Аналіз та дослідження форматних стеганоалгоритмів на основі графічних контейнерів

Рейда О.В.
Науковий керівник – к.т.н., доц. Джулій В.М.
Хмельницький національний університет

Форматні методи, по загальновизнаному висновку більшості фахівців, не відносяться до цифрової стеганографії в чистому вигляді, оскільки не використовують методи цифрової обробки сигналів. Вони засновані на надмірності форматів комп'ютерних даних, наприклад, структурі файлів, ір-пакетів. Хоча цифрові зображення теж є сигналами, але вони мають «застиглий» характер. Тому при роботі з будь-яким алгоритмом, який додає в кінець файлу JPEG байти файлу RAR, не можна строго говорити про цифрову стеганографію зображень, оскільки це є використанням форматного методу в комп'ютерній стеганографії. Тому пропонується наступне визначення форматного методу в цифровій стеганографії зображень: метод перетворення зображення, причому впроваджувана інформація не ініціює візуалізацію артефактів вбудовування інформації, але обов'язково враховується і використовується при декодуванні файлу зображення спираючись на специфікацію формату JPEG.

Розроблений стеганографічний алгоритм використовує запропоноване визначення форматного підходу для впровадження інформації в цифрове зображення. Відмітимо, що впровадження інформації відбувається не з потоком повідомлення, а із службовою і сигнальною інформацією, що не несе смислового навантаження.

Стеганоалгоритми, які використовуються в просторовій області, вбудовують інформацію в область самого зображення. Перевага в тому, що для впровадження інформації не потрібно проводити обчислювально-трудомісткі лінійні перетворення зображень. Інформація вбудовується маніпуляціями колірними складовими $(r(x,y), b(x,y), g(x,y))$ або яскравістю $l(x,y) \in \{1,...,L\}$. Ці алгоритми були розроблені, коли широко застосовувався графічний формат BMP, в якому закладений механізм зберігання інформації про колірні складові кожного пікселя в зображенні. Різновид BMP-форматів полягав в кодуванні колірних складових, тобто в кількості кольорів, півтонів і відтінків в конкретному BMP-зображенні. Тут для кодування кольору кожного пікселя виділяється три байти. Кожен байт потенційно дозволяє

закодувати 28-256 відтінків кольору. А три байти можуть представити один з 2563 = 16777216 мільйонів відтінків кольору.

Серед всіх лінійних ортогональних перетворень найбільшу популярність в стеганографії отримали вейвлет-перетворення і ДКП, що частково пояснюється їх успішним використанням при стискуванні зображень. Крім того, бажано застосовувати для приховування даних те ж перетворення зображення, як і те, якому воно піддасться при можливому подальшому стискуванні. Стеганоалгоритм може бути вельми робастним до подальшої компресії зображення, якщо він враховуватиме особливості алгоритму стискування. При цьому, звичайно стеганоалгоритм, використовуючий ДКП, зовсім не обов'язково буде робастним по відношенню до вейвлетному алгоритму стискуванню. Стеганоалгоритм, використовуючий вейвлети, може бути неробастним до стискування із застосуванням ДКП. Ще більші труднощі з вибором перетворення при приховуванні даних у відеопослідовності. Причина полягає в тому, що при стискуванні відео основну роль грає кодування векторів компенсації руху, а не лише нерухомого кадру. Робастний стеганоалгоритм повинен якимсь чином враховувати це.

Відомо багато моделей для оцінки пропускної спроможності каналу приховування даних. Розлянемо наступну модель: Нехай *S0* - початкове зображення (контейнер), *W*- вкладення. Тоді модифіковане зображення *SW=S0+W*. Модифіковане зображення візуально не відрізняється від початкового і може бути піддане стискуванню з втратами: *SW=C(SW)*, де *C()* - оператор компресії. Біти вкладення *W* мають витягуватись з $\tilde{S}_W$.

Блок-діаграма даного стеганоканала представлена на рисунку 1.

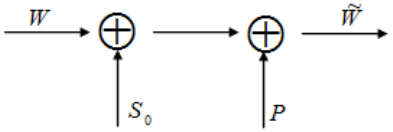

Рисунок 1 - Блок-діаграма стеганоканала

Повідомлення *W* передається по каналу. Канал має два джерела «шуму»: *S0* - зображення-контейнер і *P* - «шум», що виникає при компресії/декомпресії. $\tilde{W}$ - можливо спотворене повідомлення.

Структурна схема схема стеганосистеми приведена на рис. 2. Зображення декомпозується на *L* субсмуг. До кожної субсмуги «підмішується» прихована інформація. Після зворотного перетворення виходить модифіковане зображення *SW*. Після компресії/декомпресії

виходить зображення $\tilde{S}_W$. Воно піддається прямому перетворенню, і з кожної L субсмуг незалежно витягується приховане повідомлення.

Реальні зображення не є випадковим процесом з рівномірно розподіленими значеннями величин. Добре відомо, і це використовується в алгоритмах стискування, що велика частина енергії зображень зосереджена в низькочастотній частині спектру. Звідси і потреба в здійсненні декомпозиції зображення на субсмуги. Стеганоповідомлення додається до субсмуг зображення. Низькочастотні субсмуги містять більшу частину енергії зображення і, отже, носять шумовий характер. Високочастотні субсмуги найбільш схильні до дії з боку різних алгоритмів обробки, будь то стискування або НЧ фільтрація. Таким чином, для вкладення повідомлення найбільш відповідними кандидатами є середньочастотні субсмуги спектру зображення.

