Получение устойчивого криптографического ключа из биометрической характеристики изображения отпечатков пальцев

Ушмаев О.,С., Кузнецов В. В.
Институт проблем информатики РАН,
oushmaev@ipiran.ru, ikuvlad@gmail.com

Аннотация

В статье рассматривается метод извлечения устойчивой двоичной строки из изображения отпечатка пальца. Особые точки отпечатка – минюции – и их связи друг с другом формируют топологическое описание шаблона отпечатка пальца, которое ставит в соответствие каждой минюции 88-битный бинарный вектор. Топологическое описание само по себе является графом, и для введения на нем порядка разработаны три метода: с введением внутреннего порядка на множестве вершин, с публикацией контрольных точек, а также метод, объединяющий оба предыдущих. Предложенные методы позволяют строить вектор длиной 600-1728 битов, содержащий около 25% ошибочных позиций. Для исправления ошибок используются коды Адамара, а также каскадное кодирование, включающее БЧХ-коды и репликацию. Таким образом с вероятностью около 90% находится исходный ключ с энтропией в 20-36 битов.

Ключевые слова: *биометрическая идентификация; отпечатки пальцев; защищенная идентификация.*

1. ВВЕДЕНИЕ

Развитие телекоммуникаций последних лет привело к проникновению интернет-технологий в повседневную жизнь. Вместе с этим возникла потребность в удаленном доступе к услугам, которые одновременно предполагают и надежность аутентификации, и анонимность доступа пользователя. Для надежности подтверждения личности все чаще прибегают непосредственно к использованию биометрии, однако ей присущи свои проблемы. В сложившихся на практике системах биометрической идентификации биометрический шаблон полностью раскрывает личность человека, что сильно затрудняет применение биометрической идентификации в масштабных информационных системах. Также можно отметить сложность интеграции в традиционную инфраструктуру шифрования/ЭЦП и невозможность перевыдачи фальсифицированной ключевой информации. Решить эти проблемы позволяет генерация отзываемого криптографического (или идентификационного) ключа, которая использует биометрию пользователя, но не включает ее.

2. ОБЗОР СУЩЕСТВУЮЩИХ МЕТОДОВ

Основная проблема всех биометрических признаков состоит в их относительной нестабильности, т.е. в двух последовательных предъявлениях их образы будут побитно неустойчивыми. Как следствие, невозможно применение шифрования и обычных хеш-функций с последующей проверкой результатов разных предъявлений на равенство. Для решения этой проблемы в мировой практике сложились два подхода: «нечеткое хранилище» (“fuzzy vault”) и «нечеткий экстрактор» (“fuzzy extractor”) [2, 5]. Объединяет их использование инфраструктуры открытого хелпера, аналогичной той, что используется при шифровании с открытым ключом. На основе пары «хелпер – предъявленный идентификатор» при аутентификации происходит построение криптографического ключа. Различие между нечетким хранилищем и нечетким экстрактором состоит в том, что в первом случае открытый хелпер представляет собой множество произвольного вида, в то время как во втором – конечномерный вектор. Защита от разглашения биометрического идентификатора состоит в том, что ни открытый хелпер, ни криптографический ключ не позволяют вычислить пользовательскую биометрию. Как следствие, невозможно установить личность путем анализа других биометрических систем, но при этом возможно подтвердить, что данные, предъявленные при регистрации и аутентификации, принадлежат одному человеку с достаточной степенью достоверности. При этом оба подхода позволяют перевыдать ключевые данные в новой сессии регистрации, благодаря чему по удобству использования биометрия становится ближе к паролю и другим перевыдаваемым идентификаторам.

Большинство предыдущих исследований, посвященных совмещению криптографии с биометрией отпечатков пальцев, использовали подход нечеткого хранилища [4, 6, 7], а единственный описанный в литературе нечеткий экстрактор имеет высокую чувствительность к шуму [1]. Такой дисбаланс в количестве публикаций связан традиционными методами построения и сравнения шаблонов отпечатков. Стоит отметить, что проблемы совмещения биометрии и криптографии не популярны среди отечественных исследований, при анализе литературы удалось найти только две работы [3, 9].

