ПРОБЛЕМИ ФУНДАМЕНТАЛЬНИХ І ПРИКЛАДНИХ НАУК

МЕТРОЛОГІЯ

PROBLEMS OF BASIC AND APPLIED SCIENCES

METROLOGY

УДК 004.056.5

І.І. Бобок, магістр,
А.А. Кобозєва, д-р техн. наук, проф.,
Одес. нац. політехн. ун-т

МЕТОД ПРИХОВАНОЇ ПЕРЕДАЧІ ДАНИХ, ЩО ЗАБЕЗПЕЧУЄ АУТЕНТИФІКАЦІЮ КОНТЕЙНЕРА, ЗАСНОВАНИЙ НА МАТРИЧНОМУ АНАЛІЗІ

І.І. Бобок, А.А. Кобозєва. **Метод прихованої передачі даних, що забезпечує аутентифікацію контейнера, заснований на матричному аналізі.** Розроблено новий стеганографічний метод, що дозволяє одночасно вирішувати завдання прихованої передачі інформації і аутентифікації контейнера, заснований на матричному аналізі. Наведено результати обчислювальних експериментів.
Ключові слова: стеганографічний метод, контейнер, стеганоповідомлення, аутентифікація, стеганоаналіз.

И.И. Бобок, А.А. Кобозева. **Метод скрытой передачи данных, обеспечивающий аутентификацию контейнера, основанный на матричном анализе.** Разработан новый стеганографический метод, позволяющий одновременно решать задачи скрытой передачи информации и аутентификации контейнера, основанный на матричном анализе. Приведены результаты вычислительных экспериментов.
Ключевые слова: стеганографический метод, контейнер, стеганосообщение, аутентификация, стеганоанализ.

I.I. Bobok, A.A. Kobozeva. **Method of hidden data transfer that provides container authentication and is based on matrix analysis.** Proposed is a new steganographic method based on matrix analysis to simultaneously solve both the problem of hidden data transfer, and container authentication. The results of numerical experiments are given.
Keywords: steganographic method, container, steganomessage, authentication, steganalysis.

Вступ. Стеганографія — одне з найбільш старих [1] і одночасно найбільш перспективних сучасних напрямків захисту інформації [1…3]. В процесі стеганографування приховуване повідомлення, або додаткова інформація (ДІ), вбудовується в об’єкт, який не привертає увагу, або контейнер, що потім передається відкритим каналои зв’язку. Не обмежуючи спільності міркувань, для простоти викладу далі як контейнер, розглядається цифрове зображення (ЦЗ) у градаціях сірого. Процес вбудови ДІ в контейнер, або основне повідомлення (ОП), називатимемо стеганоперетворенням (СПР), а результат СПР — стеганоповідомленням (СП).

Зацікавленість в розробках в галузі стеганографії весь час зростає. Для цього існують дві основні причини. По-перше, це обмеження на використання криптозасобів у ряді країн світу, у

ISSN 2076-2429 (print)
ISSN 2223-3814 (on line)

тому числі, в Україні; по-друге, із зростанням обсягу інформації, представленої в цифровому виді, підвищилася актуальність проблеми захисту прав власності на таку інформацію [1, 2]. Логічним наслідком тут стала активізація досліджень у двох основних напрямках: в галузі "класичної" стеганографії (проблеми, пов'язані з організацією секретного каналу всередині відкритого каналу зв'язку); в галузі так званих цифрових водяних знаків (ЦВЗ) — спеціальних "міток", які вбудовуються в сигнал з метою контролю його використання [4].

При вбудові ЦВЗ в інформаційний контент не завжди висувається вимога забезпечення надійності сприйняття СП [2]. За певних умов вбудований знак може (або повинен) бути помітним. Це зауваження значно відрізняє методи, які можуть використовуватися при розв'язанні задачі аутентифікації, від методів розв'язання задачі прихованої передачі даних. Однак, якщо задача забезпечення надійності сприйняття при вбудові ЦВЗ ставиться, то принципового протиріччя для одночасного розв'язання двох основних задач стеганографії — аутентифікації й організації прихованої передачі інформації, які в сукупності будемо називати *double*-задачею, не виникає.

