ВСЕУКРАЇНСЬКИЙ КОНКУРС СТУДЕНТСЬКИХ НАУКОВИХ РОБІТ З ПРИРОДНИЧИХ, ТЕХНІЧНИХ ТА ГУМАНІТАРНИХ НАУК

СТУДЕНТСЬКА НАУКОВА РОБОТА

МЕТОД ПІДВИЩЕННЯ ПРОПУСКНОЇ СПРОМОЖНОСТІ СКРИТОГО КАНАЛУ ДЛЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ ОБРОБКИ ТА ПЕРЕДАЧІ ВІДЕОІНФОРМАЦІЙНИХ РЕСУРСІВ

Шифр: Приховування

Галузь наук: Інформаційні технології

Харків – 2019

АНОТАЦІЯ

Шифр: "ПРИХОВУВАННЯ"

Галузь: Інформаційні технології

Актуальність роботи підтверджується необхідністю пошуку нових стеганографічних методів приховування даних.

Мета роботи полягає в підвищенні ефективності систем прихованої передачі інформації у телекомунікаційних системах на основі стеганографічного методу з високими показниками стійкості та пропускної здатності.

Завдання наукової роботи полягає в дослідженні методів цифрової стеганографії.

Використана методика дослідження. В роботі використовувались методи дискретного вейвлет – перетворення, Бенгама – Мемона – Ео – Юнга, найменш значущого біта, метод Коха – Жао.

Виявлено, що для приховування відеоінформаційних ресурсів потребуються складні обрахування , тому для більш якісного приховування інформації пропонується використовувати комбінований метод на основі дискретного вейвлет – перетворення та Бенгама – Мемона – Ео – Юнга.

Загальна характеристика роботи. Робота включає 4 розділи, висновки, літературу. Обсяг роботи 23 сторінки, таблиць - 6, рисунків - 6, джерел інформації - 9.

Ключові слова: цифрова стеганографія, зображення – контейнер, дискретно – косинусне перетворення, дискретне вейвлет - перетворення.

ПЛАН

1 ПОСТАНОВКА ЗАВДАННЯ НА ДОСЛІДЖЕННЯ

Обмеження на використання криптографічних засобів у ряді країн світу та виникнення проблеми захисту прав власності на інформацію, представлену в цифровому вигляді зумовлюють популярність досліджень у сфері стеганографії. З появою глобальних комп'ютерних мереж доступ до інформації значно збільшився, що призвело до підвищення загрози порушення безпеки даних при відсутності заходів їх захисту. Історично напрямок стеганографії з'явився першим, але потім багато в чому був витісненим криптографією.

Спільною рисою цих способів є те, що приховуване повідомлення вкраплюється в деякий нешкідливий об'єкт, який не привертає увагу. Інтерес до стеганографії відродився в останні 15 років, що пояснюється широким поширенням мультимедійних технологій і появою нових типів каналів зв'язку.

Методи стеганографії дозволяють не тільки приховано передавати дані, але й успішно вирішувати завдання завадостійкої автентифікації, захисту інформації від несанкціонованого копіювання, відстеження поширення інформації мережами зв'язку, пошуку інформації в мультимедійних базах даних. Ці обставини дозволяють у рамках традиційно існуючих інформаційних потоків або інформаційного середовища вирішувати важливі питання захисту інформації ряду прикладних галузей.

Актуальність дослідження надійний захист інформації від несанкціонованого доступу є не вирішеною в повному обсязі проблемою. В сучасному світі широко застосовуються і бурхливо розвиваються телекомунікаційні системи в усіх сферах діяльності людини.

Тому, гостро постає питання захисту інформації. Одним з можливих рішень задачі підвищення інформаційних систем є застосування методів цифрової стеганографії.

Метою дослідження є підвищення ефективності систем прихованої передачі інформації на основі стеганографічного методу з високими показниками стійкості та пропускної здатності.

2 АНАЛІЗ МЕТОДІВ ПІДВИЩЕННЯ ПРОПУСКНОЇ СПРОМОЖНОСТІ МЕТОДІВ ЦИФРОВОЇ СТЕГАНОГРАФІЇ

Для забезпечення додаткової завадостійкості необхідно забезпечити підвищення пропускної спроможності, оскільки використання методів завадостійкого кодування чи дублювання інформації вимагає передачі додаткових біт.

В ході досліджень було визначено два методи підвищення пропускної здатності при використанні методів вбудовування в область перетворення.

