УДК 681.3.06

А.А. ТАРАНЧУК, Л.Г. ГАЛЬПЕР, О.О. МАРЦЕНЮК
Хмельницький національний університет

# СТЕГАНОГРАФІЧНИЙ МЕТОД ПРИХОВУВАННЯ ДАНИХ В ОБЛАСТІ ЧАСТОТНИХ ПЕРЕТВОРЕНЬ ЗОБРАЖЕНЬ

*В роботі запропонований стеганографічний метод приховання інформації в нерухомі графічні зображення стиснених за стандартом JPEG. Доведено, що цифрові зображення формату JPEG є найбільш ефективними в стеганографії. Перевага цього формату пояснюється відсутністю ефективних методів виявлення та зміни повідомлень, які приховані в частотній області зображень*

*In this work is offered stenographical method of dissemble information in immovable graphical images compact in standard JPEG. It is proved, that digital images of size JPEG are more effective in stenography. Privilege of this size is explained by absence of effective methods of revelation and changes of messages, which are hidden in frequency field of images.*

**Вступ**

Стеганографія, як наукова дисципліна, знаходиться на стику цифрової обробки сигналів, теорії зв'язку і криптографії. Під цифровою стеганографією розуміють приховання одних даних в інших методами цифрової обробки сигналів **[1].**

Крім приховання даних, які передаються, методи стеганографії використовують для захисту авторських або майнових прав на цифрове зображення, фотографії або інші оцифровані витвори мистецтва.

Значна частина досліджень в області стеганографії присвячена прихованню конфіденційних повідомлень і цифрових водяних знаків в нерухомі зображення. Це пов'язано з тим, що при генерації зображення, як правило, використовується значна кількість елементарних графічних примітивів, що представляє особливий інтерес для стеганографічних методів захисту.

На даний момент, дослідниками зі всього світу запропонована достатньо велика кількість алгоритмів приховання інформації і цифрових водяних знаків (ЦВЗ) в графічні файли форматів, які використовують стиснення з втратами та без втрат. І хоча розробка методів впровадження ЦВЗ є на даний момент комерційно перспективнішим, значний інтерес проявляється і до створення методів приховання інформації.

Важливим недоліком існуючих алгоритмів приховання інформації є їх низька ефективність **[1]**. Тому метою даної роботи є виявлення основних критеріїв ефективності застосування цифрових зображень в стеганографії, а також визначення основних методів її підвищення.

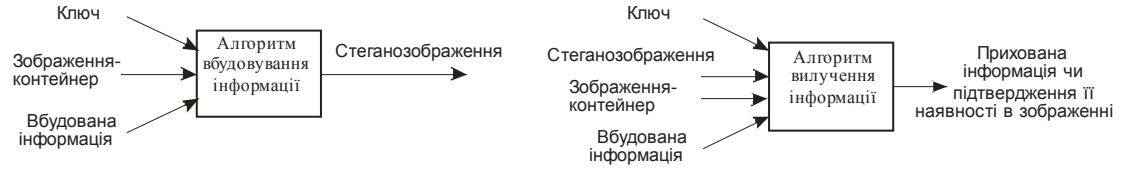
**1. Основні поняття і принципи стеганографії зображень**

Стеганосистема – система, яка здійснює приховання і виділення однієї бітової послідовності з іншої. Послідовність, яка підлягає утаєнню, називається повідомленням. Послідовність, в яку здійснюється приховання, називається контейнером. Якщо контейнером є зображення, то приховану інформацію простіше представити у вигляді двовимірного масиву біт. В цілях підвищення секретності приховання повідомлення в контейнер може здійснюватися за допомогою ключа. Якщо в контейнер не вбудовувалося повідомлення, то він називається порожнім, інакше – заповненим. Як правило, у складі стеганосистеми додатково виділяють підсистеми, такі як прекодер, стеганокодер, стеганодетектор, декодер **[2]**.

У будь-якій стеганосистемі важливу роль грає стеганографічний протокол – порядок дій, до яких вдаються дві або більше сторін, з метою вирішення певних завдань. Загальна схема приховання інформації в зображення та схема їх вилучення представлена на рис. 1, а і на рис. 1, б, відповідно.

