ДОСЛІДЖЕННЯ МЕТОДІВ ЗАХИСТУ БІОМЕТРИЧНОГО ШАБЛОНУ РАЙДУЖНОЇ ОБОЛОНКИ ОКА

Чернікова В.Г. Стрілець А.М. Скирда С.О.
Науковий керівник – к.т.н., доцент Філіппенко О.І.
Харківський національний університет радіоелектроніки
(61166, Харків, пр. Науки,14, каф. Інфокомунікаційної інженерії,
тел. (057) 702-55-92)

This work is devoted to actual problem of choosing a method for protection biometric template of the iris based on using fuzzy extractors. The above-mentioned protection method was also investigated under the conditions of a combination with methods of processing the iris image from the CASIA-Iris-Interval database. The scientific novelty of the work is to further improve the methods of protection biometric template of the individual by the iris for remote biometric authentication.

На зміну захисту інформації за допомогою паролю приходять біометричні системи, , деякі з яких за останні роки придбали досить велику популярність серед користувачів завдяки своїй захищеності та зручності використання. Біометрична система розпізнавання встановлює відповідність конкретних поведінкових або фізіологічних характеристик користувача деякому заздалегідь заданому шаблону. Цей процес відбувається наступним чином. На етапі реєстрації виконується запис зразка біометричної риси користувача за допомогою датчика. Наприклад, при проведенні автентифікації по райдужній оболонці ока таким датчиком виступатиме камера, а зразком буде око користувача. Далі система витягує індивідуальні риси з біометричного зразка. Тобто, в зазначеному вище прикладі на даному етапі буде відбуватися виділення окремої ділянки райдужної оболонки та її перетворення в код. На наступному етапі система зберігає виділені риси в якості шаблону поряд з іншими ідентифікаторами. Це може бути ідентифікаційний номер, ім’я користувача та ін. Для отримання доступу користувач пред'являє датчику ще один біометричний зразок. При автентифікації шаблон, що зберігається в базі, порівнюється з новим зразком за допомогою алгоритму зіставлення, і повертається рейтинг відповідності, що відображає ступінь схожості між шаблоном і запитом. Після цього системою приймається рішення про надання даному користувачу доступу до певної інформації або об’єкту. Основною проблемою всіх біометричних ознак є їх відносна нестабільність. Тобто в двох послідовних пред'явленнях їх образи будуть побітно нестійкими. Через це неможливе застосування шифрування і звичайних хеш-функцій з подальшою перевіркою результатів різних пред’явлень на рівність. Одним із шляхів вирішення проблеми, що найбільш задовольняють вимогам є використання нечітких екстракторів.

Використання нечітких екстракторів дозволяє однозначно відновлювати секретний ключ з неточно відтворюваних біометричних даних. Довжина ключа задається у вигляді параметра, при цьому для відтворення ключа потрібні додаткові відкриті дані, які відповідні ключу і зберігаються в пам'яті.

Метод нечітких екстракторів витягує випадкову рівномірно розподілену послідовність з первинних вхідних даних і відновлює її з будь-яких даних, які є достатньо схожі на початкові. Нечіткий екстрактор дозволяє отримувати тільки один ключ, якість вихідної ключової послідовності якого задовольняє всім критеріям якості криптографічних ключів.

Захист біометричних шаблонів необхідно здійснювати криптографічними перетвореннями з використанням ключових даних. До перетворень, які не змінюють відстань Хемінга при порівнянні, відносяться шифрування гамуванням, перестановкою, підстановкою. Шифрування гамуванням визначається простотою реалізації.

Отже, до зашумленого біометричного шаблону за операцією побітового складання додаються біти гамми і таким чином отримується результуюча послідовність.

Виходячи з вищенаведеної інформації можна зробити наступні висновки. Застосування шифрування гамуванням є ефективним засобом для створення багаторазових нечітких екстракторів. За рахунок ключової гамми збільшується ентропія біометричного шаблону, що забезпечує стійкість до криптографічних атак. Ключова послідовність гамми зберігається у пристрої користувача і використовується тільки при початковій фазі реєстрації, або при поновленні бази даних і повинна постійно додаватися до зашумленого біометричного образу. Застосування коротких кодів, що коректують помилки для зашумлення біометричних шаблонів, є ефективним засобом побудови захищених біометричних образів.

Перелік посилань:

1. Конахович Г.Ф. Цифрова стеганографія / Г.Ф. Конахович, А.Ю. Пузиренко. – К.: МК-Пресс, 2006, 40 с.

2. Колешко В.М. Традиційні методи біометричної аутентифікації і ідентифікації / В.М. Колешко, Е.А. Воробей, П.М. Азізов. – М. : БНТУ, 2009, 107 с.