Рисунок 2.1 – Приклад блоку коефіцієнтів ДКП складової яскравості

Перший метод базується на твердженні, що вбудовування у середньочастотні коефіцієнти ДКП забезпечить достатню стійкість зображення, оскільки вони зазвичай не піддаються модифікаціям та втратам

збоку алгоритмів стиснення. В той же час людське око не володіє такою високою чутливістю, щоб відчути зміни цих коефіцієнтів. Тому запропоновано метод, що максимально використовує середньочастотні компоненти зображення. Приклад блоку коефіцієнтів ДКП складової яскравості приведений на рис. 2.1. Де: НЧ - низькі частоти; СЧ - середні частоти; ВЧ - високі частоти.

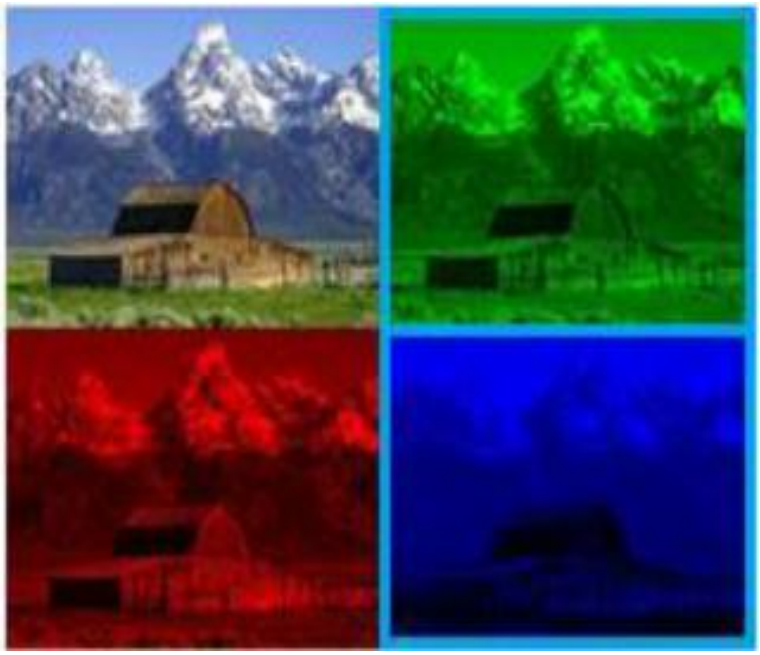

Рисунок 2.2 - Використання матриці *B* та *G, R* для вбудовування повідомлення

Другий метод підвищення стійкості зображення використовує для вбудовування не тільки синю матрицю зображення, як це прийнято у загальновідомих методах, але також зелену та червону. Для використання даного методу рекомендується використовувати в якості контейнерів зображення із перевагою зеленого або червоного кольору і без великих однотонних ділянок (рис. 2.2).

3 КРИТЕРІЇ ОЦІНКИ МЕТОДІВ ЦИФРОВОЇ СТЕГАНОГРАФІЇ

Сьогодні запропонована дуже велика кількість різних стеганографічних методів, деякі з них є універсальними, інші призначені для широкого кола завдань. Для порівняльного оцінювання якості стеганографічних засобів можна використовувати загальновідомі показники, що дають кількісні та якісні оцінки.

Для порівняльного оцінювання ефективності стеганографічних засобів використовуються існуючі кількісні показники, які оперують із зображеннями на рівні пікселів, хоча після належної адаптації вони можуть бути застосовні й до інших способів опису зображення, а також до аудіо даних:

– відносна стеганографічна ємність $w_{відн}$ стеганографічної системи.

Значення відносної стеганографічної ємності показує процентне відношення об’єму $w_{вбуд}$ вбудовуваної інформації відносно об’єму $w_{поч}$ ЗК. Дана величина використовується для оцінки ефективності стеганографічної системи по питомому об'єму вбудовуваної інформації відносно об'єму ЗК. Величина $w_{відн}$ відносної стеганографічної ємності системи обчислюється за наступною формулою:

$$w_{відн} = \frac{w_{вбуд}}{w_{поч}}, \tag{3.1}$$

$$w_{вбуд} = \frac{3 \cdot z_{рядк} z_{стовп}}{\omega}, \tag{3.2}$$

де $z_{рядк}$ – розмір зображення оригіналу по вертикалі;

$z_{стовп}$ – розмір зображення оригіналу по горизонталі;

ω – кількість елементів необхідних для вбудовування 1 біта.