При побудові стеганосистеми повинні враховуватися наступні положення, багато з яких лежать в основі критеріїв ефективності стеганографічних алгоритмів зображень:

- стеганосистема повинна мати прийнятну обчислювальну складність реалізації;
- заповнений контейнер повинен бути візуально непомітний від незаповненого;
- методи приховання повинні забезпечувати автентичність і цілісність секретної інформації для авторизованої особи;
- потенційний порушник має повне уявлення про стеганосистему і деталі її реалізації, єдине, що йому невідоме – це ключ, за допомогою якого тільки його власник може встановити факт наявності і зміст прихованого повідомлення;
- порушник повинен бути позбавлений будь-яких технічних і інших переваг в розпізнаванні або, принаймні, розкритті змісту секретних повідомлень.




**а)** **б)**

**Рис. 1. Загальна схема приховування інформації в зображення (а); б) схема вилучення інформації**

На даний час більшість досліджень в області стеганографії присвячені використанню стеганоконтейнерів нерухомих цифрових зображень [2].

Це обумовлено наступними причинами:

- розмір контейнера заздалегідь відомий;
- відсутні обмеження режиму передачі в реальному часі;
- можливість приховання інформації великого об'єму;
- слабка чутливість ока людини до деяких змін характеристик зображення.

Високорівневі властивості людського зору (ВЛЗ) рідко враховуються при побудові стеганоалгоритмів. Їх відмінністю від низькорівневих є те, що ці властивості виявляються «повторно», обробивши первинну інформацію від ВЛЗ мозок видає команди на її «підстроювання» під зображення (див. табл. 1) [3].

Таблиця 1

**Властивості системи людського зору**

| Низькорівневі | Високорівневі |
|---|---|
| 1. Чутливість до зміни яскравості зображення.<br>2. Частотна чутливість.<br>3. Ефект маскування. | 1. Чутливість до контрасту, розміру, місцеположенню, кольору, форми, зовнішнім подразникам.<br>2. Підвищена увага до зображень переднього плану. |

Стеганографія заснована на використанні наявної в зображеннях психовізуальної надмірності.

Око людини подібне до низькочастотного фільтру, якому непомітні спотворення у високочастотній області зображень. Це пов'язано з нерівномірністю амплітудно-частотної характеристики системи зору людини. Тому в стеганоалгоритмах часто використовуються ті ж перетворення, що і в сучасних алгоритмах стиснення (дискретне косинусне перетворення (ДКП) – в JPEG, вейвлет – перетворення – в JPEG2000). При цьому існують три можливості. Приховання інформації може проводитися в початкове зображення, або одночасно із здійсненням стиснення зображення-контейнера, або у вже стисле алгоритмом JPEG зображення. Другу з перерахованих вище можливостей, а саме приховання інформації одночасно із здійсненням стиснення зображення-контейнера у формат JPEG і пропонується застосувати в даній роботі.

Встановлено, що людський зір більше реагує на зміну яскравості, ніж колірного тону в зображенні, це пояснюється функціональними особливостями зору. Тому важливіше зберегти велику точність при передачі Y- компоненту яскравості, ніж при передачі Cb і Cr- компонент кольоровості.

Перетворення колірної моделі RGB в модель YCbCr здійснюється за допомогою наступних співвідношень [4]:

$$\begin{aligned} Y &= 0{,}299\,R + 0{,}587\,G + 0{,}114\,B \\ Cb &= -0{,}1687\,R - 0{,}3313\,G + 0.5\,B + 128 \\ Cr &= 0{,}5\,R - 0{,}4187\,G - 0{,}0813\,B + 128 \end{aligned} \qquad (1)$$

Процес вбудовування прихованої інформації в зображення в якомусь сенсі дуальний процесу їх стиснення. Приховання інформації часто здійснюють в незначущі області для того, щоб не змінити візуальне представлення зображення. Відомо, що стійкішими до різних спотворень, зокрема стиснення, є методи, які використовують для захована даних не часову, а частотну область **[1]**.

**2. Методи приховання в частотній області зображень**

Один з найбільш популярних методів приховання секретної інформації в частотній області зображення заснований на відносній зміні величин коефіцієнтів ДКП.

Дані перетворення можуть застосовуватися як до всього зображення, так і до деяких його частин. При цифровій обробці зображення часто використовується двовимірна версія ДКП [5]:

$$S(u,v) = \frac{2}{N} C(u)C(v) \sum_{x=0}^{N-1}\sum_{y=0}^{N-1} S(x,y) \cos\left(\frac{\pi u(2x+1)}{2N}\right) \cos\left(\frac{\pi u(2y+1)}{2N}\right),$$

$$S(x,y) = \frac{2}{N} \sum_{x=0}^{N-1}\sum_{y=0}^{N-1} C(u)C(v)S(u,v) \cos\left(\frac{\pi u(2x+1)}{2N}\right) \cos\left(\frac{\pi u(2y+1)}{2N}\right), \qquad (2)$$

де $C(u) = 1/\sqrt{2}$, якщо $u = 0$ і C *(u)*=1 в іншому випадку.

