



KAPITEL 6 / CHAPTER 6⁶

INCREASING RESISTANCE TO ATTACKS OF THE STEGANOGRAPHIC METHOD WITH CODE MANAGEMENT

DOI: 10.30890/2709-2313.2024-35-00-023

У стеганографії вибір кольорового простору відіграє ключову роль у забезпеченні ефективного приховування інформації та підвищенні стійкості до атак [27]. Традиційно використовується кольоровий простір RGB, де кожен піксель зображення представлений трьома компонентами: червоним (Red), зеленим (Green) та синім (Blue). Однак застосування кольорового простору YCbCr може надати значні переваги у стеганографічних методах [28].

Кольоровий простір RGB є адитивною моделлю, де кольори формуються шляхом додавання трьох базових кольорів. Ця модель широко використовується в комп'ютерній графіці та дисплеях. Натомість YCbCr є простором, що розділяє інформацію про яскравість (Y) та кольорові компоненти: синьо-жовту (Cb) та червоно-зелену (Cr). Це розділення дозволяє більш ефективно обробляти та передавати відео- та зображення, особливо в цифрових форматах [29].

Перехід до використання YCbCr у стеганографічних методах має кілька переваг:

1. Розділення яскравості та кольору – оскільки людське око більш чутливе до змін яскравості, ніж до змін кольору, приховування інформації в кольорових компонентах зменшує ймовірність візуального виявлення стеганографічного втручання;
2. Зменшення впливу на якість зображення – внесення змін лише в кольорові компоненти мінімально впливає на загальне сприйняття зображення, що підвищує непомітність прихованої інформації;
3. Підвищення стійкості до атак – завдяки розділенню яскравісної та кольорових компонентів, атаки, спрямовані на виявлення прихованої інформації, стають менш ефективними, оскільки зміни в кольорових каналах менш помітні.

⁶Authors: Melnyk Marharyta, Hulid Dmytro

Number of characters: 15379

Author's sheets: 0,38



Використання YCbCr не вимагає значних обчислювальних ресурсів, оскільки перетворення між RGB та YCbCr є лінійним і може бути виконане з мінімальними витратами [30]. Це означає, що перехід до YCbCr не впливає негативно на продуктивність стеганографічного методу, забезпечуючи при цьому підвищену стійкість до атак [31].

Нижче у таблиці 2.1 наведено порівняльну таблицю характеристик кольорових просторів RGB та YCbCr.

Таблиця 1.1 – Таблиця характеристик кольорових просторів RGB та YCbCr

Характеристика	RGB	YCbCr
Модель	Адитивна	Розділення яскравості та кольору
Компоненти	Red, Green, Blue	Y (яскравість), Cb (синьо-жовта), Cr (червоно-зелена)
Чутливість людського ока	Висока до змін яскравості та кольору	Висока до змін яскравості, низька до змін кольору
Використання в стеганографії	Менш ефективно приховування інформації	Більш ефективно приховування інформації в кольорових компонентах
Вплив на якість зображення	Можливе помітне погіршення	Мінімальний вплив при зміні кольорових компонентів

Дослідження показують, що стеганографічні методи, які працюють у YCbCr, здатні приховувати значно більше інформації без видимого погіршення якості зображення, ніж методи в RGB [32]. Крім того, такі методи є більш стійкими до виявлення за допомогою методів аналізу зображень, таких як порівняння гістограм або аналіз спектральних компонентів. Це особливо важливо для стеганографії в мережових умовах, де зображення можуть



піддаватися додатковій компресії та обробці [33].

Таким чином, кольоровий простір YCbCr забезпечує більш ефективне приховування інформації та підвищену стійкість до атак, особливо до атак стиснення та шуму [34]. Застосування YCbCr у стеганографії дозволяє приховувати інформацію в менш помітних для людського ока областях, зберігаючи при цьому загальну якість зображення. Це робить його більш придатним для стеганографічних методів порівняно з традиційним RGB, що обмежує можливості приховування та надійність захисту даних.

Стиснення зображень у форматі JPEG є стандартною процедурою, яка значно зменшує розмір файлів, але водночас може вплинути на приховану в зображенні інформацію. Особливо це стосується стеганографічних методів, де дані вбудовуються в різні компоненти зображення. Для підвищення стійкості до таких атак доцільно використовувати кольоровий простір YCbCr та вбудовувати інформацію в Y-компоненту.

