Міністерство освіти і науки України

Харківський національний університет імені В.Н. Каразіна

Факультет комп'ютерних наук

Спеціальність 125 «Кібербезпека»

Освітня програма «Безпека інформаційних та комунікаційних систем»

«Допущено до захисту»

Зав.кафедрою БІСТ

Сергій РАССОМАХІН

_____

« » 2022 р.

Пояснювальна записка

до кваліфікаційної роботи магістра

на тему: «Математичні моделі, методи та обчислювальні алгоритми приховування даних у контейнери-зображення із розширенням спектру методом прямої послідовності»

оцінка « »

Голова ЕК

Доценко С.І. _____

Керівник проф. Кузнецов О.О.

Рецензент проф. Толстолузька О.Г.

Виконавець: студентка групи КБ-61

Локоткова Ірина Романівна

Харків – 2022

РЕФЕРАТ

Кваліфікаційна робота магістра: 64 сторінок, 39 рисунків, 7 таблиць, 30 джерел за переліком посилань;

Робота містить вступ, 3 розділи, висновки, перелік використаних джерел та один додаток.

Метою роботи є дослідження математичних моделей, методів та алгоритмів приховування даних у стеганоконтейнери-зображення з використанням технології розширення спектру методом прямої послідовності.

Виходячи з мети, *завдання дослідження*:

– провести аналіз форматів цифрових зображень;

– здійснити визначення критеріїв та показників ефективності стеганосистем;

– застосувати порівняльний аналіз стеганосистем та обґрунтувати напрямки досліджень;

– провести дослідження технології прямого розширення спектру та її застосування в стеганографії;

– здійснити розробку математичної моделі приховування даних у контейнери-зображення із розширенням спектру методом прямої послідовності;

– навести порівняльні характеристики стеганосистем із розширенням спектру методом прямої послідовності;

– провести розробку алгоритмів приховування та вилучення даних у контейнери-зображення із розширенням спектру методом прямої послідовності;

– здійснити обґрунтування вибору мови та середовища розробки для програмної реалізації запропонованих алгоритмів;

– побудувати програму реалізацію алгоритмів приховування та вилучення даних;

– проаналізувати результати експериментальних досліджень.

Предметом дослідження є використання стеганографічних систем приховування даних у контейнери-зображення.

Об'єктом дослідження є технологія прямого розширення спектру в стеганографії.

Методи дослідження. Теоретико-методологічною основою роботи є наукові концепції, розроблені вітчизняними та закордонними науковцями у сфері захисту інформації, стеганографії, математичного моделювання та суміжних галузей.

Ключові слова: СТЕГАНОГРАФІЯ, ПРИХОВУВАННЯ ДАНИХ, ЦИФРОВІ ЗОБРАЖЕННЯ, ПРЯМЕ РОЗШИРЕННЯ СПЕКТРА, ЛІЗА МАРВЕЛ, УОЛШ-АДАМАР, ПСЕВДОВИПАДКОВІ ПОСЛІДОВНОСТІ.

ABSTRACT

Qualifying work of a master, 64 pages, 39 figures, 7 tables, 30 references.

The work consists of the introduction, 3 sections, conclusion, list of references, and one application.

The aim of the work is to study mathematical models, methods and algorithms for hiding data in steganocontainers-images using the technology of spectrum expansion by direct sequence method.

Based on the goal, we can formulate the following *research tasks:*

– to analyze the formats of digital images;

– to determine the criteria and performance indicators of steganosystems;

– to apply a comparative analysis of quilting systems and substantiate the directions of research;

– to conduct a study of direct spread spectrum technology and its application in steganography;

– to develop a mathematical model of data hiding in containers-images with spectrum expansion by direct sequence method;

– to give comparative characteristics of steganosystems with spectrum expansion by direct sequence method;

– to develop algorithms for hiding and extracting data into image containers with spectrum expansion by the direct sequence method;

– to justify the choice of language and development environment for the software implementation of the proposed algorithms;

– to build a program to implement the algorithms for hiding and extracting data;

– to analyze the results of experimental studies.

The subject of research is the use of steganographic systems for hiding data in image containers.

The object of research is the technology of direct spectrum expansion in steganography.

Research methods. The theoretical and methodological basis of the work are scientific concepts developed by domestic and foreign scientists in the field of information security, steganography, mathematical modeling, and related fields.

Key words: STEGANOGRAPHY, HIDING DATA, DIGITAL IMAGES, SPREAD SPECTRUM, LIZA MARVEL, WALSH-HADAMARD, PSEUDORANDOM SEQUENCES.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ СКОРОЧЕНЬ І ТЕРМІНІВ

ПВП	–	Псевдовипадкова послідовність.
ГПВП	–	Генератор псевдовипадкових послідовностей.
Стеганосистема	–	це сукупність засобів та методів, які використовуються з метою формування прихованого каналу передачі інформації.
Стеганоконтейнер	–	заповнений контейнер, що містить у собі приховану інформацію, та який візуально не відрізняється від контейнера-оригіналу.
ЦВЗ	–	цифровий водяний знак.
Дискретний сигнал	–	інформаційний сигнал, який представляється у вигляді окремих значень, взятих за часом.

ВСТУП

Актуальність теми. В сучасному світі велика увага приділяється захисту інформації різними методами, в тому числі і шляхом її приховування від сторонніх. Більшість методів приховує зміст повідомлень методами криптографії тощо, проте більш надійним способом є приховування самого повідомлення, щоб сторонній спостерігач взагалі не здогадався про існування інформації. Вивченням методів та алгоритмів приховування інформації візуально займається стеганографія. Стеганографічні засоби приховування використовуються у різних сферах, наприклад, для підтвердження авторства графічного чи аудіовізуального твору. Автор може ставити власний «підпис» на зображенні шляхом використання певних поєднань кольорів, взаємного розташування предметів, форми окремих об’єктів тощо.

З розвитком цифрового контенту виник новий напрямок стеганографічного виду роботи з інформацією – цифрова стеганографія. Даний вид використовує мультимедійні об’єкти у якості стеганоконтейнерів для передачі зашифрованого повідомлення. Такий вид передачі прихованих повідомлень є зручним, оскільки мультимедійні файли ні в кого не викликають підозри у приховуванні, а пересилка таких файлів не викличе зайвого інтересу у сторонніх користувачів. Приховане повідомлення можна передати навіть через розміщені у соцмережах фотографії.

Питання стеганографії в цілому та використання зображень у якості стеганоконтейнерів досліджували ряд науковців. Д.О. Навроцький [13] досліджував стеганографічне приховування в файлах зображень як засіб захисту інформації. С.В. Мельник [16] вивчав світові тенденції розвитку цифрової стеганографії. О.М. Кінзерявий [8, 9, 10, 11] у ряді робот самостійно чи разом з співавторами досліджував питання приховування даних у зображення векторного типу. Існує дуже багато досліджень, що розглядають саме цифрові зображення в ролі стеганоконтейнера. Ця ситуація виникає через наступні фактори:

– достатньо об’ємний розмір цифрового представлення зображень, що надає змогу вбудовувати повідомлення обширного розміру або збільшувати робастність вбудовування;

– якщо розмір контейнеру був відомий раніше, при цьому не маючи обмежуючих факторів, які виникають унаслідок вимогами реального часу;

– присутність у значній кількості реальних зображень шумової структури, іншими словами - природньої надлишковості, що чудово може використовуватися для того, щоб вбудовувати необхідні дані;

– той факт, що око людини має низьку чутливість до невеликих змін кольорів, яскравості та контрасності рисунку, спотворень, що виникають біля границь малюнку тощо;

– способи цифрової обробки зображень, що мають велику ефективність.

Якщо розглядати такий метод, як пряме розширення спектра, то можна сказати, що він є досить перспективним і повинен розвиватися у напрямку способів вбудовування прихованих повідомлень. Даний спосіб надає змогу, окрім ефективності розподілу ресурсів каналу передачі, уникати помилок, що можуть виникнути в ході роботи. Завдяки цьому способу можна обрати найоптимальніший рівень спотворення необхідного стеганоконтейнера, і забезпечити екологічну передачу сигналів, і при цьому мати надійний обмін скритими повідомленнями між ними.

Практичне значення одержаних результатів – створення програмної реалізації алгоритмів приховування та вилучення даних на базі методу прямої послідовності з розширенням спектру, яка дозволить спростити та значно покращити процес прийняття використання стеганоконтейнерів-зображень.

Методи дослідження. За основу даної роботи було взято певні наукові теоретичні дані, що були досліджені вітчизняними та закордонними науковцями, які займаються безпосередньо галуззю захисту інформації, математичного моделювання, стеганографії та інших схожих галузей. Під час виконання даної роботи було використано наступні загальнонаукові принципи дослідження: логічний,

діалектичний, історичний та порівняльний, для того, щоб пояснити роботу наукових принципів та удосконалити дослідження об’єктів роботи; методи, які дозволяють спостерігати, узагальнювати, формалізувати та аналізувати дані для опису методичних даних створення програмної реалізації алгоритмів приховування та вилучення даних; програмно-цільовий спосіб використовувався для того, щоб пояснити механізми розробки та реалізації програмних частин.

Значну частину роботи займає інформаційна частина досліджень наукових робіт, публікації вчених, офіційні матеріали за даною темою, нормативно-правові акти у лагузях стеганографії та математичного моделювання. Окрім цього, було опрацьовано наукові розробки за темою моделювання складних систем, теорії нечітких систем, автоматизованих систем управління, інформаційної аналітики, прийняття рішень, захисту інформації тощо.

1 АНАЛІЗ, ПОРІВНЯЛЬНІ ДОСЛІДЖЕННЯ ТА ОБҐРУНТУВАННЯ ВИМОГ ДО ПЕРСПЕКТИВНИХ СТЕГАНОГРАФІЧНИХ СИСТЕМ ПРИХОВУВАННЯ ДАНИХ У КОНТЕЙНЕРИ-ЗОБРАЖЕННЯ

1.1 Аналіз форматів цифрових зображень

Стеганографія у якості контейнера для приховування даних досить часто використовує графічні зображення, тому для визначення можливостей стеганографічних систем доцільно спочатку розглянути існуючі формати цифрових зображень та можливості їх використання у якості стеганографічного контейнеру.

Стеганографічні методи з контейнерами у вигляді графічних зображень у більшості випадків використовуються з таких причин:

– поширення цифрових фото- та відеозаписів, що мають бути захищеними від протизаконного копіювання або поширення;

– порівняно значна кількість графічних зображень, з чого випливає наявність великого простору для приховування даних (великий розмір);

– відомий завчасно розмір контейнеру, що, в свою чергу, дає змогу підібрати найоптимальніший контейнер;

– відносно невелика чутливість ока людини до неістотних змін у цифровому графічному зображенні ;

– способи обробки цифрових зображень, що були розроблені нещодавно [2, с. 18].

На думку науковців, найбільше значення для надійності стеганосистеми та можливості вияву випадку передачі секретного повідомлення має обрання графічного контейнера, так як на захист та неспотворення повідомлення впливає і тип графічного зображення, і формат необхідного файлу.

Графічні зображення, представлені у електронному вигляді, поділяються на дві великі групи за принципом формування зображення – растрова та векторна графіка. Тому розглянемо формати цифрових зображень в цьому розрізі.

На рисунку 1.1 наведена класифікація форматів для цифрових зображень. Матриці пікселів, або двовимірні масиви даних, відносять до растрових зображень, кожен елемент яких – ділянка оригіналу з обчисленим пересічно колірним показником.

Існує два способи для отримання растрових зображень. Перший носить назву “сканування растрового зображення”, і здійснюється він за допомогою певного пристрою – сканера, де кожен оптичний елемент ПЗЗ-матриці (або ПЗЗ-лінійки) зчитує характеристики яскравості і колірні характеристики зображення-оригіналу. Далі ці характеристики перетворюються у двійковий код з колірної палітри і посилаються до матриці пікселів. Другий спосіб використовує проєктування оригіналу на ПЗЗ-матрицю через об’єктив. Такий спосіб для перетворення растрових зображень використовується у цифрових фотоапаратах та відеокамерах.

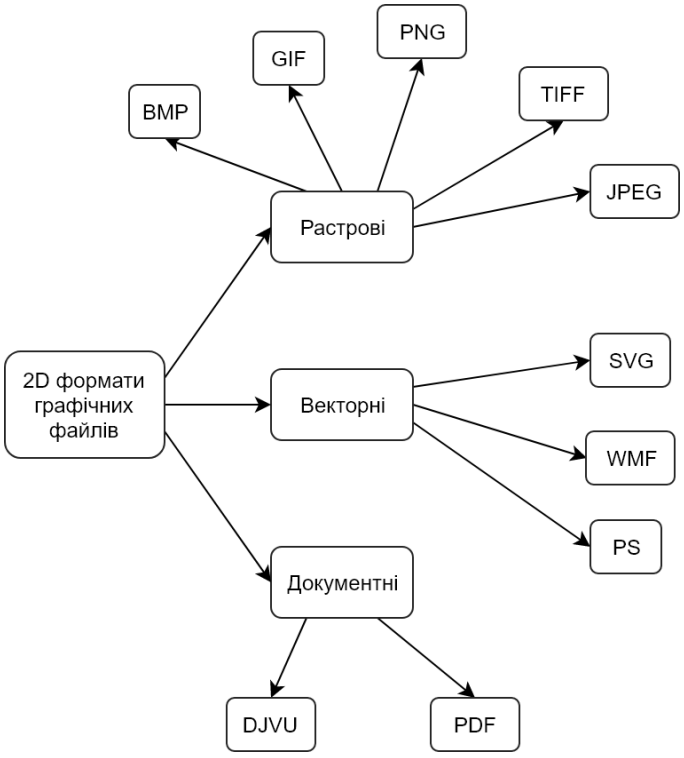

Рисунок. 1.1 – Класифікація форматів для графічних цифрових зображень

Глибина кольору і розмір зображення – основні характеристики растрового зображення.

Глибина кольору – характеристика, що призначена визначати кількість відтінків, що можуть відобразити елементи матриці пікселів, та якість відтворення кольорів зображення. Кожен елемент масиву матриці – число у двійковій системі числення. Розмірність цього елемента визначається у бітах. Тобто, глибину кольору можна визначити кількістю біт на піксель зображення. Вісім біт (або один байт) можуть задати 256 кольорів, як правило, чорно-білих. Колір пікселя задається за колірною схемою RGB (рисунок 1.2), тобто за поєднанням червоного, зеленого і синього кольорів у певних пропорціях.

Розмір зображення – кількість стовбців і рядків матриці, що були використані для збереження зображення. Щоб змінити розмір зображення, можна змінити фізичний розмір цього зображення під час друку, у такому випадку розмір матриці пікселів лишиться незмінним.

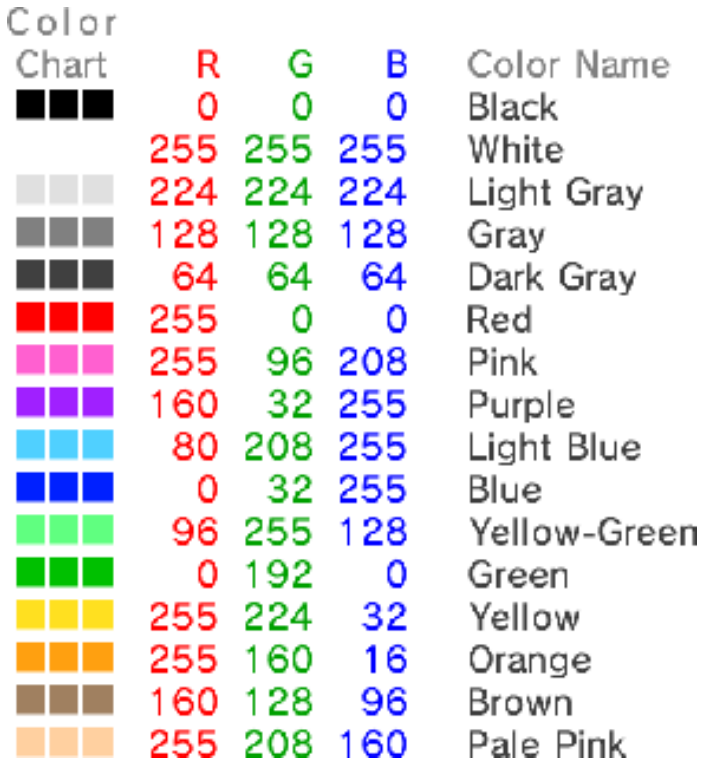

Рисунок 1.2 – Приклади представлення кольорів пікселя через три кольорових компоненти (схема RGB)

Під час аналого-цифрового перетворення втрати певної кількості інформації неминучі, так як дискретизація проводиться за допомогою усереднення і підсумування потоку аналогової вихідної інформації. З цього витікає головна вада растрових цифрових зображень – їх неможливо масштабувати без втрати якості.

Ключова сфера використання растрових зображень – фотографічні ілюстрації. У випадках, коли необхідно відтворити аналоговий оригінал (наприклад, фотографію, малюнок, або будь-який елемент, який складно та нераціонально переводити у вектори), використовуються растрові зображення. Векторні зображення, у свою чергу, є зовсім іншим видом цифрових зображень. Вектор і крива Безьє – найменші елементи векторного зображення. Контрольна вершина, або як її ще називають, контрольна точка або вузол – основний керуючий елемент кривої Безьє. Координати вузла і дві керуючі точки визначають ступінь кривизни лінії. Контур зображення – масив даних, який вміщає в собі координати контрольних і керуючих точок, та характеристики кривої, такі як: товщина, колір, напрямок, а у випадку замкнутої кривої – колір та тип заливки.

Векторні зображення можна отримати такими методами: ручне трасування оригіналу та автоматичне трасування. Головним плюсом векторного зображення є можливість масштабувати зображення без втрати якості. Також ще одна перевага векторних зображень – відносно невеликий розмір файлів, що є вигідним під час передачі векторних зображень по електронних каналах зв’язку.

Основний мінус векторних зображень – відтворення оригіналу у спрощеному вигляді майже у всіх випадках. У векторному зображенні буває неможливо відтворити певні деталі оригінального зображення. Векторні зображення часто важко назвати повноцінними ілюстраціями. Цифрові зображення змішаного типу – це масиви даних, які вміщують в собі інформацію у вигляді і матриці пікселів, і опису векторів, текстових блоків, кривиї Безьє і примітивів. [4].

Поняття шару лежить у основі вертикальної структури векторно-растрових зображень. Шар – це сфера даних, яка включає в себе інформацію про окремі елементи вертикальної структури зображення.

