Міністерство освіти і науки України
Харківський національний університет імені В. Н. Каразіна
Навчально-науковий інститут комп'ютерних наук та штучного інтелекту

Кафедра кібербезпеки інформаційних систем, мереж і технологій

До захисту допущено
Кафедрою КІСМіТ протокол №____ від «___» грудня 2025 р.

завідувач кафедри _____ Марина ЄСІНА
(підпис) *(ім'я, прізвище)*
«___» грудня 2025 р.

Кваліфікаційна робота

здобувача другого (магістерського) рівня вищої освіти

Удосконалення методу розширення спектра для вбудовування динамічних цифрових водяних знаків в аудіосигнал
(назва роботи)

Спеціальність (спеціалізація) 125 «Кібербезпека та захист інформації»

Освітня програма «Безпека інформаційних і комунікаційних систем»

Виконавець _____ Микита Бодня
(підпис) *(ім'я, прізвище)*

Науковий керівник _____ Олексій Нарєжній
(підпис) *(ім'я, прізвище)*

Харків – 2025

РЕФЕРАТ

Пояснювальна записка до проекту магістра містить 69 сторінок, 70 рисунків, 21 таблиць, 3 додатки, 33 посилань на джерела.

Мета роботи полягає в дослідженні та аналізі методу розширення спектра для вбудування цифрових водяних знаків та варіаційних цифрових ідентифікаторів на основі акустичних каналів, особливостей, концепцій та формули експлуатації алгоритму для вирішення питань безпеки.

Об’єкт дослідження – технологія прихованої передачі даних в звукових сигналах на основі особливостей слухової системи людини.

Предмет дослідження – основні засоби та способи для прихованої передачі чутливого контенту на основі розширення спектра сигналу, застосування технологій прихованого зв’язку в програмно-апаратних платформах для побудови стратегії безпеки.

Основними методами досліджень є аналіз та порівняння емпіричних даних основних засобів та методів стеганографічного кодування на основі акустичних каналів. Інтелектуальний огляд періодичних видань та літературних джерел про положення стеганографічних підходів інформаційної безпеки.

У роботі досліджено: методологію розширення спектра, математичні показники продуктивності процедур внесення даних, статистичні та алгебраїчні дані аудіооболонок, спектральних структур, а також потенціал впровадження технології в кіберпростір.

Результати роботи можуть бути використані у різних наукових виданнях, а також в глобальних технічних проектах. Викладені положення – теоретична основа для поглиблення у технології прихованого зв’язку та забезпечення інтелектуального права.

Ключові слова: АУДІОСТЕГАНОГРАФІЯ, АКУСТИЧНИЙ КАНАЛ, СЕКРЕТНЕ ПОВІДОМЛЕННЯ, СЛУХОВА СИСТЕМА ЛЮДИНИ, СТЕГАНОАНАЛІЗ, ПРИХОВАНИЙ ЗВ’ЯЗОК, РОЗШИРЕННЯ СПЕКТРА.

ABSTRACT

The explanatory work to the master`s project contains 69 pages, 70 figures, 21 tables, 3 appendices, and 33 references.

The goal of the work is the research and analysis of spread spectrum method for embedding digital watermarks and various digital identifiers based on acoustic channels, peculiarities, concepts and implementation of the algorithm for security issue solving.

The object of research is a covert transmitting technology in sound signals based on the peculiarities of the human auditory system.

The subject of research is the main features and methods for the covert transmission of sensitive content based on signal spectrum expansion, and the use of the covert communication technology in software and hardware platforms to implement a security strategy.

The main research methods are the analysis and comparison of empirical data regarding the main means and methods of steganographic encoding based on acoustic channels. An intelligent review of periodical publications and literary reports on the status of steganographic approaches to information security.

The work investigates: the spread spectrum methodology, mathematical performance indicators for data embedding procedures, statistical and algebraic data of audio containers and spectral structures, as well as the potential for implementing the technology in cyberspace.

The results of the work can be used in various scientific publications, as well as in global technical projects. The stated provisions constitute the theoretical basis for further research into covert communication technologies and ensuring intellectual property rights.

Keywords: AUDIO STEGANOGRAPHY, ACOUSTIC CHANNEL, SECRET MESSAGE, HUMAN AUDITORY SYSTEM, STEGANALYSIS, COVERT COMMUNICATION, SPREAD SPECTRUM.

ЗМІСТ

ПЕРЕЛІК ПОЗНАЧЕНЬ І СКОРОЧЕНЬ…….. 5
ВСТУП……. 7
1 ТЕОРЕТИЧНІ ПОЛОЖЕННЯ АУДІОСТЕГАНОГРАФІЇ…….. 9
1.1 Теоретична база стеганографії……. 9
1.2 Положення аудіостеганографії……... 11
1.3 Потенціал стеганографічного апарату……13
1.4 Математичні показники оцінки продуктивності стеганографії…….. 16
2 СПЕЦИФІКАЦІЯ МЕТОДУ РОЗШИРЕННЯ СПЕКТРА…….. 20
2.1 Аналіз аудіоконтейнерів…….. 20
2.2 Сутність методу розширення спектра…… 30
2.3 Оцінка та дослідження параметрів безпеки способу……... 36
2.4 Порівняльний аналіз методів…….. 43
2.5 Вектори удосконалення алгоритму…… 50
3 ОПИС ПРОГРАМНОГО КОМПЛЕКСУ……. 57
3.1 Загальні положення…….. 57
3.2 Мережевий аналіз графічної частини……. 58
3.3 Характеристика графічного інтерфейсу продукту…… 61
3.4 Подальші плани оптимізації…… 65
ВИСНОВКИ…….. 67
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ……. 69
ДОДАТОК А…….. 73
ДОДАТОК Б…….. 77
ДОДАТОК В…….. 80

ПЕРЕЛІК ПОЗНАЧЕНЬ І СКОРОЧЕНЬ

ADC – Analog-to-Digital Converter
AD – Average Absolute Difference
AF – Audio Fidelity
AES – Advanced Encryption Standard
BER – Bit Error Rate
CQ – Correlation Quality
CRC – Cyclic Redundancy Check
DAC – Digital-to-Analog Converter
DSSS – Direct Sequence Spread Spectrum
DC – Direct Current
FFT – Fast Fourier Transform
FT – Fourier Transform
GSSNR – Global Sigma Signal to Noise Ratio
GF – Galois Field
HS – Histogram Similarity
OSI – Open Systems Interconnection
PSNR – Peak Signal to Noise Ratio
PDF – Portable Document Format
IFFT – Inverse Fast Fourier Transform
IFT – Inverse Fourier Transform
IF – Image Fidelity
LSB – Least Significant Bit
LMSE – Laplacian Mean Square Error
MMS – Multimedia Messaging Service
MPEG – Moving Picture Experts Group
MP3 – MPEG-1 Audio Layer III
MD – Maximum Difference

MSE – Mean Square Error
NAD – Normalized Average Absolute Difference
NMSE – Normalized Mean Square Error
NC – Normalized Cross-Correlation
NSER – Normalized Sigma to Error Ratio
SMS – Short Message Service
SNR – Signal to Noise Ratio
SC – Structural Content
SSNR – Sigma Signal to Noise Ratio
WAV – Waveform Audio File Format
АС – Ансамбль Сигналів
АКФ – Аперіодична Функція Автокореляції
БД – База Даних
БЧХ – Боуза-Чоудхурі-Хоквінгема
ДПФ – Дискретне перетворення Фур’є
ЗДПФ – Зворотне Дискретне Перетворення Фур’є
ІБ – Інформаційна Безпека
ІзОД – Інформація з Обмеженим Доступом
ІТС – Інформаційно-Телекомунікаційні Системи
КЗ – Канал Зв’язку
НЗБ – Найменш Значущого Біту
НСД – Несанкціонований Доступ
ПВП – Псевдовипадкова Послідовність
ПДПФ – Пряме Дискретне Перетворення Фур’є
ПЗ – Програмне Забезпечення
ШІ – Штучний Інтелект
ССЛ – Слухова Система Людини
ЦВЗн – Цифровий Водяний Знак
ЦОС – Цифрова Обробка Сигналів

ВСТУП

Технології інформаційної безпеки (ІБ) є невід'ємною складовою сучасних технічних систем. Стабільне функціонування інформаційного простору, його застосування суспільством та державою забезпечується інструментами кібербезпеки. Кіберпростір асоціюється із театром воєнних дій [1], тому держава повинна мати спроможність для захисту національних інтересів. Розвиток цифрової інфраструктури сприяє модернізації засобів кібератак, що спонукає до оптимізації підходів безпеки. Еволюція квантових обчислень стала новим викликом для механізмів захисту. Компоненти структури концепції ІБ державних інститутів, комерційних та військових платформ потребують модернізації та оснащення. Основні вітки кібербезпеки [2, 3] – це криптографія, стеганографія та елементи цифрових водяних знаків (ЦВЗн).

Існуючі обчислювальні можливості відкрили нові тренди в парадигмі ІБ. Засоби протидії несанкціонованому доступу (НСД) широко використовувалися на практиці, починаючи зі стародавніх часів. Розвиток інформаційних систем та мереж [2] спричинив появу напряму комп'ютерної стеганографії. Принцип стеганографії активно досліджується у науковому просторі. Динаміка експериментів стеганографічних засобів набула революційного імпульсу. Розвиток техніки вбудованих ЦВЗн у медіаоб'єктах, зумовлений поширенням електронного копіювання та плагіату. В умовах вразливості традиційних інструментів захисту – вони стали базовим елементом цифрового середовища, безпеки та монетизації цифрового контенту.

Стеганографічні заходи використовують структурну збитковість [2, 3] контейнера-переносника. Оболонка медіапакета не зазнає маніпуляції. Технологія використовується в комерційних, фінансових структурах та підприємствах. Правоохоронними та державними органами для прихованої передачі інформації.

Виділяють дві причини популярності стеганографічного вектора: високі обчислювальні потреби для криптографічних операцій та проблеми забезпечення авторського права. Потокова стеганографічна упаковка як оптимальна

альтернатива криптографії є перспективним інструментом. Криптографічні комплекси доступні в обмежених локаціях із великими обчислювальними властивостями. Фундамент криптографічних методів заснований на теорії чисел та алгебраїчних кодах. Засоби шифрування вимагають високих показників швидкості та ресурсів пам’яті. Своєю чергою, стеганографічні функції здійснюють маніпуляції над мультимедійними об’єктами [3]. Спектр алгоритмів стеганографії є стійким варіантом для забезпечення надійності інформаційних артефактів.

Мета роботи – дослідження методу розширення спектра для потокового кодування двійкового алфавіту, можливості вдосконалення та застосування в інноваційних проектах. Галузь застосування включає сегменти мереж служб спеціального зв’язку [1], військову розвідку та додатки автентифікації. Стеганографічна процедура є гарантією забезпечення прав інтелектуальної власності.

Стеганографічні вектори [2] пов’язані з елементами криптографічного коду. Закриті стеганосистеми використовують способи криптографії для захисту від НСД. Алгоритми цифрової обробки сигналів (ЦОС) інтегровані у процедуру пакування в призмі стеганографії. Стеганографічні засоби використовують функції гешування для створення цифрових ідентифікаторів.

1 ТЕОРЕТИЧНІ ПОЛОЖЕННЯ АУДІОСТЕГАНОГРАФІЇ

1.1 Теоретична база стеганографії

Стеганографічна архітектура (додаток А) включає сукупність засобів та інструментів для запису двійкового алфавіту до структури медіафайлів. Концепція стеганографії має історичний генезис, що набув варіаційних форм у цифрову епоху. Комп'ютерна стеганографія використовує потокові та графічні контейнери для внесення інформаційних відомостей [2]. Базова концепція [2-5] підходу приховування – передати заповнений контейнер із чутливою інформацією у цілісному вигляді. Стеганографія – це парадигма ІБ та мистецтво ініціювання каналу зв'язку (КЗ), при якому приховується факт існування комунікаційного тунелю. Вітка прихованого зв'язку [4] доповнює загальну парадигму кібербезпеки в частині забезпечення фундаментальних властивостей (табл. 1.1).

Таблиця 1.1 – Порівняння властивостей векторів кібербезпеки

Технологія захисту інформації	Шифрування	Цифровий підпис	Стеганографія
Незмінність	✅	❌	✅
Цілісність	❌	✅	✅❌
Конфіденційність	✅	❌	✅❌

Стеганографічна технологія входить в розділ інформаційного приховування парадигми цифрового захисту. Динамічний темп розвитку вектора стеганографії доводить її перспективність у галузі інформаційних технологій. Алгоритми розраховані на збалансоване розсіювання інформації по контейнеру. Для забезпечення стійкості системи проти методів штучного інтелекту (ШІ) та стегоаналізу. Стеганографія є елементом сценаріїв безпеки, контролю доступу та систем підтвердження особистості. КЗ, створений технологіями [2] приховування інформації не повинен викликати підозр у сторонніх спостерігачів. Загальна модель цифрового захисту, що охоплює положення приховування даних, представлена на рис. 1.1.

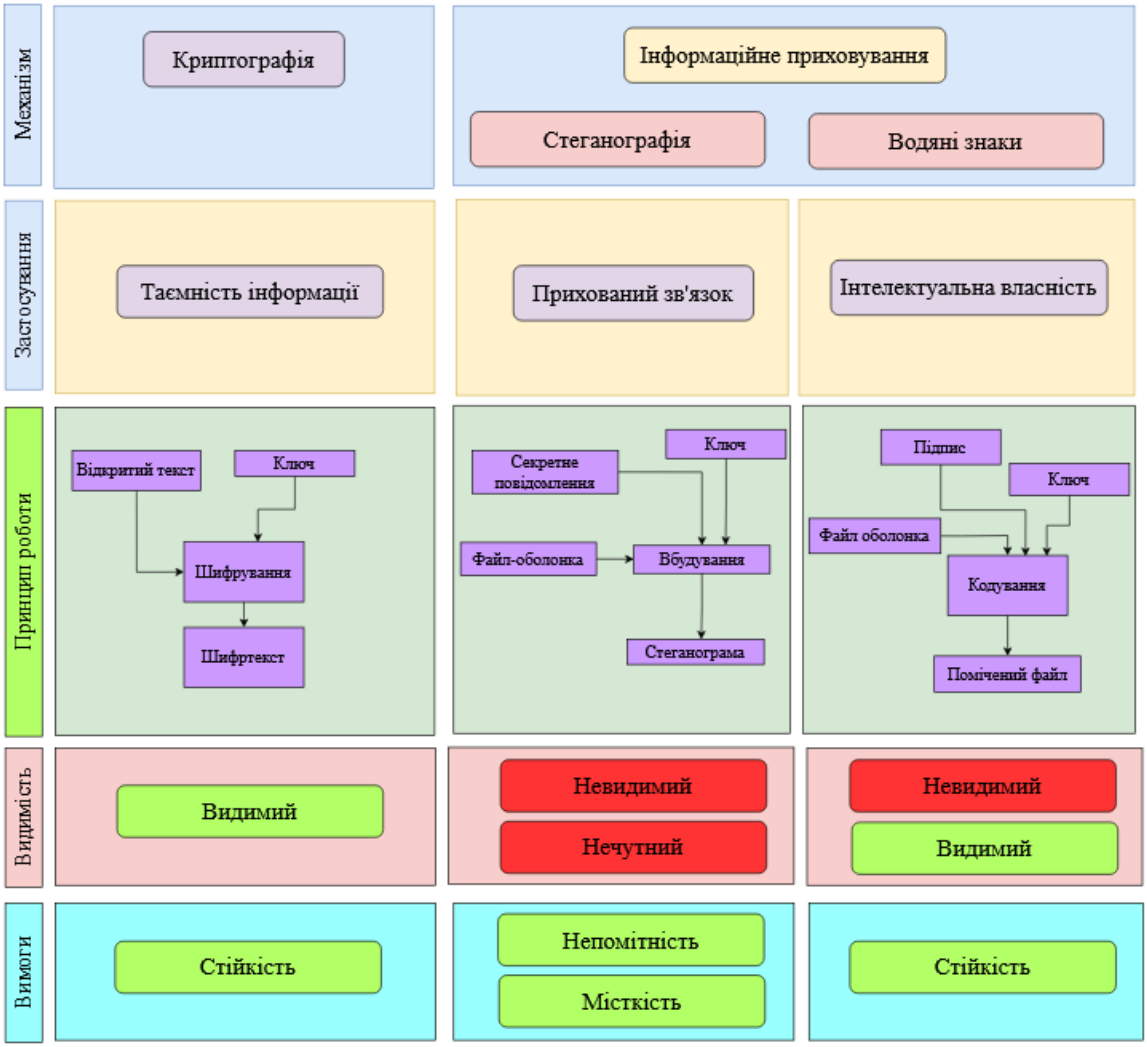


Рисунок 1.1 – Парадигми ІБ

Стеганографічна система є варіантом системи зв’язку [2-6]. Стеганографічна схема класифікується за характером підходу вбудовування (рис. 1.2). Підхід визначає конфігурацію вбудування та результат процедури. Архітектура системи стеганографії породжує стеганоканал, який транспортує заповнений контейнер – стеганограму. Гіпотетично, при передачі по лініях зв’язку об’єкт піддається зовнішнім впливам та перетворенням порушників. Способи стеганографії [2] – це компроміс між місткістю, непомітністю та обчислювальною складністю. Стеганосистема взаємодіє із потоком даних, який підмішується у структуру пакета-переносника. Особливий інтерес [2, 3] проявляється до закритих та робастних систем стеганографії. Ефективний метод внесення даних повинен відповідати вимогам стеганографічних систем.

