6. Sarkis G., Gross W.J. Increasing the throughput of polar decoders. *IEEE Communications Letters*, 2013, vol. 17, no. 4, pp. 725–728.
7. Sarkis G. et al. Fast polar decoders: Algorithm and implementation. *IEEE Journal on Selected Areas in Communications*, 2014, vol. 32, no. 5, pp. 946–957.
8. Hashemi S.A., Condo C., Gross W.J. Fast and flexible successive-cancellation list decoders for polar codes. *IEEE Transactions on Signal Processing*, 2017, vol. 65, no. 21, pp. 5756–5769.
9. Giard P. et al. PolarBear: A 28-nm FD-SOI ASIC for decoding of polar codes. *IEEE Journal on Emerging and Selected Topics in Circuits and Systems*, 2017, vol. 7, no. 4, pp. 616–629.
10. Karpuhina E.K. Methods for protecting the cluster number in the procedure of lexicographic decoding of block codes. *Sovremennye problemy proektirovanija, proizvodstva i ekspluatatsii radiotehnicheskih sistem: sb. nauch. trudov*, 2019, pp. 130–132. (In Russ.)
11. Namestnikov S.M., Chilihin N.Yu., Karpuhina E.K. Conceptual model of decision making by a quasi-intelligent decoder when processing information in a communication channel with unknown parameters. *Radiolokatsija, navigatsija, svjaz': sb. trudov XXV Mezhdunarodnoj nauchno-tehnicheskoj konferentsii, posvjaschennoj 160-letiju so dnja rozhdenija A.S. Popova. V 6-ti tomah*, 2019, pp. 177–182. (In Russ.)

Received 14.10.2021

ЭЛЕКТРОМАГНИТНАЯ СОВМЕСТИМОСТЬ И БЕЗОПАСНОСТЬ ОБОРУДОВАНИЯ

УДК 004.056

АНАЛИЗ СОВРЕМЕННОГО УРОВНЯ РАЗВИТИЯ БИОМЕТРИЧЕСКОЙ КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ

Баянов Б.И.
Казанский национальный исследовательский технический университет им. А.Н. Туполева – КАИ, Казань, РФ
E-mail: bayanov_bulat@mail.ru

В статье представлен анализ современных научных достижений в сфере биокриптографической защиты информации. Основным предметом исследования являются алгоритмы формирования криптографического ключа на основе биометрических параметров пользователя. Проведен сравнительный анализ этих алгоритмов – преобразователей «биометрия-код»: нечетких экстракторов и нейросетевых преобразователей. В качестве биометрических параметров в первую очередь рассматривается динамический рукописный почерк, также частично биометрические параметры клавиатурного почерка, голосового отпечатка, биометрии лица. Приведена классификация задач биометрической защиты информации, указаны рекомендации по разработке методов первичной обработки биометрических данных. Представлены оценки качества работы анализируемых алгоритмов, преимущества и недостатки преобразователей Биометрия-код доступа на их основе. Представленные результаты могут быть полезны специалистам в сфере биометрической защиты информации при выборе перспективных научных исследований.

Ключевые слова: *информационная безопасность, аутентификация, автоматическая верификация подписи, идентификация, распознавание образов, нечеткие экстракторы, нейросетевой преобразователь «биометрия-код»*

Введение

История развития биометрической защиты информации с точки зрения автоматизированной системы распознавания биометрических образов берет начало с 60-х годов XX века, когда впервые разрабатываются автоматизированные системы идентификации отпечатков пальцев (АСИОП) [1]. Появление таких систем обусловлено развитием электронных вычислительных машин общего назначения, потребностью их применения в правоохранительных органах из-за большого роста объемов данных биометрических образов и т. д.

Начало современной истории развития биометрической защиты информации связано с крупным историческим событием – страшной трагедией 11 сентября 2001 года. Такое положение событий

побудило внести кардинальные изменения в системе безопасности учреждений и организаций крупных мегаполисов, что в свою очередь побудило граждан изменить свое отношение к нововведениям в процедурах обеспечения общественной информационной безопасности [2].

Будущее биометрической защиты информации стоит за использованием биометрических данных (БД) в криптографических системах. Это позволит использовать биометрические показатели в системах электронной цифровой подписи (ЭЦП). Такие новые биометрические технологии будут вводиться в системах шифрования, а также использоваться в системах аутентификации для усовершенствования систем контроля доступа.

Одни из первых шагов в области формирования криптографического ключа (КК) на основе биометрических параметров (БП) пользователя сделаны в 2008 году. В январе 2008 года вышла в свет работа [3] американских ученых с упоминанием метода нечетких экстракторов (НЭ, Fuzzy Extractors). Подход НЭ активно развивается за рубежом и утвержден в стандартах ISO/IEC 24745:2011, ISO/IEC 24761:2009, ISO/IEC 19792:2009.

