DOI 10.15276/imms.v10.no1-2.31
УДК 004.056.5

Informatics and Mathematical Methods in Simulation
Vol. 10 (2020), No. 1-2, pp. 31-44

ДОСЛІДЖЕННЯ ВЛАСТИВОСТЕЙ НОРМОВАНОЇ ВІДОКРЕМЛЕНОСТІ МАКСИМАЛЬНОГО СИНГУЛЯРНОГО ЧИСЛА БЛОКУ МАТРИЦІ ЦИФРОВОГО ЗОБРАЖЕННЯ

А.А. Кобозєва, І.І. Бобок

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

На сьогоднішній день одним з найпоширеніших і затребуваних стеганографічних методів є метод модифікації найменшого значущого біта - LSB-метод. Це залишає актуальними задачі виявлення наявності й декодування прихованої інформації, вбудованої в контейнер з використанням цього методу, зокрема в умовах малої пропускної спроможності прихованого каналу зв'язку. Існуючі стеганоаналітичні алгоритми, розроблені для LSB-методу, вирішують, як правило, основну задачу стеганоаналізу - детектування прихованого каналу зв'язку, залишаючи невирішеною задачу декодування (відновлення) додаткової інформації, для якої важливою складовою є визначення/оцінка пропускної спроможності прихованого каналу. *Метою* роботи є додаткові дослідження властивостей нормованої відокремленості максимального сингулярного числа блоків матриці оригінальних цифрових зображень, які розглядаються як контейнери, та побудованих на їх основі LSB-методом стеганоповідомлень, результати якого дадуть змогу для оцінки пропускної спроможності прихованого каналу зв'язку. В роботі досліджуються властивості дискретної функції $y(QF)$, яка визначає кількість блоків зображення, в яких відбувається збільшення нормованої відокремленості максимального сингулярного числа в результаті перезбереження зображення в формат з втратами з коефіцієнтом якості QF. Виявлені особливості зміни функції $y(QF)$ при стеганоперетворенні досліджуваного зображення в залежності від того, контейнером чи стеганоповідомленням воно є; досліджені властивості $y(QF)$ залежно від формату цифрового зображення та коефіцієнта якості для зображення в форматі з втратами, від величини пропускної спроможності прихованого каналу зв'язку, при одноразовому та дворазовому стеганоперетворенні. В результаті проведених досліджень отримані однобічні (зверху) оцінки величини пропускної спроможності прихованого каналу зв'язку, побудованого за допомогою LSB-методу на основі контейнера в форматі з втратами.

Ключові слова: стеганоаналітичний метод, цифрове зображення, пропускна спроможність прихованого каналу, LSB-метод, нормована відокремленість сингулярного числа.

Вступ

Стеганографія сьогодні – один з наймогутніших і широко використовуваних напрямів в області захисту інформації. Стеганографічні системи дають можливість приховати сам факт наявності секретної інформації шляхом організації прихованого каналу зв'язку всередині каналу загального користування. Одним з основних питань тут є питання про те, у чиїх руках перебуває такий потужний засіб захисту, оскільки використання стеганографії, на жаль, може приводити до прихованої комунікації, цілі якої є антидержавними, протизаконними, антигуманними [1,2]. У таких випадках критично важливим є якнайшвидше виявлення прихованої комунікації, що має місце. Основною «зброєю» для цього є стеганоаналіз [3]. Потужні зусилля вчених усього світу спрямовані сьогодні на розв'язок основної задачі стеганоаналізу – виявлення наявності прихованої (додаткової) інформації (ДІ) в інформаційному контенті [4], однак в умовах інформаційного протиборства, яке має місце в сучасному світі [2], цього виявляється

недостатньо. Лише декодування прихованої інформації, її відновлення дозволить повністю досягти мету стеганоаналізу. Задача витягу прихованої інформації, її декодування є найбільш складною, розв'язку якої сприяє визначення/оцінка пропускної спроможності організованого стеганографічного каналу зв'язку [3,5], на забезпечення чого й спрямована дана робота.

Аналіз досліджень та публікацій

На сьогоднішній день одним з найпоширеніших і затребуваних стеганографічних методів залишається метод модифікації найменшого значущого біта (LSB-метод) [3], хоча останнім часом його використання має певні нетипові особливості – малу пропускну спроможність прихованого каналу зв'язку (ПСПК), що організується (≤0.1 біт/піксель), на яку, як правило, не розраховані існуючі стеганоаналітичні методи, що залишає актуальною задачу виявлення наявності прихованої інформації, вбудованої з використанням LSB-методу. Крім того, сучасні стеганоаналітичні методи, як правило, не визначають/не оцінюють ПСПК, що є важливою складовою процесу декодування (відновлення) додаткової інформації. Так в [6] запропонований метод виявлення LSB-вкладень в цифровому зображенні (ЦЗ), заснований на врахуванні значення кореляції між довжиною додаткової інформації й регресією кількості ідентичних по яскравості пікселів, при цьому кожний піксель ЦЗ аналізується окремо. Цей метод дає можливість для використання нової стеганоаналітичної функції для виміру подібності між вагою пікселів, що, як стверджують автори, дозволяє забезпечити значну чутливість стеганоаналізатора. Однак метод не є дієздатним при ПСПК менше, ніж 0.125 біт/піксель, як і метод, запропонований в [7]. Для методу, розробленого в [8], нижня межа ПСПК склала лише 0.1 біт/піксель. Оцінка ПСПК в жодному методі не відбувається.

В [9] був запропонований стеганоаналітичний метод, орієнтований на виявлення прихованого каналу зв’язку з малою пропускною спроможністю, заснований на властивостях нормованої відокремленості максимального сингулярного числа (НВМСЧ) блоку матриці зображення, а саме на врахуванні кількості блоків досліджуваного ЦЗ, отриманих шляхом стандартної розбивки матриці [10], в яких збільшується НВМСЧ в результаті перезбереження ЦЗ в формат з втратами з різними коефіцієнтами якості *QF*. Цю кількість відображала дискретна функція $y(QF)$ ($QF \in \{1,2,...,100\}$ для формату Jpeg, $QF \in \{1,2,...,20\}$ для формату Jpeg2000), яка будувалась для ЦЗ, що піддавалось експертизі.

