УДК 004.056

СИНТЕЗ СТЕГАНОГРАФІЧНОГО МЕТОДУ, ЕФЕКТИВНОГО ЗА КРИТЕРІЯМИ НАДІЙНОСТІ ТА ЗАХИЩЕНОСТІ

О.О. Вовк, А.А. Астраханцев
Харківський національний університет радіоелектроніки

Abstract *– Was carried out the complex analysis of the most relevant data hiding algorithms by multi-objective optimization. Own method of embedding information in still pictures was synthesized based on the advantages and disadvantages of the existing algorithms. New algorithm used additional blocks of cropping and stability under the previous image processing. This ensured the reliability of the system and increased the probability of correct recognition of embedded data. Was carried out the comparative analysis of the existing and proposed steganographic system based on quantitative and qualitative characteristics. Synthesized method showed excellent results regarding the most common methods. And showed resistance to statistical stegoanalysis, finding no significant deviations of calculated parameters. Also calculated characteristics indicated a high level of invisibility of steganographic embeddings by the developed method.*

Анотація *– Проведено комплексний аналіз найактуальніших стеганографічних методів приховування даних. Синтезовано власний метод вбудовування інформації у нерухомі зображення. Оцінено можливість методів адаптуватись до характеристик реальних каналів зв'язку. Продемонстровано надійність та захищеність стеганографічних систем на основі запропонованого методу..*

Аннотация *– Проведен комплексный анализ самых актуальных стеганографических методов скрытия данных. Синтезирован собственный метод встраивания информации в неподвижные изображения. Оценена возможность методов адаптироваться к характеристикам реальным каналам связи. Продемонстрирована надежность и защищенность стеганографических систем на основе предложенного метода.*

Вступ

Стеганографія являє собою перспективну науку, яка може бути успішно застосована для вирішення широкого спектру задач. Одним з її напрямів, що стрімко набуває не аби якого поширення у всіх сферах життя, є вбудовування цифрових водяних знаків. Цифровий водяний знак (ЦВЗ) – це спеціальна мітка, яка непомітно розміщується у зображення або інший сигнал [1] з метою тим чи іншим чином захистити інформацію від несанкціонованого копіювання, відстежувати розповсюдження інформації у мережах зв'язку, забезпечувати пошук інформації в мультимедійних базах даних.

У всі часи була потреба передати інформацію так, щоб її не зміг отримати потенційний зловмисник. Стеганографія ж допомагає виключити саму імовірність того, що потенційний порушник, чи то злодій, чи необережний користувач отримає

інформацію про те, що зображення є контейнером, що зберігає в собі приховані дані. Отже, високу увагу необхідно приділяти саме передачі цифрових зображень мережами зв'язку. А зважаючи на сучасні технології, необмежені можливості користувачів телекомунікаційних систем та цікавість науковців до стегоаналізу, існує гостра необхідність у застосуванні алгоритмів приховування даних, що здатні забезпечити надійність та захищеність даних, що передаються у прихованому вигляді.

I. Огляд існуючих стеганографічних методів приховування даних у цифрових зображеннях

На сьогоднішній день існує велика кількість методів приховування даних у цифрових зображеннях. Найбільш поширені методи використовують просторові і частотні області для приховування інформації.

Методи приховування інформації в просторовій області вбудовують секретні дані в області первинного зображення. Загальний принцип цих методів полягає в заміні надлишкової, малозначимої частини зображення бітами секретного повідомлення [2]. Їх перевага полягає в тому, що для вбудовування не потрібно виконувати обчислювально складні і тривалі перетворення зображень. Але в більшості своїй вони мають низьку стеганографічну стійкість до атак як пасивного, так і активного порушників. Основний недолік таких методів – висока чутливість до спотворень контейнера [3].

Більш стійкими до різноманітних спотворень, в тому числі і компресії, є методи, що використовують для приховування даних частотну область контейнера [4].

Існує декілька способів представлення зображення в частотній області. При цьому використовується та чи інша декомпозиція зображення, що застосовується в якості контейнера [5]. Наприклад, існують методи на основі використання дискретного косинусного перетворення (ДКП), дискретного перетворення Фур'є (ДПФ), вейвлет-перетворення (ВП), перетворення Карунена-Лоєва (ПКЛ) і деякі інші [6], [10]. Подібні перетворення можуть застосовуватися або до окремих частин зображення, або до зображення в цілому.

Найбільш актуальними на даний момент вважаються: найпоширеніший метод заміни найменш значущого біта [1, 2], метод Куттера-Джордана-Боссена [2, 7] як один з кращих в просторової області, модифікований метод Коха-Жао [2, 8] як один з основних в частотній області, метод Бенгама-Мемона-Ео-Юнга, що є вдосконаленням попереднього [2, 9], метод, заснований на ДВП [11-15] та методи, засновані на розширенні спектра [16, 17].