Зображення змішаного типу отримуються за допомогою зведення вихідних растрових і векторних елементів у графічних редакторах. Також до зображень змішаного типу відносяться результати програм комп'ютерної верстки, в яких основним векторним елементом є текстові блоки.

Векторнорастрові зображення поєднують в собі плюси та мінуси тих типів зображень, які присутні в них у вигляді елементів або шарів.

Головна перевага зображень змішаного типу – можливість вільного редагування кожного шару окремо, а провідний недолік – великий обсяг масиву даних і, відповідно, кінцевого файлу. [4]

Тож, всупереч недолікам растрових зображень, вони є найпопулярнішими у використанні – растрова графіка використовується майже всюди. За допомогою такого виду графіки можна створити практично будь-яке зображення, не дивлячись на складність, на відміну від векторної, у якій неможливо передати ефект плавності переходу кольорів без втрат у розмірі файлу.

Існує декілька десятків форматів растрових зображень. У кожного з цих форматів є свої плюси та мінуси, які визначають доцільність їх використання при роботі з тими чи іншими зображеннями:

– BMP (англ. BitMap image – бітова карта зображення). Зображення такого формату зберігаються у файлі без стискання, попіксельно, тому ці файли досить великі, але у той же час зручні для точної передачі даних. Стандартне розширення імені файлів цього типу BMP. З файлами цього формату працюють майже всі графічні редактори растрової графіки.

– JPEG (англ. Joint Photographic Expert Group – об'єднана експертна група в галузі фотографії). Даний формат використовує ефективні алгоритми стиснення даних, що дозволяє зменшити розмір кінцевих файлів, однак цей результат

досягається через втрату частини даних та погіршення якості зображення. Цей формат варто використовувати для зберігання багатокольорових зображень з такими переходами кольорів, де втрата якості буде малопомітна. Стандартним розширенням імені файлів такого формату є JPG або JPEG. Практично всі редактори растрової графіки можуть працювати з файлами цього формату.

– GIF (англ. Graphics Interchange Format – графічний формат для обміну). «Найщільніший» з графічних форматів, тому що є підходящим для стиснення, оскільки використовує невелику кількість кольорів. Найбільше розповсюдження отримав через можливість зберігання та передачі анімованих зображень, але звісно окрім цього він дає змогу працювати з зображеннями, що містять до 256 кольорів (наприклад, мальовані ілюстрації).

– PNG (англ. Portable Network Graphic), на відміну від GIF, являється універсальним форматом графічних файлів та має в рази вищий ступінь стиснення даних у файлі, при цьому не допускаючи їх втрати. Таким чином з його допомогою можна використовувати набагато більше кольорів, ніж у форматі GIF.

– TIFF (англ. Tagged Image File Format), на відміну від попередніх, навпаки має значно більший розмір файлу. Пов’язано це з тим, що з його допомогою зберігають зображення з високою якістю, що відкриває можливості для більш точної деталізації, а тому, як наслідок, й обумовлення настільки широкого його застосування в поліграфії або, наприклад, при скануванні зображень.

Передача зображень мережею Інтернет накладає певні вимоги та обмеження, адже великий розмір зображень буде викликати як труднощі при передачі, так і зайві питання серед людей. Саме тому, дуже важливо зберігати незначний розмір файлів, адже це напряму впливає на швидкість передачі даних. Саме тому, при розробці та проектуванні веб-сторінок, зазвичай перевага надається тим графічним форматам, які мають високий коефіцієнт стиснення даних. Наприклад - JPEG, GIF, PNG.

Векторна ж графіка має дещо іншу ситуацію. Навіть не дивлячись на те, що майже кожен векторний графічний редактор зберігає файли у власному форматі, їх

різноманітність значно менша. Серед існуючих форматів варто згадати декілька найбільш виразних. Наприклад:

– WMF (англ. Windows MetaFile) – універсальний формат для програм, що працюють в ОС Windows. Використовується для зберігання колекції графічних зображень Microsoft Clip Gallery. Можливі розширення імен файлів – WMF, EMF, WMZ, EMZ.

– CGM (англ. Computer Graphic Metafile) – широко використовується як стандартний формат векторних графічних даних в мережі Інтернет.

– SVG (Scalable Vector Graphics) – це універсальний формат для двовимірної графіки, який дає змогу з високою якістю зберігати у файлі текст, графічне зображення і анімацію, а також вони можуть додатково стискатися програмами-архіваторами. З ним можуть працювати практично усі векторні графічні редактори. Широке застосування отримав у інженерній графіці і при розробці веб-сайтів.

– CDR (англ. CorelDRaw files) – стандартний формат файлів векторного графічного редактора CorelDraw. Зображення у файлі може мати кілька сторінок, дає змогу зберігати не тільки векторну графіку, а й текст і растрові зображення. Максимальний розмір об’єктів, створених за допомогою даного редактора складає 45 х 45 м. Файли даного формату можуть мати розширення CDR або CDT.

– AI (англ. Adobe Illustrator files) – стандартний формат файлів редактора векторної графіки Adobe Illustrator. На відміну від згаданого вище CDR, зберігає у файлі тільки одну сторінку, а максимальний розмір об’єктів, що були створені за допомогою даного редактора, складає лише 3х3 м.

Також до графічних зображень можна віднести файли, створені у креслярських та конструкторських програмах, таких як AutoCAD, ArhiCAD, KOMPAS тощо, але вони є досить специфічними.

Окрім формату, існують наступні класифікаційні характеристики графічних контейнерів:

За протяжністю контейнери можна поділити на два типи: безперервні(потокові) і обмеженої (фіксованої) довжини. Потоковий контейнер має за особливість те, що у ньому неможливо визначити його початок або кінець [23]. Разом із тим та як певний наслідок, немає можливості дізнатися заздалегідь, якими будуть наступні шумові біти. Через це, приховуючі повідомлення біти необхідно включати в потік в реальному масштабі часу. Що ж стосується безпосередньо генерації цих бітів, то для цього прибігають до використання спеціального генератора, що задає відстань між послідовними бітами в потоці.

Передача даних у безперервному потоці накладає певні умови та складності як на відправника повідомлення, так і на отримувача. Для одержувача головна складність полягає у тому, щоб достовірно визначити коли саме починається передача прихованого повідомлення. Якщо у потоковому контейнері присутні сигнали синхронізації або відомі кордони пакета, що передається, то приховане повідомлення починається відразу після одного з цих маркерів. Що стосується відправника, то головною проблемою для нього є невизначеність у тому чи буде потік контейнера достатньо довгим для розміщення цілого таємного повідомлення.

Таким чином, ми маємо наступну ситуацію: використання файлів-контейнерів фіксованої довжини дає нам можливість заздалегідь знати розмір файлу і, як наслідок, можливість вибрати приховуючи біти у псевдовипадковій послідовності; з іншого боку, як зазначалося раніше, контейнери фіксованої довжини мають і обмежений обсяг простору для вбудовування повідомлення, через що повідомлення, яке вбудовується може не поміститися в файл-контейнер.

Також, існує й інший недолік: у той час, як справжній випадковий шум має експоненціальний розподіл довжин інтервалу, в нашому випадку відстані між приховуючими бітами рівномірно розподілені між найбільш короткими і найбільш довгими заданими відстанями. Безперечно, можна долучитися до допомоги апаратних генераторів та породити псевдовипадкові експоненціально розподілені числа, але цей шлях зазвичай занадто трудомісткий. Саме тому, на практиці зазвичай

використовуються саме контейнери фіксованої довжини, як найбільш поширені і доступні.

Нижче наведено список можливих варіантів контейнерів [24]:

– генерується самою стеганосистемою (також, цей підхід відомий як конструююча стеганографія). Наприклад, коли для вбудовування повідомлення, у якості контейнера генерується фрактал Мандельброта, який може бути згенерований, наприклад, за допомогою програми MandelSteg.

– обирається з вибірки деякої безлічі контейнерів, або більш відоме як селектуюча стеганографія. Для цього способу складається або генерується вибірка з великої кількості альтернативних контейнерів, щоб потім вибрати найбільш підходящий для приховування повідомлення. Головним критерієм при остаточному виборі контейнера з такої вибірки є його природність. Але, попри все, головною проблемою лишається те, що навіть оптимальна організація контейнеру не дозволяє заховати значну кількість даних навіть при великому обсязі самого контейнера.

– контейнер надходить ззовні, і в нього потрібно вбудувати повідомлення. В даному випадку відсутня можливість вибору контейнера. Такий підхід називають безальтернативною стеганографією.Отже, ми розглянули основні типи форматів цифрових зображень з точки зору використання їх у якості контейнерів для стеганографічних цілей.

1.2 Визначення критеріїв та показників ефективності стеганосистем

Для формування сукупності критеріїв та показників ефективності розглянемо структурну схему стеганосистеми для визначення її окремих елементів та критеріїв їх важливості.

Приймаючи стеганосистему як систему зв’язку, отримуємо наступну структурну схему (рисунок 1.3).

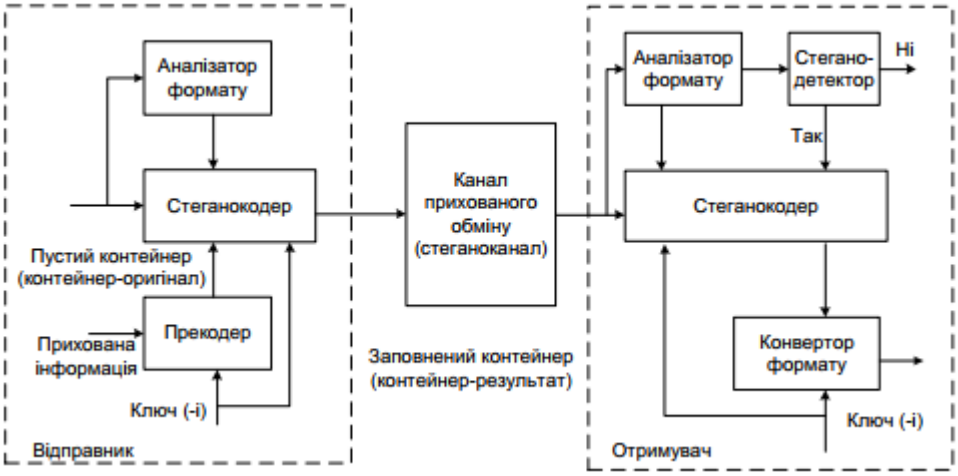

Рисунок 1.3 – Структурна схема стеганосистеми

При передачі повідомлення методом прямого розширення спектру для контейнерів-зображень приймається двійкова ПВП $\Phi_i = \left(\varphi_{i_0}, \varphi_{i_1}, \dots, \varphi_{i_{n-1}}\right)$ як дискретний сигнал довжини n із деякої множини $\Phi = \{\Phi_0, \Phi_1, \dots, \Phi_{M-1}\}$, при цьому повідомлення позначається як послідовність $m_0, m_1, \dots, m_{k-1}$ окремих бітів у полярному вигляді $m_i \in \{-1; 1\}$.

Суть полягає у тому, щоб розподілити повідомлення по контейнеру, який приймається за шум, так, щоб приховати будь-яке цілenаправлене втручання з метою приховання даних. Тому, щоб задовільнити цю умову, контейнер мусить бути набагато більшим, ніж саме повідомлення, що приховується.

Таким чином Рисунок 1.3 перетворюється на Рисунок 1.4.

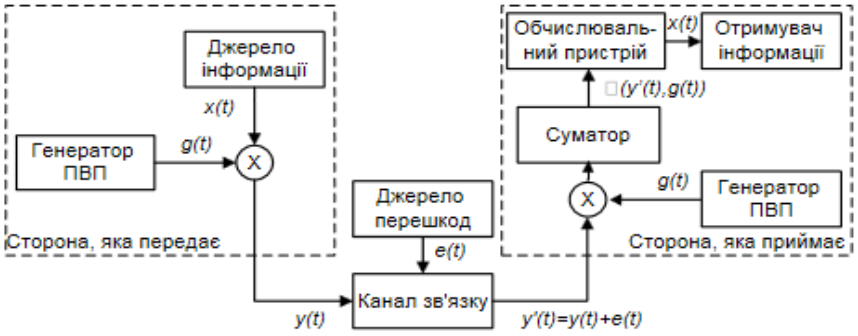

Рисунок 1.4 – Структурна схема передачі інформації з використанням прямого розширення спектру

Кожен сигнал являє собою ПВП, які описуються наступним чином:

$$\forall i \in \{0,1,\dots,M-1\}: \Phi_i = \left(\varphi_{i_0}, \varphi_{i_1}, \dots, \varphi_{i_{n-1}}\right),$$
$$\forall j \in \{0,1,\dots,n-1\}: \varphi_i \in \{-1,1\} \quad (1.1)$$

Кратність розширення спектра задається базою дискретних сигналів:

$$B = T \cdot \Delta F, \quad (1.2)$$

де T - тривалість одного елементарного сигналу φ_i,

ΔF - смуга частот сигналу Φ_i.

Якщо $B = 1$, то сигнали називаються простими. Якщо $B > 1$, то сигнали називаються складними.

Для послідовностей з множини Φ виходить, що $F = n\frac{1}{T}$. Звідки отримуємо, що $B = n \gg 1$, тобто використання $\Phi_i \in \Phi$ дозволяє в n раз розширити спектр частот переданих сигналів.

Береться до уваги, що різні сигнали з множини Φ є слабокорельовані, тобто коефіцієнт їх взаємної кореляції приблизно дорівнює нулю:

$$\forall i \neq j: \rho\left(\Phi_i, \Phi_j\right) = \sum_{u=0}^{n-1} \varphi_{i_u} \varphi_{j_u} \approx 0. \quad (1.3)$$

Стегано-контейнер S формується наступним чином:

$$S = C + G \cdot E, \quad (1.4)$$

де C – вихідний контейнер,

E - посилений модульований сигнал, який, в свою чергу, визначається як:

$$E = \sum_{i=0}^{k-1} m_i \Phi_i \tag{1.5}$$

$G > 0$ – коефіцієнт посилення, який грає роль «потужності» модульованого сигналу *E*.

Відновлення відбувається наступним чином:

$$\forall i : \ \rho(\Phi_i, C) \approx 0 \tag{1.6}$$

Важливо, що кожен сигнал з множини Φ не корельований з вихідним контейнером.

Значення коефіцієнта кореляції визначається як:

$$\rho(\Phi_i, S) = \rho(\Phi_i, C + G \cdot E) = \rho\ (\Phi_i, C) + G \cdot \rho(\Phi_i, E) \approx$$
$$\approx G * \sum_{j=0}^{k-1} m_j \sum_{u=0}^{n} \varphi_{i_u} \varphi_{j_u}. \tag{1.7}$$

Для всіх $j \neq i$ остання сума:

$$\sum_{u=0}^{n} \varphi_{i_u} \varphi_{j_u} \approx 0 \tag{1.8}$$

отже, маємо:

$$\rho(\Phi_i, S) \approx G \cdot m_i \cdot n, \tag{1.9}$$

тобто знак $\rho(\Phi_i, S)$ збігається зі значенням m_i (3):

$$m_i = sign\big(\rho(S, \Phi_i)\big) = \{-1, \rho(S, \Phi_i) < 0;\ +1, \rho\ (S, \Phi_i) > 0. \tag{1.10}$$

На основі зазначених характеристик формуються критерії ефективності стеганосистеми.

Коли мова йде про «ефективність», зазвичай мається на увазі змога стеганосистеми виконувати головні задачі стеганографії, а саме: секретна передача та її висока швидкість при великому об’ємі інформації. На те, наскільки ефективною виявиться створена стеганосистема, маж свій вплив безліч факторів, до яких можна віднести перелік технічних характеристик, що мають бути точно описані математично і мати певні кількісні ознаки. Якісні характеристики відрізняються тим, що немає змоги описати їх математичним способом, але при цьому вони грають не менш значну роль у створенні ознак ефективності:

– Невидимість – стеганографічний опір. Дана обов’язкова ознака має бути присутньою у всіх абсолютно стеганосистемах. Якщо розглядати графічну стеганосистему, то її надійність значно залежить від спотворень, які можуть виникнути в оригінальному зображені в процесі вбудовування повідомлення. При умові, якщо атака на зображення відбувається із використанням простого візуального аналізу, то вимогу стеганографічного опору не можна вважати задовільною.

– Ємність. Ефективність роботи цифрового зображення при зберіганні секретної інформації у багатьох факторах залежить від того, скільки важить інформація, що передається через нього. Якщо розглядати у вигляді чилового виразу, то дана характеристика часто представлена у вигляді відсоткового співвідношення об’єму повідомлення, що вбудовується, до величини контейнера. Між розміром повідомлення та стеганографічною стабільністю був встановлений міцний зв'язок, тривка залежність. Вона обернено пропорційна, тобто чим більшого обсягу буде використане повідомлення, яке вкладене у передніше виділений контейнер, тим менш надійним буде його приховування.

– Заповнений контейнер може характеризуватись стійкістю до модифікації ймовірністю відновлення повідомлення за тієї умови, що він зазнав певного стиснення. Стиснення з втратами є окремим випадком модифікації. Особливе

значення для технології цифрових водяних знаків (ЦВЗ) має цей коефіцієнт ефективності. Можемо вирізняти два варіанти здійснення модифікації заповненого контейнера: ненавмисна і та, яка здійснена навмисно. Перша, де стиснення, помилки з'являються при передачі файлу по каналах зв'язку із різними перешкодами, і друга - через спроби порушення авторських прав шляхом знищення цифрових водяних знаків.

– Обсяг розрахунків, які необхідні для вбудовування повідомлення в цифрове зображення. Попри те, що спостерігається швидке зростання потужності комп'ютерів найновішого часу, проблема складності обчислення алгоритмів вбудовування продовжує відігравати провідну роль у деяких випадках здійснення стеганографії. Здебільшого це IT-системи реального часу, що мають рамками виконання алгоритму з обмеженням у часі. Наприклад, канал прихованого голосового зв'язку: Audio-інформація, що вбудована в потік графічних файлів, які надсилаються по мережі. В цьому випадку, щоб уникнути будь-яких втрат у якості інформації, яка передається, цифрові зображення (пакети даних) повинні бути заповнені повідомленнями та доставлені моментально, без затримки.

– Використаний графічний формат. Ефективність використання цифрових зображень у стеганографії здебільшого буде залежати від формату їх зберігання. Широковідомим типом носія у стеганографії комп'ютерної графіки є файли зображень BMP. Можемо пояснити це тим, що для стеганографії більш за все підійдуть файли у форматах, із методами стиснення без втрат. Такі типи стиснення типові для зображень у таких форматах, як BMP, TIFF, PNG, TGA , також вибір формату BMP аргументується високою якістю зображення та простотою формату [4].