В России в этой сфере активно развивается направление использования нейросетевых моделей. Подробное описание и список замечаний по практической реализации преобразователей для решения задач подобного рода утверждены в документах серии стандартов ГОСТ Р 52633 [4]. С этого момента история развития интересующей нас отрасли науки связана с совершенствованием двух вышеперечисленных научных подходов.

Основной причиной интенсивного развития рассматриваемой научной дисциплины послужил высокий общественный интерес к биометрической защите информации, а также высокий уровень развития распознавания биометрических образов, математического аппарата нейронных сетей, технических средств считывания БД и т. д. Таким образом, приступая к задаче построения алгоритмов формирования КК на основе конкретного рода БП пользователя, рекомендуется рассматривать и другие смежные отрасли наук (биометрическая аутентификация, верификация, идентификация пользователя), в том числе и другие типы БП.

Классификация задач биометрической защиты информации

Представим следующую систему классификации задач биометрической защиты информации с указанием необходимых литературных источников:

– тип БП: динамические БП (динамический рукописный почерк [5–12], клавиатурный почерк [13–16], голосовой отпечаток [10; 11; 17–19]) и статические (статический рукописный почерк [6; 20; 21], биометрия лица [15; 22; 23], отпечатки пальцев и т. д.), мультифакторные системы (например, голосовой отпечаток совместно с рукописным и клавиатурным почерками) [9; 10; 15; 18];

– тип задачи: аутентификация [10; 12; 24], верификация [6; 11; 25], идентификация [9; 18], формирование КК на основе БП пользователя [5; 7; 8; 13–15; 17; 19–23];

– сфера использования: шифрование [26; 27], электронная цифровая подпись [28], аутентификация;

– тип парольной фразы: в секрете [13; 14; 19], публичная [5–8; 11–14; 19; 21–23], произвольный текст (freely typed text) или мониторинг [13–15; 19];

– наличие в базе данных биометрических образов «Свой» или «Чужой»;

– тип преобразователя «биометрия-код» (ПБК): НЭ [5; 7; 13; 14; 17; 19; 21; 23], НПБК [7; 8; 10; 11; 15; 20; 22; 23].

Отметим, что задача формирования КК на основе БП пользователя является универсальной и используется в решении всех остальных типов задач (верификация, идентификация и т. д.), а также внедряется во все вышеописанные сферы использования (формирование ЭЦП, шифрование, аутентификация). Принцип работы НЭ подробно описан в работах [14; 17]. Известны схожие версии изложения данного алгоритма (Fuzzy Extractors): Fuzzy Vault (нечеткое хранилище), Fuzzy Commitment [7; 29]. Принцип работы НПБК подробно описывается в источниках [2; 4; 30].

Сравнительный анализ преобразователей «биометрия-код»

В алгоритме НЭ для формирования КК на основе БП пользователя изначально формируется ключевая информация – случайная битовая последовательность, которая кодируется помехоустойчивым кодом (Адамара, Боуза – Чоудхури – Хоквингема и т. д.). Данная последовательность «объединяется» с битовой последовательностью, характеризующей биометрический образ пользователя (сложением по модулю 2 или алгоритмами нечеткого вывода). Результатом объединения является открытая строка, которая может храниться на общедоступном сервере. Также хранится вспомогательная информация помехоустойчивого кодирования. Для восстановления ключевой информации пользователь предоставляет свой биометрический образ, на основе которого фор-

Таблица 1. Преимущества и недостатки преобразователей Биометрия-код

Преимущества НЭ	Недостатки НЭ	Преимущества НПБК	Недостатки НПБК
Не требует наличия в базе данных биометрических образов «Чужой»	Относительно высокие показатели EER	Относительно низкие показатели EER	Требует наличия в базе данных биометрических образов «Чужой»
КК и БП не хранятся в базе данных	Высокая избыточность классических самокорректирующих кодов, в результате плохое качество работы при высокой степени разброса БП	КК и БП не хранятся в базе данных	Ресурсные затраты в программной реализации
Не требует наличия большой длины последовательности БП	Фиксированное количество разрядов (бит), определяющих значение БП	Не требователен к процессу отбора качественных БП	Требует наличия достаточно большой длины последовательности БП
Прост в реализации системы	Неустойчивость к сдвигам значений БП по времени	Устойчив к сдвигам значений БП по времени	Сложность реализации системы
	Наличие уязвимостей, позволяющих ускорить перебор значений БП в целях фальсификации ключа доступа		

мируется соответствующая битовая последовательность. Затем она применяется в «вычитании» из открытой строки (сложением по модулю 2 или алгоритмами нечеткого вывода). Результативная битовая последовательность корректируется в процессе помехоустойчивого кодирования и преобразуется в исходную ключевую информацию [14].