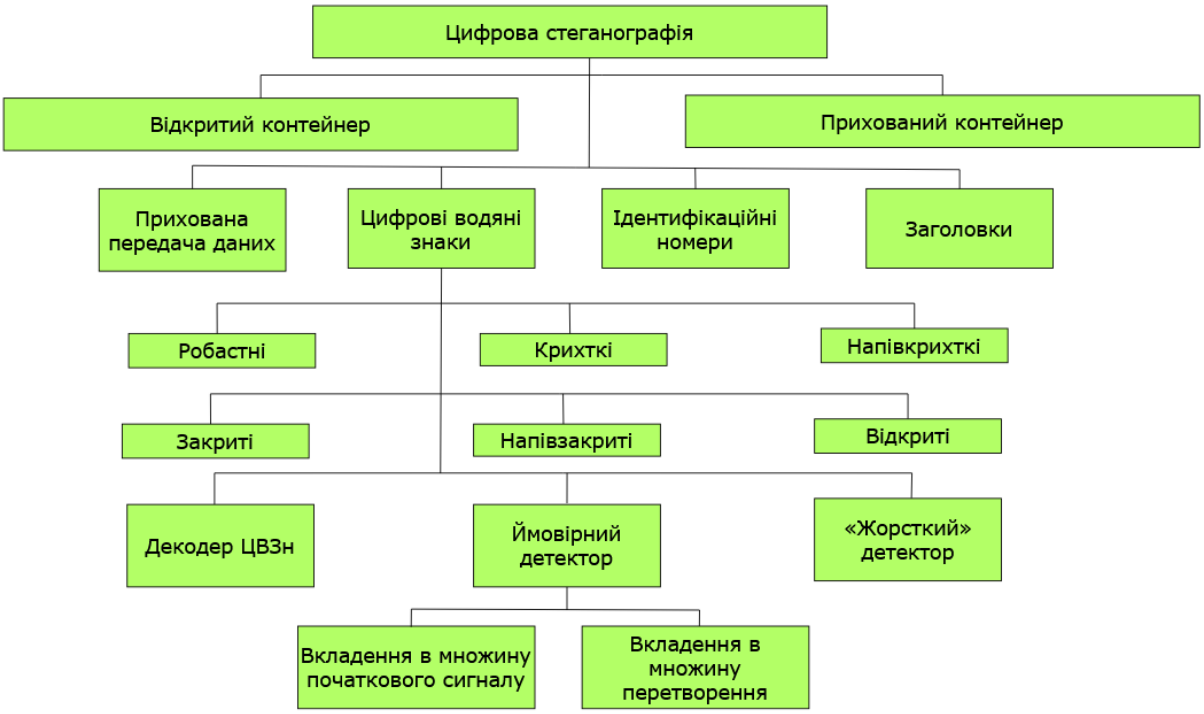


Рисунок 1.2 – Класифікація стеганосистем

1.2 Положення аудіостеганографії

Звукова стеганографія передбачає монтування інформаційних відомостей у надмірність аудіосигналу. Цифрові артефакти записуються у дискретизований аудіопотік, що призводить до модифікації двійкового контексту файлового об’єкта. Методологія аудіоприховуванння орієнтована на особливості слухової системи людини (ССЛ). Виділяють ряд властивостей ССЛ на основі яких формується підхід інкапсуляції [2, 3]:

– слабка чутливість ССЛ до незначної модифікації звучності аудіопотоку;

– ефект маскування;

– несприйнятливість ССЛ до зміни абсолютної фази аудіосигналу;

– частотна чутливість;

– слабка чутливість ССЛ до незначної зміни ехосигналів.

Бітовий контент кодується в оболонці аудіотреку та пересилається по КЗ. Під час передачі на інформаційну суміш можуть впливати зовнішні чинники: шуми та перетворення стегоаналізу. Пасивний вплив може спотворити частину інформації або знищити інформаційну посилку. Декодування здійснює стеганографічний декодер на основі алгоритму декапсуляції за допомогою секретного ключа. Перед

процедурою здійснюється оцінка отриманого сигналу. Методи аудіостеганографії [7] можуть вбудовувати будь-які повідомлення у звукові файли WAV (Waveform Audio File Format) і навіть MP3 (MPEG-1 Audio Layer III). Узагальнена модель роботи системи прихованого спілкування наведена на рис. 1.3.

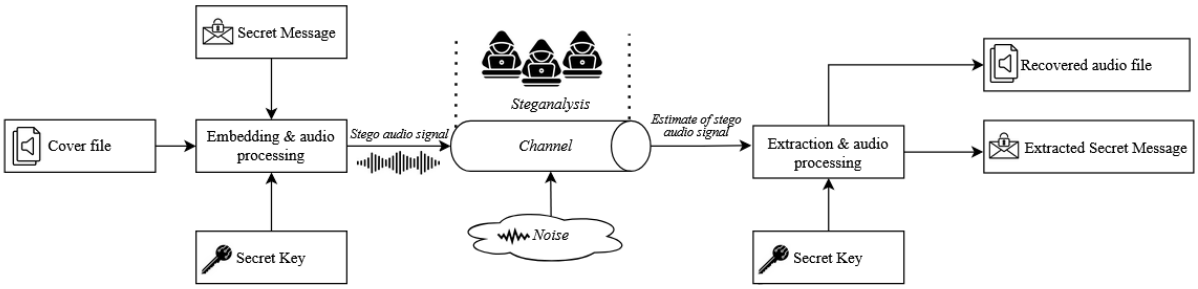


Рисунок 1.3 – Узагальнена архітектура роботи стеганографічного апарату

Парадигма звукового вбудування має ряд особливостей, що дозволяють приховувати дані. ССЛ менш чутлива до додавання шумового компонента у середовище звуку. Експлуатація способів аудіостеганографії (рис. 1.4) дозволяє вбудовувати великі масиви даних. Для вбудування даних використовуються спектральні елементи сигналу, модифікація яких несуттєва. Розміри аудіооб’єктів перевищують розміри стосовно інших варіантів контейнерів.

Еволюція методів звукового приховування [4] динамічно розвивається. Основна мета – досягнення високих показників надійності та конфіденційності. Головним фактором залишається величина внесених спотворень, що повинна бути менше за поріг чутливості ССЛ. Нині парадигма звукового вбудовування налічує широкий спектр методів. Підтримується гібридний сценарій [6] застосування математичних обчислень. Способи акустичних маніпуляцій підтримують модифікації у часовій та частотній областях. Сучасні дослідження часто схиляються до адаптивних методів та методів у частотній області, оскільки вони забезпечують найкращий захист від сучасних методів стегоаналізу. Методи приховування підтримують баланс між показниками обсягу внесення даних та величиною спотворення. Мета підходу – досягнення природної величини шуму, що неможливо класифікувати як інформаційний пакет. В контексті статистичних розрахунків та практичних експертиз заповненого контейнера. Обчислювальний баланс обходить машинні аналізатори стеганографічних вкладень.

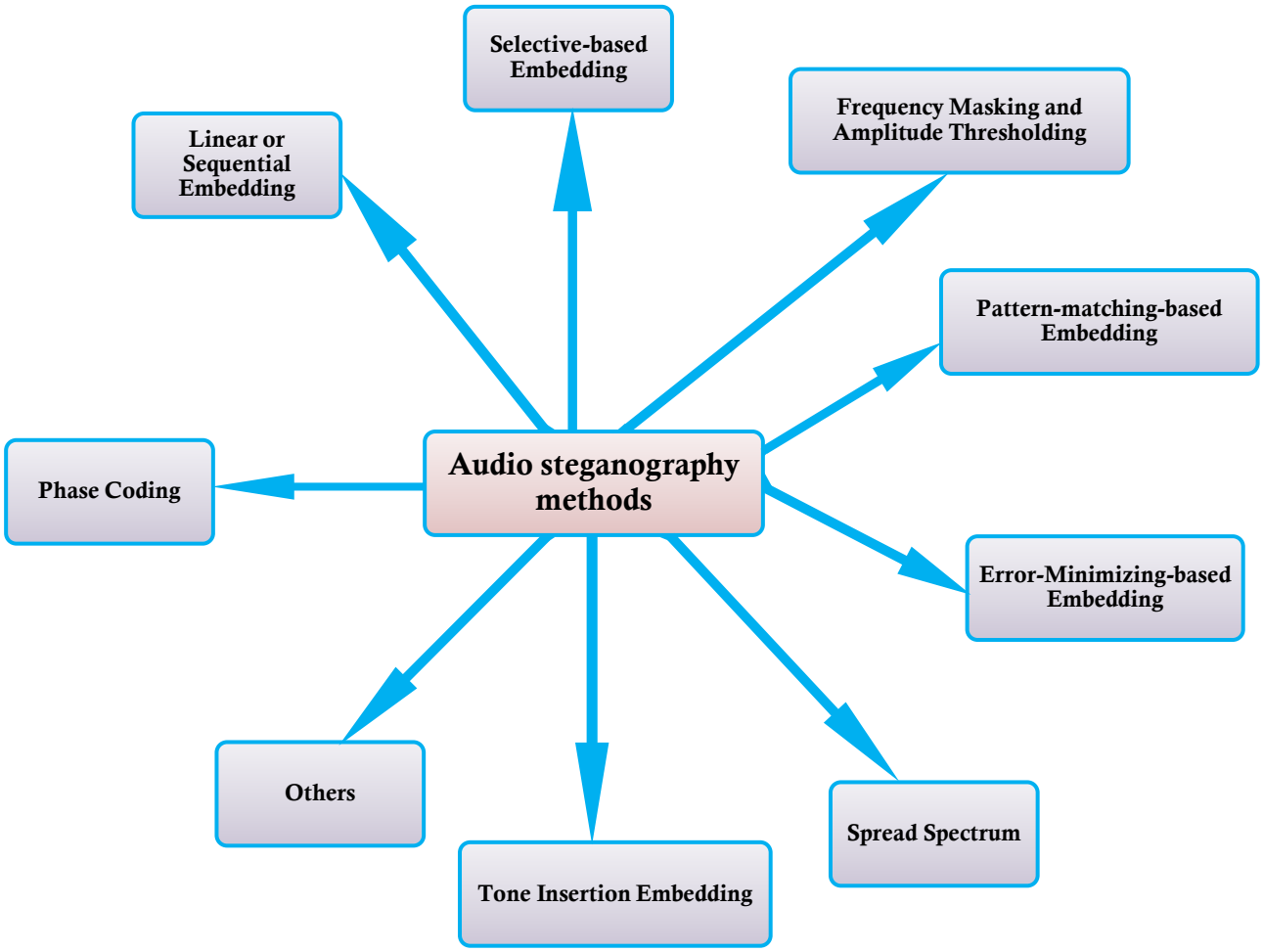


Рисунок 1.4 – Варіанти методів звукового приховування

Сучасні методи вбудування мають проблеми з визначенням [8] точного розташування інформаційного контенту у звуковому контейнері. Цей фактор може викликати загрози безпеці та цілісності даних. Тому важливо попередньо налаштувати дані локалізації контенту на стороні приймача, щоб отримати інформаційний потік без спотворень.

1.3 Потенціал стеганографічного апарату

Апріорна схема стеганографії [2-4] використовується у технологіях маркування медіаоб’єктів. Гарантія авторського права є невід’ємною частиною забезпечення власності контенту. Акцент стеганографії [2] спрямований на приховування даних в межах контейнера, коли ЦВЗн забезпечує права інтелектуальної власності на цифровий продукт. Напрям ЦВЗн підтримує

технології та інструменти інформаційного приховування, але здебільшого належить до відкритих систем стеганографії. Стеганографічні методи дозволяють вбудовувати ЦВЗн у найменш помітні області сигналу. Використання адаптивної стеганографії дозволяє системі аналізувати контент і вибирати оптимальні параметри вбудовування ЦВЗн. ЦВЗн може приймати різні контексти та включати таємні відомості, які доступні авторизованим користувачам. Напівзакрита стеганосистема [2] дозволяє вилучати цифровий ідентифікатор, що є ознакою легітимності авторського права. При цьому певний контингент абонентів може обмінюватися конфіденційними артефактами. Експлуатація секретного ключа є гарантією таємності інформації. Галузі практичної інтеграції (табл. 1.2) охоплюють різні сектори суспільства.

Таблиця 1.2 – Практичні аспекти застосування ЦВЗн

Сфера	Внесок стеганографії
Фотографія	Створення невидимих ЦВЗн, що залишаються навіть після кадрування та фільтрації.
Аудіоіндустрія	Вбудовування ЦВЗн у звукові треки для відстеження незаконного поширення в стримінгових сервісах.
Кінематограф	Приховування у відеопотоку унікальних ЦВЗн для кожного кінопрокатника
Документообіг	Маркування конфіденційних PDF-файлів для виявлення джерела витоку.

Інший аспект перспективи застосування стеганографічних механізмів: лежить в парадигмі акустичних каналів. В системах обміну голосовими потоками (додаток Б), встановлюється стеганографічна приставка [2]. Сутність апарату – закодувати цінні відомості у фрагментах мови непомітним чином. При цьому абоненти зв'язку не помічають ознак прихованого КЗ у потоці обміну. Стеганографічна архітектура реалізується у закритому форматі із застосуванням секретного ключа (рис. 1.5).

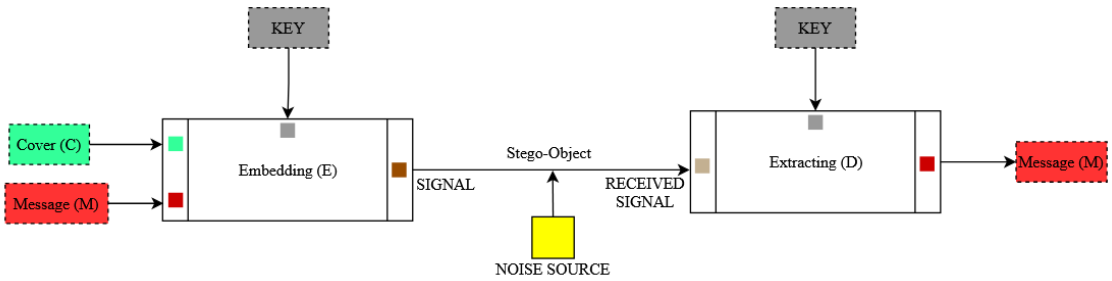


Рисунок 1.5 – Модель стеганосистеми із секретним ключем

Відсутність контексту [6] секретного ключа забезпечує таємницю цінних відомостей і унеможливлює факт доведення їх існування. У потоковій розмові по мобільним мережам може вкладатися вторинна смуга спілкування. Канал таємного спілкування може бути розгорнутий без суворих вимог до частотної смуги спектра. Приклади експлуатації підходу організації таємного спілкування має велику практичну множину. У статті [4] наводиться ситуація, коли необхідно відправити графічне зображення діагнозів пацієнтів медзакладу. Для забезпечення непомітності та секретності даних пацієнтів використовується акустичний канал із застосуванням секретного ключа. Кодер вкладає у звуковому потоці графічний знімок для подальшого збереження до бази даних (БД). Стеганографічний декодер вилучає дані із контейнера та заносить до БД. Як контейнер використовуються голосові SMS (Short Message Service) або MMS (Multimedia Messaging Service). SMS або MMS надсилаються по КЗ та обробляються на стороні отримувача. Корисна інформація вилучається на основі секретного ключа. Однак існує динамічний вебзастосунок [4], який приховує текст на медіаобгортці (додаток Б), а потім поширює його в MMS. Узагальнена модель роботи системи таємного спілкування наведена на рис. 1.6.

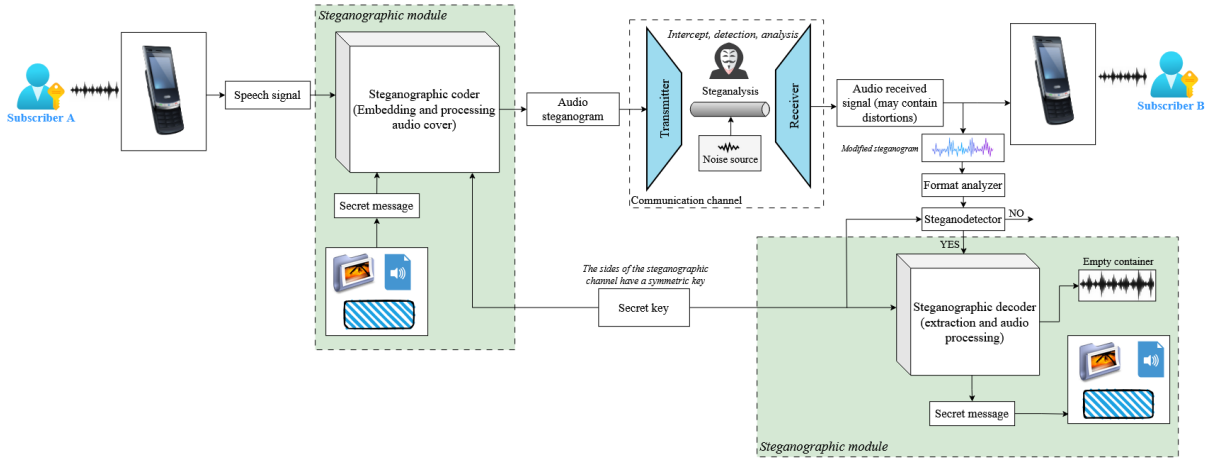


Рисунок 1.6 – Схема таємного спілкування в акустичних каналах

В аудіосигналах інформація вкладається у часові відліки сигналу-переносника. Після всіх перетворень DAC (Digital-to-Analog Converter) перетворює цифровий сигнал (дискретні значення, біти) на аналоговий сигнал (безперервну хвилю). Хвиля передається по КЗ та обробляється приймачем. ADC (Analog-to-

Digital Converter) перетворює безперервний аналоговий сигнал на дискретний цифровий код (послідовність бітів). Компоненти стеганографічного апарату здійснюють декапсуляцію потоку двійкового алфавіту. Пристрої реалізують функцію стеганографії. Рис. 1.7 демонструє алгоритм вкладання інформації у форму потокового сигналу та є теоретичною основою для КЗ.

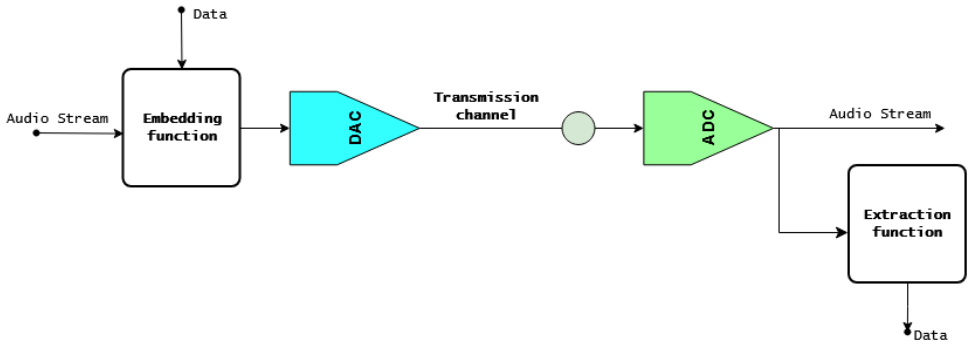


Рисунок 1.7 – Принцип стеганографічного кодування в акустичних каналах

1.4 Математичні показники оцінки продуктивності стеганографії

Процедура продуктивності монтування оцінюється за допомогою математичних показників. Такі показники становлять корисність у дослідженні результатів стеганограми та процедури запису. Це необхідно для факторів підбору атрибутів при підмішуванні артефакту. Оцінка внесених даних прогнозує потенціал виявлення порушником чи ШІ факту прихованого елементу. З метою порівняння варіативних інструментів приховування розробляють показники якості. Такі показники приймають застосовність до масивів пікселів зображень та відліків аудіотреків. Популярністю користується вилучене [3, 5] з галузі радіотехніки відношення «сигнал/шум». Одиниця вираження обчислювальної метрики у децибелах. Клас різницевих показників охоплює більшу множину використовуваних величин. Оцінюється математична відмінність між оригінальним потоком та стеганографічним відображенням. На основі цього машинні аналізатори роблять висновки про існування прихованих сегментів даних. Оцінки якості сприяють дослідженню позитивних та пасивних сторін способу запису. Вторинна група охоплює кореляційні функції, що визначають міру пов’язаності між об’єктами експериментів. Теорія статистики та оцінок якості

реалізує механізм детектування для верифікації медіаструктур. В практичній площині – це програмування спеціалізованих детекторів на оцінку наявності прихованих фрагментів. Розгорнутий перелік [3] показників (1.1)-(1.18) наводиться у табл. 1.3.

