УДК 004.056.5

НОВИЙ ПІДХІД ДО ПРОБЛЕМИ СТЕГАНОАНАЛІЗУ

А.А. Кобозєва

Одеський національний політехнічний університет,
просп. Шевченка, 1, Одеса, 65044, Україна; e-mail: alla_kobozeva@ukr.net

Робота присвячена створенню принципово нового підходу до проблеми рішення задач стеганоаналізу на основі адаптації розробленого автором раніше загального підходу до аналізу стану й технології функціонування інформаційних систем. Основним результатом є отримання якісних характерних рис сингулярних спектрів матриць зображень, що дозволяють відокремити контейнер від стеганоповідомлення, сформованого на основі цифрового зображення, збереженого у форматі з втратами.

Ключові слова: стеганоаналіз, контейнер, стеганоповідомлення, збурення, сингулярні числа

Вступ

Активізація в даний момент наукової діяльності в галузі стеганографії, де приховується сам факт існування таємного повідомлення, що викликана забороною шифрування на законодавчому рівні в багатьох країнах світу, привела до зростання можливостей використання отримуваних нових розробок різними терористичними структурами [1]. Завдяки цьому надзвичайно актуальним у даний момент є рішення питань, пов'язаних з підвищенням ефективності стеганоаналізу (СА) [2]. При всім різноманітті наявних стеганоаналітичних методів [1, 3-5] загального підходу до проблеми СА (у сенсі виявлення проведеної вбудови секретної, або додаткової, інформації (ДІ) у деякий об’єкт – основне повідомлення (ОП), або контейнер, чи висновку про відсутність такої вбудови) до теперішнього часу не існує.

Не обмежуючи спільності міркування, далі у якості ОП для спрощення викладу матеріалу розглядається цифрове зображення (ЦЗ). Процес вбудови ДІ в контейнер будемо називати стеганоперетворенням (СПР), а результат цієї вбудови – стеганоповідомленням (СП).

В [6-8] був розроблений новий загальний математичний підхід до аналізу стану й технології функціонування інформаційних систем (ЗПАІС), основна ідея якого полягає в наступному.

Довільна інформаційна система, зокрема, стеганографічна система (або окремо взятий контейнер, СП), формалізується у вигляді двовимірної $m \times n$-матриці F (скінченної множини таких матриць), що дозволяє звести аналіз стану системи до аналізу відповідних матриць. Не обмежуючи спільності міркувань [6], скрізь далі для представлення довільної інформаційної системи використовується одна матриця.

Результат будь-яких дій над системою у загальному випадку формально можна представити у вигляді:

$$\overline{F} = F + \Delta F, \qquad (1)$$

де $\Delta F = f(F)$ – збурення матриці F, при цьому ΔF є деякою функцією F, $\overline{F}$ – матриця перетвореної системи. Як набір формальних параметрів, що однозначно визначають і всебічно характеризують інформаційну систему, використовується множина син-

гулярних чисел (СНЧ) і сингулярних векторів (СНВ), отриманих за допомогою нормального сингулярного розкладання матриці [8], що відповідає розглянутій системі. Будь-яке перетворення інформаційної системи, у тому числі й СПР, представляється у вигляді сукупності збурень СНЧ і (або) СНВ, що дозволяє звести задачу аналізу процесу перетворення (а тому потенційно й СА) і підсумкового стану системи до аналізу цих збурень. Враховуючи це,

Метою автора є розробка нового загального теоретичного підходу до рішення проблеми СА шляхом адаптації ЗПАІС в галузь стеганографії, на основі якого згодом можуть бути побудовані ефективні стеганоаналітичні методи й алгоритми.

Основними математичними інструментами виступають теорія збурень і матричний аналіз.