Використовуючи метод багатокритеріальної оптимізації в роботі [18] було проведено порівняльний аналіз найактуальніших методів з урахуванням важливості характеристик стеганографічних алгоритмів, таких як пропускна спроможність, стійкість, невидимість, захищеність, складність вбудовування та складність виявлення. В результаті було отримано зважену оцінку якості методів, яка представлена коефіцієнтом *WW* (табл. 1).

Таблиця 1. Порівняння методів з врахуванням важливості (ваги) характеристик

Метод (*a*)	Значення (*WW*)
заміни найменш значущих бітів	0,200
Куттера-Джордана-Боссена	0,149
Коха-Жао	0,151
Бенгама-Ео-Юнга	0,121
із розширенням спектра	0,139
засновані на ДВП	0,240

Таким чином, при комплексному порівнянні методів вбудовування інформації для прихованої передачі мережами зв'язку найкращий результат показали інтегровані методи, засновані на ДВП [18].

II. Синтез методу для підвищення надійності та захищеності

Спираючись на результати дослідження переваг і недоліків існуючих методів вбудовування інформації [4], [12], [18-20], було розроблено власний метод стеганографічного приховування інформації. Схема, що відтворює запропонований метод, зображена на рис. 1 у вигляді алгоритму. Алгоритм був реалізований у програмному середовищі Matlab 2014a у вигляді окремих скриптів приховування (Insertion.m) та вилучення (Extraction.m). Суть розробленого стеганографічного методу полягає в тому, що зображення та секретна інформація піддаються попередній обробці для підвищення загальної надійності та стійкості стегосистеми.

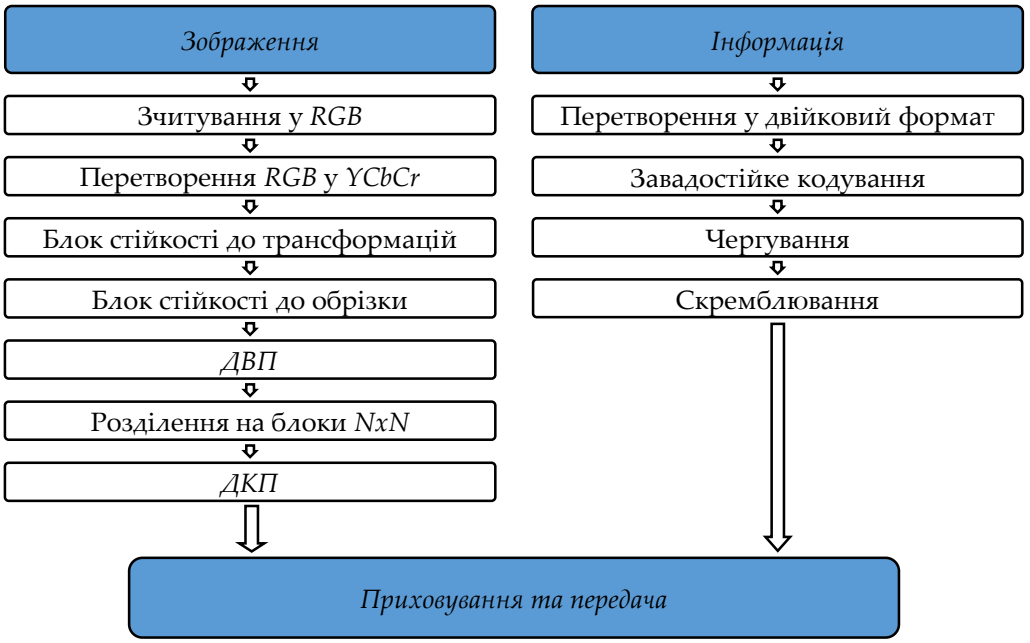

Рис. 1. Запропонована стеганографічна система приховування даних у цифрове зображення

Обробка зображення

Зображення зчитується у звичному форматі адитивної колірної моделі *RGB*. Але потім виконується перетворення у просторове кодування *YCbCr* за допомогою формул:

$$Y = 0{,}299R + 0{,}587G + 0{,}114B,$$
$$Cb = 128 + (37{,}797R - 74{,}203G + 112B),$$
$$Cr = 128 + (112R - 93{,}786G - 18{,}214B).$$

Для приховування використовується *лише* синій компонент різниці кольорів Cb колірного простору $YCbCr$.