3. НЕЧЕТКИЙ ЭКСТРАКТОРА ДЛЯ ОТПЕЧАТКА ПАЛЬЦА

В данной работе рассматривается нечеткий экстрактор для отпечатков пальцев, т.е. алгоритм преобразования изображения отпечатка в побитно устойчивый вектор. Структура экстрактора представляет собой объединение двух алгоритмов: построения зашумленного биометрического вектора и коррекции ошибок. Для построения зашумленного биометрического вектора из изображения отпечатка пальца на сегодняшний день не существует общепринятого подхода, что связано с особенностями шаблона отпечатка пальца. Традиционно шаблон отпечатков представляется контрольными точками (разветвлениями и окончаниями папиллярных линий) и их локальными атрибутами. Глобально эту структуру невозможно описать конечномерным вектором, однако локальные особенности контрольной точки допускают подобное описание с использованием топологии, описанной в совместной статье О. С. Ушмаева и Ю.В.Гудкова [3]. Топология описывает отпечаток как граф,

в котором контрольные точки связаны ближайшими к ним папиллярными линиями. Это позволяет дополнить локальные описания контрольных точек вектором (называемым топологическим), описывающим связь с другими точками. На основе этих описаний реализованы два метода получения устойчивого криптографического ключа: с введением канонической нумерации особых точек через публикацию части координат (метод с введением внешнего порядка) и метод с введением внутреннего порядка в пространстве топологических векторов.

3.1 Метод с введением канонической нумерации

Метод с введением канонической нумерации предусматривает публикацию координат нескольких контрольных точек. Их координаты используются в качестве точки отсчета для введения на отпечатке системы координат, благодаря чему появляется возможность занумеровать паппилярные линии и ключевые точки каноническим образом. Каноническая нумерация позволяет сопоставлять особые точки в разных предъявлениях и из их топологических векторов формировать конечномерный вектор (называемый биометрическим) относительно большой размерности – вплоть до 704 битов. Биометрические вектора не являются побитно устойчивыми: в среднем, ошибка наблюдается в 22% битов. Открытый хелпер включает координаты контрольных точек для позиционирования (от пяти до восьми) и результат логического сложения биометрического вектора с криптографическим ключом. Во время аутентификации по точкам из открытого хелпера вводится нумерация паппилярных линий на предъявленном отпечатке, строится биометрический вектор, который складывается с вектором-суммой из хелпера, и результат подвергается этапу коррекции ошибок, что делает возможным построение непосредственно криптографического ключа.

3.2 Исправление ошибок

Исправление ошибок реализовано с использованием каскадного кодирования, включающего кодирование с последовательным применением корректирующих кодов Боуза-Чоудхури-Хоквингхема и репликацию. Такое кодирование обусловлено структурой ошибок: БЧХ корректируют шумовые ошибки, в то время как репликация позволяет справляться с блочными (связанных с «выпадением» минюции).

3.3 Метод с введением внутреннего порядка

Метод, основанный на введении внутреннего порядка, состоит в разбиении пространства топологических векторов на кластеры. Каждый бит биометрического вектора сопоставляется с кластером. В качестве исходных данных выступает множество топологических векторов обрабатываемого отпечатка. Для каждого вектора находятся k ближайших в метрике Хемминга кластеров. Биты биометрического вектора, сопоставленные с этими кластерами, полагаются единичными. В качестве центров кластеров используются вектора-столбцы матрицы Адамара, что делает распределение векторов по кластерам более устойчивым к помехам. Биометрический вектор содержит в среднем 35% ошибочных битов, но при этом он имеет большую длину (до 1024 битов) и значительно устойчивее к блочным ошибкам. Этапы регистрации, аутентификации и коррекции ошибок, в целом, аналогичны предыдущему методу.

Для ключа длиной 30 битов первый метод позволяет достичь уровня ошибок FRR < 19% при FAR < 0.01%. Второй метод в тех же условиях дает FRR = 37% при FAR = 3%. К тому же регулировка осуществляется подбором параметров этапа коррекции ошибок, что далеко не всегда оптимально. С другой стороны, при относительно большой энтропии метод с введением внешнего порядка имеет околонулевой FAR, но высокий уровень FRR, и имеет смысл снизить последний ценой некоторого увеличения уровня ложного допуска. Для решения этой задачи были проанализированы биометрические вектора, на которых метод с введением внешнего порядка дает ошибку ложного недопуска, и было установлено, что бóльшая часть из них связана с блочными ошибками. Действительно, даже если биометрический вектор строится из восьми минюций, из которых выпадают две, то это ограничивает снизу число ошибочных битов 25%, что находится на границе возможностей БЧХ (при условии полного отсутствия других шумовых ошибок). Основная идея борьбы с блочными ошибками состоит в совмещении биометрических векторов, полученных методами с введением внутреннего порядка (устойчивых к блочным ошибкам) и внешнего порядка. Поскольку в работе [8] была продемонстрирована связь эффективности коррекции ошибок с методами группирования битов с разной вероятностью единичной ошибки, в рамках построения итогового метода были исследованы различные алгоритмы объединения векторов. Первый алгоритм заключался в простом конкатенировании векторов, второй – в последовательном чередовании битов из разных векторов (например, при объединении векторов равной длины биты первого биометрического вектора займут нечетные позиции, а второго – четные) и полностью случайный порядок следования битов. Была показана корреляция между эффективностью коррекции ошибок в рамках выбранного алгоритма кодирования. Результаты для совмещения векторов равной длины приведены в таблицах 1-5. Таким образом, для ключа с энтропией в 30 битов была показана возможность более чем двукратного уменьшения ошибки ложного недопуска за счет увеличения FAR на 0,8%.

