УДК: 519.2, 612.087

П.С. Ложников

Омский государственный технический университет

ИСПОЛЬЗОВАНИЕ СЕТИ МНОГОМЕРНЫХ ФУНКЦИОНАЛОВ БАЙЕСА ДЛЯ НЕЙРОСЕТЕВОГО ПРЕОБРАЗОВАНИЯ РУКОПИСНОЙ ПОДПИСИ ЧЕЛОВЕКА В СЕКРЕТНЫЙ КЛЮЧ ЕГО ЭЛЕКТРОННОЙ ПОДПИСИ

Представлен метод нейросетевого преобразования параметров воспроизведения и внешнего вида рукописной подписи человека в секретный ключ его электронной подписи с использованием сети многомерных функционалов Байеса. Наилучший результат по верификации автографа получен с использованием сети Байеса-Хемминга: вероятности ошибок 1-ого и 2-ого рода составили 0,0288 и 0,0232, соответственно.

Ключевые слова: электронная подпись, рукописная подпись, нейросетевой преобразователь биометрия-код, сети квадратичных форм, сети многомерных функционалов Байеса, сети Байеса-Хемминга

В XXI веке большинство документов создаются при помощи специального программного обеспечения: текстовых редакторов, учетных систем и др. Далее у юридически значимого документа может быть две среды распространения: аналоговая (бумажный документ) и цифровая (электронный документ). В первом случае документ распечатывается на принтере, заверяется рукописной подписью автора, печатью организации. Во втором – документ остается в электронном виде, а для обеспечения аутентичности и целостности заверяется электронной подписью. Сегодня мы наблюдаем, как целые сегменты документооборота переносятся в цифровую среду: государственные услуги, банковское обслуживание, электронные закупки.

В связи с этим возрастает количество судебных разбирательств, связанных с несанкционированным созданием электронных документов. Пользователи допускают доступ посторонних лиц к секретным ключам своей электронной подписи, передают эти ключи неуполномоченным лицам, допускают наличие на компьютерах вредоносных программ. Перечисленные нарушения маркируют главную проблему информационной безопасности в цифровой среде при использовании электронной подписи: она в отличие от рукописного автографа отчуждаема от владельца. Если злоумышленник завладел секрет-

ным ключом чужой электронной подписи и подписал с её помощью документ, то такой документ будет юридически значимым согласно законодательству. Сегодня подавляющее большинство судебных решений выносится не в пользу владельцев таких дискредитированных электронных подписей.

В аналоговой среде, где для придания юридической силы бумажному документу на него ставится рукописная подпись, проблемы её отчуждения от владельца нет. Там есть другая проблема – подделка рукописной подписи злоумышленником. Чтобы доказать подделку подписи в суде необходимы большие временные затраты для проведения почерковедческой экспертизы. При этом у хозяина рукописной подписи, которую воспроизвел злоумышленник, всегда есть шансы доказать факт подделки.

Таким образом, обозначены две проблемы связанные с использованием подписей для заверения документов в аналоговой и цифровой средах. Сам термин «подпись» имеет разную природу в каждой среде: в аналоговой – это динамический биометрический образ зафиксированный на бумаге в виде изображения автографа, в цифровой – это результат криптографического преобразования секретного (закрытого) ключа и хэш-функции документа.

Предлагается перейти к гибридной среде документооборота, которая предполагает взаимоисключенье выше обозначенных проблем. Гибридный документ может находиться на электронном или бумажном носителе и содержать изображение автографа, защищенное с помощью электронной подписи, а также тайных или открытых биометрических образов, благодаря чему можно быстро (за приемлемое время) проверить его целостность и аутентичность независимо от типа носителя. Ключевым атрибутом гибридного документа является электронная подпись, при формировании которой используются биометрическая рукописная подпись субъекта (автограф или рукописный пароль). При этом применяются алгоритмы преобразования биометрических признаков в секретный ключ электронной подписи. Под признаками подразумеваются особенности внешнего вида и воспроизведения рукописной подписи, которые характеризует владельца электронной подписи [1].