У відсотках значення відносної стеганографічної ємності системи оцінюється на основі наступного виразу:

$$w_{відн} = \frac{w_{вбуд}}{w_{поч}} \cdot 100\% . \qquad (3.3)$$

– ймовірність $P_{вил}$ безпомилково вилучених даних авторизованим користувачем.

Дана величина використовується для оцінки безпомилково вилученої інформації при авторизованому доступі. Дана ймовірність обчислюється за наступною формулою:

$$P_{вил} = \frac{w_{вил}}{w_{вбуд}}, \qquad (3.4)$$

де $w_{вбуд}$ – об'єм вбудовуваної інформації, біт;

$w_{вил}$ – об'єм безпомилково вилучених даних, біт.

У випадку, коли $P_{вил}$ приймає значення одиниці, кількість безпомилково вилучених вбудованих даних авторизованим користувачем дорівнює 100%.

– пікове відношення сигнал шум (ПВСШ) h зображення з вбудованими данимим при неавторизованому доступі вимірюється в дБ.

Дана величина характеризує візуальні спотворення, які вносяться в ЗК в процесі вбудовування та обчислюється за наступною формулою:

$$h = 20\lg(255 / СКВ), \qquad (3.5)$$

де $СКВ$ – середнєквадратичне відхилення зображення з вбудованими даними відносно ЗК і обчислюється на основі наступної формули:

$$СКВ = \sqrt{\frac{\sum_{i=1}^{z_{рядк}} \sum_{j=1}^{z_{стовп}} (a_{ij} - a'_{ij})}{z_{рядк} z_{стовп}}}, \quad (3.6)$$

де a_{ij}, a_{ij}`– елементи відповідно початкового і стеганографічно перетвореного зображення;

$z_{рядк}$ – розмір зображення оригіналу по вертикалі;

$z_{стовп}$ – розмір зображення оригіналу по горизонталі.

Чим більше значення ПВСШ, тим менше візуальних спотворень вноситься до зображення в процесі вбудовування.

До найважливіших якісних характеристик стеганографічних систем, утворених з використанням різних методів, відносяться:

– пропускна здатність.

Кількість бітів прихованого повідомлення, які можуть бути передані за допомогою цього методу в зображенні фіксованого розміру;

– стійкість.

Здатність вилучити приховану інформацію після загальних операцій з обробки зображень: лінійні і нелінійні фільтри (розмитість, підвищення різкості, медіанна фільтрація), стиснення з втратами, регулювання контрастності, перефарбування, передискретизації, масштабування, обертання, додавання шуму, обрізки, друку, копіювання, сканування, перестановки пікселів у вузькій околиці квантування кольорів тощо. Поняття стійкості не виключає атаки на метод вбудовування, які ґрунтуються на знанні алгоритму приховування або вилучення. Стійкість означає, стійкість до «сліпих», нецільових модифікацій, або загальних операцій з зображеннями;

– невидимість.

Характеристика, що відповідає за неспроможність людського зору виявити стеганографічне повідомлення без використання 28 спеціальних

засобів. Це поняття спирається суто на властивості зорової системи людини (ЗСЛ).

Прихована інформація вважається непомітною, якщо середньостатистична людина не здатна відрізнити носій з прихованою інформацією від носія без неї. Загальноприйнята схема експерименту (так званий сліпий тест), що часто використовується в психовізуальних експериментах, засновується на тому, що суб'єктам пропонується в довільному порядку велика кількість носіїв із вбудованою інформацією і без, та пропонується обрати, які саме носії містять приховані дані. Відзначимо, що поняття невидимості може бути визначене й іншим способом та бути пов'язаним із статистичною моделлю джерела зображення. Тоді вважається, що прихована інформація є невидимою, якщо заповнене зображення-контейнер узгоджується з моделлю джерела, звідки було взяте вихідне зображення, і може бути розраховане об'єктивним шляхом;

– захищеність.

Поняття захищеності включає в себе процедурні атаки, такі як атаки ІВМ або атаки на основі знання про часткову модифікацію носія через наявність вкладення. Вбудована інформація не може бути видалена цілеспрямованими атаками, заснованими на відомому алгоритмі вбудовування та вилучення (окрім секретного ключа), і знанні принаймні одного носія з прихованим повідомленням;

– складність вбудовування і вилучення.

