ИС. В случае компрометации парольной информации трудно сгенерировать новый шаблон для легального пользователя. С другой стороны, динамические системы позволяют неограниченное количество раз изменять пароль пользователя. Из всего множества биометрических параметров человека в данной работе будет рассмотрена такая характеристика, как динамика почерка. Использование такого рода парольных систем требует наличия технической возможности для ввода пароля, например, графического планшета, устройства с сенсорным экраном и стилусом [5].

В настоящей работе авторами сделана попытка применения искусственных нейронных сетей (ИНС) для решения задачи классификации векторов признаков пользователей, состоящих из динамических характеристик процесса рукописного написания парольного слова.

Цифровая предобработка сигналов

Применение ИНС для решения задачи аутентификации по динамике почерка требует предварительной цифровой обработки данных с устройства ввода для формирования векторов признаков. При удаленном доступе к ИС система аутентификации предполагает использование ограниченного функционала устройства ввода. Это связано с тем, что не во всех устройствах существует техническая возможность считывания таких параметров динамики рукописного написания, как давление пера на поверхность, угол наклона пера относительно плоскости написания и др. По этой причине в качестве данных, характеризующих процесс написания парольного слова, использовались декартовы координаты пера или стилуса в плоскости написания, а также время регистрации положения пера. Имея вышеперечисленные параметры, в качестве динамической характеристики рассматривалось значение проекций скорости перемещения пера между соседними точками траектории на оси абсцисс и ординат.

На первоначальном этапе массивы данных с устройства ввода одного пользователя должны быть выровнены по длине с помощью цифровых фильтров либо каким-либо другим образом. Так, например, часто используются алгоритмы динамической трансформации временной шкалы [6, 7]. Пример использования этого алгоритма совместно с применением ИНС представлен в [8]. В настоящей работе применен алгоритм построения ломаной кривой – модернизированный алгоритм Форсена [9]. Эта процедура необходима для того, чтобы число входных сигналов ИНС при обучении и использовании было постоянным.

Следующим этапом обработки данных является нормировка. Для корректной работы ИНС на вход, как правило, подают данные из интервала [–1; 1] [10].

[1] ГОСТ Р ИСО/МЭК 17799:2005 Информационная технология. Практические правила управления информационной безопасностью. Введен 01.01.2007. Изд-во.Стандартинформ, 2006. 55 с.

Следует обратить внимание на формирование векторов признаков пользователя по динамике почерка, из которого будет составляться обучающая выборка. На данный момент существует несколько подходов и их комбинаций, выделяющих динамические параметры почерка. Наиболее известные из них основаны на спектральном анализе с помощью дискретного преобразования Фурье или Радона [11], дискретном вейвлет-преобразовании [6, 12], скрытых марковских моделях [13, 14], детектировании экстремальных точек [15].

В данной работе в качестве метода формирования вектора признаков авторами предложено использование дискретного преобразования Фурье над уже выровненными по длине и нормированными данными:

$$x[i] = \sum_{k=0}^{N/2} \mathrm{Re}X[k] \cos\left(\frac{2\pi k i}{N}\right) + \sum_{k=0}^{N/2} \mathrm{Im}X[k] \sin\left(\frac{2\pi k i}{N}\right),$$

где $x[i]$ – это исходный сигнал в виде массива, элементами которого являются нормализованные значения проекций скоростей перемещения пера между соседними точками, а N – длина массива $x[]$. $\mathrm{Re}X[k]$ и $\mathrm{Im}X[k]$ – массивы, элементами которого являются амплитуды косинусных и синусных компонентов соответственно. Таким образом, на выходе дискретного преобразования Фурье получаются два массива, которые отображают исходный сигнал в частотной области [16]. Здесь набор амплитуд является вектором признаков динамики почерка, который будет подаваться на вход ИНС.

При оценке эффективности систем аутентификации, как правило, рассматриваются такие два основополагающих фактора, как вероятности ошибок первого (FRR) и второго (FAR) рода. К ошибкам первого рода относятся те, которые возникают, когда доступ пытается получить легальный пользователь, а система отказывает ему в этом. К ошибкам второго рода относятся те, которые возникают при допуске к информационным ресурсам нелегальных пользователей [17].

