УДК 004.056 + 003.26 Вестник УрФО № 2(36) / 2020, с. 29–33

Казаковцев М. С., Рогачев С. С., Михайлова У. В.

DOI: 10.14529/secur200205

ИСПОЛЬЗОВАНИЕ ОСОБЫХ ТОЧЕК ОТПЕЧАТКОВ ПАЛЬЦЕВ В БИОКРИПТОГРАФИИ И КОДИРОВАНИИ ИНФОРМАЦИИ

В статье рассмотрен процесс создания криптографической последовательности из биометрических данных человека. Представлены краткие сведения о признаках папиллярного узора, а также алгоритмах предварительной обработки изображения отпечатка пальца. Проведена сравнительная характеристика алгоритмов на этапах генерации, хранения и сравнения информации о ключе. Результатом проведенного исследования является выбор наиболее эффективных алгоритмов создания биокриптографического ключа и защиты информации о нем.

Ключевые слова: *биокриптография, отпечаток пальца, последовательность, бинаризация, алгоритм, ключ.*

Kazakovtsev M. S., Rogachev S. S., Mikhailova U. V.

USE OF FINGERPRINT SPECIFIC POINTS IN BIOCRYPTOGRAPHY AND INFORMATION CODING

This article discusses the process of creating a cryptographic sequence from human biometric data. Brief information about the features of the papillary pattern, as well as algorithms for the preliminary processing of the fingerprint image are presented. A comparative characteristic of the algorithms at the stages of generation, storage and comparison of key information is carried out. The result of the study is the selection of the most effective algorithms for creating a biocryptographic key and protecting information about it.

Keywords: *biocryptography, fingerprint, sequence, binarization, algorithm, key.*

В разрезе современных тенденций цифровизации и киберфизических систем появилось и такое понятие как биокриптография. Это весьма интересная коллаборация биометрии и криптографии. Появилась она в связи с всеобщей цифровизацией общества и поиском более удобных способов для хранения ключевой информации. Основная ее область исследования – применение биометрических данных, в нашем случае отпечатков пальцев.

Для идентификации личности наиболее часто используются такие биометрические данные, как отпечатки пальцев и сканирование радужной оболочки, в качестве преимуществ первого можно выделить:

• устойчивость отпечатков к изменениям с возрастом человека;

• крайне малая вероятность встречи идентичных отпечатков, как у разных людей, так и у одного человека. В истории пока не случалось совпадений или их просто не находили;

• невозможность утери.

У любого отпечатка существуют две категории признаков:

• глобальные;

• локальные.

Признаки первого типа можно увидеть без использования специальных приборов. Они состоят из счетчика линий, ядра, пункта «дельта», области образа и папиллярного узора. Уникальные точки малого размера являются в свою очередь признаками второго типа - они не повторяются на разных пальцах, в отличие от глобальных признаков. Их уникальность обеспечивается с помощью минуций – точек, где линии заканчиваются, делятся или меняют направление. Все по причине того, что линии отпечатков пальцев не образуют прямые линии ни при каких обстоятельствах, ведь они постоянно разветвляются, ломаются и заканчиваются.

Процесс идентификации, как правило, состоит из двух этапов. Первым этапом проходит классификация отпечатков по признакам, видным невооруженным глазом, для разделения на классы. Второй этап заключается в распознавании отпечатка пальца на основе сравнения структуры и коэффициента совпадения точек минуции.

Немаловажным будет упомянуть и предварительный этап в улучшении изображения отпечатка фильтром Габора. Все потому, что на изображении до обработки из-за помех разного рода, как грязь, складки и других, линии отпечатков могут деформироваться, а это в свою очередь влечет за собой ошибки распознавания признаков. С целью устранения этих ошибок изображение улучшают. При нем падает зашумленность изображения, а достоверность модели возрастает.

Функция фильтра Габора в классическом виде выглядит следующим образом:

Стоит отметить, что параметры σ и f относятся к маске фильтра, а угол θ – к ориентации маски над изображением. Формула является произведением гауссиана и периодической функции, что подразумевает улучшение монотонных областей повторяющихся частей изображения.

$$h(x,y) = e^{\left(-\frac{x^2+y^2}{2\sigma^2}\right)} cos2\pi f(xsin\theta + ycos\theta)$$

Эмпирическим путем были определены значения параметров σ и f, которые равны 7 и 10, соответственно. Это означает снижение коэффициентов от центра окружности по радиусу длинной в 7 точек и периодическое повторение изображение через 10.

Таблица 1

Параметр	Значение
x, y	Координаты точек
σ	Стандартное отклонение предполагаемого нормального распределения
f	Частота
θ	Ориентация фильтра

Далее следует алгоритм Базена, основополагающий смысл которого состоит в перпендикулярности линий отпечатка пальца градиенту изображения отпечатка, соответствующему перепадам цветов от белого к черному. Таким образом, определяется поле направлений (рис. 1).