Кількість стандартних операцій, які будуть виконані для вбудовування і виявлення прихованого повідомлення.

Вищевказані вимоги взаємно конкуруючі і не можуть бути оптимальними одночасно. Якщо необхідно приховати велике повідомлення всередині зображення, то неможливо вимагати абсолютної невидимості і високої стійкості. Завжди необхідний оптимальний компроміс.

З іншого боку, якщо потребується стійкість до великих спотворень, то повідомлення, що має бути надійно сховане, не може бути занадто довгим.

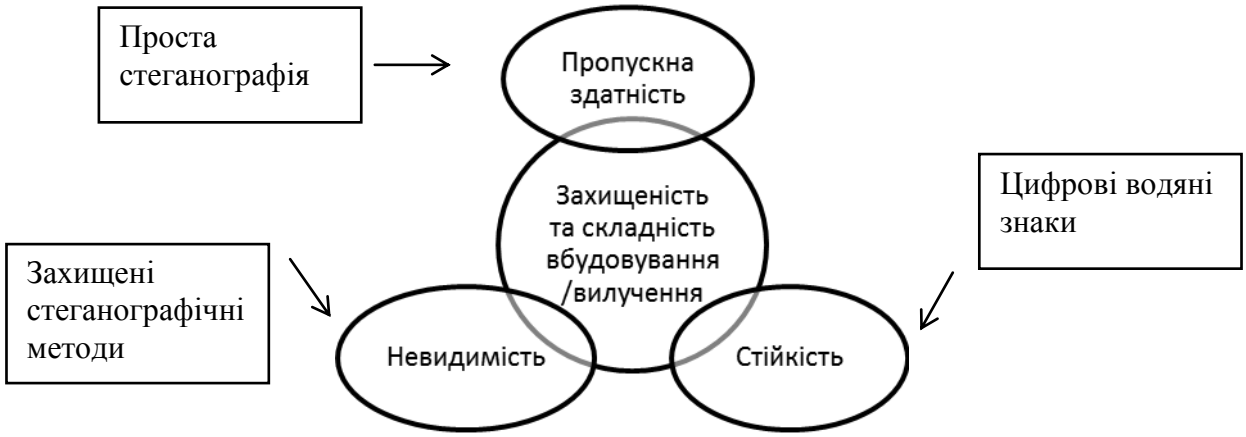

Рисунок 3.1 - Ключові характеристики методів цифрової стеганографії

Отримані оцінки використовуються для аналізу обраних стеганографічних методів вбудовування інформації та для багатокритеріального вибору найкращого методу. За формулами 3.1 – 3.6 проведемо обчислення кількісних показників для наступних методів:

- найменш значущого біта;
- методу Подільчука;
- методу Тао.

З аналізу таблиці 3.1 можна побачити, що дані існуючі стеганографічні методи мають низьку ймовірність вилучення даних та низький показник відношення ПВСШ. Це робить стеганограму вразливою до різного роду атак. В таблиці 3.2 показані основні атаки.

Таблиця 3.1 – Значення кількісних показників методів стеганографії

Показник якості	Методи стеганографії		
	НЗБ	Подільчука	Тао
Відносна ємність, %	6,25	12,5	3,1
Ймовірність вилучення даних	0,5	0,75	0,7
Пікове відношення сигнал шум, дБ	12,53	19,43	18,54

Таблиця 3.2 – Основний спектр атак на стеганосистему

Види атак	Ціль проведення атаки		
	Виявлення факту наявності вбудовування	Руйнування вбудованого повідомлення	Вилучення вбудованого повідомлення
Активні (навмисні)	Візуальна атака	Шуми в каналі передачі даних	
Пасивні (ненавмисні)	Стеганографічний аналіз	Постановка перешкод, компресійні атаки	Стеганографічний аналіз

Проведемо порівняльний аналіз кількісних показників для наступних методів:

- А1 (метод найменш значущого біта);
- А2 (метод Бенгама – Мемона – Ео – Юнга);
- А3 (методу ДВП);
- А4 (метод Коха – Жао).

Для розуміння значень, що описані в таблиці 3.3, нижче наведений розрахунок коефіцієнтів для пропускної здатності.