При рішенні задач СА не може не враховуватися той факт, що в теперішній час зберігання й передача інформації по каналах телекомунікацій у зв'язку зі значним збільшенням її об'ємів здійснюється в стисненому виді. Тому як контейнери нижче розглядаються ЦЗ, збережені з втратами. У зв'язку з цим у рамках досягнення поставленої мети необхідно розв'язати наступні задачі:

1. Виявити якісні характерні риси формальних параметрів, що визначають ЦЗ, збережені у форматах з втратами, до й після СПР. Ці особливості згодом дозволять відокремити ОП від СП, сформованого на основі ЦЗ, збереженого у форматі з втратами. Складовими частинами рішення цієї задачі є наступні:
2. Визначити формальні параметри ЦЗ, збурення яких будуть однаковими, незалежно від області аналізу ЦЗ (просторової, частотної) – універсальні параметри (УП). Рішення даної задачі забезпечить універсальність розроблювальних згодом методів СА з погляду можливості їх ефективної роботи як у просторовій, так і в частотній області (залежно від зручності й специфіки конкретної задачі);
3. Визначити й обґрунтувати якісні відмінності УП ЦЗ, збереженого без втрат, від УП ЦЗ, коефіцієнти якого зазнали операцію квантування;
4. Виявити якісну залежність збурень УП матриць ЦЗ від об'єму інформації, що вбудовується (ОВІ);
5. Визначити й обґрунтувати якісні відмінності множини УП СП, сформованого на базі контейнера, збереженого у форматі з втратами, від множини УП контейнера.

Загальна схема стискання (з втратами) для ЦЗ складається із трьох основних кроків (після попередньої стандартної розбивки матриці зображення на блоки 8×8): відображення в частотну область, квантування отриманих коефіцієнтів, ентропійне кодування [7]. Тому, ніяк не обмежуючи область міркувань, нижче розглядається один з найпоширеніших форматів з втратами для ЦЗ – формат JPEG (заснований на дискретному косінусному перетворенні (ДКП), хоча це не має принципового значення).

Якісні характеристики універсальних параметрів матриць зображень при різних способах їх зберігання

Стан як ОП, так і СП, згідно з ЗПАІС визначається набором СНЧ і СНВ відповідних матриць. Говорячи про СПР, будемо припускати, що результуюче збурення матриці контейнера є малим. Таке обмеження викликане вимогою забезпечення надійності сприйняття СП, що є обов'язковим при роботі будь-якого стеганографічного методу [7].

Аналіз стану контейнера (СП) доцільно звести до аналізу тільки СНЧ, які відповідно до співвідношення [6]

$$\max_{1\le j\le n}\left|\sigma_j(F)-\sigma_j(F+\Delta F)\right|\le\left\|\Delta F\right\|_2, \qquad (2)$$

де $\sigma_j(F)$, $\sigma_j(F+\Delta F)$ – СНЧ матриць F, $F+\Delta F$ відповідно, $\|\Delta F\|_2$ – спектральна норма матриці збурення, є нечутливими до збурних дій (інакше – добре обумовленими), оскільки реакція СНВ на збурні дії різна, а в деяких випадках – об'єктивно непередбачена [6, 7]. Відмітимо, що вибір такого набору формальних параметрів розв'язує задачу 2, оскільки, як показано в [9], СНЧ (збурення СНЧ) матриці яскравості (просторова область) і матриці коефіцієнтів ДКП (частотна область) ЦЗ однакові. Таким чином, як набір УП виступає множина СНЧ матриці (матриць) ОП (СП).

Квантування коефіцієнтів, отриманих у частотній області, що відбувається в процесі стиску ЦЗ, є необоротною процедурою й приводить до деяких закономірних відмінностей СНЧ блоків зображень, збережених з втратами й без втрат. Для останніх у середньому менш, ніж 3% загального числа блоків (ЗЧБ) мають нульові СНЧ [6-8]. Даний факт не є випадковим. Ранг будь-якої матриці визначається кількістю її ненульових СНЧ [6]. Для довільного ЦЗ імовірність того, що рядки (стовпці) чергового блоку відповідної матриці виявляться лінійно залежними, невелика. Найчастіше це виникає у випадку колінеарності (або просто співпадіння) векторів, яка для реального ЦЗ, збереженого без втрат, зустрічається рідко, що й підтверджується обчислювальним експериментом.

Далі, говорячи про відновлення ЦЗ після стиску, будемо розглядати два можливі способи: часткове відновлення (ЧВ) після «повернення» матричних коефіцієнтів із частотної області в просторову не припускає їх округлення на відміну від повного відновлення (ПВ).