Якщо позначити через *F* матрицю ЦЗ, яка в процесі аналізу розбивається стандартним чином на неперетинні $l \times l$-блоки з сингулярними числами (СНЧ) [11]

$$\sigma_1 \geq \sigma_2 \geq ... \geq \sigma_l \geq 0, \tag{1}$$

які утворюють вектор $\sigma = (\sigma_1, \sigma_2, ..., \sigma_l)^T$, то нормований вектор СНЧ $\bar{\sigma} = (\bar{\sigma}_1, \bar{\sigma}_2, ..., \bar{\sigma}_l)^T$ визначиться як $\bar{\sigma} = \sigma / \|\sigma\|$, де $\|\sigma\|$ норма вектора σ. Тоді нормована відокремленість СНЧ $\sigma_i, i = \overline{1,l}$, визначається наступним чином [9]:

$$svdgap_n(i) = \min_{i \neq j} |\bar{\sigma}_j - \bar{\sigma}_i|. \tag{2}$$

З (2) з урахуванням (1) випливає, що НВМСЧ – це

$$svdgap_n(1) = \bar{\sigma}_1 - \bar{\sigma}_2,$$

при цьому $0 < svdgap_n(1) \le 1$.

Алгоритмічна реалізація запропонованого в [9] методу виявилася такою, що перевищує по ефективності виявлення наявності прихованого каналу зв'язку сучасні аналоги в умовах малої ПСПК, тобто математичний базис методу, заснований на властивостях НВМСЧ та дискретної функції $y(QF)$, забезпечує чутливість до малих збурень контейнера в процесі стеганоперетворення, а тому може вважатися перспективним для використання з метою розв'язку задачі визначення/оцінки пропускної спроможності прихованого каналу, яка є важливою для процесу декодування ДІ, але в методі, запропонованому в [9], не передбачена. Для забезпечення можливості визначення/оцінки ПСПК необхідні додаткові дослідження властивостей НВМСЧ блоків ЦЗ та функції $y(QF)$.

Мета і задачі дослідження

Метою роботи є подальше дослідження властивостей НВМСЧ блоків та функції $y(QF)$ оригінальних ЦЗ та побудованих на їх основі стеганоповідомлень, результати якого будуть корисними для оцінки ПСПК, сформованого за допомогою LSB-методу.

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

- виявити особливості зміни дискретної функції $y(QF)$ при стеганоперетворенні досліджуваного ЦЗ в залежності від того, контейнером чи стеганоповідомленням воно є;
- дослідити властивості функції $y(QF)$ залежно від формату ЦЗ та коефіцієнта якості для зображення в форматі з втратами;
- дослідити властивості функції $y(QF)$ залежно від величини ПСПК;
- дослідити властивості функції $y(QF)$ при одноразовому та дворазовому стеганоперетворенні за допомогою LSB-методу.

Основна частина

В [9] основною ознакою для виявлення стеганоповідомлення (СП), сформованного на основі ЦЗ-контейнера, що зберігалося в форматі з втратами, було порушення монотонності дискретної функції $y(QF)$, значення якої визначаються кількістю блоків досліджуваного зображення, в яких збільшується НВМСЧ при перезбереженні з втратами з коефіцієнтом якості *QF*. При цьому перезбереження оригінального ЦЗ в форматі без втрат приводило до монотонно спадаючої функції $y(QF)$.

Нехай є оригінальне Jpeg-ЦЗ, збережене з коефіцієнтом якості QF_1. Згадану вище дискретну функцію для оригінального зображення позначимо $y_0(QF)$. Вона не тільки не є монотонною, але в точці $QF = QF_1$, як правило, буде мати локальний мінімум [9].

Параметри й вид кривої, що є графіком $y_0(QF)$, для оригінальних ЦЗ в форматі з втратами з коефіцієнтом якості QF_1 буде залежати від QF_1: чим менше QF_1, тем нижче вздовж осі ординат буде розташована крива $y_0(QF)$ в координатній площині (рис.1), хоча для значних *QF* (для формата Jpeg для *QF*>75), використовуваних при перезбереженні ЦЗ в ході експертизи, ця картина може порушуватися. Дійсно, чим нижче коефіцієнт якості оригінального ЦЗ, тем менше його високочастотна

складова [10], тим більша кількість СНЧ блоків будуть порівнянні з нулем [12], тим більше в таких блоках оригінального ЦЗ буде НВМСЧ, тим у меншій кількості блоків вона збільшиться при перезбереженні у формат із втратами. Коли при перезбереженні в ході експертизи будуть використовуватися значні коефіцієнти якості (QF>75), кількість блоків, у яких відбувається збільшення НВМСЧ, різко знижується (через зменшення елементів матриці квантування [10]), і тут уже значну роль будуть відігравати обчислювальні похибки в процесі округлень до цілих значень частотних коефіцієнтів після квантування. Це приводить до деякого «змішання» кривих $y_0(QF)$ в області QF>75, що ілюструє рисунок 1.

Раніше показано [12], що при стеганоперетворенні Jpeg-контейнера за допомогою методу модифікації найменшого значущого біта властивості СНЧ блоків ЦЗ із втратами починають «прямувати» до властивостей СНЧ блоків ЦЗ без втрат, зокрема, зростає швидкість зміни найменших СНЧ, мінімальні СНЧ, які в блоці оригінального ЦЗ порівнянні з нулем, після вбудови ДІ вже такими не будуть, причому, чим більше буде ПСПК, за допомогою якої отримано СП, тим більше зростуть значення найменших СНЧ блоків матриці контейнера та швидкість їх зміни. Взагалі існують стеганографічні методи, які в результаті вбудови ДІ дають стеганоповідомлення, матриця якого практично не відрізняється від матриці оригінального відповідного ЦЗ у форматі без втрат [13]. При цьому відповідними будемо називати такі ЦЗ, які відрізняються лише форматом (з/без втрат) збереження [9]. Поведінка функції $y(QF)$ змінюється аналогічним чином: чим більше ПСПК, тим «ближче» крива $y(QF)$ для СП, сформованого на основі контейнера в форматі з втратами, до $y(QF)$ для відповідного оригінального ЦЗ у форматі без втрат, тобто чим більше ПСПК, тим вище вздовж осі ординат крива $y(QF)$ на координатній площині для відповідного СП, тим менше відмінність між значеннями відповідних функцій для СП і «чистого» відповідного ЦЗ без втрат, що проілюстровано на рисунку 2 для оригінального ЦЗ в форматі Jpeg, отриманого з QF=75. Зауважимо, що із зростанням ПСПК для функції $y(QF)$ локальний мінімум в QF=75 стає все менш вираженим (рис.2). Для деяких ЦЗ він взагалі може стати відсутнім.

