УДК 004.056.55:004.932

Нікіта ФІЛІППЕНКО

Національний університет Одеська політехніка

РОЗРОБКА ТЕОРЕТИЧНОГО БАЗИСУ СТЕГАНОМЕТОДУ, ЗАСНОВАНОГО НА ЗБУРЕННЯХ СИНГУЛЯРНИХ ЧИСЕЛ

Вступ: Ефективність забезпечення захисту інформації, зокрема стеганографічного [1], головним чином залежить від теоретичного базису, який покладений в основу використовуваних методів та алгоритмів. В роботі з метою створення теоретичного базису стеганографічного методу, стійкого до атак проти вбудованого повідомлення, проведені дослідження властивостей сингулярних чисел блоків матриці цифрового зображення в умовах додаткових збурних дій. Визначені сингулярні числа блоків цифрового зображення, які мають найменшу чутливість до змін вхідних даних. Збурення саме цих сингулярних чисел в результаті стеганоперетворення повинно забезпечити стійкість до збурних дій відповідного стеганографічного методу.

Мета: розробка теоретичного базису, що забезпечить для стеганографічних методів, розроблених на його основі, стійкість до атак проти вбудованого повідомлення, шляхом дослідження властивостей сингулярних чисел блоків матриці ЦЗ в умовах додаткових збурних дій.

1. Теоретичні основи алгоритму шифрування графічної інформації

З кожним днем разом з поширенням та впровадженням інформаційних технологій у всі сфери життя суспільства, створення значного обсягу конфіденційних та критично важливих даних у цифровому вигляді зростає пріоритет задач інформаційної безпеки, зокрема стеганографії. Ефективність забезпечення захисту інформації в будь-якій галузі, головним чином залежить від того теоретичного базису, який покладено в основу використовуваних методів та алгоритмів. Огріхи в теоретичному базисі можуть призвести до недієздатності використовуваного методу в критичний момент і, як наслідок, до катастрофічних наслідків як для окремої людини, фірми, підприємства, так суспільства в цілому. Основна увага в роботі при розробці базису приділяється забезпеченню стійкості відповідного методу до атак проти вбудованого повідомлення.

Серед цифрових контентів на сьогодні найбільше поширення отримали цифрові зображення (ЦЗ), які використовуються в роботі, та цифрові відео, при цьому очевидно, що цифрове відео може розглядатися як послідовність кадрів-зображень, що робить можливим застосовувати отримані для зображень результати для відео послідовностей [2].

Для задач стеганографії добре зарекомендував себе загальний підхід до аналізу стану інформаційних систем (ЗПАІС), заснований на матричному аналізі та теорії збурень [3], відповідно з яким будь-які зміни, що відбуваються з системою, зокрема системою захисту інформації, формально можуть бути представлені у вигляді сукупності збурень повного набору формальних параметрів - сингулярних чисел (СНЧ) і сингулярних векторів (СНВ) матриці, що ставиться у відповідність інформаційній системі. ЗПАІС є перспективним і таким,

удосконалення якого дасть можливість покращити властивості тих систем захисту інформації, зокрема стеганографічних систем, які на ньому базуються. Одним з напрямів такого удосконалення є детальне дослідження властивостей сингулярних чисел в сенсі їх чутливості до збурних дій, що робиться в роботі.

Поняття стійкості стеганоалгоритму до атак проти вбудованого повідомлення нерозривно пов'язано з поняттям чутливості параметрів, що визначають контейнер, стеганоповідомлення, до збурних дій. Від характеру реакції цих параметрів на збурну дію (атаку проти вбудованого повідомлення) буде залежати ефективність декодування вбудованої інформації, кількість помилок, що виникають в результаті змін в матриці стеганоповідомлення при атаці.

2. Практична реалізація алгоритму

Всі СНЧ будь-якої матриці F, зокрема матриці цифрового зображення, є нечутливими до збурних дій, чи добре обумовленими, у відповідності з формулою [2]:

$$\max_i |\sigma_i(F) - \sigma_i(F + \Delta F)| \le \|\Delta F\|_2 \qquad (1)$$

де $\sigma_i(F)$, $\sigma_i(F + \Delta F)$ - СНЧ поданої F та збуреної $F + \Delta F$ матриць відповідно, ΔF - матриця збурення, $\|\cdot\|_2$ - спектральна матрична норма.

Але все ж таки різні СНЧ матриці/блоку матриці ЦЗ будуть реагувати по-різному на одну й ту саму збурну дію, не перевищуючи величини $\|\Delta F\|_2$, залишаючи актуальною задачу виявлення найстійкіших з них.