Вимоги, які висуваються до будь-якої стеганосистеми наступні: [19]:

– властивості контейнера необхідно модифікувати, для унеможливлення виявлення змін при візуальному способі контролю. Вказана вимога встановлює якість приховування повідомлення, що впроваджується: для забезпечення вільного проходження стеганоповідомлення по каналу зв'язку необхідно, щоб воно жодним

чином не привернуло увагу об'єкти, що атакує.

– стеганоповідомлення повинно мати стійкість до спотворень, включно із зловмисними. Під час передавання зображення може трансформуватися різними способами: зменшуватися чи збільшуватися, переходити в інший формат, тощо. В окремих випадках воно може бути стисненим, включно з використанням алгоритмів стиснення з втратою даних.

– щоб зберегти цілісність вбудованого повідомлення потрібно використовувати код з виправленням помилки.

– з метою підвищення надійності вбудованого повідомлення, воно повинно дублюватись.

1.3 Порівняльний аналіз стеганосистем та обґрунтування напрямку досліджень

Порівняння стеганосистем відбувається за низкою різноманітних показників залежності від мети та завдань, які ставить конкретний користувач. Загальний принцип формування показників для оцінки стеганосистем показано на рис 1.5.

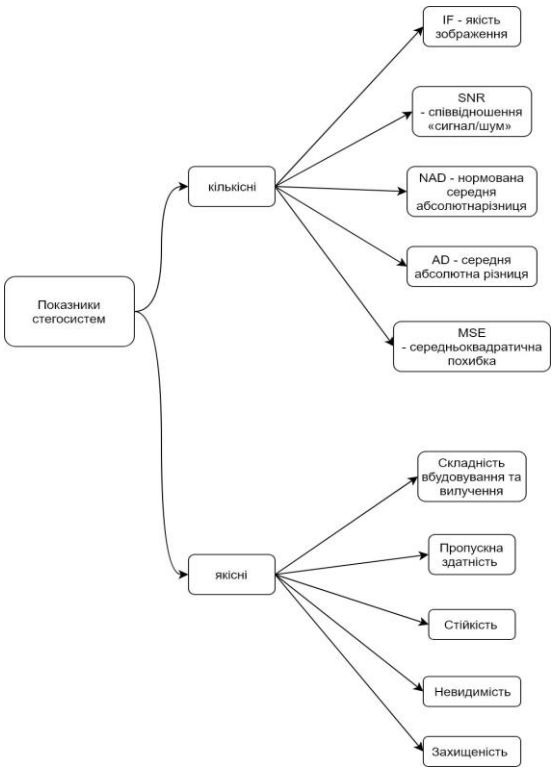

Рисунок. 1.5 – Орієнтовний перелік показників для порівняння стегосистем

Стеганографічним системам притаманні різного роду атрибути, проте, серед них найважливішими можна визначити наступні:

– Ємність (Capacity) – кількість бітів прихованого повідомлення, які можуть бути передані за допомогою цього методу в зображенні фіксованого розміру. Стегосистема повинна забезпечувати необхідну ємність [4].

– Стійкість (Robustness) – це характеристика, що показує можливість вилучення прихованої інформації після проведення загальних операцій з обробки зображень: лінійні та нелінійні фільтри (додавання розмитості, покращення різкості зображення, медіанна фільтрація), стиснення з допустимими втратами, зміни контрастності, операції з кольорами, передискретизації, зміна масштабу, зміна орієнтації зображення, додавання шумових ефектів, зміна розмірів зображення, роздруку/зняття копіюй/сканування, зміна розташування пікселів у невеликій прилеглій ділянці, розкладання кольорів та інші. При цьому враховуємо, що за визначенням стійкість не включає атаки на методи імплементації, які основуються на знанні алгоритму приховування або вилучення.

Стійкість - це характеристика, що показує можливість до протидії «випадковим», незапланованим модифікаціям, або загальним операціям із вибраними зображеннями. Невидимість (Invisibility, Perceptual transparency) – це критерій, що характеризує можливості зорової системи людини (ЗСЛ) виявити існування секретного повідомлення без застосування для цього спеціальних засобів. Секретні дані рахуються непомітними тоді, коли середньостатистична людина не може відрізнити порожній контейнер від заповненого. Цей показник можна оцінити за допомогою досліду, в якому інформація про тестування прихована від учасників (сліпий тест), і який широко використовується в психо-візуальних експериментах: при цьому суб’єктам в довільному порядку надається можливість вибору з великої кількості заповнених і порожніх контейнерів. Суб'єкти повинні визначити, які саме контейнери містять секретну інформацію [3]. Поняття невидимості можна визначити іншим способом, який пов’язаний із статистичною моделлю джерела зображення. При

цьому ми рахуємо, що прихована інформація є невидимою, у випадку, коли заповнене зображення-контейнер відповідає моделі джерела, з якого було отримано початкове зображення. При цьому зображення-контейнер можна об'єктивно обчислити, зокрема, за допомогою показника IF.

Захищеність (Security) – здатність, за допомогою якої вбудовані дані не можуть бути видалені при застосуванні цільових атак, що основані на відомому алгоритмі вилучення та вбудовування, та наявності інформації щонайменше про один носій з прихованим повідомленням. Уявлення захищеності також містить в собі процедурні атаки, такі, що грунтуються на знанні про наявність часткової модифікації контейнера з огляду на присутність вбудовування [1].

Складність вбудовування/вилучення – чисельність стандартних операцій, що виконуються для вбудовування і визначення наявності секретного повідомлення. (Як було наголошено, стегосистеми зобов'язані мати прийнятну обчислювальну складність реалізації). Вищезазначені вимоги є взаємно суперечливими і не можуть бути оптимальними водночас. При необхідності приховати повідомлення великого розміру всередині зображення, нереально вимагати великої невидимості і виняткової стійкості. Завдання можна виконати лише при досягненні певного компромісного рішення, що задовольняє вимоги для даного випадку. І навпаки, якщо вимагається стійкість до великих спотворень, то повідомлення, що ретельно приховується, не може бути дуже довгим. [3]

В даний час найбільш відомими і широко використовуваними наборами тестів для оцінки якості цифрових водяних знаків (тобто алгоритмів вбудовування цифрових водяних знаків (ЦВЗ)) є StirMark, UnZign тощо. Спеціальні тести не призначені для націлювання на будь-які конкретні алгоритми і в принципі можуть вважатися універсальними тестами стабільності останніх. Стеганографічні алгоритми тестуються на виявлення наявності вбудованого ЦВЗ і, якщо отримано позитивний результат, розкодовується вбудоване повідомлення. Коли виявлено ЦВЗ і/або вміст повідомлення повністю використано за допомогою частини набору тестової атаки,

алгоритм тестування позначається як невдалий для цього типу атаки (зазвичай значення «1» встановлюється відповідно до значення цієї атаки, інакше "0"). Відсоток правильно виявлених ЦВЗ (кількість завершених атак проти загальної кількості атак) є показником ефективності, який використовується для порівняння відносної ефективності алгоритмів стеганографії [3; с. 5].

Дозволяючи виявити наявні слабкі сторони алгоритмів інвазії ЦВЗ (в основному це стосується геометричних спотворень, ці програми мають багато недоліків, які не дозволяють прийняти безпомилкове і продумане рішення щодо ефективності того чи іншого алгоритму.

Основний недолік полягає в цьому. який не враховує ймовірність «помилкової тривоги», ймовірність виявлення ЦЗВ у порожніх контейнерах). Таким чином, для двох алгоритмів з однаковою ймовірністю «промаху» (ймовірність невиявлення цілі в заповненому контейнері), але різною ймовірністю «хибного спрацьовування» буде прийнято однакове рішення з точки зору їх ефективності. Крім того, немає окремої оцінки теганодецхор і якості декодера, а помилково витягнуте повідомлення вважається неправильно виявленим ЦВЗ. що, звичайно, спотворює результати. Також при оцінці стійкості алгоритмів до конкретних атак програми використовують один і той же ключ. Однак, оскільки результати визначення наявності ЦВЗ залежать від кількості ключів, очевидно, що для отримання більш точного опису продуктивності детектора і декодера слід використовувати велику кількість ключів. Ще одним недоліком є відсутність оцінки часу впровадження та виявлення/відновлення ЦВЗ. Нарешті. оцінки продуктивності, отримані для різноспрямованих атак, об’єднуються як такі, що мають однакову вагу в загальному індексі продуктивності – іншими словами, передбачається, що на практиці всі атаки та контейнери мають однакову ймовірність виникнення. Однак у багатьох практичних випадках цей підхід має недоліки, оскільки деякі типи атак (наприклад, стиснення з втратами) можуть виконуватися набагато частіше, ніж інші (наприклад, віддзеркалення) [3; с. 5].

Окрім ефективності стегетодетектора та декодера, дві інші особливості стеганосистем також вирішують: пропускна здатність та кінцева стійкість до перетворення обмежені для деяких типів атак.

Пропускна здатність - це максимально можливий середній обсяг інформації, який можна вбудувати в один елемент контейнера (наприклад, піксель або часовий вимірс) і надійно витягнути згодом — без помилок або з відсотком помилкових бітів. яка не перевищує заздалегідь визначений поріг. Межа стійкості до атаки алгоритму під час трансформації контейнера визначає межу трансформації структури контейнера або найскладнішу атаку, яку може витримати алгоритм, за умови, що надійне виявлення/вилучення повідомлень продовжується.

При проєктуванні стегосистем має виконуватися ряд вимог для того, щоб її можна було вважати надійною та якісною. До таких вимог можна віднести наступне: [2]

– Контейнер, після вбудовування повідомлення, не має містити візуальних шумів та дефектів, тобто не повинен відрізнятися від незаповненого контейнеру. Першою думкою у цьому випадку буде впроваджувати приховане повідомлення у візуально незначущі області сигналу, але, ця думка хибна! Хибна вона через те, що ці ж самі області, як правило, використовують і алгоритми стиснення, тому, якщо зображення буде надалі піддаватися стисненню, то приховане повідомлення може зруйнуватися. Саме тому, біти повинні вбудовуватися в візуально значущі області, а відносна непомітність може бути досягнута за рахунок використання спеціальних методів.

– Стегосистеми цифрового водяного знаку (ЦВЗ) повинні мати як можна нижчу ймовірність помилкового виявлення прихованого повідомлення в сигналі, що насправді цього повідомлення не містить. У критичних системах таке виявлення може призвести до серйозних та навіть катастрофічних наслідків.

– Повинна забезпечуватися необхідна ємність (пропускна здатність).

Стегосистеми повинна мати прийнятну обчислювальну складність реалізації. При цьому можлива асиметрична за складністю реалізації система ЦВЗ, тобто складний стеганокодер і простий стеганодекодер. [4]

За рівнем забезпечення таємності стегосистеми поділяються на нестійкі системи, теоретично стійкі та практично стійкі [11].

Використання стеганоконтейнерів-зображень дуже перспективна тема для наукових досліджень, які можна обґрунтувати наступним чином:

– нагальна потреба всебічного захисту будь-якого медіаконтенту від його нелегального розповсюдження;

– Цифрове представлення відносно великої кількості зображень, що дозволяє вбудовувати туди широкоформатні ЦВЗ або підвищувати стабільність таких вбудовувань;

– Відсутні обмеження реального часу, які могли б створювати додаткові вимоги при використанні прихованих елементів у стеганоконтейнері;

– Натуральні забраження мають відносно великі ділянки із шумовою структурою, що є сприятливим для вбудовування інформації;

– Природня властивість будови людського ока, при якій незначні зміни у кольорі, яскравості, контрастності, рівню шумів та/або зміна контурів маленьких деталей залишаються непоміченими;

– Активний сучасний розвиток методів цифрової обробки зображень. Проте цей розвиток також завдає певні труднощі для забезпечення стабільності ЦВЗ - у міру вдосконалення техніки стиснення можливостей для вбудовування секретних повідомлень стає все менше. Розвиток теорії та практики алгоритмів стиснення зображень змінив також і погляди на техніку самого вбудовування знаку. Якщо вперше було запропоновано вбудовувати інформацію в нерелевантні біти, щоб зменшити видимість, то сьогодення диктує вбудування ЦВЗ лише у найважливіші області зображення, при знищенні якої неодмінно будуть непоправні наслідки, які однозначно призведутть до погіршення самого зображення або його контексту.

З вищенаведених причин стає зрозуміло, що при розробці сучасних методів стеганографії слід обов’язково враховувати не тільки властивості ЦВЗ, але й алгоритми стиснення цифрових зображень та інші засоби. Тому це обумовило напрямок дослідження математичних моделей, методів та обчислювальних алгоритмів приховування даних у контейнери-зображення із розширенням спектру. Враховуючи різноманітність методів стеганографії, запропоновано проводити приховування методом прямої послідовності, який ще має назву методу прямого розширення спектра дискретних сигналів.

Отже, ми визначили основні критерії та методи, які будуть використовуватись в практичному дослідженні, тому можемо перейти до розробки алгоритмів стеганосистеми.

2 ДОСЛІДЖЕННЯ МОДЕЛЕЙ ТА МЕТОДІВ ПРИХОВУВАННЯ ДАНИХ У КОНТЕЙНЕРИ-ЗОБРАЖЕННЯ ІЗ РОЗШИРЕННЯМ СПЕКТРУ МЕТОДОМ ПРЯМОЇ ПОСЛІДОВНОСТІ

2.1 Дослідження технології прямого розширення спектру та її застосування в стеганографії

Розглянемо сутність технології прямого розширення спектру. Для передачі даних у стеганосистемі як системі зв'язку інформаційний сигнал $x(t) = \{+1\ -1\}$ модулюється за допомогою множення на розширюючий сигнал g(t)

$$g(t) = \Phi_i \in \Phi, \tag{2.1}$$

де Ф – ПВП з дискретних сигналів методів, які будуть розглянуті нижче.

Таким чином, розширений сигнал представляється як:

$$y'(t) = y(t) + e(t), \tag{2.2}$$

де e(t) – помилки у каналі зв'язку.

Обчислення коефіцієнта кореляції на прийомній стороні відбувається за наступним правилом:

$$\rho\big(y'(t), g(t)\big) \approx \rho\big(y(t), g(t)\big) = x(t)\frac{1}{n}\sum_{z=0}^{n-1} e(t)\Phi_{i_z}. \tag{2.3}$$

Але оскільки критерії ГПВП визначають, що у ПВП кількість одиниць співпадає з кількістю нулів (у нашому випадку, це «-1»), то правило представляється у наступному вигляді:

$$\rho\big(y'(t), g(t)\big) \approx \rho\big(y(t), g(t)\big) = x(t)\frac{1}{n}\sum_{z=0}^{n-1} \quad (\Phi_{i_z})^2 = x(t). \qquad (2.4)$$

Звідси,

$$x(t) = \{+1, \rho\left(y'^{(t)}, g(t)\right) \approx +1 \ \ -1, \rho\left(y'^{(t)}, g(t)\right) \approx -1 \qquad (2.5)$$

Використання підходу прямого розширення спектра забезпечує передачу багатьох сигналів одночасно в одній смузі частот, тому прийнята аддитивна сума модульованих сигналів на прийомній стороні не доставить неприємностей. Коефіцієнт кореляції обчислюватиметься наступним чином:

$$\rho\big(\sum_l \ y_l(t), g(t)\big) = \frac{1}{n}\sum_l \ \sum_{z=0}^{n-1} x_l(t)\Phi_{l_z}\Phi_{i_z} \qquad (2.6)$$

Метод розширення спектра методом прямої послідовності (РСПП) за ефективністю перевершує метод псевдовипадкового перестроювання частоти, але складніший для реалізації. Такий метод має на меті збільшення тактової частоти модуляції, заразом із цим кожний символ повідомлення, яке передається, перебуває в певній відповідності, співвідношенні досить довгій псевдо випадковій послідовності.

Метод розширення спектра прямою послідовністю (РСПП) - це модуляція функції сигналу, яка приймає псевдовипадкові значення у встановлених межах, помножена на тимчасову константу (швидкість проходження елементів сигналу). Сигнал, що отримано, містить складові всіх частот, які при розширенні корегують енергію сигналу в широкому діапазоні.

Найбільш популярний вид методу розширення спектра прямої послідовності, спрямованим на вбудовування інформації у зображення - модифікація за авторством Смітта (JR Smith) та Коміскі (B.O. Comiskey). Модуляція за наступним алгоритмом:

кожен біт повідомлення m_i є деякою базисною функцією ϕ_i розмірністю X*Y, яка помножена на +1 або -1 , залежно від значення біта (1 або 0):

$$E(x,y) = \sum_i m_i * \varphi_i(x,y) \tag{2.7}$$

Модульоване повідомлення E(x,y) попіксельно підсумовується іззображенням-контейнером C(x,y). Результатом є зображення, що містить S(x, y)= C(x, y) + E(x, y), при $x = 1..X$, $y = 1..Y$.

Щоб домогтися відсутності спотворень вже вбудованого біта повідомлення, базисні функції мають бути ортогональними:

$$\langle \varphi_i, \varphi_j \rangle = \sum_{x,y}^{X,Y} \varphi_i(x,y) * \varphi_j(x,y) = n_\varphi * G^2 * \delta_{i,j} \tag{2.8}$$

де n_ϕ – кількість значущих пікселів у базовій функції;

G^2 – середня потужність, що припадає на піксель;

$$\delta_{i,j} = \begin{cases} 1, \text{при } i = j \\ 0, \text{при } i \neq j \end{cases}$$ – дельта символ Кронекера. (2.9)

В ідеалі всі базові функції ϕ_i повинні бути ортогональними до зображення-контейнера: $\langle \widetilde{N}, \varphi_i \rangle = 0, \forall i$. Однак насправді практично неможливо підібрати контейнер, який був би повністю ортогональним довсіх базисних функцій $\boldsymbol{\phi}_i$. У такому разі має бути введена величина похибки $\langle \widetilde{N}, \varphi_i \rangle = \Delta \approx 0$, яка враховується збільшенням потужності G^2.

Для того, щоб ефективно приховати інформацію, необхідно використовувати велику кількість базисних функцій, ортогональних до типових зображень. Кодування зображень висуває прямо протилежну вимогу: ідеальною вважається невелика кількість базисних функцій, які перекривають всю область зображення. Ці вимоги

входять у конфлікт, коли стеганокотейнер піддається стиску: ідеальна схема компресії неспроможна повністю відобразити базиси, які використовувалися для приховування.