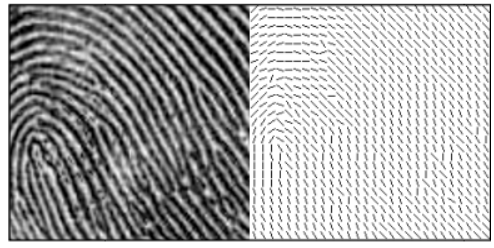

Рис. 1. Определение поля направлений

После этого происходит фильтрация и бинаризация изображения, которая наглядно изображена на рис. 2.

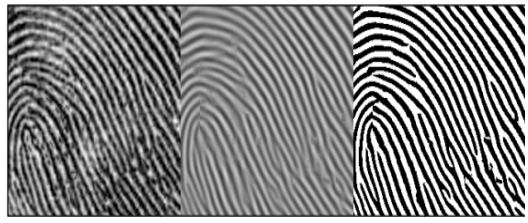

Рис. 2. Фильтрация и бинаризация изображения

Слева – начальное изображение, посередине – темное фильтрованное, а справа уже бинаризованное конечное улучшенное изображение.

Следующим этапом идет генерация биометрической последовательности.

Справиться с задачей преобразования входного набора биометрических данных в последовательность битов помогает блок ге-

нерации биометрической последовательности. Полученная последовательность требуется в дальнейшем для того, чтобы сформировать криптографический ключ.

Для получения биометрической последовательности предлагается использование n, t-пороговой схемы Шамира. Схожим алгоритмом действия обладают такие схемы, как, например, схема Шнорра и схема Блэкли. Однако первая не подходит для идентификации с помощью отпечатка пальца по причине того, что, в сравнении со схемой Шамира, она имеет меньший размер цифровой подписи. Вторая же менее эффективна: в схеме Шамира каждая часть такого же размера, как и секрет, а в схеме Блэкли каждая часть в t раз больше.

По центру папиллярного узора ставится точка O, которая является центром новой системы координат (эта и последующие операции производятся на уже обработанном изображении).

Сначала вычисляются особые точки, являющиеся элементами конечного поля, что задано простым числом. Над этим полем формируется многочлен таким образом, что его график проходит через подмножество особых точек. На базе построенного полинома выбираются случайные точки, после чего из них вычисляются координаты, из которых формируется множество. Данным образом получается система, информацию о которой можно открыто хранить в базе данных. Биометрическая последовательность получается посредством соединения элементов полинома и аналогично не требует защищенного хранения, ибо воссоздается из вновь полученного отпечатка пальца.

За тем эта информация сравнивается с ранее имеющейся информацией, также сформированной из особых точек отпечатка. С помощью интерполяционного многочлена Лагранжа образуется полином, который должен совпадать с эквиваленцией исходного и вновь полученного множеств особых точек папиллярного узора, не меньше значения t.

Выполнение всех вычислений в пределах конечного поля приводит к высокой точности системы, а использование проблемы восстановления полинома из определенного числа точек – к высокой степени безопасности.

Далее в формировании биокриптографического ключа идет блок fuzzy extractor.

В стандартных системах идентификации с помощью отпечатка пальца есть один существенный недостаток – это относительная постоянность совпадений поступающей и исходной биометрической последовательностей, из-за чего в случае получения доступа к информации посторонним лицом, заменить ее не представляется возможным. В таком случае необходимо внедрить следующие требования к биометрической системе:

• каждый новый криптографический ключ в процедуре регистрации пользователя должен отличаться от предыдущего;

• один из входных параметров функции генерации ключа должен быть случайным;

• случайный параметр в открытом виде не должен нигде храниться, как и биометрическая последовательность.

Реализация подобных требований стала возможна после появления блока fuzzy extractor. Добавление в генерацию криптографического ключа стала хоть и необязательной, но очень желательной для добавления. Также данный блок способен сформировать случайную последовательность из вновь сгенерированной биометрической и открытой информации.

Для достижения наилучшего результата мы для алгоритма рассмотрели 3 блока fuzzy и выбрали fuzzy extractor, а не один из других двух, потому что методы fuzzy commitment и fuzzy vault имеют ограничения, в том числе – неспособность генерировать много несвязанных шаблонов из одного и того же набора биометрических данных. Один из возможных способов преодоления этой проблемы - применение функции трансформации черт к биометрическому шаблону до того, как она будет защищена с помощью биометрической криптосистемы. Биометрические криптосистемы, которые объединяют трансформацию с генерацией защищенного эскиза, называют гибридными.

Создание алгоритмов, основанных на биометрии и криптографии, позволит разработать системы, в которых отсутствуют недостатки обоих направлений, например, возможность хищения закрытого криптографического ключа или незащищенность биометрического образа.