В ході алгоритму вбудовування передбачається визначення блоку стійкості до трансформації. Це дозволяє отримувачу інформації виявити геометричні маніпуляції і виконати зворотні трансформації (якщо можливо), які були виконані із зображенням в процесі передачі. *Для* цього у зображення впроваджується 5 точок: центр зображення і вершини трапеції, описаної навколо кола радіусом R (рис. 2). Параметри трапеції обрані таким чином, щоб верхня основа була удвічі менша за нижню:

$$a = \sqrt{2}R.$$

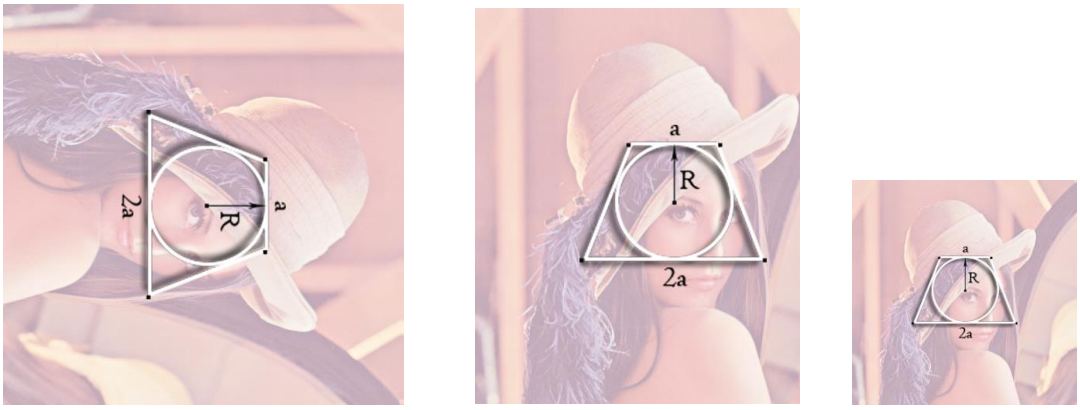

Рис. 2. Впроваджуваний шаблон і приклади трансформацій, які можливо детектувати: поворот, обрізка, маштабування

Наступним етапом є визначення блоку стійкості до обрізки. Він регулюється за допомогою коефіцієнта обрізки *N*, який визначається як відсоток пікселів з кожної сторони зображення, які недопустимі для приховування. Цей блок визначає розміри допустимого простору для приховування інформації.

До зображення застосовується дискретне вейвлет-перетворення (ДВП) і обирається область вертикальних (HL_1) і горизонтальних (LH_1) коефіцієнтів перетворення (рис. 3).

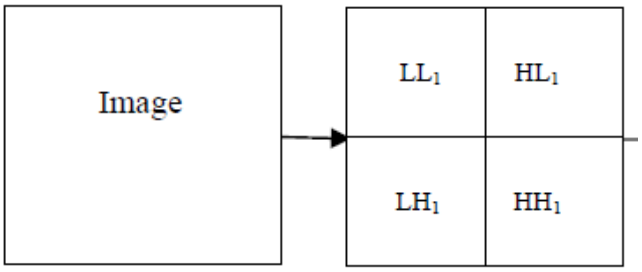

Рис. 3. Коефіцієнти *ДВП*

Безпосередньо вбудовування секретного повідомлення відбувається у коефіцієнти, отримані шляхом застосування ДКП до попередньо підготовленого простору зображення. Для цього обрані ДВП області зображення-носія (LH_1 та HL_1) розбиваються на блоки розмірами 8×8 пікселів. ДКП застосовується до кожного блоку:

$$\Omega(\upsilon,\nu)=\frac{\xi(\upsilon)\cdot\xi(\nu)}{\sqrt{2N}}\cdot\sum_{x=0}^{N-1}\sum_{y=0}^{N-1}C(x,y)\times\cos\left[\frac{\pi\cdot\upsilon\cdot(2x+1)}{2N}\right]\cdot\cos\left[\frac{\pi\cdot\nu\cdot(2y+1)}{2N}\right],$$

де $C(x,y)$ – елементи оригінального зображення розмірністю $N\times N$; x,y – просторові координати пікселів зображення; $\Omega(\upsilon,\nu)$ – масив коефіцієнтів ДКП; (υ,ν) – координати в частотній області; $\xi(\upsilon)=\frac{1}{\sqrt{2}}$, якщо $\upsilon\approx 0$, і $\xi(\upsilon)=1$, якщо $\upsilon>0$.

Внаслідок цього отримуємо матриці 8×8 коефіцієнтів ДКП, які позначають як $\Omega_b(\upsilon,\nu)$, де b – номер блоку контейнера C, а (υ,ν) – позиція коефіцієнта в цьому блоці.

Далі на основі секретного ключа генерується псевдовипадкова послідовність, та у відповідності до неї вибирається по одному блоку $\Omega_b(\upsilon,\nu)$ для приховування кожного b-го біта повідомлення.

