DOI 10.15276/imms.v11.no3.216
УДК 004.056.5

Informatics and Mathematical Methods in Simulation
Vol. 11 (2021), No. 3, pp. 216-226

МЕТОД РОЗВ'ЯЗКУ ЗАДАЧІ ПРО ВИБІР КОНТЕЙНЕРА, ЩО ЗАБЕЗПЕЧУЄ МАЛУ ЧУТЛИВІСТЬ СТЕГАНОПОВІДОМЛЕННЯ ДО ЗБУРНИХ ДІЙ

О.Ю. Надвоцький, А.А. Кобозєва

Національний університет «Одеська політехніка»
1, пр.Шевченка, Одеса, 65044, e-mail: alla_kobozeva@ukr.net

З розвитком інформаційних технологій зростають вимоги до стеганографічних систем. Сьогодні стеганосистема повинна протистояти стеганоаналітичним атакам, що використовують найсучасніші математичні базиси, атакам проти вбудованого повідомлення, які просто і якісно реалізуються в будь-якому сучасному програмному середовищі, забезпечувати значну пропускну спроможність при організації прихованого каналу зв'язку, тощо. Для забезпечення цих вимог потрібно використовувати всі можливі засоби. Одним із способів, що сприяє забезпеченню певної вимоги, є вибір контейнера, в якості якого в роботі розглядається цифрове зображення. Вибір контейнера відбувається з метою забезпечення кращих характеристик стеганоповідомлення в певному сенсі. Метою роботи є забезпечення можливості вибору цифрового зображення-контейнера, що породжує стеганоповідомлення, нечутливе до збурних дій. В роботі отримані наступні результати: теоретично обгрунтовано та практично підтверджено доцільність використання збурень власних векторів матриці контейнера як показників захищеності вбудованої в контейнер додаткової інформації; запропонована кількісна оцінка збурення власного вектору матриці цифрового зображення в результаті стеганоперетворення, яка дає змогу для відокремлення чутливого власного вектора від нечутливого, адекватно відображає збурення вектора незалежно від величини кута повороту; запропонована умова вибору захищених від збурної дії власних векторів, що враховує індивідуальні характеристики контейнера; запропонована формула для розрахунку обсягу захищеної додаткової інформації; розроблений метод вибору контейнера, що забезпечує малу чутливість стеганоповідомлення до збурних дій з наявної множини потенційних контейнерів.

Ключові слова: стеганосистема, стеганоповідомлення, вибір контейнера, цифрове зображення, атака проти вбудованого повідомлення, чутливість стеганоповідомлення до збурних дій, власне значення, власний вектор.

Вступ

Стеганографія сьогодні є одним з найпотужніших засобів захисту інформації, яка передбачає приховування самого факту наявності секретної інформації [1,2]. З розвитком інформаційних технологій зростають вимоги до стеганографічних систем. Сьогодні стеганосистема повинна протистояти стеганоаналітичним атакам, що використовують найсучасніші математичні базиси, атакам проти вбудованого повідомлення, які просто і якісно реалізуються в будь-якому сучасному програмному середовищі, забезпечувати значну пропускну спроможність при організації прихованого каналу зв'язку, надійність сприйняття формованого стеганоповідомлення, малу обчислювальну складність використовуваних стеганоалгоритмів для роботи в режимі реального часу тощо.

Переважна кількість сучасних стеганоалгоритмів розраховані на застосування випадкового контейнера, що взагалі вважається їх позитивною характеристикою, але, враховуючи значні труднощі для забезпечення згаданих вище вимог до стеганосистеми, не можна нехтувати таким додатковим джерелом, як вибір контейнера, в якості якого в роботі розглядається цифрове зображення (ЦЗ). В відкритих джерелах питання вибору контейнеру є маловивченим, одною з причин чого є обов'язково присутня значна обчислювальна складність такої задачі, оскільки передбачає, як правило, прямий перебір всіх можливих варіантів (ЦЗ-контейнерів) [3]. Але очевидно, що тут можливий деякий компроміс між

забезпеченням певної вимоги до стеганосистеми (стеганоповідомлення) та обчислювальною складністю (кількістю потенційно можливих контейнерів), досягнення якого буде залежити від ступеня критичності кожної з цих складових в конкретних умовах функціонування стеганосистеми. Таким чином, задача вибору контейнеру з метою забезпечення кращих характеристик стеганоповідомлення в певному сенсі є важливою та актуальною задачею сучасної стеганографії. Взагалі така задача може розв'язуватися з урахуванням різних критеріїв. Так вибір контейнера є актуальним в умовах організації прихованого каналу зв'язку при забезпеченні стійкості стеганосистеми до стеганоаналізу, зокрема при використанні LSB-методу [4], де оригінальне зображення принципово можна підібрати так, щоб воно вже містило в собі необхідну додаткову інформацію з урахуванням стеганошляху та секретного ключа, що зробить будь-який стеганоаналітичний метод неспроможним тут виявити факт обміну даними [3]. Задача вибору контейнера (локалізації частини контейнера, яка використовується для стеганоперетворення) може ставити за мету забезпечення, по можливості, найменшого спотворення в результаті стеганоперетворення обраним алгоритмом [5] та ін.

