Технічні науки

УДК 004.056.55

Мітряєв Сергій Сергійович

студент

Харківського національного університету радіоелектроніки

Митряев Сергей Сергеевич

студент

Харьковского национального университета радиоэлектроники

Mitriaiev Serhii

Student of the

Kharkiv National University of Radioelectronics

Сергієнко Олександра Сергіївна

студентка

Харківського національного університету радіоелектроніки

Сергиенко Александра Сергеевна

студентка

Харьковского национального университета радиоэлектроники

Serhiienko Oleksandra

Student of the

Kharkiv National University of Radioelectronics

Олійник Олександр Олександрович

асистент кафедри Програмної інженерії

Харківський національний університет радіоелектроніки

Олейник Александр Александрович

ассистент кафедры Программной инженерии

Харьковский национальный университет радиоэлектроники

Oliinik Oleksandr

Assistant of the Software Engineering Department

Kharkiv National University of Radioelectronics

ІДЕНТИФІКАЦІЯ ТА АУТЕНТИФІКАЦІЯ НА ОСНОВІ ВІДБИТКУ ПАЛЬЦЯ З ВИКОРИСТАННЯМ ВІЗУАЛЬНОЇ КРИПТОГРАФІЇ

ИДЕНТИФИКАЦИЯ И АУТЕНТИФИКАЦИЯ НА ОСНОВЕ ОТПЕЧАТКА ПАЛЬЦА С ИСПОЛЬЗОВАНИЕМ ВИЗУАЛЬНОЙ КРИПТОГРАФИИ

IDENTIFICATION AND AUTHENTICATION BASED ON FINGERPRINT USING VISUAL CRYPTOGRAPHY

Анотація. *Захист біометричних даних викликає все більший інтерес, та, таким чином, методи створення цифрових водяних знаків є одним з найкращих способів захисту біометричних даних від випадкових та умисних атак. Ми пропонуємо схему створення водяних знаків відбитків пальців, що заснована на візуальній криптографії, для ідентифікації та аутентифікації.*

Ключові слова: *відбиток пальця, цифровий слід, візуальна криптографія, ідентифікація, аутентифікація.*

Аннотация. *Защита биометрических данных приобретает все больший интерес, и, следовательно, методы создания цифровых водяных знаков являются одним из лучших способов защиты биометрических данных от случайных или преднамеренных атак. Мы предлагаем схему создания водяных знаков отпечатков пальцев, основанную на визуальной криптографии, для идентификации и аутентификации.*

Ключевые слова: *отпечаток пальца, цифровой след, визуальная криптография, идентификация, аутентификация.*

Summary. *Protecting biometric data is gaining more and more interest, and therefore, digital watermarking techniques are one of the best ways to protect biometric data from accidental or deliberate attacks. We propose a fingerprint watermarking scheme based on visual cryptography for identification and authentication.*

Key words: *fingerprint, Digital watermarking, Visual cryptography, Identification, Authentication.*

Біометрія – це наука про встановлення особистості на основі фізичних характеристик, таких як обличчя, відбитки пальців, хода тощо [1]. Відбитки пальців є найбільш широко використовуваною формою біометричної ідентифікації. Завдяки своїм унікальним характеристикам біометрична аутентифікація вважається надійним методом аутентифікації в найближчому майбутньому.

Дослідники пропонують кілька способів підвищення безпеки систем аутентифікації. Серед них використання цифрових водяних знаків [2] для безпечного обміну даними між клієнтом і сервером, особливо в мережевих середовищах. Крім того, цей метод можна використовувати для мульти біометричних систем аутентифікації, в яких один або кілька біометричних даних можуть бути вбудовані в інші біометричні дані для підвищення точності та зменшення пропускної здатності [3].

Біометричний водяний знак був введений як синергетична інтеграція біометричних даних і технології цифрових водяних знаків [4]. На сьогоднішній день водяний знак використовується разом із кількома біометричними показниками, включаючи відбиток пальця, підпис, обличчя, руку, райдужну оболонку, голос, сітківку.

Відбитки пальців – це унікальні біометричні дані, які в основному використовуються для миттєвого встановлення особистості [5]. Однак вони сприйнятливі до випадкових та умисних атак під час передачі по мережі. Таким чином, необхідна захисна схема, яка збереже правильність і не допустить змін. Це є найбільш важливим для біометричних ідентифікаторів з урахуванням їх унікальності. Рішенням розглянутої ситуації є використання водяних знаків.

Наведемо короткий опис (2, 2) схеми візуальної криптографії. Для шифрування секретної інформації, використовуючи (2, 2) схему візуальної

криптографії, секретна інформація поділяється на дві частки так, що кожен піксель у вхідному зображенні замінюється блоком з двох субпікселів, що не перекриваються. Кожен, хто володіє лише однією часткою, не буде мати змогу відновити секретну інформацію, бо єдина частка не містить повну секретну інформацію.

На рис. 1 зображено схему кодування для (2, 2) візуальної криптографічної схеми, яка буде застосовуватися до кожного пікселю секретної інформації. Якщо піксель P білий, то він буде замінений на два однакових блоків субпіселів. Якщо піксель P чорний, то він буде замінений на два доповнюючих блока субпікселів. Для того, щоб розшифрувати секретну інформацію, субпікселі кожної частини накладаються одне на одного, роблячи їх прозорими.