В алгоритме НПБК используется многослойная искусственная нейронная сеть. В процессе обучения нейронной сети входными значениями являются значения БП примеров биометрического образа «Свой» и значения БП примеров биометрических образов «Чужой». При этом выходными значениями нейронной сети для примеров биометрического образа «Свой» являются значения последовательности ключевой информации, которая представляет КК. Для примеров биометрических образов «Чужой» выходными значениями являются значения последовательности случайно сгенерированной информации, не совпадающей с заранее сформированной ключевой информацией. Для восстановления ключевой информации при тестировании и использовании обученной нейронной сети предоставляются тестовые значения БП биометрического образа «Свой» и архитектура обученной нейронной сети (количество слоев, нейронов, весовые коэффициенты и т. д.). В этом случае, если пользователь обладает БП биометрического образа «Чужой», то нейронной сетью формируется бесполезная последовательность случайных значений, а не ключевая информация. В соответствии с ГОСТ Р 52633.5-2011 рекомендуется использовать однослойные или двухслойные нейронные сети, большее количество слоев считается избыточным и необоснованным. Первый слой обогащает биометрические данные, второй слой играет роль кодов, исправляющих ошибки. При этом для обучения персептронов требуется не менее 21 реализаций образа «Свой» и 64 независимых реализаций образа «Чужой» [8].

По данным [7; 8; 11; 15; 22] и результатам проведенных нами исследований, выделим следующие преимущества и недостатки НЭ и НПБК, представленные в таблице 1.

Формирования перечня групп высококачественных биометрических параметров

Одним из основных недостатков НЭ является их относительно низкое качество работы с динамическими БП, т. к. НЭ неустойчивы к сдвигам БП по оси времени и по оси значений БП. Таким образом, при применении подхода НЭ необходимо произвести первичную обработку БД. Это является одним из самых важных этапов процесса разработки алгоритмов формирования КК на основе БП пользователя:

– разработка программного обеспечения по считыванию БД пользователя, сбор эмпирических данных;

– разработка методов преобразования БД в БП;

– формирование групп высококачественных БП;

– анализ качества сформированных БП;

– формирование обучающей и тестовой выборок БП;

– разработка алгоритмов формирования КК на основе БП;

Таблица 2. Оценки качества работы алгоритмов (№ – номер источника в списке литературы)

№	Тип задачи	Тип БП	Исходные данные испытаний	Тип ПБК	Средняя оценка качества работы преобразователей
17	Формирование КК	Голосовой отпечаток	10 испытуемых; всего 100 опытов	НЭ	FRR+FAR=0,16
19			60 испытуемых по 50 попыток ввода; 9000 реализаций публичных, 6000 секретных парольных фраз		FRR=0,188 (публичная, в секрете); FAR=0,044–0,091 (в секрете); FAR=0,156–0,214 (публичная); FRR=0,14–0,151 FAR=0,101–0,153 (60 с)
13, 14		Клавиатурный почерк	80 испытуемых по 50 попыток ввода; 3 публичные парольные фразы (всего 12000 реализаций), одна в секрете (всего 4000 реализаций), мониторинг (9000 символов)		FRR=0,064–0,104; FAR=0,009–0,01 (в секрете); FAR=0,021–0,025 (публичная); FRR=0,061 FAR=0,023 (1500 символов)
5		Динамическая рукописная подпись	–		FRR=0,089 FAR=0,096
7, 8			65 испытуемых по 50 попыток ввода	НПБК, НЭ, сети квадратичных форм	FRR=0,0288–0,045 FAR=0,0232–0,039 (НПБК); FRR=0,148 FAR=0,05 (НЭ)
22		Биометрия лица	–	НПБК	EER=0,069
23			70 испытуемых, съемка длительностью в 30-60 сек.	НПБК, НЭ	FRR=0,032 FAR=0,014 (НЭ); FRR=0,0039–0,014 FAR=0,0022–0,029 (НПБК)
15		Мультифакторная система (клавиатурный почерк, биометрия лица)	100 испытуемых при мониторинге длительностью в 1 час	НБПК	FRR=0,002 FAR=0,0036 (30 с); FRR=0,002 FAR=0,0009 (60 с); FRR<0,0005 FAR<0,0005 (150 с)
12	Аутентификация	Динамическая рукописная подпись	280 оригинальных подписей одного испытуемого, 1281 фальсификаций подписи семи испытуемых	нечеткие классификаторы	FRR=0,0057–0,038 FAR=0,0016–0,005
11	Верификация	Динамическая рукописная подпись, голосовой отпечаток	90 испытуемых, общее количество реализаций 10000, период испытаний для каждого испытуемого сроком на 1 месяц	искусственные нейронные сети	EER=0,023–0,043 FRR=0,17 FAR<0,001 (рукописный); EER=0,065–0,092 FRR=0,34 FAR<0,001 (голосовой)
18	Идентификация	Мультифакторная система (голосовой отпечаток, клавиатурный почерк, динамическая рукописная подпись)	10 незарегистрированных пользователей по 100 попыток ввода; эталоны 60 зарегистрированных пользователей по 10 попыток ввода	теорема Байеса	FRR=0,03 FAR=0,001