У кольоровому просторі YCbCr зображення розділяється на три компоненти: Y (яскравість), Cb (синьо-жовта) та Cr (червоно-зелена). Яскравісна компонента Y містить основну інформацію про структуру зображення, тоді як Cb та Cr відповідають за кольорові відтінки. Під час стиснення JPEG яскравісна компонента зазвичай піддається менш агресивному квантуванню порівняно з кольоровими, це означає, що інформація, вбудована в Y-компоненту, з більшою ймовірністю збережеться після стиснення.

Додатково, використання кодових слів, що впливають на коефіцієнти перетворення Адамара, зокрема на коефіцієнт (1,1), сприяє підвищенню стійкості до стиснення. Це пов'язано з тим, що такі коефіцієнти відповідають за низькочастотні компоненти зображення, які менш схильні до втрат під час стиснення.

Експериментальні дослідження підтверджують, що вбудовування інформації в Y-компоненту кольорового простору YCbCr значно підвищує стійкість стеганографічного методу до стиснення JPEG. На рисунку 1.1 нижче представлено порівняння рівня збереження прихованої інформації після



стиснення для різних компонентів. Таким чином, вбудовування в Y-компоненту забезпечує найвищий рівень збереження інформації після стиснення, що підтверджує ефективність запропонованого підходу.

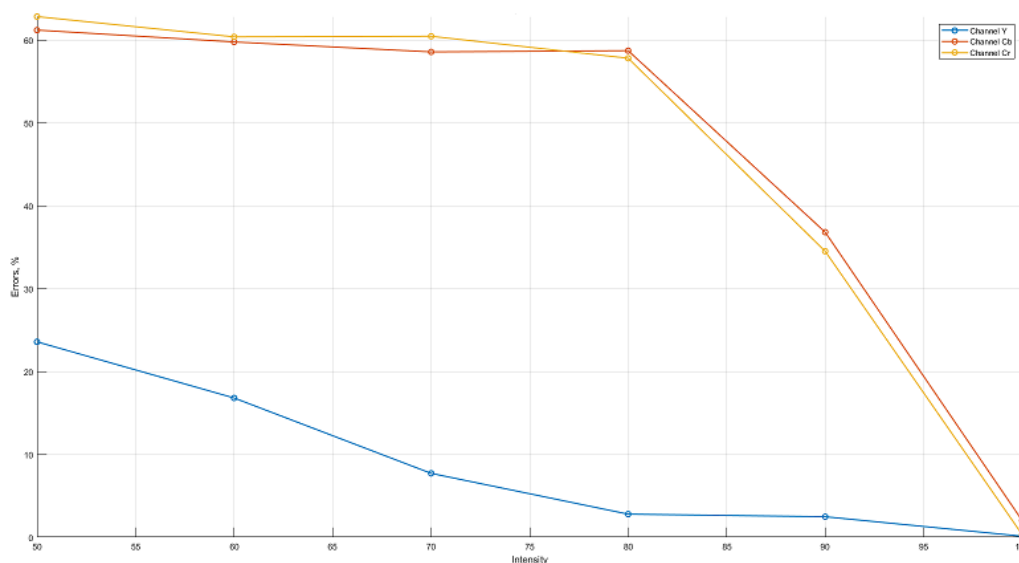


Рисунок 2.1 – Вплив стиснення JPEG на збереження прихованої інформації в різних компонентах кольорового простору YCbCr для кодового слова розміром 16

На рисунку 1.2 представлено аналіз стійкості стеганографічного методу до стиснення JPEG при вбудовуванні інформації в Y-компоненту кольорового простору YCbCr порівняно з попереднім методом, що використовував RGB-компоненти.

Дослідження проводилося для кодових слів довжиною 4, 8 та 16 біт. Результати показують, що використання Y-компоненти значно підвищує стійкість до стиснення, що забезпечує оптимальне збереження прихованої інформації після стиснення.

Перехід до використання кольорового простору YCbCr та вбудовування інформації в Y-компоненту дозволяє значно підвищити стійкість стеганографічного методу до атак стиснення JPEG. Це досягається завдяки менш агресивному квантуванню яскравісної компоненти під час стиснення та використанню кодових слів, що впливають на низькочастотні коефіцієнти перетворення Адамара.