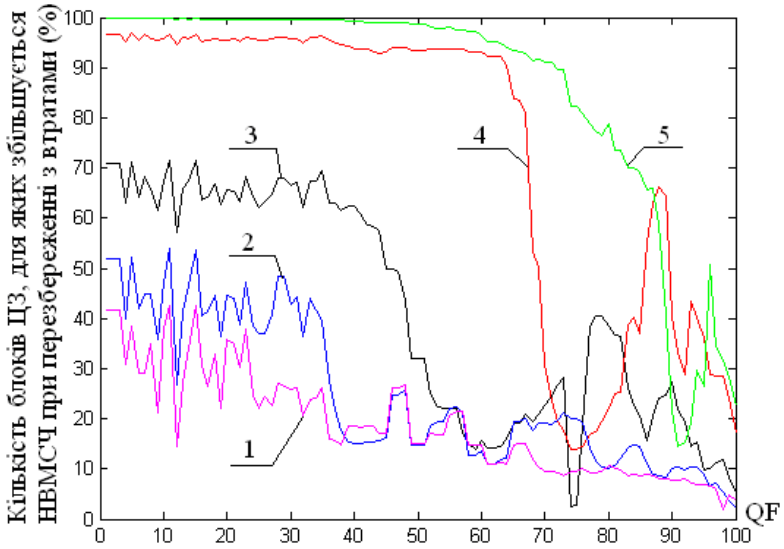

Рис. 1. Графіки функції $y(QF)$ для оригінальних ЦЗ в форматі Jpeg з коефіцієнтом якості QF, який дорівнює: 1 – 55; 2 – 65; 3 – 75; 4 – 85; 5 – 95

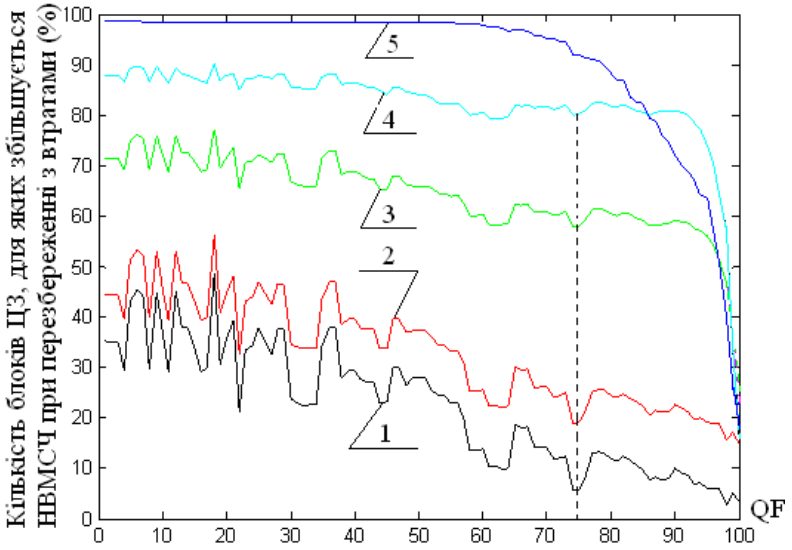

Рис. 2. Зміна властивостей $y(QF)$ залежно від ПСПК, яка використовується при отриманні стеганоповідомлення: 1 – оригінальне ЦЗ-контейнер в форматі Jpeg (*QF*=75); 2 – СП з ПСПК=1%; 3 – СП з ПСПК=5%; 4 – ПСПК=10%; 5 – оригінальне відповідне ЦЗ без втрат

Описані зміни СНЧ при вбудові ДІ в контейнер у форматі із втратами приведуть до збільшення кута між нормованим вектором СНЧ $\bar{\sigma}$ $l\times l$-блоку і першим вектором e_1 стандартного базису простору R^l, у порівнянні з кутом в оригінальному Jpeg-ЦЗ, тобто НВМСЧ у більшості блоків стеганоповідомлення буде не більше, чим у блоках контейнера. Якщо тепер перезберігати із втратами контейнер і СП, то кількість блоків, у яких буде збільшуватися НВМСЧ, у СП буде більше, чим у контейнері для одного *QF*, оскільки в загальному випадку можна стверджувати, що чим менше НВМСЧ у блоці ЦЗ, тим більше ймовірність її збільшення при перезбереженні зображення із втратами, тому що збереження із втратами в більшості блоків збільшує НВМСЧ [9].

Нехай ДІ вбудовується в ЦЗ-контейнер у форматі без втрат. У цьому випадку якісні зміни СНЧ, що відбуваються в блоках матриці контейнера, передбачити складно, вони не будуть тут настільки явними, оскільки тут немає таких характерних рис СНЧ, як для ЦЗ у форматі із втратами, зокрема, порівнянності з нулем найменших СНЧ блоків. Хоча при вбудові ДІ й тут збільшується кількість блоків при перезбереженні СП у формат з втратами, у порівнянні з перезбереженням контейнера, тобто графік $y\,(QF)$ для СП буде вище вздовж осі ординат, ніж $y\,(QF)$ для контейнера. Дійсно, у загальному випадку вбудова LSB-методом ДІ, яка розглядається як випадково сформована матриця відповідного зображенню розміру, елементи якої належать множині $\{-1,0,1\}$, не зменшує високочастотну складову ЦЗ [10], тобто приводить до незбільшення, а на практиці до зменшення НВМСЧ. Тому кількість блоків у ЦЗ-СП, для яких зросте НВМСЧ при перезбереженні із втратами з коефіцієнтом якості *QF*, буде більше, чим у ЦЗ-контейнера при перезбереженні з тим самим *QF*. Виключення тут може становити перезбереження з $QF \approx 100$. Якщо $QF \approx 100$, то кількості блоків, для яких збільшиться НВМСЧ при перезбереженні із втратами, і ЦЗ-СП, і ЦЗ-контейнера у форматі без втрат, будуть незначними й такими, що практично не відрізняються одна від іншої (що є наслідком використовуваних для таких коефіцієнтів якості *QF* матриць квантування, що мають незначні елементи [10]) (рис.3).

Таким чином, встановлено, що крива $y\,(QF)$ для контейнера завжди нижче вздовж осі ординат на координатній площині, ніж для СП, сформованого на його основі, тобто кількість блоків ЦЗ-СП, для яких зросте НВМСЧ при перезбереженні з

втратами, є більшою, ніж у ЦЗ-контейнері, незалежно від формату (з/без втрат) контейнера.

Зауважимо, що оскільки LSB-метод є нестійким до атак проти вбудованого повідомлення, зокрема, до стиску із втратами, то стеганоповідомлення, як правило, буде зберігатися у форматі без втрат.

Нехай розглядається ЦЗ, що формально збережене у форматі без втрат. Це може бути: оригінальне ЦЗ; СП, яке сформовано на основі контейнера у форматі з втратами й збережене без втрат; СП, сформоване на основі контейнера без втрат, збережене без втрат. Будемо припускати, що СП формуються в умовах малої ПСПК, а саме: ПСПК $\leq 10\%$. Побудувавши для досліджуваного ЦЗ функцію $y\left(QF\right)$, можна відокремити оригінальне ЦЗ у форматі без втрат або СП, побудоване на основі контейнера без втрат, від ЦЗ, яке зазнало перезбереження з формату із втратами у формат без втрат (з/без стеганоперетворення), досліджуючи монотонність $y\left(QF\right)$ [9].