Настройки искусственной нейронной сети

ИНС нашли большое применение в области машинного обучения. Их применяют во множестве областей, в том числе и в распознавании образов. Выбор ИНС как основного классификатора обусловлен тем, что иные методы классификации: байесовский классификатор, алгоритм k-средних и другие – как правило, должны содержать информацию минимум о двух классах данных (легальный пользователь и злоумышленник), либо набор классов легальных пользователей, как продемонстрировано в [14].

В рамках рассматриваемой задачи данные о злоумышленниках неизвестны. В случае применения ИНС не обязательно указывать второй класс данных, так как близость очередного образца пользователя к обучающей выборке выражается численно через значение нейрона выходного слоя. При близком значении выходного нейрона к единице делается вывод о принадлежности образца к классу легального пользователя, в противном случае – к классу злоумышленника.

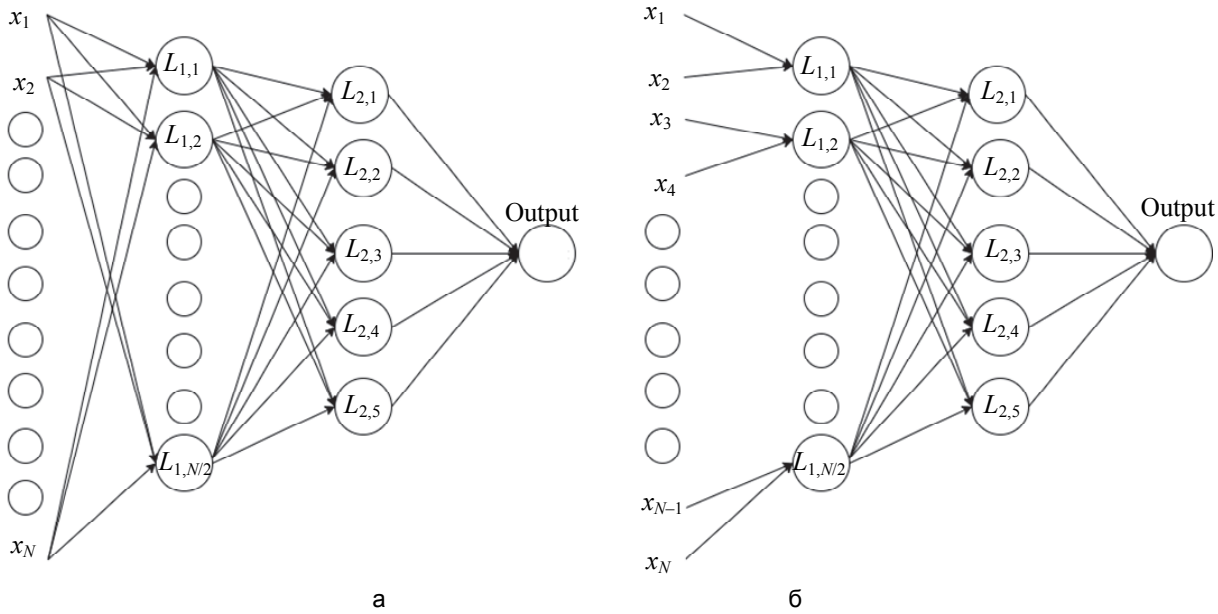

Рис. 1. Структуры искусственных нейронных сетей: соединение между входным слоем и первым скрытым «каждый с каждым» (а); соединение между входным слоем и первым скрытым «два к одному» (б); x_i – значение i -го элемента вектора признаков; N – размерность вектора признаков, $L_{i,j}$ – нейрон i-го скрытого слоя с j-м порядковым номером в слое; output (пер. с англ. – «выходной сигнал») – нейрон выходного слоя

В настоящей работе предлагается нейронная сеть, обладающая следующими настройками:

- многослойный перцептрон [18] с двумя скрытыми слоями, с прямым распространением сигнала, без обратных связей, обучаемый учителем;
- число входных нейронов N определяется размерностью вектора признаков;
- число нейронов первого скрытого слоя $N/2$;
- число нейронов второго скрытого слоя 5, выходного 1.

В работе рассмотрены две структуры ИНС, представленные на рис. 1.