Як вже зазначалося вище, одною з основних вимог до стеганосистеми є вимога стійкості до атак проти вбудованого повідомлення, тобто атак, що збурюють матрицю стеганоповідомлення. Рівень розвитку графічних редакторів на сьогодні є настільки високим, що змінення ЦЗ з їх допомогою стає легким, простим, непомітним, що призводить до значного полегшення проведення атак проти вбудованого повідомлення [3], серед яких накладання різноманітних шумів, фільтрація, розмиття, стиск з втратами, геометричні атаки. В таких умовах навіть використання стійких до збурних дій стеганоалгоритмів часто не забезпечує бажану ефективність декодування додаткової інформації (ДІ), підвищення якої можливо шляхом вибору контейнера (зі скінченної множини потенційно можливих), який би забезпечував найменшу чутливість стеганоповідомлення до збурних дій. В [6] розглядалося питання розв'язку задачі вибору контейнера з наявної множини ЦЗ для забезпечення, по можливості, малої чутливості формованого стеганоповідомлення до атак проти вбудованого повідомлення, запропонований відповідний метод. Значною перевагою згаданого методу є відсутність обмежень на область його застосування як в сенсі використовуваних стеганографічних алгоритмів, так і в сенсі конкретики атак проти вбудованого повідомлення, що є результатом використання в якості математичного базису загального підходу до аналізу стану й технології функціонування інформаційних систем, заснованого на теорії збурень та матричному аналізі [7], тому саме цій роботі приділена основна увага в даній статті. В [6] було введено поняття додаткової інформації, захищеної від збурення (ЗІ), формальним представленням якого є матриця E з розмірами, відповідними розмірам зображення, що піддається збурній дії. Обсяг ЗІ обчислювався з урахуванням збурень захищених власних векторів (ВВ) і абсолютних відокремленостей відповідних власних значень (ВЗ) матриці ЦЗ [7], в якості кількісного показника збурення захищеного ВВ з урахуванням його нормованості розглядався синус кута його повороту в результаті стеганоперетворення (не враховуючи можливість того, що кут повороту ВВ на практиці може бути не обов'язково гострим), а захищені власні вектори визначалися з урахуванням абсолютної відокремленості відповідного власного значення, при цьому ця абсолютна відокремленість виступала ще як ваговий коефіцієнт при розрахунках обсягу ЗІ, тобто враховувалася двічі, доцільність чого не була достатньо обгрунтована. Вищенаведене залишає актуальною задачу вибору ЦЗ-контейнера, що забезпечує для відповідного стеганоповідомлення нечутливість до збурних дій, яка розглядається в даній роботі, удосконалення процесу цього вибору.

Мета статті й постановка досліджень

Метою роботи є забезпечення можливості вибору цифрового зображення-контейнера, що породжує стеганоповідомлення, нечутливе до збурних дій, шляхом розробки

відповідного методу на основі загального підходу до аналізу стану й технології функціонування інформаційних систем [7].

Для досягнення поставленої мети в роботі розв'язуються наступні *задачі*:

1. Обгрунтувати вибір формальних параметрів цифрового зображення, їх кількісні характеристики, збурення яких можуть використовуватися як показники захищеності вбудованої в контейнер ДІ;
2. Обгрунтувати спосіб кількісної оцінки збурення ВВ в результаті стеганоперетворення;
3. Визначити поняття ВВ, захищеного від збурної дії;
4. Отримати кількісну оцінку для обсягу додаткової інформації, захищеної від збурної дії;
5. Розробити метод вибору контейнера, що забезпечує малу чутливість стеганоповідомлення до збурних дій.

Основна частина

Нехай формальним представлення ЦЗ-контейнера є одна $n \times n$-матриця F. По аналогії з [6] будемо вважати, що в процесі стеганоперетворення було проведено перетворення матриці контейнера, що забезпечує її симетричність, тобто: $F = F^T$. Симетричність матриці забезпечує наявність для неї нормального спектрального розкладання [6]:

$$F = U \Lambda U^T, \tag{1}$$

де $\Lambda = diag(\lambda_1, \lambda_2, ..., \lambda_n)$ - діагональна матриця власних значень F, U – ортогональна матриця, тобто $U^T U = I$, де I – одинична $n \times n$-матриця, стовпці $u_1, u_2, ..., u_n$ матриці U – ортонормовані лексикографічно додатні ВВ F.

