УДК 681.31.05

СТЕГАНОГРАФІЧНІ МЕТОДИ ПРИХОВУВАННЯ ІНФОРМАЦІЇ

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

Завдання захисту інформації від несанкціонованого доступу вирішувалася в усі часи протягом історії людства. Уже в стародавньому світі виділилося два основних напрямки вирішення цього завдання існуючі і по сьогоднішній день: криптографія і стеганографія. Метою криптографії є приховування вмісту повідомлень за рахунок їх шифрування. На відміну від цього, при стеганографії приховується сам факт існування таємного повідомлення. Повідомлення тепер вбудовують у різні види цифрових даних, що мають, як правило, аналогову природу. Це - мова, аудіозаписи, зображення, відео. Розглянемо найбільш вживані методи стеганографії.

Метод найменш значущих бітів (Least Significant Bit, LSB). Цей метод є найбільш поширеним в цифровій стеганографії. У BMP-зображеннях 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.

Метод обчислення різниці величини пікселів (Pixel Value Differencing, PVD). Пікселі, які знаходяться на краях областей зображення з різною інтенсивністю можуть вмістити більше інформації. Метод PVD використовує цю властивість, поміщаючи великі порції укриваємих даних в зображеннях з великим контрастом.

Метод з використанням стохастичної модуляції. Метод з використанням стохастичної модуляції вміщує біти відомості в пікселях зображення через додавання до зображення шуму з розподілом, симетричним відносно нуля. Носієм для методу є цифрове зображення з 8-бітовою шкалою сірого. Зазвичай використовується розподіл Гауса з випадково змінними знаками.

Метод Langelaar. Даний алгоритм працює з блоками 8x8 пікселів і є вдосконаленням методу LSB. Спочатку створюється псевдовипадкова маска нулів і одиниць. Далі кожен блок ділиться на два субблоки і, залежно від значення маски, для кожного субблоку обчислюється середнє значення яскравості. Перевагою алгоритму є те, що досить складно виявити факт присутності стеганоповідомлення. Недоліком же є погана роботоздатність (нестійкість до перетворень, таких як стиснення). Даний алгоритм можна використовувати для вбудовування повідомлення, але це пов'язане зі складнощами, такими як скасування перетворення файлу контейнера.