УДК 004.94; 519.21
М.К. Комарніцький, А.М. Луцків канд. техн. наук, доц.
Тернопільський національний технічний університет імені Івана Пулюя, Україна

ОГЛЯД МЕТОДІВ ОБРОБКИ БІОМЕТРИЧНИХ ДАНИХ ЗА ДОПОМОГОЮ ЕКСТРАКТОРІВ

M.K. Komarnitskyy, A.M. Lutskiv Ph.D., Assoc. Prof.

REVIEW OF THE BIOMETRIC DATA PROCESSING METHODS USING EXTRACTORS

Авторами проводяться дослідження та створення системи біометричної аутентифікації за динамічно введеним підписом, створено низку дослідних прототипів відповідного програмного забезпечення. Оскільки, кожного разу при аутентифікації отримуються різні біометричні дані, актуальним є розроблення методів формування біометричного еталону, алгоритму допуску в інформаційну систему та зберігання даних.

Безпосереднє використання біометричних даних у якості ключа у криптографії є неможливим через мінливість біометричного еталону при кожному зчитуванні. У роботі[1] запропонована математична модель біометричного екстрактора, яка дає змогу згенерувати сильний криптографічний ключ з нерівномірно розподілених вхідних біометричних даних.

В роботі[2] запропоновано алгоритм роботи нечіткого сховища (англ. fuzzy vault), що базується на використанні коду Соломона-Ріда. Як і в попередній праці, наведено математичну модель сховища для зашумлених даних (англ. noisy data), але не наведено практичну реалізацію даного сховища.

Використання фізично неклонованих функцій (англ. Physical Unclonable Function, PUF) для аналізу роботи нечіткого екстрактора (англ. Fuzzy Extractor) продемонстровано у роботі[3]. Авторами також використовуються циклічні коди попередньої корекції Боуза–Чоудхурі-Хоквінгема (БЧХ-коди, англ. BCH code). Подана схема дозволяє реалізувати запропонований алгоритм і для біометричних даних.

У роботі[4], на відміну від вищезгаданої, використовуються циклічний залишковий код (англ. Cyclic redundancy check, CRC) та нечітке сховище. Подана схема дозволяє згенерувати криптографічний ключ з використанням динамічно введеного підпису. Проте, не всі складові алгоритму є роз'ясненими, що викликає труднощі у практичній реалізації. Авторами здійснюється розроблення методів опрацювання біометричних даних, які б давали змогу формувати криптографічний ключ використовуючи екстрактори та нечітке сховище. Також можливе використання даних методів для зберігання біометричного еталону.

Література

1. Русин Б. П. Біометрична аутентифікація та криптографічний захист / Русин Б.П., Варецький Я. Ю. – Львів: Коло, 2007. – 287 с.

2. Ari Juels. A fuzzy vault scheme. / Ari Juels, Madhu Sudan. // Designs, Codes and Cryptography, - 2006., - p. 237-257.

3. Hyunho Kang. The Implementation of Fuzzy Extractor is Not Hard to Do : An Approach Using PUF Data. / Hyunho Kang, Yohei Hori, Toshihiro Katashita, Manabu Hagiwara // The 30th Symposium on Cryptography and Information Security (SCIS2013), Kyoto, Japan, Jan. 22-25, 2013.

4. M. Freire-Santos. Cryptographic key generation using handwritten signature / M. Freire-Santos, J. Fierrez-Aguilara, J. Ortega-Garcia // Biometric technologies for human identification III, - 2006., p. 225–231.