– оценка качества разработанных алгоритмов.

Для разработки приложения по считыванию БД, методов формирования качественных БП, алгоритмов формирования КК на основе БП можно воспользоваться встроенными пакетами данных языка программирования Python, соответственно: PyQt5, numpy, fuzzy_extractors, keras. Например, с помощью пакета данных «PyQt5» возможно добиться не менее 140 Гц частоты считывания положения курсора. При этом стоит обратить внимание на технические характеристики считывающих устройств. Помимо этого, рекомендуем рассмотреть существующие ныне базы данных рукописных подписей [6; 31]. С помощью функции «corrcoef» пакета данных «numpy» вычисляется матрица коэффициентов корреляции. Подобная функция позволит выявить некорректные реализации попыток ввода [9]. С помощью функции «rfft» с указанием метода «real» пакета данных «numpy» получаем группу БП, представляющих реальную составляющую результата быстрого преобразования Фурье. Для создания эталона биометрического образа можно воспользоваться методом Dynamic time warping [32], реализовав его с помощью пакета данных «dtw». Также нами рекомендуется рассматривать гистограммы значений последовательностей БП (функция «histogram» пакета данных «numpy»), например, гистограмма значений положения пера по оси ординат [20]. Это частично устраняет проблему со сдвигами динамических БП.

При формировании полного перечня групп БП рекомендуется воспользоваться источниками [5; 7–12; 15; 18; 20; 23]. При утверждении окончательного перечня групп БП, при формировании обучающей и тестовой выборок важным является процесс ранжирования наилучших по информативности БП [11; 12; 33]. Информативность демонстрирует, насколько хорошо БП характеризует биометрический образ. Информативность также можно отобразить оценкой качества сформированных групп БП и вычислить по показателю качества БП, указанному в документе ГОСТ Р 52633.5-2011.

Оценки качества работы алгоритмов

Оценками качества работы построенных алгоритмов являются значения ошибки 1-го рода FRR (False Rejection Rate – ложный отказ в доступе зарегистрированного пользователя) и 2-го рода FAR (False Acceptance Rate – ложный доступ незарегистрированного пользователя), а также оценка EER (Equal Error Rate – равный уровень ошибок), при которой выполняется условие равенства оценок FRR и FAR.

В таблице 2 представлены средние оценки качества работы ПБК по данным, приведенным в [5–8; 10–15; 17–19; 22; 23].

При выборе типа БП, типа ПБК, типа выполняемой задачи необходимо отталкиваться от требований пользователя и поставленных условий. Отметим, что задача формирования КК на основе БП пользователя является универсальной и применима в информационных системах различного типа. При этом рекомендуется использовать соответствующие ПБК (НЭ и НПБК).

Выводы

Рассматривая вышеописанные результаты научных исследований в области создания биокриптографических систем защиты информации, отметим следующее. Не рекомендуется использовать в этих системах голосовой отпечаток (угроза копирования биометрических образов, низкие показатели качества работы ПБК), отпечатки пальцев (невозможность изменения биометрического образа). Целесообразно использовать в первую очередь динамический рукописный почерк и мультифакторные системы, включающие данный тип БП (высокие показатели качества работы ПБК, возможность изменения биометрического образа и хранения его в секрете).

Таким образом, анализ биокриптографических систем защиты информации показал, что перспективным направлением их развития является разработка ПБК на основе БП динамического рукописного почерка и мультифакторных систем (например, рукописный и клавиатурный почерки), включающих поведенческие черты эксплуатации мобильных устройств (смартфонов) [34; 35]. Современная подобная техника позволяет считывать качественные биометрические данные различного типа и производить их первичную обработку. В будущем подобные мобильные устройства позволят реализовывать работу алгоритмов ПБК, что в свою очередь многократно увеличит сферу использования таких преобразователей.