При РСПП модулююча функція складається з постійного коефіцієнта посилення G (ціле число), помноженого на псевдовипадковий масив базисних функцій ϕ_i значень ±1. Кожен масив ϕ_i має індивідуальне розташування в (x, y)-масиві. Крім того, масиви ϕ_i перекривають весь (x, y) - масив без проміжків. Також вважатимемо, що всі базисні функції мають однакову кількість значущих елементів (n_φ). Повна потужність виражається формулою:

$$P = \sum_{x,y}^{X,Y}(\sum_i G * m_i * \varphi_i(x,y))^2 = \sum_i \sum_{x,y}^{X,Y}\left(G * m_i * \varphi_i(x,y)\right)^2 = \\ = \mathrm{G}^2 * \mathrm{X} * \mathrm{Y} = \mathrm{N}_\varphi * \mathrm{n}_\varphi * G^2 \quad (2.10)$$

На етапі отримання даних необов'язково володіти інформацією провихідний контейнер C. Операція декодування полягає у відновленні прихованого повідомлення шляхом проектування отриманого зображення S на всі базисні функції φ_i.

Значення біт повідомлення m_i допомогою знакової функції:

$$m_i = sign(\sigma_i) = \begin{cases} -1 \text{ при } \sigma_i < 0 \\ 1 \text{ при } \sigma_i > 0, \text{за умови } G^2 > 0 \\ \text{невизначена при } \sigma_i = 0 \end{cases} \quad (2.11)$$

При значенні σ_i =0 прихована інформація втрачається.

Оскільки ми плануємо будувати систему на основі вбудовування повідомлення Лізи Марвел, то для порівняння залучимо такі методи:

1) Метод нелінійної модуляції

Формується нелінійна множина за правилом:

$$(\varphi_i)_j = \begin{cases} \Phi^{-1}((u_i)_j), b_i = -1; \\ \Phi^{-1}((u'_i)_j), b_i = 1, \end{cases} \quad (2.12)$$

де

$$(u'_i)_j = \begin{cases} (u_i)_j + 0.5, u_i < 0.5; \\ (u_i)_j - 0.5, u_i \geq 0.5, \end{cases} \quad (2.13)$$

$(u_i)_j$ рівномірно розподілена на інтервалі (0,1) випадкова величина,

Φ^{-1}- зворотна кумулятивна функція розподілу для стандартної гаусом випадкової величини.

Таким чином, розширюючий спектр послідовності з $\varphi = \{\varphi_0, \varphi_1, \dots, \varphi_{M-1}\}$ представляє собою реалізацію випадкової величини, розподіленої за нормальним законом з нульовим середнім і одиничним середньоквадратичним відхиленням. Ця випадкова реалізація обчислюється за формулою (2.12), тобто з використанням методу зворотного перетворення.

2) Метод формування множини на основі випадкових чисел на інтервалі від -1 до 1

Множина, що формується, $\varphi = \{\varphi_0, \varphi_1, \dots, \varphi_{M-1}\}$ складається з рівномірно розподіленими випадковими числами на інтервалі (-1,1).

Правило формування послідовностей має вигляд:

$$(\varphi_i)_j = rnd(2) - 1 \quad (2.14)$$

3) Метод на основі сигналів Уолша-Адамара

Ортогональні дискретні послідовності Уолша утворюються на основі рядків матриці Адамара за рекурентним правилом:

$$H_{2^i} = \left[H_{2^{i-1}}\ H_{2^{i-1}}\ H_{2^{i-1}}\ -H_{2^{i-1}}\right], H_1 = [1]. \tag{2.15}$$

Таке правило дозволяє сформувати матрицю будь-якого розміру, для якої характерна взаємна ортогональність всіх стовпчиків та рядків.

4) Метод на основі квазіортогональних дискретних сигналів

Квазіортогональні дискретні сигнали формуються з окремих елементів послідовностей, які генеруються вбудованою функцією генерації псевдовипадкових чисел *rnd()*, що формує раціональне число, яке, в свою чергу, знаходиться в заданому діапазоні. Функцією *ceil()* округляється отриманий результат до найближчого цілого числа. Після перетворення «0» в «–1» отримаємо масив, елементами якого є псевдовипадкові послідовності – сформовані дискретні сигнали. Значення коефіцієнта взаємної кореляції сформованих сигналів (через псевдовипадковість їх формування) значно не відрізняються від нуля, тобто сформовану множину послідовностей можна вважати ансамблем квазіортогональних дискретних сигналів.

5) Метод на основі адаптивних квазіортогональних сигналів

Для реалізації адаптивної генерації послідовностей вводиться обмеження на модуль коефіцієнта кореляції контейнера і формованого сигналу:

$$\forall i: |\rho(\Phi_i, C)| \le \rho_{max} \tag{2.16}$$

Значення ρ_{max} визначає максимально допустиму схожість контейнера C на формований сигнал Φ_i (або на його інверсію $-\Phi_i$). Фактично, відбраковуються ті сигнали, для яких $|\rho(\Phi_i, C)| > \rho_{max}$, і при малих значеннях ρ_{max} частка відбракованих Φ_i різко зростає.

Слід зазначити, що в разі, коли

$$\rho_{max} < G \cdot n \tag{2.17}$$

і одночасно

$$\forall i \neq j: \rho(\Phi_i, \Phi_j) = 0 \tag{2.18}$$

буде забезпечено безпомилкове відновлення інформаційного повідомлення. У цьому випадку всі сигнали з множини Ф взаємно ортогональні. Умова не може бути виконана і помилки у відновлених за правилом бітах неможливі.

Процес приховування і відновлення інформаційних повідомлень реалізуються так само, як і у попередніх способах. Використовувані послідовності з множини Φ будуть дійсно некорельовані із контейнером C, тобто припущення буде виконуватися для малих ρ_{max}.

Перевагою даної методики формування сигналу є дуже низька вірогідність помилок. Також слід зазначити, що для формування сигналів потрібно дуже багато часу, що негативно позначається на швидкодії методу.

2.2 Розробка математичної моделі приховування даних у контейнери-зображення із розширенням спектру методом прямої послідовності

Процес звичайного стеганографічного перетворення описується такими залежностями [58]:

$$E : C \times M \rightarrow S; \tag{2.19}$$

$$D : S \rightarrow M, \tag{2.20}$$

де $S = \{(c_1, m_1),(c_2, m_2),...,(c_q, m_q)\} = \{s_1, s_2,...,s_q\}$ – множина заповнених контейнерів (стеганограм). Розглянута формула (2.19) відношень пояснює механізм приховування інформації, у свою чергу, відношення (2.20) – отримання інформації, що була прихована. Однією із важливих умов є саме те, щоб не було співпадінь, наприклад, якщо $m_a \neq m_b$ (причому $m_a, m_b \in M$, а $(c_a, m_a),(c_b, m_b) \in S$),то $E(c_a, m_a) \cap E(c_b, m_b) = \emptyset$. Слід зазначити, що стеганосистему можна описати за допомогою сукупності ∑(C,M,S,E,D) контейнерів, перетворень та повідомлень, які їх об'єднують. Контейнери зазвичай мають вибиратися так, щоб повний та порожній контейнери майже не мали відмінностей. Тільки при умові, якщо sim[c, E(c, m)] = 1 (де sim – функція подібності), стеганосистема називається надійною. Слід зазначити процес вибору контейнеру, який може проходити двома шляхами: сурогатним методом, тобто довільно, та за допомогою вибору контейнера, що підходить у конкретному випадку більше за всіх, та при перетворенні завдасть найменших змін. Якщо розглядати останнє твердження, тоді контейнер має бути обрано за наступною умовою:

$$c = \max sim[x, E(x, m)]. \qquad (3.3)$$

Все ж таки, обов'язковим є факт того, при прямому та зворотньому перетворенні (E та D), щоб два контейнери відповідали один одному та виконувалась умова, при якій незначне спотворення контейнера (на величину δ) не викликає наслідків викривлення прихованої інформації:

$$E(c,m) \approx E(c + \delta,m) \text{ або } D[E(c,m)] \approx D[E(c + \delta,m)] = m. \qquad (3.4)$$

Розглянемо, як працює алгоритм системи:

1) Першим етапом є саме отримання вхідних даних, до яких відносяться зображення-контейнер, у який планується вбудувати скрите повідомлення, ключ, за допомогою якого буде вилучатися повідомлення із контейнера, та саме повідомлення,

що повинно бути передано через стеганосистему, а також учасники, що мають отримати дане повідомлення тощо.

2) Виконання вбудування із застосуванням обраного методу до початкового повідомлення зі вказаними параметрами;

3) Формування ключа, який контролює вбудовування повідомлення у контейнер за допомогою алгоритму;

4) Вбудовування повідомлення у всі копії початкового контейнера та їх подальша передача;

5) Отримання стеганоконтейнерів з повідомленнями у кількості вказаній у параметрі, що відповідав кількості учасників експерименту;

6) Вилучення повідомлень з стеганоконтейнерів;

7) Перевірка цілісності повідомлення за ключем.

Алгоритм у вигляді блок-схеми зображено у додатку А

2.3 Порівняльні характеристики стеганосистем із розширенням спектру методом прямої послідовності

Для порівняння стеганосистем із розширенням спектру методом прямої послідовності скористаємось наступними показниками ефективності стеганосистем:

BER – це одиничний показник ефективності, який використовується для оцінки достовірності відновлених даних.

$$BER = \frac{N_{error}}{N_{total}}, \tag{2.21}$$

де N_{error} – кількість бітових помилок,

N_{total}-загальна кількість переданих бітів.

MSE – це показник значення спотвореного помилками наближення (noisy approximation):

$$MSE = \frac{1}{mn}\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}\left[I_{i,j} - N_{i,j}\right]^2. \quad (2.22)$$

PSNR – логарифмічний показник відношення між максимально можливою потужністю сигналу і потужністю спотвореного шуму:

$$PSNR = 10 \cdot \left(\frac{I^2{}_{max}}{MSE}\right) = 20 \cdot \left(\frac{I_{max}}{\sqrt{MSE}}\right) =$$
$$= 20 \cdot (I_{max}) - 10 \cdot (MSE)\,, \quad (2.23)$$

де I_{max} є максимально можливе значення контейнера.

SNR – відношення сигналу до прихованих даних, які представляються як шум (noise).

$$SNR = \frac{\sigma^2{}_{signal}}{\sigma^2{}_{noise}}, \quad (2.24)$$

де σ^2 - являє собою вибіркову дисперсію перспективних сигналів.

Графіки побудовані на основі розрахунків для потужності (g) у діапазоні від 0 до 5 з кроком у 0,25 та для кількості бітів у одному блоці контейнера (k) у діапазоні від 0 до 10 р з кроком у 1 для кожного методу описаного вище.

1) Використання нелінійної модуляції

У цьому методі показник BER дуже високий (рисунок 2.1), MSE стрімко зростає (рисунок 2.2), PSNR – повільно спадає (рисунок 2.3), SNR повільно збільшується (рисунок 2.4).

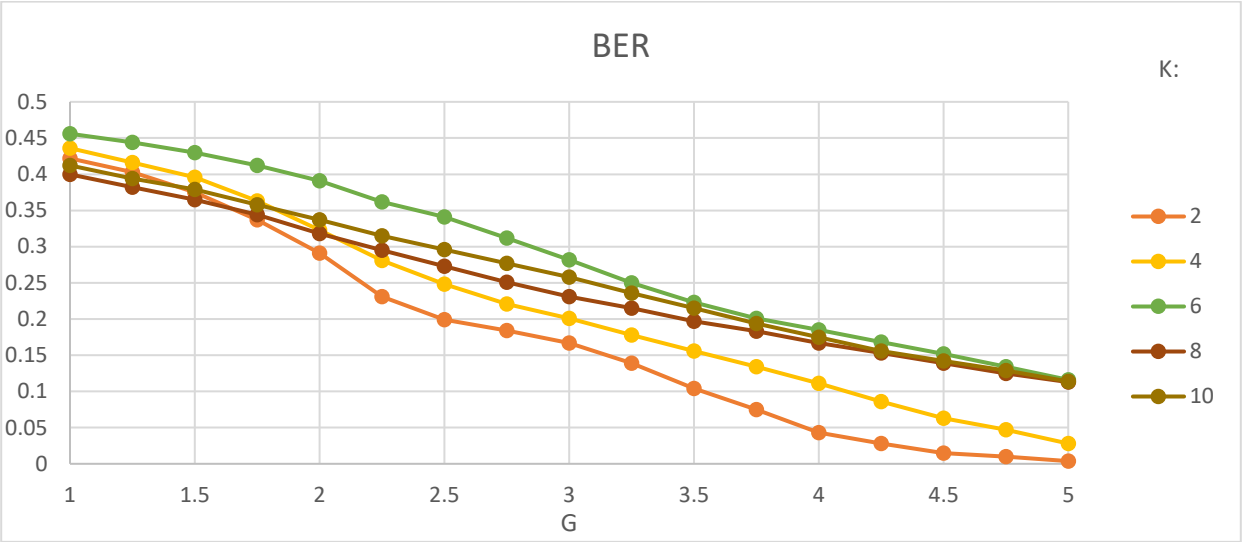

Рисунок 2.1 – Показник BER для методу нелінійної модуляції при різних параметрах k

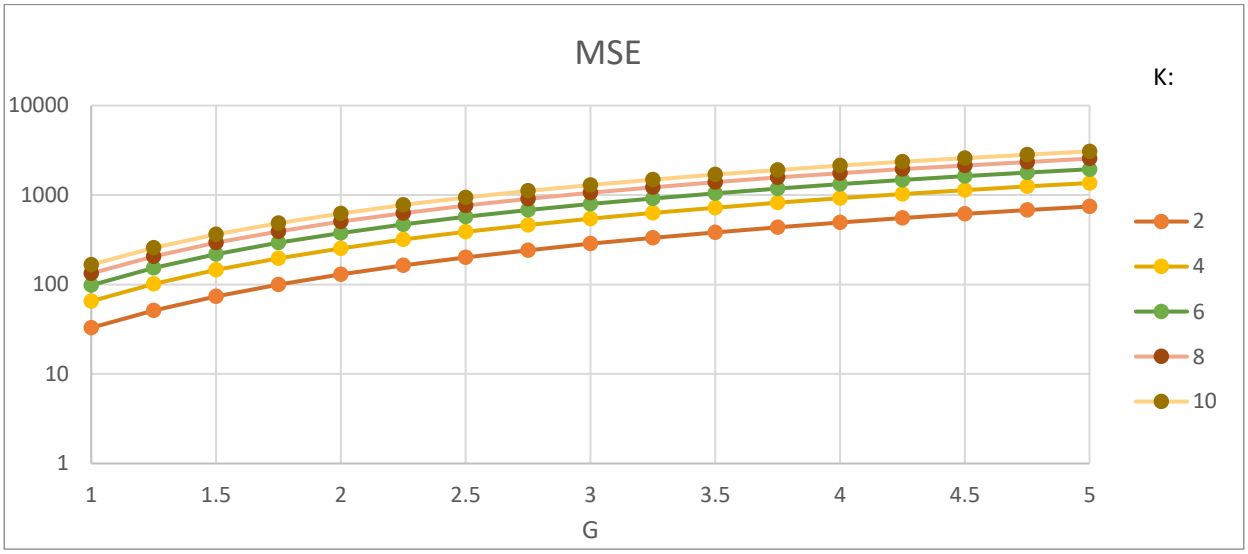

Рисунок 2.2 – Показник MSE для методу нелінійної модуляції при різних параметрах k

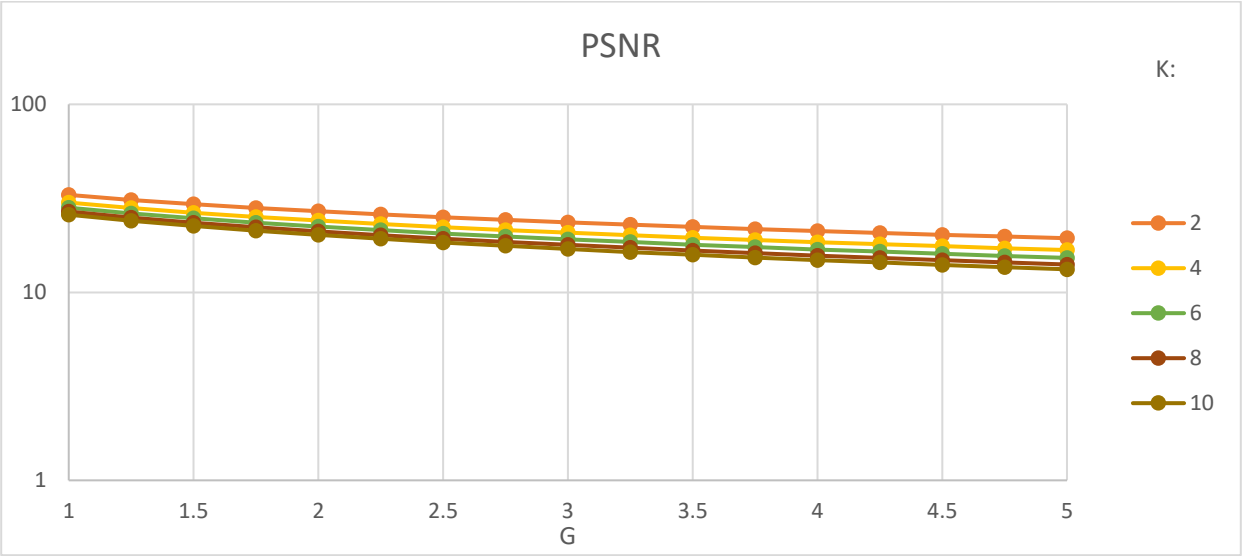

Рисунок 2.3 – Показник PSNR для методу нелінійної модуляції при різних параметрах k

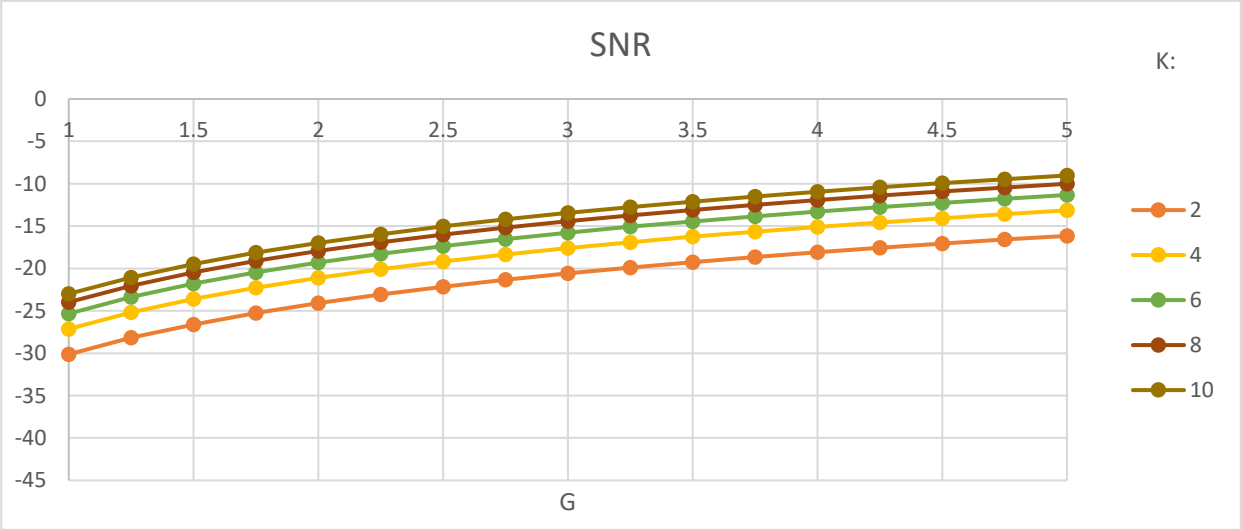

Рисунок 2.4 – Показник SNR для методу нелінійної модуляції при різних параметрах k

2) Використання рівномірно розподілених на інтервалі (-1;1) випадкових чисел

У цьому методі показники BER (рисунок 2.5) - вище, MSE (рисунок 2.6) - високі, але нижчі, ніж у попереднього методу, PSNR (рисунок 2.7) – вище, SNR (рисунок 2.8) – нижче за попередній метод відповідно.

