УДК 004.087.5

БИОМЕТРИЯ В КРИПТОГРАФИЧЕСКИХ СИСТЕМАХ

Головко И.А.
Харьковский национальный университет радиоэлектроники, студент

В настоящее время существуют два основных направления применения биометрии: аутентификация личности и криптография. Использование биометрии для аутентификации личности является традиционным, имеет большую историю изучения и применения. Применение биометрических методов в криптографии имеет свои особенности.

Криптографические методы широко применяются для обеспечения секретности и аутентичности информации. Их стойкость основана на предположении, что секретный ключ известен только законному пользователю. На практике сохранение секретности ключа - основная задача при эксплуатации криптосистем. Биометрические методы аутентификации личности имеют ряд преимуществ по сравнению с традиционными: 1) биометрические признаки трудно фальсифицировать; 2) уникальность биометрических признаков; 3) биометрический идентификатор нельзя забыть или потерять; 4) для биометрической аутентификации требуется присутствие владельца биометрических признаков. Таким образом, биометрические системы предоставляют естественное и надежное решение задачи аутентификации в криптографических системах.

Недавно биометрии в криптографических системах стала применяться в качестве источника ключевого материала. Стоит заметить, что применение биометрического материала в качестве источника ключей вызывает множество сложностей: биометрические данные нечетко воспроизводимы, не имеют равномерного распределения, а большинство криптографических преобразований биективны – требуют точного значения ключа. В зависимости от цели применения биометрии в криптографии появилось несколько видов биометрических криптографических систем: системы с освобождением ключа, системы со связыванием ключа, системы с генерацией ключа.

Биометрические криптографические системы с освобождением ключа. В режиме освобождения ключа биометрическая аутентификация осуществляется независимо от механизма освобождения ключа. Биометрический эталон и ключ хранятся отдельно друг от друга, при этом ключ освобождается только при условии, что биометрическая аутентификация прошла успешно. Данный метод биометрической аутентификации неприменим в большинстве криптографических приложений, он использует незашифрованную биометрическую информацию в незащищенных каналах связи [1].

Биометрические криптографические системы со связыванием ключа. В системах такого типа ключ и биометрический эталон криптографически связаны между собой и представляют единое целое. В этом случае декодирование ключа из биометрического эталона без знания биометрических данных пользователя является вычислительно сложной задачей. Данный вид биометрических криптосистем изначально был разработан для защиты криптографических ключей. Тем не менее он также может быть применим и в качестве механизма защиты биометрических эталонов.

Биометрические криптографические системы с генерацией ключа. В такой биометрической криптосистеме ключ извлекается непосредственно из биометрических данных пользователя и не хранится в базе данных. Из биометрических данных пользователя извлекаются параметры, из которых при помощи специального алгоритма генерируется секретный ключ пользователя. Таким образом, главным отличием двух последних видов биометрических криптосистем является то, что в одном из них криптографический ключ только закрывается при помощи биометрического эталона, а в другом ключ генерируется непосредственно из биометрических данных пользователя.

Основное отличие таких криптосистем от традиционных заключается в том, что биометрия в них служит не только для защиты, но и для генерации криптографических ключей. Главное преимущество - ключ, извлеченный непосредственно из биометрических данных пользователя, не требуется хранить в базе данных, при необходимости использования он всегда может быть восстановлен из биометрических данных пользователя. Также возможно применения таких систем в идентификационных криптосистемах, в протоколах аутентификации и распределения ключей.

Список использованной 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.