Під час організації секретного каналу абоненти повинні завчасно домовитися про два конкретні коефіцієнти ДКП з кожного блоку, які використовуватимуться для приховання даних. Дані коефіцієнти задаються їх координатами в масивах коефіцієнтів ДКП: (υ_1,ν_1) і (υ_2,ν_2). Окрім цього, вказані коефіцієнти повинні відповідати косинус-функціям з середніми частотами, що забезпечить прихованість інформації в суттєвих для ЗСЛ областях сигналу, до того ж інформація не спотворюватиметься при JPEG-компресії з малими коефіцієнтами стиснення. При реалізації алгоритму змінювалися коефіцієнти $(\upsilon_1=4,\nu_1=5)$ і $(\upsilon_2=5,\nu_2=4)$.

Вбудовування інформації здійснюється таким чином, щоб різниця абсолютних значень коефіцієнтів ДКП перевищувала деяку позитивну величину P, наприклад $P=50$, при передачі біта «0», а для передачі біта «1» ця різниця робиться меншою в порівнянні з цією ж негативною величиною P:

$$\begin{cases} \left|\Omega_b(\upsilon_1,\nu_1)\right| - \left|\Omega_b(\upsilon_2,\nu_2)\right| > P, \ при \ \ m_b = 0; \\ \left|\Omega_b(\upsilon_1,\nu_1)\right| - \left|\Omega_b(\upsilon_2,\nu_2)\right| < -P, \ при \ \ m_b = 1. \end{cases}$$

Обробка інформації

Для підвищення стійкості впроваджуваної інформації до впливу випадкових перешкод в каналі передачі даних інформація, що підлягає приховуванню, попередньо кодується кодом корекції помилок. У розробленій системі використовується код Хемінга (8, 12), що дозволяє підвищити ймовірність правильного прийому символу в середньому на 55% із відношенням сигнал/шум в межах 20-40 дБ.

Після застосування завадостійкого коду ми зменшуємо імовірність групових помилок і підвищуємо криптографічну стійкість стегосистеми за допомогою процедур чергування та скремблювання.

III. Порівняльний аналіз методів

Для того, щоб продемонструвати переваги розробленого методу необхідно провести порівняльний аналіз найактуальніших стеганографічних методів. На сьогоднішній час уваги заслуговують наступні методи:

A1 – метод заміни найменш значущих біт (НЗБ) [1, 2];

A2 – метод Куттера-Джордана-Боссена [2, 7];

A3 – метод Коха-Жао [2], [8];

A4 – метод Бенгама-Мемона-Ео-Юнга [2, 9];

A5 – методи із розширенням спектра [11 – 15];

A6 – методи, засновані на *Д*ВП [16, 17].

Порівняння стеганографічних методів з використанням багатокритеріальної оптимізації

В ході дослідження доцільно взяти за основу результати, отримані в роботі [18], де проводився порівняльний аналіз вищезгаданих методів методом попарних порівнянь. Використовуючи методику оцінювання, запропоновану в роботі [18], були отримані порівняльні оцінки методів *A1 – A6 для* кожної з характеристик стеганографічних систем, таких як пропускна спроможність, невидимість, захищеність, складність вбудовування та складність виявлення. Оцінка була дана об'єктивним шляхом, результати наведені в табл. 2 у вигляді нормованих коефіцієнтів.

Виходячи з отриманих результатів, можна однозначно стверджувати, що методи, засновані на вейвлет-перетворенні (*A6*), виявляють найліпші властивості щодо невидимості та захищеності системи відносно інших найпоширеніших методів приховування даних *для* передачі мережами зв'язку. Під захищеністю мається на увазі

стійкість стеганографічної системи до стегоаналізу. Необхідно також відзначити хороші показники методів вбудовування у частотну область зображення (*A3*, *A4*, *A5*).

Таблиця 2. Нормовані коефіцієнти характеристик для стеганографічних методів

Метод	Пропускна здатність	Невидимість/ прихованість	Захищеність	Складність вбудовування	Складність виявлення
A1	0,509	0,147	0,018	0,453	0,453
A2	0,261	0,147	0,049	0,291	0,291
A3	0,038	0,044	0,216	0,120	0,120
A4	0,023	0,076	0,216	0,072	0,072
A5	0,106	0,293	0,120	0,044	0,044
A6	0,063	0,293	0,381	0,020	0,020

Кількісні оцінки

Для порівняльного оцінювання якості стеганографічних засобів можна використовувати загальновідомі показники, що дають кількісні оцінки [2]. Вони оперують із зображеннями на рівні пікселів.