Авторами применена сигмоидальная функция активации нейронов

$$f(x) = \frac{1}{1+e^{-x}},$$

где x – значение, подаваемое на вход нейрона.

Обучение ИНС для конкретного пользователя происходило на обучающей выборке с помощью алгоритма обратного распространения ошибки [19] или генетического алгоритма [20].

Определение значений ошибок первого и второго рода

Определение вероятностей ошибок первого и второго рода произведено на общедоступной базе данных First International Signature Verification Competition (SVC 2004[1]). База содержит 100 наборов легальных пользователей, преимущественно англоязычных, каждый из которых на время проведения эксперимента придумал временный рукописный пароль и предоставил 20 его образцов (далее «пользователь»). Кроме этого, в базе присутствует информация об участниках, специализирующихся на подделке подписей, имеющих возможность наблюдать за процессом написания паролей (далее «злоумышленник 1»). Злоумышленникам 1 предоставлялось 20 попыток подделать подпись. Обучение ИНС производилось на базе 40 наборов пользователей. Обучающая выборка постепенно увеличивалась с 1 до 10 образцов для каждого набора. Для определения значения ошибки первого рода по окончании каждого обучения на вход ИНС подавались оставшиеся образцы почерка пользователя (от 19 до 10 соответственно). Определение значения ошибки второго рода для злоумышленника 1 производилось на 20 образцах почерков каждого участника. Оставшиеся 60 наборов образцов почерков подавались на вход ИНС с целью определения вероятности доступа при вводе случайных подписей (далее «злоумышленник 2»).

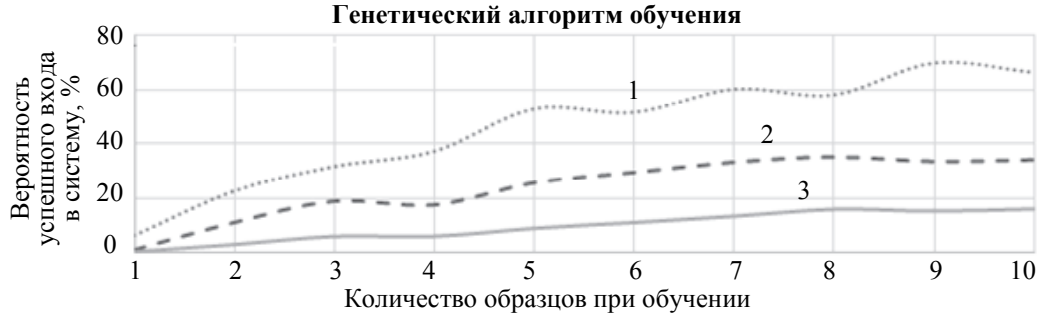

Рис. 2. Вероятность успешного входа в информационную систему при использовании искусственной нейронной сети со структурой, изображенной на рис. 1, а, и генетическим алгоритмом обучения (1 – Пользователь, 2 – Злоумышленник 1, 3 – Злоумышленник 2)

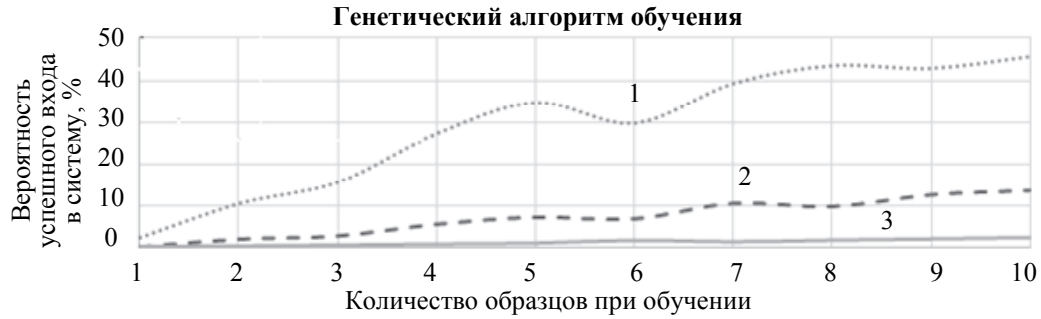

Рис. 3. Вероятность успешного входа в информационную систему при использовании искусственной нейронной сети со структурой, изображенной на рис. 1, б, и генетическим алгоритмом обучения (1 – Пользователь, 2 – Злоумышленник 1, 3 – Злоумышленник 2)

[1] SVC 2004: First International Signature Verification Competition // Department of Computer Science and Engineering The Hong Kong University of Science and Technology. URL: http://www.cse.ust.hk/svc2004/ (дата обращения: 03.06.2017).