Зазначимо, що останнім часом переважна більшість розроблюваних стеганографічних методів є блоковими, тобто такими, що здійснюють вбудову/декодування додаткової інформації поблоково. Це дає можливість забезпечити порівняно незначну обчислювальну складність методу у випадку його послідовної реалізації, а також дає простий спосіб розпаралелювання такого методу, оскільки обробка кожного блоку відбувається незалежно. Враховуючи цей факт, подальше дослідження проводиться для блоків матриці ЦЗ, отриманих шляхом її стандартної розбивки.

В ході дослідження було проведено обчислювальний експеримент, в якому було задіяно 100 оригінальних ЦЗ різного формату (з втратами (JPEG) та без втрат (TIFF)), різного розміру, отриманих професійними та непрофесійними відео камерами. В ході експерименту матриця F оригінального ЦЗ розбивалася на непересічні $l \times l$-блоки. Для кожного блоку окремо будувалося сингулярне розкладання [4]:

$$B = USV^T, \qquad (2)$$

де U, V - ортогональні l×l-матриці лівих і правих СНВ блоку B, $S = diag(\sigma_1, \sigma_2, ..., \sigma_l)$ - діагональна матриця сингулярних чисел; в результаті якого отримувалися СНЧ блоку σ_1, $\sigma_2, ..., \sigma_l$. Після отримання СНЧ оригінальне ЦЗ піддавалося збурній дії, в якості якої в роботі використовувалися різні шуми (гауссівський, мультиплікативний) з різними параметрами. Використання саме шумів, зокрема гауссівського, є традиційним при моделюванні збурних дій на ЦЗ, навіть стеганоперетворення. В ході експерименту збурене зображення

зберігалося в форматі без втрат, після чого розбивалося на $l \times l$-блоки, для кожного з яких будувалося сингулярне розкладання (2), за допомогою якого визначалися СНЧ кожного блоку ЦЗ після атаки: $\bar{\sigma}_1$, $\bar{\sigma}_2$,...,$\bar{\sigma}_l$. Збурення $\Delta\sigma_i$ для кожного СНЧ в кожному блоці визначалося за формулою: $\Delta\sigma_i = \left|\sigma_i - \bar{\sigma}_i\right|$, $i = \overline{1,l}$, після чого розраховувалися середні значення $\Delta\sigma_i$ по всім блокам ЦЗ.

В результаті експерименту встановлено, що найбільш стійкими до збурних дій в блоках ЦЗ є максимальне СНЧ σ_1 і декілька (два σ_{l-1}, σ_l) найменших СНЧ, які встановлюють найбільш сприятливу зону (НСЗ) для вбудови додаткової інформації при стеганоперетворенні, стійкому до атак проти вбудованого повідомлення.

Характер зміни середніх значень збурень СНЧ блоків не залежить

- від формату ЦЗ,
- від конкретних характеристик ЦЗ,
- від характеристик збурної дії, якій піддається ЦЗ,
- від розміру l використовуваного блоку,

тобто НСЗ для будь-якого ЦЗ-контейнера (з втратами, без втрат) при довільній збурній дії визначається як σ_1, σ_{l-1}, σ_l.

Важливо, що означена картина характеру збурень СНЧ в цілому зберігається для кожного блоку ЦЗ: звісно кількісно залежність $\Delta\sigma_i$ від номеру і може відрізнятися від залежності для середніх значень, але якісно зберігається та ж сама концепція - найменших змін зазнають перше та декілька останніх СНЧ.

Висновок. В роботі визначено найбільш сприятливу для вбудови додаткової інформації при стеганоперетворенні, стійкому до атак проти вбудованого повідомлення, зону, яка є актуальною для будь-якого ЦЗ-контейнера (з втратами, без втрат) при довільній збурній дії: СНЧ σ_1, σ_{l-1}, σ_l блоків ЦЗ, отриманих шляхом стандартної розбивки. Отримані результати свідчать про те, що використання НСЗ є перспективним для розробки нових стеганометодів.

Перелік використаних джерел.

1. Кобозєва А.А., Мокріцький В.А., Батієне Л.Е.М., Бобок І.І. Удосконалення стеганографічного алгоритму, заснованого на SIGN-нечутливості сингулярних векторів блоків матриці зображення / Інформатика та математичні методи в моделюванні. 2021.- Том 7, №1-2, 19-28.

2. Менеджмент інформаційної безпеки : навчальний посібник для студентів спеціальності 125 Кібербезпека / О.Г. Корченко, М.Є. Шелест, С.В. Казмірчук, Ю.М. Ткач, Є.В. Іванченко. - Ніжин: ФОП Лук'яненко В.В. ТПК Орхідея, 2019. - 408 с.

3. Кобозєва А.А., Хорошко В.О. Аналіз інформаційної безпеки: монографія. К.: ДУІКТ, 2009. 251 с

4. Кобозєва А.А., Єнакієв Б.Г. Метод виявлення фотомонтажу на цифровому зображенні. Інформатика та математичні методи в моделюванні, 2024.- Том 14, № 1-2, 24-36.