МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ

ДЕРЖАВНА СЛУЖБА СПЕЦІАЛЬНОГО ЗВ'ЯЗКУ
ТА ЗАХИСТУ ІНФОРМАЦІЇ УКРАЇНИ

НАУКОВА АСОЦІАЦІЯ КІБЕРБЕЗПЕКИ УКРАЇНИ

ТЕЗИ

НАУКОВО-ПРАКТИЧНОЇ КОНФЕРЕНЦІЇ

«ПРОБЛЕМИ ЕКСПЛУАТАЦІЇ ТА ЗАХИСТУ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМ»

7 – 9 червня 2023 р.

м. Київ

MINISTRY OF EDUCATION AND SCIENCE OF UKRAINE
NATIONAL AVIATION UNIVERSITY
STATE SERVICE OF SPECIAL COMMUNICATION
AND INFORMATION PROTECTION OF UKRAINE
SCIENTIFIC CYBER SECURITY ASSOCIATION OF UKRAINE

PROCEEDINGS

OF THE SCIENTIFIC AND PRACTICAL CONFERENCE

«OPERATIONAL AND SECURITY PROBLEMS OF INFORMATION AND COMMUNICATION SYSTEMS»

June, 7 – 9, 2023
Kyiv, Ukraine

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ
ДЕРЖАВНА СЛУЖБА СПЕЦІАЛЬНОГО ЗВ'ЯЗКУ
ТА ЗАХИСТУ ІНФОРМАЦІЇ УКРАЇНИ
НАУКОВА АСОЦІАЦІЯ КІБЕРБЕЗПЕКИ УКРАЇНИ

ТЕЗИ

НАУКОВО-ПРАКТИЧНОЇ КОНФЕРЕНЦІЇ

«ПРОБЛЕМИ ЕКСПЛУАТАЦІЇ ТА ЗАХИСТУ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМ»

7 – 9 червня 2023 р.
м. Київ, Україна

УДК 621.39: 004.9 (082)

Проблеми експлуатації та захисту інформаційно-комунікаційних систем: Тези науково-практичної конференції; м. Київ, 7 – 9 червня 2023 р., Національний авіаційний університет. – К.: Вид-во НАУ, 2023. – 117 с.

ISBN: 978-611-01-0740-2

ОРГКОМІТЕТ КОНФЕРЕНЦІЇ

Голова:

ШКУРАТОВ О.І. — проректор Національного авіаційного університету з наукової роботи та інноваційного розвитку, доктор економічних наук, професор;

Члени оргкомітету:

ОДАРЧЕНКО Р.С. — доктор технічних наук, професор, завідувач кафедри телекомунікаційних та радіоелектронних систем Національного авіаційного університету, **головний редактор редколегії**;

ЮДІН О.Ю. — кандидат технічних наук, заступник начальника Державного науково-дослідного інституту технологій кібербезпеки та захисту інформації;

КОРЧЕНКО О.Г. — доктор технічних наук, професор, завідувач кафедри безпеки інформаційних технологій Національного авіаційного університету, лауреат Державної премії України в галузі науки і техніки;

БАХТІЯРОВ Д.І. — кандидат технічних наук, заступник декана Факультету аеронавігації, електроніки та телекомунікацій Національного авіаційного університету;

Секретар:

ЛАВРИНЕНКО О.Ю. — кандидат технічних наук, доцент кафедри телекомунікаційних та радіоелектронних систем Національного авіаційного університету.

УДК 043.2

Д.П. Присяжний, П.В. Павловський, І.В. Абрамчук
Вінницький національний технічний університет, м. Вінниця

ЗАХИСТ ПОТОКОВОГО ВІДЕО ВІД НЕСАНКЦІОНОВАНОЇ МОДИФІКАЦІЇ З ВИКОРИСТАННЯМ КРИХКИХ ЦВЗ

У роботі розглянуто метод вбудовування крихких ЦВЗ, в якому при створенні водяного знаку для збільшення безпеки алгоритму замість хеш-функції MD5 використано функцію з ключем HMAC-SHA-256, а також використано псевдовипадкова послідовність для знаходження 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 бітів завдяки алгоритму HMAC-SHA256. Особливості кожного кадру, такі як кольорова насиченість та яскравість елементів можуть бути використані при генерації водяних знаків для виявлення просторових змін та маніпуляцій над кольоровими характеристиками. 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 у кадрі збільшити компресію статичних областей. Дані характеристики, що використовується 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 усіх 4×4 пікселях та коефіцієнти з найбільшою енергією у 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. Усі отримані дані та коефіцієнти зберігаються в буфері для кожного кодованого блоку в кожному кадрі до моменту миттєвого оновлення декодера (IDR), який свідчить