Таблиця 1.3 – Показники оцінки стеганографічного запису

Математична оцінка	Формула
Максимальна різниця (Maximum Difference)	$MD = \max_{xy}\left\|C_{xy} - S_{xy}\right\|$ (1.1)
Середня абсолютна різниця (Average Absolute Difference)	$AD = \frac{1}{XY}\sum_{xy}\left\|C_{xy} - S_{xy}\right\|$ (1.2)
Нормована середня абсолютна різниця (Normalized Average Absolute Difference)	$NAD = \frac{\sum_{xy}\left\|C_{xy} - S_{xy}\right\|}{\sum_{xy}\left\|C_{xy}\right\|}$ (1.3)
Середньоквадратична помилка (Mean Square Error)	$MSE = \frac{1}{XY}\sum_{xy}\left(C_{xy} - S_{xy}\right)^2$ (1.4)
Нормована середньоквадратична помилка (Normalized Mean Square Error)	$NMSE = \frac{\sum_{xy}\left(C_{xy} - S_{xy}\right)^2}{\sum_{xy}\left(C_{xy}\right)^2}$ (1.5)
L^p – норма (L^p – norm)	$L^p = \left(\frac{1}{XY}\sum_{xy}\left\|C_{xy} - S_{xy}\right\|^p\right)^{\frac{1}{p}}$ (1.6)
Лапласова середньоквадратична помилка (Laplacian Mean Square Error)	$LMSE = \frac{\sum_{xy}\left(\nabla^2 C_{xy} - \nabla^2 S_{xy}\right)^2}{\sum_{xy}\left(\nabla^2 C_{xy}\right)^2}$, де $\nabla^2 C_{xy} = C_{x+1y} + C_{x-1y} + C_{xy+1} + C_{xy-1} - 4C_{xy}$. (1.7)
Відношення сигнал/шум (Signal to Noise Ratio)	$SNR = \frac{\sum_{xy}\left(C_{xy}\right)^2}{\sum_{xy}\left(C_{xy} - S_{xy}\right)^2}$ (1.8)
Максимальне відношення сигнал/шум (Peak Signal to Noise Ratio)	$PSNR = XY\frac{\max_{xy}\left(C_{x,y}\right)^2}{\sum_{xy}\left(C_{xy} - S_{xy}\right)^2}$ (1.9)
Якість зображення (Image Fidelity) / Якість звучання (Audio Fidelity)	$IF / AF = 1 - \frac{\sum_{xy}\left(C_{xy} - S_{xy}\right)^2}{\sum_{xy}\left(C_{xy}\right)^2}$ (1.10)

Продовження таблиці 1.3

Нормована взаємна кореляція (Normalized Cross-Correlation)	$$NC = \frac{\sum_{xy} C_{xy} S_{xy}}{\sum_{xy} \left(C_{xy}\right)^2} \quad (1.11)$$
Якість кореляції (Correlation Quality)	$$CQ = \frac{\sum_{xy} C_{xy} \cdot S_{xy}}{\sum_{xy} C_{xy}} \quad (1.12)$$
Додатковий набір показників	
Структурний зміст (Structural Content)	$$SC = \frac{\sum_{xy} \left(C_{xy}\right)^2}{\sum_{xy} \left(S_{xy}\right)^2} \quad (1.13)$$
Загальне сигма відношення сигнал/шум (Global Sigma Signal to Noise Ratio)	$$GSSNR = \frac{\sum_b \sigma_b^2}{\sum_b \left(\sigma_b - \tilde{\sigma}_b\right)^2}, \quad (1.14)$$ де $\sigma_b = \sqrt{\frac{1}{n}\sum_{block\,b}\left(C_{xy}\right)^2 - \left(\frac{1}{n}\sum_{block\,b} C_{xy}\right)^2}$.
Сигнал-відношення сигнал/шум (Sigma Signal to Noise Ratio)	$$SSNR' = \frac{1}{n}\sum_b SSNR_b, \quad (1.15)$$ де $SSNR_b = 10\lg\left[\frac{\sigma_b^2}{\left(\sigma_b - \tilde{\sigma}_b\right)^2}\right]$.
Нормоване відношення сигма/помилка (Normalized Sigma to Error Ratio)	$$NSER = \frac{1}{\max\left(SER\right)}\sum_b SER_b, \quad (1.16)$$ де $SER_b = \frac{\sigma_b^2}{\left[\frac{1}{n}\sum_{block\,b}\left(C_{xy} - S_{xy}\right)^2\right]}$.
Подібність гістограм (Histogram Similarity)	$$HS = \sum_{c=0}^{255} \left| f_c(c) - f_s(c) \right|, \quad (1.17)$$ де $f_c(c)$ – відносна частота градації кольору *c* у зображенні з 256 рівнями кольорів; $f_s(c)$ – частоти градації кольорів для стеганографічного образу. Для зіставлення аудіопотоку можна налаштувати таку формулу: $$HS = \sum_{a=-32768}^{32767} \left| f_c(a) - f_s(a) \right|, \quad (1.18)$$ де $f_c(a)$ – відносна частота інтенсивності звуку *a* в потоці сигналу з 65 536 рівнями амплітуди (напруги сигналу). Середня точка (напруга сигналу) асоціюється із 0;

Продовження таблиці 1.3

	$f_s(a)$ – часні частотні компоненти інтенсивностей звучності для стеганографічного образу сигналу.

У наведених співвідношеннях [3, 5] через C_{xy} позначаються відліки для потокового об’єкта з координатами (x,y). S_{xy} – позначення відноситься до семплів стеганографічного образу із власними координатами. Позначення виражені для звукових контейнерів. Деякі показники (GSSNR, SSNR та SER) вимагають поділу структури контейнеру на блоки кількістю N розміром n. Наведені математичні вирази орієнтовані для графічних зображень. При цьому їх можна адаптувати для досліджень звукових потоків. Оскільки аудіосигнал може мати декілька паралельних потоків, розглянуті формули дозволяють проводити аналіз стану інтенсивностей напруги сигналу.

Політика інформаційно-телекомунікаційних систем (ІТС) направлена на прозорість циркулюючого контенту. Тому в структуру ІТС вбудовані детектори, які здійснюють перевірку вихідного медіасегменту. Налаштування правильних даних є головною метою вбудування. З метою безперебійного та таємного передавання чутливих даних до пункту призначення. На базі статистичних метрик та показників якості системи ШІ приймають рішення про існування прихованого КЗ. На основі метрик спотворень знаходиться межа допустимих викривлень та оптимальний обсяг внесеної інформації. Пошук оптимального компромісу є важливим аспектом оптимізації тактики запису.

2 СПЕЦИФІКАЦІЯ МЕТОДУ РОЗШИРЕННЯ СПЕКТРА

2.1 Аналіз аудіоконтейнерів

Аудіопотік є контейнером, який використовується для стеганографічного кодування інформаційного контенту. Аудіофайл (табл. 2.1) охоплює ряд властивостей та спектральну структуру.

Таблиця 2.1 – Атрибути аудіофайлів-переносників

Ідентифікатор звукового потоку	Кількість каналів	Частота дискретизації	Кількість біт кодування	Середня кількість біт за секунду
DCF77.wav	1	24000	16	48000
RBU_with_carrier_audio.wav	1	8000	16	16000

Статистична оцінка допомагає систематично провести дослідження набору амплітуд звукового сигналу (табл. 2.2). Розробити модель для дослідження та аналізу деякого феномену.

Таблиця 2.2 – Статистичний аналіз даних

Статистична величина	DCF77.wav	RBU_with_carrier_audio.wav
Об’єм вибірки	1508415	98675
Середнє значення	-0.263	-26.586
Максимальне значення	4263	12888
Мінімальне значення	-4216	-12299
Мода	384	Багатомодальний (4615, 4689, 4714, -4880)
Медіана	0	-30
Стандартне відхилення	1705.125	3392.172
Дисперсія	2907452.31	11506832.051

Графічне представлення результатів наведено на рис. 2.1-2.7. Статистика аудіосигналів демонструє загальні числові характеристики. Ці властивості надають план для розуміння природи сигналу, його якості та динаміки. Статистика – це

потужний апарат, який перетворює великий масив даних вибірки напруги у числові дані, які демонструють характер звукової хвилі.