Відповідно до загального підходу до аналізу стану й технології функціонування інформаційних систем [7] будь-яке перетворення симетричної матриці F, зокрема стеганоперетворення (незалежно від конкретного стеганоалгоритму), може бути формально представлено у вигляді сукупності збурень власних значень та/або власних векторів матриці, які однозначно визначаються її нормальним спектральним розкладанням. Таким чином, сукупність таких збурень може розглядатися як формальне представлення додаткової інформації, вбудованої в контейнер з матрицею F, результатом «розподілу» ДІ по ВЗ і ВВ в області нормального спектрального розкладання. В [6] для оцінки обсягу ДІ, захищеної від збурної дії E, враховувалися як характеристики ВВ, так і ВЗ, зокрема, їх абсолютних відокремленостей, що для ВЗ λ_i визначається відповідно до формули:

$$gap_{abs}(i, F) = \min_{i \neq j} \left\| \lambda_j \right| - \left| \lambda_i \right\|.$$

Однак ВЗ симетричної матриці F є нечутливими [8] до збурних дій згідно з формулою:

$$\max_{1 \le j \le n} \left| \lambda_j(F) - \lambda_j(F + E) \right| \le \|E\|_2 \tag{2}$$

де E – $n \times n$-матриця збурення, $\|\cdot\|_2$ - спектральна матрична норма [8], $\lambda_j(F)$, $\lambda_j(F + E)$ - ВЗ матриць F, $F+E$ відповідно, а тому їх абсолютна відокремленість майже не змінюється при вбудові ДІ, оскільки збурна дія, що є формальним представленням стеганоперетворення, є незначною, бо інакше таке стеганоперетворення не гарантувало б забезпечення надійності сприйняття стеганоповідомлення. Отже, збурення ВЗ, їх абсолютних відокремленостей практично «не несуть в собі» вбудованої інформації. Збурення ВЗ не залежать від розподілу ДІ по (збуренням) ВВ матриці контейнера. Крім того, оскільки ВЗ є нечутливими до збурних дій, то вони принципово не можуть характеризувати чутливість до збурних дій формованого

стеганоповідомлення, яке може бути як чутливим, так і нечутливим, чого не можна сказати про ВВ, враховуючи, що чутливість ВВ u_i, який відповідає ВЗ λ_i, в межах матриці F визначається відповідно до співвідношень [8]:

$$\frac{1}{2}sin\theta_i \le \frac{\|E\|_2}{gap_{abs}(i,F)},\ \frac{1}{2}sin\theta_i \le \frac{\|E\|_2}{gap_{abs}(i,F+E)}, \qquad (3)$$

де θ_i — кут між u_i і $\bar{u}_i$, $\bar{u}_i$ — нормований збурений ВВ u_i. Врахування абсолютної відокремленості ВЗ як вагового коефіцієнта при розрахунку обсягу захищеної інформації в [6] є не тільки недоцільним, але й шкідливим. Дійсно, $\|E\|_2$ - це верхня межа збурень ВЗ в результаті стеганоперетворення відповідно з (2), але конкретні збурення, що зазнаються різними ВЗ в результаті вбудови ДІ є різними, на практиці залежать не від обсягу ДІ, а від величини модуля ВЗ (найбільше збурюються найбільші за модулем ВЗ), відмінності в збуреннях не залежать від особистостей стеганоперетворення, не характеризують процес вбудови ДІ.

Такий теоретичний висновок знайшов своє практичне підтвердження: експериментально встановлено, що на величину обсягу захищеної інформації впливає величина відхилення саме власних векторів, а не абсолютної відокремленості відповідних ВЗ (в ході експерименту відбувалося поступове зниження вкладу абсолютної відокремленості власного значення, тобто вектору ваги під час побудови вектору розподілу додаткової інформації по власним векторам стеганоповідомлення).

Таким чином, для обчислення обсягу ЗІ доцільним є врахування збурень лише ВВ матриці ЦЗ-контейнера. Але кількісна оцінка такого збурення може робитися різними способами. В [6] показником збурення ВВ u_i виступає $sin\theta_i$ (див.(3)), але така оцінка не є адекватною з урахуванням можливості на практиці значного збурення ВВ, аж до розгорнутого результуючого кута повороту. Взагалі на практиці можлива ситуація, коли два різні ВВ u_1 і u_2 після свого збурення можуть мати одне й те саме значення функції синуса для відповідних кутів повороту, при цьому один з цих векторів u_1 є нечутливим до збурних дій, а інший u_2 навпаки (рис.1).