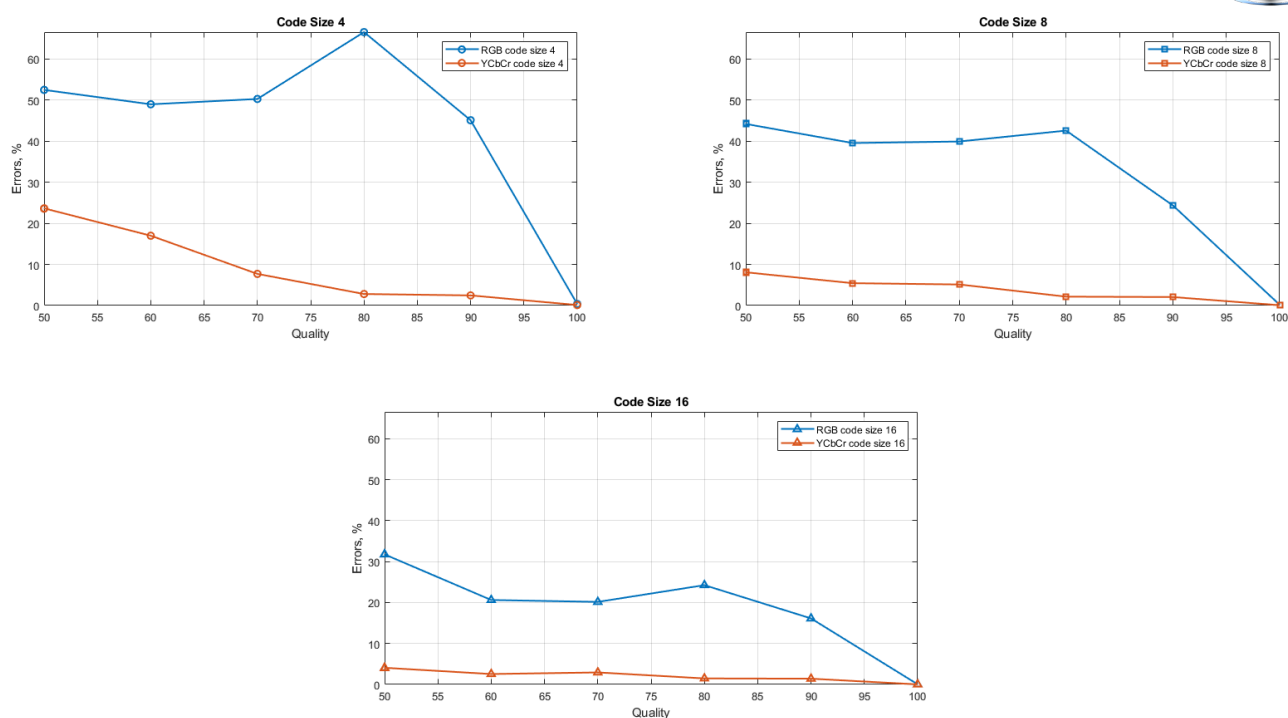


Рисунок 1.2 – Порівняння стійкості до атак стиснення для RGB і YCbCr (Y канал) з різними розмірами кодових слів

У процесі покращення методу було виявлено, що використання кодових слів довжиною 8 біт призводить до значного приросту ефективності порівняно з кодовими словами довжиною 4 біти. Однак подальше збільшення довжини кодового слова до 16 біт не дає суттєвого покращення порівняно з 8-бітними кодовими словами. При цьому спостерігається різке погіршення пропускну здатності, що робить вибір кодових слів довжиною 16 біт недоцільним. Таким чином, оптимальним варіантом є використання 8-бітних кодових слів, оскільки вони забезпечують найкращий баланс між ефективністю та пропускну здатністю.

Підвищення стійкості до зашумлення адитивним білим гаусівським шумом

Адитивний білий гаусівський шум (АБГШ) є одним із найпоширеніших видів зашумлення в цифровій обробці зображень. Він має рівномірний розподіл по всіх частотних компонентах сигналу, тобто впливає як на високочастотні, так і на низькочастотні області з однаковою інтенсивністю. Це створює значні труднощі для його придушення чи фільтрації, оскільки відфільтровування шуму лише в одній частотній області не дає бажаних результатів. У стеганографії така



природа шуму означає, що прихована інформація може бути спотворена незалежно від частоти, в якій вона розміщена, що вимагає особливих підходів для захисту даних.

Одним із методів протидії АБГШ у стеганографії є збільшення енергії кодового слова. Це означає, що для захисту прихованої інформації можна підвищити інтенсивність даних, що вбудовуються, роблячи їх менш чутливими до зашумлення.