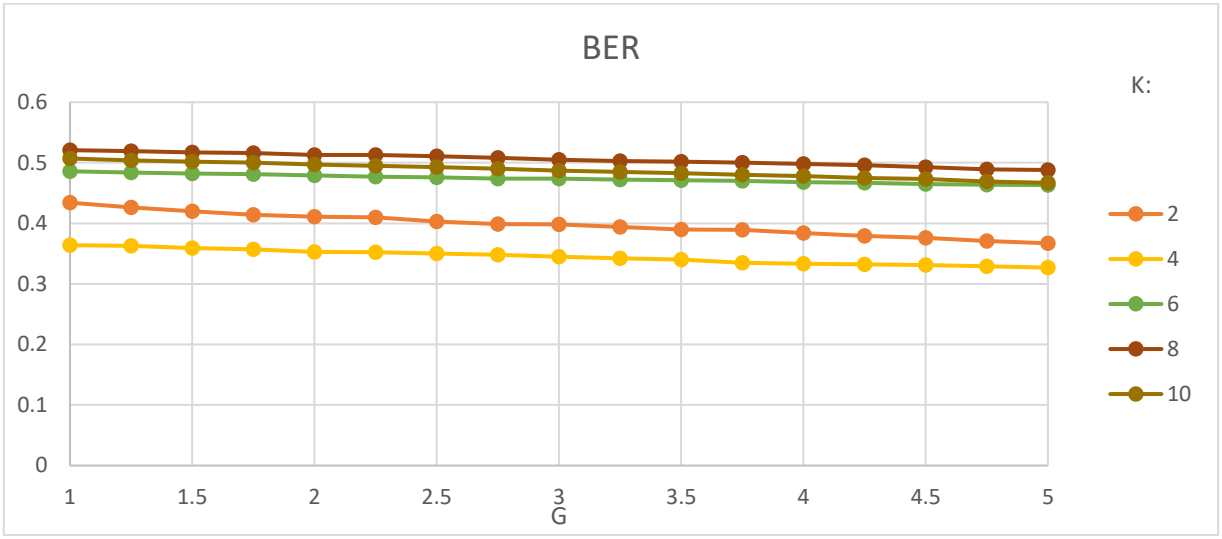

Рисунок 2.5 – Показник BER для методу рівномірно розподілених на інтервалі (-1;1) випадкових чисел при різних параметрах k

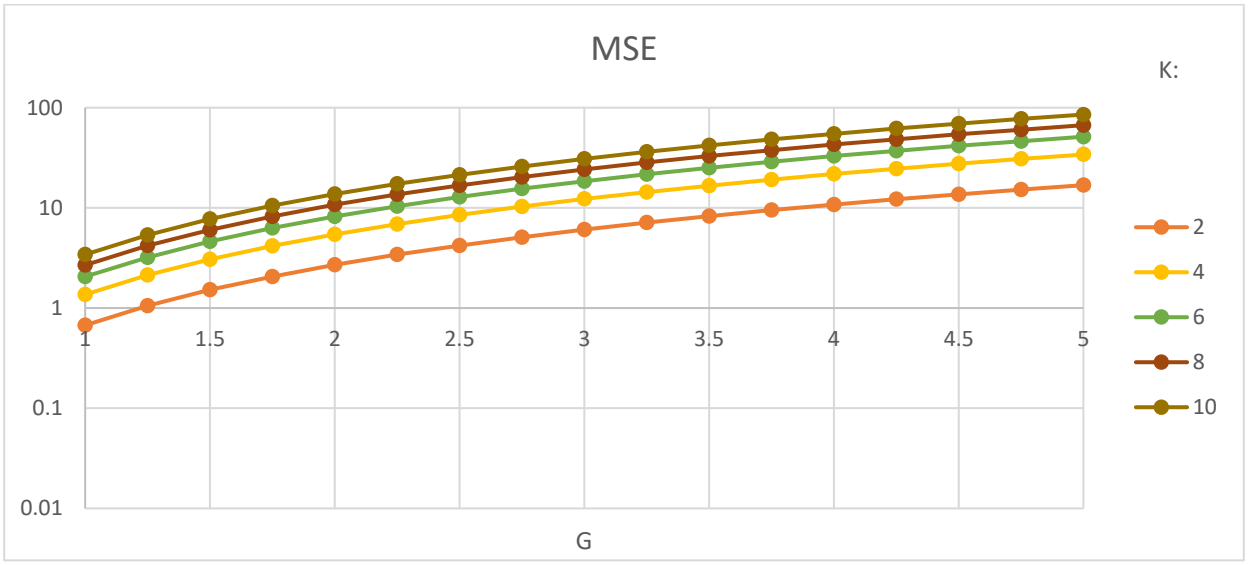

Рисунок 2.6 – Показник MSE для методу рівномірно розподілених на інтервалі (-1;1) випадкових чисел при різних параметрах k

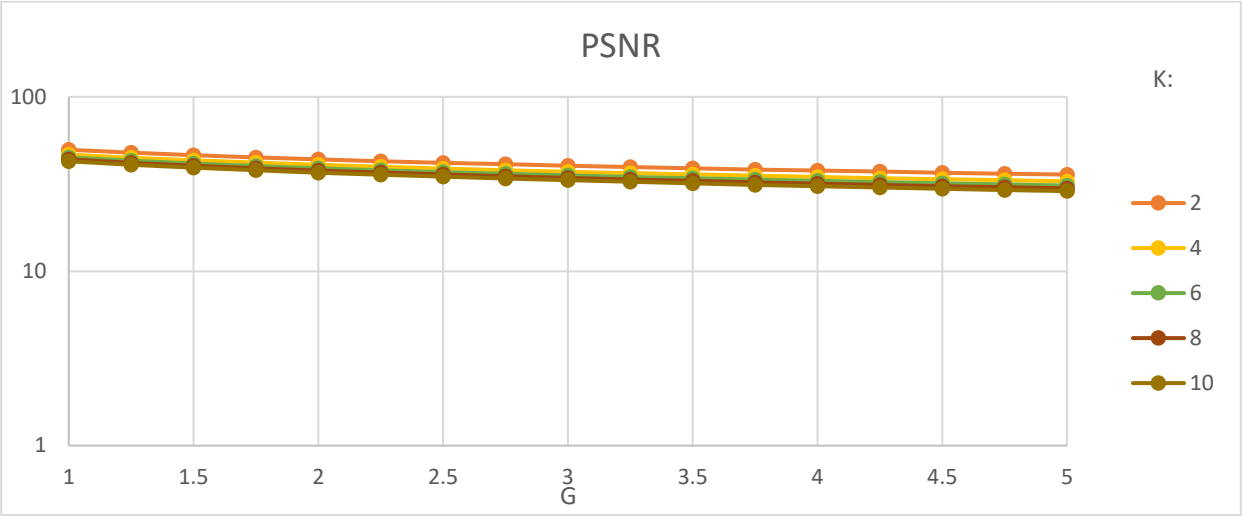

Рисунок 2.7 – Показник PSNR для методу рівномірно розподілених на інтервалі (-1;1) випадкових чисел при різних параметрах k

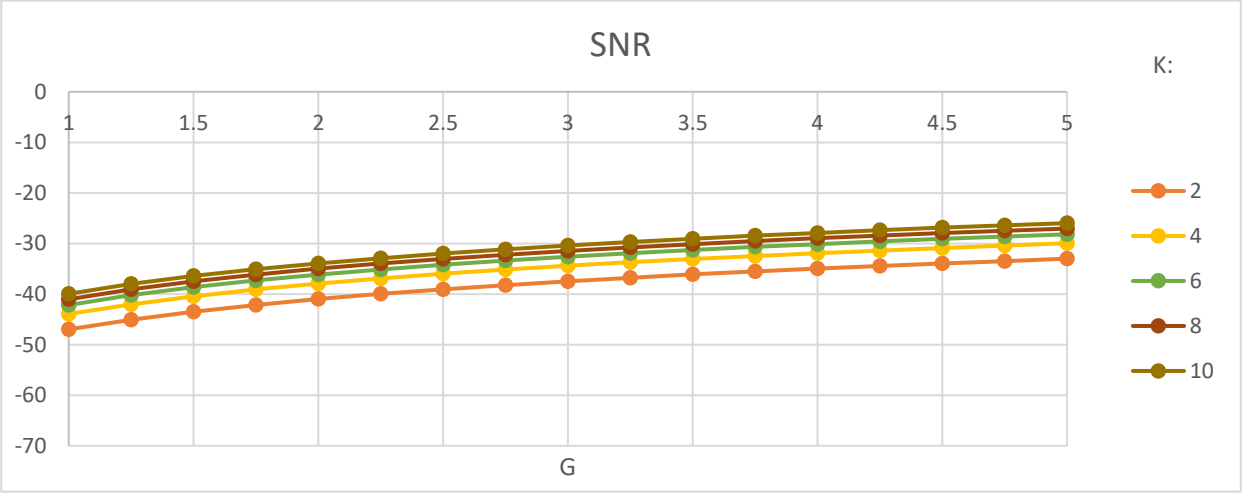

Рисунок 2.8 – Показник SNR для методу рівномірно розподілених на інтервалі (-1;1) випадкових чисел при різних параметрах k

3) Використання сигналів Уолша-Адамара

У цьому методі показники BER (рисунок 2.9) – набагато нижче, MSE (рисунок 2.10) - вищі, ніж у попереднього методу, PSNR (рисунок 2.11) – нижче, SNR (рисунок 2.12) – вище за попередній метод відповідно.

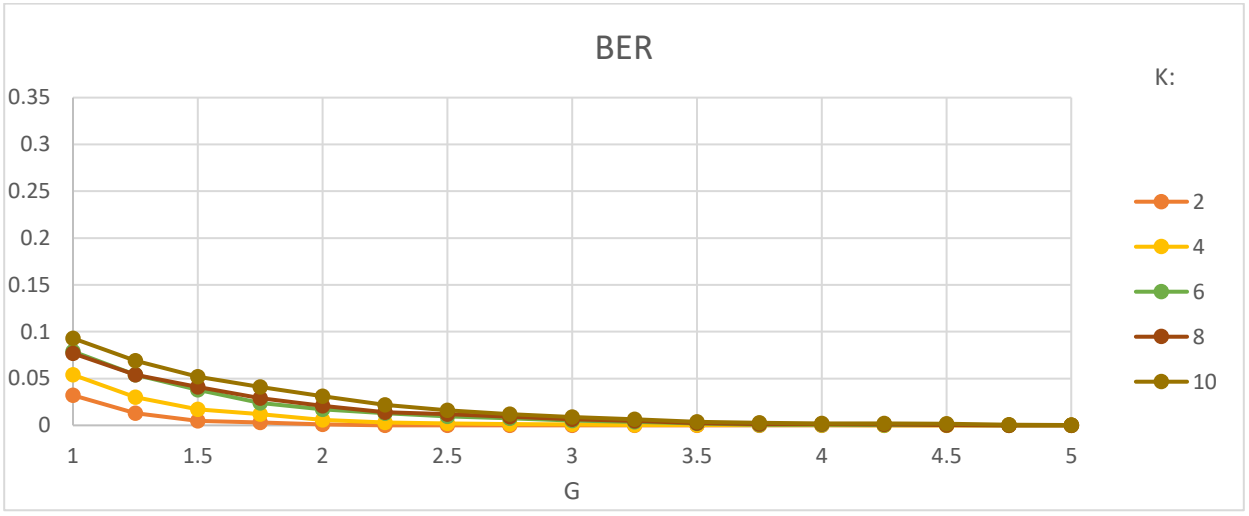

Рисунок 2.9 – Показник BER для методу на основі сигналів Уолша-Адамара при різних параметрах k

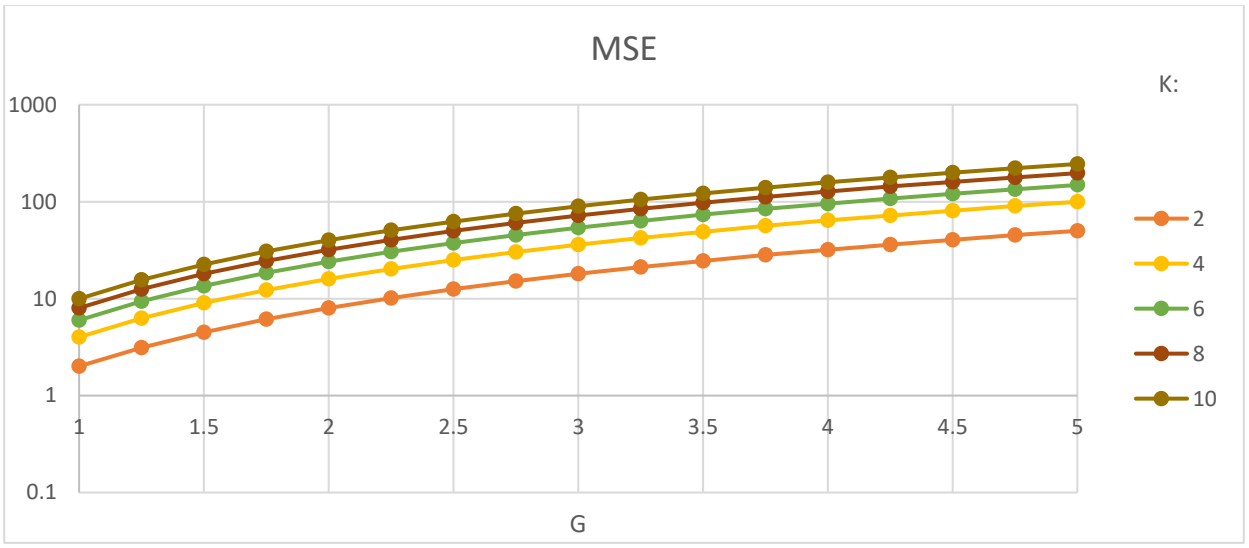

Рисунок 2.10 – Показник MSE для методу на основі сигналів Уолша-Адамара при різних параметрах k

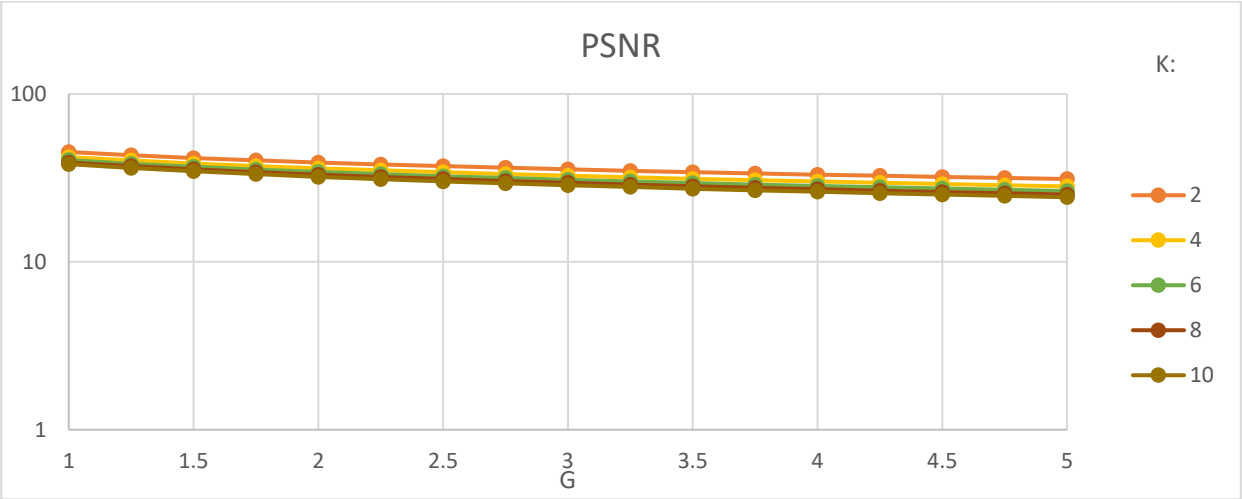

Рисунок 2.11 – Показник PSNR для методу на основі сигналів Уолша-Адамара при різних параметрах k

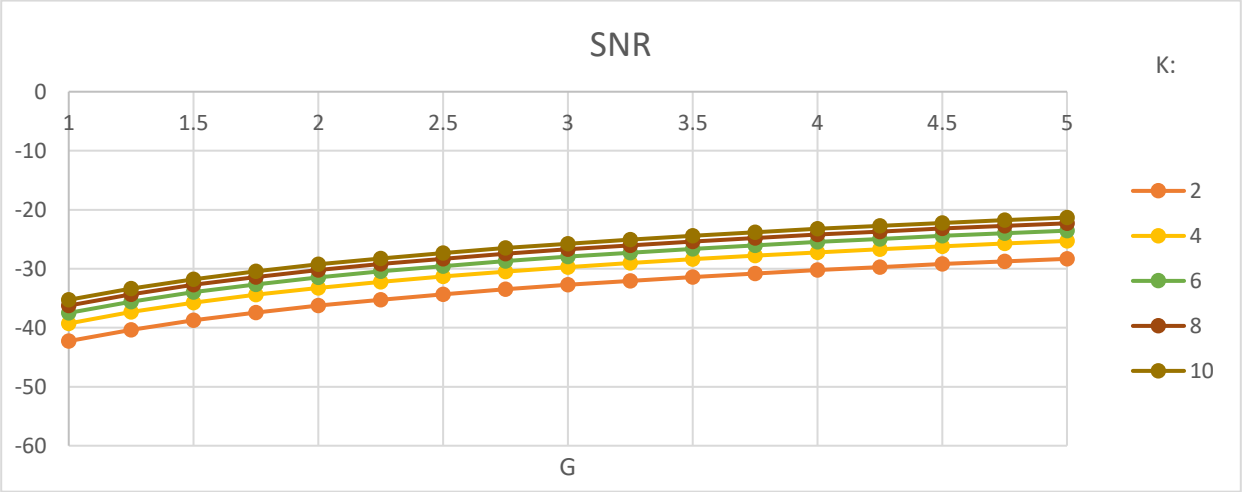

Рисунок 2.12 – Показник SNR для методу на основі сигналів Уолша-Адамара при різних параметрах k

4) Використання квазіортогональних сигналів

У цьому методі показники BER (рисунок 2.13) – вище, ніж у попереднього методу, але MSE (рисунок 2.14), PSNR (рисунок 2.15) та SNR (рисунок 2.16) – практично такі самі.