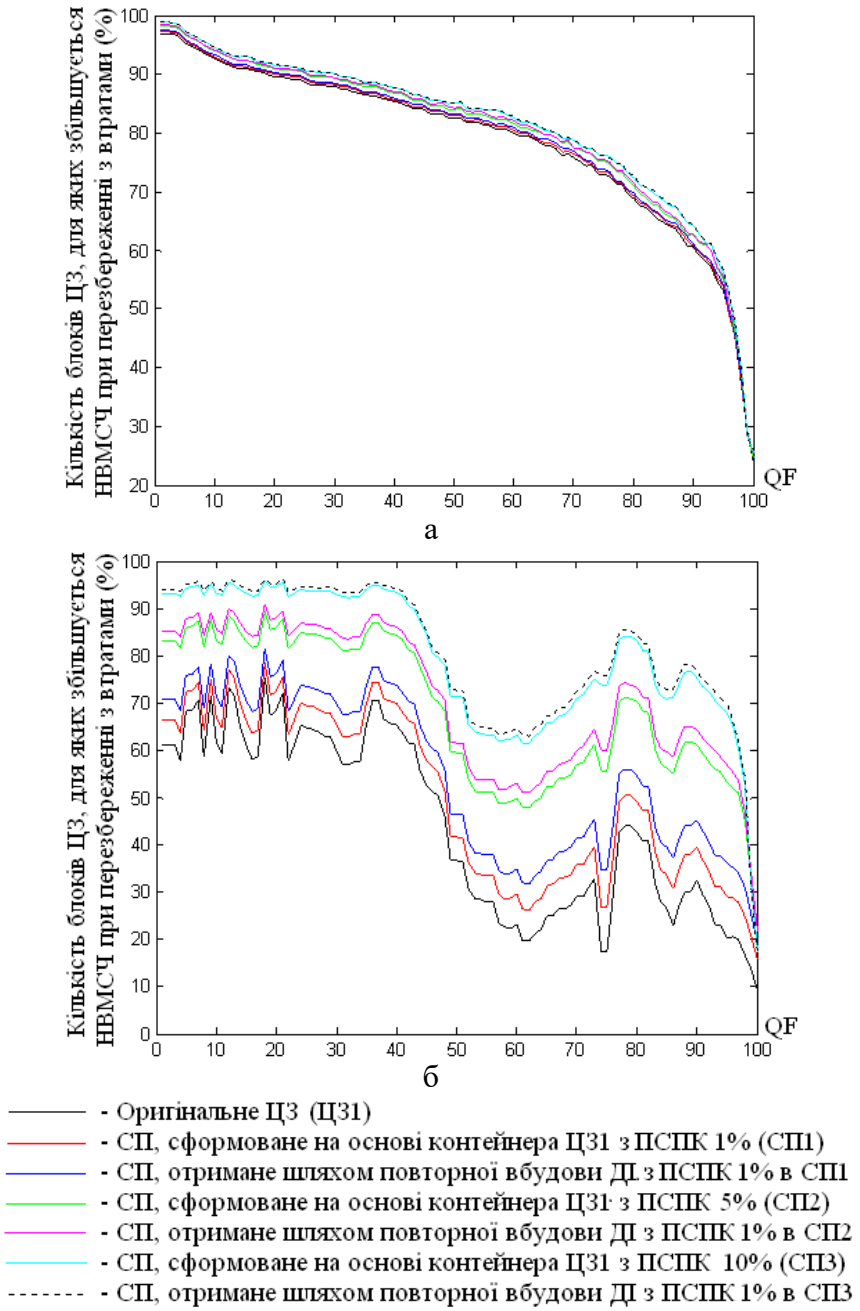

Рис. 3. Графіки функції $y\left(QF\right)$: а – ЦЗ без втрат, б – ЦЗ з втратами (Jpeg (QF=75))

Однак наступні задачі залишаються тут невирішеними:

- відокремити спочатку збережене у форматі із втратами цз, що піддалося стеганоперетворенню, від такого, яке не зазнало вбудову ді, а просто було перезбережено у формат без втрат;
- відокремити оригінальне цз без втрат від сп, побудованого на основі контейнера без втрат.

Розглянемо в даній роботі детально задачу 1. Нехай ЦЗ спочатку зберігалися в форматі з втратами; F_1 – матриця ЦЗ, яке піддається експертизі. Формально воно збережено в форматі без втрат. Якщо F_1 – це СП, то будемо вважати, що воно отримане на основі Jpeg-контейнера з матрицею F. Піддамо F_1 стеганоперетворенню з малою ПСПК (наприклад, 1%), формальним відображенням якого є співвідношення [14]:

$$F_{1,1} = F_1 + \Delta F, \tag{3}$$

де ΔF – матричне представлення ДІ, $F_{1,1}$ – матриця ЦЗ-СП. Визначимо функції $y\left(QF\right)$ для F_1 і $F_{1,1}$, перезберігаючи їх з втратами з усіма можливими значеннями коефіцієнта якості QF. З вищенаведеного випливає, що для конкретного QF, як правило, значення $y\left(QF\right)$ для $F_{1,1}$ буде більше, ніж для F_1, що геометрично відобразиться в тому, що графік $y\left(QF\right)$ для $F_{1,1}$ буде вище вздовж осі ординат, ніж графік $y\left(QF\right)$ для F_1, незалежно від того, СП чи контейнеру відповідає матриця F_1. Однак відмінність між значеннями функції $y\left(QF\right)$ (між відповідними графіками) буде різною залежно від того, оригінальному ЦЗ чи СП відповідає матриця F_1.

Нехай F_1 – матриця контейнера, тоді стеганоперетворення (3) для нього буде першим і єдиним. Якщо F_1 відповідає СП, то для нього (3) – повторне стеганоперетворення. Покажемо, що первинне перетворення (3) за допомогою матриці ΔF «підніме» графік функції $y\left(QF\right)$ вздовж осі ординат відносно побудованого для F_1 більше, ніж повторне перетворення за допомогою тієї ж матриці ΔF.