Нехай для зберігання ЦЗ використовується схема JPEG з ЧВ. В отриманих матриць у середньому більш, ніж 95% блоків від ЗЧБ містять нульові СНЧ [7]: після квантування й округлення багато з коефіцієнтів ДКП, що відповідають високим і середнім частотам, стануть нульовими, залишаючись нулями після ЧВ, що відповідно до [7] приведе до того, що нульовими виявляться найменші (а можливо й середні за значенням) СНЧ матриць блоків.

Нехай вхідне ЦЗ, що зазнало JPEG-стиску, відновлюється повністю. Ця дія збурить матрицю ЦЗ, отриману після ЧВ, змінить кількість нульових СНЧ у блоках. У тих блоках, де після ЧВ не було елементів, значно менших 0 або більших 255 (як показує обчислювальний експеримент, таких блоків більшість), збурення матриці буде малим, а оскільки СНЧ відповідно до (2) є нечутливими до збурних дій, у цьому випадку – до округлень, їх збурення також будуть незначними [6, 7]. Нульові СНЧ блоків матриці ЧВ ЦЗ хоч і стануть ненулями після ПВ, але їх значення будуть порівнянні з похибкою округлення й між собою, а швидкість зміни близька до нуля, що не є характерним для блоків ЦЗ, збереженого без втрат. Така якісна особливість, яка повністю підтверджуються результатами обчислювального експерименту, дає можливість розрізняти блоки ЦЗ, ПВ після стиску, і ЦЗ, збереженого у форматі, що не передбачає квантування коефіцієнтів, і розв'язує задачу 3. Для практичного використання цієї знайденої особливості необхідне встановлення порогу для значення швидкості зміни найменших СНЧ блоків ЦЗ, збережених у різних форматах.

Зіставлення властивостей СНЧ блоків зображень, збережених без втрат і в стисненому стані, дає можливість передбачити характер змін властивостей СНЧ JPEG-контейнера в ході СПР. Виходячи з вищесказаного, очікуваним результатом СПР є зменшення кількості нульових СНЧ в блоках, причому це зменшення буде тим більше, чим більшим буде ОВІ.

Аналіз результатів роботи стеганографічного методу модифікації найменшого значущого біта

Відповідно до (1), довільне СПР можна представити у вигляді аддитивної вбудови деякої інформації в просторовій області, при цьому F розглядається як матриця контейнера, а $\overline{F}$ – матриця СП. ДІ представляється у вигляді випадково сформованої бінарної послідовності.

Для рішення задач 4,5 розглянемо докладно роботу стеганографічного методу модифікації найменшого значущого біта (LSB) [2]. Даний метод обраний автором, головним чином, тому, що СПР тут, з урахуванням випадкового характеру формування стеганошляху [2] і відмінностей в об'ємах ДІ, може приводити до дуже незначних і випадкових збурень ΔF матриці контейнера. Можливість виявлення результатів такої збурної дії дасть для розроблювального автором стеганоаналітичного методу реальну перспективу його ефективної роботи з виявлення «слідів» застосування інших стеганографічних методів. Крім того, LSB є одним з найпоширеніших і широко використовуваних стеганографічних методів на сьогоднішній день. Результат його роботи представляється відповідно до (1), при цьому матриця збурення ΔF має елементи, значення яких належать множині $\{-1,0,1\}$. При вбудові ДІ надалі будемо враховувати лише ті її біти, які збурюють відповідні пікселі ОП. Так, будемо казати, що ОВІ становить, наприклад, 20%, якщо при вбудові цієї ДІ п'ята частина загального числа пікселів ОП зазнала збурень. Під час роботи LSB-метода, як правило [1, 3-5], вбудовується ДІ, для якої ОВІ приймає значення від 10% до 100%.

Проаналізуємо й оцінимо кількісно збурення СНЧ матриці (блоку матриці) JPEG-контейнера, що виникають внаслідок вбудови ДІ.