Якість стегосистем, що наведені у цій роботі, оцінювалась за такими характеристиками:

– відношення сигнал/шум (*SNR*), що є безрозмірною величиною, рівною відношенню корисного сигналу до шуму. Чим більше це відношення, тим менше шум спотворює зображення:

$$SNR = \frac{\sum_{x,y}\left(C_{x,y}\right)^2}{\sum_{x,y}\left(C_{x,y} - S_{x,y}\right)^2};$$

– нормована середня абсолютна різниця (*NAD*), що показує ступінь відмінності між вихідним контейнером і контейнером з вбудованим секретним файлом, розраховується в такий спосіб:

$$NAD = \frac{\sum_{x,y}\left|C_{x,y} - S_{x,y}\right|}{\sum_{x,y}\left|C_{x,y}\right|};$$

– якість зображення (*IF*) є однією з основних оціночних характеристик для стегоалгоритмів, які працюють із зображеннями. Тому що візуальна атака заснована на здатності зорової системи людини аналізувати зорові образи й виявляти істотні роз-

ходження в зображеннях. Вона характеризує ступінь відповідності порожнього контейнера до заповненого:

$$IF = 1 - \frac{\sum_{x,y}\left(C_{x,y} - S_{x,y}\right)^2}{\sum_{x,y}\left(C_{x,y}\right)^2};$$

– середньоквадратична похибка (*MSE*):

$$MSE = \frac{1}{X \cdot Y}\sum_{x,y}\left(C_{x,y} - S_{x,y}\right)^2;$$

– середня абсолютна різниця (*AD*), що визначає середнє значення модуля різності між пікселями порожнього і заповненого контейнеру. Велике значення *AD* вказує на низьку якість зображення:

$$AD = \frac{1}{X \cdot Y}\sum_{x,y}\left|C_{x,y} - S_{x,y}\right|.$$

В цих співвідношеннях через $C_{x,y}$ позначається піксель пустого контейнера з координатами (x, y), а через $S_{x,y}$ – відповідний піксель заповненого контейнера.

Методи були протестовані на зображеннях різних розмірів, а саме: *128x128*, *256x256*, *512x512*, *1024x1024*, *2048x2048* пікселів, з різною потужністю приховування для розробленого алгоритму: *P = 50*, *30*, *10*, *5*.

Результати розрахунку запропонованих характеристик наведені в табл. 3.

Таблиця 3. Результати порівняння характеристик розробленого та існуючих методів. Тестове зображення розміром *128x128*, контейнер заповнений повністю

Показн. Викривл	**Ориг.**	**Розроб. метод (P=50)**	**Розроб. метод (P=30)**	**Розроб. метод (P=15)**	**Розроб. метод (P=5)**
AD	0	0,649	0,539	0,456	0,406
SNR	∞	9375	19040	34983	46978
IF	1	≈1	≈1	≈1	≈1
MSE	0	2,113	1,04	0,566	0,422

Показн. Викривл	**Коха-Жао (P=0.5)**	**Коха-Жао (P=25)**	**НЗБ**	**Розшир. спектру**	**Куттера**	**Бенгама**
AD	9,5	11,400	0,494	0,006	4,588	3,042
SNR	197,42	137,69	4975	41480	192,2	781,6
IF	0,995	0,993	≈1	≈1	0,995	0,998
MSE	124,4	178,3	0,494	0,006	235,7	–

Порівнюючи кількісні та якісні характеристики, отримані шляхом побітового порівняння оригінального та спотвореного контейнера, можна зробити висновок, що розроблений метод є стійким до статистичного аналізу і не видає прихованого повідомлення суттєвими відхиленнями показників.

Порівняння завадостійкості систем прихованої передачі

Для того щоб оцінити можливість методів на основі вейвлет-перетворення адаптуватись до реальних каналів зв'язку, був створений програмний комплекс, що імітує обрані канали. Після накладання певних завад були оцінені порогові значення спотворень, для яких ще можливе відновлення прихованої інформації.

Для досліджень було обрано наступні канали зв'язку:

1) Канал із адитивним білим гаусовим шумом, який можна описати станом сигналу на виході та його складовими:

$$Z(t) = \gamma u(t-\tau) + N(t) = s(t) + N(t),$$

де $N(t)$ – гаусів адитивний шум із нульовим математичним очікуванням та заданою кореляційною функцією. Часто при аналізі можна не враховувати τ, що відповідає зміні початку відліку часу на виході каналу.

Дана модель вдало описує багато провідних каналів, радіоканалів при зв'язку у прямій видимості, а також радіоканали з повільними загальними завмираннями, при яких можна точно передбачити значення γ та τ.

2) Канал із мультиплікативною завадою, що описується як дискретний симетричний канал без пам'яті, у якому кожен переданий символ може бути прийнятий помилково із фіксованою ймовірністю $P_{помилки}$ та вірно із ймовірністю $1-P_{помилки}$. Імовірність помилкового прийому не залежить від передісторії передачі.