Литература

1. Схемы идентификации [Электронный ресурс] URL: http://www.dialektika.com/PDF/978-5-9908462-4-1/part.pdf

2. Биометрическая аутентификация: защита систем и конфиденциальность пользователей [Электронный ресурс] URL: https://www.osp.ru/os/2012/10/13033122

3. В.Ю. Гудков, А.В. Бойцов. Улучшение изображений отпечатков пальцев с помощью фильтра Габора [Электронный ресурс] URL: https://cyberleninka.ru/article/n/15705550

4. Juels A., Wattenberg M.A Fuzzy Commitment Scheme [Электронный ресурс] URL: https://www.arijuels.com/wp-content/uploads/2013/09/JW99.pdf

5. Uludag U., Pankanti S., Jain A.K. Fuzzy Vault for Fingerprints [Электронный ресурс] URL: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.73.5939&rep=rep1&type=pdf

6. Fuzzy extractor [Электронный ресурс] URL: https://en.bitcoinwiki.org/wiki/Fuzzy_extractor

7. Коновалов М.В., Михайлова У.В., Хусаинов А.А. и др. Алгоритмы шифрования данных // Актуальные проблемы современной науки, техники и образования. 2013. Т. 2. № 71. С. 159–-161.

8. Михайлова У.В., Коновалов М.В., Гуринец К. и др. Идентификация личности // Актуальные проблемы современной науки, техники и образования. 2013. Т. 2.№ 71. С. 164–166

9. Михайлова У.В., Лукьянов Г.И., Дончан Д.М. Анализ биометрической аутентификации на устойчивость при воздействии внешних факторов // Актуальные проблемы современной науки, техники и образования. Тезисы докладов 76-ой междунар. науч.-техн. конф. Изд-во Магнитогорск. гос. техн. ун-та им. Г.И. Носова, 2018. Т. 1. С. 295–295.

References

1. Skhemy identifikatsii [Elektronnyy resurs] URL: http://www.dialektika.com/PDF/978-5-9908462-4-1/part.pdf

2. Biometricheskaya autentifikatsiya: zashchita sistem i konfidentsial'nost' pol'zovateley [Elektronnyy resurs] URL: https://www.osp.ru/os/2012/10/13033122

3. V.YU. Gudkov, A.V. Boytsov. Uluchsheniye izobrazheniy otpechatkov pal'tsev s pomoshch'yu fil'tra Gabora [Elektronnyy resurs] URL: https://cyberleninka.ru/article/n/15705550

4. Juels A., Wattenberg M.A Fuzzy Commitment Scheme [Elektronnyy resurs] URL: https://www.arijuels.com/wp-content/uploads/2013/09/JW99.pdf

5. Uludag U., Pankanti S., Jain A.K. Fuzzy Vault for Fingerprints [Elektronnyy resurs] URL: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.73.5939&rep=rep1&type=pdf

6. Fuzzy extractor [Elektronnyy resurs] URL: https://en.bitcoinwiki.org/wiki/Fuzzy_extractor

7. Konovalov M.V., Mikhaylova U.V., Khusainov A.A. i dr. Algoritmy shifrovaniya dannykh // Aktual'nyye problemy sovremennoy nauki, tekhniki i obrazovaniya. 2013. T. 2. № 71. S. 159–161.

8. Mikhaylova U.V., Konovalov M.V., Gurinets K. i dr. Identifikatsiya lichnosti // Aktual'nyye problemy sovremennoy nauki, tekhniki i obrazovaniya. 2013. T. 2.№ 71. S. 164–166

9. Mikhaylova U.V., Luk'yanov G.I., Donchan D.M. Analiz biometricheskoy autentifikatsii na ustoychivost' pri vozdeystvii vneshnikh faktorov // Aktual'nyye problemy sovremennoy nauki, tekhniki i obrazovaniya. Tezisy dokladov 76-oy mezhdunar. nauch.-tekhn. konf. Izd-vo Magnitogorsk. gos. tekhn. un-ta im. G.I. Nosova, 2018. T. 1. S. 295–295.

КАЗАКОВЦЕВ Михаил Сергеевич, студент 2 курса кафедры Информатики и Информационной Безопасности Магнитогорского Государственного Технического Университета им. Г.И. Носова. 455000, г. Магнитогорск, пр. Ленина, 38. E-mail: misha.mk74@mail.ru

РОГАЧЕВ Станислав Сергеевич, студент 2 курса кафедры Информатики и Информационной Безопасности Магнитогорского Государственного Технического Университета им. Г.И. Носова. 455000, г. Магнитогорск, пр. Ленина, 38. E-mail: misha.mk74@mail.ru

МИХАЙЛОВА Ульяна Владимировна, кандидат технических наук, доцент кафедры Информатики и Информационной Безопасности Магнитогорского Государственного Технического Университета им. Г.И. Носова. 455000, г. Магнитогорск, пр. Ленина, 38. E-mail: ylianapost@gmail.com

KAZAKOVCEV Mihail, 2-year student o department of Informatics and Information Security Nosov Magnitogorsk State Technical Universit., 455000, Magnitogorsk, av. Lenina, 38. E-mail: misha.mk74@mail.ru

ROGACHEV Stanislav, 2-year student o department of Informatics and Information Security Nosov Magnitogorsk State Technical University. 455000, Magnitogorsk, av. Lenina, 38. E-mail: misha.mk74@mail.ru

MIKHAILOVA Uliana, candidate of technical sciences, associate professor of the Department of Informatics and Information Security Nosov Magnitogorsk State Technical University. 455000, Magnitogorsk, av. Lenina, 38. E-mail: ylianapost@gmail.com