В. В. Кузнецов, **О. С. Ушмаев** (Москва, ИПИ РАН). **Извлечение криптографического ключа из изображения отпечатка пальца.**

С начала 2000-х годов мы наблюдаем активное проникновение интернет-технологий в повседневную жизнь. Уже сейчас возникла необходимость в электронном доступе к услугам, которые одновременно предполагают надежную аутентификацию и анонимность доступа (например, процедура тайного голосования). Для аутентификации обычно используются идентификаторы, которые основываются на том, что человек знает (например, пароль), или на устройствах, которыми обладает. Такой идентификатор может быть утерян или передан другому лицу. Применение биометрических идентификаторов позволяет решить проблему.

В данной работе рассматривается алгоритм извлечения побитно точного ключа из изображения отпечатков пальцев. Шаблон отпечатка пальца стандартно представляется контрольными точками (разветвлениями и окончаниями папиллярных линий) и их локальными атрибутами. Такая структура принципиально не является вектором, однако локальные особенности контрольной точки допускают описание с использованием топологии, описанной в статье [1]. Папиллярные линии описываются посредством контрольных точек, расположенных на них, а также их соседством. При использовании нескольких контрольных точек в качестве точки отсчета, папиллярные линии и их описания можно занумеровать каноническим образом. Полученные нумерованные векторы описаний папиллярных линий конкатенируются в единый топологический вектор. В среднем ошибка наблюдается в 15% бит результирующего вектора, что в целом позволяет применять помехоустойчивое кодирование. В нашей работе для этого используется каскадное кодирование: на первом этапе ключ кодируется БЧХ-кодами, на втором шаге — репликацией. Открытый ключ включает контрольные точки для позиционирования и результат логического сложения кодированного топологического вектора с криптографическим ключом. Во время аутентификации по точкам из открытого ключа вводится нумерация папиллярных линий на отпечатке, строится топологический вектор. Полученный ключ исключительным «или» складывается с хранимой в шаблоне бинарной строкой. После этого из результата путем исправления ошибок находится исходный ключ.

Стоит отметить, что на этот ключ не накладывается никаких дополнительных ограничений, и он может быть отозван и перевыдан в случае фальсификации. Рассмотренный метод получения устойчивого криптографического ключа в полной мере отвечает требованиям в области анонимности аутентификации и возможности перевыдачи ключа и использует существующую инфраструктуру шифрования с открытым ключом.

Работы выполнена при поддержке гранта Президента РФ МД-72.2011-9.

СПИСОК ЛИТЕРАТУРЫ

1. *Gudkov V. Yu.*, *Ushmaev O. S.* A Topological Approach to User-Dependent Key Extraction from Fingerprint. — In: 20th International Conference on Pattern Recognition (ICPR 2010). (Istanbul, 23–26 August 2010). Piscataway, NJ: IEEE/Computer Cociety, 2010, p. 1281–1284.