УДК 004.056.5

О. П. Білик[1]

ПІДВИЩЕННЯ ЗАХИСТУ ПОТОКОВОГО ВІДЕО У СИСТЕМАХ БЕЗПЕКИ ВІД НЕСАНКЦІОНОВАНОЇ МОДИФІКАЦІЇ З ВИКОРИСТАННЯМ КРИХКИХ ЦИФРОВИХ ВОДЯНИХ ЗНАКІВ

[1] Вінницький національний технічний університет;

Анотація

Запропоновано покращення методу вбудовування крихких цифрових водяних знаків у контейнер потокового відео, що дозволяє підвищити захищеність у системах безпеки з метою виявлення незаконних змін та автентифікації відео .

Ключові слова: стеганографія, захист, потокове відео, автентифікація, цифрові водяні знаки.

Abstract

The proposed imprоment for method of embedding fragile digital watermarks into a streaming video container allows to increase safety in security systems in order to detect unauthorized changes and video authentication.

Keywords: steganography, protection, streaming video, authentication, digital watermarks.

Вступ

Цифрові дані, такі як відео, можуть бути перехоплені при передачі через відкриті середовища, отже існують проблеми безпеки та захисту контенту, а саме несанкціоноване копіювання модифікація та поширення з метою компрометації джерела даних.

Метою роботи є покращення стеганографічного методу для підвищення захисту потокового відео у системах безпеки від несанкціонованої модифікації з використанням крихких цифрових водяних знаків.

Результати дослідження

Для збільшення безпеки алгоритму, функція з ключем HMAC-SHA-256 використовується при створенні водяного знаку замість хеш-функції MD5 через більшу захищеність та, як наслідок, надійність збереження даних від несанкціонованого доступу [1]. Результат виконання хеш-функцій для повідомлення ("The quick brown fox jumps over the lazy dog") з ключем ("key") наведено далі:

Назва функції	Результат
MD5	9e107d9d372bb6826bd81d3542a419d6
HMAC_MD5	80070713463e7749b90c2dc24911e275
HMAC_SHA1	de7c9b85b8b78aa6bc8a7a36f70a90701c9db4d9
HMAC_SHA256	f7bc83f430538424b13298e6aa6fb143ef4d59a14946175997479dbc2d1a3cd8

Таблиця 1.1 – Порівняння хеш-функцій

Також, з ціллю збільшення надійності використовується псевдовипадкова послідовність при знаходженні позиції для вбудовування блоків згенерованого ЦВЗ, поріг значень якої генерується динамічно. Біти згенерованого ЦВЗ вбудовуються у два останні найменш значущі біти векторів руху для розширення корисного навантаження вбудовування до 256 біт завдяки алгоритму HMAC-SHA256.

Для забезпечення ефективності автентифікації слід використовувати сильні візуальні особливості, які можуть бути сприйняті неозброєним оком. Досліження показують, що такі особливості можна обчислити коефіцієнтами ДКП, що є середніми значеннями кожного окремого блоку та зосереджують найбільше енергії (інформативності) блоку [2].

Сильні візуальні особливості, які використовуються для генерації крихкого цифрового знаку складаються з набору коефіцієнтів, отриманих з передбачуваних INTRA та INTER блоків, що використовуються при стисненні відеопотоку. Різниця складається у тому, що INTRA-метод використовує для

стиснення дані лише поточного кадру, в той час як INTER-метод дозволяє проаналізувати наступні кадри та на основі отриманої інформації про мінімальні зміни в кадрі збільшити компресію статичних областей.