Для цього зображення розбивається на блоки розміром 8×8 пікселів (рис. 2), а потім до кожного блоку застосовується дискретне косинусне-перетворення (окремо для компонент Y, Cb і Cr).

У отримуваній матриці низькочастотні компоненти розташовані ближче до лівого верхнього кута, а більш високочастотні зміщуються вправо вниз (рис. 2). У зв'язку з тим, що основна частина графічних образів на екрані складається з низькочастотної інформації, використовуючи отриману матрицю можна диференційовано відкидати найменш важливу інформацію з мінімальними візуальними втратами.

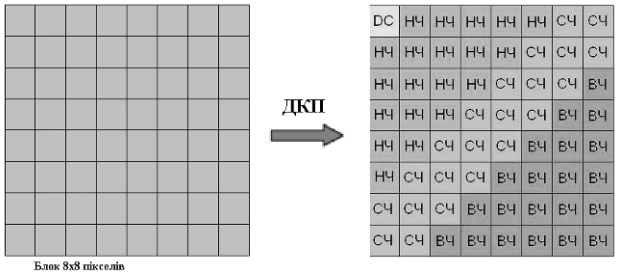



**Рис. 2. Блокове кодування. ДКП – дискретне косинусне – перетворення: DC – нульовий спектральний коефіцієнт, ВЧ – високочастотні коефіцієнти**

Придатними для приховання інформації вважаються блоки зображення, які не мають дуже м'яких переходів, а також ті, що не містять малого числа контурів. Для першого типу блоків характерна рівність нулю високочастотних коефіцієнтів, для другого типу – дуже великі значення декількох низькочастотних коефіцієнтів. Ці особливості і є критерієм відсікання непридатних блоків.

Кожен блок призначений для приховання одного біта секретного повідомлення. Процес приховування починається з вибору блоку $b_{i,}$ призначеного для кодування $i$-го біта повідомлення. Для вибраного блоку зображення $b_i$ проводиться ДКП: $B_i = D\{b_i\}$. При організації секретного каналу абоненти повинні заздалегідь домовитися про конкретні два коефіцієнти ДКП, які будуть використовувати для приховання секретних даних. Позначимо їх як $B_i$ $(u_2,v_2)$. Ці два коефіцієнти повинні відповідати косинус-функціям з середніми частотами, що забезпечить збереження інформації в істотних областях сигналу, яка не знищуватиметься при JPEG-стисканні. Оскільки коефіцієнти ДКП – середніх є подібними, то процес захования не внесе помітних змін до зображення.

Якщо для блоку виконується умова $B_i$ $(u_l, v_l) > B_i$ $(u_2,v_2)$, то вважається, що блок кодує значення 1, інакше – 0. На етапі вбудовування інформації вибрані коефіцієнти міняють між собою значення, якщо їх відносний розмір не відповідає кодованому біту.

На кроці квантування JPEG-стиснення (етап на якому кожний елемент отриманої матриці коефіцієнтів ДКП ділиться націло на відповідний коефіцієнт матриці квантування (рис. 3)) може впливати на відносні розміри коефіцієнтів, тому, додаючи випадкові значення до обох величин, алгоритм гарантує що $B_i$ $(u_l, v_l) > B_i > x$, де $x > 0$. Чим більше $x$, тим алгоритм буде стійкішим до стиснення. Після відповідного коректування коефіцієнтів виконується зворотне ДКП **[6]**.

Вилучення прихованої інформації проводиться шляхом порівняння вибраних двох коефіцієнтів для кожного блоку.

Шаги квантування для області нижніх частот

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 6 | 4 | 4 | 6 | 9 | 11 | 12 | 16 |
| 4 | 5 | 5 | 6 | 8 | 10 | 12 | 12 |
| 4 | 5 | 5 | 6 | 10 | 12 | 14 | 19 |
| 6 | 6 | 6 | 11 | 12 | 15 | 19 | 28 |
| 9 | 8 | 10 | 12 | 16 | 20 | 27 | 31 |
| 11 | 10 | 12 | 15 | 20 | 27 | 31 | 31 |
| 12 | 12 | 14 | 19 | 27 | 31 | 31 | 31 |
| 16 | 12 | 19 | 28 | 31 | 31 | 31 | 31 |

Шаги квантування для області високих частот

**Рис. 3. Типова матриця квантування**

Останній етап роботи алгоритму кодування JPEG-стискання. Після обробки матриці ДКП за допомогою матриці квантування, в результаті у вихідній матриці появляється велика кількість нулів, особливо в високочастотній області (правий нижній кут (рис. 4)).