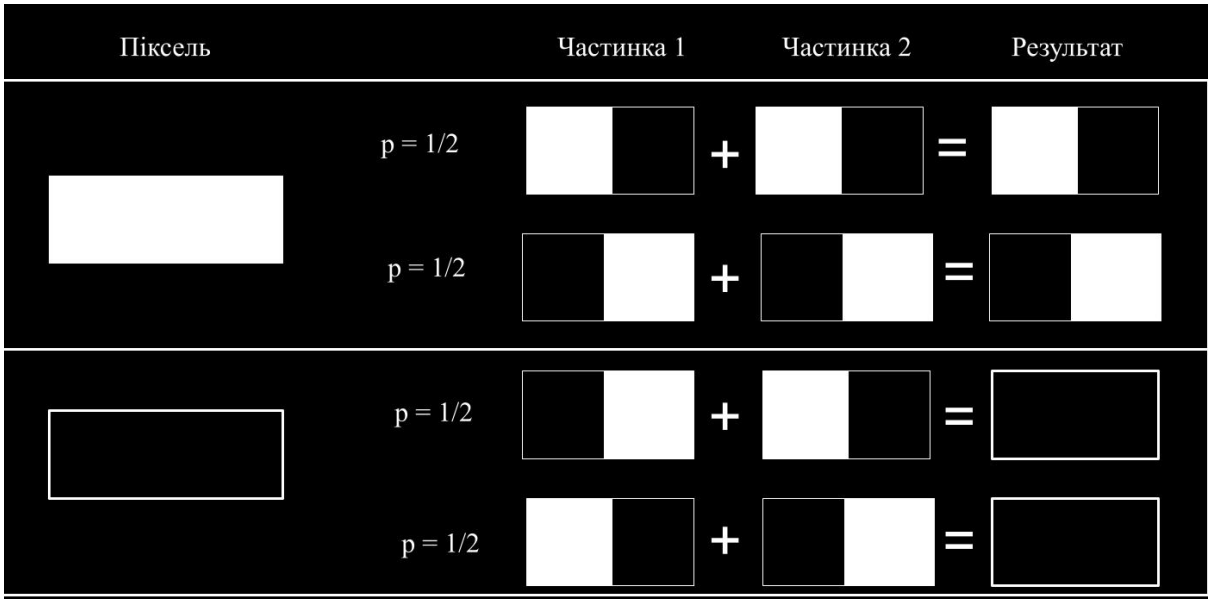

Рис. 1. Схема кодування для (2, 2) візуальної криптографічної схеми

На рис. 2 зображена запропонована схема водяних знаків відбитків пальців. Оригінальний відбиток пальця і зображення мають бути зареєстровані у організації. Організація використовує цю інформацію разом з секретним ключем для того, щоб згенерувати частину патерну відбитку пальця, потрібного для верифікації частин, використовуємих у (2, 2) візуальній криптографічний схемі. Під час виконання ідентифікації та аутентифікації організація використовує позначене зображення, спільний

ресурс перевірки та секретний ключ для створення другого спільного ресурсу- шаблону відбитка пальця, який називається основним ресурсом. Ці дві частки використовуються для вилучення візерунка відбитків пальців. Співвідношення між вилученим візерунком відбитків пальців і оригінальним візерунком відбитків пальців є вирішальним фактором для ідентифікація та аутентифікація.

Рис. 2. Схема водяних знаків відбитків пальців

Схема вбудовування відбитків пальців. Щоб вставити відбиток пальця H розміру P * Q на зображення I розміру X * Y, вибирається число «K» як секретний ключ. Секретний ключ повинен бути різним для різних зображень і його потрібно зберігати таємно. Схема вбудовування включає в себе наступні кроки:

Вхід: секретний ключ (K), зображення (I) розміром X * Y.

Вихід: Помічене зображення (M) розміром X * Y.

Крок 1. Виберіть число K як секретний ключ для зображення (I) і відбитка пальця (H).

Крок 2. Перетворіть H на дворівневе зображення (W) за допомогою im2bw функції MATLAB.

Крок 3. Використовуйте «K» як початкове значення для випадкового генерування P * Q числа на проміжку [1, h], де h = X * Y.

Крок 4. Призначте і-ю пару (Vi1, Vi2) частки-перевірки (V) на основі інформації, наведеної в таблиці 1, використовуючи значення пікселя W і матриці Z.

Крок 5. Зберіть всі значення пари, щоб побудувати частку-перевірки (V). Розмір частки перевірки буде P * 2Q, оскільки один піксель відбитка пальця H розділений на два субпікселі для створення спільної перевірки.

Таблиця 1

Правила генерації частини-перевірки

Колір і-го пікселя в патерні Wi	і-й елемент в бінарній матриці Z	Пари бітів (Vi1, Vi2), які будуть призначені в частині-перевірки
Чорний	1	(0.1)
Чорний	0	(1.0)
Білий	1	(1.0)
Білий	0	(0.1)

Література

1. Low C. Fusion of LSB and DWT biometric watermarking using offline handwritten signature for copyright protection / C. Low, A. Teloh, C. Tee. 2009. №5558. P. 786–795.
2. Ratha N. A. Secure data hiding in wavelet compressed fingerprint images / N. A. Ratha, J. G. Connell, R. M. Bolle // Proceeding of the ACM multimedia workshops. 2000. P. 127–130.
3. Schaathun H. G. On watermarking/fingerprinting for copyright protection / H. G. Schaathun // IEEE Computer Society. 2006. №3. P. 50–53.

4. A study on iris feature watermarking on face data / K. Ryoung, D. S. Jeong, B. J. Kang, E. C. Lee // Proceedings of the 8th international conference on adaptive and natural computing algorithms №4432. P. 414–423.
5. Tzouveli P. Human face watermarking based on zernike moments / P. Tzouveli, K. Ntalianis, S. Kollias // Proceedings of the fifth IEEE international symposium on signal processing and information technology. 2005. P. 399-404.