Стеганоперетворення Jpeg-контейнера, як згадано вище, практично завжди приводить до збільшення найменших СНЧ (оскільки від'ємними вони стати не можуть у силу (1), а до вбудови ДІ є порівнянними з нулем), зменшення НВМСЧ у блоках, задіяних у стеганоперетворенні, збільшуючи тим самим імовірність зростання НВМСЧ при перезбереженні ЦЗ у формат із втратами. Якщо ж вбудова ДІ відбувається в ЦЗ-СП, то там вже НВМСЧ у блоках, задіяних у первинному стеганоперетворенні, менше, ніж в відповідних блоках оригінального контейнеру. Після вбудови ДІ в СП найменші СНЧ відповідних блоків, задіяних у повторному стеганоперетворенні, які вже не порівнянні з нулем у тих блоках, що були задіяні в первинному стеганоперетворенні, можуть як зменшитися, так і збільшитися, що може привести як до збільшення, так і до зменшення НВМСЧ. Повторна вбудова ДІ в СП у загальному випадку збільшить результуючу ПСПК, додатково збурюючи СНЧ, але відносна зміна найменших СНЧ блоків контейнера буде більше, ніж найменших СНЧ блоків СП при однаковій збурній дії. Таким чином, кількість блоків, у яких зросте НВМСЧ при перезбереженні із втратами СП, отриманого в результаті послідовного дворазового стеганоперетворення, хоча й буде більше, чим при перезбереженні первинного СП, але ступінь цього збільшення буде менше, ніж ступінь збільшення при такому ж (що характеризується матрицею ΔF), але первинному стеганоперетворенні щодо порожнього контейнера. Більше того, ступінь збільшення буде тим менше, чим більше ПСПК первинного стеганоперетворення. Дійсно, чим більше ПСПК первинного стеганоперетворення, тим більше кількість блоків контейнера, у яких зменшиться НВМСЧ у результаті

стеганоперетворення, тим менше НВМСЧ у блоках F_1, задіяних у стеганоперетворенні, тим «вище» буде графік функції $y\left(QF\right)$, отриманої при перезбереженні F_1 з втратами. При повторній вбудові ДІ в СП, сформоване з порівнянно значною первинною ПСПК, буде значна кількість блоків, де після повторного стеганоперетворення НВМСЧ збільшиться, а не зменшиться, у порівнянні із НВМСЧ у блоці вхідного СП, що приведе до того, що при перезбереженні СП, отриманого в результаті дворазового стеганоперетворення, хоча графік функції $y\left(QF\right)$ буде вище, ніж графік аналогічної функції для вхідного СП (отриманого в результаті однократного стеганоперетворення), але ця різниця буде тим менше, чим більше була ПСПК первинного стеганоперетворення, що практично підтверджується результатами обчислювального експерименту, докладно описаного нижче, наведеними в табл.1 (використані позначення введені нижче) і проілюстрованими на рис.3.

Описану вище картину, що полягає в тому, що чим більша ПСПК первинного стеганоперетворення, тим менше відмінність між відповідними функціями $y\left(QF\right)$ для СП, отриманих одноразовим і дворазовим стеганоперетворенням, складно відстежити для ЦЗ-контейнера у форматі без втрат, де це не буде вже так строго виконуватися, хоча для середніх по експерименту значень має місце (табл.1).

Таблиця 1.

Середні по експерименту значення $T_{i,1}$, $i \in \{0,1,5,10\}$

Множина, з якої обирався контейнер	$T_{0,1}$	$T_{1,1}$	$T_{5,1}$	$T_{10,1}$
M_{Tif}	1.95	1.90	1.82	1.68
$M_{Jpeg,70}$	60.44	51.40	26.14	12.19
$M_{Jpeg,75}$	46.16	39.54	20.81	10.08
$M_{Jpeg,80}$	33.12	28.29	15.49	8.16

Для цього є дві причини. По-перше, у блоках ЦЗ в форматі без втрат практично відсутні нульові/порівнянні з нулем СНЧ [15], внаслідок чого зміни, які відбуваються в ЦЗ без втрат при вбудові ДІ, можуть приводити як до зменшення, так і до збільшення СНЧ блоків, незалежно від їхнього порядкового номера. По-друге, кількість блоків, у яких відбувається збільшення НВМСЧ при перезбереженні у формат із втратами, при малих і середніх значеннях *QF* близько до 100% (див. рис.3). Зростання цієї кількості при вбудові ДІ в цьому випадку взагалі не може бути значним. Крім того, у силу малої зміни оцінюваної кількості блоків тут критичну роль відіграє накопичення обчислювальної похибки. У силу цього для більшості протестованих ЦЗ спостерігалося порушення монотонності для величини, що характеризує зміну значень дискретної функції $y\left(QF\right)$, із зростанням ПСПК первинного стеганоперетворення (табл.2), причому порушення монотонності могло спостерігатися на будь-якому кроці збільшення ПСПК первинного стеганоперетворення (рис.4 – тут ПСПК первинного стеганоперетворення вважається рівною 0 для ЦЗ-контейнера).

Таблиця 2.

Кількість ЦЗ, використаних у якості контейнерів, для яких порушувалася монотонна залежність відмінності між значеннями функцій $y\left(QF\right)$ для СП, отриманих одноразовим і дворазовим стеганоперетворенням, із зростанням ПСПК первинного стеганоперетворення (в % від загального числа ЦЗ в експерименті)

Формат ЦЗ-контейнера			
без втрат (Tif)	з втратами (Jpeg, QF=80)	з втратами (Jpeg, QF=75)	з втратами (Jpeg, QF=70)
84.7	6.3	3.8	2.5

Наведені таблиці 1, 2, рисунки 3, 4 частково відображають результати обчислювального експерименту, який підтверджує висновки, теоретично отримані вище. В обчислювальному експерименті були задіяні наступні множини ЦЗ: M_{Tif} – 500 ЦЗ в форматі без втрат (Tif) (150 ЦЗ з бази 4cam_auth [16], 275 ЦЗ з бази img_Nikon_D70s [17], 75 ЦЗ отриманих непрофесійною відеокамерою); $M_{Jpeg,70}$, $M_{Jpeg,75}$, $M_{Jpeg,80}$ – по 500 ЦЗ, отриманих з ЦЗ з множини M_{Tif} шляхом перезбереження у формат Jpeg з QF=70, 75, 80 відповідно (значення QF обрані як такі, що найбільш часто використовуються на практиці).

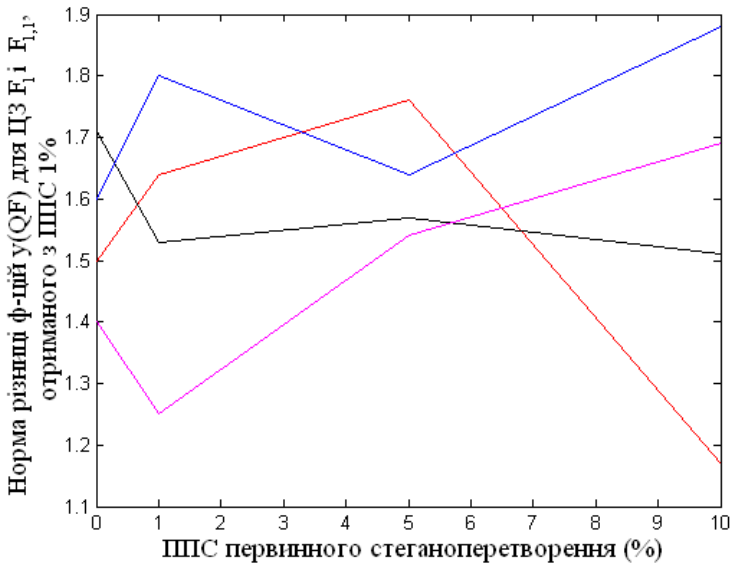

Рис. 4. Залежність для 4-х конкретних ЦЗ в форматі без втрат норми вектора різниці значень дискретних функцій $y\left(QF\right)$ для досліджуваного ЦЗ і ЦЗ, отриманого вбудовою ДІ з ПСПК=1% в досліджуване, від ПСПК первинного стеганоперетворення