Литература

1. Руководство по биометрии / Р.М. Болл [и др.]; пер. с англ. М.: Техносфера, 2007. 368 с.
2. Иванов А.И. Многомерная нейростевая обработка биометрических данных с програм-

мным воспроизведением эффектов квантовой суперпозиции: монография. Пенза: ПНИЭИ, 2016. 133 с.
3. Fuzzy extractors: How to generate strong keys from biometrics and other noisy data / Y. Dodis [et al.] // SIAM Journal on Computing. 2008. No. 1 (38). P. 97–139.
4. ГОСТ Р 52633.5-2011. Защита информации. Техника защиты информации. Автоматическое обучение нейросетевых преобразователей биометрия-код доступа. М.: Стандартинформ, 2018. 15 с.
5. Кузнецов В.В. Новый метод получения устойчивого ключа из динамической биометрической подписи // Системы и средства информатики. 2015. Т. 25, № 2. С. 85–95.
6. Достигнутые результаты и перспективный анализ в области распознавания субъектов по параметрам рукописной подписи / Э.А. Рахимжанов [и др.] // Информационная безопасность: современная теория и практика: сб. труд. второй Межвузовской научно-практической конференции. Омск: СибАДИ, 2019. С. 102–111.
7. Экспериментальная оценка надежности верификации подписи сетями квадратичных форм, нечеткими экстракторами и персептронами / П.С. Ложников [и др.] // Информационно-управляющие системы. 2016. № 5 (84). С. 73–85.
8. Иванов А.И., Ложников П.С., Сулавко А.Е. Оценка надежности верификации автографа на основе искусственных нейронных сетей, сетей многомерных функционалов Байеса и сетей квадратичных форм // Компьютерная оптика. 2017. Т. 41, № 5. С. 765–774.
9. Сулавко А.Е., Еременко А.В., Самотуга А.Е. Исключение искаженных биометрических данных из эталона субъекта в системах идентификации // Информационные технологии и вычислительные системы. 2013. № 3. С. 96–101.
10. Сулавко А.Е. Высоконадёжная двухфакторная биометрическая аутентификация по рукописным и голосовым паролям на основе гибких нейронных сетей // Компьютерная оптика. 2020. Т. 44, № 1. С. 82–91.
11. Сулавко А.Е., Жумажанова С.С., Фофанов Г.А. Перспективные нейросетевые алгоритмы распознавания динамических биометрических образов в пространстве взаимозависимых признаков // Динамика систем, механизмов и машин. 2018. Т. 6, № 4. С. 130–145.
12. Аутентификация пользователя по динамике подписи на основе нечёткого классификатора / И.А. Ходашинский [и др.] // Компьютерная оптика. 2018. Т. 42, № 4. С. 657–666.
13. Способы генерации ключевых последовательностей на основе клавиатурного почерка / П.С. Ложников [и др.] // Динамика систем, механизмов и машин. 2016. № 4. С. 265–270.
14. Нечеткий экстрактор для генерации ключей шифрования на основе параметров клавиатурного почерка / А.Е. Сулавко [и др.] // Информационные технологии и вычислительные системы. 2016. № 4. С. 69–79.
15. Аутентификация пользователей компьютера на основе клавиатурного почерка и особенностей лица / П.С. Ложников [и др.] // Вопросы кибербезопасности. 2017. № 3 (21). С. 24–34.
16. Крутохвостов Д.С., Хиценко В.Е. Парольная и непрерывная аутентификация по клавиатурному почерку средствами математической статистики // Вопросы кибербезопасности. 2017. № 5 (24). С. 91–99.
17. Генерация криптографических ключей на основе голосовых отпечатков человека / Р.В. Борисов [и др.] // Труды научно-технической конференции кластера пензенских предприятий, обеспечивающих безопасность информационных технологий. Пенза: ПНИЭИ, 2014. Т. 9. С. 79–82.
18. Комплексированная система идентификации личности по динамике подсознательных движений / Б.Н. Епифанцев [и др.] // Безопасность информационных технологий. 2011. Т. 18, № 4. С. 97–102.
19. Сулавко А.Е., Еременко А.В., Борисов Р.В. Генерация криптографических ключей на основе голосовых сообщений // Прикладная информатика. 2016. Т. 11, № 5 (65). С. 76–89.
20. Качайкин Е.И., Куликов С.В. Получение биометрических параметров высокого качества из статического изображения рукописной подписи // Инфокоммуникационные технологии. 2015. Т. 13, № 4. С. 446–450.
21. Eskander G.S., Sabourin R., Granger E. A biocryptographic system based on offline signature images // Information Sciences. 2014. Vol. 259. P. 170–191. DOI: https://doi.org/10.1016/j.ins.2013.09.004