Проблема створення стеганографічних алгоритмів для розв'язання *double*-задачі вже розглядалася у відкритих джерелах, однак запропоновані в них розробки мають ряд суттєвих недоліків [5, 6]. Так алгоритм у більшості випадків свого можливого використання не може забезпечити надійність сприйняття СП для довільного ЦЗ-контейнера, хоча така ціль ставиться [5]. Алгоритм, запропонований іншими авторами, формує СП, чутливе не тільки до навмисних, але й до ненавмисних атак, дозволяє проводити аутентифікацію тільки зображень у градаціях сірого, збережених у форматах TIF і PNG.

Все сказане залишає актуальною проблему створення нових стеганографічних алгоритмів і методів для розв'язання *double*-задачі [6].

Метою роботи є розробка нового стеганографічного методу для розв'язання *double*-задачі, що забезпечує надійність сприйняття СП, і може бути застосованим до ЦЗ, збереженого у довільному форматі.

Для досягнення поставленої мети необхідно розв'язати завдання:

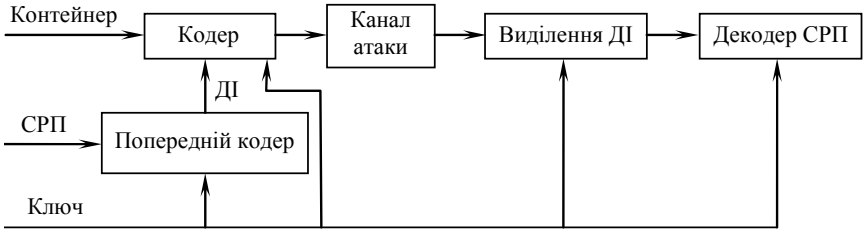
— організації процесу попереднього кодування секретного повідомлення таким чином, щоб сформована в результаті ДІ несла в собі поряд з секретною інформацією інформацію для розв'язання задачі аутентифікації контейнера;

— побудови секретного ключа, що використовується при попередньому кодуванні секретного повідомлення, а також при виділенні з СП ДІ, таким чином, щоб ці процеси були вільні від обчислювальної похибки;

— забезпечення можливості ефективної роботи розробленого методу в умовах неідеального каналу зв'язку з метою декодування переданої секретної інформації у разі порушення автентичності сигналу.

Основним математичним інструментом, що використовується в роботі, є матричний аналіз [7].

Позначимо $n \times m$ -матрицю монохромного ЦЗ, що використовується як контейнер, $\mathbf{F}$. Надалі будемо розрізняти ДІ та секретне повідомлення (СРП): під СРП розумітимемо інформаційне повідомлення, що передається адресату, до процесу попереднього кодування; під ДІ, як і раніше, розумітимемо повідомлення, яке безпосередньо вбудовується в контейнер. ДІ формується на основі СРП за допомогою секретного ключа (див. рисунок). Як СРП надалі розглядається довільно сформована бінарна послідовність $p_1, p_2, ..., p_l$, елементи якої належать множині $\{-1,1\}$.



Основні елементи використовуваної стеганосистеми

Основні кроки базового методу для вбудови СРП мають такий вигляд:

— Матриця **F** розбивається на $r \times r$-блоки, $r > 1$ (позначатимемо довільний $r \times r$-блок **B**). Кожний блок у базовому методі використовується для вбудови в нього 1 біта СРП.

— *Стеганоперетворення*. Нехай **B** — черговий блок ОП з елементами b_{ij}, $i, j = \overline{1,r}$, в який вбудовується черговий біт СРС p_k. Для **B** обирається найменше $b_{\min}$ і найбільше $b_{\max}$ значення яскравості пікселів блоку.

— *Побудова ключа*. По матриці **B** будується нижня трикутна $r \times r$-матриця **L**, елементи l_{ij} якої визначаються як

$$l_{ij} = \begin{cases} 0, \text{ якщо } i < j, \\ r, \text{ якщо } i = j, \\ 0, \text{ якщо } (i > j) \,\&\, \left(b_{ij} < \dfrac{b_{\min} + b_{\max}}{2} \right), \\ 1, \text{ якщо } (i > j) \,\&\, \left(b_{ij} \geq \dfrac{b_{\min} + b_{\max}}{2} \right). \end{cases}$$

Матриця **L** використовується для попереднього кодування елементів СРП.

