Теоретический и прикладной научно-технический журнал

ISSN 1694-5557

ИЗВЕСТИЯ

Кыргызского государственного технического университета им. И. Раззакова

№ 2 (42)

БИШКЕК 2017

СОДЕРЖАНИЕ

УДК 681.322

АНАЛИЗ ИСПОЛЬЗОВАНИЯ ТЕХНОЛОГИЙ РАСПОЗНАВАНИЯ БИОМЕТРИЧЕСКИХ ОБРАЗОВ

***Алимсеитова Жулдыз**, аспирант КГТУ им. И. Раззакова Кыргызской Республики +7 777 359 81 05, e-mail: zhuldyz_al@mail.ru*
***Акматалиева Жазгул Зарылбековна** аспирант КГТУ им.И.Раззакова, Кыргызской Республики 720044 (+996) 54-54-35, e-mail: zakmatalieva@gmail.com*
***Боскебеев Калычбек Джетмишбаевич**, к.т.н., профессор, КГТУ им. И. Раззакова, 720044, Кыргызская Республика 720044 (+996) 56-13-15, e-mail: kboskebeev@mail.ru.*

В связи с частой компроментацией, утерей таких идентификаторов, как пароль, пин-код, пластиковые карты с ключом, е-токенов все чаще в качестве идентификаторов используются биометрические параметры человека. Эти параметры нельзя забыть дома, потерять или передать другому, так как они неотъемлемая часть человека. Это поставило перед научным обществом вопрос их распознавания.

США и страны Евросоюза применяют «нечеткие экстракторы» для того, чтобы связать биометрические данные человека с его криптографическим ключом. «Нечеткие экстракторы» рассматривают как алгоритмы, которые в условиях зашумленности выделяют из биометрических данных случайные, равномерно распределенные последовательности битов. Кроме того, они могут компенсировать ошибки возникающие из-за того, что невозможно абсолютно точно повторно воспроизвести биометрические данные [1-2].

В России и Казахстане используют преобразователи биометрия-код. Такие преобразователи строятся с использованием искусственных нейронных сетей [3-4]. Для этого сначала необходимо выбрать структуру связей нейронов сети, затем ее обучить. Обучение производиться так, чтобы примеры биометрического образа «Свой» на выходе преобразователя давали код личного криптографического ключа гражданина России или Казахстана, а для примеров образов «Чужой» на выходе преобразователя получалась случайная кодовая комбинация.

Для получения одного бита криптографического ключа одного биометрического параметра недостаточно. Для того, чтобы в «нечетких экстракторах» исправлять ошибки кодирования или нейронной сетью преобразователя «обогащать» входные биометрические данные необходимо обязательно использовать избыточное число биометрических параметров.

Ключевые слова: аутентификация, «нечеткий экстрактор», ключ, нейросетевые преобразователи биометрия-код, нейросетевой контейнер, самокорректирующийся код, искусственные нейроны, обучение нейрона.

ANALYSIS OF THE USE OF BIOMETRIC TECHNOLOGIES OF RECOGNITION OF IMAGES

***Alimseitova Zhuldyz,** the graduate student of KGTU of I. Razzakov of the Kyrgyz Republic +7 777 359 81 05, e-mail: zhuldyz al@mail.ru Akhunov Toichubek Beshenaliyevich*
***Akmatalieva Jazgul Z.,** the graduate student of KGTU of I.Razzakov of the Kyrgyz Republic, 720044 (+996) 54-54-35, e-mail: zakmatalieva@gmail.com*
***Boskebeev Kalychbek D.,** Ph.D. (Engineering), Professor, KGTU of I.Razzakov Kyrgyz Republic, 720044 (+996) 56-13-15,e-mail:kboskebeev@mail.ru*

In connection with frequent complementaria, loss of identifiers such as a password, pin number, plastic cards with key, e-token, increasingly, the identifiers used in biometric parameters of the person. These parameters cannot be forgotten at home, lost or transferred to another, as they are an integral part of man. This has set the scientific community on the issue of their recognition.

The US and the EU use "fuzzy extractors" in order to associate biometric data of the person with its cryptographic key. "Fuzzy extractors" are considered as algorithms, which in terms of noise isolated from the biometric data random, uniformly distributed sequence of bits. In addition, they can compensate for the error arising from the fact that it is impossible exactly to be replayed biometric data [1-2].