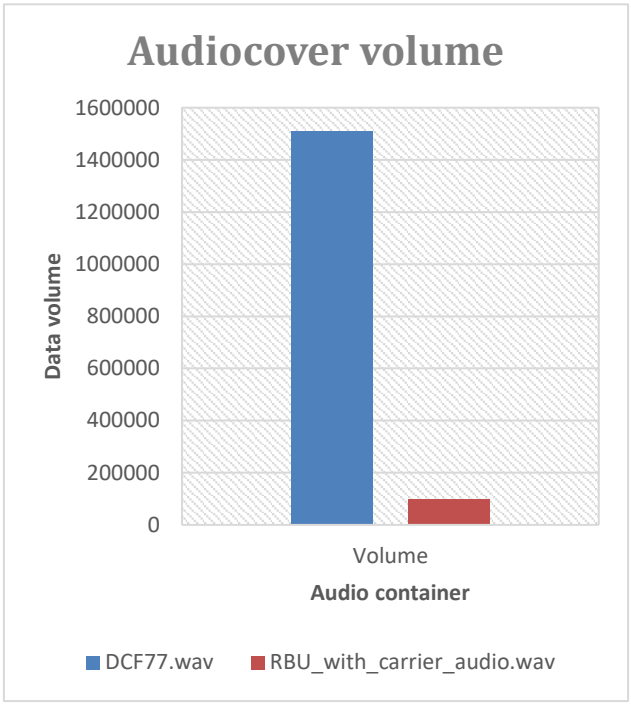


Рисунок 2.1 – Обсяг звукових сигналів

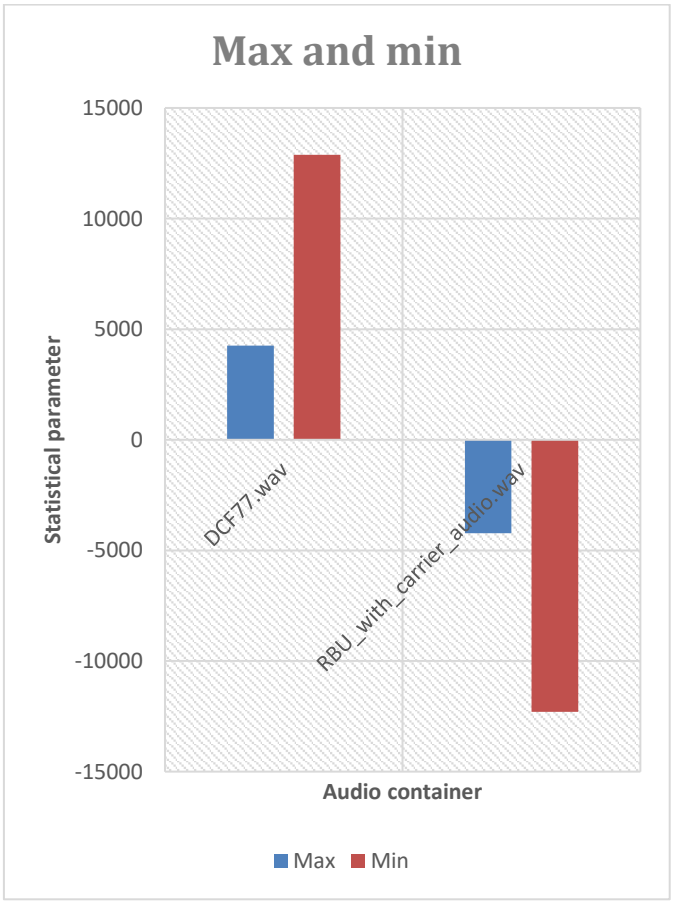


Рисунок 2.2 – Статистичні показники максимальних та мінімальних значень

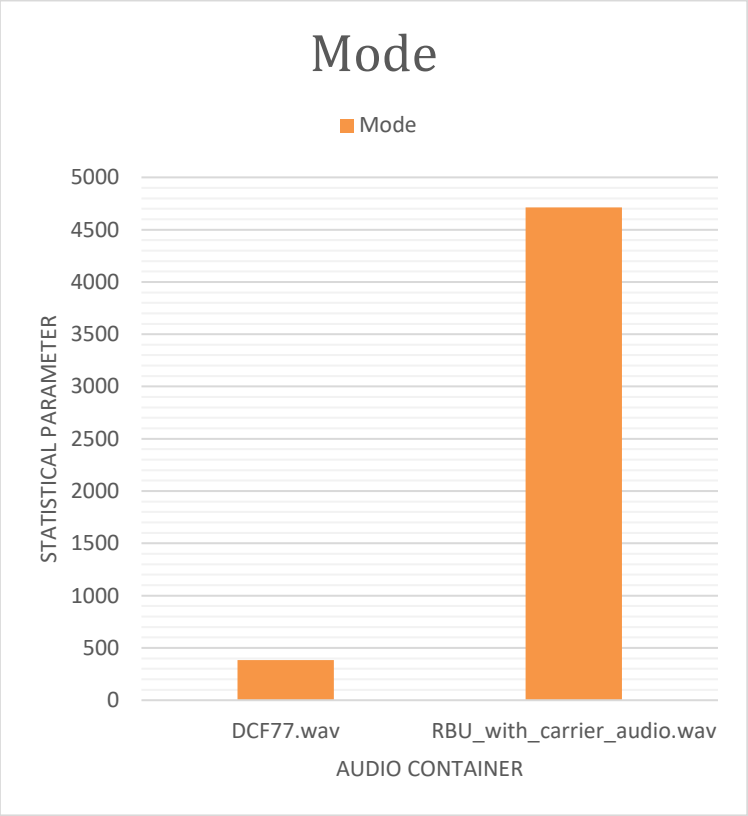


Рисунок 2.3 – Статистичні показники

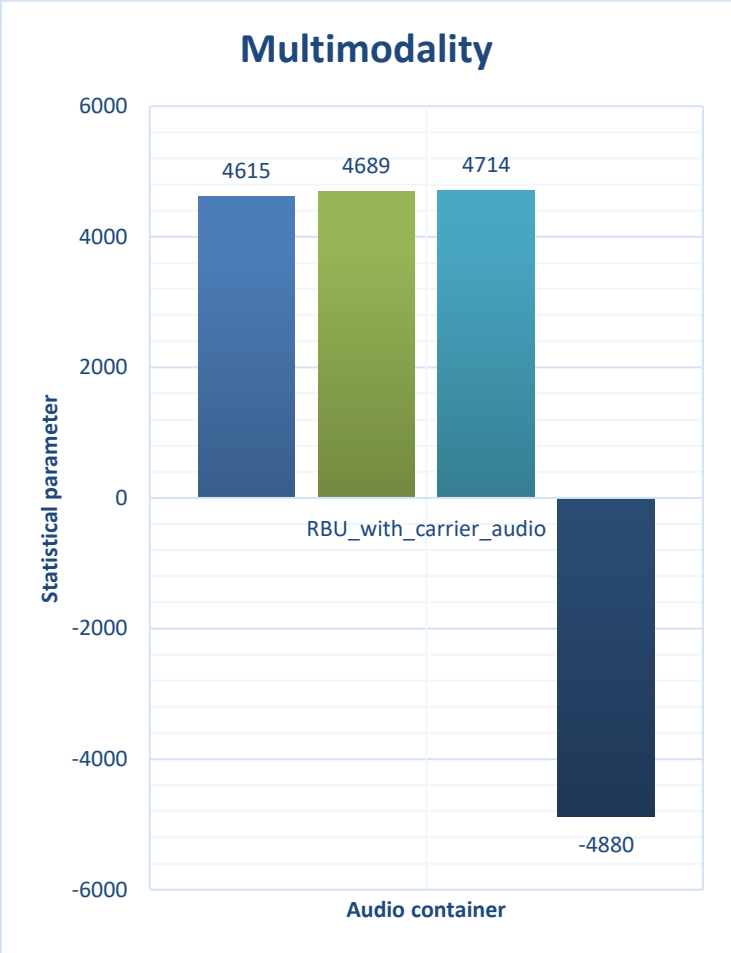


Рисунок 2.4 – Багатомодальність аудіосиигналу RBU_with_carrier_audio.wav

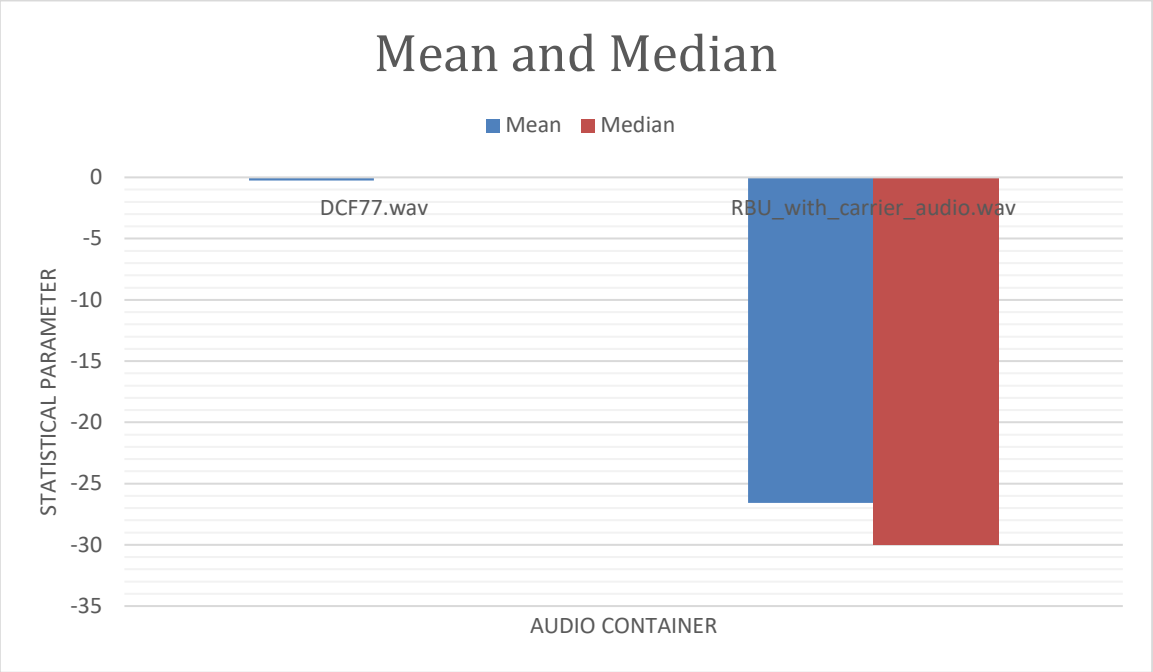


Рисунок 2.5 – Статистичні показники аудіопотоків

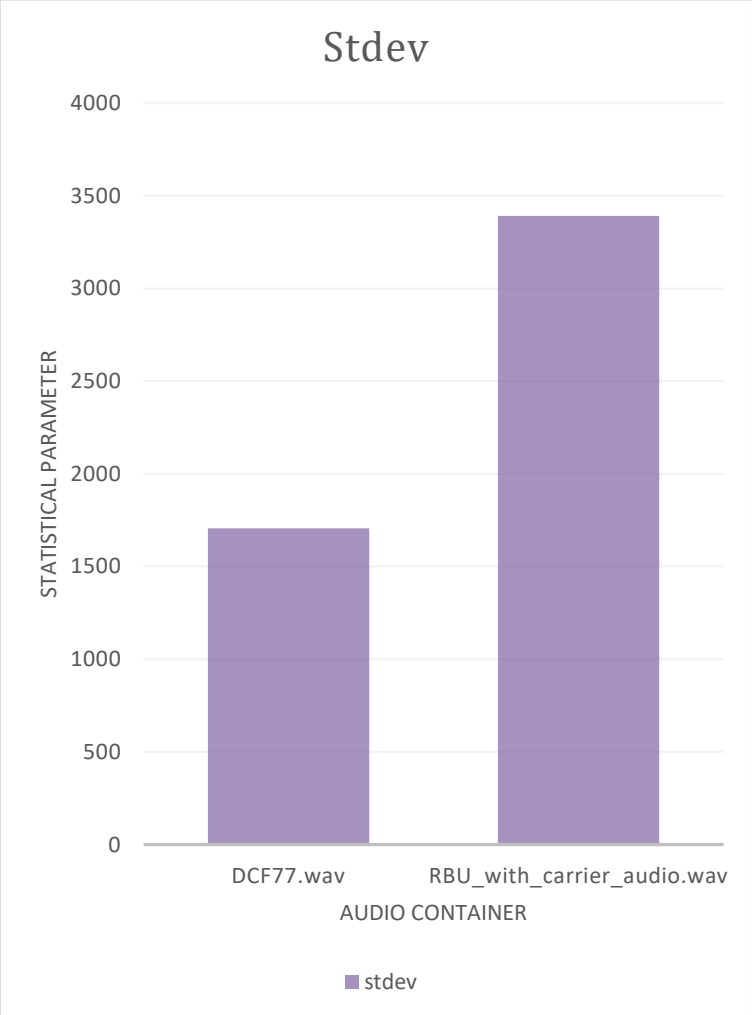


Рисунок 2.6 – Стандартне відхилення

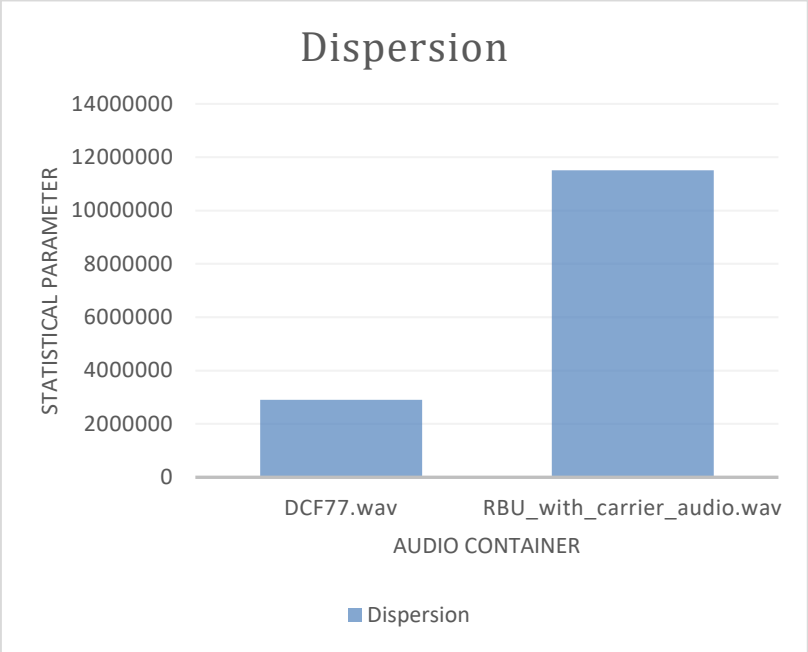


Рисунок 2.7 – Дисперсія аудіоконтейнерів

Графічне подання звукових контейнерів змодельоване у обчислювальному середовищі Mathcad зображено на рис. 2.8-2.9.

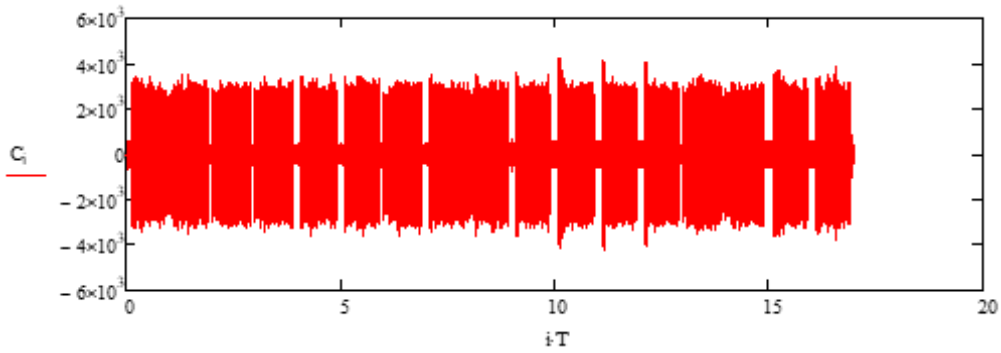


Рисунок 2.8 – Графічне представлення звукового файлу DCF77.wav

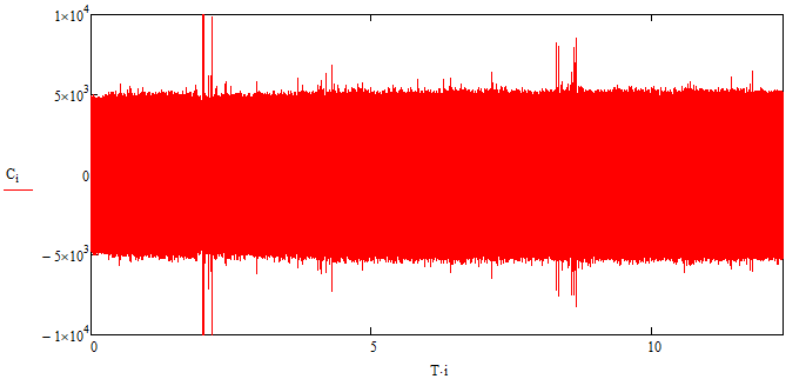
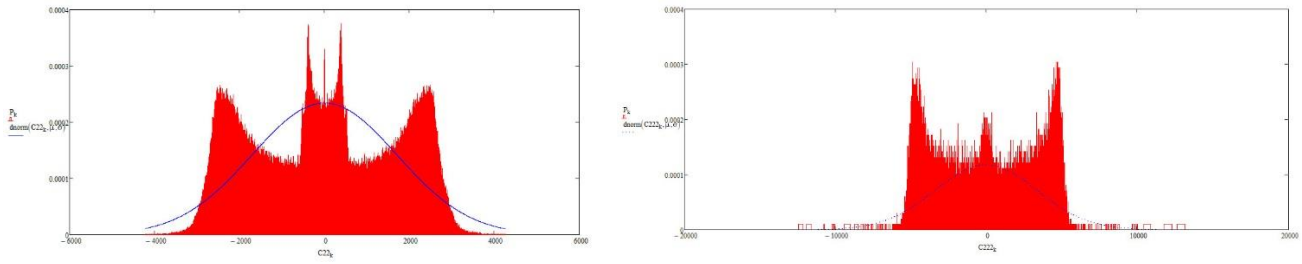


Рисунок 2.9 – Графічне представлення звукового файлу RBU_with_carrier_audio.wav

Дослідження статистичних властивостей включає побудову варіаційного ряду потокових носіїв. Побудова розподілу вказує як влаштовані дані у вибірці сигналу. Побудова гістограми (рис. 2.10 (а, б)) демонструє розподіл частот рівнів інтенсивності звуку в числовому наборі. Висота кожного стовпця показує, як часто значення вимірюваної величини потрапляють у відповідний інтервал. На основі конфігурації розподілу приймається рішення про варіант методу для виконання числових маніпуляцій.



а) *б)*

Рисунок 2.10 – Гістограми для числових вибірок інтенсивностей звуку (а) DCF77.wav та (б) RBU_with_carrier_audio.wav

Крім візуальних зіставлень існують математичні критерії для перевірки приналежності вихідного ряду до деякого розподілу. У математичній статистиці для об'єктивної перевірки критерію належності емпіричного розподілу до певного теоретичного закону використовуються спеціальні критерії згоди (або критерії узгодженості).

Аналіз сигналів включає дослідження частотного спектра сигналу (рис. 2.11). Частотні компоненти обчислюються за допомогою перетворення Фур’є (англ. Fourier Transform – FT). Відновлення часової функції реалізує математичний апарат оберненого перетворення Фур’є (англ. Inverse Fourier Transform – IFT). В повсякденному житті стикаються з дискретними у часі сигналами. Розрахунки частотних характеристик дискретних сигналів здійснюються через дискретне перетворення Фур’є (ДПФ). Перехід у частотну площину здійснює пряме дискретне перетворення Фур'є (ПДПФ) (рис. 2.12 (а)), зворотною процедурою є

зворотне дискретне перетворення Фур'є (ЗДПФ) (рис. 2.12 (б)) відповідно. Тривіальні моделі перетворень наведені на рис. 2.12.

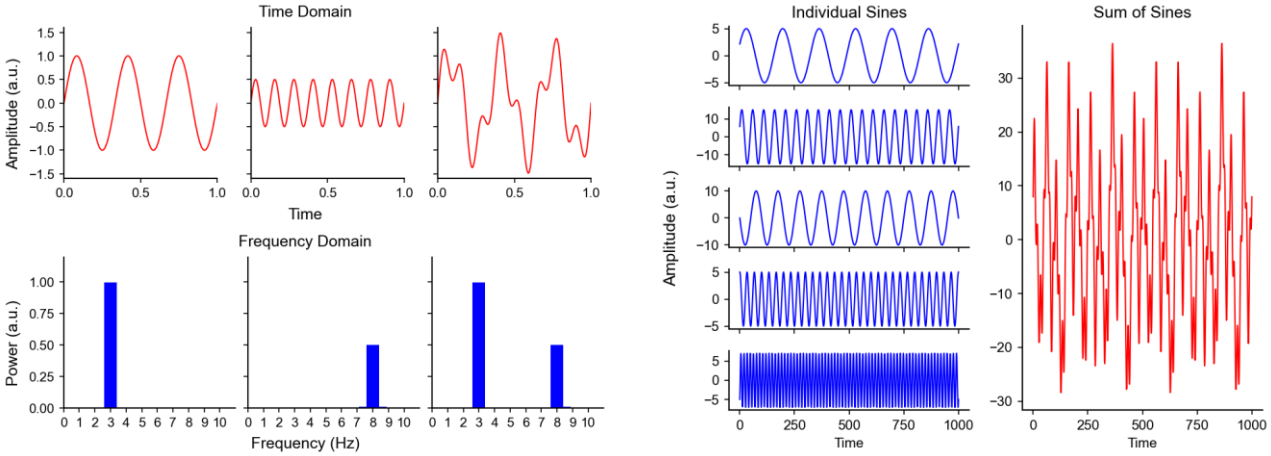
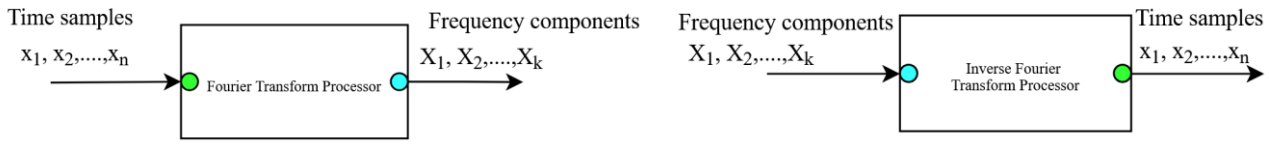


Рисунок 2.11 – Сутність частотного спектра сигналу



а) *б)*

Рисунок 2.12 – Модель ПДПФ (а) та ЗДПФ (б)

Швидке перетворення Фур'є (англ. Fast Fourier Transform – FFT) та обернене швидке перетворення Фур'є (англ. Inverse Fast Fourier Transform – IFFT) реалізують логіку стандартного FT, але за альтернативним алгоритмом. Ключові умови для застосування FFT та IFFT [9]:

1) Поточні аргументи є дійсні числа;

2) Вектор даних має довжину 2^m елементів.

Перша умова, що асоціюються із FFT/IFFT базується на теорії, що друга частина FFT є комплексно спряженою [9] до першої половини. Середовище Mathcad реалізує функції fft/ifft, що відкидають другу половину масиву-результату. Аналіз спектра покривних носіїв здійснювався через функцію cfft/icfft відповідно. Функції CFFT/ICFFT приймають вектори довільних довжин. З точки зору швидкодії розрахунок спектра краще обчислювати через FFT/IFFT. Але вектор дискретних значень сигналу повинен відповідати вимогам до розмірності даних [9]. Результат процедури комплекснозначний вектор синусоїдальних сигналів. Аналіз використаних функцій [9] наведений в табл. 2.3.

Таблиця 2.3 – Специфікація функцій FT

Функція	Характеристика
cfft (A)	Повертає дискретне перетворення Фур'є комплекснозначного вектора або матриці. Повертається масив аналогічний розмірності, того масиву, що використовуваний як аргумент.
icfft (A)	Повертається IFT вектору або матриці даних. Функція icfft – зворотна до функції cfft. По аналогії cfft, ця функція повертає масив того самого розміру, що і аргумент.

Математична конструкція ДПФ динамічно використовується в парадигмі ЦОС. Вищерозглянуті формули реалізують ідею ДПФ [2, 10, 11], що описується формулами для ПДПФ та ЗДПФ відповідно:

$$X_k = \sum_{n=0}^{N-1} x_n e^{-\frac{2\pi i}{N}kn} = \sum_{n=0}^{N-1} x_n \left[\cos\left(\frac{2\pi kn}{N}\right) - i \cdot \sin\left(\frac{2\pi kn}{N}\right) \right], k = 0,1,\ldots,N-1 \quad . \qquad (2.1)$$

$$x_n = \frac{1}{N}\sum_{k=0}^{N-1} X_k e^{\frac{2\pi i}{N}kn} = \frac{1}{N}\sum_{k=0}^{N-1} X_k \left[\cos\left(\frac{2\pi kn}{N}\right) + i \cdot \sin\left(\frac{2\pi kn}{N}\right) \right], n = 0,1\ldots,N-1 \quad , \qquad (2.2)$$

де N – кількість відліків, виміряних за період часу T, також кількість вхідних компонент розкладу;

$x_n = x(t_n), n = 0,1,\ldots,N-1$ – виміряні значення сигналу в дискретних точках часу $t_n = \frac{n}{N}T$; набір значень потоку в дискретні моменти часу є вектором входу для ПДПФ та вихідним для ЗДПФ;

$X_k, k = 0,1,\ldots,N-1$ – N комплексні амплітуди синусоїдальних сигналів:

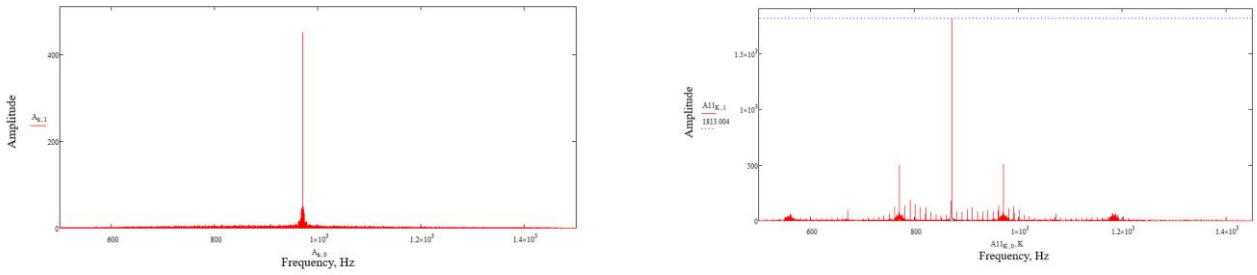
$$X_k = \mathrm{Re}(X_k) + i\,\mathrm{Im}(X_k),$$

які є частотними компонентами спектра або набором синусоїд, що в сумі утворюють вихідний сигнал. Комплексні амплітуди містять дані для отримання атрибутів спектральних елементів: початкової фази φ_k, амплітуди A_k та частоти f_k для k-тої синусоїди спектра. Кратність N – довжини спектра сигналу [10], впливає на арифметику виділення множин додатних та від’ємних частот:

$$X_k = \left[\underbrace{X_0, X_1, X_2, \ldots, X_{\frac{N-1}{2}}}_{Positive\ Frequency\ Terms}, \underbrace{X_{\frac{N+1}{2}}, \ldots, X_{N-1}}_{Negative\ Frequency\ Terms} \right], \mathrm{mod}(N,2) \neq 0$$

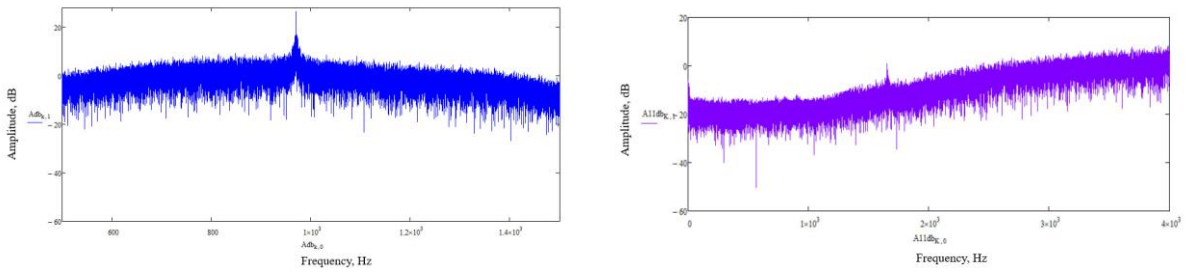
$$X_k = \left[\underbrace{X_0, X_1, X_2, \ldots, X_{\frac{N}{2}}}_{Positive\ Frequency\ Terms}, \underbrace{X_{\frac{N}{2}+1}, \ldots, X_{N-1}}_{Negative\ Frequency\ Terms} \right], \mathrm{mod}(N,2) = 0 \quad . \qquad (2.3)$$

Проведено аналіз частотних складових звукових сигналів, застосовуючи інструментарій ДПФ та спектрального аналізу. На рис. 2.13-2.15 наведені основні спектральні характеристики (амплітудна (2.13-2.14 (а,б)) та фазова (рис. 2.15 (а,б))) аналізованих сигналів. Спектральний аналіз відображає розподіл енергії за частотами. Лише перша половина $\frac{n}{2}+1$ вектора частот є унікальними атрибутами спектра вихідного сигналу, інша дзеркальне відображення першого. Спектр показує із яких гармонічних складових складається складний сигнал. Комплексування елементів спектра дозволяє відновити складний сигнал.



