УДК 004.056.5
Ю. Гулка
(Тернопільський національний технічний університет імені Івана Пулюя)

КРИТЕРІЇ ПОРІВНЯННЯ СТЕГАНОГРАФІЧНИХ МЕТОДІВ ПРИХОВУВАННЯ ІНФОРМАЦІЇ В ЗОБРАЖЕННЯХ

UDC 004.056.5
Y. Hulka
(Ternopil Ivan Puluj National Technical University, Ukraine)

CRITERIA FOR STEGANOGRAPHIC METHODS OF HIDING INFORMATION IN IMAGES COMPARISON

Інформаційні технології впевнено входять в різноманітні сфери людського життя, що, в свою чергу, породжує нові загрози та ставить серйозні виклики перед кібербезпекою. Математичні методи криптографії стали невід'ємною частиною захисту даних при їх передачі в мережі Інтернет та виконують функції забезпечення конфіденційності, цілісності та аутентифікації даних. Основна мета шифрування даних – це зробити їх нечитабельними для третьої сторони. Проте криптографічні методи не в силі приховати сам факт передачі секретної інформації. Якщо виникає потреба передати деякі дані секретно, то використовують стеганографічні методи передачі інформації. Для досягнення вищого ступеня захисту часто використовують комбінації криптографічних та стеганографічних методів. Отже стеганографія – це наука про передачу чи зберігання секретних даних з приховуванням факту існування секрету. Сфера застосування стеганографічних методів є досить широкою і включає в себе захист авторських прав на цифрову інформацію, системи контролю доступу поширення цифрового контенту, приховування паролів та багато інших напрямків.

В загальному, модель стеганосистеми може мати вигляд

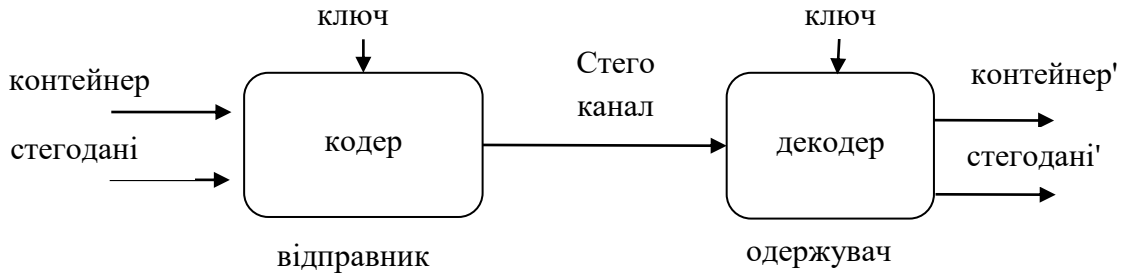

Рисунок 1 – Модель стеганосистеми

Стегодані – це дані, факт передачі яких необхідно приховати, контейнер – відкриті дані, в які приховують секретні дані, ключ – додаткова інформація, що може вимагатись вбудовування та вилучення секретних даних, кодер – стеганографічний алгоритм, що вбудовує дані в контейнер, декодер – алгоритм вилучення даних з контейнеру.

Згідно [1] під час вбудовування даних необхідно враховувати такі критерії:

– Секретні дані повинні бути вбудовані в інші дані контейнеру.

– Стегодані повинні бути стійкими до атак, таких як фільтрування, обертання, відбір.

– Спотворення під час атак повинна бути зрозумілим та усуватись за допомогою верифікаційних кодів перевірки цілісності

– Частина вбудованих даних повинна бути вилучена, навіть якщо лише частина контейнеру доходить до одержувача.

Ефективність стеганографічних методів встановлюється на основі порівняння заповненого та чистого контейнера даних на основі наступних критеріїв: стійкість, непомітність, середньо-квадратичне відхилення, відношення сигнал-шум, кореляція. Існує багато досліджень, що аналізують методи приховування інформації за кожним з цих критеріїв зокрема, проте задача багатокритеріального прийняття рішень для вибору стеганографічного методу для певного застосунку є актуальним науковим дослідженням.

1. Macit, Hüseyin & Koyun, Arif & Güngör, Orhan. A review and comparison of steganography techniques. IV INES International Academic Research Congress Antalya 30 November 2018