— *Попереднє кодування*. Елементу p_k СРП ставиться у відповідність вектор $\mathbf{x_P}$ довжини r за наступним правилом:

$$\mathbf{x_P} = \mathbf{L}\mathbf{x},$$

де $\mathbf{x} = \left(p_k, p_k, ..., p_k, p_k \right)^T$ — вектор довжини r. Вектор $\mathbf{x_P}$ — складова частина ДІ, для якої виконується її безпосередня вбудова в контейнер.

— *Вбудова ДІ*. Елементи вектора $\mathbf{x_P}$ вбудовуються в блок **B** відповідно до обраного стеганографічного алгоритму (наприклад, адитивно). Результатом є блок СП із матрицею $\overline{\mathbf{B}}$. Вбудову елемента p_k завершено.

Побудова ключа — нижньої трикутної матриці може здійснюватися різними способами. Зокрема, нижній трикутник такої матриці може генеруватися довільним чином. Важливим є лише добра обумовленість цієї матриці, що гарантується відсутністю нулів на головній діагоналі.

Необхідно зауважити, що елементи вектора $\mathbf{x_P}$, отриманого як результат попереднього кодування, за модулем не перевищують $2r - 1$. Тому вибір розміру блоку r повинен проводитися таким чином, щоб навіть при адитивній вбудові ДІ надійність сприйняття СП порушена не була. Через те прийнятним тут буде $r \leq 8$ [3]. Взагалі ж надійність сприйняття СП в запропонованому методі забезпечується обраним для вбудови вектора $\mathbf{x_P}$ стеганографічним алгоритмом і ніяк не погіршується (поліпшується) самим методом.

Нехай $\overline{\mathbf{F}}$ — матриця аналізованого СП. Основні кроки алгоритму декодування СРП та перевірки автентичності:

— Матриця $\overline{\mathbf{F}}$ розбивається на $r \times r$-блоки. Кожний блок $\overline{\mathbf{B}}$ використовується для декодування з нього 1 біта СРП.

— Нехай $\overline{\mathbf{B}}$ — черговий блок СП з елементами b_{ij}, $i, j = \overline{1,r}$, з якого добувається черговий біт СРП p_k. Для добування:

— *Декодування ДІ*. З врахуванням використаного при вбудові ДІ стеганографічного алгоритму із блока $\overline{\mathbf{B}}$ СП за допомогою відповідного алгоритму добувається ДІ — вектор $\overline{\mathbf{x}}_\mathbf{P}$.

— *Побудова ключа*. По матриці $\overline{\mathbf{B}}$ будується нижня трикутна $r \times r$-матриця $\overline{\mathbf{L}}$, елементи $\bar{l}_{ij}$ якої визначаються аналогічно елементам матриці **L**,

ISSN 2076-2429 (print)
ISSN 2223-3814 (on line)

$$\bar{l}_{ij} = \begin{cases} 0, \text{ якщо } i < j, \\ r, \text{ якщо } i = j, \\ 0, \text{ якщо } (i > j) \,\&\, \left(\bar{b}_{ij} < \dfrac{\bar{b}_{\min} + \bar{b}_{\max}}{2} \right), \\ 1, \text{ якщо } (i > j) \,\&\, \left(\bar{b}_{ij} \geq \dfrac{\bar{b}_{\min} + \bar{b}_{\max}}{2} \right). \end{cases}$$

де $b_{\min}$ і $b_{\max}$ — відповідно мінімальний і максимальний елементи матриці $\bar{\mathbf{B}}$.

— *Декодування елемента СРП*. Для декодування елемента p_k СРП розв'язується відносно невідомого вектора $\bar{\mathbf{x}}$ система лінійних алгебраїчних рівнянь (СЛАР):

$$\bar{\mathbf{L}}\bar{\mathbf{x}} = \bar{\mathbf{x}}_{\mathbf{p}}. \quad (1)$$

— *Аналіз*. Якщо всі елементи отриманого вектора $\bar{\mathbf{x}}$ однакові й дорівнюють одиниці або –1, то порушення цілісності ОП не відбулося, при цьому в першому випадку $p_k = 1$, в другому – $p_k = -1$. Якщо ж не всі елементи $\bar{\mathbf{x}}$ однакові, або серед них є елементи, що відрізняються від 1, –1, то цілісність контейнера була порушена.