In Russia and Kazakhstan use converters biometrics code. Such converters are constructed using artificial neural networks [3-4]. To do this, you must first choose the pattern of connections of neurons of the network, and then to train her. The training is carried out so that the examples of the biometric image "Own" at the Converter output was given code of personal cryptographic key of a citizen of Russia or Kazakhstan, and for examples of images of "Alien" at the output of the Converter will get a random code combination.

To obtain one bit of cryptographic key from one biometric parameter is not enough. In order to "fuzzy extractors" fix coding error or a neural network transducer to "enrich" the input biometric data must necessarily use an excessive number of biometric parameters.

Key words: authentication, "fuzzy extractor", key, neural network converters biometrics code of neural network container, self-correcting code, the artificial neurons, learning of the neuron.

В настоящее время исследованиями, связанными с преобразованием неоднозначных нечетких биометрических образов личности в длинный пароль или полноценный ключ занимаются в России, Белоруссии, Казахстане, США, Канаде, странах Евросоюза и Южной Корее. Все преобразователи биометрии в код делятся на «нечеткие экстракторы» [1-2] и нейросетевые преобразователи биометрия-код [3-4]. Исследователи США, Канады, стран Евросоюза и Южной Кореи внесли основной вклад в развитие технологии «нечетких экстракторов». Исследователями России, Белоруссии и Казахстана разрабатываются нейросетевые преобразователи биометрия-код. Эти две технологии отличаются только положением квантователя непрерывных биометрических данных.

Для решения вопроса идентификации США, Канада, страны Евросоюза и Южная Корея предлагает использовать аппарат нечетких множеств. Англоязычная криптографическая общественность основным преимуществом «нечетких экстракторов» считала их относительно высокий уровень защищенности и простоту (прозрачность) используемой защиты. Рисунок 1 показывает принцип защиты данных «нечетких экстракторов».

Рисунок 1 – Формирование нечетких контейнеров и их использование

Чтобы защитить «сырые» биокоды используют секретный ключ. На этот ключ накладывают любой избыточный самокорректирующийся код, способный обнаруживать и исправлять ошибки. Обычно используются коды БЧХ (Боуза-Чоухуры-Хоквингема) и получают гамму в десять раз длиннее кода секретного ключа. Потом на «сырой» биокод накладывают гамму и получают «нечеткий контейнер». «Нечеткий контейнер» хранится в памяти средств биометрической аутентификации. Такой способ считается относительно безопасным в США и странах НАТО, и за рубежом эта технология активно развивается.

В процессе аутентификации из памяти извлекают «нечеткий контейнер» и его данные складывают с введенным и оцифрованным биометрическим образом по модулю два. При этом восстанавливается избыточный самокорректирующийся код криптографического ключа, который содержит ошибки, унаследованные от двух биокодов. Это от биокода формирования нечеткого контейнера и биокода аутентификации. Если исправляющая способность самокорректирующегося кода больше числа таких ошибок, то они правятся.

Схема предлагаемой обработки информации показана на рисунке 2.

Начинается схема с использования безопасной схемы преобразования. В ней для указания рамок осуществления преобразования необходимо задать допустимую разность множеств. Нечеткие преобразования осуществляются если входное биометрическое воздействие не сильно отличается от эталонного множества и они безопасны.

Рисунок 2 – Схема преобразования нечетких биометрических данных личности в код

Эту технологию фактически можно рассматривать как синтез некоторой нечеткой хэш-функции, где заданной длины входная последовательность предварительно корректируется некоторым линейно взвешенным кодом с обнаружением и исправлением ошибок.

Проводимые в Казахстане, России и Белоруссии исследования показали, что использование искусственных нейронных сетей в существующих биометрических технологиях дает значительное их усиление [3-4]. Они в непрерывной форме осуществляют обогащение данных. Для корректировки всех входных ошибок оказывается достаточно двукратной избыточности. Например, нейронная сеть практически без ошибок преобразует 512 входных биометрических параметров в 256 бит выходного кода.