про відсутність зображення у потоці бітів, що вимагають посилання в порядку декодування до кадрів безпосередньо перед I-кадром. Кадри IDR є I-кадрами, які не посилаються на будь-які кадри поза поточної групи кадрів (GOP). GOP складається з I-кадру та усіх інших P-кадрів, які розташовані між кадрами IDR. Тому кодована підпослідовність відео починається з кадру IDR і закінчується, коли з'являється новий кадр IDR, сигналізуючи про наявність нової підпослідовності, що підлягає кодуванню або закінченню передавання. У кінці кожної групи кадрів ознаки присутні в буфері проходять через захищену функцію хешування HMAC-SHA256.

Процес створення ЦВЗ. Змішування характеристик, що зберігаються у буфері, з секретним ключем K. Створення хешу з отриманої послідовності за допомогою SHA-256. Змішування хешу з секретним ключем K. Застосування обробки SHA-256. Отримана хеш-послідовність довжиною 256 біт використовується в якості крихкого водяного знаку, який вбудовується у вектори руху (MV) в H.264/AVC. 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. Для ретельного вибору блоків вбудовування необхідно розглянути два обмежувальні параметри. Сусідні блоки пропущених блоків відкидаються. Інше обмеження – необхідність уникнення вбудовування інформації у блоки з відсутністю руху та блоки з незначними рухами.

Процес вилучення цифрового водяного знаку виконується на рівні декодеру H.264/AVC та без потреби у оригінальному відеопотоці. Цей процес схожий на процес вбудовування, адже включає в себе обчислення кадрів з найбільшою руховою активністю, вибір позиції вбудовування на основі ключа K, ентропійне декодування векторів руху і застосування двох умов, які виконуються у процесі вбудовування. Біти водяного знаку потім вилучаються з двох останніх найменш значущих бітів компонентів MV_x і MV_y для кожного блоку вбудовування.

На етапі автентифікації необхідно визначити візуальні особливості, які були використані при вбудовуванні. Ці особливості видобуваються перед оберненим квантуванням і операціями перетворення усередині алгоритму H.264/AVC-декодера. Наприкінці кожної неза-

лежної групи кадрів, визначеної декодером, ці дані шифруються з використанням функції HMAC-SHA-256 для перевірки цілісності, використовуючи той самий ключ K, щоб отримати хеш-значення, які будуть порівнюються з вилученими бітами водяного знаку. Будь-які зміни особливостей або хеш-значень будуть означати зміни у контейнері. Таким чином, вміст автентифікується лише, якщо оригінальні та обчислені значення хешу однакові. У разі невдалої автентифікації виявлення фальшивих кадрів виконується окремо. Щоб визначити розташування фальсифікованих кадрів у межах пошкодженої групи кадрів отримувач обчислює хеш-значення усіх кадрів у GOP на рівні декодера, та обчислюються хеш-значення оригінальної групи кадрів.

Для аналізу ефективності крихкого цифрового водяного знаку необхідно провести перевірку на можливість втручання у просторову, часову та область кольору. Втручання можливе шляхом зміни порядку кадрів, їх заміну, зміна розмірів, повертання та зміна кольору області чи окремих областей. У запропонованому алгоритмі ємність водяного знаку залежить від рухової активності та спотворенням, що спричиняються вбудовуванням. Для потоку відео зі значною руховою активністю ($\sigma \geq 3{,}870$) кількість підходящих блоків для вбудовування звичайно більша, ніж у відео з незначною руховою активністю, отже і об'єм даних для вбудовування може бути збільшений. Під час аналізу отримані значення оцінки якості відео (VQM) у діапазоні від 0,292 до 0,398, що призводить до незначного розходження між оригіналом та відеопослідовності з водяним знаком. Отримано індекс SSIM, який зазвичай використовується при оцінюванні відео з водяними знаками щодо оригіналу з точки зору подібності або розбіжностей яскравості, контрасту і структурних подібностей. Значення SSIM, близьке до 1, вказує на високу подібність двох відео і 0 – на повну невідповідність. З отриманих результатів аналізу відео можна зробити висновок, що на відео немає якихось видимих змін після процесу вбудовування, оскільки усі значення SSIM дуже близькі до 1.

Висновки. Запропоновано метод вбудовування крихких ЦВЗ та проведено оцінювання його ефективності. У результаті оцінювання виявлено, що запропонований метод є дієвим, забезпечує можливість виявлення несанкціонованої модифікації та дозволяє вбудувати в середньому у 2,03 рази більше інформації зі збільшенням пікового співвідношення сигналу до шуму на 0.05, що є непомітним для неозброєного ока.