22. Чуйков А.В., Вульфин А.М., Васильев В.И. Нейросетевая система преобразования биометрических признаков пользователя в криптографический ключ // Доклады Томского государственного университета систем управления и радиоэлектроники. 2018. Т. 21, № 3. С. 35–41.
23. Генерация ключевых последовательностей и верификация субъектов на основе двумерного изображения лица / А.Е. Сулавко [и др.] // Автоматизация процессов управления. 2017. № 1 (47). С. 58–66.
24. Казачук М.А. Динамическая аутентификация пользователей на основе анализа работы с клавиатурой компьютера: дис. … канд. физ.-мат. наук. М., 2019. 155 с.
25. Анисимова Э.С. Распознавание динамической рукописной подписи человека на базе методов теории нечётких множеств: дис. … канд. техн. наук. Казань, 2020. 158 с.
26. Варфоломеев А.А. Некоторые рекомендации по повышению стойкости шифра с малым размером ключа к методу полного опробования // Вопросы кибербезопасности. 2015. № 5 (13). С. 60–62.
27. Молдовян Н.А., Горячев А.А., Муравьев А.В. Протокол стойкого шифрования по ключу малого размера // Вопросы защиты информации. 2015. № 1 (108). С. 3–8.
28. Ложников П.С. Методология защиты смешанного документооборота на основе многофакторной биометрической аутентификации с применением нейросетевых алгоритмов: дис. … д-ра техн. наук. Омск, 2019. 317 с.
29. Maiorana E., Campisi P. Fuzzy commitment for function based signature template protection // IEEE Signal Processing Letters. 2010. Vol. 17, no. 3. P. 249–252.
30. Технология использования больших нейронных сетей для преобразования нечетких биометрических данных в код ключа доступа: коллективная монография / Б.С. Ахметов [и др.]. Алматы: ТОО «Издательство LEM», 2014. 144 с.
31. Сарин К.С., Ходашинский И.А. Метод баггинга и отбор признаков в построении нечётких классификаторов для распознавания рукописной подписи // Компьютерная оптика. 2019. Т. 43, № 5. С. 833–845.
32. Feng H., Wah C.C. Private key generation from on-line handwritten signatures // Information Management & Computer Security. 2002. Vol. 10, no. 4. P. 159–164. DOI: https://doi.org/10.1108/09685220210436949
33. Баянов Б.И. Нечеткие экстракторы в задаче формирования криптографического ключа на основе биометрических параметров клавиатурного почерка // Двадцать четвертые туполевские чтения (школа молодых ученых): мат. Международной молодёжной научной конференции. Казань: ИП Сагиева А.Р., 2019. С. 536–539.
34. Козлов Ю.Е., Евсеев В.Л. Математическая модель мультимодальной жестовой аутентификации при помощи двух независимых мобильных устройств // Безопасность информационных технологий. 2017. Т. 24, № 1. С. 49–56.
35. Kim J., Kang P. Freely typed keystroke dynamics-based user authentication for mobile devices based on heterogeneous features // Pattern Recognition. 2020. Vol. 108. P. 1–15. DOI: https://doi.org/10.1016/j.patcog.2020.107556

Принято 10.05.2021

Баянов Булат Ильмирович, аспирант кафедры систем информационной безопасности Казанского национального исследовательского технического университета им. А.Н. Туполева – КАИ. 420111, Российская Федерация, г. Казань, ул. Карла Маркса, 10. Тел. +7 919 628-45-90. E-mail: bayanov_bulat@mail.ru

MODERN ACHIEVEMENTS INTO CRYPTO-BIOMETRIC PROTECTION OF INFORMATION BASED ON HANDWRITING

Bayanov B.I.
Kazan National Research Technical University named after A.N. Tupolev – KAI, Kazan, Russian Federation
E-mail: bayanov_bulat@mail.ru

The article presents the results of scientific achievements in the field of biometric-cryptographic security of information. A modern area in the development of biometric information security is the solution of the task of formation a cryptographic key based on the biometric features of the user. A comparative analysis of Biometrics-access code converters: fuzzy extractors and neural network Biometrics-code converters, was carried out. Biometric data of handwriting, keystroke dynamics, voice features and biometric data of the face are considered. The classification of biometric security of information tasks, the table of advantages and disadvantages, the table of the results of average estimates of the quality of algorithms for formation a cryptographic key based on the user's biometric features are presented. The presented results can be useful for specialists in the field of biometric information security when choosing promising scientific research.