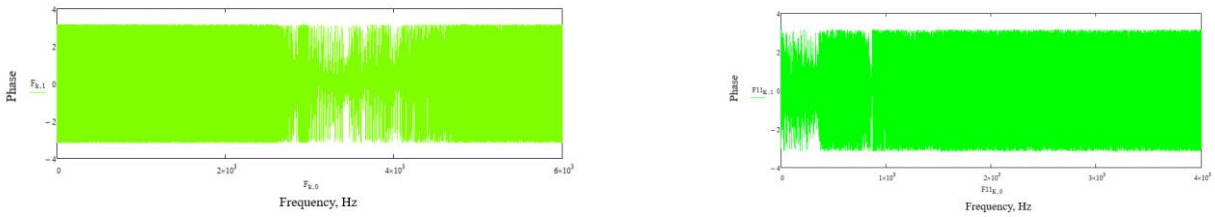
а) *б)*

Рисунок 2.13 – Амплітудно-частотна характеристика (а) DCF77.wav та (б) RBU_with_carrier_audio.wav акустичних носіїв



а) *б)*

Рисунок 2.14 – Амплітудно-частотна характеристика виражена в децибелах (дБ) для (а) DCF77.wav та (б) RBU_with_carrier_audio.wav акустичних носіїв



а) *б)*

Рисунок 2.15 – Фазово-частотна характеристика (а) DCF77.wav та (б) RBU_with_carrier_audio.wav акустичних носіїв

Сигнал [10], що складається із N точок дозволяє отримати спектр потужності лише з $\frac{N}{2}+1$ точками. Перша точка [10] – це нульова частота (постійна) складова, що відповідає постійному струму (англ. Direct Current – DC) складовій сигналу. Друга точка [11] відповідає частоті $\frac{1}{N\Delta T}$ (період якої точно дорівнює тривалості даних), наступна точка – $\frac{2}{N\Delta T}$, наступна точка – $\frac{3}{N\Delta T}$ тощо, де ΔT – це інтервал між сусідніми значеннями часової осі T, а N – загальна кількість точок. Остання точка (з найвищою частотою) у спектрі потужності $\frac{\left(\frac{N}{2}\right)}{N\Delta T}=\frac{1}{2\Delta T}$, що становить половину частоти дискретизації. Згідно з теоремою відліків Віттекера-Найквіста-Котельникова-Шеннона максимальна частота, що може бути представлена в спектрі дискретного сигналу дорівнює половині частоти дискретизації $f_Д$. Така частота отримала назву частоти Найквіста. Частоти вище частоти Найквіста [3, 11] складаються назад до нижчих частот, що сильно спотворює сигнал. Роздільна здатність за частотою, тобто різниця між частотами сусідніх точок у розрахованому частотному спектрі [10, 11], є просто оберненою величиною тривалості сигналу. Спектр потужності – це оптимальний варіант для демонстрації сукупної

потужності, зосередженої на *k*-тій частоті для синусоїдних та косинусоїдних складових сигналу.

Спектр сигналу дозволяє побачити частоти в межах частоти Найквіста включно. Оскільки теорема відліків забороняє частоти вище допустимої частоти спектра. В табл. 2.4 та 2.5 наводяться основні характеристики досліджені в границях спектрального аналізу сигналів звуку.

Таблиця 2.4 – Атрибути спектрів акустичних сигналів

Звуковий потік	Потужність DC, Вт	Базова частота, Hz	Ширина смуги частот, Hz	Роздільна здатність за частотою, Hz	Період дискретизації, сек
DCF77.wav	0,2631	0,016	11999,992	0,016	0,000042
RBU_with_carrier_audio.wav	26,586	0,081	3999,959	0,081	0,000125

Таблиця 2.5 – Характеристики спектра сигналів

Акустичний носій	Тривалість сигналу, сек.	Максимальна потужність спектру, Вт	Частоти макс. потужності, Hz	Частота Найквіста, Hz	Максимальна фаза
DCF77.wav	62,851	450,499	970,332 23029,668	12000	3,142
RBU_with_carrier_audio.wav	12,334	1813,004	871,143 1399,031	4000	3,142

В таблицях вище наведені основні характеристики спектра для дослідження структури та природи сигналу. Спектральний аналіз – це потужний інструмент для оцінки розподілу енергії складного сигналу по частотним елементам.

2.2 Сутність методу розширення спектра

Основна ідея методу розширення спектра [5, 12, 13] розчинити інформаційний сигнал по частотному спектру сигналу-переносника, максимально як це допустимо. Сучасні системи передачі інформації навпаки, реалізують політику концентрації інформації у вузькій смузі частот і зменшення потужності сигналу [3, 5]. Перевага методу розширення спектра полягає в тому, що інформація розмивається (рис. 2.4) по кодованих псевдовипадкових послідовностях (ПВП). На основі властивостей ПВП, кореляційних зв’язків та структури кодів можливо вилучити дані навіть в умовах шумових завад. Сутність способу [13-18] полягає в

розширенні бітового алфавіту в довгу ПВП. Діапазон частот для передавання сигналів збільшується пропорційно до довжини послідовності розширень [13]. Перспективним вектором розширення спектра є метод розширення спектра методом прямої послідовності (англ. Direct Sequence Spread Spectrum – DSSS). Теорема Шеннона-Гартлі (2.4) є фундаментальним співвідношенням [13-15], що накладає обмеження на можливу пропускну здатність. З обмеженою частотною смугою та потужністю адитивного Ґауссівського шуму [13].

$$C = \Delta F \log_2\left(1 + \frac{P_S}{P_N}\right), \tag{2.4}$$

де С – пропускна здатність, біт/с;

ΔF – частотна смуга, Hz;

P_S – бажана потужність сигналу;

P_N – потужність білого адитивного Ґауссівського шуму;

$\frac{P_S}{P_N}$ – співвідношення сигнал/шум (SNR).

Математичний вираз (2.4) демонструє, що при обмеженій SNR можливо збільшити пропускну здатність КЗ через розширення частотної смуги. Сутність DSSS реалізує дане завдання. Технологія розширення спектра реалізує високошвидкісний канал передачі інформації [13] із високою ефективністю.

Розглянемо принцип високошвидкісного комунікаційного КЗ через принцип DSSS. Визначимо $s = (s_1, s_2, \ldots, s_k)$ бітові ПВП (вектори):

$$\begin{aligned} s_1 &= (s_{1,0}, s_{1,1}, \ldots, s_{1,n-1}), \\ s_2 &= (s_{2,0}, s_{2,1}, \ldots, s_{2,n-1}), \\ &\ldots, \\ s_k &= (s_{k,0}, s_{k,1}, \ldots, s_{k,n-1}), \end{aligned}$$

Які представлені у полярній конфігурації,

$$\forall i, j : s_{i,j} = \begin{cases} 1, \\ -1. \end{cases}$$

Вектори, що породжені для розширення спектра [13] вихідного повідомлення та визначаються як чіп-коди. Кожний компонент $s_{i,j}$ називається [13-15] елементом послідовності чи чіпом.

Формуються чіпові коди таким чином, щоб їх взаємно-кореляційна міра була несуттєва та наближалася до нуля:

$$\forall i \neq j : \rho\left(s_i, s_j\right) = \sum_{v=0}^{n-1} s_{i,v} s_{j,v} \approx 0 \qquad (2.5)$$

В якості прикладу можливо розглянути ансамблі сигналів (АС), що формуються перетворенням матриць Уолша-Адамара. Вони взаємно ортогональні, що представляють випадкові чіпи для модуляції інформаційних сигналів.

$$\forall i \neq j : \rho\left(s_i, s_j\right) = 0$$

Існує безліч методів для генерації ПВП при модуляції сигналів, можливо реалізувати випадкову генерацію значень послідовностей у діапазоні [-1,1]. При цьому необхідне виконання алгебраїчного правила (2.5).

Нехай є деяке інформаційне повідомлення [10, 13], що складає бінарний алфавіт k бітів $m_1, m_2, \ldots, m_k$, необхідно переписати біти повідомлення m_i, $i=1,2,\ldots,k$ у полярній формі:

$$\forall i : m_i = \begin{cases} 1, \\ -1. \end{cases}$$

Процедура модуляції бітів інформаційного вектору m_i, $i=1,2,\ldots,k$ досягається різними способами. Можливим варіантом є відношення із полярними позначенням за математичним співвідношенням:

$$\forall i : M_i = m_i s_i = \left(m_i s_{i,0}, m_i s_{i,1}, \cdots, m_i s_{i,n-1}\right) \qquad (2.6)$$

Замість одиничного двійкового елементу m_i передається послідовність M_i бінарних елементів по КЗ. Завдяки техніці розширення спектра [12] за допомогою АС вихідний інформаційний сигнал поширюється по коду. Частота кодованої послідовності розраховується як

$$F_{chip} = \frac{1}{T_{chip}} = \frac{n}{T} Hertz. \qquad (2.7)$$

У (2.7) частота в n разів більша [13-18] за частоту інформаційних бітів $F = \frac{1}{T}$. В результаті перетворень (2.6) підвищується частота [13,15] інформаційного потоку (рис. 2.16) на n разів.

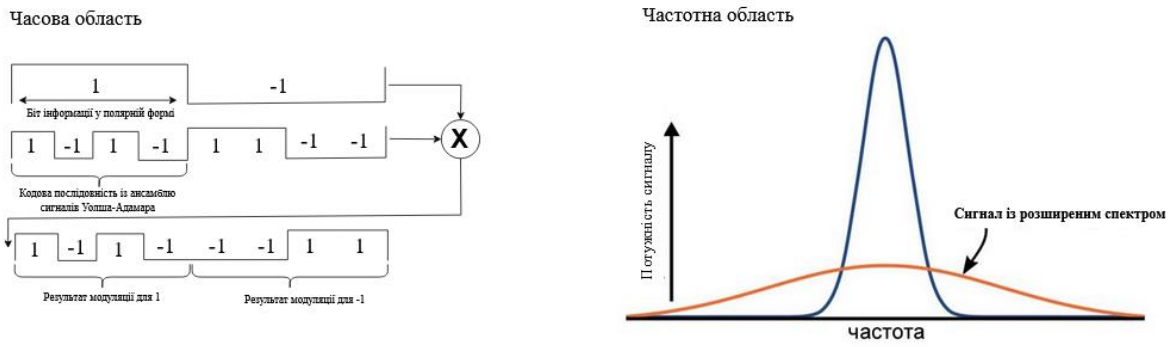


Рисунок 2.16 – Принцип розширення спектра на основі DSSS

А інформаційний сигнал розсіюється [3] по спектру кодованої послідовності. Ускладнюється знищення посилки відомостей за рахунок розгортання даних по спектральній площині.

Набір бітів може бути одночасно транспортований [15] по каналу передачі, через додавання інформаційної суміші у вихідний потік переносника:

$$Mix = N + \sum_{i=1}^{k} M_i \,, \tag{2.8}$$

де N – послідовність символів випадкових елементів, що виражає елемент природного шуму.

За сценарієм приймачу відомі кодові слова – чіп-коди $s_1, s_2, \ldots, s_k \in s$. Процедура відновлення [13, 15] інформації передбачає розрахунок показника кореляції між отриманою версією сигналу та відповідного чіпу. В якості прикладу, для відновлення значення m_i в (2.6) обчислювальний блок розраховує $\rho(s_i, Mix)$. Математичний вираз (2.5) має лінійний характер, що описується як [13]:

$$\rho(s_i, Mix) = \rho(s_i, N) + \rho\left(s_i, \sum_{j=1}^{k} M_j\right) \tag{2.9}$$

Для випадкового шуму N рівень кореляційної метрики відповідає:

$$\rho(s_i, N) \approx 0 \tag{2.10}$$

Якщо, $\forall i \neq j : \rho(s_i, s_j) \approx 0$, тоді,

$$\rho(s_i, Mix) \approx \sum_{j} \rho(s_i, m_j s_j) \approx \rho(s_i, m_i s_i) \tag{2.11}$$

Виходячи з наведеного, складається математична модель для прийняття рішення про отриманий біт:

$$m_i = \rho(s_i, Mix) = \begin{cases} -1, \ \rho(s_i, Mix) < 0 \\ +1, \ \rho(s_i, Mix) > 0 \end{cases} \quad (2.12)$$

Реалізація розширення спектра створює багатоканальну модель для передачі сукупності повідомлень. Реалізується множинний доступ із кодовим поділом [10, 15].

Теорія розширення спектра застосована до функцій приховування інформації. Дослідники по стеганографії [13, 21] пропонують методологію вбудування для просторої області нерухомих зображень. Принцип можливо реалізувати для широкого ряду мультимедійних контейнерів. На прикладі, аудіосигналу, що містить вбудований ЦВЗн або інформаційний потік. Концептуальна модель приховування [13-15] наведена на рис. 2.17.

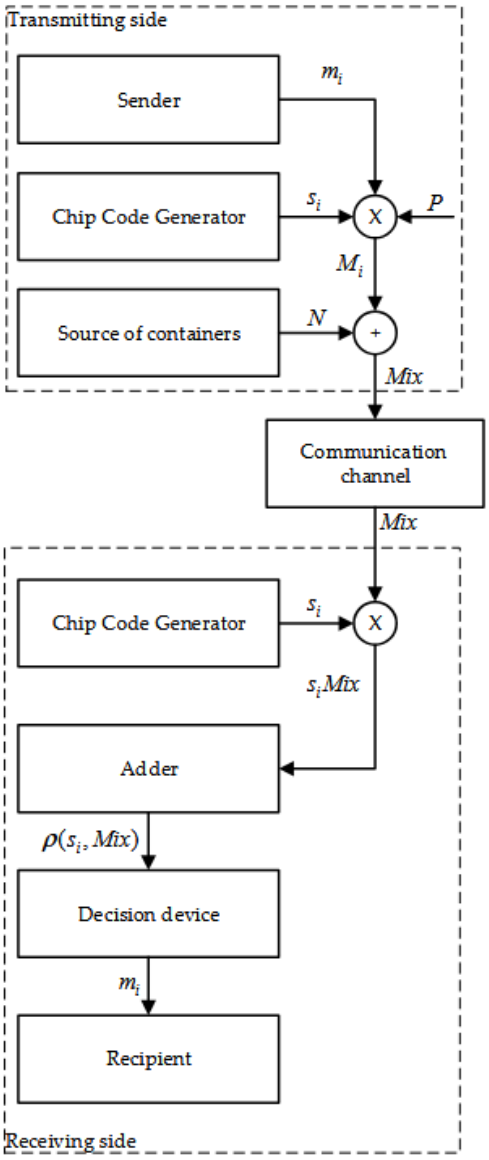


Рисунок 2.17 – Узагальнена модель приховування та вилучення

Монтування інформації здійснюється через модифікації звучності сигналу. Базується алгоритм [2] на 1-й властивості ССЛ – слабка чутливість ССЛ до незначної зміни гучності аудіосигналу. Алгоритм приховування цифрових артефактів включає такі кроки [13]:

1) Представлення бітів двійкового алфавіту в полярній формі m_i;

2) m_i побітово перемножується на кодовий чіп як у співвідношенні (2.6);

3) Мультимедійні об'єкти (графічні зображення, відеофрагменти, аудіосигнали тощо) класифікуються як шум в КЗ. Позначення потоку шуму в (2.8) як N.

4) Внесення даних здійснюється за виразом (2.8). Мають місце наступні визначення [13]: N – контейнер (файл-оболонка) куди приховуються інформаційні відомості; Mix – заповнений контейнер (модифікована версія) після здійснення вбудування даних.

Вилучення інформації передбачає здійснення наступних операцій:

1) Розрахунок показника кореляції.

– розрахунок суміші $s_i Mix$;

– обчислення суми $\rho(s_i, Mix) = \sum_{v=0}^{n-1} s_{i,v} Mix_v$.

2) У випадку виконання рівностей (2.10) та (2.11), контекст відповідного біту інформації відновлюється за допомогою рівняння (2.12);

3) Отриманий масив даних конвертується у зрозумілий формат.

Розглянутий метод має один дефект [13], що проявляється у високому рівні помилок. Стоїть завдання у зниженні показника BER (Bit Error Rate). Варіанти рішення стосуються застосування завадостійкого кодування або методів фільтрації [2, 13]. Найпростішим варіантом є збільшення потужності кодових послідовностей. З урахуванням наведених фактів, формула (2.8) набуває наступної конфігурації:

$$Mix = N + P\sum_{j=1}^{k} M_j = N + \sum_{j=1}^{k} m_j (Ps_j), \qquad (2.13)$$

де P – коефіцієнт підсилення потужності кодових послідовностей $s_j = (s_{j,0}, s_{j,1}, \ldots, s_{j,n-1})$.

Застосування прийому підсилення потужності кодового сигналу позитивно впливає на зниження динаміки BER (частоти бітових помилок). Але значний показник *P* вносить суттєві спотворення в аудіопотік *N*. Тому величина *P* повинна встановлюватись [14] під слуховий поріг ССЛ для збереження таємності факту існування посилки. Важливим аспектом є балансування між величиною помилок та рівнем внесених спотворень.