Однак такий підхід має свої обмеження: надмірне збільшення енергії кодового слова може призвести до появи візуальних артефактів на зображенні, які легко помітні для ока. Це, в свою чергу, може розкрити сам факт приховування інформації, що є неприпустимим для стеганографічних методів. Таким чином, необхідно знайти баланс між достатнім рівнем енергії кодового слова для стійкості до шуму та збереженням якості зображення.

Для збереження якості зображення та водночас підвищення стійкості до АБГШ, було запропоновано вбудовувати інформацію одночасно в два кольорові канали кольорового простору YCbCr – Cb та Cr. Цей підхід дозволяє розподілити енергію кодового слова між двома каналами, зменшуючи навантаження на кожен з них окремо.

В результаті ми отримуємо збільшення стійкості до шуму, оскільки приховані дані менш вразливі до одночасного зашумлення обох каналів, а візуальна якість зображення залишається на високому рівні. Така комбінація дозволяє зберегти надійність стеганографічного приховування навіть у складних умовах, забезпечуючи баланс між невидимістю даних і їх стійкістю до атак.

Ще одним важливим аспектом підвищення стійкості до АБГШ є вибір оптимального кодового слова. Оскільки шум рівномірно впливає на всі частотні компоненти, доцільно використовувати кодові слова, які також мають рівномірний спектральний розподіл.

У цьому контексті особливо ефективними є кодові слова, створені на основі bent-послідовностей. Bent-послідовності характеризуються властивістю рівномірного розподілу енергії по всьому частотному спектру, що дозволяє



захистити приховану інформацію в різних частотних діапазонах від одночасного впливу шуму. Завдяки використанню bent-послідовностей ми можемо досягти додаткового рівня захисту, підвищивши загальну стійкість до зашумлення.

На рисунку 1.3 наведено порівняння стійкості до адитивного білого гаусівського шуму при використанні кольорового простору RGB та двох кольорових каналів YCbCr (Cb та Cr) для кодових слів різної довжини – 4, 8 та 16.

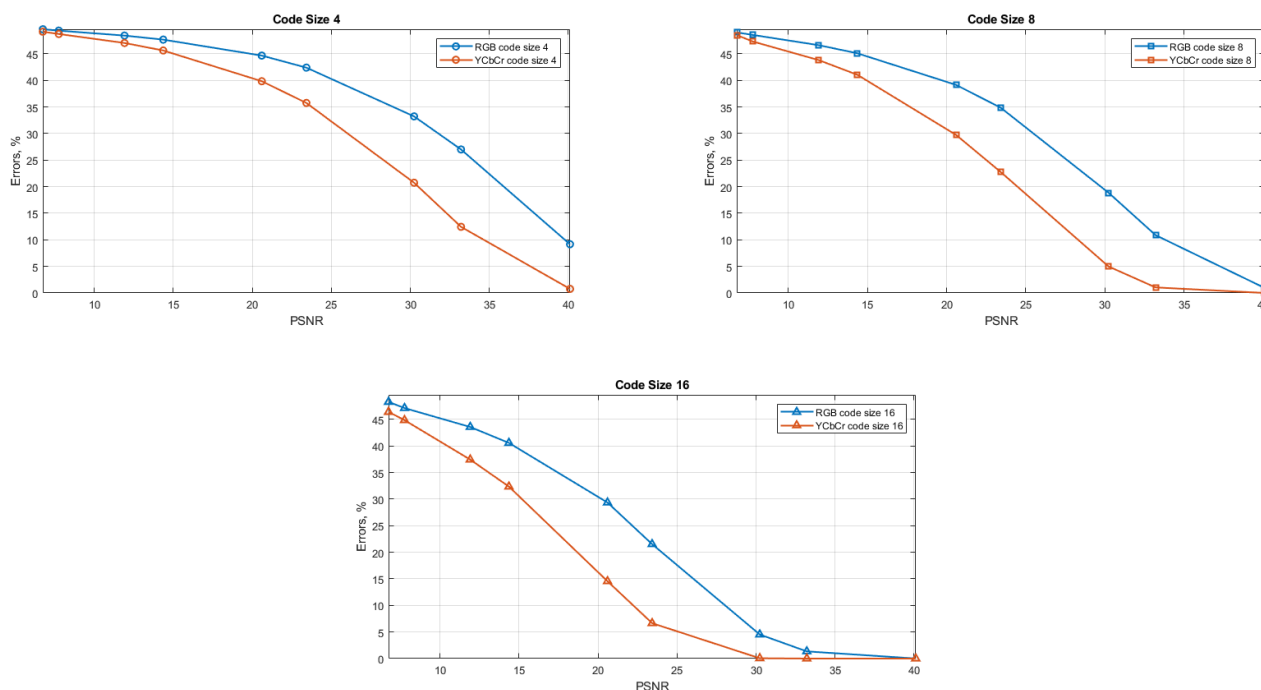


Рисунок 1.3 – Порівняння стійкості до адитивного білого гаусівського шуму для RGB і YCbCr (Cb і Cr канали) з різними розмірами кодових слів