Таблиця 3.3 – Порівняльний аналіз якісних показників методів стеганографії

	пропускна здатність	складність виявлення	невидимість	захищеність	складність вбудовування
А1	0,509	0,453	0,147	0,018	0,453
А2	0,023	0,072	0,076	0,216	0,072
А3	0,063	0,020	0,293	0,381	0,020
А4	0,038	0,120	0,044	0,216	0,120

Для методу НЗБ пропускна здатність залежить від розмірів зображення (h – висота, w – ширина) і розраховується згідно з:

(3.7)

Метод Коха-Жао використовує для вбудовування одного біту інформації блок коефіцієнтів ДКП розміром *8x8*, тому пропускна здатність визначається:

(3.8)

Методи, що використовують ДВП перетворення першого рівня, можуть запропонувати пропускну здатність:

(3.9)

Щодо інших характеристик, то стійкість була оцінена через кількість загальних операцій з обробки зображення, які можливо здійснити зі стеганографічною системою, утвореною певним методом, без втрати можливості детектувати вбудовану інформацію.

Невидимість оцінювалася кількісним показником якості зображення (*IF*). Захищеність враховувала стійкість методів до атак.

Складність вбудовування і вилучення розраховувалася за кількістю стандартних операцій, які необхідно виконати для вбудовування і вилучення прихованого повідомлення.

При цьому стеганографічний контейнер заповнювався лише на 10% від максимальної пропускної здатності.Проаналізувавши існуючі методи приховування даних в ЗК було визначено основні недоліки.

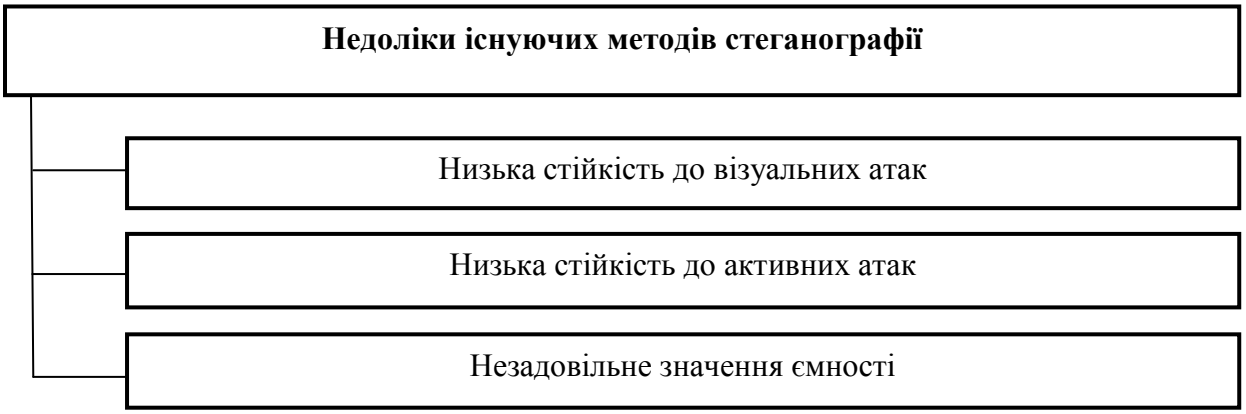

Рисунок 3.2 – Основні недоліки існуючих методів приховування даних

Низьке значення стійкості стеганограми до візуальних атак зловмисника. Даний недолік обумовлений тим, що вбудовування приховуваної інформації досягається шляхом модифікації елементів подання стеганограми.

Це супроводжується внесенням візуальних спотворень зображення погіршенням його якості. У разі наявності у зловмисника вихідного зображення-контейнера може бути виявлений факт наявності прихованого вбудовування в стеганограмі.

Низька стійкість вбудованих даних до активних атак зловмисника. Серед таких атак найбільш поширеними є компресійні атаки. Вони спрямовані на усунення психовізуальної надмірності, яка також використовується для непрямого стеганографічного приховування інформації.

Застосовуючи дані атаки, супротивник здатний безповоротно зруйнувати вбудоване повідомлення. Незадовільне значення стеганографічної ємності. Існуючі методи вбудовування не забезпечують необхідного обсягу вбудованої інформації. Даний недолік обумовлений тим, що збільшення обсягу вбудовування супроводжується збільшенням числа модифікованих елементів і як наслідок збільшенням спотворення зображення.