Нейросетевые преобразователи биометрия-код с точки зрения получения биометрических свойств лучше «нечетких экстракторов». Этот тезис никто не оспаривает. Рассмотрев биометрические данные, которые дают ошибки в 50% и более разрядах биокода можно это легко продемонстрировать. Классические самокорректирующиеся коды не могут исправить больше 50% ошибок. Если избыточность нейронных сетей повысить до трех раз (входов в три раза больше, чем выходов), то они справляются с данной проблемой.

Использование больших нейронных сетей позволяет учитывать как «хорошие» биометрическими данные, так и «плохие» и «очень плохие» биометрические данные. И чем «хуже» используемые биометрические данные, тем большая сеть искусственных нейронов необходима и тем сложнее ее обучать.

Общая структура системы биометрико-нейросетевой аутентификации показана на рисунке 3.

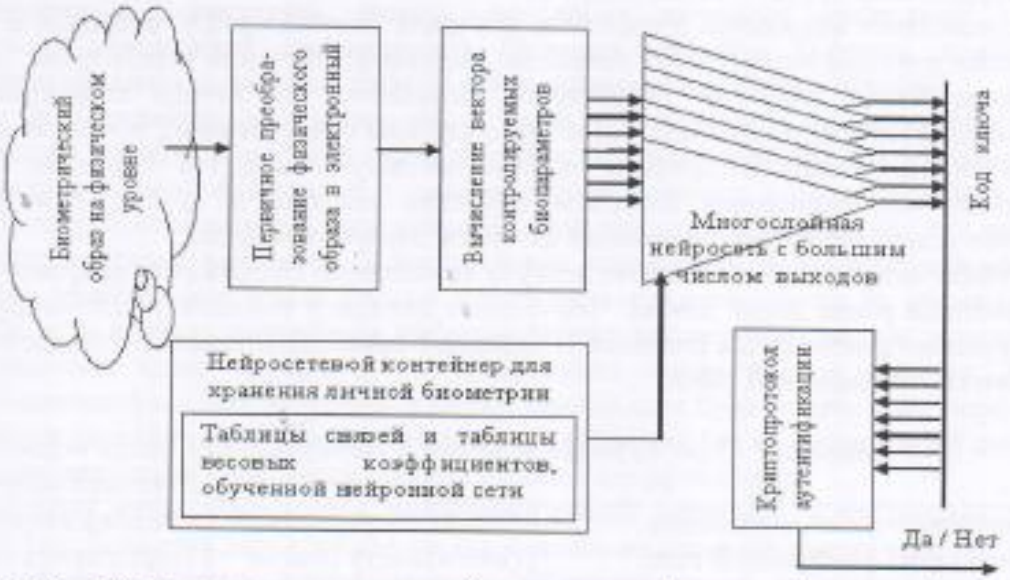

Рисунок 3 – Общая структура системы биометрико-нейросетевой аутентификации

Для решения подобной задачи искусственные нейронные сети низкой размерности непригодны [3-4].

На рисунке 4 в виде схемы представлен процесс преобразования входного биометрического образа в выходной длинный пароль (ключ).

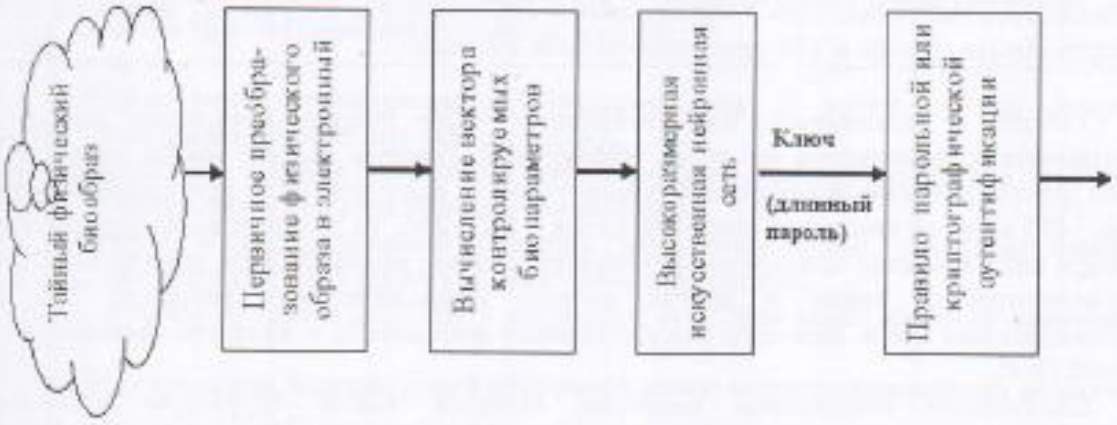

Рисунок 4 – Схема обработки информации в системах биометрико-нейросетевой аутентификаци