Нехай ОВІ дорівнює 10%. Позначимо F_B 8×8-матрицю довільного блоку контейнера. При зроблених вище припущеннях відповідний 8×8-блок ΔF_B матриці ΔF, яка є матрицею збурення для F_B, буде мати в середньому 6-7 ненульових значень, які дорівнюють 1 або (-1). Оцінка норми Фробеніуса $\|\Delta F_B\|_F$ не викликає труднощів й не вимагає додаткових обчислювальних витрат:

$$\|\Delta F_B\|_F \approx \sqrt{6} \approx 2.45 .$$

Однак оцінка (2) збурення СНЧ блоку контейнера припускає знання спектральної матричної норми $\|\Delta F_B\|_2$. Відповідно до [10]:

$$\|A\|_2 \le \|A\|_F ,$$

з урахуванням чого оцінка (2) для блоку F_B при ОВІ 10% здобуває вид:

$$\left|\sigma_j(F_B) - \sigma_j(F_B + \Delta F_B)\right| \le 2.45, \quad j = \overline{1,8} . \tag{3}$$

Оскільки найменші СНЧ блоків, як правило, мають значення, порівнянні з одиницею, виходячи з (3), можна було б сподіватися на явні кількісні відмінності в сингулярних спектрах блоків зображення до й після СПР, принаймні, у частині, що містить найменші СНЧ. Однак на практиці абсолютні похибки СНЧ блоків у переважній більшості випадків виявляються набагато менше зазначеної верхньої межі в (3), а тому її використання для розпізнавання ОП і СП викликає труднощі.

Незважаючи на те, що абсолютні похибки СНЧ – збурення, що виникають за рахунок СПР, для всіх СНЧ обмежені зверху однаково, для відносних похибок картина

буде принципово іншою. Для ілюстрації цього в таблиці 1 наведена частина типових результатів обчислювального експерименту для п'яти обраних випадково тестових JPEG-ЦЗ.

Таблиця 1.

Відносні похибки СНЧ блоків ЦЗ-контейнера, які виникають під час стеганоперетворення LSB-методом при ОВІ 10%

№ ЦЗ	Відносні похибки СНЧ блоків ЦЗ-контейнера при СПР LSB-методом для ОВІ 10% (%)							
	Номер СНЧ							
	1	2	3	4	5	6	7	8
1	0.0605	1.9531	1.4846	17.2256	5.2750	19.2736	137.1945	12.4750
2	0.0274	0.0831	0.1253	0.7436	2.4138	8.3467	11.3690	26.1539
3	0.0203	0.1300	1.3231	1.9764	9.2759	9.4315	35.1892	33.4940
4	0.2488	2.2687	20.5072	41.0460	26.3921	6.4525	10.8207	0.4913
5	0.1943	1.8031	1.4811	3.3200	49.6878	38.8003	76.4647	91.1596

Очевидно, що в результаті СПР найбільше «страждають» найменші СНЧ. До того ж для переважної більшості блоків ЦЗ абсолютне значення швидкості зміни двох найменших СНЧ після СПР зростає (частина типових результатів для ілюстрації сказаного наведена в таблиці 2). Це явище є теоретично очікуваним і пояснюється наступним чином. Після ПВ ЦЗ, як вже було відзначено вище, найменші СНЧ, що були нульовими після ЧВ, стають порівнянними між собою (і незначно відрізняються від 0), тобто швидкість їх зміни близька до нуля. Тому навіть мала збурна дія у таких блоках приведе до збільшення відокремленості [6] найменших СНЧ і, як наслідок, до зростання швидкості зміни. Кількісна картина для ЦЗ №4 у табл. 1, відповідає блокам, які вже після ЧВ не мали (або мали малу кількість) нульових СНЧ (такі блоки на зображенні відповідають областям, що містять контури), і ніяк не суперечить очікуваним результатам.

Таблиця 2.

