

ПРОГРАМНА РЕАЛІЗАЦІЯ СТЕГАНОГРАФІЧНОГО ЗАХИСТУ ПОВІДОМЛЕНЬ

Пустовий А. О.

Науковий керівник – доц., к.т.н. Огородник К.В.

Розвиток засобів обчислювальної техніки в останнє десятиліття дав новий поштовх для розвитку комп'ютерної стеганографії (приховування інформації в певних контейнерах). З'явилося багато нових сфер застосування. Повідомлення вбудовують тепер також і в цифрові дані, що мають, як правило, аналогову природу. Це - мова, аудіозаписи, зображення, відео.

Для програмної реалізації стеганографічного захисту повідомлень було обрано метод найменш значущих бітів (Least Significant Bit, LSB). Цей метод є найбільш поширеним в цифровій стеганографії. LSB метод було розглянуто на прикладі 24-бітного BMP-зображення. Кожна точка кодується 1-м байтом, що визначає інтенсивність кольору зображення. Науково підтверджений факт, що система людського зору найменш чутлива до змін інтенсивності кольору. Заміна молодшого біту пікселя дозволяє помістити в зображення закодовану інформацію та візуально не змінює зображення. Було розроблено програмну реалізацію даного методу (рис. 1).

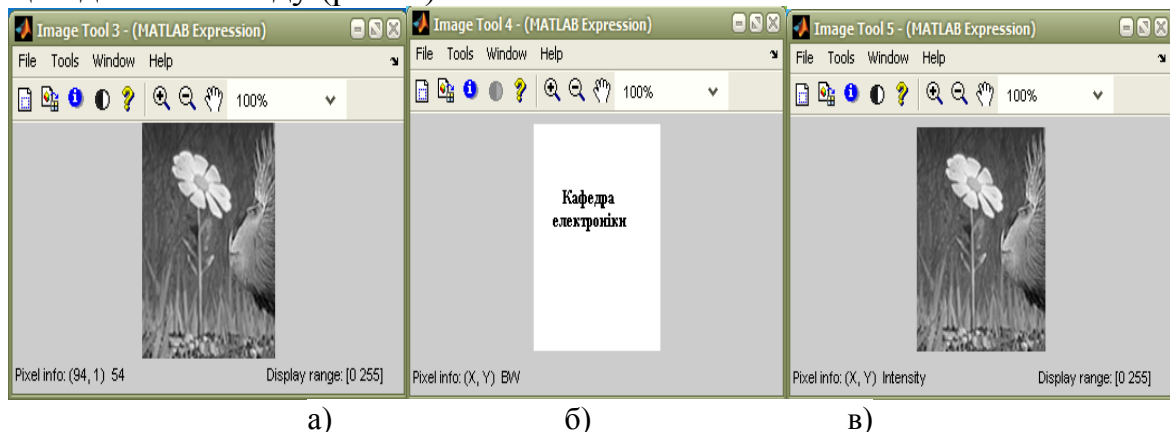


Рисунок 1 – Результат стеганографічного захисту повідомлення (а – зображення-контейнер; б – повідомлення; в – стеганографічне повідомлення)

Даний метод не повністю забезпечує секретність вбудовування інформації, оскільки точно відомо місце розташування зашифрованої інформації. Для подолання вказаного недоліку було розроблено та реалізовано метод, при якому повідомлення не тільки приховується в зображення-контейнер, але й відбувається перемішування закодованих пікселів на вихідному зображенні за певним законом в залежності від введенного ключа. Ступінь захисту даної стеганосистеми залежить від кількості пікселів на зображенні. При зображеннях розміром понад 500x500 пікселів розкодування без ключа є практично неможливим (вимірюється роками).