Першим кроком, значення в лівому верхньому куті матриці заміняється на відносне. Оскільки сусідні блоки зображення похожі між собою, то кодування наступного елемента (0,0) через різницю з попереднім буде більш ефективним. Другим кроком – використання самого алгоритму кодування повторів (LZW), для обробки більшої кількості нулів, які знаходяться рядом. Експеременті тестування показали, що кращих результатів можна досягти, якщо обходити матрицю зигзагом, як показано на рис. 4 [6].

Третім останнім кроком – отриманий результат стискається як звичайні дані за допомогою алгоритму Хаффмана або арифметичного кодування залежно від реалізації. Цей етап називається «кодування ентропії» (в термінології JPEG) [4].

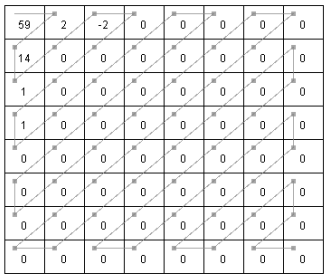



**Рис. 4. Порядок обходу матриці зигзагом**

### 3. Критерії ефективності застосування цифрових зображень в стеганографії

Під терміном «ефективність» в стеганографії розумітимемо можливість вирішення за допомогою цифрових зображень основних завдань стеганографії: швидко і скритно передавати великі об'єми інформації. Існує дуже велика кількість чинників, які впливають на ефективність стеганографії цифрових зображень.

Проаналізуємо найбільш важливі критерії ефективності застосування цифрових зображень в стеганографії:

а) скритність або стеганографічна стійкість. Задоволення вимозі скритності є обов'язковим для абсолютно будь-якої стеганосистеми. У застосуванні до графічної стеганосистеми, стійкість пов'язана із змінами (спотвореннями), які вносяться до початкового зображення при прихованні повідомлення. Вимога стійкості вважається невиконаною, якщо зображення піддається атаці за допомогою простого візуального аналізу. Така стеганосистема володіє украй низькою ефективністю і не може знайти практичного застосування, оскільки не відповідає мінімальному рівню безпеки (рис. 1).

1 2

**а) б)**

**Рис. 5. Результат роботи алгоритму, що не відповідає вимогам стійкості: 1 – початкове зображення, 2 – зображення з вбудованим повідомленням**

б) розмір прихованого повідомлення. Ефективність використання цифрового зображення для зберігання секретної інформації значною мірою визначається максимальним можливим розміром секретного повідомлення. Як правило, чисельно цей критерій характеризується процентним співвідношенням між об'ємом прихованого повідомлення і початковим об'ємом контейнера. Тому необхідно використовувати механізми, які дозволяють варіювати балансом між скритністю і розміром повідомлення, що підвищує ефективність вбудовування за рахунок додання йому універсальних якостей: один і той же контейнер може забезпечувати як підвищену скритність, так і збільшені розміри прихованого повідомлення (рис. 5).

**а) б)**

**Рис. 6. Результат приховання інформації в JPEG зображення: а) пустий контейнер (розширення 800x600, розмір 123665 байт), б) заповнений контейнер (розширення 800x600, розмір 125015 байт, вбудовано 40196 біт)**

в) стійкість до модифікації заповненого контейнера (стисненню). Стійкість до модифікації характеризує вірогідність відновлення повідомлення за умови деякої модифікації заповненого контейнера. Окремим випадком модифікації є стиснення з втратами. Підвищення стійкості до стиснення здійснюється шляхом ретельного дослідження алгоритмів компресії з метою визначення областей контейнера, що не піддаються модифікаціям. Традиційним і достатньо могутнім способом боротьби з «перешкодами» може служити збільшення надмірності прихованого повідомлення (рис. 7).

г) використовуваний графічний формат. В значній мірі ефективність застосування цифрових зображень в стеганографії залежить від формату їх зберігання.