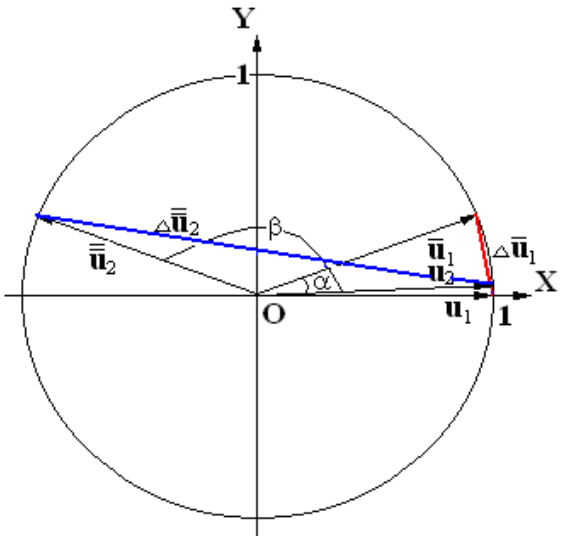

Рис. 1. Відмінність між збуреннями ВВ u_1 і u_2 при $sin\alpha = sin\beta$

Така ситуація є неприйнятною, оскільки для адекватної кількісної оцінки обсягу додаткової інформації, захищеної від збурної дії Е, кількісна оцінка збуреня ВВ повинна

відображати його чутливість/нечутливість до збурних дій. Для цього в роботі запропоновано використання в якості кількісної оцінки збурення ВВ евклідової норми вектору різниці між оригінальним і збуреним ВВ (рис.1): більшому збуренню вектора (більшому куту між поданим і збуреним векторами) відповідає більше значення норми вектора різниці і навпаки, що витікає з відомих властивостей довжин сторін довільного трикутника.

В [6] вводиться поняття захищеного ВВ від збурної дії E, що передбачає необхідність визначення ВЗ з достатньою абсолютною відокремленістю по відношенню до збурення E, а оцінка для цього збурення обирається у відповідності з наступним:

1. Для j=1,2,…,k, де k — кількість наявних контейнерів:

1.1. Побудувати $\overline{F}_j = E(F_j)$, де F_j — матриця j-го контейнера, $\overline{F}_j$ — матриця j-го контейнера після накладання деякого очікуваного збурення $E(F)$;

1.2. Знайти $E_j = F_j - \overline{F}_j$.

2. Знайти середнє значення показника збурення $\|E\| = \frac{1}{k}\sum_{j=1}^{k}\|E_j\|_2$.

Але кожне із зображень є унікальним за характеристиками матриці. Використання у якості кількісної оцінки збурної дії E, за якою обираються захищені власні вектори, усередненого значення норм $\|E_j\|_2$ з серії проведених попередньо експериментів приводе до «прив'язки» $\|E\|$ до характеристик тих зображень, на яких було виконано розрахунок. Це вводить додаткові умови щодо того, які саме зображення необхідно використовувати для обчислення розрахункового значення збурення, а також не враховує особливості безпосередньо тих контейнерів, що розглядаються, замінюючи критично важливу характеристику лише усередненим значенням. Обчислюючи середнє значення $\|E\|$ для певної кількості зображень, немає ніякої гарантії в тому, що $\|E\|$ однакового добре може бути застосовано для будь-яких інших зображень, а також для кожного конкретного зображення навіть з цієї ж множини.

З урахуванням цього в роботі пропонується метрика, яка нижче позначається $Capacity(j)$, що не розраховується попередньо для певної вибірки зображень, а враховує особливості безпосередньо такого контейнера F_j, об'єм захищеної інформації якого досліджується. Для її отримання після вбудовування додаткової інформації стеганоповідомленню необхідно надати очікуване збурення, та для результуючої матриці знайти ортонормовані лексикографічно додатні власні вектори (за допомогою нормального спектрального розкладання). Умовою виділення елементів відповідних векторів розподілу додаткової інформації по власним векторам стеганоповідомлення є умова того, чи норма вектору різниці між початковим власним вектором контейнера і власним вектором після накладання збурення на стеганоповідомлення менша, ніж деяке K, що є параметром розробленого методу і визначається експериментально (див.(4)). В результаті обчислювального експерименту встановлено, що найбільш стабільні та очікувані результати відповідно до кількості захищеної інформації та кількості відновленої інформації при декодуванні дає K=0.005 (рис.2).