Мультиплікативні завади обумовлені сторонньою зміною коефіцієнта передачі каналу зв'язку (рис.4).

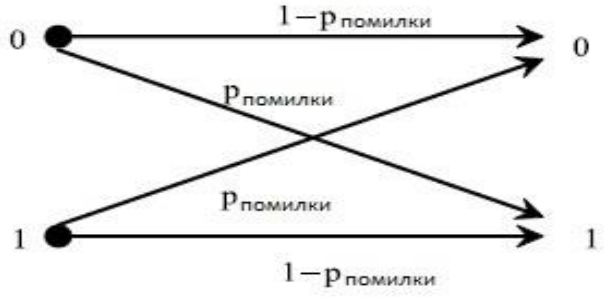

Рис. 4. Модель каналу з мультиплікативною завадою

3) Двійковий канал із стиранням, який працює так, що кожен переданий біт або правильно прийнятий без помилок, або повністю втрачений з ймовірністю

$P_{стирання}$. Під цим розуміють прийом замість «1» або «0» якогось третього символу (символу стирання), що вказує на позицію спотвореного символу (рис. 5).

Такий канал зустрічається в сучасних мережах з комутацією пакетів, високошвидкісних каналах супутникового зв'язку, тощо.

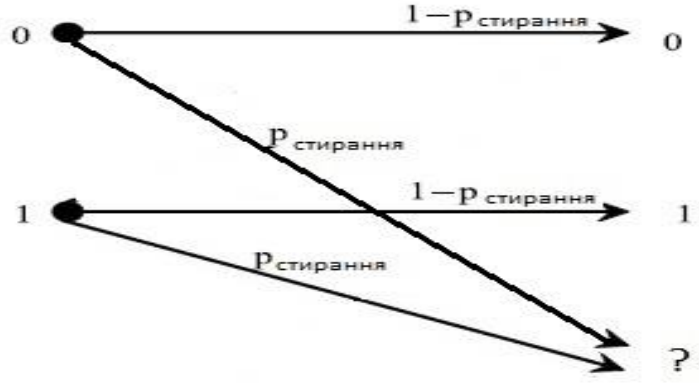

Рис. 5. Модель каналу зі стираннями

Розроблений програмний комплекс дозволяє працювати із двома типами файлів (bmp та txt) та трьома моделями каналу зв'язку. При цьому кожен файл подається в бінарному коді, отже канал впливає на інформацію побітово.

Основними результатами є отримані порогові значення спотворень, для яких ще можливе відновлення прихованої інформації (табл. 4).

Таблиця 4. Порогові значення спотворень контейнера для відновлення інформації

Метод	Канал з АБГШ, $\sigma_{завади}^2$	Канал із мультиплікативною завадою, $P_{помилки}$, %	Канал зі стираннями, $P_{стирання}$, %
A1	0,2	1	1
A2	0,2	1	1
A3	0,2	0,3	0,3
A4	0,2	0,03	0,03
A6	0,2	0,5	0,5
ДВП-ДКП (P=50)	0,2	1,4	1,4

Також були розраховані кількісні показники для оцінки методів, що досліджуються. На рис. 6 та рис. 7 представлені графіки усереднених характеристик SNR та NAD на порогових значеннях спотворень контейнерів. Тобто по осі ординат відкладені мінімальні значення SNR для кожного з методів, при якому можливе правильне вилучення прихованої інформації (рис. 6), і максимальні показники NAD відповідно (рис. 7).

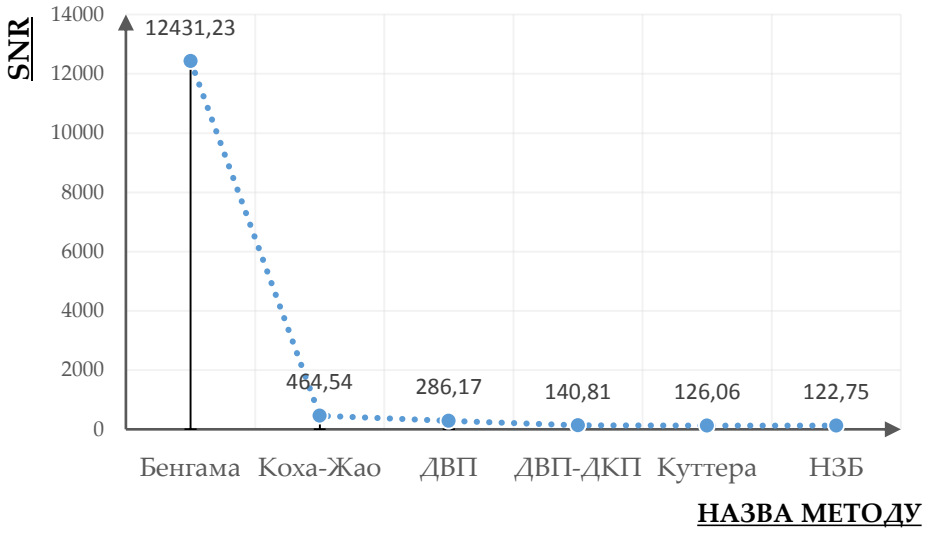

Рис. 6. SNR для порогових значень спотворень для кожного з методів

Отже, найменшого рівня SNR для вилучення вбудованого повідомлення після передачі у каналі зв'язку із завадами потребують стеганографічні методи, що використовують просторову область зображення.