Обучение искусственной нейронной сети должно проходить без вмешательства человека, то есть параметры сети должны подбираться автоматически. Пользователь должен быть уверен в том, что его длинный пароль или ключ, который участвует в обучении сети не будет скомпрометирован [3-4].

При обучении искусственной нейронной сети ее весовые коэффициенты должны подбираться автоматом обучения так, чтобы когда на входе искусственной нейронной сети появлялся вектор элементов «Свой» на выходе должен появиться длинный пароль (ключ). А если на входах искусственной нейронной сети появляются вектора данных образа «Чужой», на выходах искусственной нейронной сети должен появляться «белый шум», то есть случайные состояния. Для обучения необходимо по очереди подавать образы «Свой» и «Чужие» с промежуточным подбором коэффициентов [4].

Использование нейросетевого обогащения био-данных требует необходимость умения обучать одиночные искусственные нейроны.

Существует множество алгоритмов обучения искусственных нейронов и вариантов исполнения функции возбуждения нейронов. Например, обучение персептрона, основанное на правиле Хебба, обучение персептрона, основанное на методе коррекции ошибки, итерационный алгоритм обучения одиночного нейрона (персептрона), обучение одиночного нейрона итерационным алгоритмом поиска максимума качества обучения, абсолютно устойчивый неитерационный алгоритм обучения нейрона и другие. Мы используем абсолютно устойчивый неитерационный алгоритм обучения нейрона.

Чтобы получить биокод ключа доступа необходимо создать сеть нейронов у которых число выходов равна длине ключа. Чем больше входов и выходов у нейронной сети, тем выше качество принимаемых решений. В таблице 1 приведены данные, которые показывают насколько сильна подобная связь.

Таблица 1 - Рост качества решений в зависимости от числа входов и выходов искусственной нейронной сети

Число входов нейронной сети	Число выходов нейронной сети	Ошибка первого рода (вероятность отказа «Своему»)	Ошибка второго рода (вероятность пропуска «Чужого»)
5 входов	1 выход, 2 класса	$P_1 = 0,1$	$P_2 = 0,17$
48 входов	1 выход, 2 класса	$P_1 = 0,1$	$P_2 = 0,03$
480 входов	1 выход, 2 класса	$P_1 = 0,1$	$P_2 = 0,005$
480 входов	256 выходов, 2^{256} классов	$P_1 = 0,1$	$P_2 = 0,000000001$
Обучение нейронной сети проводилось алгоритмом ГОСТ Р 52633.5–2011. Для этого использовалась нейронная сеть с 480 входами и 256 выходами. Обучение велось на 20 примерах образа «Свой» и 128 примеров образов «Чужой».			

Таблица 1 показывает, что увеличение числа входов для числа учитываемых биометрических параметров не очень эффективно. Гораздо важнее чтобы параллельно с числом входов нейронной сети увеличивать число ее выходов. Если при одинаковом числе входов (480 входов) увеличить число выходов с 1 до 256, то это даст выигрыш примерно в миллиард раз в качестве принимаемых нейронной сетью решений. При этом примерно в 100 раз увеличиваются время и другие затраты вычислительных ресурсов. Тут видна экспоненциальная связь размеров искусственного интеллекта и качества принимаемых им решений [3-4].

Следующим важнейшим вопросом является выбор структуры используемой нейронной сети. В литературе по искусственным нейронным сетям сети разделяют на одно-, двух-, трехслойные, и сети с большим, чем три числом нейронов. ГОСТ Р 52633.5–2011 предусматривает либо однослойные, либо двухслойные нейронные сети. При выборе двухслойных нейронных сетей функции первого и второго слоев разделены. Нейроны первого слоя выполняют следующие функции: функцию обогащения биометрических данных и функцию квантования обогащенных данных. второй слой нейронов правит ошибки биокода нейронов первого слоя, если качество обогащения оказалось недостаточным [4].