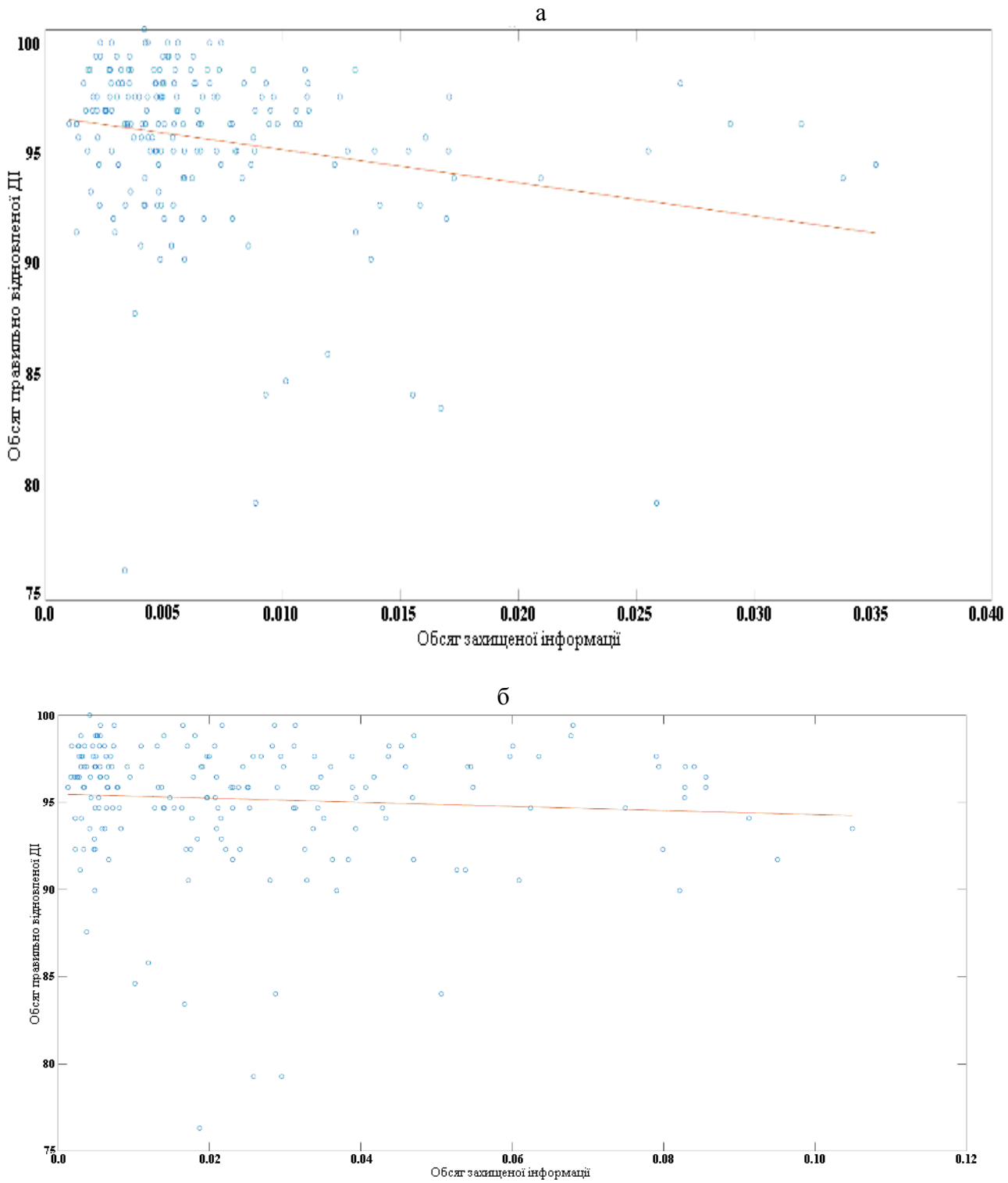

Рис. 2а. Співвідношення між обсягом захищеної інформації та відновленої при декодуванні додаткової інформації (%) при різних значеннях K: а – K = 0.01; б – K = 0.001