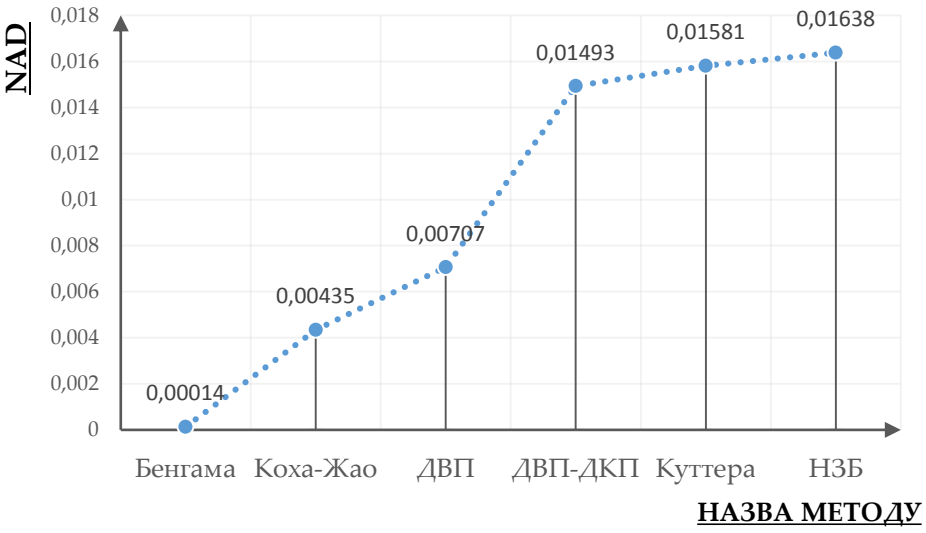

Рис. 7. NAD для порогових значень спотворень для кожного з методів

Вимоги до співвідношення сигнал/шум (SNR) збільшуються із збільшенням складності реалізації методу вбудовування, а нормована середня абсолютна різниця має обернено-пропорційний зв'язок.

Запропонований метод ДВП-ДКП демонструє показники на рівні найкращих, в той час як інші потребують значно вищого рівня SNR для детектування прихованого повідомлення.

Висновки

Провівши аналіз методів та характеристик оцінювання стеганографічних методів, для досліджень був обраний метод багатокритеріальної оптимізації [18]. На його основі було проведено комплексний аналіз найактуальніших методів приховування даних. Відштовхуючись від переваг та недоліків розглянутих методів був синтезований власний метод вбудовування інформації у нерухомі зображення.

Науковою новизною у розробці стеганографічного методу є використання додаткових блоків обрізки та стійкості при попередній обробці зображення. Вони дозволяють отримувачу інформації виявляти геометричні маніпуляції і виконувати зворотні трансформації, які були виконані із зображенням в процесі передачі. Це забезпечує надійність системи та підвищує імовірність правильного розпізнавання вкладених даних.

Для об'єктивного підтвердження переваг запропонованого методу були розраховані кількісні та якісні показники існуючих та запропонованої стеганографічної системи, на основі чого було проведено порівняльний аналіз. Синтезований метод показав відмінні результати відносно найпоширеніших методів та проявив стійкість до статистичного стегоаналізу, не виявивши суттєвих відхилень розрахованих показників. Також розраховані характеристики свідчать про високий рівень невидимості стеганографічних вкладень розробленим методом.

Вперше було оцінену можливість методів, що досліджувалися, адаптуватись до характеристик реальних каналів зв'язку. Були оцінені порогові значення спотворень, для яких ще можливе відновлення прихованої інформації. Перерахувавши величину завад у порогові значення SNR, при якому можливе вилучення прихованої інформації, отримали висновок, що запропонований метод володіє характеристиками на рівні найкращих. В той час, як більшість стеганографічних методів потребує вищого рівня SNR для детектування вбудованого повідомлення. Таким чином, синтезований метод вбудовування даних володіє високою стійкістю не тільки до навмисних атак, але і до завад у каналах зв'язку.