Рис. 4. Вероятность успешного входа в информационную систему при использовании искусственной нейронной сети со структурой, изображенной на рис. 1, а, и обучением алгоритмом обратного распространения ошибки (1 – Пользователь, 2 – Злоумышленник 1, 3 – Злоумышленник 2)

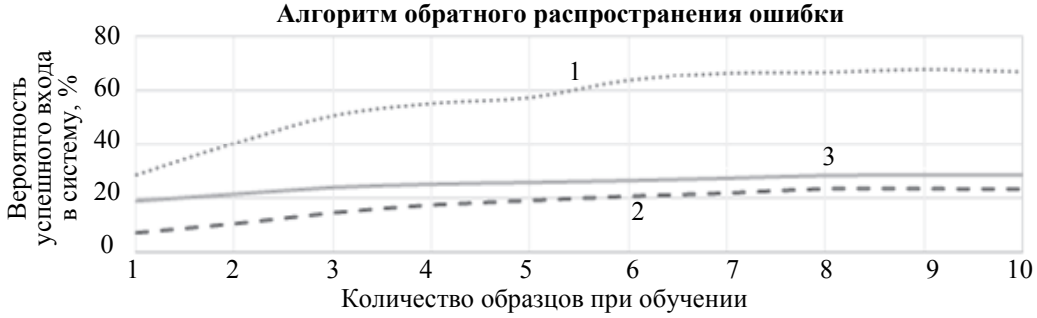

Рис. 5. Вероятность успешного входа в информационную систему при использовании искусственной нейронной сети со структурой, изображенной на рис. 1, б, и обучением алгоритмом обратного распространения ошибки (1 – Пользователь, 2 – Злоумышленник 1, 3 – Злоумышленник 2)

Как показано ранее, предложены два варианта структуры ИНС (рис. 1) и два алгоритма их обучения. Результаты проведенного эксперимента представлены на рис. 2–5.

Исходя из результатов, полученных в ходе исследования, можно сделать вывод о том, что с увеличением обучающей выборки растет вероятность успешного входа в ИС как пользователя, так и злоумышленника. Вероятность доступа при вводе случайной подписи и обучении ИНС с использованием алгоритма обратного распространения ошибки составляет более 20%. При этом использование генетического алгоритма обучения и структуры сети, изображенной на рис. 1, б, дает вероятность доступа злоумышленника 2 около 5%. Однако при этом и легальный пользователь будет допущен к информационным ресурсам с вероятностью менее 50%.

Для повышения качества верификации предложено использование корреляционного анализа сигналов. Суть предлагаемого решения состоит в вычислении математического ожидания сигнала, поступающего на вход ИНС по всей обучающей выборке. Мера взаимосвязи входных сигналов с их математическим ожиданием рассчитывалась по величине коэффициента Пирсона

$$r_j = \frac{\sum_{i=1}^{N}\left(x_{ji} - \overline{x}_j\right)\left(m_i - \overline{m}\right)}{\sqrt{\sum_{i=1}^{N}\left(x_{ji} - \overline{x}_j\right)^2 \sum_{i=1}^{N}\left(m_i - \overline{m}\right)^2}},$$

где r_j – значение искомого коэффициента корреляции j-го образца из обучающей выборки; N – размерность вектора признаков образцов обучающей выборки; x_{ji} – значение i-го элемента вектора признаков j-го образца из обучающей выборки; $\overline{x}_j$ – среднее значение элементов вектора признаков j-го образца; m_i – математическое ожидание i-го элемента вектора признаков по всем образцам из обучающей выборки, $\overline{m}$ – математическое ожидание всех элементов векторов признаков всех образцов из обучающей выборки.

