УДК 621.382

# ХАРАКТЕРИСТИКИ ОЦІНКИ ЯКОСТІ СТЕГОСИСТЕМ

**Шостак Н.В.**
*Харківський національний університет радіоелектроніки, Україна*
*E-mail: Natasha9246@yandex.ru*

**Characteristics of quality assessment stehosystem**

Reviewed steganosystem as a transmission system. Methods of hiding information in fixed images are studied. Characteristics of the steganosystem using different methods of embedding are presented.

Способи і методи приховування секретних повідомлень відомі з давніх часів, причому, дана сфера людської діяльності отримала назву стеганографія. Стеганографія - один із способів захисту інформації від несанкціонованого доступу, у системах моніторингу мережевих ресурсів, а також для захисту авторських прав на деякі види інтелектуальної власності та для автентифікації цифрових об'єктів [1]. В якості носія прихованої інформації в роботі використовується зображення, що допускає спотворення власної інформації, які не порушують його функціональність.

Один із методів приховування інформації в просторовій області є метод Куттера-Джордана-Боссена [2]. Цей метод полягає у вбудовуванні повідомлення в канал синього кольору зображення, що має кодування RGB. Функції вбудовування і видобування в даному алгоритмі не симетричні, тому правильне розпізнавання біта повідомлення хоч і є високоймовірним, але не стовідсоткове.

Для вбудовування інформації в контейнер використовуватися синій колір заданого контейнера-зображення. Зображення будемо розглядати в колірній моделі RGB.

Розглянемо алгоритм передачі одного біту прихованої інформації в цьому методі. Нехай $M_i$ – біт, що підлягає вбудовуванню, $C=\{R,G,B\}$ – зображення-контейнер, $p=(x,y)$ - псевдовипадковий піксель контейнера, у який буде виконуватись вбудовування.

Таємний біт $M_i$ вбудовується в канал синього кольору шляхом модифікації яскравості - $\lambda_{x,y} = 0{,}29890 \cdot R_{x,y} + 0{,}58662 \cdot G_{x,y} + 0{,}11448 \cdot B_{x,y}$

Інший метод приховування інформації в просторовій області – метод Дармстедтера-Делейгла-Квісквотера-Макка. Цей метод є блочним методом вбудовування в просторову область контейнера. Перед вбудовуванням інформація перетворюється в вектор двійкових даних. Кожний біт вбудовується в окремий блок пікселів розмірність якого складає 8×8 (для забезпечення відповідності блокам, що використовуються під час JPEG-компресії). Таким чином, дія компресії рівномірно розподіляється на кожен вбудований біт, а зважаючи на збитковість вбудовування зростає загальна стійкість стегосистеми. Розглянемо процес вбудовування біт повідомлення більш детально. Процес вбудовування виконується в чотири етапи:

1. Розбиття масиву зображення-контейнера на блоки 8×8 пікселів.

2. Класифікація пікселів окремого блока на зони з приблизно однорідним значенням яскравості.

3. Розбиття кожної зони на категорії відповідно до індивідуальної (псевдовипадкової) маски.

4. Вбудовування біта в залежності від співвідношення між середніми значеннями категорій кожної зони шляхом модифікації значень яскравості кожної категорії в кожній зоні.

Вилучення вбудованої інформації з контейнера вимагає наявності відомостей про розмірності блоків, на які розбивається зображення, а також про конфігурацію масок, які використовувалися при вбудовуванні. Процес вилучення складається з наступних етапів:

1. Розбиття зображення на блоки розмірністю NxN.

2. Класифікація пікселів окремого блоку на зони.

3. Розподіл кожної зони на категорії.

4. Зіставлення середніх значень яскравості для визначення значення вбудованого біта даних.

Один з найбільш поширених на сьогодні методів приховування конфіденційної інформації в частотній області зображення полягає у відносній заміні величин коефіцієнтів ДКП [3]. Спочатку зображення розбивається на блоки розмірністю 8×8 пікселів. ДКП застосовується до кожного блоку, в результаті чого утворюються матриці 8×8 коефіцієнтів ДКП. Кожний блок з яких призначений для приховання одного біту даних. Недоліком цього методу є висока складність обчислення ДКП. Розглянемо метод більш детально.