4. ЗАКЛЮЧЕНИЕ

Рассмотренный метод получения устойчивого криптографического ключа в полной мере отвечает предъявляемым требованиям в области анонимности аутентификации и использует существующую инфраструктуру шифрования с открытым ключом. Стоит отметить, что на непосредственно используемый криптографический ключ не накладывается никаких ограничений, и он может быть отозван и перевыдан в случае фальсификации. Это обеспечивает преимущество перед существующими системами шифрования и в перспективе дает возможность электронного доступа к услугам, требующим анонимного доступа, таким как процедура тайного голосования. Показан способ построения более удобного варианта нечеткого экстрактора, однако не решены проблемы потенциальной утечки информации через открытый хелпер.

Энтропия ключа, битов:

	26	30	36
FAR, %	0	0	0
FRR, %	19,3	19	19,8

Таблица 2: Результаты для метода с введением внутреннего порядка

FAR, %	11,2	3	1,4
FRR, %	30	37	46,8

Таблица 3: Результаты для объединения конкатенацией

FAR, %	5,6	2	0,8
FRR, %	6,8	9,9	13,6

Таблица 4: Результаты для объединения чередованием

FAR, %	4	0,8	0,3
FRR, %	7,8	8,5	10,6

Таблица 5: Результаты для случайного объединения

FAR, %	3,8	1,1	0,2
FRR, %	5,1	9,5	13,3

Таблица 1: Результаты для метода с введением внешнего порядка

5. ССЫЛКИ

[1] Arakala A., Jeffers J, Horadam K.J. Fuzzy Extractors for Minutiae-Based Fingerprint Authentication // Advances in Biometrics, Springer, pp. 760-769, 2007.

[2] Dodis Y., Ostrovsky R., Reyzin L., Smith A. Fuzzy extractors: How to generate strong keys from biometrics and other noisy data // SIAM Journal on Computing, vol. 38 (1), pp. 97-139, 2008.

[3] Gudkov V.Yu., Ushmaev O.S. A Topological Approach to User-Dependent Key Extraction from Fingerprint // Proc. ICPR2010, p.1281-1284.

[4] Jo J.G., Seo J.W., Lee H.W. Biometric Digital Signature Key Generation and Cryptography Communication Based on Fingerprint. // FAW 2007, LNCS 4613, Springer, pp. 38-49, 2007.

[5] Juels A., Sudan M., A fuzzy vault scheme // Proc. IEEE Intil. Symp. Inf. Theory, p. 408, 2002.

[6] Li P., Yang X., Cao K, Shi P, Tian J. Security-enhanced fuzzy fingerprint vault, based on minutiae's local ridge information // Advances in Biometrics (ICB 2009), LNCS 5558, pp. 930-939, 2009.

[7] Nandakumar K., Jain A.K., Pankanti S. Fingerprint-Based Fuzzy Vault: Implementation and Performance. // IEEE Transactions on Information Forensics and Security 2 (4), pp. 744-757, 2007.

[8] F. Scotti, Cimato S., Gamassi M., Piuri V., Sassi R. Privacy-aware Biometrics: Design and Implementation of a Multimodal Verification System // 2008 Annual Computer Security Applications Conference, IEEE, pp. 130-139.

[9] Иванов А. И., Фунтиков В. А., Ефимов О. В. Нейросетевая защита биометрических данных пользователя, а так же его личного криптографического ключа при локальной и дистанционной аутентификации // Вопросы защиты информации № 2 (81) 2008 г., с. 25-27.

Об авторах

Олег Станиславович Ушмаев – ведущий научный сотрудник ИПИ РАН, д.т.н. Его адрес: oushmaev@ipiran.ru.
Кузнецов Владислав Владимирович – младший научный сотрудник ИПИ РАН. Его адрес: ikuvlad@gmail.com.