При слабой корреляции сигналов от какого-либо образца из обучающей выборки с математическим ожиданием делается заключение о том, что образцы почерков сильно различаются. Следовательно, обучение ИНС на такой выборке некорректно. Вероятности распознавания с учетом корреляционного анализа входных сигналов с использованием ИНС, представленной на рис. 1, а, обучаемой генетическим алгоритмом, представлены на рис. 6.

Исключение выборок со слабо коррелирующими между собой образцами почерка позволяет не только уменьшить вероятность случайного доступа к ИС до 2%, но и повышает вероятность доступа для легального пользователя. На рис. 7 представлена зависимость количества отвергнутых выборок от их

размера. Явно прослеживается динамика увеличения числа выборок, не прошедших проверку, с ростом числа образцов рукописного написания почерка.

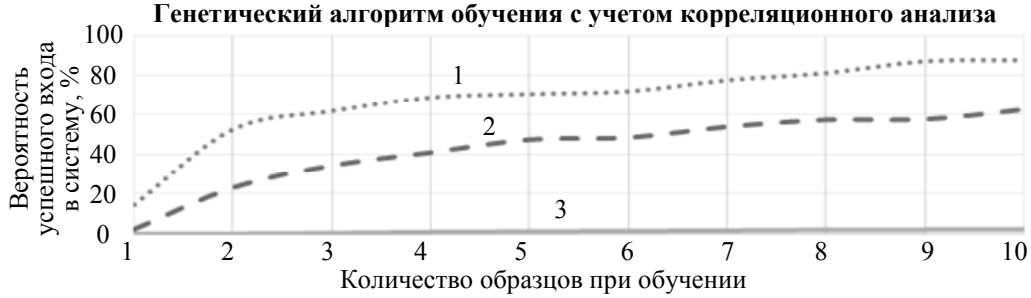

Рис. 6. Вероятность успешного входа в информационную систему при использовании искусственной нейронной сети со структурой, изображенной на рис. 1, а, и генетическим алгоритмом обучения с учетом корреляционного анализа (1 – Пользователь, 2 – Злоумышленник 1, 3 – Злоумышленник 2)

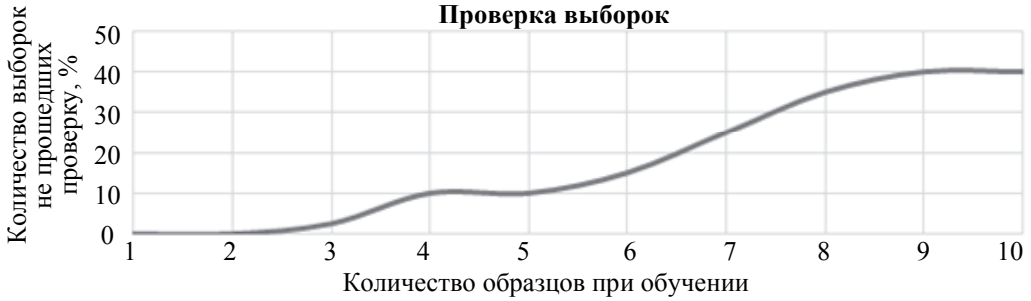

Рис. 7. Процентное соотношение обучающих выборок, не прошедших проверку корреляционным анализом, к общему числу выборок

Использование ИНС предполагает, что при обучении на одних и тех же обучающих выборках решения в виде набора значений весовых коэффициентов отличаются друг от друга, а следовательно, отличается и эффективность ИНС. Исходя из этого, были проведены два повторных эксперимента со структурой ИНС, изображенной на рис. 1, а, и генетическим алгоритмом обучения с учетом корреляционного анализа. Так как достигнутая авторами ошибка второго рода, согласно рис. 6, очень мала, то дальнейший интерес представляет ошибка первого рода. Зависимости ошибок первого рода и их среднеквадратичных отклонений от количества образцов в обучающей выборке представлены в таблице. Рассчитано среднее значение среднеквадратичных отклонений, характеризующее рассеивание ошибок первого рода (FRR) вне зависимости от количества образцов в обучающей выборке. Видно, что разброс ошибок первого рода в среднем составляет 0,99%. Это свидетельствует о том, что применение ИНС в совокупности обработкой входных сигналов статистическими методами позволяет решать поставленную задачу распознавания образов.