На початковому етапі первинне зображення розбивається на блоки розмірністю 8×8 пікселів. ДКП застосовується до кожного блоку, в результаті чого отримують матриці 8×8 коефіцієнтів ДКП, де b - номер блоку контейнера C, a - позиція коефіцієнта в цьому блоці. Кожен блок при цьому призначений для приховання одного біта даних.

Під час організації прихованого каналу абоненти повинні попередньо домовитися про два конкретні коефіцієнти ДКП з кожного блоку, які будуть використовуватися для приховування даних. Зазначені коефіцієнти повинні відповідати косинус-функції з середніми частотами, що забезпечить прихованість інформації в суттєвих для ЗСЧ областях сигналу, до того ж інформація не буде спотворюватися при JPEG-компресії з малим коефіцієнтом стиснення.

Бенгам (D. Benham), Мемон (N. Memon), Ео (B.-L. Yeo) і Юнг (M. Yeung) запропонували оптимізовану версію методу відносної заміни величин коефіцієнтів ДКП(методу Коха-Жао). Причому оптимізація була проведена ними за двома напрямками: по-перше, було запропоновано для вбудовування використовувати не всі блоки, а лише найбільш підходящі для цього, по-друге, в частотній області блоку для вбудовування вибираються не два, а три коефіцієнти ДКП, що, як буде показано надалі, істотно зменшує спотворення контейнера.

Стеганографія може бути застосована для приховання зв’язку, захисту авторських прав на зображення (автентифікація), відбитків пальців (відстеження порушника) додавання заголовків до зображень, додавання додаткової інформації, такої як субтитри до відео, захисту цілісності зображень (виявлення випадків шахрайства), управління копіюванням при DVD записі та в інтелектуальних браузерах, для автоматичного надання інформації про авторські права. Всі ці наведені методи проаналізовані і оцінені з використанням такого набору характеристик, які є показниками якості:

- пропускна здатність – кількість бітів прихованого повідомлення, які можуть бути передані за допомогою цього методу в зображенні фіксованого розміру. При цьому приховуване повідомлення повинне бути безпомилково передане одержувачу і захищене від атак порушника, таких як спроби виявлення факту наявності каналу прихованої зв'язку, читання прихованого повідомлення, навмисного введення помилкового повідомлення або руйнування вбудованої в контейнер інформації [4].

- стійкість – здатність вилучити приховану інформацію після загальних операцій з обробки зображень: лінійні і нелінійні фільтри, стиснення з втратами, регулювання контрастності, перефарбування, передискретизації, масштабування, обертання, додавання шуму, обрізки, друку/копіювання/сканування, перестановки пікселів у малій околиці, квантування кольорів тощо;

- невидимість – перцепційна прозорість, що спирається на властивості зорової або слухової системи людини;

- захищеність – характерна властивість, яка означає, що вбудована інформація не може бути видалена цілеспрямованими атаками, заснованими на відомому алгоритмі вбудовування та вилучення і знанні принаймні одного носія з прихованим повідомленням;

- складність вбудовування і виявлення – кількість стандартних операцій, які будуть виконані для вбудовування і виявлення прихованого повідомлення.

Напрямком подальших досліджень є вибір переважного методу приховування інформації в стегосистемі з використанням багатокритеріального підходу.

## Література


1. В.Г. Грибунин, И.Н. Оков, И.В. Туринцев. Цифровая стеганография. – М.: «Солон-Пресс», 2002. – 272 с.
2. M. Kutter, F. Jordan, F. Bossen, Digital Signature Of Color Images Using Amplitude Modulation //Proc.Of the SPIE Storage and Retrieval for Image and Video Databases V. 1997. Vol. 3022. Pp. 518-526.
3. Конахович Г. Ф., Пузыренко А. Ю. Компьютерная стеганография. Теория и практика. – К.: МК-Пресс, 2006. – 288 с.
4. Cox, I., Miller, M., Bloom, J., Fridrich, J., Kalker, T. Digital Watermarking and Steganography. Second Edition. (Elsevier, 2008).