— *Декодування елемента СРП у випадку порушення цілісності контейнера.* Серед елементів вектора $\bar{\mathbf{x}}$ визначається значення x, яке зустрічається з максимальною частотою. Тоді

$$p_k = \begin{cases} 1, \text{ якщо } x = 1, \\ -1, \text{ якщо } x = -1, \\ \text{не визначено, якщо } x \notin \{-1, 1\}. \end{cases}$$

Матриці $\bar{\mathbf{L}}$ та $\mathbf{L}$ є невиродженими ($\det \mathbf{L} = \prod_{i=1}^{r} l_{ij} \neq 0$; $\det \bar{\mathbf{L}} = \prod_{i=1}^{r} \bar{l}_{ij} \neq 0$) й добре обумовленими. Дійсно, це нижні трикутні матриці з ненульовими елементами на головній діагоналі, що говорить про лінійну незалежність їх рядків (стовпців). Крім того, оскільки матриці мають діагональне переважання за побудовою, їх числа обумовленості Скіла є малими [3]. Це приводить до малої чутливості до збурних дій задачі декодування СРП: навіть наявність обчислювальної похибки при розв'язанні СЛАР (1) не призведе до значної похибки результату $\bar{\mathbf{x}}$ [8], що важливо при декодуванні елемента СРП у випадку порушення цілісності контейнера.

Зауваження 1. При побудові ключів $\bar{\mathbf{L}}$ та $\mathbf{L}$ елементи їх головних діагоналей можна прийняти такими, що дорівнюють одиниці. Це, залишивши матриці невиродженими, хоча і збільшить їх числа обумовленості, але залишить матриці добре обумовленими: лінійна незалежність їх рядків (стовпців) очевидно присутня завдяки трикутного вигляду $\bar{\mathbf{L}}$ та $\mathbf{L}$ й відсутності нулів на головних діагоналях [8]. Головною перевагою ключів такого виду буде відсутність обчислювальної похибки на кроці декодування розробленого методу. Таким чином, накопичення обчислювальної похибки в запропонованому методі може відбуватися тільки при роботі попередньо обраних конкретних стеганографічних алгоритмів вбудови і декодування ДІ.

Зауваження 2. На перший погляд може здатися, що процес попереднього кодування СРС можна звести тільки до отримання вектора $\mathbf{x} = (p_k, p_k, ..., p_k, p_k)^T$ і його подальшої вбудови в блок ОП як ДІ. Тоді про збереження цілісності буде свідчити рівність всіх елементів відповідного вектора $\bar{\mathbf{x}}$, отриманого при декодуванні ДІ, або одиницям, або –1. Але, враховуючи те, що вирішується не тільки завдання перевірки автентичності, але й секретної передачі даних, такий вид ДІ може призвести до дуже чутливого до збурних дій СП (наприклад, якщо буде здійснена адитивна вбудова): достатньо змінити значення яскравості відповідного пікселя, використаного

для вбудови, всього на ± 1, щоб вбудована інформація була загублена. Використання ж для попереднього кодування ще нижньої трикутної матриці $\mathbf{L}$ приводить до того, що СП, в кожний блок якого вбудований вектор $\mathbf{Lx}$, буде менш чутливим до збурних дій. Дійсно, якщо значення елементів вектора $\mathbf{Lx}$ збурити на ± 1, це дасть можливість відновити вектор $\mathbf{x} = \left(p_k, p_k, ..., p_k, p_k \right)^T$ більш точно при розв'язанні СЛАР, ніж при безпосередньому декодуванні [3].

Зауваження 3. Запропонований метод можна використовувати для довільного зображення-контейнера. Його стійкість не залежить ні від формату зберігання ЦЗ, ні від безпосередніх властивостей матриці ЦЗ, оскільки процес декодування відбувається шляхом розв'язання СЛАР з добре обумовленими (за побудовою) матрицями.