4 МЕТОД ПРИХОВУВАННЯ ДАНИХ ДЛЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ ОБРОБКИ ТА ПЕРЕДАЧІ ВІДЕОІНФОРМАЦІЙНИХ РЕСУРСІВ ПРИХОВУВАННЯ ДАНИХ В ЗОБРАЖЕННЯ – КОНТЕЙНЕР

Розвідка, постійне спостереження та своєчасна передача інформації про дії супротивника стали запорукою успішності бойових операцій на війні. Сучасні БПЛА полегшують виконання цих завдань. Спираючись на результати дослідження переваг і недоліків існуючих методів вбудовування інформації було розроблено власний метод стеганографічного приховування інформації. Суть розробленого стеганографічного методу полягає в тому, що зображення та секретна інформація піддаються попередній обробці для підвищення пропускної спроможності та стійкості стегосистеми.

Розроблений метод повинен забезпечувати надійність приховування інформації в зображеннях, вбудовування відносно великого обсягу інформації та стійкість до спотворень. Зображення має велику кількість сегментів, що забезпечить можливість для забезпечення відносно великого обсягу для вбудовування інформації.

Крок 1– до зображення застосовується ДВП, результатом якого є розкладання зображення на чотири області: LL - низькочастотна область , і три області (LH, HL, HH) - високочастотні області.

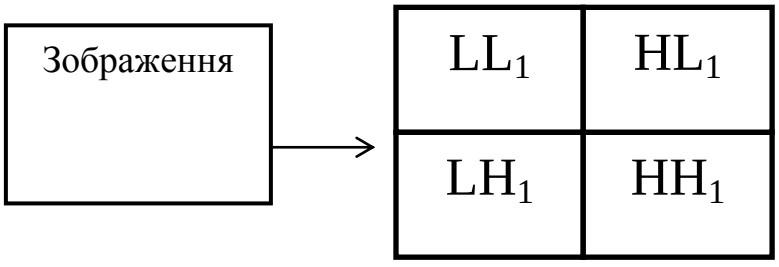

Рисунок 4.1 - Перший рівень вейвлет-перетворення

Крок 2 – обрану область (LH, HL, HH) ділять на блоки 8x8 і до кожного блоку застосовують ДКП:

де *C(x, y)* – відповідно, елементи оригінального і відтвореного за коефіцієнтами

ДКП зображення розмірністю NxN;

x, y – просторові координати пікселів зображення;

Ω(υ, ν) – масив коефіцієнтів ДКП;

(υ, ν) – координати в частотної області;

$\xi(\upsilon)=\frac{1}{\sqrt{2}}$, якщо $\upsilon\approx 0$, і $\xi(\upsilon)=1$, якщо $\upsilon>0$.

Крок 3 – для вбудовування було запропоновано використовувати не всі сегменти (блоки) контейнера, а тільки ті, що найбільш для цього придатні.

Придатними для вбудовування приховуваної інформації вважаються ті сегменти зображення, що одночасно задовольняють наступним двом вимогам:

- у сегменті відсутні різкі перепади яскравості;
- сегмент не є занадто монотонним.

Сегменти, що не відповідають першій вимозі, характеризуються наявністю декількох занадто великих значень НЧ коефіцієнтів ДКП, порівнянних за своєю величиною з DC-компонентою.

Для блоків, що не задовольняють другій вимозі, є характерною рівність нулеві більшості ВЧ коефіцієнтів. Таким чином, вказані особливості виступають критерієм відбраковування елементів контейнера, непридатних для заповнення.

Зазначені вимоги відбраковування враховуються використанням двох порогових коефіцієнтів: P_L, (для першої вимоги) і P_H (для другої вимоги),

перевищення (P_L) або недосягнення (P_H) яких вказуватиме на те, що візуальна помітність модифікації сегмента у частотній області буде надзвичайно високою, через що останній для перенесення біта повідомлення є непридатним.

Крок 4 – з блока, приналежного СЧ області, обираються (для більшої стійкості стеганосистеми — псевдовипадково) три коефіцієнти ДКП з координатами $(\upsilon_1,\nu_1),(\upsilon_2,\nu_2)$ та (υ_3,ν_3) відповідно.

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.

Крок 5 – якщо необхідно провести вбудовування «0», ці коефіцієнти змінюються таким чином, щоб третій коефіцієнт став менше кожного з перших двох; якщо ж потрібно приховати «1», то коефіцієнт з координатами (υ_3,ν_3) робиться більшим за інші:

де M_b – номер блоку;

– координати коефіцієнтів ДКП;

Ω_b – матриця 8x8 коефіцієнтів розкладу.