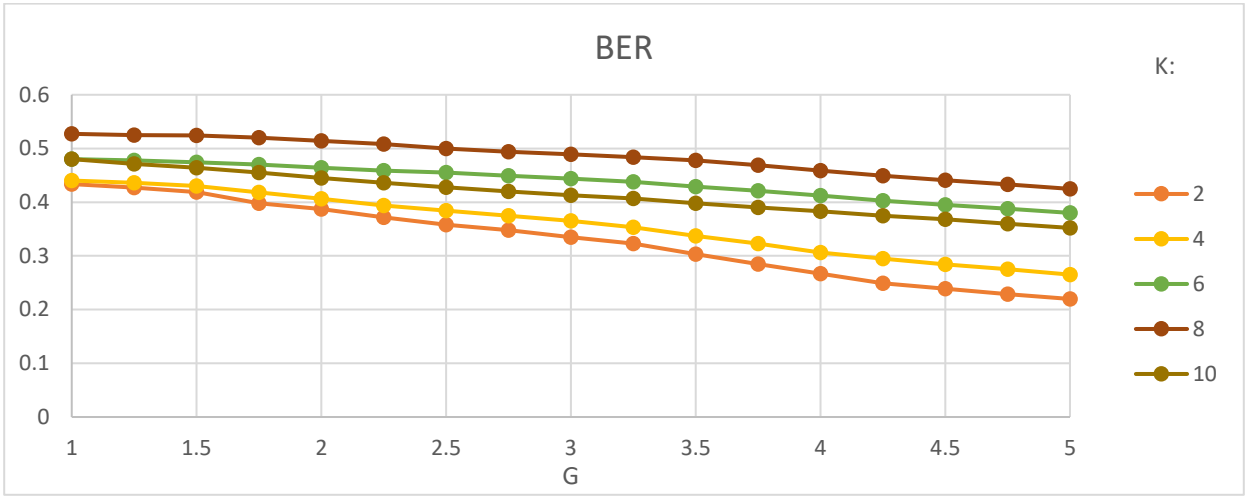

Рисунок 2.13 – Показник BER для методу на основі квазіортогональних сигналів при різних параметрах k

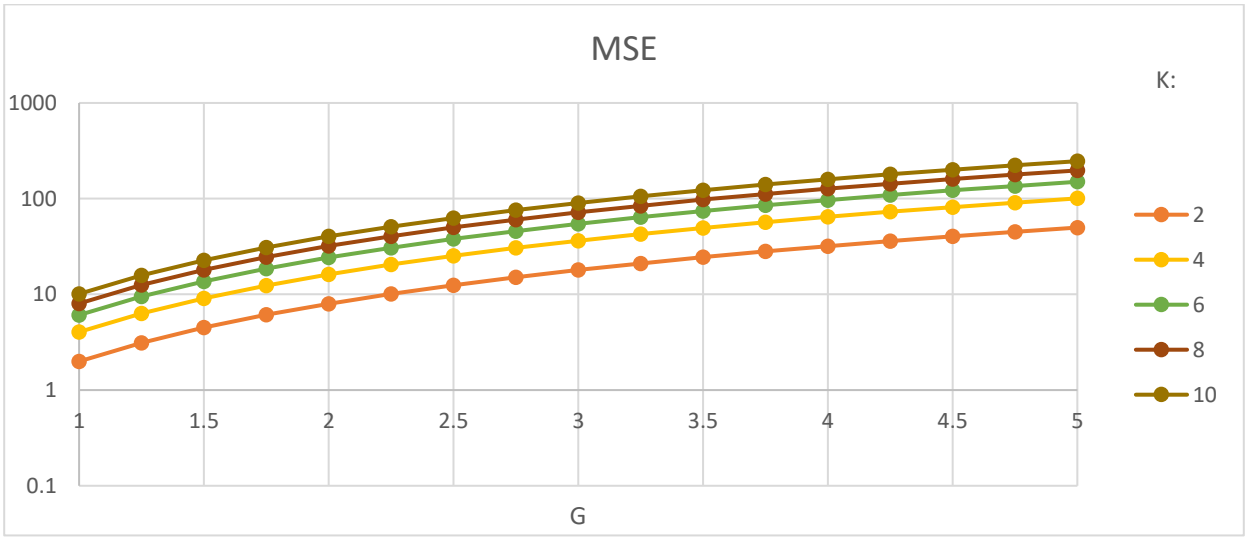

Рисунок 2.14 – Показник MSE для методу на основі квазіортогональних сигналів при різних параметрах k

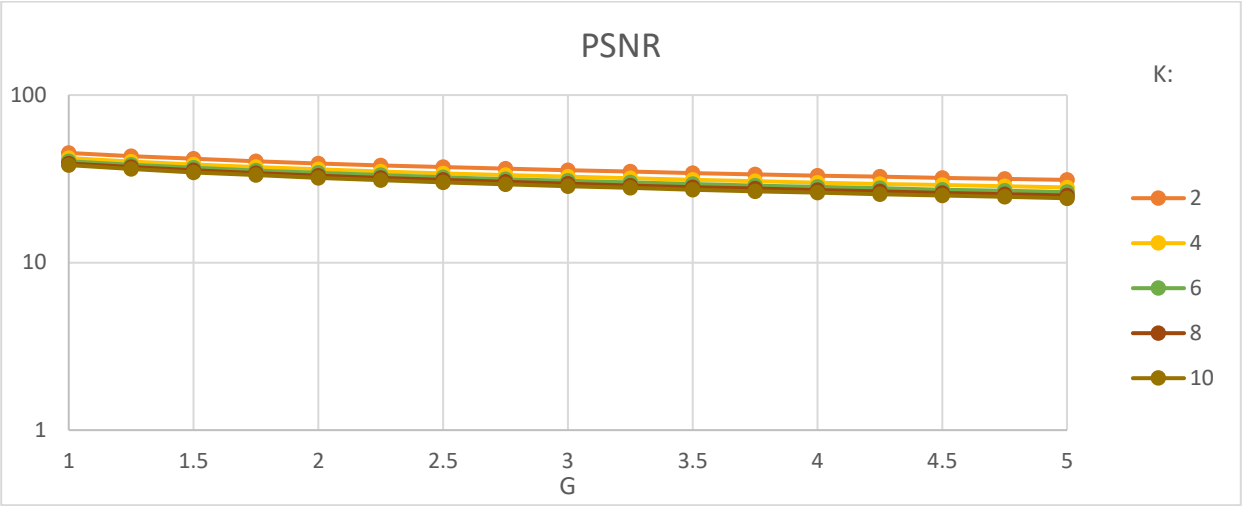

Рисунок 2.15 – Показник PSNR для методу на основі квазіортогональних сигналів при різних параметрах k

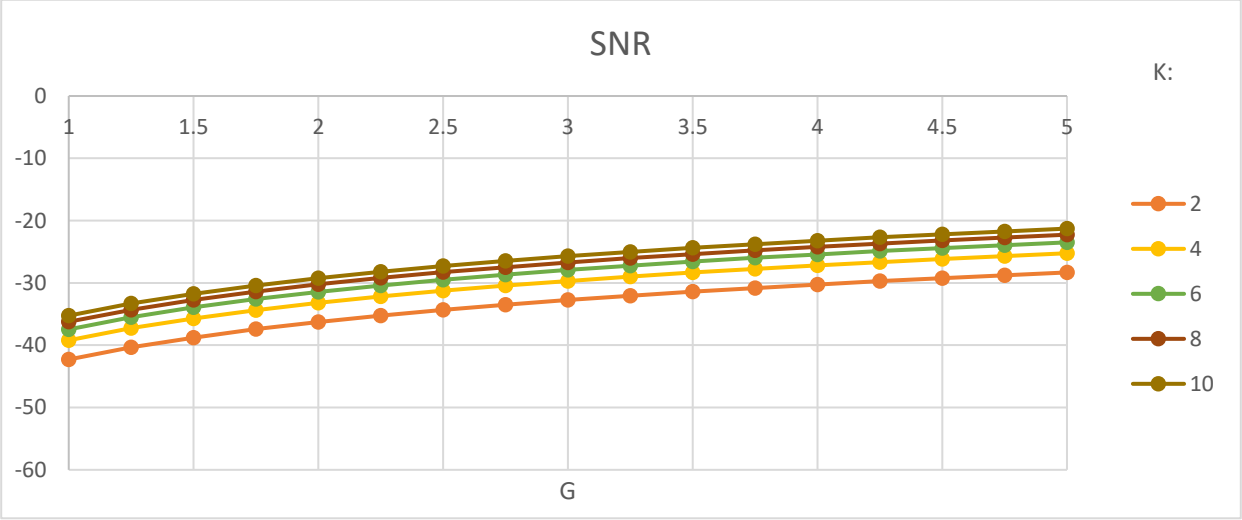

Рисунок 2.16 – Показник SNR для методу на основі квазіортогональних сигналів при різних параметрах k

5) Використання адаптивних квазіортогональних сигналів

У цьому методі показники BER (рисунок 2.17) - вище, проте MSE (рисунок 2.18), PSNR (рисунок 2.19) та SNR (рисунок 2.20) – подібні до попереднього.

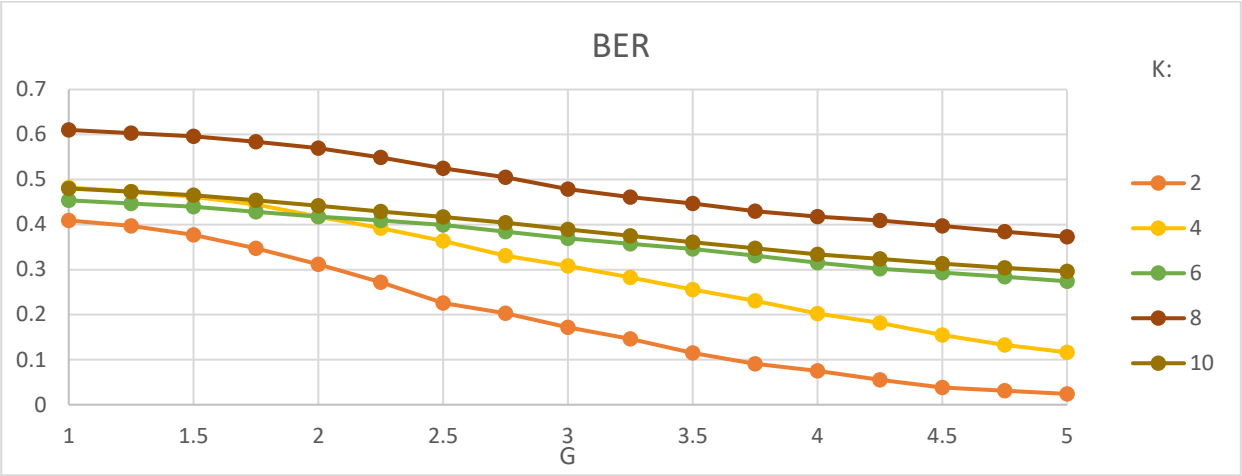

Рисунок 2.17 – Показник BER для методу на основі адаптивних квазіортогональних сигналів при різних параметрах k

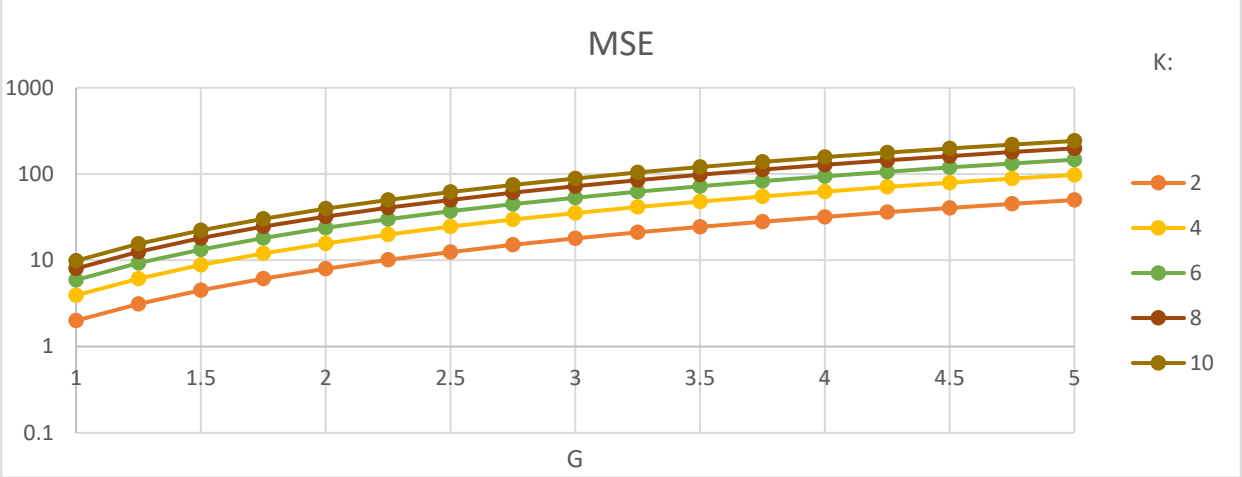

Рисунок 2.18 – Показник MSE для методу на основі адаптивних квазіортогональних сигналів при різних параметрах k

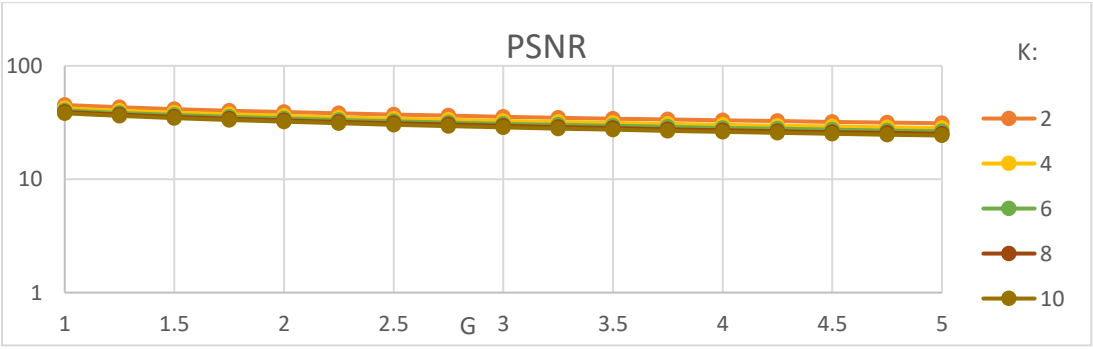

Рисунок 2.19 – Показник PSNR для методу на основі адаптивних квазіортогональних сигналів при різних параметрах k

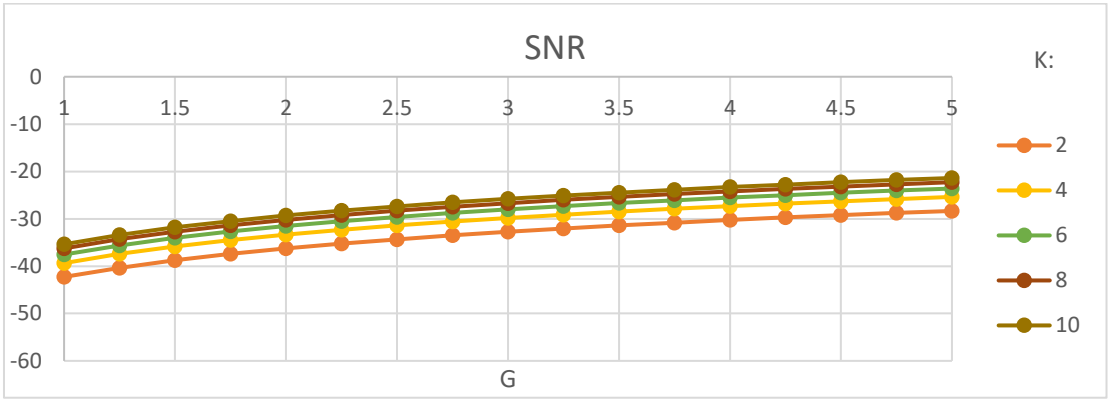

Рисунок 2.20 – Показник SNR для методу на основі адаптивних квазіортогональних сигналів при різних параметрах k

Порівняльна характеристика методів наведена в табл. 2.1.

Таблиця 2.1. – Порівняльні характеристики методів вбудовування стеганоконтейнерів з прямим розширенням спектру

Метод	BER	MSE	PSNR	SNR
Сміт-Комiскі	Низький (+)	Високий (-)	Високий (+)	Спадання (-)
нелінійної модуляції	Високий (-)	Високий (-)	Зниження (-)	Зростання (+)
формування множини на основі випадкових чисел	Низький (+)	Високий (-)	Зростання (+)	Низький (-)
сигналів Уолша-Адамара	Низький (+)	Високий (-)	Середній (+)	Зростання (+)
квазіортогональних дискретних сигналів	Низький (+)	Високий (-)	Низький (-)	Зростання (+)
адаптивних квазіортогональних сигналів	Низький (+)	Високий (-)	Середній (+)	Зростання (+)

Значення PSNR при використанні послідовностей Уолша в більшості випадків можна порівняти з наведеними далі методами модуляції сигналів, він дещо вищий, тому віднесений до рівня середнього. Отже, з таблиці можемо зробити висновок, що

метод Уолша-Адамара має найкращі результати (три плюсових показники) в порівнянні з іншими методами, крім методу адаптивних квазіортогональних сигналів, який теж отримав три плюси, але в свою чергу сигнали Уолша формуються значно швидше й простіше.