Keywords: *information security, authentication, automatic signature verification, identification, pattern recognition, Fuzzy extractors, neural network Biometrics-code converter*

DOI: 10.18469/ikt.2021.19.3.14

Bayanov Bulat Ilmirovich, Kazan National Research Technical University named after A.N. Tupolev – KAI, 10, Karl Marx Street, Kazan, 420111, Russian Federation; PhD Student of Information Security Systems Department. Tel. +7 919 628-45-90. E-mail: bayanov_bulat@mail.ru

References

1. Boll R.M. et al. *Biometrics Guide*. Trans. from English. Moscow: Tehnosfera, 2007, 368 p. (In Russ.)
2. Ivanov A.I. *Multidimensional Neural Processing of Biometric Data with Programmed Reproduction of the Effects of Quantum Superposition*. Monograph. Penza: PNIEI, 2016, 133 p. (In Russ.)
3. Dodis Y. et al. Fuzzy extractors: How to generate strong keys from biometrics and other noisy data. *SIAM Journal on Computing*, 2008, no. 1 (38), pp. 97–139.
4. GOST R 52633.5-2011. Data Protection. Information Security Technology. Automatic Training of Neural Network Converters Biometrics-Access Code. Moscow: Standartinform, 2018, 15 p. (In Russ.)
5. Kuznetsov V.V. A new method for obtaining a stable key from a dynamic biometric signature. *Sistemy i sredstva informatiki*, 2015, vol. 25, no. 2, pp. 85–95. (In Russ.)
6. Rahimzhanov E.A. et al. Achieved results and prospective analysis in the field of recognition of subjects by parameters of handwritten signature. *Informatsionnaja bezopasnost': sovremennaja teorija i praktika: sb. trud. vtoroj Mezhvuzovskoj nauchno-prakticheskoj konferentsii*. Omsk: SibADI, 2019, pp. 102–111. (In Russ.)
7. Lozhnikov P.S. et al. Experimental assessment of the signature verification reliability by networks of quadratic forms, fuzzy extractors and perceptrons. *Informatsionno-upravljajuschie sistemy*, 2016, no. 5 (84), pp. 73–85. (In Russ.)
8. Ivanov A.I., Lozhnikov P.S., Sulavko A.E. Assessment of the reliability of autograph verification based on artificial neural networks, networks of multidimensional Bayesian functionals and networks of quadratic forms. *Komp'juternaja optika*, 2017, vol. 41, no. 5, pp. 765–774. (In Russ.)
9. Sulavko A.E., Eremenko A.V., Samotuga A.E. Exclusion of distorted biometric data from the reference of the subject in identification systems. *Informatsionnye tehnologii i vychislitel'nye sistemy*, 2013, no. 3, pp. 96–101. (In Russ.)
10. Sulavko A.E. Highly secure two-factor biometric authentication for handwritten and voice passwords based on flexible neural networks. *Komp'juternaja optika*, 2020, vol. 44, no. 1, pp. 82–91. (In Russ.)