2.3 Оцінка та дослідження параметрів безпеки способу

Стеганографічна система на основі розширення спектра є закритою системою із експлуатацією секретного ключа. Відсутність секретного ключа [2] унеможливлює компрометацію контенту та доведення факту його присутності. Стійкість системи стеганографії базується на структурі секретного ключа. У технології для зашифрування та розшифрування інформації [3, 6] – використовується симетричний ключ. Псевдовипадковий шум [5], що має сталу характеристику спектра в усій частотній смузі в ідеальному сценарії. Стійкість системи приховування заснована на ПВП, оскільки прихована інформація модулюється кодовою послідовністю. Захист інформації з обмеженим доступом (ІзОД) потребує високої стійкості ключових елементів. Досягнення високих показників стійкості для ЦВЗн або ІзОД є головним завдання ключової стеганографії. Варіантом методології формування ключів для методу розширення спектра є АС на основі матриці Уолша-Адамара [2, 3, 13]:

$$H_{2^w} = \begin{bmatrix} H_{2^{w-1}} & H_{2^{w-1}} \\ H_{2^{w-1}} & -H_{2^{w-1}} \end{bmatrix}, \quad H_1 = [1]. \tag{2.14}$$

Дискретні АС формуються із довжиною $n = 2^w$, w=1,2,…, які є згенерованими компонентами стовпців та рядків матриці H_n за формулою (2.14) порядку $n = 2^w$. АС Уолша-Адамара формується [11] як модель із ортогональними властивостями:

$$\forall i \neq j : \rho(s_i, s_j) = 0,$$

що відповідає відношенню (2.5). Стеганосистема працює як технічна модель захисту інформації через реалізацію сценарію приховування. Оцінка

стеганосистеми реалізується через показники ефективності та метрики якості [2, 13, 16]:

1) Пропускна спроможність – відношення обсягу V вмонтованої в об'єкт інформації до загального об'єму контейнера D:

$$Q = \frac{V}{D}. \tag{2.15}$$

2) Об'єм ключових даних (у бітах):

$$l_{KEY} = \log_2 |KEY|, \tag{2.16}$$

де $|KEY|$ – потужність множини ключових даних.

3) Ймовірнісний показник підбору секретного ключа:

$$W = \frac{1}{|KEY|} = 2^{-l_{KEY}} \tag{2.17}$$

4) Ентропія джерела H описується наступним співвідношенням [19]:

$$H(K) = -\sum_{i=1}^{K} p(K_i) \log_2 p(K_i), \tag{2.18}$$

де $p(K_i)$ – ймовірність вгадування деякого секретного ключа.

Якщо $p(K_i) = \frac{1}{K}$ для всіх K_i, то вираз ентропії перетворюється до вигляду:

$$H(K) = -\sum_{i=1}^{K} \frac{1}{K} \log_2 \frac{1}{K}. \tag{2.19}$$

Математичне рівняння (2.17) збігається із формулою Шеннона для рівномірного розподілу [19], де всі аргументи випадкової величини містять однакові величини ймовірності. Із наведених тверджень, можна перетворити вираз на спрощену форму:

$$H(K) = -\sum_{i=1}^{K} \frac{1}{K} \log_2 \frac{1}{K} = -K * \frac{1}{K} * \log_2 \frac{1}{K} = -\log_2 \frac{1}{K} = \log_2 K. \tag{2.20}$$

5) Bit Error Rate, BER

$$BER = \frac{k_{error}}{k}, \tag{2.21}$$

де k_{error} – це кількість помилково відновлених біт;

k – загальна кількість біт в інформаційному повідомленні.

6) MSE – величина, за допомогою якої оцінюється рівень спотворення контейнеру [13-18], що відповідає усередненому квадрату різниці між оригінальною інтенсивністю сигналу та звучністю отриманої після модифікації оболонки сигналу.

$$MSE = \frac{1}{n}\sum_{i=0}^{n-1}\left[Mix_i - N_i\right]^2 \tag{2.22}$$

7) Пікове співвідношення сигнал/шум (англ. Peak signal-to-noise ratio), PSNR:

$$PSNR = 10\log_{10}\left(\frac{N_{\max}^2}{MSE}\right) = 20\log_{10}\left(\frac{N_{\max}}{\sqrt{MSE}}\right) = \\ = 20\log_{10}\left(N_{\max}\right) - 10\log_{10}\left(MSE\right), \tag{2.23}$$

де $N_{\max}$ – максимальне можливе значення у вихідному потоці N.

Оскільки кодування часових відліків [13, 16] дискретизованого аудіосигналу відбувається двома байтами на один часовий семпл. Максимальне значення в аудіосигналі може приймати $N_{\max}=2^B-1$. В рамках експериментальних досліджень $B=15$, оскільки один найстарший біт виділяється для кодування знаку інтенсивності напруги звуку, тому $N_{\max}=2^{15}-1=32767$.

Множиною ключових даних для АС Адамара вважається множина варіативних (неізоморфних) матриць Адамара [20, 21], кожна з яких налаштовує ансамбль дискретних сигналів. В табл. 2.6 наведені оцінки [20-23] потужності M_A даної множини.

Таблиця 2.6 – Число ансамблів дискретних сигналів Уолша-Адамара

Порядок матриці n	Потужність ключової множини M_A
24	4
40	5
64	19
100	1
256	54
512	102
1024	162
1032	4
1088	4
1500	4
2000	9
4000	16
9000	12

Графічне подання виділених результатів представлено у вигляді залежності на рис. 2.18-2.19. Обчислені оцінки для емпіричних даних (табл. 2.7) потужності ключів параметрів безпеки системи приховування на основі АС Адамара-Уолша. Результати дослідження ключових механізмів у координатній площині проілюстровані на рис. 2.19. Потужність ключової множини [20-22] для різних просторів АС Адамара-Уолша визначається його розмірністю n. Вибір розмірності n для ортогональних векторів залежить від ймовірності підбору секретного ключа. Оптимальним є варіантом при ймовірності вгадування W, що наближається до нуля. Для забезпечення надійності системи від впливу потенційних зловмисників.

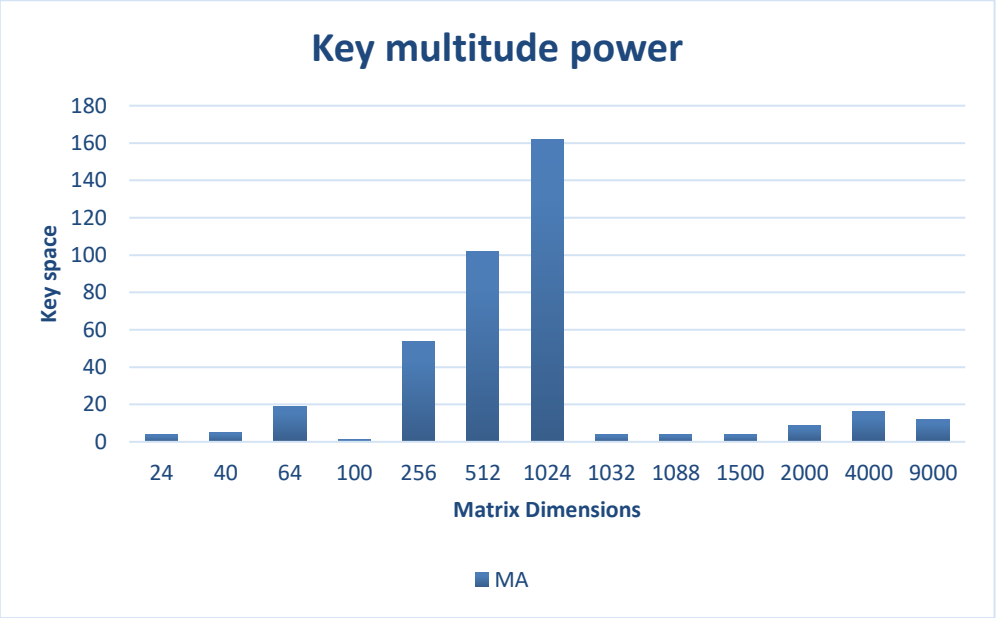


Рисунок 2.18 – Потужність множини ключів

Таблиця 2.7 – Характеристики ключів

n	Об’єм ключових даних, l_{KEY}	Ймовірнісний показник підбору секретного ключа, W	Ентропія H джерела підбору	Ентропія H джерела підбору, $\log_2 K$
24	2	0,25	2	2
40	2,321928095	0,2	2,321928095	2,321928095
64	4,247927513	0,052631579	4,247927513	4,247927513
100	0	1	0	0
256	5,754887502	0,018518519	5,754887502	5,754887502
512	6,672425342	0,009803922	6,672425342	6,672425342
1024	7,339850003	0,00617284	7,339850003	7,339850003
1032	2	0,25	2	2
1088	2	0,25	2	2
1500	2	0,25	2	2
2000	3,169925001	0,111111111	3,169925001	3,169925001

Продовження таблиці 2.7

4000	4	0,0625	4	4
9000	3,584962501	0,083333333	3,584962501	3,584962501
Сумарна ймовірність для будь-якого простору ключів		$\sum_{i=1}^{m} p_i(n)=1$		

Порядок матриці Адамара *n* впливає на кількість елементів множини ключів. У сенсі теорії інформації, криптографії та захисту даних наближення ймовірності вгадування (*W*) деякого ключа k_i до нуля означає досягнення максимальної невизначеності для зловмисника, що є еквівалентом максимальної надійності системи. З отриманих результатів можна спостерігати ефект зростання ентропії (рис. 2.20) на фоні спадання ймовірності вгадування *W*. Це означає, що для злому такої системи потрібно виконати нескінченно велику кількість обчислень. Абсолютна стійкість механізму згідно з теореми Шеннона забезпечується при виконанні ряду вимог. Однією з важливих – рівноймовірний (рівномірний) розподіл ймовірностей. Ймовірність підбору для кожного ключа дорівнює $\frac{1}{|K|}$.

Сумарна ймовірність для кожної ключової групи відповідає одиниці.

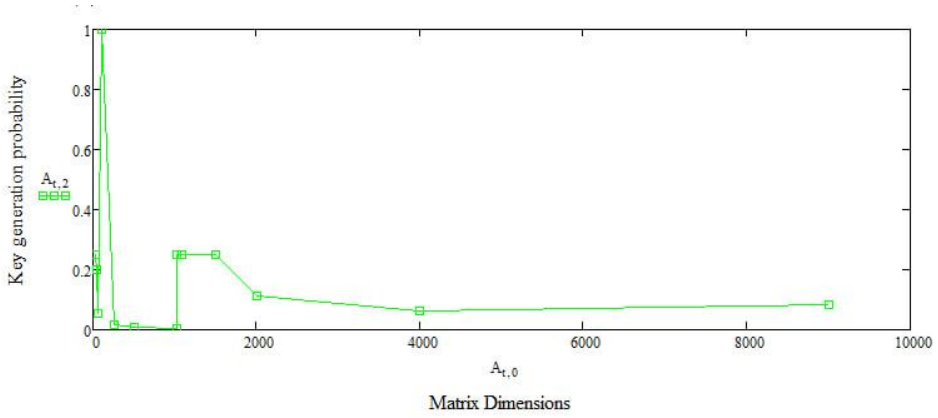
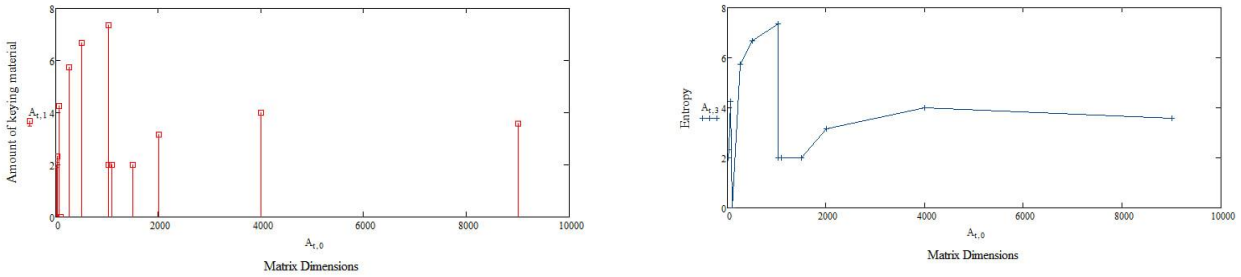


Рисунок 2.19 – Результати оцінки ймовірності генерації ключа



а) *б)*

Рисунок 2.20 – Оцінка об'єму ключової множини та ентропії

На рис. 2.21 наведені ортогональні дискретні сигнали, які використовувалися для досліджень методу розширення спектра. Базиси створені на основі формули (2.14). Розрахунки коефіцієнту кореляції та графічне подання представлені на рис. 2.22-2.23 (а,б).

Keys

$ArrayFunction_1^T$ =

	0	1	2	3	4	5	6	7	8	9
0	1	-1	1	-1	1	-1	1	-1	1	...

$ArrayFunction_2^T$ =

	0	1	2	3	4	5	6	7	8	9
0	1	1	-1	-1	1	1	-1	-1	1	...

$ArrayFunction_3^T$ =

	0	1	2	3	4	5	6	7	8	9
0	1	-1	-1	1	1	-1	-1	1	1	...

$ArrayFunction_4^T$ =

	0	1	2	3	4	5	6	7	8	9
0	1	1	1	1	-1	-1	-1	-1	1	...

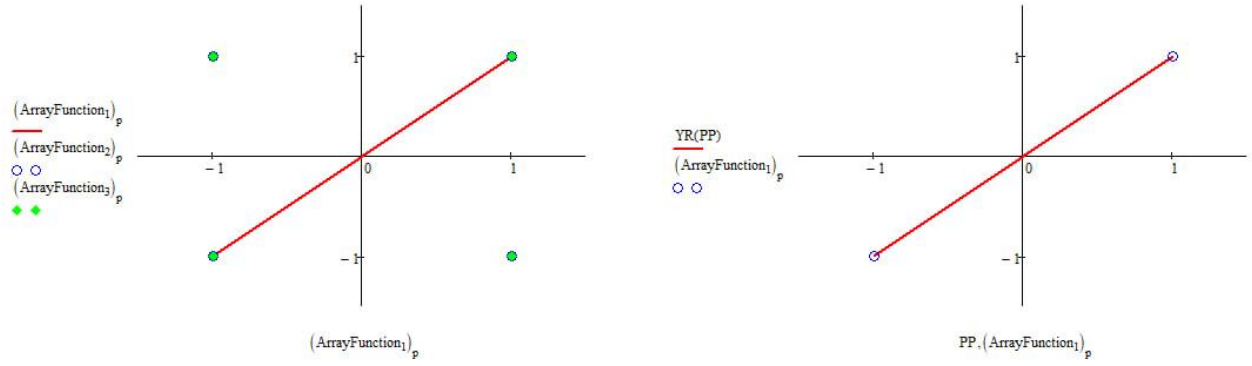
H_{10} =

	0	1	2	3	4	5	6	7	8	9
0	1	1	1	1	1	1	1	1	1	1
1	1	-1	1	-1	1	-1	1	-1	1	-1
2	1	1	-1	-1	1	1	-1	-1	1	1
3	1	-1	-1	1	1	-1	-1	1	1	-1
4	1	1	1	1	-1	-1	-1	-1	1	1
5	1	-1	1	-1	-1	1	-1	1	1	-1
6	1	1	-1	-1	-1	-1	1	1	1	1
7	1	-1	-1	1	-1	1	1	-1	1	-1
8	1	1	1	1	1	1	1	1	-1	-1
9	1	-1	1	-1	1	-1	1	-1	-1	1
10	1	1	-1	-1	1	1	-1	-1	-1	-1
11	1	-1	-1	1	1	-1	-1	1	-1	1
12	1	1	1	1	-1	-1	-1	-1	-1	-1
13	1	-1	1	-1	-1	1	-1	1	-1	1
14	1	1	-1	-1	-1	-1	1	1	-1	-1
15	1	-1	-1	1	-1	1	1	-1	-1	...

Рисунок 2.21 – Сигнали Уолша-Адамара

$$ArrayFunction_1 \cdot ArrayFunction_2 = 0$$
$$ArrayFunction_1 \cdot ArrayFunction_3 = 0$$
$$ArrayFunction_2 \cdot ArrayFunction_3 = 0$$
$$ArrayFunction_1 \cdot ArrayFunction_1 = 1024$$
$$ArrayFunction_2 \cdot ArrayFunction_2 = 1024$$
$$ArrayFunction_3 \cdot ArrayFunction_3 = 1024$$

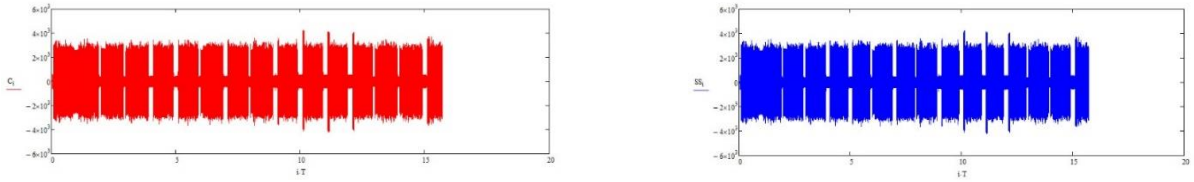
Рисунок 2.22 – Кореляційні властивості АС



а) *б)*

Рисунок 2.23 – Ілюстрація кореляційних зв’язків

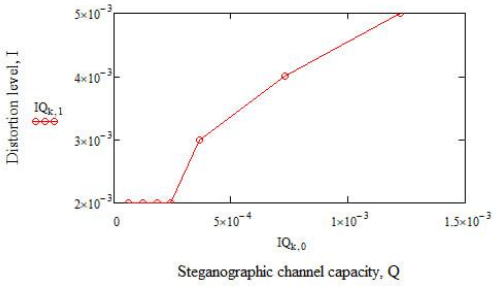
Після вбудування даних методом розширення спектра (рис. 2.24, *G*=1, *k*=4, АС Адамара Уолша – секретні ключі) модифікований варіант по зоровому та слуховому співставленні не відрізняється від оригіналу.



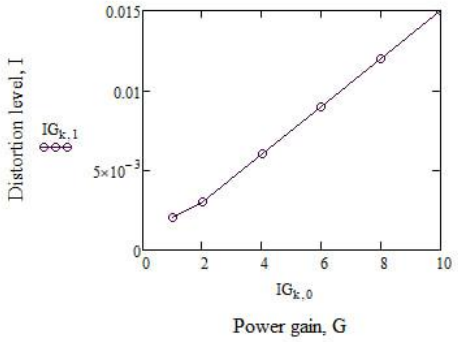
а *б*

Рисунок 2.24 – Приховування ЦВЗн (а) оригінал (б) стеганограма

Емпіричні дані досліджень методу розширення спектра (додаток В) із застосуванням ансамблів Уолша-Адамара подані на рис. 2.25 (а, б).



а)



б)

Рисунок 2.25 – Графіки емпіричних даних досліджень (а) *I*(*Q*) (б) *I*(*G*)

В табл. 2.8 наведені оцінки пропускної спроможності стегаканалу *Q*. Фіксуються показники пропускної здатності при варіаційних значеннях *k* – кількості біт на один сегмент та *n* – довжина сегменту аудіовибірки.