3 РОЗРОБКА ТА ПРОГРАМНА РЕАЛІЗАЦІЯ АЛГОРИТМІВ ПРИХОВУВАННЯ ТА ВИЛУЧЕННЯ ДАНИХ У КОНТЕЙНЕРИ-ЗОБРАЖЕННЯ ІЗ РОЗШИРЕННЯМ СПЕКТРУ МЕТОДОМ ПРЯМОЇ ПОСЛІДОВНОСТІ

3.1 Розробка алгоритмів приховування та вилучення даних у контейнери-зображення із розширенням спектру методом прямої послідовності

Для дослідження було обрано 3 алгоритми: алгоритм адаптивних квазіортогональних сигналів (Adapt), алгоритм Уолша-Адамара (Walsh) та алгоритм Сміта-Коміски (Smith). Кожен з них має непогані характеристики за визначеними критеріями, тому ми маємо дослідити їх основні властивості і обрати один критерій для подальшого вдосконалення.

Як повідомлення була обрана тестова фраза «God bless army of Ukraine», подана у вигляді рядка символів ASCII (8 біт однією символ). Довжина рядка – 25 символів, розмір повідомлення – 200 біт

Будемо використовувати стегосистеми з контейнером Lena.bmp, дане зображення є портретом у форматі BMP (точковий малюнок) з невеликою роздільною здатністю 512x512. Формат BMP забезпечує максимальну якість зображення, тому що не передбачає стиснення.

Рисунок 3.1 – Зображення «Lena.bmp»

Використання даного типового контейнеру обґрунтоване тим, що портрет містить досить велику кількість дрібних деталей, які додають природного шуму і приховують повідомлення. Кольори приглушені, оскільки фото датоване серединою XX століття, і не має такої деталізації, як сучасні цифрові фото. Домінує червоний колір, зелені та сині компоненти виражені середньо.

Для оцінювання якостістеганографічних алгоритмів використаємо показники, які дають кількісні оцінки, оскільки їх легше порівнювати. Найбільш важливими показниками для аналізу рівня візуального спотворення зображення під час приховування інформації, є співвідношення «сигнал/шум», обчислене в децибелах і якість зображення, що вимірюється у відсотках. Також можна використати середню абсолютну різницю значень пікселів, нормовану середню абсолютну різницю значень пікселів та максимальне відношення «сигнал-шум». Наведемо формули для обчислення вищезгаданих показників.

Середня абсолютна різниця (САР):

$$\text{САР} = \frac{1}{XY}\sum_{x,y}\left|C_{x,y} - S_{x,y}\right| \tag{3.1}$$

Нормована середня абсолютна різниця (НСАР):

$$\text{НСАР} = \frac{\sum_{x,y}|C_{x,y}-S_{x,y}|}{\sum_{x,y}|C_{x,y}|} \tag{3.2}$$

Відношення «сигнал/шум» (СШ):

$$\text{СШ} = \frac{\sum_{x,y}\left(C_{x,y}\right)^2}{\sum_{x,y}\left(C_{x,y}-S_{x,y}\right)^2} \tag{3.3}$$

Максимальне відношення "сигнал/шум" (МСШ):

$$\text{МСШ} = XY * \frac{\max_{x,y}(C_{x,y})^2}{\sum_{x,y}(C_{x,y}-S_{x,y})^2} \quad (3.4)$$

Якість зображення (ЯЗ)

$$\text{ЯЗ} = 1 - \frac{\sum_{x,y}(C_{x,y}-S_{x,y})^2}{\sum_{x,y}(C_{x,y})^2} \quad (3.5)$$

Отримані значення параметрів візуального спотворення по віх алгоритмах для зображення наведено в таблиці 3.1.

Таблиця 3.1 – Показники візуального спотворення при вбудовуванні повідомлення в зображення Lena.bmp

	САР	НСАР	СШ	МСШ	ЯЗ
Walsh	0,512022	0,004546	23521,9	103221	99,9939%
Adapt	0,986612	0,009361	1722,11	7110,22	99,9421%
Smith	0,859214	0,008254	11854,3	48892,1	99,9917%

Найкращі показники візуального спотворення мають алгоритми Walsh та Smith. Хороші показники має алгоритм Adapt. Це пов'язано з не найвищою яскравістю зображення та високою кореляцією між сусідніми пікселями. Хоча цей алгоритм має більшу візуальну помітність для фахівця.

Розглянемо пропускну спроможність при параметрах, підібраних кожного зображення щодо візуальних спотворень. Під пропускною спроможністю розумітимемо максимальну кількість символів ASCII (1 символ=8 біт), яку можна передати за один такт роботи стегосистеми. Приховану пропускну спроможність визначимо як максимальну кількість символів, яку можна вбудувати у зображення-стеганоконтейнер без істотних втрат для зображення (візуальної непомітності). Для зображення Lena.bmp $\tau = 200; \upsilon = 0,05$.

Таблиця 3.2 – Показники пропускної спроможності при вбудовуванні повідомлення в зображення Lena.bmp

	Пропускна спроможність	Прихована пропускна спроможність	Середня
Walsh	500	220	360
Adapt	200	200	200
Smith	3200	750	1975

Отже, найбільшу пропускну спроможність має алгоритм Сміта-Коміски, оскільки він працює з більш об’ємними повідомленнями.

Розглянемо робастність стегосистем, використовують у вбудовуванні досліджувані у роботі алгоритми, до найпоширенішим видам атак. Отримані результати зведемо до таблиць для стегосистем з різними контейнерами. Знаком "+" позначимо робастність стегосистеми до цієї атаки, знаком "-" - нестійкість до атаки.

У таблиці 3.3 наведено результати експерименту для стегосистем з контейнером Lena.bmp.

Таблиця 3.3 – Робастність стегосистем, що використовують контейнер Lena.bmp до атак

	Walsh	Adapt	Smith
Масштабування	-	-	-
Поворот	-	-	+
Контрастність	-	+	+
Підвищенняскравості	-	+	+
Зниження яскравості	-	+	+
Ерозія	-	-	+
Обрізання праворуч	-	+	-
Обрізання зліва	-	+	-
Обрізання знизу	+	+	-
Обрізання зверху	-	+	-

Отже, алгоритм Уолша-Адамра має невисоку стійкість до більшості атак. Для стійкості стегосистеми, що використовує алгоритм Уолш-Адамара до обрізання частини зображення (трохи більше 20% з кожної із сторін) праворуч, необхідно зменшити кількість символів до 10 (внаслідок невеликого розміру зображення).

Проаналізуємо швидкодію кожного з алгоритмів (Табл. 3.4.)

Таблиця 3.4 – Показники швидкодії при вбудовуванні та вилученні повідомлення в зображення Lena.bmp, с

	Шифрування+ Генерування	Вбудовування	Вилучення+ Дешифрування	Загальне
Walsh	0,152	0,462	0,367	0,981
Adapt	0,008	0,283	0,285	0,576
Smith	10,201	0,052	4,211	14,464

Як бачимо, перші два алгоритми є порівняними по часу швидкодії, а алгоритм Сміта-Коміски є досить тривалим, тому при потребі у швидкій передачі повідомлення він не є зручним.

Таким чином, всі обрані алгоритми мають різні показники стійкості до атак, тому варто обрати усереднений алгоритм Уолша-Адамара, оскільки він є досить швидкодійним і легко адаптованим, і в попередньому підрозділі показав досить високі параметри ефективності. Ми проведемо вдосконалення даного алгоритму з метою підвищення стійкості до атак (як було визначено, даний метод має низьку робастність, тому потребує доопрацювання).

Розглянемо основні властивості функції Уолша, які ми використовуємо у алгоритмі Уолша-Адамара:

1) Функції Уолша $wal(i,x)$ приймають тільки два значення +1, -1 при $i \geq 1$.

2) Функція $wal(0,x)$ на інтервалі $x \in [0,1)$ чи $x \in [-0.5,0.5)$ дорівнює одиниці. Функції Уолша ортонормовані на інтервалі $x \in [0,1)$:

3) Функції Уолша мають властивість мультипликативності, тобто добутокдвох функцій Уолша дає іншу функцію Уолша, причому $wal(k, x) \cdot wal(i, x) = wal(k \oplus i, x)$, де цілі числа k, i = 0,1,2... додаються в двійковійсистемі числення без переносу одиниці в старший розряд, тобто 0+0 = 0, 0+1 = 1, 1+0 = 1, 1+1 = 0.

4) Функції Уолша $wal(i,x)$ мають властивість симетрії, яка проявляється в тому, що усі висновки відносно i справедливі також і відносно x_i. Наприклад, властивість мультипликативності з урахуванням властивостей симетрії запишеться у вигляді

$$wal(i,x_1) \cdot wal(i,x_2) = wal(i,x_1 \oplus x_2).$$

5) Середнє значення функції Уолша при $i \neq 0$ дорівнює нулю (що свідчить про те, що число нулів і одиниць є однаковим). Для функції $wal(0, x)$ середнє значення дорівнює одиниці.

6) Оскільки на інтервалі визначення N у систему функцій Уолша входить N ортогональних функцій, то вона є повною. Це означає, що її не можна доповнити на цьому інтервалі ні однією новою функцією, що була б ортогональна одночасно до всіх інших функцій, що входять у систему.

Тоді можна запропонувати скористатись швидким перетворенням Уолша, яке прискорить обробку інформації, оскільки прискорення розрахунків при швидкому перетворенні забезпечується зменшенням числа операцій додавання (складові, що повторюються, не треба визначати для кожного відліку заново). Підвищити робастність системи можна, додавши зсув бітів, щоб зменшити залежність якості при обрізанні зображення з різних боків.

3.2 Обґрунтування вибору мови та середовища розробки для програмної реалізації запропонованих алгоритмів

Нові інформаційні технології докорінно змінили спосіб вирішення математичних задач. Тепер розв’язувати задачі та виконувати математичні перетворення доцільно за допомогою спеціальних програм. Сьогодні існує багато програмних пакетів для проведення аналізу та створення звітів за допомогою комп’ютерних технологій. Однак кожна з цих програм має ряд своїх особливостей, обмежень і можливостей.

Розгляньмо детальніше декілька пакетів математичних і статистичних комп’ютерних програм. Застосування математичних систем Derive, MatLab, Mathematica, MathCAD та Maple V дає змогу успішно вирішувати різноманітні технічні, систематичні, наукові, економічні та статистичні задачі.

Система Derive здатна виконувати аналітичне перетворення математичного виразу, що є її значною перевагою. Найчастіше такий процес перетворення називають символьною математикою чи комп’ютерною алгеброю. За допомогою Derive дуже

зручно виконувати інтегрування, диференціювання, знаходження меж та розширення функцій до рядів. У систему вбудовані набори елементарних функцій, а також набори статистичних та спеціальних математичних функцій. За допомогою цієї системи, можна виконувати операції регресійного аналізу, працювати із матрицями, а також виконувати перетворення Лапласа та Фур'є. Система здатна працювати з комплексними числами - це забезпечує можливість використання її для електротехнічних та радіотехнічних розрахунків.

За допомогою системи Mathematica можна створювати високоякісну графіку та використовувати сотні символьних математичних команд. Робочий процес із цією системою дещо складніший, ніж із іншими математичними системами, зокрема через те, що цей пакет розрахований на вирішення науково-технічних та математичних задач. Ця система здатна виконувати широкий спектр завдань. Ще на етапі створення, головною метою було об'єднання в єдиній та цілісній формі усіх відомих математичних методів розв'язання наукових задач, зокрема і чисельні та налітичні розрахунки. Mathematica можна використовувати для диферинціювання, спрощення математичних виразів, обчислення визначених та невизначених інтегралів, обчислення нескінченною та нескінченної суми та добутку, розв'язування диференціальних та алгебраїчних систем та рівнянь, а також для розкладання функцій на множники та встановлювлення межей.

Mathematica здатна розв'язувати задачі, що неможливі для вирішення аналітично чисельними методами(наближеними методами); задачі математичної статистики та оптимізаційні задачі (знаходження екстремумів функцій, лінійне програмування). Також у системі передбачена довідкова база даних, за допомогою якої в інтерактивному режимі можна отримати доступ до документації, що включає в себе посібник зі стандартних доповнень, посібник користувача, посібник для початківців та демонстраційні файли. Варіативність застосування графічних можливостей, широкі символьні та числові можливості, чисельні способи побудови гіпертекстових зв'язків між документами, інтегрована мова програмування

створюють умови для використанн цієї системи для практичних і дослідницьких занять так і для нання студентів.

Основої математичої системи MatLab (Matrix Laboratory) є принцип гнучнокстi, що адаптовує систему до вимог користувача. Принцип роботи системи полягає в тому, що користувачеві надається можливість створювати майже необмежену функцій, що зберігаються на накопичувачах даних, що є в комп'ютері. У стандартному пакеті MatLab є алгебрахчні, арифметичні, тригонометричні функції та деякі спеціальні функції, функції для зворотного та простого перетворення Фур'є, векторні та матричні функції та функції цифрової фільтрації.

За допомогою MatLab можна виконувати операції над комплексними числами та поліномами, створювати зображення тривимірних поверхонь будувати графіки в полярній та декартовій системах координат. MatLab зтатен розраховувати та проектувати аналогові та цифрові фільтри, будувати імпульсні, частотні характеристики та перехідні характеристики для лінійних електричних кіл, засоби синтезу та спектрального аналізу. Основне призначення Mathsoft MatLab - чисельне моделювання систем, та у нових версіях також є елементи універсальних математичних пакетів.

Для виконання завдань із моделювання MatLab є можливість доповнити пакетом SIMULINK для візуально орієнтованого програмування. Найбільшими перевагами цієї системи є потужні графічні можливості, вбудоване багатофункціональноге програмування внутрішньою мовою, а також комплексна підтримка складних символьних обчислень. Найголовнішим конкурентом є Wolfram Research Inc. Mathematica.

Пакет Maple V дає змоуг не витрачати час на чисельне виконання окремих задач, а зосередитися на виконанні основної задачі. Значна кількість докладних прикладів та інтегрованих математичних функцій, дозволяють інженерам, вченим і дослідникам розв'язувати складні теоретичні та прикладні завдання. Ліцензований обчислювальний символічний блок Maple V використовується в MathWorks, MatLab

та MathCAD.MathCAD значною мірою вбудований у Windows. Система має зрозумілий інтерфейс, великі ресурси, підтримку та велику публічну базу даних. Система дає можливість перекладу чисел подружжя та аналітичних перетворень. Багатоколірна, дво- та тривимірна графіка створюється миттєво з автоматичним масштабуванням.

Відмінною рисою системи є використання загальноприйнятих в математиці символів для позначення операцій інтегрування, диференціювання, обчислення рядів тощо. Багато чисельних методів для вирішення лінійних і нелінійних рівнів, обчислення визначених інтегралів, оптимізації, вирішення диференціальних рівнів, інтерполяції сплайнів тощо дуже легко реалізувати в MathCAD.

MathCAD — це інтегрована система, яка дозволяє створювати проекти, в яких дані циркулюють через систему MatLab, електронні таблиці Excel і пакет наукової графіки Axum.

Для обробки експериментальних даних використовуються спеціальні статистичні пакети:

– професійні — SAS, BMDP, IMSL (розраховані переважно на висококваліфікованих математиків);

– популярні (тобто для широкого кола користувачів) - STATGRAPHICS, SPSS, SYSSTAT, STADIA, STATISTICA, MiniLab. Перераховані пакети є універсальними і призначені для вирішення широкого кола завдань. Розробляються завдання або навіть окремі завдання

Програмна реалізація запропонованих алгоритмів приховування та вилучення даних у контейнери-зображення із розширенням спектру методом прямої послідовності виконана у середовищі MathCAD. Вибір даного середовища обґрунтовується наступними підставами: дана система є легко масштабованою, призначеною для математичних обчислень, на яких побудовані алгоритми приховування та зчитування стеганоповідомлень, а також придатна для обробки графічних зображень, вбудовуючи туди повідомлення.

3.3 Програмна реалізація алгоритмів приховування та вилучення даних

У дослідженні використовувалася програма Mathcad і наведені вище текстове повідомлення і стеганоконтейнер.