Видно, що застосування двох каналів YCbCr забезпечує значний приріст стійкості до шуму у всіх варіантах кодових слів. Зокрема, для всіх розмірів кодових слів стійкість до шуму помітно покращується у порівнянні з традиційним RGB-підходом.

Використання кодових слів довжиною 16 забезпечує найбільшу стійкість до шуму, оскільки вони дозволяють інтегрувати більше енергії та, відповідно, підвищити стійкість до зашумлення.

Проте це рішення також має свій компроміс – із збільшенням довжини кодового слова знижується пропускна здатність стеганографічного методу, що



зменшує кількість інформації, яку можна приховати. Отже, хоча використання 16-бітних кодових слів є оптимальним з точки зору захисту від шуму, воно потребує обмеження обсягу переданих даних.

Таким чином, для забезпечення стійкості до адитивного білого гаусівського шуму рекомендується використовувати дві кольорові компоненти YCbCr – Cb та Cr, а також застосовувати кодові слова на основі bent-послідовностей довжиною 16 біт. Цей підхід забезпечує оптимальний баланс між захистом від шуму та збереженням якості зображення, хоча й призводить до зниження пропускну здатності методу.

Шум «Сіль і перець» є типовим прикладом імпульсного шуму, що виникає внаслідок апаратних збоїв, помилок передачі даних або дефектів сенсорів. Він проявляється у вигляді випадкових чорних, білих і кольорових пікселів, які різко контрастують із сусідніми елементами зображення.

Така природа шуму особливо негативно впливає на зображення, порушуючи його локальну текстуру та однорідність. Це створює суттєві труднощі для стеганографії, оскільки пошкоджені пікселі можуть спричиняти спотворення вбудованої інформації та ускладнювати процес її вилучення.

Дослідження показали, що збільшення розміру кодового слова у стеганографічному методі із кодовим керуванням не завжди є доцільним, особливо в умовах присутності шуму типу «Сіль і перець».

У процесі аналізу було виявлено, що великі блоки зображення, які використовуються для вбудовування інформації, мають вищу ймовірність потрапляння в них аномальних пікселів. Це, у свою чергу, призводить до значного спотворення всієї структури блоку та погіршує як точність вилучення даних, так і загальну якість приховання.

Запропоноване вдосконалення методу полягає в тому, що під час аналізу кожного блоку зображення виявляються аномальні пікселі – тобто ті, що значно відрізняються від інших. Результати покращення такого механізму показані на рисунку 2.4. Ці пікселі виключаються зі стеганографічних перетворень, щоб вони не впливали на результати, оскільки метод вбудовує лише



один біт додаткової інформації в кожен блок, і один піксель не має вирішального впливу на весь блок.