Номер эксперимента	Число образцов в обучающей выборке									
	1	2	3	4	5	6	7	8	9	10
1	85,7	47,4	38,1	31,2	29,4	28,0	22,5	18,9	13,0	12,5
2	84,0	52,2	41,1	33,9	29,6	27,8	22,6	20,5	12,8	12,7
3	83,9	50,0	41,5	31,6	30,3	28,1	23,3	22,0	13,5	12,7
Среднеквадратичное отклонение	1,02	2,39	1,86	1,47	0,49	0,20	0,46	1,56	0,38	0,11
Средняя величина	0,99									

Таблица. Сравнение значений ошибок первого рода, FRR, %

Заключение

В работе предложено использование искусственных нейронных сетей для систем аутентификации пользователей по динамике написания ими рукописного пароля или подписи. Отличительными чертами работы являются использование алгоритма Форсена для выравнивания длины образцов и применение только декартовых координат и времени регистрации положения пера. Это способствует применению данной системы аутентификации на большинстве мобильных устройств, обладающих сенсорными экранами. Показано эффективное совместное использование искусственных нейронных сетей и метода корреляционного анализа.

Показано, что искусственные нейронные сети могут быть применимы для решения подобных задач. Подготовка данных соответствующим образом позволяет существенно повысить эффективность искусственных нейронных сетей. Этот этап включает не только цифровую обработку сигналов, но и статистические методы работы с данными.

Увеличение размеров обучающих выборок приводит к увеличению вероятности доступа не только легального пользователя, но и злоумышленников. Это связано с тем, что легальные пользователи не повторяют динамику написания пароля или подписи точь-в-точь, а следовательно, искусственная нейронная сеть настраивается менее строго, чтобы учитывать особенности всех образцов обучающей выборки.

По значениям проекций средних скоростей перемещения пера между соседними точками траектории невозможно с необходимой точностью идентифицировать, принадлежат они пользователю или злоумышленнику, который наблюдал за процессом написания и специализируется на подделке подписей.

Таким образом, искусственные нейронные сети представляют собой инструмент, способный качественно решить задачу распознавания по динамике почерка. Так, для обучающей выборки из десяти образцов ошибка первого рода (FRR) составляет около 12,6%, а второго рода (FAR) – 2,26%. Показано, что для более эффективного применения искусственных нейронных сетей желательно использовать обучающие выборки, включающие в себя не только координаты траектории и временные отсечки, но и другие данные, например, давление и угол наклона (при наличии технической возможности).

Литература

1. Holtmanns S., Rao S.P., Oliver I. User location tracking attacks for LTE networks using the interworking functionality // Proc. IFIP Networking conference (IFIP Networking) and workshops. Vienna, Austria, 2016. P. 315–322. doi: 10.1109/IFIPNetworking.2016.7497239
2. Padma P., Srinivasan S. A survey on biometric based authentication in cloud computing // Proc. Int. Conf. on Inventive Computation Technologies (ICICT). Coimbatore, India, 2016. V. 1. P. 275–279. doi: 10.1109/INVENTIVE.2016.7823273
3. Yadav D., Tyagi R. Comparative analysis of offline signature verification system // International Journal of Security and its Applications. 2015. V. 9. N 9. P. 141–150. doi: 10.14257/ijsia.2015.9.9.13
4. Boriev Z., Sokolov S., Nyrkov A., Nekrasova A. Mathematical and information maintenance of biometric systems // Proc. Int. Conf. on Mechanical Engineering, Automation and Control Systems (MEACS2015). Tomsk, Russia, 2015. V. 124. Art. 012046. doi: 10.1088/1757-899X/124/1/012046
5. Omri F., Foufou S., Hamila R., Jarraya M. Cloud-based mobile system for biometrics authentication // Proc. 13th Int. Conf. on ITS Telecommunications (ITST). Tampere, Finland, 2013. P. 325–330. doi: 10.1109/ITST.2013.6685567
6. Fahmy M.M.M. Online handwritten signature verification system based on DWT features extraction and neural network classification // Ain Shams Engineering Journal. 2010. V. 1. P. 59–70. doi: 10.1016/j.asej.2010.09.007
7. Petrovska-Delacretaz D., Chollet G., Dorizzi B. Guide to Biometric Reference Systems and Performance Evaluation. Springer, 2009. 414 p. doi: 10.1007/978-1-84800-292-0
8. Putz-Leszczynska J. Signature verification: a comprehensive study of the hidden signature method // International Journal of Applied Mathematics and Computer Science. 2015. V. 25. P. 659–674. doi: 10.1515/amcs-2015-0048
9. Прэтт У. Цифровая обработка изображений. Т. 2. М.: Мир, 1982. 480 с.
10. Люггер Дж.Ф. Искусственный интеллект: стратегии и методы решения сложных проблем. 4-е изд. М.: Вильямс, 2003. 864 с.
11. Kashi R.S., Turin W., Nelson W. On-line handwritten signature verification using stroke direction coding // Optical Engineering. 1996. V. 35. N 9. P. 2526–2533.
12. Thumwarin P., Pernwong J., Matsuura T. FIR signature verification system characterizing dynamics of handwriting features // EURASIP Journal on Advances in Signal Processing. 2013. N 183. P. 1–15. doi: 10.1186/1687-6180-2013-183
13. Kashi R.S., Hu J., Nelson W.L., Turin W. On-line handwritten signature verification using hidden Markov model features // Proc. 4th Int. Conf. on Document Analysis and Recognition. Ulm, Germany, 1997. V. 1. P. 253–257.
14. Talebinejad M., Miri A., Chan A.D.C. A computationally efficient HMM-based handwriting verification system // Proc. IEEE