На першому етапі в оригінальне ЦЗ (з втратами або без втрат) вбудовувалася ДІ з ПСПК 1, 5, 10%. Оригінальне ЦЗ-контейнер і отримані СП перезберігалися у формат із втратами (Jpeg) з усіма коефіцієнтами якості $QF \in \{1,2,...100\}$. В результаті визначалися дискретні функції $y_0\left(QF\right)$ (для контейнера), $y_1\left(QF\right)$, $y_5\left(QF\right)$, $y_{10}\left(QF\right)$, $QF \in \{1,2,...100\}$ для СП відповідно, що визначають для кожного $QF \in \{1,2,...100\}$ кількість блоків ЦЗ, для яких зростає НВМСЧ у результаті перезбереження у формат із втратами з коефіцієнтом якості QF. У якості кількісної характеристики змінення ЦЗ в результаті первинного стеганоперетворення розглядалася величина, що характеризує змінення функції $y_0\left(QF\right)$:

$$T_{0,i} = \left(\sum_{1}^{100} \left| y_0(QF) - y_i(QF) \right|^2 \right)^{\frac{1}{2}}, \quad i \in \{1,5,10\}. \tag{4}$$

Співвідношення (4) являє собою евклідову норма вектора різниці векторів значень функцій $y_0(QF)$ і $y_1(QF)/\, y_5(QF)/\, y_{10}(QF)$ в відповідних аргументах.

На другому етапі в сформовані на першому етапі СП повторно вбудовувалася ДІ з ПСПК=1% (матриця ДІ ΔF тут формувалася випадковим чином і використовувалася одна й та сама для СП з ПСПК 1, 5, 10%, сформованих на основі одного контейнера). Отримані після повторного стеганоперетворення СП перезберігалися із втратами (формат Jpeg) з $QF \in \{1,2,...100\}$. У результаті були отримані дискретні функції $y_{1,1}(QF)$, $y_{5,1}(QF)$, $y_{10,1}(QF)$, $QF \in \{1,2,...100\}$ для СП з ПСПК первинного стеганоперетворення 1, 5, 10% відповідно. У якості кількісної характеристики зміни ЦЗ-СП після повторного стеганоперетворення за аналогією з (4) розглядалася величина:

$$T_{i,1} = \left(\sum_{1}^{100} \left| y_i(QF) - y_{i,1}(QF) \right|^2 \right)^{\frac{1}{2}}, \quad i \in \{1,5,10\}. \tag{5}$$

Результати експерименту для оригінальних ЦЗ у форматі з втратами, крім таблиць і рисунків, наведених вище, знайшли своє відображення для випадку формату Jpeg з коефіцієнтом якості *QF*=75 на рис.5 і в табл.3, де наочно виражена загальна тенденція якісної зміни значень оцінок (4), (5) із зростанням ПСПК первинного стеганоперетворення зображення: зменшення моди гістограми значень $T_{i,1}$ з одночасним збільшенням значення в моді; зменшення довжини інтервалу можливих значень $T_{i,1}$ за рахунок зменшення максимального значення $T_{i,1}$. Отримані якісні результати є типовими для ЦЗ в форматі з втратами, незалежно від конкретики формату (Jpeg) та використаного коефіцієнта якості (*QF*=75), оскільки базуються на отриманих в роботі теоретичних висновках і підтверджують їх. Використання іншого формату з втратами (наприклад, Jpeg2000) чи іншого коефіцієнту якості змінить лише кількісні показники гістограм.

Таблиця 3.

Максимальні й мінімальні по експерименту значення $T_{i,1}$, $i \in \{0,1,5,10\}$ для ЦЗ-контейнерів, спочатку збережених в форматі Jpeg з *QF*=75

$T_{0,1}$		$T_{1,1}$		$T_{5,1}$		$T_{10,1}$	
макс.	мін.	макс.	мін.	макс.	мін.	макс.	мін.
146	2.1	124	2.4	61	1.7	26	2

Аналіз числових значень величин (4), (5) з використанням отриманих гістограм (рис.5) дозволяє зробити висновки, важливі для оцінки величини ПСПК, де використовувалося у якості контейнера ЦЗ у форматі Jpeg (*QF*=75):

- якщо для досліджуваного ЦЗ значення $T_{i,1} \geq 125$, то воно не зазнавало стеганоперетворення;
- якщо $61 < T_{i,1}$, то для аналізованого ЦЗ ПСПК<5%, у тому числі ЦЗ може бути «чистим» контейнером;

- якщо $26 < T_{i,1}$, то для аналізованого ЦЗ ПСПК<10%.