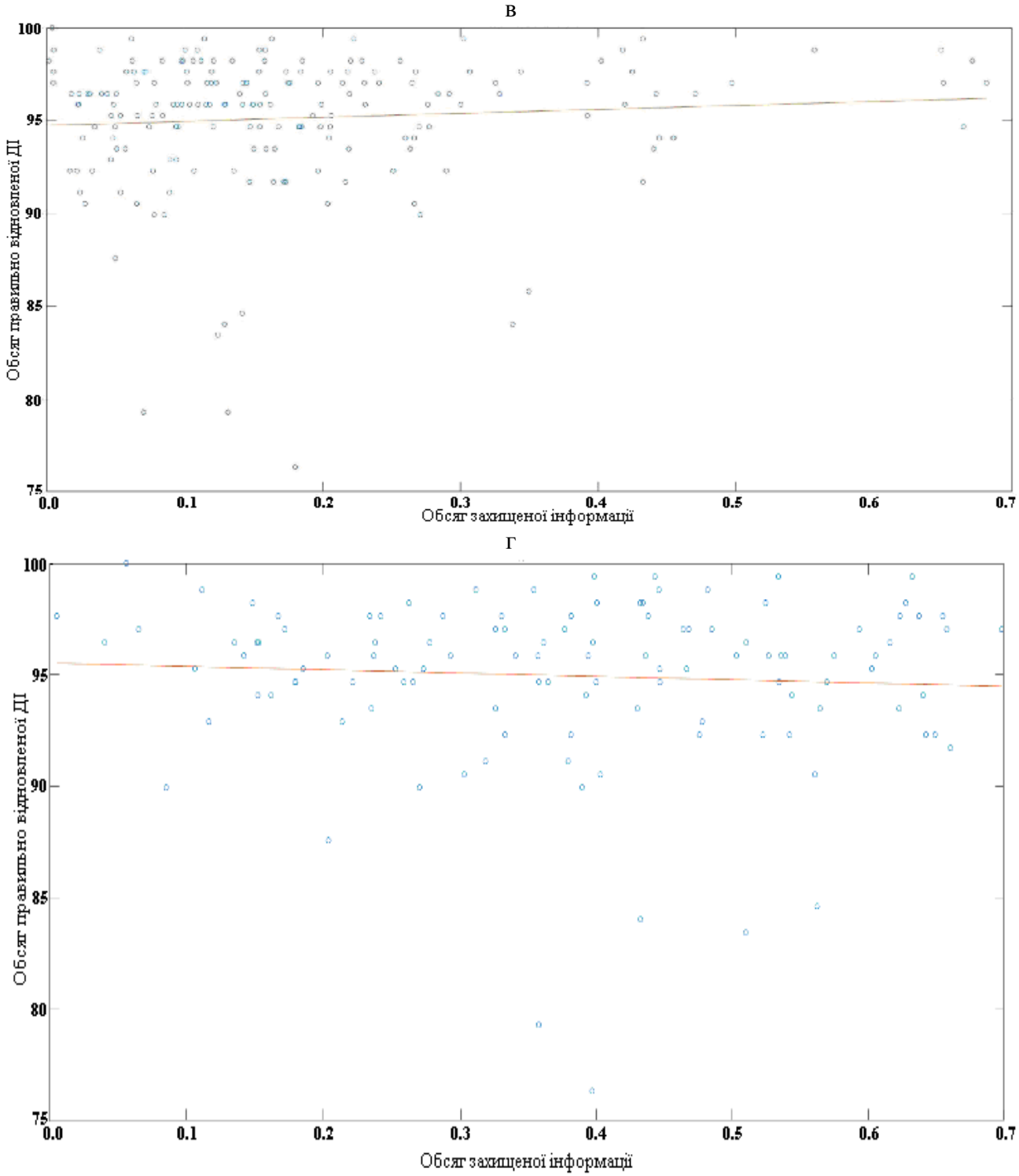

Рис. 2б. Співвідношення між обсягом захищеної інформації та відновленої при декодуванні додаткової інформації (%) при різних значеннях K: в – K = 0.002; г – K = 0.005

При проведенні всіх обчислювальних експериментів для визначеності використовувався стеганометод Коха і Жао з параметром P=30 [9] (вбудова ДІ проводилася шляхом зміни значень (4,5) - і (5,4) - коефіцієнтів дискретного косинусного перетворення 8×8-блоків матриці контейнера), що ніяк не обмежує спільності міркувань, враховуючи універсальність використовуваного загального підходу до аналізу стану й технології функціонування інформаційних систем. Цей вибір був зроблений з урахуванням: наявності стійкості методу Коха і Жао до атак проти вбудованого повідомлення, його загальної поширеності, відсутності обмежень на область застосування, наявності гнучких параметрів

вбудовування інформації для управління ступенем внесення змін до контейнеру в результаті стеганоперетворення.

Критеріями вибору збурних дій для моделювання в роботі процесу атак проти вбудованого повідомлення були: наявність можливості для атакуючої сторони забезпечення надійності сприйняття збуреного стеганоповідомлення, оскільки інакше неавторизоване втручання буде одразу виявленим, в чому порушник очевидно є незацікавленим; поширеність конкретних атак на практиці.

Однією із найбільш поширених атак проти вбудованого повідомлення є атака стиском. Враховуючи величезні обсяги інформації, що передається по каналах зв'язку, ця інформація зберігається, як правило, у форматах з втратами, тому атака стиском не привертає уваги, але вносить зміни у зображення при будь-якому коефіцієнті стиску. Як атака стиском в роботі використовується збереження ЦЗ в форматі Jpeg.