References

1. Holtmanns S., Rao S.P., Oliver I. User location tracking attacks for LTE networks using the interworking functionality. *Proc. IFIP Networking conference (IFIP Networking) and workshops*. Vienna, Austria, 2016, pp. 315–322. doi: 10.1109/IFIPNetworking.2016.7497239
2. Padma P., Srinivasan S. A survey on biometric based authentication in cloud computing. *Proc. Int. Conf. on Inventive Computation Technologies, ICICT*. Coimbatore, India, 2016, vol. 1, pp. 275–279. doi: 10.1109/INVENTIVE.2016.7823273
3. Yadav D., Tyagi R. Comparative analysis of offline signature verification system. *International Journal of Security and its Applications*, 2015, vol. 9, no. 9, pp. 141–150. doi: 10.14257/ijsia.2015.9.9.13
4. Boriev Z., Sokolov S., Nyrkov A., Nekrasova A. Mathematical and information maintenance of biometric systems. *Proc. Int. Conf. on Mechanical Engineering, Automation and Control Systems, MEACS2015*. Tomsk, Russia, 2015, vol. 124, art. 012046. doi: 10.1088/1757-899X/124/1/012046
5. Omri F., Foufou S., Hamila R., Jarraya M. Cloud-based mobile system for biometrics authentication. *Proc. 13th Int. Conf. on ITS Telecommunications, ITST*. Tampere, Finland, 2013, pp. 325–330. doi: 10.1109/ITST.2013.6685567
6. Fahmy M.M.M. Online handwritten signature verification system based on DWT features extraction and neural network classification. *Ain Shams Engineering Journal*, 2010, vol. 1, pp. 59–70. doi: 10.1016/j.asej.2010.09.007
7. Petrovska-Delacretaz D., Chollet G., Dorizzi B. *Guide to Biometric Reference Systems and Performance Evaluation*. Springer, 2009, 414 p. doi: 10.1007/978-1-84800-292-0
8. Putz-Leszczynska J. Signature verification: a comprehensive study of the hidden signature method. *International Journal of Applied Mathematics and Computer Science*, 2015, vol. 25, pp. 659–674. doi: 10.1515/amcs-2015-0048
9. Pratt W.K. *Digital Image Processing*. NY, Wiley, 1978.
10. Luger G.F. *Artificial Intelligence. Structures and Strategies for Complex Problem Solving*. 4th ed. Addison Wesley, 1999, 880 p.
11. Kashi R.S., Turin W., Nelson W. On-line handwritten signature verification using stroke direction coding. *Optical Engineering*, 1996, vol. 35, no. 9, pp. 2526–2533.
12. Thumwarin P., Pernwong J., Matsuura T. FIR signature verification system characterizing dynamics of handwriting features. *EURASIP Journal on Advances in Signal Processing*, 2013, no. 183, pp. 1–15. doi: 10.1186/1687-6180-2013-183
13. Kashi R.S., Hu J., Nelson W.L., Turin W. On-line handwritten signature verification using hidden Markov model features. *Proc. 4th Int. Conf. on Document Analysis and Recognition*. Ulm, Germany, 1997, vol. 1, pp. 253–257.
14. Talebinejad M., Miri A., Chan A.D.C. A computationally efficient HMM-based handwriting verification system. *Proc. IEEE International Instrumentation and Measurement Tech-*