Второй слой нейронов может быть заменен обычным классическим кодом, обнаруживающим и исправляющим ошибки. Однако нейросетевое корректирование ошибок выгоднее. Причина выгодности состоит в том, что при обучении второго слоя на примерах биокодов «Свой» оценивают реальный показатель стабильности каждого из разрядов биокода.

При обучении второму слою выделяют следующие функции: корректировка нестабильные разрядов и одновременно хэширование (перемешивание) стабильных и

нестабильных разрядов. Все классические коды с обнаружением и исправлением ошибок строятся в рамках гипотезы о равновероятном распределении ошибок между разрядами кода [4]. Нейросетевые корректоры ошибок во время обучения учитывают реальное распределение показателей стабильности биокодов «Свой». Поэтому классические самокорректирующиеся коды проигрывают нейросетевым корректорам ошибок.

При формировании сети кроме числа слоев нейронов сети нужно выбирать число входов каждого нейрона и задавать связи входов с номерами входов сети. Например, если вся нейронная сеть имеет 480 входов и средняя информативность входов составляет порядка 0.3 бита, то потребуется использовать нейроны с числом входов от 1 до 18. Это зависит от качества используемых нейроном биометрических параметров и корреляционных связей между ними. Необходимое число входов может быть найдено только во время обучения нейрона. То есть сначала случайным выбором задают малое число входов и потом, если качество решения ниже заданного, то увеличивают число входов нейрона. В итоге получается однослойная сеть нейронов. Каждый нейрон сети будет иметь свое число входов, подключенных случайно к входам всей сети. После обучения для входных связей каждого из нейронов дополнительно получается таблица весовых коэффициентов.

Обученная сеть описывается таблицами связей нейронов и таблицами весовых коэффициентов. Если сеть двухслойная, то для каждого из слоев создаются таблицы номеров связей и таблицы весовых коэффициентов. Обучение слоев нейронов производиться последовательно. После обучения первого слоя нейронов примеры образов «Свой» и «Все Чужие» транслируются с входа нейронной сети на выходы нейронов. В итоге получают примеры биокодов и обучают на них нейроны второго слоя.

Таблицы связей нейронной сети и таблицы весовых коэффициентов, обученных нейронов, образуют так называемые нейросетевые контейнеры. В нейросетевом контейнере храниться достаточно информации, чтобы при необходимости можно было воспроизвести программно обученную нейросеть и преобразовать биометрические данные человека в код его криптографического ключа доступа [4].

Выводы:

- нейросетевые преобразователи биометрия-код с точки зрения получения биометрических свойств «нечетких экстракторов»;
- больше 50% ошибок позволяют скорректировать нейронные сети с трехкратной избыточностью (входов в три раза больше, чем выходов);
- переход к использованию больших нейронных сетей позволяет учитывать «хорошие», «плохие» и «очень плохие» биометрические данные;
- чем больше входов и выходов у нейронной сети, тем выше качество принимаемых решений;
- выбор структуры, используемой нейронной сетью является важнейшим вопросом.

Список литературы

1. Uludag U., Pankanti S., Prabhakar S., Jain A. K. Biometric cryptosystems: issues and challenges // Proceedings of the IEEE. – 2004. – Vol. 92. – № 6. – P. 948–960.

2. Baek J., Susilo W., Zhou J. New construction of fuzzy identity-based encryption // Proceedings of the 2nd ACM Symposium on Information, Computer and Communications Security. ACM New York. NY, USA, 2007. – P. 368–370.

3. Ахметов Б.С., Надеев Д.Н., Фунтиков В.А., Иванов А.И., Малыгин А.Ю. Оценка рисков высоконадежной биометрии: монография. – Алматы: КазНТУ, 2014. – 123с.

4. Ахметов Б.С., Иванов А.И., Фунтиков В.А., Малыгин А.Ю. Основы биометрической аутентификации личности. Учебное пособие - Алматы: КазНТУ им. К.И. Сатпаева, 2014. - 151с.