**Д.техн.н. Шумейко О.О., Вовченко Д.Ю.**

*Дніпродзержинський державний технічний університет*

**ВИКОРИСТАННЯ ФОРМАТУ JPEG ДЛЯ СТЕГАНОГРАФІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ**

Безпека є однією з головних умов комфорту людини. А в будь-якій Конституції гарантується захист приватних даних, що ніяким чином не пов’язано з секретністю інформації у мережі Інтернет. Якщо говорити про неналежну захищеність інформації, то можуть виникнути такі проблеми як: крадіжка та несанкціоноване використання даних, або витік секретної інформації та її небажана доступність третій стороні.

Для захисту приватних документів існують різні криптографічні протоколи, які засновані на складно вирішуваних математичних проблемах, наприклад таких, як розподіл простих чисел. Але з появою новітніх технологій, існує велика ймовірність того, що існуючі криптографічні алгоритми буде виявлено та розшифровано.

За допомогою ж стеганографічних методів захисту інформації можна як безпечно передати таємну інформацію отримувачу, так і залишити свій невидимий водяний знак, за допомогою якого доводиться авторство, при цьому, зробити це так, що про наявність вкладеної інформації потенційний перехоплювач не буде здогадуватися.

У якості контейнера для вкладення інформації потрібно використовувати сучасний та розповсюджений у Інтернеті формат файлів. Цим умовам відповідає формат JPEG**,** робота з яким ускладнюється тим, що це формат зі стиском, під час якого перебудовується структура даних. Донедавна, стеганографія у JPEG вважалася неможливою. Для формату BMP, що вже майже не зустрічається у мережі, часто використовується метод останнього значущого біта, що непомітно для людського зору замінює останній біт значення кольору пікселя на біт інформації що приховується. Враховуючи вищевказану специфіку формату JPEG, було вирішено застосовувати даний метод до коефіцієнтів дискретного косинусного перетворення, що вираховуються на одному з етапів стиску файлу даного формату, коли кожна матриця пікселів розміру NxN, частіше 8х8, перетворюється на матрицю частотних коефіцієнтів відповідного розміру. Приховувати дані потрібно лише після квантування, та ретельно підбираючи коефіцієнти, інакше, усі дані буде знищено, а зображення зіпсовано.

Такий метод приховування інформації вважається стійким. Зображення майже не втрачають якості, витримують певний стиск, та деякі маніпуляції, без втрат даних, або з частковою втратою.

На основі даної ідеї реалізовано програмний продукт. Використовуючи дану програму, було проведено експерименти. Результати наведено у таблиці 1.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Зображення | Без стиску | Стиск (10%) | Стиск (25%) | Обрізання |
| Dogs.jpg (color) | sold for 55 | sold for 55 | sold for 55 |   x |
| Dudes.jpg (color) | Sold |   X | sold  | sold |
| Road.jpg (grayscale) | sold for 2k | sold for 2k |   x |   х |
| Egg.jpg (color) | too much eyes |   X | too much eyes | too -uch |

Таблиця 1 – Результати експериментів

Як видно з таблиці, хоч інформація може витримати деякі маніпуляції, категорично не рекомендується стискати зображення, або псувати їх будь-яким іншим чином, оскільки важливо, щоб повідомлення надійшло до адресата у цілості.