УДК 004.556.53

ПІДХІД ДО 3D СТЕГАНОГРАФІЧНОГО ВБУДОВУВАННЯ ДАНИХ ТА ЙОГО ПРОГРАМНА РЕАЛІЗАЦІЯ

Михайлов Д.О.,
старший викладач кафедри КС Іванова О.М.,
д.т.н., доцент каф. КІСМ Защолкін К.В.
Государственный университет «Одесская политехника», УКРАИНА

АННОТАЦИЯ. Стеганографія є напрямком теорії захисту інформації, який конкурує з криптографією. В роботі пропонується 3D підхід до стеганографічного вбудовування даних в просторову область стего-контейнера. Виконана програмна реалізація запропонованого підходу. В середовищі цієї реалізації здійснено експериментальне дослідження, яке показало ефективність пропозицій роботи.

Вступ. Цифрова стеганографія є одним з ефективних напрямків теорії захисту інформації. Цей напрямок є конкурентом криптографії. В практичних реалізаціях систем захисту стеганографічні методи комбінуються з криптографічними, взаємно доповнюючи один одного [1]. Стеганографія базується на приховуванні інформації одного виду в середовищі інформації іншого виду. Найбільшого розвитку на теперішній час досягли стеганографічні методи, які в якості середовища приховування (стего-контейнера) використовують мультимедійний контент: растрові зображення, цифрове відео та звук.

Мета роботи. В даній роботі ставиться мета розширити існуючі методи просторового стеганографічного вбудовування додаткових даних в стего-контейнер шляхом використання 3D підходу. 3D підхід полягає в обробці стего-контейнера на рівні двовимірних блоків перші два виміри яких становить простір елементарних одиниць контейнера, а третій вимір утворено значеннями елементарних одиниць в окремих колірних каналах.

Основна частина роботи. Одним з найпоширеніших видів стего-контейнерів є растрові зображення. Для просторового стеганографічного вбудовування даних в контейнери цього виду зазвичай використовується базовий метод молодшого значущого біта. Цей метод оснований на тому, що елементарні одиниці мультимедійних контейнерів зазвичай мають аналогову природу утворення. Дані елементарних одиниць отримуються за допомогою аналогових датчиків, після цього перетворюються в цифрову форму та зберігаються у відповідному цифровому форматі. Такі данні є приближеними та мають ділянки розрядів різної значущості для подання елементарної одиниці контейнера. Оскільки молодші біти елементарних одиниць контейнера мають малу вагу та вносять незначний вклад в кількісний еквівалент даних цих одиниць, вони біти використовуються в якості сховища для стего-даних. Зміна цих бітів при вбудовуванні не призводить до візуальної зміни растрового зображення та не може бути явно виявлена.

При стеганографічному просторовому вбудовуванні за методом молодшого значущого біта суттєвою є процедура розподілення вбудовуваних даних по стего-контейнеру. В практичних реалізаціях систем стеганографічного вбудовування використовують детерміновані та псевдовипадкові процедури [2] локалізації цільових пікселів та їх колірних каналів. В межах цих процедур у кожному цільовому пікселі використовуються тільки один з трьох колірних каналів. При цьому один піксель може зберігати один біт стеганографічно вбудованих даних.

Також використовують блочний підхід до вбудовування. Цей підхід полягає у розділенні зображення на прямокутні блоки, в кожний з яких вбудовується один біт секретного повідомлення [3]. В процесі вбудовування обчислюється згортка за модулем два значень молодших розрядів всіх пікселів блока у визначеному колірному каналі. У випадку, якщо обчислене значення відрізняється від значення біту, що вбудовується, виконується інвертування молодшого біту будь-якого одного пікселя блоку.

3D-підхід, що пропонується в даній роботі, полягає в наступному. В середовищі растрового стего-контейнера формується тривимірний простір. Перші два виміри цього простору утворюються простором пікселів контейнеру. Третій вимір утворюється значеннями пікселів в

кожному з трьох колірних каналів (рис. 1). для виконання вбудовування та витягання даних формуються однакові 3D блоки вбудовування, утворені пікселями та їх значеннями у відповідних колірних каналах.

Процедура вбудовування складається з наступних кроків. 1) Побудова 3D блоки вбудовування відповідно до параметрів стего-ключа. 2) Обчислення згортки за модулем два молодших бітів кожного 3D блока. 3) Порівняння значення, яке потрібно вбудувати в блок зі значенням згортки. 4) У випадку відмінності цих значень, виконання корекції значення згортки шляхом інвертування будь-якого молодшого біта 3D блока. Для цього у псевдовипадковий або детермінований спосіб визначається локалізація інвертованого біта.

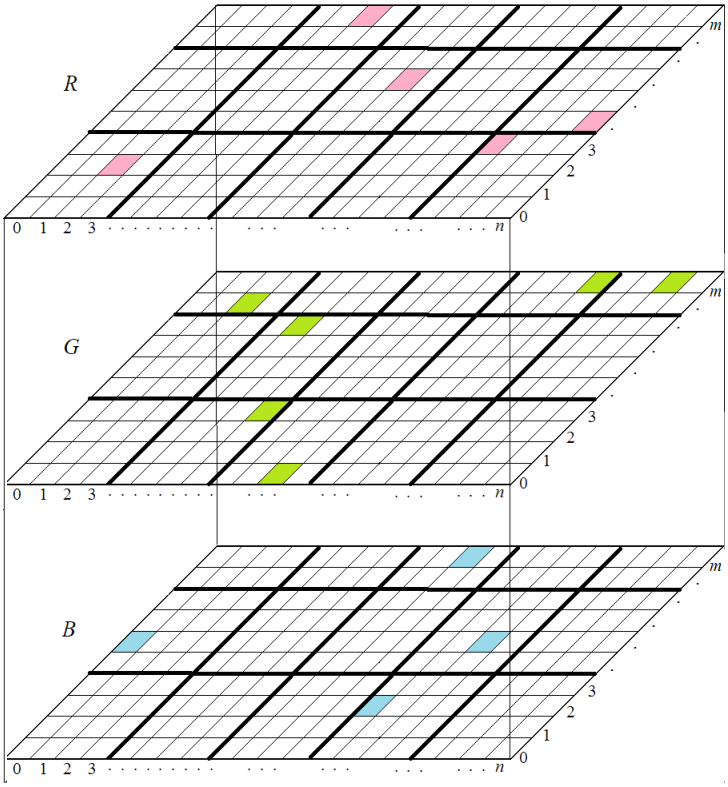

Рис. 1 – Схема стеганографічного 3D-вбудовування

Запропонований підхід було реалізовано програмно. Реалізація була виконана в межах програмної платформи .Net мовою C#. В середовищі розробленого додатку виконано експериментальне порівняння запропонованого відходу з попіксельнім та відомим блочним вбудовуванням. Результати експериментів показали ефективність запропонованого підходу в частині протидії засобам стегоаналізу.

Висновки. В роботі запропоновано 3D підхід до стеганографічного вбудовування даних в просторову область стего-контейнера. Виконана програмна реалізація запропонованого підходу. В середовищі цієї реалізації здійснено експериментальне дослідження, яке показало ефективність пропозицій роботи. Підхід показав переваги за параметром ймовірності виявлення вбудованих даних програмними засобами стегоаналізу.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Shih F. Digital Watermarking and Steganography: Fundamentals and Techniques. 2nd ed. CRC Press, USA, Boca Raton, 2017.
2. Yahya A. Steganography Techniques for Digital Images. Springer, 2018.
3. Fridrich J. Steganography in Digital Media. Cambridge University Press, New York, 2010.