УДК 004.056
І.Тернавчук
(Тернопільський національний технічний університет імені Івана Пулюя)

АНАЛІЗ МЕТОДІВ ЦИФРОВОЇ СТЕГАНОГРАФІЇ НА ОСНОВІ ДИСКРЕТНОГО КОСИНУСНОГО ПЕРЕТВОРЕННЯ

I.Ternavchuk

ANALYSIS OF DIGITAL STEGANOGRAPHY METHODS BASED ON DISCRETE COSINE TRANSFORMATION

З переходом до цифрового представлення інформації загострилася і без того актуальна проблема захисту конфіденційної інформації від несанкціонованого доступу. Дану проблему вирішують дві науки: криптографія та стеганографія. Але більший інтерес являє собою наука – стеганографія, тому що найбільш успішний спосіб захистити інформацію – це приховати сам факт наявності в ній чогось конфіденційного, що може привернути увагу зловмисника.

Існує два напрямки методів цифрової стеганографії:

– приховування інформації у часовій області мультимедійного об'єкта;

– приховування конфіденційної інформації в частотній області мультимедійного об'єкта.

Методи першої категорії працюють безпосередньо з зображенням. Принцип вбудовування інформації у часовій області контейнера полягає в наступному: інформацію вбудовують в незначущі біти області зображення, щоб не змінити візуальне представлення зображення для зорової системи людини. Вони застосовні тільки до зображень, які не були підвернені стисненню, тому що при стисненні малозначима інформація просто відсікаються. У разі впровадження в частотній області модуляції піддаються амплітудні складові комплексного спектра зображення-контейнера. Для цього попередньо здійснюється обчислення амплітудної і фазової складових компонентів перетворення Фур'є.

Серед лінійних ортогональних перетворень було обрано найбільш популярне дискретне косинусне перетворення [1], його застосовують при стисненні зображень і відео в стандартах JPEG, MPEG. Метод стеганографічного приховування буде стійкий до наступної компресії зображення, тільки в тому випадку, якщо враховує особливості використовуваного методу компресії [2].

Перевагами методу є стійкість до JPEG-компресії з малим коефіцієнтом стиснення. Але при цьоцу, основним недоліком – невелике візуальне спотворення зображення-контейнера при великому пороговому значенні різниці між коефіцієнтами ДКП блоків та малий обсяг повідомлення, який можна вбудувати. Проведений аналіз методів цифрової стеганографії показав, що всі існуючі на сьогоднішній час методи базуються в основному на надлишковості інформації, а також на невеликій чутливості людського ока в зміні характеристик зображення. Звичайно, найбільш ефективними є методи які використовують частотну область для вбудовування конфіденційної інформації, бо вони більш стійкі до різних викривлень, в тому числі стиснення, вбудовування інформації відбувається на етапі перетворень вихідного зображення. Методи цифрової стеганографії базуються на дискретно косинусному (DC) перетворенні забезпечують велику стійкість до атак.

Середнє значення змін DC-коефіцієнтів практично для всіх зовнішніх впливів з великою інтенсивністю, розглянутих в даній роботі, не перевищує 3%, що гарантує стійкість впровадженої інформації.

Література.

1. Мельник С. Методи цифрової стеганографії: стан та напрями розвитку // С. Мельник, В. Кащук. // Information Security of the Person, Society and State. – 2013. – №3. – С. 65–70

2. Генне О.В. Основные положения стеганографии // Защита информации. Конфидент – 2000. №3 – 56 с.