Опишем принцип работы предлагаемого метода. Для генерации секретного ключа электронной подписи из биометрических данных строится преобразователь биометрия-код (ПБК). Основное отличие ПБК от методов обычной биометрической аутентификации состоит в том, что каждый образец биометрических данных предварительно преобразуется в битовую (ключевую) последовательность, которую возможно использовать в целях аутентификации субъекта или криптографической защиты документов (в качестве кода досту-

па, ключа шифрования и т.д.). При этом эталон субъекта должен храниться в виде вспомогательной информации, не позволяющей восстановить из нее биометрические характеристики субъекта. Требования к защите биометрического эталона при разработке систем высоконадежной биометрической аутентификации прописаны в ГОСТ Р 52633.0-2006 (пункты 5.2-5.3 стандарта). Если генерируется нехарактерный для субъекта код, происходит ошибка 1-ого рода. За ошибку 2-ого рода принимается ситуация, при которой коды, полученные из биометрических данных двух различных субъектов, совпадают. Вероятности ошибок 1-ого (FRR, False Rejection Rate) и 2-ого (FAR, False Acceptence Rate) рода характеризуют надежность ПБК. При верификации кода решение принимается исходя из допустимого расстояния Хемминга H между генерируемым и верным кодами.

Изначально сложилось два основных подхода к реализации ПБК: «нечеткий экстрактор» и нейросетевой ПБК [2]. По результатам исследований и экспериментального сравнения данных подходов установлено, что нечеткие экстракторы на основе классических самокорректирующихся кодов существенно уступают нейронным сетям в надежности генерации ключевых последовательностей, а также обладают множеством недостатков [1-4]. Нейросетевой ПБК основан на идее использования искусственных нейронных сетей. Эффективнее использовать большие нейронные сети с малым числом слоев и их модификации. Использование данного подхода в приложениях биометрической аутентификации является рекомендуемым в России. Данный подход стандартизован. В ГОСТ Р 52633.5-2011 описан первый не итерационный абсолютно устойчивый алгоритм обучения сети персептронов, разработанный для биометрии. Рекомендуется использовать однослойные или двухслойные нейронные сети, большее количество слоев считается избыточным. Согласно ГОСТ Р 52633.5-2011 для обучения персептронов требуется не менее 21 реализации образа «Свой» и 64 независимых реализации образа «Чужой». Модули весов нейронов первого слоя вычисляются по формуле:

$$\mu_j = |M_{\text{ч}}(a_j) - M_{\text{с}}(a_j)| \,/\, \sigma_{\text{ч}}(a_j) \cdot \sigma_{\text{с}}(a_j), \qquad (1)$$

где $M_{\text{с}}(a_j)$ – математическое ожидание значений j-ого признака образа «Свой», $\sigma_{\text{с}}(a_j)$ – среднеквадратичное отклонение значений j-ого признака образа «Свой», $M_{\text{ч}}(a_j)$ и $\sigma_{\text{ч}}(a_j)$ – аналогичные показатели образа «Чужой».

Если нейрон настроен на выдачу единицы при поступлении реализации образа «Свой», то знак весового коэффициента выбирается исходя из правила: «+» при $M_{\text{ч}}(a_j) < M_{\text{с}}\langle a_j \rangle$, иначе «-». Если нейрон настроен на нуль, знаки ин-

вертируются. (1), а выход сумматора нейрона на этапе верификации определяется по формуле:

$$y_i = \sum_{j=1}^{m} \mu_j \cdot a_j + \mu_0, \qquad (2)$$

где a_j – значение j-ого входа i-ого нейрона, ассоциированного с одним из признаков, m – число входов нейрона, μ_j – весовой коэффициент j-ого входа i-ого нейрона, μ_0 – нулевой вес, отвечающий за переключатель квантователя нейрона (пороговое значение), m – количество входов нейрона.