Таблиця 2.8 – Дані пропускної здатності

Потоковий файл	Потужність вибірки звуку	*n*, біти	*k*	*G*	*Q*
DCF77.wav	1508415	1024	1	1	0,000976563
			2		0,001953125
			3		0,002929688
			4		0,00390625
			6		0,005859375
			12		0,01171875
			20		0,01953125
		4080	1		0,000245098
			2		0,000490196
			3		0,000735294
			4		0,000980392
			6		0,001470588
			12		0,002941176
			20		0,004901961

Продовження таблиці 2.8

		16384	1		0,000061
			2		0,0001221
			3		0,0001831
			4		0,0002441
			6		0,0003662
			12		0,0007324
			20		0,0012207
		32768	1		$3{,}05176 \cdot 10^{-5}$
			2		$6{,}10352 \cdot 10^{-5}$
			3		$9{,}15527 \cdot 10^{-5}$
			4		0,00012207
			6		0,000183105
			12		0,000366211
			20		0,000610352

Пропускна спроможність стегаканалу Q визначається [15] об’ємом бітів блоку n та кількістю вбудованих даних двійкового алфавіту k в сегмент n.

2.4 Порівняльний аналіз методів

Парадигма приховування даних в акустичні канали підтримує широкий ряд алгоритмів. Ці способи орієнтовані на експлуатацію властивостей ССЛ для реалізації непомітного приховування. Методи приховування використовують різні області цифрового потоку для реалізації запису даних. В табл. 2.9 наведені порівняння властивостей поширених методів [24] звукового приховування.

Таблиця 2.9 – Теоретичні основи методів звукового приховування

Назва способу	Концептуальна основа	Переваги	Недоліки
Методи кодування із розширенням спектра	Ґрунтується на розмитті вузькосмугового сигналу по ширшій частотній полосі, імітуючи природний шум. Незначна зміна амплітуди сигналу носія.	Висока стійкість до модифікації контейнера.	Невисока пропускна здатність стегоканала. Можливе вдосконалення міри пропускної здатності за рахунок застосування властивостей акустичного носія.
Кодування початкових фаз	Використовують для вбудовування ЦВЗн слабку чутливість системи слуху людини до незначних	Один з найбільш ефективних способів кодування за критерієм відношення сигнал-шум.	Низька пропускна здатність.

Продовження таблиці 2.9

	змін фази аудіосигналу.		
Вбудування на основі кодування ехосигналу	Вбудовує ЦВЗн шляхом зміни затримки.	Гарна непомітність.	Невисока пропускна здатність.
Метод LSB (Least Significant Bit)	Використовує слабку чутливість ССЛ до незначної зміни інтенсивності аудіоконтейнеру.	Висока пропускна здатність стегаканалу.	Вразливість до конвертування потокового контейнера.

Особливий інтерес у науковців проявляється до закритих систем реалізації стеганографічних каналів. Оскільки впроваджується ключ, який володіє властивостями ПВП. Відсутність ключа [2, 3, 19] у стороннього суб'єкта унеможливлює отримання контексту чутливої інформації та отримання аргументів існування прихованого КЗ. В табл. 2.10 уточнюються види стеганографічних систем [2, 3], які реалізує певний алгоритм кодування.

Таблиця 2.10 – Властивості методів звукової стеганографії

Алгоритм	Властивість ССЛ	Тип системи
Кодування найменш значущих біт (НЗБ)	Слабка чутливість ССЛ до незначної зміни інтенсивності аудіосигналу	Відкрита, крихка стеганосистема
Фазового кодування	Несприйнятливість ССЛ до зміни абсолютної фази аудіосигналу	Відкрита, напівкрихка стеганосистема
Ехо-приховування	Слабка чутливість ССЛ до незначної зміни ехосигналів	Закрита, робастна стеганосистема
Розширення спектра	Слабка чутливість ССЛ до незначної зміни інтенсивності аудіосигналу	Закрита, робастна стеганосистема

Із табл. 2.10 видно, що лише два способи стеганографії в парадигмі акустичних систем використовують секретні ключі. Застосування відкритих систем з точки зору системи захисту інформації можливе у комбінації із кодами криптографії. Тобто гібридний підхід до реалізації концепції безпеки. В табл. 2.11 розглядаються основні положення інкапсуляції інформації [4, 5, 13] в акустичний носій. Внесені теоретичні величини [2, 3] пропускної здатності (рис. 2.26) отримані на основі експериментальних тестів. Ключова сутність полягає в меті – досягти максимально низький рівень BER, при цьому забезпечити непомітність прихованого контенту.

Таблиця 2.11 – Порівняння технік акустичного приховування

Метод	Сутність технології монтування	Сильні сторони	Теоретична пропускна здатність, С
Метод НЗБ (Найменш значущого біту)	Кожен молодший біт відліку в методі LSB замінюється одним бітом інформаційного тексту	Простий варіант для запису інформації в потоковий контейнер	16 Kbps
Ехо приховування	Кодує бітові дані через внесення ехо послідовностей в акустичну оболонку	Стійкий до втрати інформації за рахунок стиску	16 Bps
Фазове кодування	Модулює фазу вихідного сигналу, вбудовує інформацію у частотну область сигналу	Стійкий до маніпуляцій над акустичним контейнером, для успішного відновлення необхідна модель вилучення та вихідний сигнал	8 Bps
Розширення спектра	Розсіює інформаційні сигнали по частотному спектру акустичного каналу	Демонструє хороші показники стійкості, придатний до удосконалення структури процедури, можливе покращення пропускної здатності та надійності	4 Bps

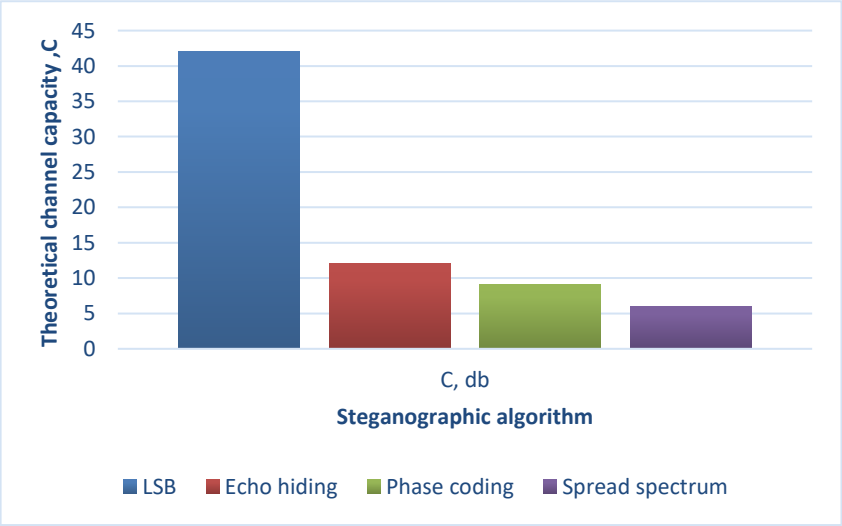


Рисунок 2.26 – Теоретичні оцінки пропускної здатності

Найбільшу пропускну здатність показує алгоритм НЗБ. Проте його стійкість при спотворенні контейнера не гарантує безпомилкове вилучення інформації. Метод LSB вразливий до статистичного стегааналізу та неефективний для надійної передачі інформації. При обміні ІзОД застосування алгоритму LSB та фазового кодування не рекомендується. Не реалізуються захисні механізми прихованої інформації. Кількість інформації внесеної до медіаоб'єкту методом розширення спектра може варіюватися. Залежно від властивостей кодових послідовностей та кількості каналів встановлених процедурою. Дослідження алгоритмів на критерій ефективності включає [3] розрахунок математичних показників (табл. 2.12).

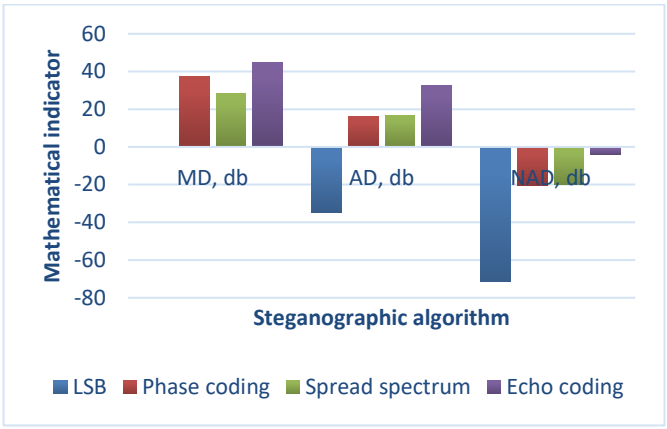
Таблиця 2.12 – Математичні оцінки алгоритмів акустичної стеганографії

Назва показника спотворення	Оригінальний потік	Заміна НЗБ з псевдовипадковим інтервалом	Фазове кодування	Розширення спектра	Кодування луно-сигналу
Кількість бітів у повідомленні	–	232	176	176	176
Кількість модифікованих відліків контейнера	0	103	146994	146942	146994
Максимальна абсолютна різниця, MD	0	1	5575	655	30300
Середня абсолютна різниця, AD	0	$3{,}504*10^{-4}$	41,093	47,321	$1{,}912*10^{3}$
Нормована середня абсолютна різниця, NAD	0	$7{,}612*10^{-8}$	$8{,}928*10^{-3}$	$1{,}028*10^{-2}$	0,404
Середньо квадратична помилка, MSE	0	$3{,}504*10^{-4}$	$1{,}656*10^{4}$	$8{,}024*10^{3}$	$7{,}416*10^{6}$
Нормована середньо квадратична помилка, NMSE	0	$9{,}130*10^{-12}$	$4{,}315*10^{-4}$	$2{,}019*10^{-1}$	0,185
L^p–норма, при p=2	∞	0,019	128,670	89,576	$2{,}723*10^{3}$
Відношення сигнал/шум, SNR	∞	$1{,}095*10^{11}$	$2{,}318*10^{3}$	$4{,}782*10^{3}$	5,41
Максимальне відношення сигнал/шум, PSNR	∞	$3{,}065*10^{12}$	$6{,}486*10^{4}$	$1{,}338*10^{5}$	144,782

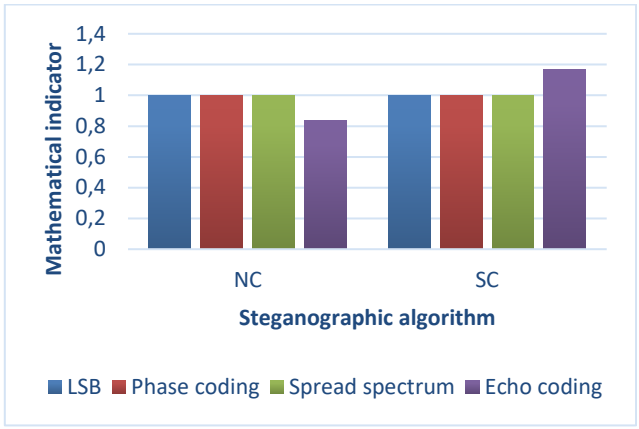
Продовження таблиці 2.12

Якість звучання, AF	1	1,000000	0,999569	0,999791	0,815146
Нормована взаємна кореляція, NC	1	1,000000	0,999784	0,999970	0,836138
Якість кореляції, CQ	8337,127	8337,127	8335,328	8336,880	7088,592
Структурний зміст, SC	1	1,000000	1,000000	0,999850	1,166683
Загальне сигма-відношення сигнал/шум, GSSNR	∞	$3{,}501*10^{16}$	$4{,}727*10^{14}$	$1{,}777*10^{8}$	181,669
Сигма-відношення сигнал/шум, SSNR	∞	165,441	146,746	82,497	22,593
Нормоване відношення сигнал/шум, NSER	∞	$1{,}095*10^{11}$	$2{,}318*10^{3}$	$4{,}782*10^{3}$	5,41
Подібність гістограм, HS	0	206	71983	73153	73701

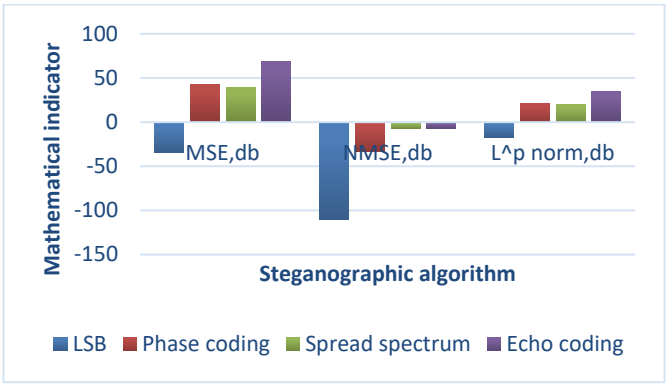
На основі складеної табл. 2.12 [3] побудовані графічні ілюстрації (рис. 2.27) результатів. Графічні дані відображають рівень спотворень заповненого контейнера через маніпуляції деякого алгоритму. Оцінювані показники спотворень потокового контейнера та метрики кореляції. Об’єктом досліджень були аудіо потоки інтенсивностей напруги для тестування можливостей алгоритмів звукової стеганографії. Показники рівня внесених спотворень (рис. 2.27 (а, в, г, д, е)) та кореляції (рис. 2.27 (б)) зображені на координатній площині. Показники SNR та PSNR найбільші для способу НЗБ серед розглянутих екземплярів на рис. 2.27 (г). У звукових потоках [4] SNR нижче 20 дБ зазвичай означає зашумлення об’єкта звуку, тоді як співвідношення сигнал/шум 30 дБ і вище вказує на те, що якість аудіосигналу збережена. Високий рівень SNR для НЗБ забезпечується за рахунок вбудування у наймолодший біт інтенсивності звуку. При застосуванні методу НЗБ в більш значущих розрядах амплітуд відбувається суттєве спотворення сигналу. Метод розширення спектра потребує модифікації базису ключів для збереження стійкості системи.



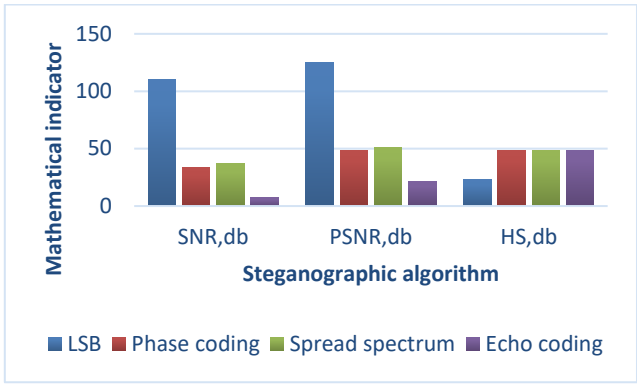
а)



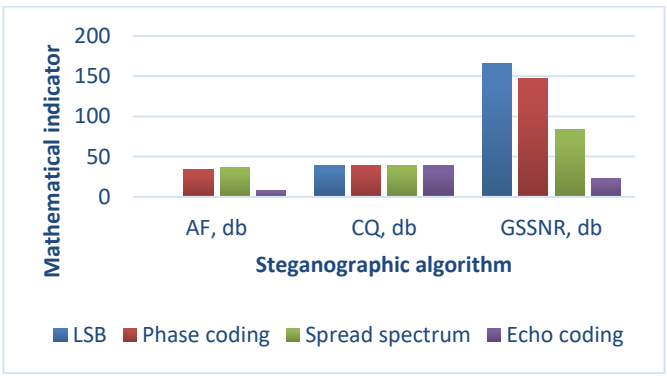
б)



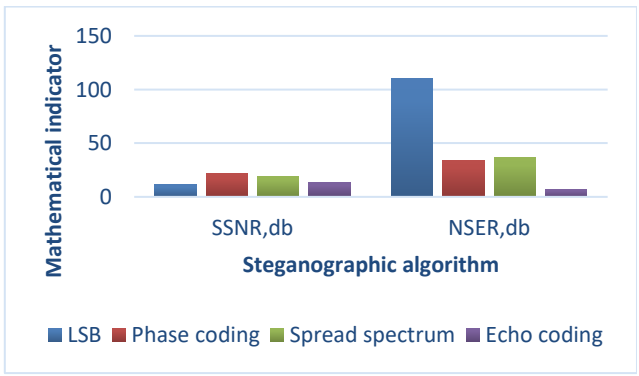
в)



г)



д)



е)

Рисунок 2.27 – Графіки емпіричних даних

В таблиці 2.13 представлені емпіричні дані отримані при дослідженні аудіосигналу на деякому потоці відліків сигналу (DCF77.wav, $f_д$=24000 Hz). Графічне подання результатів досліджень подані на рис. 2.28 (а, б, в, г, д, е). Результати досліджень виражені цифровими показниками якості вбудовування інформаційного контенту. Більше значення SNR демонструє збереження якості оригінального сигналу на фоні шумів.

Таблиця 2.13 – Оцінки практичних досліджень методів приховування

Метрика оцінки	Оригінал	Метод НЗБ, стандартний	Кодування фази	Розширення спектра (k=1, G=1, n =1024)	Exo кодування
Кількість бітів у повідомленні	–	52480	513	32406	23568
Кількість модифікованих відліків контейнера	0	1508415	15088352	1508352	1508352
Максимальна абсолютна різниця, MD	0	0	0	0	0
Середня абсолютна різниця, AD	0	0.017438835	1649.69	1	603.822
Нормована середня абсолютна різниця, NAD	0	0.000012032	1.138182556	0.001	0.416598968
Середньо квадратична помилка, MSE	0	0.017526344	5189873.0827	1	605697.06210
Нормована середньо квадратична помилка, NMSE	0	0	1.78502	0	0.20833
L^p–норма, при p=2	∞	0.132387099	2278.13	1	778.26541880
Відношення сигнал/шум, SNR	∞	165890410.42	0.56021647	2907573.816	4.800175799
Максимальне відношення сигнал/шум, PSNR	∞	247509.01217	14.383292502	32767.684	16.243089476
Якість звучання, AF	1	0.999999994	-0.785024278	1	0.20833
Нормована взаємна кореляція, NC	1	0.999999521	0.107220985	1	0.772464447
Якість кореляції, CQ	$-1{,}105\cdot10^{7}$	$-1.11\cdot10^{7}$	$-1{,}18487\cdot10^{6}$	$-1{,}105\cdot10^{7}$	$-8{,}54\cdot10^{6}$
Структурний зміст, SC	1	1.000000951	1.000534037	1	1.327572383
Загальне сигма-відношення сигнал/шум, GSSNR	10.346342058	10.346339452	9.537607487	10.346	9.568914951
Сигма-відношення сигнал/шум, SSNR	15.485692312	15.485867024	14.634730729	15.486	15.761586123
Нормоване відношення сигнал/шум, NSER	∞	38.750774312	272.0891	2805.456	3072.055
Подібність гістограм, HS	0	14138	482472	86846	592450

При дослідженні були використані популяризовані алгоритми звукового приховування ЦВЗн в науковій та практичній площині.