International Instrumentation and Measurement Technology Conference. Victoria, Canada, 2008. P. 1868–1872. doi: 10.1109/IMTC.2008.4547350
15. Колядин Д.В., Петров И.Б. Алгоритм выделения экстремальных точек применительно к задаче биометрической верификации рукописной подписи // Исследовано в России. 2005. С. 532–540.
16. Смит С. Цифровая обработка сигналов. Практическое руководство для инженеров и научных работников. М.: Додэка-XXI, 2012. 720 с.
17. Лебеденко Ю.И. Биометрические системы безопасности: Учебное пособие. Тула: ТулГу, 2012. 158 с.
18. Rosenblatt F. The perceptron: a probabilistic model for information storage and organization in the brain // Psychological Review. 1958. V. 65. N 6. P. 386–408. doi: 10.1037/h0042519
19. Rumelhart D.E., Hinton G.E., Williams R.J. Learning internal representation by error propagation / In: Parallel Distributed Processing. V. I Foundations. Eds. D.E. Rumelhart, J.L. McClelland. Cambridge: MIT Press, 1988. P. 399–421. doi: 10.1016/b978-1-4832-1446-7.50035-2
20. Alabbas M., Jaf S. Abdullah A.H.M. Optimize BpNN using new breeder genetic algorithm // Proc. Int. Conf. on Advanced Intelligent Systems and Informatics. 2016. N 533. P. 373–382. doi: 10.1007/978-3-319-48308-5_36

nology Conference. Victoria, Canada, 2008, pp. 1868–1872. doi: 10.1109/IMTC.2008.4547350
15. Kolyadin D.V., Petrov I.B. Algorithm for highlighting extreme points according to the task of biometric verification of a handwritten signature. *Issledovano v Rossii*, 2005, pp. 532–540. (In Russian)
16. Smith S.W. *The Scientist and Engineer's Guide to Digital Signal Processing*. California Technical Pub., 1997, 626 p.
17. Lebedenko Yu.I. *Biometric Security Systems: Textbook*. Tula, TulSU Publ., 2012, 158 p.
18. Rosenblatt F. The perceptron: a probabilistic model for information storage and organization in the brain. *Psychological Review*, 1958, vol. 65, no. 6, pp. 386–408. doi: 10.1037/h0042519
19. Rumelhart D.E., Hinton G.E., Williams R.J. Learning internal representation by error propagation / In *Parallel Distributed Processing. V. I Foundations*. Eds. D.E. Rumelhart, J.L. McClelland. Cambridge, MIT Press, 1988, pp. 399–421. doi: 10.1016/b978-1-4832-1446-7.50035-2
20. Alabbas M., Jaf S. Abdullah A.H.M. Optimize BpNN using new breeder genetic algorithm. *Proc. Int. Conf. on Advanced Intelligent Systems and Informatics*, 2016, no. 533, pp. 373–382. doi: 10.1007/978-3-319-48308-5_36

Авторы

Дикий Дмитрий Игоревич – студент, Университет ИТМО, Санкт-Петербург, 197101, Российская Федерация, Dimandikiy@mail.ru

Артемьева Виктория Денисовна – студент, Балтийский федеральный университет имени И.Канта, Калининград, 236016, Российская Федерация, vika_med2019@mail.ru

Authors

Dmitriy I. Dikiy – student, ITMO University, Saint Petersburg, 197101, Russian Federation, Dimandikiy@mail.ru

Viktoria D. Artemeva – student, Immanuel Kant Baltic Federal University, Kaliningrad, 236016, Russian Federation, vika_med2019@mail.ru