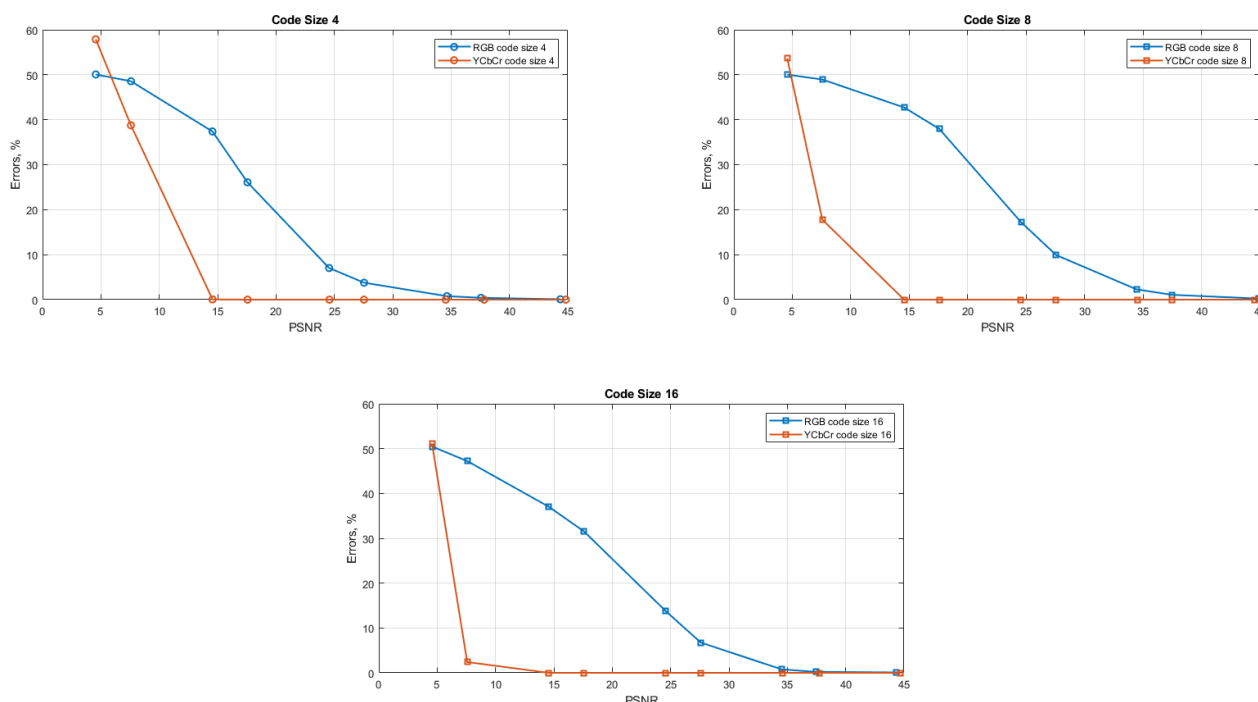


Рисунок 1.4 – Порівняння стійкості до атак стиснення для RGB і YCbCr (з функцією аналізу блоку) з різними розмірами кодових слів

Декодування в цьому підході базується на аналізі відмінностей між блоками пікселів модифікованого зображення і початкового контейнера. Для кожного блоку обчислюється різниця значень пікселів, після чого ці відхилення зважуються за допомогою кодового слова.

Вагове підсумовування дозволяє виділити ті зміни, які відповідають внесенню стеганографічної інформації, при цьому випадкові або несуттєві відхилення, викликані шумом, суттєво не впливають на результат.

Таким чином, застосування аналізу блоків для ідентифікації аномальних пікселів та їх виключення із процесу вбудовування є ефективним засобом підвищення стійкості стеганографічного методу до шуму «Сіль і перець». Це рішення не лише мінімізує негативний вплив шуму, але й розширює можливості методу для практичного застосування в умовах реальних загроз.



Висновки

У розділі докладно проаналізовано методи покращення стійкості стеганографічного методу з кодовим управлінням. Основна увага приділена використанню кольорового простору YCbCr, що забезпечує суттєве підвищення захисту інформації під час стиснення зображень у форматі JPEG. Особливість цього підходу полягає в менш агресивному квантуванні яскравісної компоненти Y, що сприяє збереженню прихованих даних навіть після компресії. Експерименти підтвердили, що вбудовування інформації в компоненти кольорового простору YCbCr значно зменшує ризик її втрати.

Для протидії адитивному білому гаусівському шуму рекомендовано інтегрувати інформацію одночасно у дві кольорові компоненти YCbCr – Cb та Cr. Це дозволяє рівномірно розподілити навантаження між каналами, забезпечуючи захист прихованих даних від спотворень. Додатково, застосування кодових слів на основі bent-послідовностей довжиною 16 біт виявилось ефективним інструментом для підвищення стійкості до шуму. Такий підхід створює оптимальний баланс між захистом від зашумлення і збереженням високої якості зображення, хоча й супроводжується деяким зниженням пропускної здатності стеганографічного методу.

Крім того, для підвищення стійкості до імпульсного шуму типу «сіть і перець» запропоновано підхід із використанням аналізу блоків зображення. Метод передбачає ідентифікацію аномальних пікселів, які значно відрізняються від сусідніх, та їх виключення із процесу вбудовування інформації. Така стратегія дозволяє уникнути викривлення прихованих даних через пошкоджені пікселі та забезпечує стабільність процесу вилучення інформації.

Під час дослідження був розроблений програмний продукт, призначеного для реалізації модифікованого стеганографічного методу з кодовим керуванням вбудовування додаткової інформації з метою підвищення стійкості до атак. Для реалізації стеганографічного методу з кодовим керуванням вбудовування додаткової інформації було обрано середовище програмування MATLAB.