Серед атак проти вбудованого повідомлення поширеними залишаються атаки накладанням різноманітних шумів. Це пов'язано з тим, що сам результат вбудови ДІ в стеганографії часто трактується як накладання шуму, зокрема, при застосуванні LSB-методу. Ці атаки є такими, що важко виявляються, особливо, коли параметри шуму обрані так, що величина збурної дії є незначною, але очевидно призводять до змін в стеганоповідомленні. При моделюванні атак проти вбудованого повідомлення в роботі використовувалися: гаусівський шум з нульовим математичним очікуванням; мультиплікативний шум з різними значеннями дисперсії.

З урахуванням вищенаведеного основні кроки методу вибору контейнера, що забезпечує нечутливе стеганоповідомлення, наступні:

Крок 1. Нехай F_1, F_2, …, F_k - матриці наявних потенційних ЦЗ-контейнерів.

Для $j = 1,2,...,k$, де k — кількість контейнерів, робити:

1.1. Побудувати стеганоповідомлення з матрицею $F_j^{(S)}$, що відповідає контейнеру F_j;

1.2. Піддати стеганоповідомлення $F_j^{(S)}$ очікуваній збурній дії $E(F)$. Результат – ЦЗ з матрицею $\overline{F}_j^{(S)}$;

1.3. Побудувати нормальні спектральні розкладання (1) для F_j, $F_j^{(S)}$, $\overline{F}_j^{(S)}$:

$$F_j = U_j \Lambda_j U_j^T;\ F_j^{(S)} = U_j^{(S)} \Lambda_j^{(S)} \left(U_j^{(S)}\right)^T;\ \overline{F}_j^{(S)} = \overline{U}_j^{(S)} \overline{\Lambda}_j^{(S)} \left(\overline{U}_j^{(S)}\right)^T;$$

1.4. Побудувати вектор $Deviation_j$:

1.4.1. $\overline{Deviation}_j(i) = \left\| U_j(i) - U_j^{(S)}(i) \right\|$,

де $U_j(i), U_j^{(S)}(i)$ - i-ий стовпець матриці $U_j, U_j^{(S)}$ відповідно; i=1, 2,…, n, де n — кількість власних векторів F_j;

1.4.2. $Deviation_j(i) = \dfrac{\overline{Deviation}_j(i)}{\left\| \overline{Deviation}_j \right\|}$, i=1, 2,…, n.

1.5. Побудувати вектор $Distribution_j$ розподілу додаткової інформації по власних векторах стеганоповідомлення:

1.5.1. $\overline{Distribution}_j(i) = Deviation_j(i)$;

1.5.2. $Distribution_j(i) = \dfrac{\overline{Distribution}_j(i)}{\sum_{i=1}^{n} \overline{Distribution}_j(i)} \cdot 100\%,\ i = 1,2,...,n$,

де n — кількість власних векторів F_j;

1.6. Визначення об'єму захищеної від збурної дії $E(F)$ інформації в стеганоповідомленні:

$$Capacity(j) = \begin{cases} \sum_{i=1}^{n} Distribution_j(i), \text{ якщо } \left\| U_j(i) - \overline{U}_j^{(S)}(i) \right\| < K, \\ 0, \quad \text{інакше} \end{cases} \qquad (4)$$

де K – параметр.

Крок 2. Визначення контейнера з найбільшим обсягом захищеної від збурної дії $E(F)$ інформації:

$$m = arg\max_j Capacity(j).$$

F_m — шуканий контейнер.

Зауваження 1. Кожний пункт кроку 1 запропонованого методу використовує лише конкретний контейнер, який розглядається, без суміжних зв'язків з іншими контейнерами, а тому може виконуватися одночасно для кількох контейнерів, використовуючи технології розпаралелювання або навіть кластеризації.

Зауваження 2. Запропонований метод не може однозначно передбачити показник (відсоток) відновлення додаткової інформації після накладання на стеганоповідомлення збурень, що наочно підтверджує рис.2(г): беручи у якості зрізу невеликі значення обсягу захищеної інформації, наприклад, 0.07, легко переконатися у тому, що для різних зображень можливе як абсолютне (100%) відновлення ДІ, так і взагалі неефективне декодування – близько 75%. Аналізуючи ситуацію при збільшенні обсягу захищеної інформації, стає очевидним, що чим більшим є обсяг захищеної інформації, тим більш стабільним є результат ефективного відновлення додаткової інформації із стеганоповідомлення після атаки проти вбудованого повідомлення. При значному обсязі захищеної ДІ отримане стеганоповідомлення є нечутливим до збурних дій.

Висновки

В роботі розв'язано важливу науково-практичну задачу забезпечення можливості вибору цифрового зображення-контейнера, що породжує стеганоповідомлення, нечутливе до збурних дій.