11. Sulavko A.E., Zhumazhanova S.S., Fofanov G.A. Perspective neural network algorithms for the recognition of dynamic biometric patterns in the space of interdependent features. *Dinamika sistem, mehanizmov i mashin*, 2018, vol. 6, no. 4, pp. 130–145. (In Russ.)
12. Hodashinskij I.A. et al. User authentication based on signature dynamics based on fuzzy classifier. *Komp'juternaja optika*, 2018, vol. 42, no. 4, pp. 657–666. (In Russ.)
13. Lozhnikov P.S. et al. Methods for generating key sequences based on keyboard handwriting. *Dinamika sistem, mehanizmov i mashin*, 2016, no. 4, pp. 265–270. (In Russ.)
14. Sulavko A.E. et al. Fuzzy extractor to generate encryption keys based on keyboard handwriting parameters. *Informatsionnye tehnologii i vychislitel'nye sistemy*, 2016, no. 4, pp. 69–79. (In Russ.)
15. Lozhnikov P.S. et al. Authentication of computer users based on keyboard handwriting and facial features. *Voprosy kiberbezopasnosti*, 2017, no. 3 (21), pp. 24–34. (In Russ.)
16. Krutohvostov D.S., Hitsenko V.E. Password and continuous authentication by keystroke handwriting by means of mathematical statistics. *Voprosy kiberbezopasnosti*, 2017, no. 5 (24), pp. 91–99. (In Russ.)
17. Borisov R.V. et al. Generation of cryptographic keys based on human voice fingerprints. *Trudy nauchno-tehnicheskoj konferentsii klastera penzenskih predprijatij, obespechivajuschih bezopasnost' informatsionnyh tehnologij*. Penza: PNIEI, 2014, vol. 9, pp. 79–82. (In Russ.)
18. Epifantsev B.N. et al. Integrated personality identification system based on the dynamics of subconscious movements. *Bezopasnost' informatsionnyh tehnologij*, 2011, vol. 18, no. 4, pp. 97–102. (In Russ.)
19. Sulavko A.E., Eremenko A.V., Borisov R.V. Generation of cryptographic keys based on voice messages. *Prikladnaja informatika*, 2016, vol. 11, no. 5 (65), pp. 76–89. (In Russ.)
20. Kachajkin E.I., Kulikov S.V. Obtaining high quality biometric parameters from a static image of a handwritten signature. *Infokommunikatsionnye tehnologii*, 2015, vol. 13, no. 4, pp. 446–450. (In Russ.)
21. Eskander G.S., Sabourin R., Granger E. A bio-cryptographic system based on offline signature images. *Information Sciences*, 2014, vol. 259, pp. 170–191. DOI: https://doi.org/10.1016/j.ins.2013.09.004
22. Chujkov A.V., Vul'fin A.M., Vasil'ev V.I. Neural network system for converting user biometric features into a cryptographic key. *Doklady Tomskogo gosudarstvennogo universiteta sistem upravlenija i radioelektroniki*, 2018, vol. 21, no. 3, pp. 35–41. (In Russ.)
23. Sulavko A.E. et al. Generation of key sequences and verification of subjects based on a two-dimensional image of a face. *Avtomatizatsija protsessov upravlenija*, 2017, no. 1 (47), pp. 58–66. (In Russ.)
24. Kazachuk M.A. Dynamic user authentication based on the analysis of working with a computer keyboard: dis. … kand. fiz.-mat. nauk. Moscow, 2019. 155 p.
25. Anisimova E.S. Recognition of a dynamic handwritten signature of a person based on methods of the theory of fuzzy sets: dis. … kand. tehn. nauk. Kazan, 2020. 158 p.
26. Varfolomeev A.A. Some recommendations for improving the strength of small key size ciphers to full test method. *Voprosy kiberbezopasnosti*, 2015, no. 5 (13), pp. 60–62. (In Russ.)
27. Moldovjan N.A., Gorjachev A.A., Murav'ev A.V. Small key strong encryption protocol. *Voprosy zaschity informatsii*, 2015, no. 1 (108), pp. 3–8. (In Russ.)
28. Lozhnikov P.S. Methodology for protecting mixed document circulation based on multifactor biometric authentication using neural network algorithms: dis. … d-ra tehn. nauk. Omsk, 2019. 317 p.
29. Maiorana E., Campisi P. Fuzzy commitment for function based signature template protection. *IEEE Signal Processing Letters*, 2010, vol. 17, no. 3, pp. 249–252.

30. Ahmetov B.S. et al. *The Technology of Using Large Neural Networks to Transform Fuzzy Biometric Data into an Access Key Code*. A Collective Monograph. Almaty: TOO «Izdatel'stvo LEM», 2014, 144 p. (In Russ.)
31. Sarin K.S., Hodashinskij I.A. Bugging method and feature selection in the construction of fuzzy classifiers for handwritten signature recognition. *Komp'juternaja optika*, 2019, vol. 43, no. 5, pp. 833–845. (In Russ.)
32. Feng H., Wah C.C. Private key generation from on-line handwritten signatures. *Information Management & Computer Security*, 2002, vol. 10, no. 4, pp. 159–164. DOI: https://doi.org/10.1108/09685220210436949
33. Bajanov B.I. Fuzzy extractors in the problem of forming a cryptographic key based on biometric parameters of keyboard handwriting. *Dvadtsat' chetvertye tupolevskie chtenija (shkola molodyh uchenyh): mat. Mezhdunarodnoj molodezhnoj nauchnoj konferentsii*. Kazan': IP Sagieva A.R, 2019, pp. 536–539. (In Russ.)
34. Kozlov Yu.E., Evseev V.L. Mathematical model of multimodal gesture authentication using two independent mobile devices. *Bezopasnost' informatsionnyh tehnologij*, 2017, vol. 24, no. 1, pp. 49–56. (In Russ.)
35. Kim J., Kang P. Freely typed keystroke dynamics-based user authentication for mobile devices based on heterogeneous features. *Pattern Recognition*, 2020, vol. 108, pp. 1–15. DOI: https://doi.org/10.1016/j.patcog.2020.107556

Received 10.05.2021