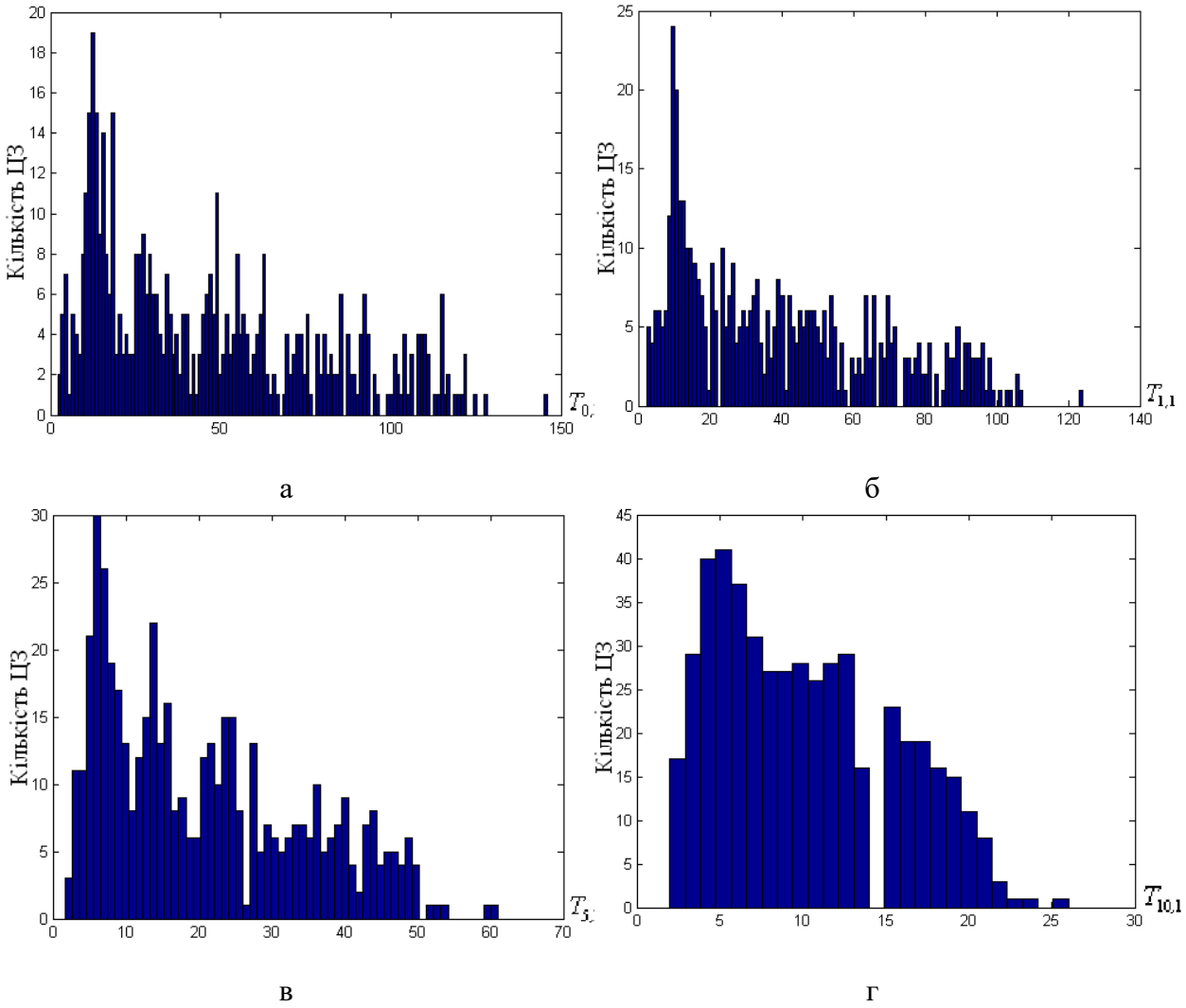

Рис. 5. Гістограми значень $T_{i,1}$, $i \in \{0,1,5,10\}$, для оригінального ЦЗ-контейнера, збереженого у форматі Jpeg з QF=75: а – $T_{0,1}$ (мода дорівнює 13, значення в моді 19); б – $T_{1,1}$ (мода 10, значення в моді 24); в – $T_{5,1}$ (мода 6, значення в моді 30); г – $T_{10,1}$ (мода 5, значення в моді 41)

Отримані результати на даному етапі досліджень не є остаточними, отримані для ПСПК кількісні оцінки є однобічні (оцінки зверху), такі, що залежать від величини ПСПК первинного стеганоперетворення ЦЗ в форматі Jpeg (QF=75). Розширюючи обчислювальний експеримент, збільшуючи різноманітність значень ПСПК для первинного стеганоперетворення (наприклад, від 1 до K% з кроком h%), отримані результати можна уточнити, що буде зроблено при розробці безпосередньо методу оцінки ПСПК. Використання іншого формату з втратами (наприклад, Jpeg2000) чи іншого коефіцієнту якості QF змінить кількісні показники гістограм, тому розробка методу потребує отримання кількісних характеристик для всіх можливих (самих використовуваних) значень коефіцієнта якості. Враховуючи їх можливу різноманітність, необхідним попереднім кроком перед використанням методу оцінки ПСПК повинен бути крок визначення QF для контейнера в форматі з втратами, що можливо зробити за допомогою, наприклад, методу, запропонованому в [18].

Висновки

У роботі проведені дослідження властивостей НВМСЧ блоків матриці ЦЗ, дискретної функції $y(QF)$, яка ставиться у відповідність ЦЗ в умовах його перезбереження із втратами з різними коефіцієнтами якості й відображає кількість блоків, у яких у результаті перезбереження збільшується НВМСЧ.

Встановлено теоретично й підтверджено практично шляхом обчислювального експерименту:

- чим більше коефіцієнт якості оригінального ЦЗ в форматі з втратами, тим більше значення функції $y(QF)$ для конкретного $QF \le 75$; установлені причини, по яких дане твердження може порушуватися для QF>75;
- чим більше ПСПК, що використовувалася для отримання СП, тим більше значення $y(QF)$ для конкретного QF, тобто, чим більше ПСПК, тим вище крива $y(QF)$ для відповідного СП, тим «ближче» графік функції $y(QF)$ для СП, сформованого на основі контейнера в форматі з втратами, до $y(QF)$ для відповідного оригінального ЦЗ у форматі без втрат;
- кількість блоків ЦЗ-СП, для яких зросте НВМСЧ при перезбереженні з втратами, є більшою, ніж у ЦЗ-контейнері незалежно від формату (з/без втрат) контейнера;
- первинне стеганоперетворення ЦЗ за допомогою матриці ΔF змінює («піднімає» графік) функцію $y(QF)$ більше, ніж повторне стеганоперетворення за допомогою тієї ж матриці ΔF;
- чим вище ПСПК первинного стеганоперетворення, тим менше відмінність між відповідними функціями $y(QF)$ для СП, отриманих шляхом одноразового й дворазового стеганоперетворення, при цьому для повторної вбудови ДІ використовується одна й та сама матриця ΔF незалежно від ПСПК первинного стеганоперетворення.

У результаті проведених досліджень отримані однобічні оцінки (зверху) величини ПСПК в умовах ЦЗ-контейнера в форматі Jpeg (QF=75). Проведені дослідження не є завершеними, але говорять про перспективність обраного шляху для оцінки величини ПСПК первинного стеганоперетворення ЦЗ і в даний час продовжуються авторами.

Список літератури

1. Information Hiding in Communication Networks: Fundamentals, Mechanisms, Applications, and Countermeasures / W. Mazurczyk et al. Hoboken: Wiley, 2016. 296 p.
2. Информационное противоборство в современных условиях / Л.Г. Пирцхалава и др. К.: ЦП «Компринт», 2019. 226 с.
3. Стеганография, цифровые водяные знаки и стеганоанализ / А.В. Аграновский и др. М.: Вузовская книга, 2009. 220 с.
4. Karampidis K., Kavallieratou E., Papadourakis G. A review of image steganalysis techniques for digital forensics. *Journal of Information Security and Applications.* 2018. V.40. P. 217–235.
5. Метод оценки величины скрытой пропускной способности стеганографического канала связи. Информационные системы в управлении, образовании, промышленности: монография / под ред. В.С. Пономаренко. Х.: Вид-во ТОВ «Щедра садиба плюс», 2014. С.190–203
6. Chaeikar S.S., Ahmadi A. Ensemble SW image steganalysis: A low dimension method for LSBR detection. *Signal Processing: Image Communication*. 2019. 70. P. 233–245.
7. PSW statistical LSB image steganalysis / S. Shojae Chaeikar et al. *Multimedia Tools and Applications*. 2018. V.77. P. 805–835.
8. Veena S.T., Arivazhagan S. Universal secret payload location identification in spatial LSB stego images. *Annals of Telecommunications*. 2019. V.74. P. 273–286.