Отримані наступні результати:

1. Теоретично обгрунтовано та практично підтверджено неінформативність та шкідливість урахування при розрахунку обсягу захищеної в стеганоповідомленні додаткової інформації абсолютних відокремленостей власних значень матриці цифрового зображення, як це робиться в [6], що привело до усунення власних значень з множини параметрів, збурення яких враховується при кількісній оцінці захищеності стеганоповідомлення;
2. Запропонована кількісна оцінка збурення власного вектору матриці цифрового зображення в результаті стеганоперетворення, яка, на відміну від [6], дає змогу для відокремлення чутливого власного вектора від нечутливого, адекватно відображає

збурення вектора незалежно від величини кута повороту, що дало можливість для удосконалення формули для розрахунку обсягу захищеної додаткової інформації;
3. Запропонована умова вибору захищених власних векторів, що враховує індивідуальні характеристики контейнера, замість попереднього обчислення над певною наперед визначеною, а отже небездоганною вибіркою зображень, що дозволяє враховувати особливості кожного ЦЗ-контейнера;
4. Розроблений метод вибору контейнера, що забезпечує малу чутливість стеганоповідомлення до збурних дій з наявної множини потенційних ЦЗ-контейнерів.

Список літератури

1. Goel M. Review on Steganography Techniques. *Journal of Emerging Technologies and Innovative Research*. 2019. V.6(2). P.148-153.
2. Subramanian N., Elharrouss O., Al-Maadeed S., Bouridane A. Image Steganography: A Review of the Recent Advances. *IEEE Access.* 2021. V.9. P.23409-23423.
3. Аграновский А.В. Стеганография, цифровые водяные знаки и стеганоанализ. М.: Вузовская книга, 2009. 220 с.
4. Amarendra K., Mandhala V.N., Gupta B.C., Sudheshna G.G., Anusha V.V. Image Steganography Using LSB. *International Journal of Scientific & Technology Research*. 2019. V.8 (12). P. 906-909.
5. Кушниренко Н.И., Кирмичиева А.С., Яковенко А.А., Калашников Н.В., Лозан А.Э. Метод встраивания информации в цифровые изображения jpeg, минимизирующий психовизуальные искажения для малых объемов встроенной информации. *Інформатика та математичні методи в моделюванні.* 2018. Т.8, № 4. С. 313-323.
6. Кобозева А.А., Нариманова Е.В. Оценка чувствительности стегосообщений к возмущающим воздействиям. *Системні дослідження та інформаційні технології*. 2008. No 3. С. 52-65.
7. Кобозева А.А., Хорошко В.А. Анализ информационной безопасности: монография. К.: ГУИКТ, 2009. 251 с.
8. Деммель Д. Вычислительная линейная алгебра: теория и приложения. М.: Мир, 2001. 430 с.
9. Конахович Г.Ф., Пузыренко А.Ю. Компьютерная стеганография: теория и практика. Киев: МК-Пресс, 2006. 288 с.

A COVER IMAGE SELECTION METHOD PROVIDING STEGO-OBJECT ROBUSTNESS TO VARIOUS IMAGE PROCESSING ATTACKS

A.Yu. Nadvotskiy, A.A. Kobozeva

National Odessa Polytechnic University
1, Shevchenko Ave., Odessa, 65044, Ukraine, e-mail: alla_kobozeva@ukr.net

With the development of information technology, the requirements for steganography systems are growing. Today, the steganography system must resist steganalysis attacks using the latest mathematical bases, attacks and countermeasures, which can be easily and efficiently implemented in any modern software environment, providing significant bandwidth when organizing a secret communication channel, and so on. All possible means must be used to meet these requirements. One of the ways to meet a certain requirement is to choose the cover as which the digital image is considered in the study. The cover deciding is to be done in order to provide the best characteristics of stego-object in a sense. The aim of the study is to provide the possibility to choose a cover image, which results in the stego-object that is robust to various image processing attacks. The following results are obtained in the study: the expediency of using perturbations of eigenvectors of the cover image matrix as indicators of security of secret message embedded into the cover is theoretically substantiated and practically confirmed; the quantitative estimation of the perturbation of the eigenvector matrix of the digital image as a result of embedding is proposed, which allows separating the sensitive eigenvector from the insensitive one, adequately reflects the perturbation of the eigenvector regardless of the angle of rotation; the proposed condition for the selection of eigenvectors protected from influence, taking into account the individual characteristics of the cover image; the formula for calculating the amount of protected additional information is proposed; a cover image selection method from the available set of potential containers is developed, which provides stego-object robustness to various image processing attacks.

Keywords: steganography system, stego-object, container selection, digital image, attacks against the embedded secret message, stego-object robustness, eigenvalue, eigenvector.