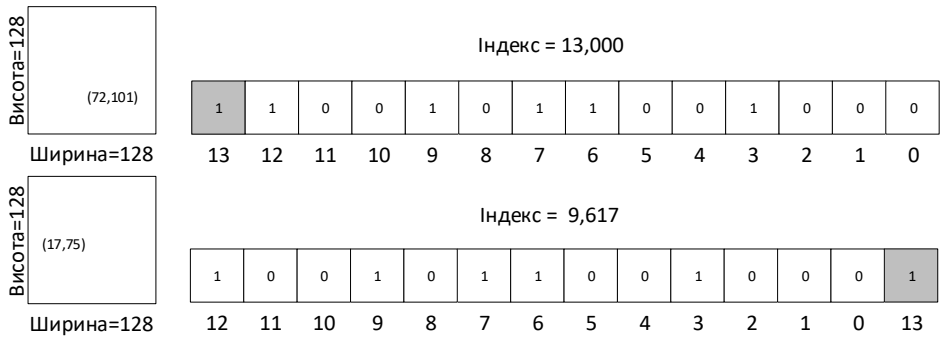

Рисунок 1.1 – Приклад використанням генерації випадкової послідовності для зміни розташування пікселю

Дані характеристики, що використовуються для генерації водяного знаку, складаються з квантованих постійних коефіцієнтів (DC) і перших двох змінних коефіцієнтів (AC), що входять до низькочастотних коефіцієнтів у порядку сканування зиґзаґом кожного блоку в межах INTRA 4×4 і INTER 4×4. Обирається DC-коефіцієнт, який є показником середньої енергії по всіх 4×4 пікселях та коефіцієнти з найбільшою енергією, що міститься в межах перших декількох низькочастотних коефіцієнтів. Високочастотні коефіцієнти майже близькі до нуля та ігноруються під час квантування коефіцієнтів ДКП. Також коефіцієнт DC і два перших коефіцієнта AC є більш стабільними, ніж інші коефіцієнти, при маніпуляції зображенням.

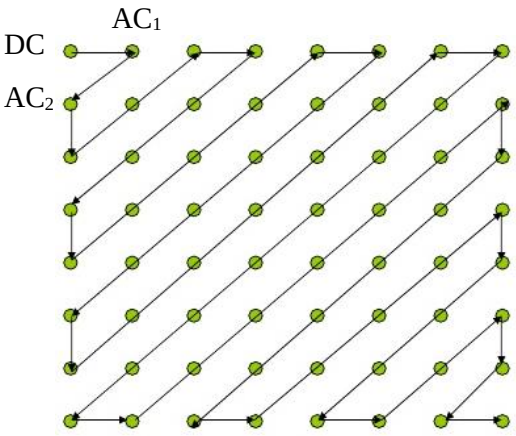

Рисунок 1.2 – DC та AC коефіцієнти

Вбудовування крихкого водяного знаку виконується над векторами руху в межах P-кадрів, які мають високі показники руху (зміни) та належать до вибраних блоків вбудовування. Секретний ключ K використовується для генерування псевдовипадкової послідовності для вибору позиції блоків вбудовування.

Висновки

Встановлено, що запропоноване покращення методу вбудовування крихких цифрових водяних знаків у потокове відео дозволяє підвищити захищеність оригінальності відео шляхом виявлення несанкціонованих модифікацій.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Замула О. А.. Аналіз і обґрунтування критеріїв і показників ефективності криптографічних генераторів псевдовипадкових чисел / О. А. Замула, Д. О. Семченко, Ю. В. Землянко // Системи обробки інформації. — 2014.

2. Feng, D., Siu, W.-C., & Zhang, H. J. Multimedia information retrieval and management: Technological fundamentals and applications: Springer Science & Business Media. — 2013.

Білик Олександр Петрович — студент групи УБ-17м, факультет менеджменту та інформаційної безпеки, Вінницький національний технічний університет, Вінниця

Науковий керівник: ***Карпінець Василь Васильович*** – канд.техн.наук, доцент кафедри менеджменту та безпеки інформаційних систем, Вінницький національний технічний університет, м. Вінниця

Bilyk Oleksandr P. — student of group UB-17m, Department of Management and Information Security, Vinnytsia National Technical University, Vinnytsia

Supervisor: ***Karpinets Vasyl V.*** — Ph. D. Assistant professor, management and security of information Systems department; Vinnitsa, Ukraine