9. Bobok I.I., Kobozeva A.A. Steganalysis method efficient for the hidden communication channel with low capacity. *Радіотехніка*. 2019. V.198. С. 19–31
10. Гонсалес Р., Вудс Р. Цифровая обработка изображений. М.: Техносфера, 2006. 1070 с.
11. Деммель Д. Вычислительная линейная алгебра: теория и приложения. М.: Мир, 2001. 430 с.
12. Бобок И.И. Стеганоаналитический метод для цифрового сигнала-контейнера, хранящегося в формате с потерями. *Сучасний захист інформації*. 2011. V.2. С. 50–60.
13. Кобозева А.А., Альфалуджи С.А. Стеганографический алгоритм, обеспечивающий большую пропускную способность канала скрытой связи. *Вестник Нац. техн. ун-та "ХПИ": сб. науч. тр. Темат. вып.: Системный анализ, управление и информационные технологии*. 2012. V.29. С. 30–41.
14. Кобозева А.А., Хорошко В.А. Анализ информационной безопасности: монография. К.: ГУИКТ, 2009. 251 с.
15. Бобок И.И., Кобозева А.А. Общий стеганоаналитический подход, основанный на матричном анализе. *Вісник Національного технічного університету «ХПІ».* 2011. V.35. С. 12–20.
16. Hsu Y., Chang S. Detecting image splicing using geometry invariants and camera characteristics consistency. *2006 IEEE International Conference on Multimedia and Expo*, Toronto, 2006. P. 549–552
17. Gloe T., Böhme R. The “Dresden Image Database” for benchmarking digital image forensics. *Proceedings of the 2010 ACM Symposium on Applied Computing (SAC ’10)*. New York, 2010. P. 1585–1591.
18. Кобозева А.А., Бобок И.И., Батиене Л.Е. Стеганоаналитический метод, основанный на анализе сингулярных чисел блоков матрицы цифрового изображения. *Problemele Energeticii Regionale*. 2018. V.3(38). URL: http://journal.ie.asm.md/ru/contents/electronni-jurnal-338-2018.

ИССЛЕДОВАНИЕ СВОЙСТВ НОРМИРОВАННОЙ ОТДЕЛЕННОСТИ МАКСИМАЛЬНОГО СИНГУЛЯРНОГО ЧИСЛА БЛОКА МАТРИЦЫ ЦИФРОВОГО ИЗОБРАЖЕНИЯ

А.А. Кобозева, И.И. Бобок

Одесский национальный политехнический университет,
просп. Шевченко, 1, Одесса, 65044, Украина; e-mail: alla_kobozeva@ukr.net

На сегодняшний день одним из самых распространенных и востребованных стеганографических методов является метод модификации наименьшего значащего бита – LSB-метод, оставляя актуальной задачу выявления наличия и декодирования скрытой информации, погруженной в контейнер с использованием этого метода, в частности в условиях малой пропускной способности скрытого канала связи. Существующие стеганоаналитические алгоритмы, разработанные для LSB-метода, решают, как правило, основную задачу стеганоанализа – детектирование скрытого канала, оставляя нерешенной задачу декодирования (восстановления) дополнительной информации, для которой важной составляющей является определение/оценка пропускной способности скрытого канала. *Целью* работы являются дополнительные исследования свойств нормированной отделенности максимального сингулярного числа блоков матрицы оригинальных цифровых изображений, которые рассматриваются в качестве контейнеров, и построенных на их основе стеганосообщений, результаты которого дадут возможность для оценки пропускной способности скрытого канала связи. В работе исследуются свойства дискретной функции $y(QF)$, которая определяет количество блоков изображения, в которых происходит увеличения нормированной отделенности максимального сингулярного числа в результате пересохранения изображения в формат с потерями с коэффициентом качества QF. Определены особенности изменения функции $y(QF)$ при стеганопреобразовании исследуемого изображения в зависимости от того, контейнером или стеганосообщением оно является; исследованы свойства $y(QF)$ в зависимости от формата цифрового изображения и коэффициента качества для

изображения в формате с потерями; от величины пропускной способности скрытого канала связи; при однократном и двукратном стеганопреобразовании. В результате проведенных исследований получены односторонние оценки (сверху) величины пропускной способности скрытого канала связи, построенного с помощью LSB-метода на основе контейнера в формате с потерями.
Ключевые слова: стеганоаналитический метод, цифровое изображение, пропускная способность скрытого канала, LSB-метод, нормованнная отделенность сингулярного числа.

RESEARCHING THE PROPERTIES OF THE NORMALIZED SEPARATION OF THE MAXIMUM SINGULAR VALUE OF THE DIGITAL IMAGE MATRIX BLOCK

A.A. Kobozeva, I.I. Bobok

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

The least significant bit modification method is one of the most widespread and demanded steganographic methods. Today this method is often used for the hidden communication channel with low capacity. Therefore, the problem of detecting and decoding LSB-embedding with low capacity is actual. Existing steganoanalytical algorithms for the LSB-method, as a rule, solve the main problem of steganoanalysis. This task is to detect a hidden channel. The problem of decoding (restoring) additional information remains unsolved. It is important to determine/to estimate the capacity of the hidden channel for decoding information. The article considers a digital image as a container. The aim of this article is additional research of the properties of the normalized separation of the maximum singular value of the blocks of the matrix of original digital images and stego. The research results will be used to assess the capacity of the hidden communication channel. The article examines the properties of the discrete function $y(QF)$. This function determines the number of image blocks in which the normalized separation of the maximum singular value increases as a result of resaving the image into a lossy format with a quality factor QF. The features of the change in the function $y(QF)$ during the steganotransformation of the image are determined. These features are different for an empty container and a stego. The properties of $y(QF)$ are investigated depending on the digital image format, on the quality factor for the image in the lossy format; on the value of the capacity of the hidden communication channel; with single and double steganotransformation. As a result of the studies, one-sided estimates (from above) of the capacity of the hidden communication channel constructed using the LSB-method were obtained.
Keywords: steganoanalytical method, digital image, capacity of the hidden channel, LSB-method, normal singularity separation.