Крок 6 – 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:

$$\begin{cases} (\Omega_b)_{\upsilon_3\nu_3} < \min\left[(\Omega_b)_{\upsilon_1\nu_1}, (\Omega_b)_{\upsilon_2\nu_2}\right] - P, \text{ при } \mathrm{M}_b = 0; \\ (\Omega_b)_{\upsilon_3\nu_3} > \max\left[(\Omega_b)_{\upsilon_1\nu_1}, (\Omega_b)_{\upsilon_2\nu_2}\right] + P, \text{ при } \mathrm{M}_b = 1. \end{cases}$$

Чим більше значення *P*, тим стеганосистема, створена на основі даного методу, є стійкішою до компресії та впливу завад, проте якість зображення при цьому може значно погіршуватись

У випадку, якщо така модифікація призводить до занадто великої деградації зображення, коефіцієнти Ω_b залишають без змін, а сам блок и якості контейнера не використовується. Використання трьох коефіцієнтів ДКП замість двох і, що найголовніше, відмова від модифікації у випадку неприйнятних спотворень зображення, суттєво зменшує помітність сгеганограми.

Розроблений метод утворений шляхом інтеграції запропонованих методів підвищення стійкості, захищеності та пропускної здатності стеганографічних систем.

За формулами 3.1 -3.6 проведемо аналіз показників розробленого методу. Отримані результати показані в таблиці 4.1.

Таблиця 4.1 – Показники якості розробленого методу

	Відносна ємність $w_{відн}$, %	Ймовірність вилучення даних $P_{вил}$	Пікове відношення сигнал шум h, дБ
Розроблений метод	4,6	1	23,56

Для порівняльного оцінювання якості стеганографічних засобів можна використовувати загальновідомі показники, що дають кількісні оцінки.

Вони оперують із зображеннями на рівні пікселів. В цих співвідношеннях через $C_{x,y}$ – позначається піксель пустого контейнера з координатами *(x,y)* а через $S_{x,y}$ – відповідний піксель заповненого контейнера. 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:

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

– якість зображення (*IF*) є однією з основних оціночних характеристик для

стегоалгоритмів, які працюють із зображеннями:

– середньоквадратична похибка (*MSE*):

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

Методи були протестовані на зображеннях різних розміром *128x128* з потужністю приховування для розробленого алгоритму: *P = 50*. Результати розрахунку запропонованих характеристик наведені в табл. 4.2.

Таблиця 4.2 – Значення кількісних показників методів стеганографії

Показник викривлення	Розроблений метод (P=50)	Метод НЗБ	Метод БМЕЮ	Метод Коха-Жао
AD	0,649	0,494	3,042	11,400
SNR	9375	4975	781,6	137,69
IF	1	≈1	0,998	0,993
MSE	2,113	0,494	-	178,3

За формулами 3.7 – 3.9 проведемо розрахунок пропускної здатності представлених методів:

Таблиця 4.3 – Значення пропускної спроможності методів стеганографії

Якісний показник	Розроблений метод	Метод НЗБ	Метод БМЕЮ	Метод Коха-Жао
Пропускна здатність	0,086	0,058	0,023	0,038