Список літератури:

1. *Грибунин В.Г.* Цифровая стеганография / В.Г. Грибунин, И.Н. Оков, И.В. Туринцев. — М.: СОЛОН-Пресс, 2002. — 272 с.

2. *Конахович Г.Ф.* Комп'ютерна стеганографія. Теорія і практика / Г. Ф. Конахович, А. Ю. Пузиренко. – Київ: МК-Пресс, 2006. — 288 с.

3. *Fidrich J.* Steganography in Digital Media: Principles, Algorithms, and Applications / J. Fidrich — Cambridge: Cambride University Press, 2009. — 438 с.

4. *Jadav. Y.* Comparison of LSB and Subband DCT Technique for Image Watermarking / Jadav, Y. // Conference on Advances in Communication and Control Systems 2013. — 2013. — P. 398-401.

5. Digital Watermarking and Steganography. Second Edition / I. Cox, M. Miller, J. Bloom, J. Fridrich, T. Kalker — Elsevier, 2008. — 592 p.

6. Watermarking / Edited by *Das Gupta*, M. — Croatia: InTech, 2012. – Vol. 1. — 212 p.

7. *Kutter. M.* A fair benchmark for image watermarking systems / M. Kutter, F. Petitcolas // Proc. of SPIE: Security and Watermarking of Multimedia Contents, 14-15 June 1999, San Jose, France. — 1999. — Volume 3657.— P. 226–239.

8. *Koch. E.,*Toward robust and hidden image copyright labeling / E. Koch, J. Zhao // Proc. of IEEE Workshop on Nonlinear Signal and Image Processing, 20-22 June 1995, Neos Marmaras, Greece. — 1995. — P. 456-459.

9. *Benham. D.* Fast watermarking of DCT-based compressed images / D. Benham, N. Memon, B. L. Yeo, M. Yeung, // Proc. of Int Conf Image Science, Systems, and Technology, 1997, Las Vegas, NV. — 1997. — P. 243-253.

10. Image Steganography Techniques: An Overview / *H. Nagham, Y. Abid, R. Badlishah Ahmad, Osamah M. Al-Qershi* // International Journal of Computer Science and Security. — 2012. — Volume 6, Issue 3. — P. 168-187.

11. *Добеши И.* Десять лекций по вейвлетам. — Ижевск, 2011. — 464 с.

12. *Лукічов В.В.* Методи та засоби стеганографічного захисту інформації в комп'ютерних системах і мережах на основі вейвлет-перетворень // Автореф. дис. канд. техн. наук: спец. 05.13.21. — К., 2010. — 20 с.

13. *Буй Т. Т. Ч.* Разложение цифровых изображений с помощью двумерного дискретного вейвлет-преобразования и быстрого преобразования Хаара / Т. Т. Ч. Буй, В. Г. Спицын // Известия Томского политехнического университета: Управление, вычислительная техника и информатика, 2011 . — Т. 318, № 5. - Томск: Томский политехнический университет. — С. 73-76.

14. *Daubechies I.* Orthonormal basis of compactly supported wavelets // Comm. Pure Appl. Math, v. XLI. —1988. — P. 909-996.

15. *Лагун А.Е.* Використання вейвлет-перетворення для приховування інформації в нерухомих зображеннях / А. Е. Лагун, І. І. Лагун // Вісник Національного університету "Львівська політехніка". Автоматика, вимірювання та керування. – 2013. – № 774. – С. 60-65. – Режим доступу: http://nbuv.gov.ua/j-pdf/**VNULP** 2013 774 11.pdf.

16. *Marvel L.M.* Capacity of the additive steganographic channel, Methodology of Spread-Spectrum. Image Steganography / L. M. Marvel, C.G. Boncelet Jr., Charles T. Retter // Proc. of IEEE transactions on image processing, August 1999. — 1999. — Vol.8, No.8. — PP. 1075-1083.

17. *Fridrich J.* Secure steganographic methods for palette images / *J. Fridrich, D. Rui* // In Inter'l Workshop on Information Hiding. —1999. — P. 47–60.

18. *Вовк О.О.* Розроблення методики оцінювання важливості характеристик стеганографічних алгоритмів / О.О. Вовк, А.А. Астраханцев // Вісник національного університету «Львівська політехніка» «Інформаційні системи та мережі», Львів: НУ ЛП, 2014. – №805. — С. 52-60.

19. *Sridev T., Kumar V.V.* A Robust Watermarking Algorithm Based on Image Normalization and DC Coefficients // IJCSI International Journal of Computer Science Issues. — 2011. — P. 226 – 232.

20. *Jiansheng M.* A Digital Watermarking Algorithm Based On DCT and DWT / *M. Jiansheng, L. Sukang, T. Xiaomei*// Proc. of the 2009 International Symposium on Web Information Systems and Applications. — 2009. — P. 104-107.