Исследования показывают, что персептроны не являются эффективными, если взаимная корреляционная зависимость признаков является высокой по шкале Чеддока (модуль коэффициента корреляции $|r|>0,7$). Для признаков со слабой взаимной зависимостью ($|r|<0,7$) лучше использовать сети малоразмерных квадратичных форм (3), для признаков с заметной, высокой и очень высокой зависимостью ($|r|>0,5$) лучше использовать сети многомерных функционалов Байеса (4). Данные функционалы в указанных случаях обогащают биометрические данные эффективней персептронов.

$$y_i = \sum_{j=1}^{m} \frac{\left(M_c\left(a_j\right) - a_j\right)^2}{\sigma_c\left(a_j\right)^2}, \qquad (3)$$

$$y_{k,j} = \sum_{i=1}^{m} \left| \frac{\left|M\left(a_k\right) - a_{k,j}\right|}{\sigma\left(a_k\right)} - \frac{\left|M\left(a_i\right) - a_{i,j}\right|}{\sigma\left(a_i\right)} \right|, \qquad (4)$$

где $a_{i,j}$ – значение i-ого признака (входа нейрона) с высоким значением модуля корреляции $|r_{i,k}|$ по отношению к k-ому биометрическому признаку $a_{k,j}$ ($i \neq k$), j – номер биометрического образца образа «Свой», для которого вычисляется функционал.

Проведен эксперимент по оценке надежности принимаемых решений каждой сетью. При формировании сети функционалов (3) обработчики признаков соединялись с нейронами случайным образом. Количество нейронов N и входов m задавалось как параметр и изменялось в процессе вычислительного эксперимента. Сеть многомерных функционалов Байеса (4) формировалась исходя из модуля равной коррелированности, под которой подразумевается, что разница $|r|$ для признаков не превышает τ (значение τ задавалось как параметр). Также как параметр задавалось максимальный модуль корреляции учитываемых признаков ϕ. Независимо от типа нейрона значение на выходе его функционала сравнивается с пороговым. Для каждого нейрона существует оп-

тимальный порог срабатывания, который вычисляется исходя из откликов обучающих примеров образа «Свой» [1].

В процессе эксперимента подтверждено, что многомерный функционал Байеса делает тем меньше ошибок, чем выше коэффициент равной коррелированности признаков и выше его размерность. Повышение размерности функционалов позволяет снизить вероятность ошибок до попадания на участок насыщения, дальнейшее повышение размерности не дает преимуществ. Если повысить пороговое значение расстояния Хемминга *H* от генерируемого до верного ключа электронной подписи, то можно получить выигрыш по сумме FRR+FAR. Наивысшим потенциалом по снижению ошибок, таким способом, обладает сеть Байеса-Хемминга. При генерации кода на основе биометрических данных аналогичного эффекта можно добиться корректировкой нескольких неверных бит на выходе первого слоя сети нейронов с помощью корректирующих кодов, предложенных в работе [5]. Увеличение количества решающих правил целесообразно проводить пока правила ошибаются по-разному, т.е. не полностью 128нновационного. Наилучший результат по генерации ключа электронной подписи из рукописной биометрической подписи получен на основе сети Байеса-Хемминга: FRR=0,0288, FAR=0,0232.

Литература

1. Ложников П.С., Сулавко А.Е., Еременко А.В., Волков Д.А. Экспериментальная оценка надежности верификации подписи сетями квадратичных форм, нечеткими экстракторами и персептронами // Информационно-управляющие системы. – 2016, № 5 (84). – С. 73-85.

2. Ахметов Б.С., Иванов А.И., Фунтиков В.А., Безяев А.В., Малыгина Е.А. Технология использования больших нейронных сетей для преобразования нечетких биометрических данных в код ключа доступа: Монография. / Алматы: ТОО «Издательство LEM», 2014 – 144 с.

3. Lozhnikov P.S., Sulavko A.E., Eremenko A.V., Volkov D.A. Methods of Generating Key Sequences based on Parameters of Handwritten Passwords and Signatures // Information. – 2016, № 7(4), 59. DOI: 10.3390/info7040059.

4. Еременко А.В., Ложников П.С., Сулавко А.Е. Генерация ключевых последовательностей на основе параметров подсознательных движений // Информационные системы и технологии. – 2017, № 1 (99). – С. 99-109.

5. Безяев А.В., Иванов А.И., Фунтикова Ю.В. Оптимизация структуры самокорректирующегося био-кода, хранящего синдромы ошибок в виде фрагментов хеш-функций // Вестник УрФО. Безопасность в информационной сфере. – 2014, № 3(13). – С. 4-13.