УДК 004.056.52

Медведєва К.В.
Кондратенко Н.Р.

ВИКОРИСТАННЯ НЕЧІТКОГО ЕКСТРАКТОРА ДЛЯ ГЕНЕРАЦІЇ КЛЮЧІВ ШИФРУВАННЯ НА ОСНОВІ ПАРАМЕТРІВ КЛАВІАТУРНОГО ПОЧЕРКУ

Анотація

Робота присвячена використанню нечіткого екстрактора на основі параметрів клавіатурного почерку для генерації ключів шифрування. Проведено експеримент у ході якого досліджувався ступінь схожості біометричного еталону w з новою реалізацією ознак w` в залежності від способу представлення. Результати оцінено за допомогою метрик.

Ключові слова: *клавіатурний почерк, біометричні методи захисту, нечіткий екстрактор, генерація ключів шифрування но основі біометричних даних, представлення еталонів*

Abstract

The work is devoted to the use of fuzzy extractor based on the parameters of handwriting keyboard input to generate encryption keys. An experiment was conducted, during which the degree of similarity of the biometric standard w with the new implementation of the features w` depending on the method of presentation was investigated. The results were evaluated using metrics.

Keywords: *keyboard handwriting, biometric protection methods, fuzzy extractor, generation of encryption keys based on biometric data, representation of features*

Вступ

Багато сфер діяльності сучасного суспільства залежать від функціонування інформаційно-комунікаційних систем. У зв'язку з цим гостро постає питання захисту інформації в них. На даних час, найпопулярнішим методом захисту є парольна ідентифікація. Якість парольного захисту напряму залежить від дотримання користувачем рекомендацій з використання паролю. Згідно з проведеним дослідження Data Insider 44% людей змінюють свій пароль лише раз на рік або рідше, 61% людей зізналися, що використовували свої паролі на кількох веб-сайтах через труднощі із запам'ятовуванням кількох паролів для кожного сайту [1]. Такі звички послаблюють рівень захищеності системи, тому потрібно знайти кращі способи для запобіганню несанкціонованому доступу. Одним з можливих способів розв'язання цієї задачі є використання біометрії.

Результати дослідження

Біометричні характеристики людини можна використовувати не лише для проведення процедури ідентифікації/автентифікації, а й створювати на основі таких даних криптографічні ключі. У криптографічних системах такого типу ключ відтворюється з біометричних даних та не потребує зберігання. Більшість таких систем базуються на технології «нечітких» екстракторів. Їх використання пов'язано з тим, що криптографія традиційно використовує рівномірно розподілені та точно відтворювані випадкові набори символів. Однак реальність ускладнює створення, зберігання та надійне відтворення таких наборів [2].

В порівнянні з іншими біометричними ознаками людини клавіатурний почерк має ряд переваг: зручність використання, ненав'язливість та простота реалізації ідентифікації на його основі. Як характеристики для клавіатурного почерку використовуються:

1. Часові інтервали між натиском клавіш.
2. Тривалість натискання клавіші.
3. Загальна швидкість набору.
4. Частота помилок [3] [4].

В роботах [5, 6] у якості біометричного еталона розглядається вектор з середніх значень використовуваних ознак. Одним з важливих питань є спосіб представлення біометричних характеристик у двійковому вигляді. Початково всі значення ознак подаються в десятковому форматі. Також важливу роль відіграє довжина бітової послідовності біометричних ознак, адже строка s має

повністю покритись при об’єднані. Досліджено, що у випадку неповного покриття відновити повністю початковий рядок *s* є неможливим, вдається відновити лише частину покриту біометричним еталоном.

Для оцінювання еталонів використовуються метрики, які є найбільш природними для біометричних даних:

1. Метрика Хеммінга (кількість позицій, які відрізняються у біометричних характеристик *w* і *w`*).
2. Метрика редагування (найменша кількість вставок та видалень для перетворення *w* і *w'*) [2].
3. Відстань Левештейна.

Кожна ознака представляється 1 байтом. Для представлення еталону у двійковому вигляді запропоновано такі способи:

1. Обраховане середнє значення переводиться в двійкову систему.
2. Обраховане середнє значення переводиться в двійкову систему та кодується кодом Грея.

Проведено експеримент у ході якого досліджувався ступінь схожості біометричного еталону *w* з новою реалізацією ознак *w`* в залежності від способу представлення. У нижче наведеній таблиці вказано середнє значення використаних метрик.

Таблиця 1 – Отримані результати

Способи представлення	Вид ознаки	Метрика Хемінга	Метрика редагування	Відстань Левенштейна
Спосіб №1	Середнє значення тривалості натискання клавіш	0.8	1.6	0.8
	Середнє арифметичне інтервалів між натиском клавіш	5.1	5	3.9
Спосіб №2	Середнє значення тривалості натискання клавіш	1.1	1.6	1.1
	Середнє арифметичне інтервалів між натиском клавіш	3.8	3.8	3.1

Відповідно до проведеного дослідження для збільшення рівня схожості можна запропонувати використання різних методів представлення для різних видів біометричних ознак.

Висновки

Отримані результати свідчать про те, що перший спосіб представлення дає кращі результати при застосуванні його до такої характеристики, як середнє арифметичне тривалості натискання клавіш. Спосіб №2 доцільніше використовувати у комбінації з такою біометричною ознакою, середнє арифметичне інтервалів між натиском клавіш.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. https://digitalguardian.com/blog/uncovering-password-habits-are-users-password-security-habits-improving-infographic
2. Dodis, Y., Reyzin, L., Smith, A. Fuzzy Extractors: How to Generate Strong Keys from Biometrics and Other Noisy Data // Proceedings from Advances in Cryptology. EuroCrypt. – 2004. – P. 79-100.
3. Keystroke dynamics J Ilonen - Advanced Topics in Information Processing–Lecture, 2003 – Citeseer
4. Брюхомицкий Ю.А., Казарин М.Н. Учебно-методическое пособие к циклу лабораторных работ «Исследование биометрических систем динамической аутентификации пользователей ПК по рукописному и клавиатурному почеркам» по курсу: «Защита информационных процессов в компьютерных системах». − Таганрог: Изд-во ТРТУ, 2004. – 38с.
5. Нечеткий экстрактор для генерации ключей шифрования на основе параметров клавиатурного почерка А.Е. Сулавко, А.В. Еременко, Е.В. Толкачева, С.С. Жумажанова
6. Transforming a pattern identifier into biometric key generators Yongdong Wu and Bo Qiu Institute for Infocomm Research, A*STAR, Singapore {wydong,qiubo}@i2r.a-star.edu.sg

Медведєва Катерина Вікторівна – студентка групи 1БС-18б, факультет інформаційних технологій та комп’ютерної інженерії, Вінницький національний технічний університет, м. Вінниця, e-mail: medvedieva.katya@gmail.com

Кондратенко Наталія Романівна - к.т.н., доцент, професор кафедри захисту інформації. Вінницький національний технічний університет.

Medvedieva Katherine V.– Department of Information Technology and Computer Engineering , Vinnytsya National Technical University, Vinnytsia.

Kondratenko Natalia Romanivna - Ph.D., Associate professor of Information Protection, Faculty of Information Technologies and Computer Engineering, Vinnytsia National Technical University, Vinnytsia