Зауваження 4. Стійкість запропонованого методу до стеганоаналізу буде визначатися стійкістю обраного для вбудови ДІ стеганографічного алгоритму.

Перевіримо справедливість зауваження 4.

Найбільш поширеними форматами для зберігання, передачі цифрових сигналів, зокрема, ЦЗ, є формати з втратами. Завдяки цьому контейнером доцільно застосовувати зображення, збережені, наприклад, у форматі JPEG з втратами, заснованому на дискретному косинусному або вейвлет-перетворенні. Перевіримо стійкість запропонованого в роботі стеганометода до стеганоаналізу, скориставшись для цього нещодавно розробленим універсальним для контейнера, що зберігається з втратами, стеганоаналітичним методом *SA_VV_OSJPEG* [9], який ґрунтується на детектуванні наявності збурень матриці цифрового зображення, що відбуваються в процесі СПР.

Розглянемо декілька стеганоалгоритмів, що реалізують безпосередню вбудову ДІ. При побудові ключів $\overline{\mathbf{L}}$ і $\mathbf{L}$ елементи їх головних діагоналей мають значення 1, $r = 8$.

Нехай СПР блока ОП здійснюється адитивно (що є одним з найпопулярніших сучасних способів вбудови ДІ) в r пікселів "контура" ЦЗ, відповідних $\mathbf{B}$, що визначаються таким чином. Для кожного пікселя блоку $\mathbf{B}$ з яскравістю b_{ij} обчислимо величину

$$S_{ij} = \begin{cases} \dfrac{\left|b_{ij} - b_{i,j-1}\right| + \left|b_{ij} - b_{i,j+1}\right| + \left|b_{ij} - b_{i-1,j}\right| + \left|b_{ij} - b_{i+1,j}\right|}{4}, \quad 1 < i < 8, 1 < j < 8, \\ \dfrac{\left|b_{1,j} - b_{1,j-1}\right| + \left|b_{1,j} - b_{1,j+1}\right| + \left|b_{1,j} - b_{2,j}\right|}{3}, \quad i = 1, 1 < j < 8, \\ \dfrac{\left|b_{8,j} - b_{8,j-1}\right| + \left|b_{8,j} - b_{8,j+1}\right| + \left|b_{8,j} - b_{7,j}\right|}{3}, \quad i = 8, 1 < j < 8, \\ \dfrac{\left|b_{i,1} - b_{i-1,1}\right| + \left|b_{i,1} - b_{i+1,1}\right| + \left|b_{i,1} - b_{i,2}\right|}{3}, \quad j = 1, 1 < i < 8, \\ \dfrac{\left|b_{i,8} - b_{i-1,8}\right| + \left|b_{i,8} - b_{i+1,8}\right| + \left|b_{i,8} - b_{i,7}\right|}{3}, \quad j = 8, 1 < i < 8, \\ \dfrac{\left|b_{11} - b_{12}\right| + \left|b_{11} - b_{21}\right|}{2}, \quad i = j = 1; \quad \dfrac{\left|b_{81} - b_{71}\right| + \left|b_{81} - b_{82}\right|}{2}, \quad i = 8, j = 1, \\ \dfrac{\left|b_{18} - b_{17}\right| + \left|b_{18} - b_{28}\right|}{2}, \quad i = 1, j = 8; \quad \dfrac{\left|b_{88} - b_{78}\right| + \left|b_{88} - b_{87}\right|}{2}, \quad i = j = 8, \end{cases}$$

яку назвемо усередненим стрибком функції яскравості для b_{ij}. Серед усіх значень b_{ij}, $i, j = \overline{1,8}$, оберемо 8 таких, для яких значення S_{ij} максимальні в межах розглянутого блока. В пікселі, відповідні обраним S_{ij}, буде здійснюватися вбудова ДІ.

ISSN 2076-2429 (print)
ISSN 2223-3814 (on line)

Після СПР отримані СП піддавалися стеганоаналізу. З цією метою в середовищі MathWorks Matlab проведено обчислювальний експеримент, в якому використовувалися 200 ЦЗ, збережених у форматі JPEG. В результаті стеганоаналізу методом *SA_VV_OSJPEG* наявність ДІ виявлено у 96 % тестованих СП.