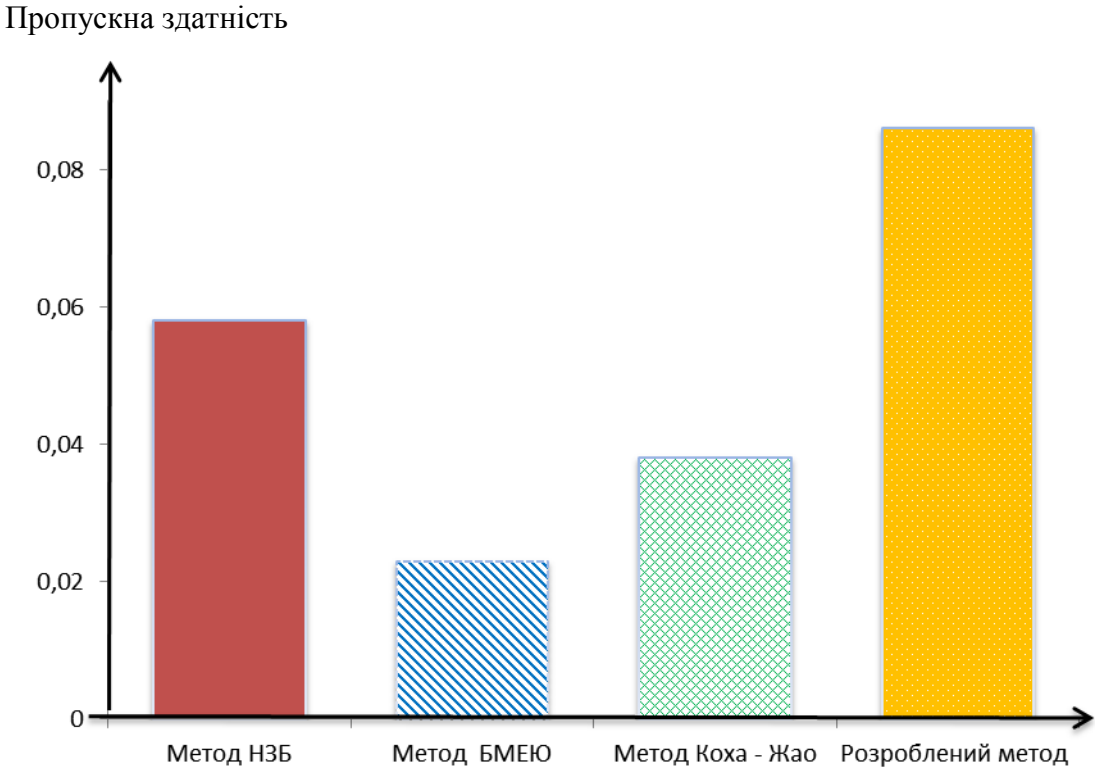

Рисунок 4.2 – Пропускна здатність методів цифрової стеганографії

ВИСНОВОК

Аналіз існуючих методів приховування даних в зображення-контейнер показав, що дані методи мають низьку ймовірність правильного вилучення даних, нестійкі до існуючих атак та мають невелику стеганографічну пропускну спроможність.

Розроблено метод для стеганографічного приховування даних за допомогою методу дискретного вейвлет-перетворення та методу Бенгама-Мемона-Ео-Юнга. Для порівняння були обрані первинні LH, HL області зображення. Вибрані блоки за допомогою метода БМЕЮ є стійкими до компресійних атак та вносять незначні спотворення до зображення, що дозволяє використовувати зображення для стеганографічного приховування даних.

Розраховано показники якості розробленого стеганографічного методу. Даний метод дозволяє приховувати біти в блоки зображення високу ймовірність правильного вилучення вбудованих даних. Розроблений метод є стійким до відомих активних атак та стеганографічного аналізу зі сторони противника.

ЛІТЕРАТУРА

1 Пєвцов Г.В., Залкін С.В., Сідченко С.О., Хударковський К.І. Інформаційна безпека у воєнній сфері: проблеми, методологія, система забезпечення: [монографія]. – Харків: Цифрова друкарня № 1, 2013. – 272 с.

2 Barannik V. A Steganographic Method Based On The Modification Of Regions Of The Image With Different Saturation/ V. Barannik, A. Lekakh, A. Bekirov, D. Barannik / Proceedings of 14th International Conference on Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering (S5). – 2018. – p. 81-85.

3 Barannik V. The method of video streams processing for information technologies of aero monitoring. / V. Barannik, A. Musienko, Yu. Ryabukha, O. Suprun, A. Slobodyanyuk / 14th International Conference [IEEE Advanced Trends in Radioelecrtronics, Telecommunications and Computer Engineering (TCSET)], 2018. – P.233 – 236.

4 Грибунин В.Г. Цифровая стеганография. / И.Н. Оков, И.В. Туринцев. – К.: Солон-Пресс, 2002. – 265 с.

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

6 Поліновський В.В. Інформаційна технологія для досліджень методів стеганографії і стегоаналізу / В.В. Поліновський // Міжвузівський збірник Комп'ютерно-інтегровані технології: освіта, наука, виробництво. – Луцьк, 2011. - №5 – с.236-242.

7 Таранчук А.А. Стеганографічний метод приховування даних в області частотних перетворень зображень / Л.Г. Гальпер // Вісник Хмельницького Університету. – Хмельницький, 2009. – № 2 Технічні науки – С.197-201.

8 Хорошко В.А. Методи й засоби захисту інформації. / А. А. Чекатков. – К.: Юніор, 2003. – 504 с.

9 Аграновський А.В. Стеганографія, цифрові водяні знаки та стегоаналіз [Текст]/ А. В. Аграновський, А. В. Балакін, В. Г. Грибунин. – М.: Вузовская книга, 2015. – 220 с.