Завантаження вхідних даних відбувається вбудованими інструментами середовища MathCad:

- Зчитування растрових даних нерухомого зображення у вигляді двомірного масиву цілих чисел:

C:= READRGB(«Lena.bmp»)

- Зчитування даних з каналу червоного кольору растрових даних:

R:= READ_RED(«Lena.bmp»)

- Зчитування інформаційних даних текстового документа у вигляді одновимірного масиву цілих чисел:

M:= READBIN(«Message.txt», byte)

Стандартні функції, що використовуються протягом усього експерементального дослідження (рисунок 3.2, рисунок 3.3, рисунок 3.4, рисунок 3.5, рисунок 3.6, рисунок 3.7, рисунок 3.8):

$$B\_D(x) := \sum_{i=0}^{7} \left(x_i \cdot 2^i \right)$$

Рисунок 3.2 — Функція перетворення вектора-стовпця з восьми біт у десятковий код

$$D\_B(x) := \left| \begin{array}{l} \text{for } i \in 0..7 \\ \quad \left| \begin{array}{l} V_i \leftarrow \text{mod}(x, 2) \\ x \leftarrow \text{floor}\left(\frac{x}{2}\right) \end{array} \right. \\ V \end{array} \right.$$

Рисунок 3.3 — Функція перетворення цілого числа в десятковому коді в двійковий вектор-стовпець

```
M_b := | for i ∈ 0.. rows(M) − 1
       |     V ← D_B(M_i)
       |     for j ∈ 0.. 7
       |       M_b_{i·8+j} ← V_j
       | M_b
```

Рисунок 3.4 — Функція перетворення масиву інформаційних цілих чисел в бітовий масив

```
m := | for i ∈ 0.. rows(M_b) − 1
     |     m_i ← 1  if M_b_i = 1
     |     m_i ← −1  if M_b_i = 0
     | m
```

Рисунок 3. 5 — Функція перетворення масиву інформаційних бітів у масив, що складається з «1» та «-1»

```
MultString(A, B) := | X ← 0
                    | for i ∈ 0.. 255
                    |   X ← X + A_i · B_i
                    | X
```

Рисунок 3.6 — Функція розрахунку коефіцієнту кореляції

```
for i ∈ 0.. rows(R) − 1
  | g1 ← g/4
  | Sum2_i ← Σ_{j=0}^{k−1} [g1 · (m_{k·i+j} · ArrayFunction1_j)]
```

Рисунок 3.7 — Функція вбодовування повідомлення

```
for i ∈ 0.. rows(R) − 1
  for j ∈ 0.. k − 1
    a ← MultString(ArrayString2_i, ArrayFunction1_j)
    M_b2_(k·i+j) ← 1  if a > 0
    M_b2_(k·i+j) ← −1  if a ≤ 0
```

Рисунок 3.8 — Функція вилучення повідомлення

Обчислення критеріїв ефективності у кожному методі та запис цих значень у файли. prn відбувається за процедурами, які продемонстровані на рисунку 3.9, рисунку 3.10, рисунку 3.11, рисунку 3.3.12:

```
A ← 0
for i ∈ 0.. rows(M_b2) − 1
  A ← A + 1  if M_b2_i ≠ m_i
BER_(g,k) ← A / (k · rows(R))
```

WRITEPRN(«BER.prn», BER)

Рисунок 3.9 — Критерій BER

```
A ← 0
for i ∈ 0.. rows(R) − 1
  for j ∈ 0.. cols(R) − 1
    A ← A + (S2_(i,j) − R_(i,j))^2
MSE_(g,k) ← A / (rows(R) · cols(R))
```

WRITEPRN(«MSE.prn», MSE)

Рисунок 3.10 — Критерій MSE

$$
\begin{aligned}
&\mathrm{PSNR}_{g,k} \leftarrow 20 \cdot \log(255, 10) - 10 \cdot \log\left(\mathrm{MSE}_{g,k}, 10\right) \\
&A \leftarrow 0 \\
&B \leftarrow 0 \\
&\text{for } i \in 0..\mathrm{rows}(R) - 1 \\
&\quad \text{for } j \in 0..\mathrm{cols}(R) - 1 \\
&\qquad A \leftarrow A + \left[\left(\mathrm{Sum2}_i\right)_j\right]^2 \\
&\qquad B \leftarrow B + \left(R_{i,j}\right)^2
\end{aligned}
$$

WRITEPRN(«PSNR.prn», PSNR)

Рисунок 3.11 — Критерій PSNR

$$\mathrm{SNR}_{g,k} \leftarrow 20 \cdot \log\left(\sqrt{\frac{A}{B}}, 10\right)$$

WRITEPRN(«SNR.prn», SNR)

Рисунок 3.12 — Критерій SNR

Процедура генерації матриць Адамара продемонстрована на рисунку 3.13:

```
X := for i ∈ 1.. 9
       F ← X_(i−1)
       for j ∈ 0.. rows(F) − 1
         for jj ∈ 0.. cols(F) − 1
           a ← F_(jj,j)
           F1_(jj,j) ← a
       for j ∈ 0.. rows(F) − 1
         for jj ∈ 0.. cols(F) − 1
           a ← F_(jj,j)
           F1_(jj+cols(F),j) ← a
       for j ∈ 0.. rows(F) − 1
         for jj ∈ 0.. cols(F) − 1
           a ← F_(jj,j)
           F1_(jj,j+rows(F)) ← a
       for j ∈ 0.. rows(F) − 1
         for jj ∈ 0.. cols(F) − 1
           a ← F_(jj,j)
           F1_(jj+cols(F),j+rows(F)) ← −a
       X_i ← F1
     X
```

Рисунок 3.13 — Функція генерації матриць Адамара

Реалізація процедури формування ансамблів ортогональних дискретних сигналів Уолша-Адамара (рисунок 3.14):

```
ArrayFunction := | for i ∈ 0..511
                 |     for j ∈ 0..511
                 |         a_j ← (X_9)_{i,j}
                 |     ArrayFunction_i ← a
                 | ArrayFunction
```

Рисунок 3.14 — Формування ансамблів ортогональних дискретних сигналів Уолша-Адамара

3.4 Експериментальні дослідження та розробка практичних рекомендацій

У такий спосіб через те, що повідомлення у випадковому порядку робиться менш помітним, не зовсім виразним, здійснюється не послідовно, з проміжком та закономірно, а у довільному порядку, то це значно ускладнює завдання на визначення прихованої інформації в контейнері та вилучення цієї конкретної інформації злочинцями-порушниками. Тому були підібрані зразки, моделі результатів RS-атаки та атаки χ-квадрат на стеганоконтейнери із вбудованим повідомленням двома методами, залежно від наповнення контейнера-зображення. Показано атаки без відхилень від обраного напрямку на стеганоконтейнери, тобто середнє відношення знайденого обсягу інформації до справжньої. В експерементальних дослідженнях брали участь 1000 контейнерів, в які вбудовували повідомлення.

Отже, детальніше про зазначені атаки та їх види.

1) Метод χ^2-стеганоаналізу

Цей метод аналізує гістограми, які отримані із елементів зображення та оцінки розподілу пар значень цієї гістограми. Для файлів BMP пари значень утворюються значеннями пікселів зображення. Частоти двох сусідніх елементів контейнера повинні бути досить віддалені від середньоарифметичного значення частоти цих елементів. Порожній стеганоконтейнер дуже рідко продукує ситуацію, коли частоти елементів зі

значеннями 2N і 2N +1 близькі один до одного. Після вбудовування інформації ці частоти зближуються або стають однаковими..

Ідея атаки χ2 полягає в пошуку цих близьких значень і підрахунку ймовірності наявності вбудованого повідомлення на основі того, як близько розташовуються значення частот парних і непарних елементів аналізованого контейнера. Послідовний аналіз зображення є особливістю цього алгоритму, який здатний також аналізувати накопичення частот елементів. Метод χ2 є універсальним, оскільки підходить для аналізу зображень, в які інформація вбудовувалась за допомогою різних стеганографічних алгоритмів. Проте результати методу за цим критерієм χ2 будуть залежати від методу приховування даних. Якщо елементи контейнера замінюються послідовно, а вбудовані повідомлення заповнюються, метод виявляє наявність прихованих даних, а при псевдовипадковому виборі молодших бітів (розподіленому вбудовуванні) метод не спрацьовує.

Таблиця 3.5 – Результати χ^2 – атаки

Наповненість контейнера	Алгоритм Уолша-Адамара	Модифікований алгоритм
0	0	0
15	60,21	42,25
30	87,15	51,13
45	92,21	63,24
60	93,13	89,91
75	95,26	93,21
100	100	100

2) Метод RS-атаки

Цей метод також відомий, як регулярно-сингулярний. Вихідний контейнер умовно розділяється на певні групи по n-пікселів $G(x_1, x_2, x_3, ..., x_n)$, де n парне число. Пікселі вибраної кількості знаходяться поруч та у горизонтальній площині. Для цієї вибраної групи пікселів визначається функція регулярності f(G), яка умовно дорівнює «гладкості» контейнеру. У якості значень, що будуть інтерпретувати функції можна обрати середньогрупову дисперсію значень або ж взяти значення, яке представлятиме

сумарний перепад усіх суміжних пікселів. Числа від 0 до 255 представляють власне значення пікселю.

Метод побудований на статистичному припущенні, що пустий контейнер буде мати подібні або незначні зміни у розподілі, у порівнянні із заповненим контейнером, у якого значення буде змінено на одиницю вправо або вліво. Для натурального зображення співвідношення між групами не повинно значно змінюватися. Уся істотна розбіжність між отриманих даних свідчить про те, що використовувалася метод заміни молодших біт зображення над стеганоконтейнером.

Аналогічним попередньому методові чином було здійснено RS-атаку, результати якої наведено в табл. 3.2

Таблиця 3.6 – Результати RS– атаки

Наповненість контейнера	Алгоритм Уолша-Адамара	Модифікований алгоритм
0	0	0
15	47,28	5,32
30	65,24	35,11
45	80,71	53,21
60	93,12	85,88
75	99,25	96,52
100	100	100

Отже, нами було здійснено розробку програмного забезпечення для вирішення поставленої задачі приховування та вилучення повідомлень методом розширення прямого спектру за допомогою прямої послідовності. Описано основні модулі програми в середовищі MathCAD та здійснено тестування засобу. Даний метод забезпечує кращу локалізацію особливостей контейнерів-зображень і потребує менших обчислювальних потужностей. Також даний алгоритм сприяє істотному підвищенню стійкості зображення із вбудованим повідомленням.

ВИСНОВКИ

Робота присвячена розробці алгоритмів приховання та вилучення повідомлень з зображень-стеганоконтейнерів за допомогою методів розширення спектру засобом прямої послідовності.

В роботі було поставлено та виконано наступні завдання дослідження:

- проведено аналіз форматів цифрових зображень. Ми розглянули основні типи форматів цифрових зображень з точки зору використання їх у якості контейнерів для стеганографічних цілей;

- здійснено визначення критеріїв та показників ефективності стеганосистем. На основі визначених критеріїв ми зможемо порівняти різні алгоритми приховування та вилучення зображень;

- застосовано порівняльний аналіз стеганосистем та обґрунтувати напрямки досліджень. Зроблено висновки, що при розробці сучасних методів стеганографії цілком зрозуміло, що слід враховувати не тільки властивості ЦВЗ, але й алгоритми стиснення цифрових зображень та інші інструменти. Тому це обумовило напрямок дослідження математичних моделей, методів та обчислювальних алгоритмів приховування даних у контейнери-зображення із розширенням спектру. Враховуючи різноманітність методів стеганографії, запропоновано проводити приховування методом прямої послідовності, який ще має назву методу прямого розширення спектра дискретних сигналів;

- проведено дослідження технології прямого розширення спектру та її застосування в стеганографії. Розглянуто алгоритми на основі роботи Лізи Марвел і їх практична реалізація, а також можливість використання для приховування та вилучення повідомлень;

- здійснено розробку математичної моделі приховування даних у контейнери-зображення із розширенням спектру методом прямої послідовності;

- наведено порівняльні характеристики стеганосистем із розширенням спектру методом прямої послідовності. Відповідно можемо зробити висновок, що метод Уолша-Адамара має найкращі результати (три плюсових показники) в порівнянні з іншими методами, крім методу адаптивних квазіортогональних сигналів, який теж отримав три плюси, але в свою чергу сигнали Уолша формуються значно швидше й простіше;

- проведено розробку алгоритмів приховування та вилучення даних у контейнери-зображення із розширенням спектру методом прямої послідовності. Всі обрані алгоритми мають різні показники стійкості до атак, тому варто обрати усереднений алгоритм Уолша-Адамара, оскільки він є досить швидкодійним і легко адаптованим, і в попередньому підрозділі показав досить високі параметри ефективності. Ми проведемо вдосконалення даного алгоритму з метою підвищення стійкості до атак (як було визначено, даний метод має низьку робастність, тому потребує доопрацювання);

- здійснено обґрунтування вибору мови та середовища розробки для програмної реалізації запропонованих алгоритмів. Програмна реалізація запропонованих алгоритмів приховування та вилучення даних у контейнери-зображення із розширенням спектру методом прямої послідовності виконана у середовищі MathCAD. Вибір даного середовища обґрунтовується наступними підставами: дана система є легко масштабованою, призначеною для математичних обчислень, на яких побудовані алгоритми приховування та зчитування стеганоповідомлень, а також придатна для обробки графічних зображень, вбудовуючи туди повідомлення;

- побудовано програму реалізацію алгоритмів приховування та вилучення даних. Наведено окремі блоки перетворень для обраного алгоритму;

- проаналізовано результати експериментальних досліджень. нами було здійснено розробку програмного забезпечення для вирішення поставленої задачі приховування та вилучення повідомлень методом розширення прямого спектру за допомогою прямої послідовності. Описано основні модулі програми в середовищі

MathCAD та здійснено тестування засобу. Даний метод забезпечує кращу локалізацію особливостей контейнерів-зображень і потребує менших обчислювальних потужностей. Також даний алгоритм сприяє істотному підвищенню стійкості зображення із вбудованим повідомленням.

ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Кузнецов О. О., Євсєєв С.П., Король О.Г. Стеганографія : навчальний посібник. Х. : Вид. ХНЕУ, 2011. 232 с.
2. Юдін О.К., Зюбіна Р.В., Фролов О.В. Аналіз стеганографічних методів приховування інформаційних потоків у контейнери різних форматів. *Радіоелектроника та інформатика*. 2015. № 3. С. 13-21.
3. Пузиренко О.Ю. Протокол оцінки ефективності алгоритмів комп'ютерної стеганографії. *Науково-технічний журнал «Захист інформації».* 2006. № 2. С. 4-10.
4. Бабенко В.Г., Зажома В.М., Нестеренко О.Б.. Метод вбудовування стегоповідомлення на основі ключового елемента. *Захист інформації*. 2014. С. 53-58.
5. Конахович Г.Ф. Комп'ютерна стеганографія. Теорія і практика / Г.Ф. Конахович, А. Ю. Пузиренко. Київ: МК-Пресс, 2006. 288с.
6. Вовк О.О. Методи підвищення стійкості та пропускної здатності систем прихованої передачі інформації. Харків, 2016. 177с.
7. Худьо В.Д., Моделювання стійкої стегофонічної системи із заданими характеристиками мережі. Тернопіль, 2017. 98с.
8. Кінзерявий О.М. Стеганографічні методи приховування даних у векторні зображення, стійкі до активних атак на основі афінних перетворень. Київ, 2015. 112 с.
9. Стеганографічний метод приховування даних у векторних зображеннях /Кінзерявий О.М., та ін. Вісник Інженерної академії України. 2013. №3-4. С. 66-68.

10. Ковтун В.Ю., Кінзерявий О.М., Стокіпний О.Л. Метод шаблонного приховування даних у векторні зображення. Захист інформації. 2014. № 2. С. 139-146.
11. Ковтун В.Ю., Кінзерявий О.М. Експериментальне дослідження методу побітового приховування даних у векторні зображення. Безпека інформації. 2014. № 1. С.66-70.
12. Ковтун В.Ю., Кінзерявий О.М., Гнатюк С.О. Систематизація сучасних методів комп’ютерної стеганографії. Ukrainian Scientific Journal of Information Security, 2013, № 19. С. 209-217.
13. Навроцький Д. О. Дослідження результатів стеганографічного приховування повідомлень у файлах зображення як засобу забезпечення захисту інформації . Вісник Національного технічного університету України «КПІ». № 50. 2012. С. 121-128.
14. Лагун А., Лагун І. Використання вейвлет-перетворення для приховування інформації в нерухомих зображеннях. Захист інформації і безпека інформаційних систем. 2013. С. 98-99.
15. Шелест М.Є., Андреев В.1. Комп'ютерна стеганографія та ЇЇ можливості. *Сучасна спеціальна техніка* № 1 (24), 2011. С.97-104
16. Мельник С.В. Світові тенденції розвитку цифрової стеганографії в контексті завдань забезпечення інформаційної безпеки держави. Актуальні проблеми управління інформаційною безпекою держави : зб. матер. наук.-практ. конф. К. : Наук.-вид. відділ НА СБ України,2010. С. 134-138.
17. “Digital Watermarking and Steganography,” 2008. doi:10.1016/b978-0-12-372585-1.x5001-3.
18. F. Y. Shin, “Digital Watermarking and Steganography,” Dec. 2017. doi:10.1201/9781315219783.

19. N. F. Johnson and S. Jajodia, "Exploring steganography: Seeing the unseen," in *Computer*, vol. 31, no. 2, pp. 26-34, Feb. 1998. doi: 10.1109/MC.1998.4655281.
20. I. V. S. Manoj, “Cryptography and Steganography,” International Journal of Computer Applications, vol. 1, no. 12, pp. 63–68, Feb. 2010. doi:10.5120/257-414.
21. A. Z. Tirkel, C. F. Osborne and R. G. Van Schyndel, "Image watermarking-a spread spectrum application," *Proceedings of ISSSTA'95 International Symposium on Spread Spectrum Techniques and Applications*, Mainz, Germany, 1996, pp. 785-789 vol.2. doi: 10.1109/ISSSTA.1996.563231.
22. J. R. Smith and B. O. Comiskey, “Modulation and information hiding in images,” Lecture Notes in Computer Science, pp. 207–226, 1996. doi:10.1007/3-540-61996-8_42.
23. Methodology of Spread-Spectrum Image Steganography/ L. M. Marvel, C. G. Boncelet, R. Jr., and Charles T. in Jun. 1998. doi:10.21236/ada349102.
24. L. M. Marvel, C. G. Boncelet and C. T. Retter, "Spread spectrum image steganography," in IEEE Transac-tions on Image Processing, vol. 8, no. 8, pp. 1075-1083, Aug. 1999. doi: 10.1109/83.777088.
25. F. S. Brundick and L. M. Marvel, “Implementation of Spread Spectrum Image Steganography,” Mar. 2001. doi:10.21236/ada392155.
26. Patent No.: US 6,557,103 B1, Int.Cl. G06F 11/30. Charles G. Boncelet, Jr., Lisa M. Marvel, Charles T. Retter. Spread Spectrum Image Steganography. Patent No.: US 6,557,103 B1, Int.Cl. G06F 11/30. – № 09/257,136; Filed Feb. 11, 1999; Date of Patent Apr. 29, 2003
27. Yu.V. Stasev, A.A. Kuznetsov, A.M. Nosik. “Formation of pseudorandom sequences with improved autocorrelation properties.” *Cybernetics and Systems Analysis*, vol. 43, Issue 1, pp. 1-11, January 2007. DOI: 10.1007/s10559-007-0021-2

28. Periodic Properties of Cryptographically Strong Pseudorandom Sequences/ A. Kuznetsov, S. Kavun, V. Panchenko, D. Prokopovych-Tkachenko, F. Kurinniy and V. Shoiko in *2018 International Scientific-Practical Conference Problems of Infocommunications. Science and Technology (PIC S&T)*, Kharkiv, Ukraine, 2018, pp. 129-134. doi: 10.1109/INFOCOMMST.2018.8632021
29. Formation of Pseudorandom Sequences with Special Correlation Properties/ A. Kuznetsov, O. Smirnov, D. Kovalchuk, A. Averchev, M. Pastukhov and K. Kuznetsova in *2019 3rd International Conference on Advanced Information and Communications Technologies (AICT)*, Lviv, Ukraine, 2019, pp. 395-399. doi: 10.1109/AIACT.2019.8847861
30. Adaptive Pseudo-Random Sequence Generation for Spread Spectrum Image Steganography Proceedings - 2020 IEEE 11th International Conference on Dependable Systems, Services and Technologies, DESSERT 2020, Kyiv, Ukraine, 2020, DOI: 10.1109/DESSERT50317.2020.9125032

ДОДАТОК А

Схема алгоритму