

СИСТЕМА СТЕГАНОГРАФІЧНОГО ШИФРУВАННЯ ПОВІДОМЛЕНЬ**Білевцов С.Ю., Поворознюк А.І.***Національний технічний університет
«Харківський політехнічний інститут»,
м. Харків*

В наш час взаємодію між інфраструктурами неможливо уявити без передачі повідомлень. Питання збереження та приховування інформації займає особливе місце в системі комунікацій. Втрата чи перехоплення інформації, може призвести до непередбачених чи небажаних наслідків. Актуальність розробки даного проекту полягає в потребі формування системи приховування повідомлень, зі укріптям самого факту передачі, у разі виникнення даної потреби в певних службах.

Для стеганографічного шифрування одним з найоптимальніших є зображення формату BMP. Кожен піксель позначаємо як x_j . RGB спектр кольору має позначення g_j . Як відомо, за для відтворення кольору, кожен піксель в зображенні має три байти для задання кожного кольору – червоного, зеленого, синього. Адитивною функція є через те, що отримання заданого кольору отримується шляхом додання кожного окремо взятого каналу ($g_1 + g_2 + g_3$). Оскільки кожен символ, що записується до зображення, у бінарному вигляді має довжину 8 біт, отримуємо наступну залежність

$$A = \frac{2 \times 3 \times a \times b}{8} - 2,$$

де A – кількість символів, котрі можна записати до зображення; a – довжина зображення у пікселях по горизонталі; b – значення висоти зображення у пікселях по вертикалі.

Коефіцієнтні значення 2 – кількість використовуваних бітів у кожному кольорі, 3 – кількість використовуваних кольорів у пікселі, 8 – довжина в бітах для кожного символа, що записується до зображення. Відняття двох бітів в кінці необхідне для резервування відомості про факт стеганографічного шифрування. Для перетворення зображення з кольорового до чорно – білого, або бінарного вигляду, необхідно виконати адитивне складання значень байтів кожного відтинку для певного пікселя, та прирівняти зі значенням z , котре користувач міг би сам обрати для себе.

$$\sum_{i=1}^{Cgi} R_{gcH1} + G_{gcH1} + B_{gcH1} = \begin{cases} 1, & \text{якщо } > z, \\ 0, & \text{якщо } < z, \end{cases}$$

де z – певне граничне значення для перетворення зображення.

Таким чином, проект, що сумісний з більшістю версій операційних систем та програмного забезпечення, використовуючий даний алгоритм стеганографічного шифрування є актуальним. Розвиток алгоритму та його покращення дасть можливість вбудовувати інформацію в потокові дані що покращить рівень її прихованості.