Нехай СПР здійснюється одним з групи стеганоалгоритмів, які вбудовують ДІ шляхом певних збурень сингулярних чисел матриць, що відповідають контейнеру [3]. Ці алгоритми мають значну завадостійкість, а тому викликають певну зацікавленість в сенсі організації стеганографічного каналу зв'язку. Використання їх в процесі СПР в запропонованому стеганометоді дають зовсім іншу якісну картину в сенсі стійкості результату їх роботи до стеганоаналізу. В результаті обчислювального експерименту, організованого з тими ж 200 ЦЗ, наявність ДІ було виявлено лише в 3...5 % тестованих СП, що підтверджує справедливість зауваження 4.

При проведенні описаних обчислювальних експериментів оцінювалася ефективність роботи запропонованого стеганометода з різними стеганоалгоритмами, що використовувались в процесі СПР. В умовах відсутності збурних дій на СП, його автентичність була підтверджена в 100 % протестованих СП. Об'єм відновленої інформації [3] у цих умовах склав 100 %.

В умовах дій активного (зловмисного) порушника фіксація порушення автентичності відбувалася в 100 % розглянутих ЦЗ.

Для перевірки ефективності декодування в умовах дій активного порушника штучно створювалася ситуація порушення цілісності СП: воно піддавалося збурній дії, що моделювалася шляхом накладення на СП гаусовського шуму з нульовим математичним очікуванням і різними значеннями дисперсії $d = 0,000001...0,0001$. Такий спосіб моделювання активних атакуючих дій, спрямованих на СП, є одним із традиційних [10]. Об'єм відновленої інформації в цих умовах у середньому склав 82…99 %, що говорить про ефективну роботу запропонованого методу.

Висновки. Розроблено новий стеганографічний метод, що дозволяє одночасно вирішувати завдання прихованої передачі довільної інформаційної послідовності і аутентифікації контейнера, який допускає використання як основного повідомлення цифрового зображення, збереженого в довільному форматі. Вибір конкретного стеганографічного алгоритму при вбудові та декодуванні ДІ виділяє із розробленого методу конкретний алгоритм, що роз'язує *double*-задачу. Надійність сприйняття СП, сформованого методом, а також ступінь стійкості до стеганоаналізу визначається попередньо обраним для використання стеганографічним алгоритмом.

Розроблений метод припускає відсутність обчислювальної похибки у разі, якщо похибка округлення відсутня в обраному стеганоалгоритмі, який використовується безпосередньо для вбудови та відновлення ДІ; дозволяє ефективно вирішувати задачу секретної передачі інформації навіть в разі встановленого порушення автентичності.

Литература

1. Грибунин, В.Г. Цифровая стеганография / В.Г. Грибунин, И.Н. Оков, И.В. Туринцев. — М.: Солон-Пресс, 2002. — 272 с.
2. Стеганография, цифровые водяные знаки и стеганоанализ / А.В. Аграновский, А.В. Балакин, В.Г. Грибунин, С.А. Сапожников. — М.: Вузов. кн., 2009. — 220 с.
3. Кобозєва, А.А. Аналіз захищеності інформаційних систем / А.А. Кобозєва, І.О. Мачалін, В.О. Хорошко. — К.: Вид. ДУІКТ, 2010. — 316 с.
4. Маракова, И.И. Повышение эффективности сокрытия информации для систем с зашумленными каналами связи / И.И. Маракова, А.А. Яковенко // Інформатика та математичні методи в моделюванні. — 2012. — Т. 2, № 1. — С. 5 — 17.
5. Глумов, Н.И. Алгоритм встраивания полухрупких цифровых водяных знаков для задач аутентификации изображений и скрытой передачи информации / Н.И. Глумов, В.А. Митекин // Компьют. оптика. — 2011. — № 2, т. 35. — С. 262 — 267.
6. Authentication and Secret Message Transmission / D. Bhattacharyya, J. Dutta, P. Das and others // Int. J. Communications, Network and System Sciences. — 2009. — № 5. — P. 363 — 370.
7. Гантмахер, Ф.Р. Теория матриц / Ф.Р. Гантмахер. — М.: Наука, 1988. — 552 с.