BMP JPEG 100% JPEG 75% JPEG 50% JPEG 25% JPEG 0%

**а) б) в) г) д) е)**

**Рис. 7. Спотворення прихованої інформації при стисненні: а) початкове зображення; б) – е) приховане зображення витягнуте з контейнера, стислого з різним ступенем**

Формат BMP, що мав широке розповсюдження у минулому, сьогодні втратив свої позиції. Не дивлячись на велику кількість алгоритмів і техніки вбудовування інформації у файли цього формату, його

не можна назвати ефективним з погляду сучасної стеганографії. По-перше, його застосування в даний час вельми обмежене. По-друге, відносно контейнерів у форматі BMP розроблена велика кількість методів виявлення прихованого повідомлення, що також знижує ефективність формату.

Одним з найбільш поширених в мережі Інтернет форматів є формат GIF, який використовує алгоритм стиснення без втрат. Відсутність втрат при компресії дозволяє використовувати для захована інформації ті ж алгоритми, що і для не стиснених зображень. Проте, це не вирішує проблеми виявлення прихованого повідомлення. До того ж, обмеженість розміру колірної палітри обмежує можливості використання його для зберігання цифрових фотографій (які є найбільш затребуваним видом контейнерів).

Найбільш ефективним виглядає формат JPEG, який використовується для зберігання переважної більшості цифрових фотографій.

**Висновки**

Проведений в роботі аналіз найбільш важливих критеріїв ефективності застосування цифрових зображень для задач стеганографії показав, що більш стійкішим до різних спотворень, зокрема стиснення зображень, є метод стиснення нерухомих зображень за допомогою алгоритму JPEG, який використовує для приховання даних частотну область зображень заснований на відносній зміні величин коефіцієнтів ДКП.

Описані вище методи дозволяють більш повніше реалізувати потенціал стискання за стандартом JPEG цифрових зображень у відношенні вбудовування інформації. Завдяки використання цього методу розмір прихованого в контейнер повідомлення приблизився до 4 % від величини контейнера.

**Література**

1. Грибунин В.Г., Оков И.Н., Туринцев И.В. Цифровая стеганография. – М.: СОЛОН-Пресс, 2002. – 258 с.

2. Оков И.Н. О требуемой пропускной способности каналов передачи аутентифицированных сообщений в безусловно стойких системах // Проблемы информационной безопасности. Компьютерные системы. – 2000. – № 3 (7). – С. 78-64.

3. Конахович Г. Ф., Пузыренко А. Ю. Компьютерная стеганография. Теория и практика. – К.: «МК-Пресс», 2006. – 288 с.

4. Voloshynovskiy S., Pereira S., Iquise V., Pun T. Attack Modeling: Towards a Second Generation Watermarking Benchmark // Preprint. University of Geneva, 2001. 58p.

5. Романец Ю.В., Тимофеев П.А., Шаньгин В.Ф. Защита информации в компьютерных системах и сетях/Под ред. В.Ф. Шаньгина. – 2-е изд., перераб. и доп. – М.: Радио и связь, 2001. – 376 с.

6. Watson A. The cortex transform: rapid computation of simulated neural images // Computer Vision, Graphics, and Image Processing. 1987. Vol. 39. № 3. P. 311-327.

Надійшла 18.3.2009 р.

УДК 621.396.6.001.63-621.396.001.65 615.47-114: 616-07-08

А.Т. БОГОРОШ
Київський національний університет «КПІ», Україна
Л.П. РИБАК
Хмельницький національний університет, Україна
А. БУБУЛІС
Каунаський технологічний університет, Литва

# РОЗРОБКИ ПРИНЦИПІВ ПОБУДОВИ СЕНСОРІВ БІОМЕДИЧНОГО ЗАСТОСУВАННЯ

*У статті вирішуються проблеми визначення сучасного стану розробки принципів побудови біосенсорів на основі магнітних принципів вимірювального перетворення.*

*In the article the problems of determination of the modern state of development of principles of construction of touchcontrols decide on the basis of magnetic principles of measuring transformation.*

**Вступ**

Домінуючою тенденцією розвитку сучасних сенсорних пристроїв є розширення їх функціональних можливостей, підвищення точності вимірювання та мінімізація масогабаритних параметрів. Найвищою ступінню такого розвитку стали автоматизовані сенсори, визначальними характеристиками яких є самодіагностика, термостабілізація, автоматичний вибір функції перетворення тощо.

**Метою** даної роботи є визначення сучасного стану розробки принципів побудови, схемотехнічних рішень та програмного забезпечення автоматизованих магнітних біосенсорів для діагностики інфекційних захворювань.

В узагальнюючому виді процес розробки біосенсорів для діагностики інфекційних захворювань може бути представленим складовими, які охоплюють: