

УДК 004.056

*Сіденко В. П., старш. викладач кафедри
Житомирський державний технологічний університет*

ПРО ЗАБЕЗПЕЧЕННЯ ДІЙСНОСТІ ЗОБРАЖЕНЬ ПРИ ПЕРЕДАЧІ ЇХ В ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМАХ СТЕГАНОГРАФІЧНИМИ МЕТОДАМИ

В даний час, незважаючи на велику кількість існуючих методів і алгоритмів маркування, не існує універсального способу захисту зображень і визначення його автентичності, тому завдання розробки моделей і алгоритмів, що дозволяють забезпечити можливість доказу автентичності та справжності захищених зображень, є актуальною.

Розробка різних методів і заходів щодо захисту інформації ведеться з найдавніших часів. Серед них можна виділити два основних напрямки – криптографія і стеганографія.

Криптографія забезпечує приховування вмісту повідомлень за рахунок їх шифрування, а стеганографія – приховування самого факту існування секретних даних при їх передачі, зберіганні або обробці.

Метою даної доповіді є знайомство з методами аналізу автентичності зображення, які включають в себе методи стеганографічного захисту інформації з використанням графічних контейнерів. Як контейнери розглядаються зображення.

Зображення – інформаційна модель, в якій використовується графічний спосіб представлення інформації. Для зберігання зображень використовуються графічні формати – векторні і растрові. Всі формати розрізняються своїми властивостями і особливостями. У представленій доповіді розглянуті растрові формати, як BMP і JPEG.

Файли формату BMP – нестиснені, складаються з чотирьох частин: заголовка, інформації про заголовок, визначення таблиці відтінків і набору растрових пікселів. Зображення файлу формується з пікселів, які можуть містити червоний, зелений і синій відтінки.

Основною перевагою BMP формату є можливість вносити зміни в кожен окремих піксель зображення, при цьому інша частина зображення не буде задіяна. BMP є несжатим файлом, значить, його розмір при перегляді в програмах залишається незмінними. Можна відкривати і зберігати зображення без порушення цілісності файлу.

JPEG не підходить для стиснення зображень при багатоступінчастій обробці, тому що спотворення в зображення будуть вноситися кожен раз при збереженні проміжних результатів обробки. JPEG не можна використовувати у випадках, коли неприпустимі навіть мінімальні втрати, наприклад, при стисненні астрономічних або медичних

зображень. Найчастіше JPEG використовується в цифровій фотографії, а також для зберігання і передачі зображень в Інтернеті.

Широке поширення глобальних мереж і зручність обробки зображень за допомогою графічних редакторів привели до підвищеного інтересу до цифрової графіки.

Вільна доступність інструментів для редагування зображень, адаптованих під непросунутого користувача, ставить під сумнів їх достовірність, коли це дуже важливо. Довести порушення авторських прав на зображення, а також підтвердити порушення їх цілісності досить складно.

Для досягнення цих цілей необхідно звернути особливу увагу на захист зображення від впливів і виявлення підробки.

Існує безліч способів, здатних відрізнити оригінальне зображення від зміненого з використанням методів виявлення підробки на підставі перевірки цифрових водяних знаків (ЦВЗ).

У доповіді розглядаються питання захисту автентичності зображення (контейнер) шляхом вбудовування в нього ЦВЗ. Розглядаються статистичний метод захисту інформації.

Основою статистичних методів приховування даних є модифікація певних статистичних властивостей фрагментів або зображення в цілому.

Під час вилучення перевіряються статистичні гіпотези або виконується перевірка наявності зазначених даних в контейнері. Основною метою статистичних методів є можливість приймаючою стороною розрізнення порожнього і заповненого контейнера.

Наводяться умови відповідності зображення і ЦВЗ; наводиться схема і алгоритм формування ЦВЗ; наводиться алгоритм вбудовування ЦВЗ в зображення; наводиться алгоритм вилучення ЦВЗ з зображення в яке він вбудований.