Зміна швидкості зростання (спадання) найменших СНЧ у блоках ЦЗ-контейнера після стеганоперетворення з ОВІ 10%

№ ЦЗ	Кількість блоків (%), для яких швидкість зміни двох найменших СНЧ після СПР		№ ЦЗ	Кількість блоків (%), для яких швидкість зміни двох найменших СНЧ після СПР		№ ЦЗ	Кількість блоків (%), для яких швидкість зміни двох найменших СНЧ після СПР	
	Зменшується	зростає		Зменшується	зростає		Зменшується	зростає
1	35.3	64.7	4	28.8	71.1	7	22.1	77.9
2	40.6	59.3	5	24.7	75.2	8	31.5	68.5
3	30.0	69.9	6	24.0	76.0	9	38.0	62.0
Середнє значення (тестувалися більш 500 ЦЗ)								
Кількість блоків (%), для яких швидкість зміни двох найменших СНЧ після СПР зменшується				Кількість блоків (%), для яких швидкість зміни двох найменших СНЧ після СПР зростає				
32				68				

Збурення, які зазнають СНЧ при навіть дуже малому ОВІ, очевидно приведуть до зміни якісної картини наявності нульових СНЧ у блоках при стандартній розбивці матриці ЦЗ, про що вже говорилося вище. Оскільки виродженість блоків визначається лінійною залежністю стовпців (рядків) відповідних матриць, а вбудова ДІ, змінюючи значення елементів стовпців (рядків), з великою ймовірністю приведе до «руйнування» цієї лінійної залежності (а тому до зростання рангу матриці блоку СП), висувається гі-

потеза: кількість вироджених блоків JPEG-ОП після СПР повинна значно поменшатися, кількість невироджених блоків буде тим більше, чим більше ОВІ.

Для перевірки цієї гіпотези в середовищі Matlab був проведений обчислювальний експеримент, у якім тестувалося більш 500 різних ЦЗ, збережених у форматі JPEG. ДІ, як і раніше, представлялася у вигляді випадково сформованої бінарної послідовності. При цьому при СПР мінімально ОВІ склав 10%. Збереження СП проводилося у форматі без втрат (TIF, BMP). В результаті для 100% тестуємих ЦЗ було отримано строге монотонне зростання кількості блоків, що не містять нульових СНЧ, разом з зростанням ОВІ, до того ж, коли ОВІ був більше 60%, практично всі блоки матриці виявлялися невиродженими (у всіх тестуємих зображеннях більш 99% ЗЧБ), тобто СП, сформоване на базі JPEG-контейнера, якісно поводиться в цьому випадку, як ЦЗ, збережене без втрат.

В ході проведеного обчислювального експерименту були отримані наступні результати, корисні для використання в СА:

1) В результаті вбудови ДІ (навіть у випадку, коли ОВІ дорівнює 10%) матриця СП не містить блоків, які б мали 7, 8 нульових СНЧ. Разом з збільшенням ОВІ в матриць СП послідовно зникають блоки з великою кількістю нульових СНЧ (у табл. 3 наведений типовий приклад результату дослідження одного з тестуємих ЦЗ). Даний результат може бути використаний у процесі СА: якщо в досліджуваного ЦЗ матриця містить блоки з 7 або 8 нульовими СНЧ, то зображення не зазнало СПР, яке збурювало б не менш 10% загального числа пікселів.

2) Для матриць СП при будь-якому ОВІ число блоків з максимально можливою кількістю нульових СНЧ завжди менше числа блоків, у яких нульових СНЧ на одиницю менше максимально можливої кількості. Ця властивість часто не виконується для блоків матриць ЦЗ-контейнерів, що сигналізує про відсутність вбудованої ДІ й може бути використана при СА.

Таблиця 3.

Залежність кількості блоків різного рангу матриці зображення від ОВІ

		Кількість блоків матриці, що містять m нульових СНЧ, стосовно загального числа блоків (%)								
		$m=0$	$m=1$	$m=2$	$m=3$	$m=4$	$m=5$	$m=6$	$m=7$	$m=8$
Подане ЦЗ		89.36	4.21	1.71	1.43	1.06	0.95	0.57	0.59	0.12
СП з ОВІ рівним k %	$k=10$	93.40	3.55	1.88	0.82	0.30	0.05	0	0	0
	$k=20$	95.45	3.42	0.91	0.21	0.01	0	0	0	0
	$k=35$	98.24	1.63	0.13	0	0	0	0	0	0
	$k=65$	99.78	0.22	0	0	0	0	0	0	0

Висновки

В роботі шляхом адаптації ЗПАІС в галузь стеганографії

- розроблені теоретичні основи загального стеганоаналітичного підходу, заснованого на зведенні процесу СА до аналізу СНЧ матриць блоків ЦЗ;
- отримані якісні відмінності сингулярних спектрів матриць блоків зображень, збережених у різних форматах;
- отримані основні якісні відмінності сингулярних спектрів блоків СП, сформованих на основі JPEG-контейнерів, з різними ОВІ від блоків ОП.