8. Кобозева, А.А. Стеганографический метод, основанный на решении системы линейных алгебраических уравнений / А.А. Кобозева, А.В. Коломийчук // Пр. УНДІРТ. — Одеса, 2006. — № 1(45) — 2(46). — С. 104 — 109.
9. Бобок, И.И. Детектирование наличия возмущений матрицы цифрового изображения как составная часть стеганоанализа / И.И. Бобок // Вісн. Східноукр. нац. ун-ту ім. В. Даля. — Луганськ, 2011. — № 7(161). — С. 32 — 41.
10. Gkizeli, M. Optimal Signature Design for Spread-Spectrum Steganography / M. Gkizeli, D.A. Pados, M.J. Medley // IEEE Trans. On Image Processing. — Vol. 16, № 2. — P. 391 — 405.

References

1. Gribunin, V.G. Cifrovaja steganografija [Digital Steganography] / V.G. Gribunin, I.N. Okov, I.V. Turincev. — M.: Solon-Press, 2002. — 272 s.
2. Steganografija, cifrovye vodjanye znaki i steganoanaliz [Steganography, Digital Watermarking and Steganalysis] / A.V. Agranovskii', A.V.Balakin, V.G. Gribunin, S.A. Sapozhnikov. — M.: Vuzovskaja kniga, 2009. — 220 s.
3. Kobozєva, A.A. Analiz zahischenosti informacijnih system [Analysis of Information Systems Security] / A.A. Kobozєva, I.O. Machalin, V.O. Horoshko. — K.: Vid. DUIKT, 2010. — 316 s.
4. Marakova, I.I. Povyshenie effektivnosti sokrytija informacii dlja sistem s zashumlennymi kanalami svjazi [Improving the Information Hiding Effectiveness for Noisy Communication Channel Systems] / I.I. Marakova, A.A. Jakovenko // Informatika ta matematichni metodi v modeljuvanni [Informatics and Mathematical Methods in Modeling]. — 2012. — T. 2, № 1. — S. 5 — 17.
5. Glumov, N.I. Algoritm vstraivanija poluhrupkih cifrovyh vodjanyh znakov dlja zadach autentifikacii izobrazhenij i skrytoj peredachi informacii [An Algorithm of Embedding Semi-Fragile Watermarks for the Tasks of Image Authentication and Hidden Information Transmission] / N.I. Glumov, V.A. Mitekin // Komp'juternaja optika [Computer Optics]. — 2011. — № 2, t. 35. — S. 262 — 267.
6. Authentication and Secret Message Transmission / D. Bhattacharyya, J. Dutta, P. Das and other // Int. J. Communications, Network and System Sciences. — 2009. — № 5. — P. 363 — 370.
7. Gantmaher, F.R. Teorija matric [Theory of Matrices]/ F.R. Gantmaher. — M.: Nauka, 1988. — 552 s.
8. Kobozeva, A.A. Steganograficheskij metod, osnovannyj na reshenii sistemy linejnyh algebraicheskih uravnenij [Steganographic Method Based on Solving a System of Linear Algebraic Equations] / A.A. Kobozeva, A.V. Kolomii'chuk // Praci UNDIRT [Proceedings of Ukrainian Research Inst. Of Radio & Television]. — Odesa, 2006. — № 1(45) — 2(46). — S. 104 — 109.
9. Bobok, I.I. Detektirovanie nalichija vozmuschenij matricy cifrovogo izobrazhenija kak sostavnaja chast' steganoanaliza [Detection of Digital Image Matrix Disturbances as a Constituent of Steganalysis] / I.I. Bobok // Visnik Shidnoukr. nac. un-tu im. V. Dalja [Herald of the East-Ukrainian Nat. Dal University]. — Lugansk, 2011. — № 7(161). — S. 32 — 41.
10. Gkizeli, M. Optimal Signature Design for Spread-Spectrum Steganography / M. Gkizeli, D.A. Pados, M.J. Medley // IEEE Trans. On Image Processing. — Vol. 16, #. 2. — P. 391 — 405.

Рецензент канд. техн. наук, доц. Одес. нац. політехн. ун-ту Чечельницький В.Я.

Надійшла до редакції 20 вересня 2012 р.