

ДОСЛІДЖЕННЯ МЕТОДУ КОХА-ЖАО ПРИ JPEG-АТАКАХ*Полякова В.О., Мілейко І.Г.*

Досліджуваний метод Коха-Жао позиціонується його авторами, як метод, який дозволяє впроваджувати стего-повідомлення в JPEG-контейнери. Це досягається за рахунок того що в досліджуваний метод закладені принципи, які є базовими для цілого сімейства алгоритмів, які використовують частотну область для вбудовування секретної інформації. Даний алгоритм добре пристосований для вбудовування секретної інформації в зображення, що піддаються алгоритму стиснення JPEG або навіть дозволяє проводити впровадження секретної інформації безпосередньо в JPEG -потік.

На сьогоднішній день ефективною є атака JPEG-стисненням, спрямована на руйнування впровадженої в стего-контейнер секретної інформації, що призводить до неможливості вилучення вбудованого повідомлення з стего-контейнера. Алгоритм стискання JPEG при обробці зображення дозволяє користувачу обрати параметри, які будуть використані в процесі стискання зображення, а саме ступень стиснення, від значення якої залежить якість та розмір зображення, це призводить до загрози руйнування вбудованого повідомлення через JPEG-атаки. Досліджуваний метод Коха-Жао здатний протистояти цим JPEG-атакам, тобто він дозволяє отримати запроваджене в JPEG-контейнер секретне повідомлення, після збереження цього контейнера в форматі JPEG з іншою якістю зображення.

Однак, в ході досліджень було виявлено, що досліджуваний метод Коха-Жао не завжди здатний протидіяти JPEG-атакам, тобто мають місце випадки, коли метод Коха-Жао не справляється з деякими з JPEG-атак. Збереження стего-контейнера з меншою ступеню стиснення, що значно відрізняється від оригінального параметра якості, призводить до непоправної втрати частини або всього секретного повідомлення, вбудованого в стего-контейнер. Ці випадки неспроможності досліджуваного методу протидіяти окремим JPEG-атакам потребують подальшого досконалого розглядання та потребують експериментального підтвердження.

Природним наслідком коригування значень коефіцієнтів є певне спотворення значень всіх пікселів промаркованих блоків. Вплив значення коефіцієнта сили вбудовування на растрове зображення та впроваджену інформацію полягає в наступному: чим більше величина, тим вбудовуване повідомлення більш стійке до стиснення з втратами, але при цьому збільшення параметра сили вбудовування значно погіршує якість промаркованого зображення, при великих значеннях можливе візуальне виявлення слідів маркування.

Стиснення зображень, збережених в графічному форматі JPEG, відбувається за складним алгоритмом перетворення, що включає внутрішнє перетворення колірної моделі, двовимірне ДКП і квантування. Суть квантування інформації полягає в відкиданні частини її обсягу відповідно до спеціальних таблицями або матрицями цілих позитивних чисел, при цьому найбільш схильні до квантування високі частоти растрових зображень.

Експерименти з дослідження стійкості захисного маркування до JPEG-атак проводилися наступним чином. В якості тестового зображення-контейнера було використано 10 зображень різної розмірності. Спочатку секретні повідомлення послідовно вбудовувалися в тестові зображення з форматом JPEG методом досліджуваном Коха-Жао, після цього зображення з вбудованою інформацією послідовно зберігалися в графічному форматі JPEG з коефіцієнтами якості з діапазоном від 12 до 1. Отримані зображення перевірялися на стійкість шляхом перевірки коректності вилученого повідомлення зі стега-контейнера відносно оригінального повідомлення, що було вбудовано.

Проведені експерименти привели до наступних результатів. У зображень з вбудованими повідомленнями і збережених у форматі JPEG з коефіцієнтами якості 12-10, тобто з найкращою якістю з мінімальним стисненням, вбудована інформація детектувалася в більшості блоків. При цьому візуально неможливо було простежити які з блоків зображення були відредактовані, тобто в яких з блоків знаходяться частини повідомлення. Після вилучення повідомлень з тестових зображень, інформація була ідентична той, що початково вбудовувалася в контейнер.

При збереженні стега-контейнерів в графічному форматі JPEG з коефіцієнтом якості 9-7, тобто з якістю вище середнього та не в більшості випадків вбудована інформація все ще детектувалася, при цьому візуально ще неможливо простежити за блоками, що містять секретне повідомлення, але при таких коефіцієнтах якості почали з'являтися блоки з помилковим значеннями, більшість інформації була ідентична оригінальній. При збереженні стега-контейнерів в графічному форматі JPEG з коефіцієнтом якості 6-4, тобто з середньою якістю та середнім стисненням, деякі з блоків вбудованої інформації вже перестали детектуватися, при цьому в деяких випадках візуально простежувалися деякі блоки з вбудованим повідомленням, при таких коефіцієнтах якості збільшується кількість блоків з помилковим значеннями, значно зменшилась кількість коректно вилученої інформації.

У зображень з вбудованими повідомленнями і збережених у форматі JPEG з коефіцієнтами якості 3-1, тобто з найгіршою якістю з максимальним стисненням, вбудована інформація не детектувалася в більшості блоків. При цьому в деяких випадках було можливо візуально простежити які з блоків зображення були відредактовані. Після вилучення повідомлень з тестових зображень, інформація не відповідала той, що початково вбудовувалася в контейнер.