Отримані результати говорять про перспективність запропонованого нового стеганоаналітичного підходу. Визначення кількісних порогових значень для знайдених якісних відмінностей дозволять розробити універсальний метод СА, що є метою подальшої роботи автора.

Список літератури

1. Gul G. SVD-Based Universal Spatial Domain Image Steganalysis / G. Gul, F. Kurugollu // IEEE Transactions on Information Forensics and Security. – 2010. – Vol.5, No.2. – PP. 349-353.
2. Грибунин В.Г. Цифровая стеганография / В.Г. Грибунин, И.Н. Оков, И.В. Туринцев. – М.: Солон-Пресс, 2002. – 272 с.
3. Gul G. Steganalytic features for JPEG compression based perturbed quantization / G. Gul, A.E. Dirik, and I. Avcibas // IEEE Signal Processing Letters. – 2007. – Vol.14, No.3. – PP. 205-208.
4. Lyu S. Detecting hidden messages using higher-order statistics and support vector machines / S. Lyu, H. Farid // Lecture Notes in Computer Science. – New York: Springer-Verlag, 2002. – Vol.2578. – PP. 340-354.
5. Avcibas I. Image steganalysis with binary similarity measures / I. Avcibas, M. Kharrazi, N. Memon, and B. Sankur // EURASIP Journal on Applied Signal Processing. – 2005. – Vol.2005, No.17. – PP. 2749-2757.
6. Кобозева А.А. Анализ информационной безопасности / А.А. Кобозева, В.А. Хорошко. – К.: Изд. ГУИКТ, 2009. – 251 с.
7. Кобозєва А.А. Аналіз захищеності інформаційних систем / А.А. Кобозєва, І.О. Мачалін, В.О. Хорошко. – К.: Вид. ДУІКТ, 2010. – 316 с.
8. Кобозева А.А. Общий подход к анализу состояния информационных объектов, основанный на теории возмущений / Вісник Східноукраїнського національного університету ім. В. Даля. – 2008. – №8(126), ч.1. – С. 72-81.
9. Кобозева А.А. Повышение эффективности метода обнаружения фальсификации цифрового изображения, основанного на анализе сингулярных чисел матрицы / А.А. Кобозева, Е.А. Трифонова // Труды Одесского политехнического университета. – 2008. – №1(29). – С. 183-190.
10. Кобозєва А.А. Спектральна матрична норма як основа різницевого показника візуального викривлення цифрового зображення / Інформатика та математичні методи в моделюванні. – 2011. – Т.1, №1. – С. 5-11.

А.А. Кобозева

НОВЫЙ ПОДХОД К ПРОБЛЕМЕ СТЕГАНОАНАЛИЗА

Работа посвящена созданию принципиально нового подхода к проблеме решения задач стеганоанализа на основе адаптации разработанного автором ранее общего подхода к анализу состояния и технологии функционирования информационных систем. Основным результатом является получение качественных характерных особенностей сингулярных спектров матриц изображений, позволяющих отделить контейнер от стеганосообщения, сформированного на основе цифрового изображения, хранимого в формате с потерями.

Ключевые слова: стеганоанализ, контейнер, стеганосообщение, возмущение, сингулярные числа

A. Kobozeva

NEW APPROACH TO STEGANALYSIS

The article is devoted to creation of a fundamentally new approach to solving problems of steganalysis based on the adaptation of a common approach to the analysis of the state and functioning of information systems developed by the author. The main result is getting qualitative characteristics of singular matrix spectra of images that allow to distinguish the cover from stego-message formed on the basis of digital image stored in a lossy format.

Keywords: steganalysis, cover, stego message, disturbance, singular values