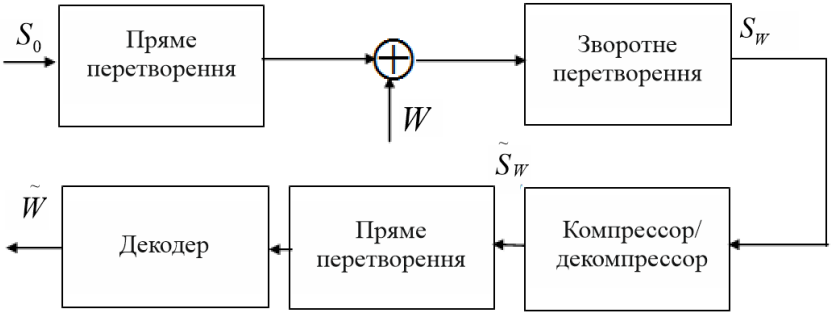

Рисунок 2 - Структурна схема схема стеганосистеми

Найбільший виграш дає перетворення Карунену-Лоева (ПКЛ) – розкладання по базису одиничного імпульсу (тобто відсутність перетворення). Перетворення, що мають високі значення виграшу від кодування, такі як ДКП, вейвлет-перетворення, характеризуються різко нерівномірним розподілом дисперсій коефіцієнтів субсмуг. Високочастотні субсмуги не підходять для вкладення через великий шум обробки, а низькочастотні – через великий шум зображення. Тому доводиться обмежуватися середньочастотними смугами, в яких шум зображення приблизно дорівнює шуму обробки. Оскільки таких смуг небагато, то пропускна спроможність стеганоканала невелика. В разі використання перетворення з нижчим виграшем від кодування, наприклад, Адамара або Фур'є, є більше блоків, в яких шум зображення приблизно дорівнює шуму обробки. Отже, і пропускна спроможність вища. Для підвищення пропускної спроможності стеганографічного каналу краще застосовувати перетворення з меншими виграшами від кодування, які погано підходять для стиску сигналів.

Ефективність використання вейвлет-перетворення і ДКП для

стискування зображень пояснюється тим, що вони добре моделюють процес обробки зображення в СЧЗ, відокремлюють «значимі» деталі від «незначимих». Отже, їх доцільніше застосовувати в разі активного порушника. Насправді, модифікація значимих коефіцієнтів може привести до неприйнятного спотворення зображення. При використанні перетворення з низькими значеннями виграшу від кодування існує небезпека порушення вкладення, оскільки коефіцієнти перетворення менш чутливі до модифікацій.

ДКП застосовують як до всього зображення в цілому, так і до окремих блоків точок зображення. Зазвичай контейнер розбивають на блоки розміром 8х8 пікселів. Потім до кожного блоку застосовують ДКП. Отримані матриці коефіцієнтів ДКП мають розмір 8х8.

Дослідження показали, що область перетворення погано підходить для впровадження великих об'ємів даних. Проте область перетворення добре підходить для впровадження ЦВЗ, що являють собою невелику послідовність з байтів. Принциповою вимогою є також і безліч обмежень, що пред'являються до контейнера.Алгоритми, які застосовуються до просторової області зображення, базуються на візуальній надмірності сприйманої інформації і тому в даний час є не такими популярними, як алгоритми області перетворення. Це пов'язано з великим поширенням формату JPEG, де колірні і яскраві складові пікселей приховані за областю перетворення.

Запропонована метрика оцінки спотворень зображень, що забезпечує об'єктивність порівняльного аналізу стійкості різних стеганоалгоритмів ДВП області вбудовування. Область перетворення, за рахунок невеликого числа потенційних місць для впровадження, більше личить для впровадження невеликої кількості інформації, наприклад ЦВЗ.

За результатами виконаного порівняльного аналізу стійкості ЦВЗ, які були вбудовані різними стеганографічними алгоритмами ДКП області вбудовування, зроблений висновок, що стійкість ЦВЗ не більше *Kjpeg-2000=60* для цифрових водяних знаків, представлених рядком символів в 8-мі бітовому кодуванню, і *Kjpeg-2000=50* для цифрових водяних знаків, представлених бітами. Контейнер з *Kjpeg-2000=50* можливо застосовувати для комерційного використання.

Література

1. Грибунин В.Г. Цифровая стеганография. /В.Г.Грибунин, И.Н.,Оков И.В.,Туринцев // М.: СОЛОН-Пресс; 2002. - 261 с.

2. Конахович Т.Ф. Компьютерная стеганография / Т.Ф Конахович, А.Ю Пузыренко // Теория и практика. Киев: МК-Пресс, 2006. -288с.

3. Мамаев М. Технологии защиты информации:в Интернете/ Мамаев М., Петренко С. //: Специальный;справочник..СИб::Иитер 2002. -848 с.

4. Аграновский А.В. Стеганография, цифровые водяные знаки и стеганоанализ. /А.В. Аграновский, А.В. Балакин, В.Г. Грибунин - М.: Вузовская книга 2009. - 220 с.