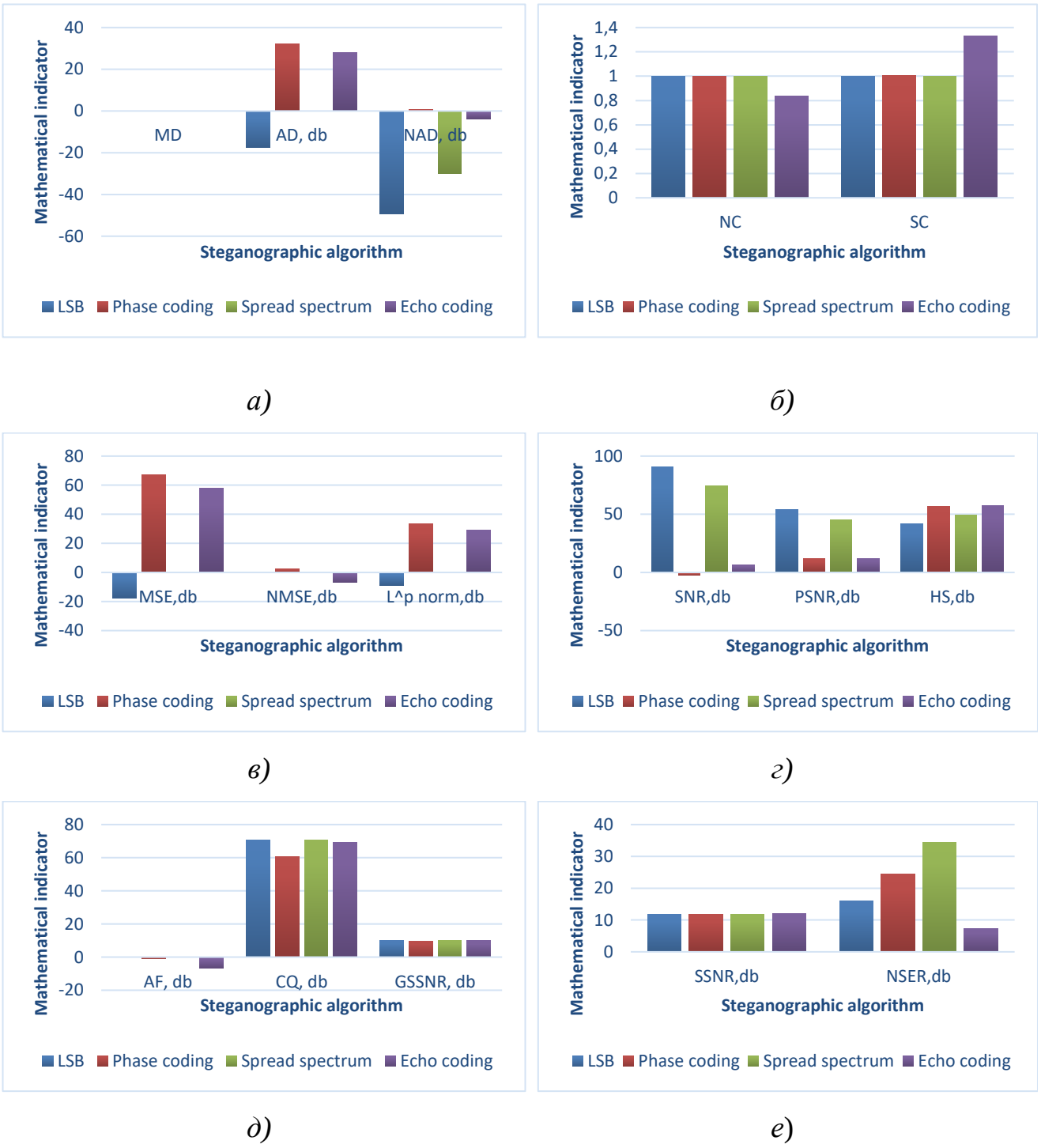


Рисунок 2.28 – Графіки емпіричних даних прикладних тестувань

2.5 Вектори удосконалення алгоритму

Алгоритм розширення спектра можливо модернізувати за рахунок покращення параметрів та інтеграції додаткових механізмів. Елемент оптимізації стосується структури процедури вставки інформації в контейнер. Алгоритм стеганографічної вставки повинен містити механізми контролю цілісності та

враховувати статистичну структуру контейнеру. Підхід дозволяє значно зменшити спотворення інформаційних сигналів. Мета покращення – досягти хороших показників безпеки та безпомилкового вилучення даних. З оптимальним показником внесення шуму до акустичного носія. Секретним ключем [2, 13] в методах розширення спектра виступає ПВП. Структура секретного ключа повинна володіти псевдовипадковими властивостями. Ймовірність генерації такого ключа зловмисним апаратом повинна прямувати до нуля. Зі збільшенням порядку ключа збільшується його двійковий набір. Тобто стеганоаналітику необхідно перебрати велику сукупність комбінацій, щоб отримати ключовий базис. В табл. 2.14 приведені направлення [2, 15, 25-31] оптимізації для алгоритму розширення спектра.

Таблиця 2.14 – Вектори покращення для алгоритму розширення спектра

Направлення оптимізації	Сутність
Гібридний підхід	Застосування елементів із різних стеганографічних алгоритмів та створення нового варіанту алгоритму вбудування. Застосування різних підходів приховування можуть покращити показники стійкості. Комплексування алгоритмів приховування ЦВЗн для покращення пропускної спроможності та моделі безпеки.
Інтеграція криптографічних кодів	Стеганографія є доповненням до криптографічної парадигми та допускає синхронізацію технологій. Застосування шифрів для забезпечення безпеки підвищить рівень захисту. Реалізується подвійний шар захисту.
Завадостійке кодування	Методи розширення спектра засновані на оцінці кореляції, тому бітова інформація може спотворюватися за рахунок шумів. Інтеграція кодів, що виправляють помилки є оптимальною основою для рішення. Коди Хемінга та Ріда Соломона є поширеними кодами для забезпечення правильного прийому інформації.
Модифікація ПВП	Зміна структури та правила генерації ПВП, які використовуються для модуляції інформаційних сигналів. ПВП підбираються, таким чином, щоб їх можна було відокремити один від одного в інформаційній суміші. Відокремлення реалізується через хороші кореляційні властивості. ПВП володіє властивостями випадковості для заходів надійності секретного ключа. ПВП повинні підтримувати хороші показники автокореляції та бути взаємно ортогональними. Для генерації придатних послідовностей використовуються рекурентні регістри в скінченних полях Галуа (англ. Galois Field — GF). Сучасний напрямок оптимізації — заміна класичних бінарних кодів на хаотичні сигнали, що генеруються динамічними системами. Вони мають велику ентропію і кращу прихованість.

Продовження таблиці 2.14

Оптимізація структури алгоритму	Метод розширення спектра має ряд похідних, які є вдосконаленою його версією. Це проявляється у підборі ключів із нульовим показником кореляції із потоковим контейнером. Модифікації структури ключової таблиці. Зміна стратегії інкапсуляції інформації в акустичний потік. Вдосконалення моделі алгоритму перш за все орієнтована на ефективність обчислень. Тобто досягнення максимальної непомітності інструментами ШІ та стороннім спостерігачем. Також безпомилкова доставка відомостей в пункт призначення. Інформаційний контент повинен імітувати природний шум, щоб ввести в оману спеціалізовані аналізатори.
Розрахунок контрольних сум	Забезпечення достовірної доставки даних є завданням методології стеганографії. Механізм контролю цілісності дозволяє виявити факт присутності помилок в інформаційному сегменті. Оскільки механізм допускає помилки при передачі Cyclic Redundancy Check (CRC) код є необхідним елементом контролю цілісності. Він є супровідним елементом із інформаційним пакетом.
Проблема синхронізації	Виникає потреба маркування прихованої посилки задля виявлення передавачем його положення. Можливо в динамічному потоці звуку вбудувати інформаційний блок із спеціальним синхрословом. Стеганографічний апарат на основі цього слова виявить контент та виконає його вилучення. Перевага полягає у вибірковій зоні вставки інформаційного сигналу та забезпечення синхронізації. Заміна послідовного пошуку на спеціальну фільтрацію сигналу. Предмет пошуку – інформаційний потік на основі унікального слова.
Вибір частотного спектра	Людський слух володіє спеціальними особливостями до сприйняття частотного діапазону. Можливо використати частотну площину для інтеграції інформації. Володіння певним звуковим сигналом незначний вплив, якого не провокує чутливість ССЛ. Щоб прихований сигнал не "спровокував чутливість", його енергія повинна знаходитись нижче порогу маскування. Спектр спеціального сигналу використовується як об’єкт розмазки інформаційної посилки.
Статистичні особливості	Можливо використовувати статистичні особливості контейнеру для монтування ЦВЗн. Вплив на інтенсивності звуку, що менше за частотою будуть мати несуттєвий вплив. Вставка даних в межах норми статистичних порогів не повинна провокувати чутливість та детектованість сигналу. Замість того, щоб змінювати конкретні біти в конкретних семплах, ми змінюємо інтегральні статистичні показники великої групи семплів. ССЛ погано розрізняє мікроскопічні зміни в розподілі ймовірностей амплітуд, якщо загальна енергія та огинаюча сигналу залишаються незмінними.

В табл. 2.14 окреслені загальні вектори [27] для оптимізації методу розширення спектра для ефективного вбудування ЦВЗн. Похідні методи розширення спектра [2, 15, 28]: метод приховування даних із адаптованим формуванням складних сигналів та спосіб приховування на основі адресації

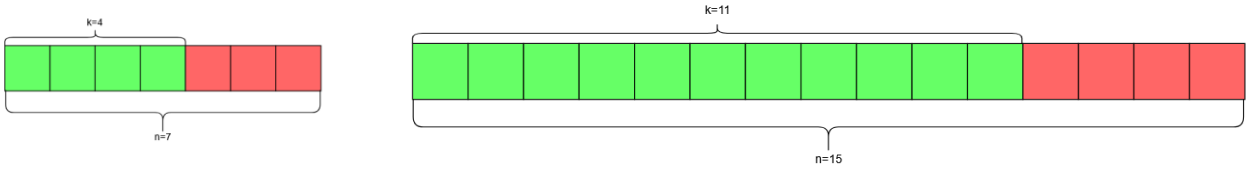
сигналів. Мета оптимізації досягти наближеного до нуля рівня кореляції та вдосконалити ключову таблицю. Отримати максимум безпомилкового обсягу виділеної інформації із джерела зберігання. На основі джерела [2, 15, 28], сформовані наступні особливості реалізацій методів розширення спектра (табл. 2.15).

Таблиця 2.15 – Особливості похідних методів розширення спектра

	Метод Лізи Марвел	Адаптивний метод	Метод із адресацією сигналів
Стійкість до афінних атак	-	+	+
Показник втрати достовірності, $P_{\text{пом}}$	$\approx 0{,}5$	≈ 0	≈ 0
Обмеження для безпомилкової передачі контенту	Достовірність не забезпечується	$kG \le \rho_{\max}$	$G \le \rho_{\max}$
Пропускна здатність	(k/n), де $k \le M$	(k/n), де $k \le M$	(k/n), де $k = \log_2 M$
Величина внесених спотворень	не перевищує $\left(\frac{kG}{65536}\right)100\%$	не перевищує $\left(\frac{kG}{65536}\right)100\%$	не перевищує $\left(\frac{G}{65536}\right)100\%$
Питома обчислювальна складність вилучення	1	1	$\frac{2^k}{k}$

Вдосконалення різновиду технології розширення спектра направлене на досягнення стійкості системи безпеки. Наближення до безпомилковості вилучення підмішаної інформації у сигнал. Підвищення потужності сигнальної частини за рахунок G – не єдиний метод досягнення завадостійкості. Занадто високе значення параметру G підсилює сигнал, але сильно спотворює потік звуку. Порушується базова концепція стеганографії [2, 6] – внесення інформації непомітним чином для необізнаних спостерігачів. Популярним варіантом [25] є коди Хемінга, що відносяться до класу групових кодів із параметром кодової відстані d ($d_{\min}$=3; $d_{\min}$=4) [3, 25], що дозволяють виправляти одинокі помилки та виявляти дворазові помилки. Коди Хемінга відносяться до категорії систематичних кодів [25], де інформаційні та перевірочні символи займають чітко визначену позицію. Генерація коду реалізується [2, 25] через створення породжувальної матриці G розміром $n \times k$ та перевірочної матриці H розмірністю $n-k \times n$. Пошук похибок у інформаційному

слові здійснюється на базі системи синдромів. Кодове слово є інформаційною послідовністю, що передається через мережу. На рис. 2.29 (а, б) зображені схеми деяких кодів Хемінга [25].



а *б*

Рисунок 2.29 – Схема кодів (а) Хемінга (7,4) та (б) Хемінга (15,11)

В табл. 2.16 наведені характеристики деяких кодів Хемінга. Код Хеммінга застосовує кілька контрольних бітів. Для можливості коректування та визначення помилок. Інформаційна частина *k* біт залишається незмінною [25], що комбінується із надмірними перевірочними бітами $n-k=r$.

Таблиця 2.16 – Характеристики кодів Хемінга

Контрольні біти, *r*	Довжина блоку, *n*	Інформаційні біти, *k*	Код	Відносна швидкість R
3	7	4	Хемінг (4,7)	0,571429
4	15	11	Хемінг (15,11)	0,733333
5	31	26	Хемінг (31,26)	0,838770
6	63	57	Хемінг (63,57)	0,904761

Сучасний досконалий код завадостійкого кодування є код Ріда-Соломона. Вимога [25] якого є два перевірочні символи, що припадають на одну потенційну помилку. Інтерпретація коду Ріда-Соломона [2, 11, 25] визначається як недвійкові коди БЧХ (Боуза-Чоудхурі-Хоквінгема), який використовує в якості елементів коду компоненти поля $GF(q^m)$, де m – символів інформації зображуються окремою складовою кінцевого поля. Коди Ріда-Соломона – це лінійні недвійкові систематичні циклічні коди [11, 25], символи яких є *r*-бітові послідовності, де *r* – ціле позитивне число, більше 1. Більшість (*n*, *k*)-кодів Ріда-Соломона; (*n*, *k*) = (2^r–1, 2^r–1–2*t*), де *t* – кількість спотворених символів , які можуть виправити код, а *n*-*k* = 2*t* – кількість контрольних символів. Перевага даного коду [25] – це найбільша величина мінімальної кодової відстані $d_{\min}$ для можливого лінійного коду, що відповідає *n*–*k*+1. За теорією блокових кодів [2, 25] коректуюча здатність

визначається величиною мінімальної кодової відстані $d, d = u + 1$, тобто $\left\lfloor \frac{d-1}{2} \right\rfloor$. Точніше мається на увазі при $u = 2t$, код може виправити t спотворень [25]. Інструменти кодів, що виправляють помилки та CRC є одними з дієвих методів контролю правильності контенту передачі за джерелами [3, 15].

У наведених вище напрямах оптимізації алгоритму наведений аспект формування секретного ключа. Кодова послідовність, яка використовується для розмиття інформаційних сигналів може генеруватися різними методами. Спосіб формування впливає на кореляційні властивості та аспекти стійкості. Використаний базис ПВП повинен відповідати умовам виразу (2.5). Щоб відокремити канали інформації один від одного в спектральній смузі. Відмінними властивостями автокореляції [29-31] володіють коди Баркера. Нині відомо 7 кодів-послідовностей (табл. 2.17), які володіють [31] такими властивостями. Потенціал експлуатації таких кодів обумовлений через кореляційні властивості. Для заданого вектору даних, функція кореляції [29] зосереджує максимум в центральному піку відносно піків бічних пелюсток.

Таблиця 2.17 – Послідовності Баркера

Довжина коду	Структура послідовності	
2	+1 -1	+1 +1
3	+1 +1 -1	
4	+1 -1 +1 +1	+1 -1 -1 -1
5	+1 +1 +1 -1 +1	
7	+1 +1 +1 -1 -1 +1 -1	
11	+1 +1 +1 -1 -1 -1 +1 -1 -1 +1 -1	
13	+1 +1 +1 +1 +1 -1 -1 +1 +1 -1 +1 -1 +1	

Для дискретного сигналу x довжиною N (де елемент x_i відповідає +1 або −1) автокореляційна функція (АКФ) для зсуву k розраховується як сума добутків. АКФ такої послідовності [31] визначається наступним виразом:

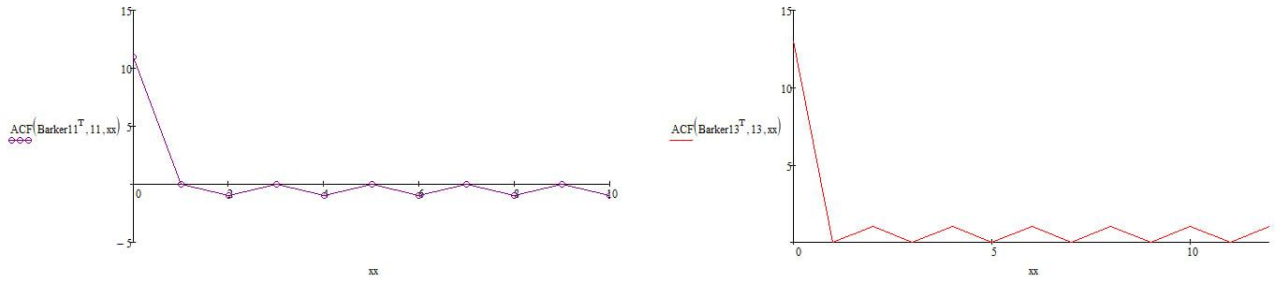
$$R(k) = \sum_{i=0}^{N-1-k} x_i x_{i+k}, \tag{2.24}$$

де k – величина зсуву;

x_i – сигнал в момент i;

x_{i+k} – значення сигналу, зсунутого на k.

На рис. 2.30 продемонстровано поведінку АКФ для кодів Баркера довжиною 11 (рис. 2.30 (а)) та 13 (рис. 2.30 (б)) в залежності від величини зсуву *k*.



а *б*

Рисунок 2.30 – АКФ для кодів (а) Баркера-11 (б) Баркера-13

Структурні властивості АКФ кодів Баркера дозволяють відокремити їх один від одного в багатоканальних системах. Максимум енергії АКФ зосереджено при нульовому зсуві *k*. Потрібно підкреслити, що максимум енергії відповідає довжині коду. При зміні величини зсуву *k* АКФ не перевищує 1 за модулем. Бічні пелюстки співвідносяться до шуму та не виходять за межі порогу. За рахунок взаємних властивостей кореляції кодів можливий варіант впровадження їх у систему розширення спектра. В якості ПВП використовуються коди Баркера бажано максимальної потужності. Довжина коду визначає енергетичний виграш при обробці сигналу. Процес модуляції для варіанту Баркера-13 представлений на рис. 2.31.

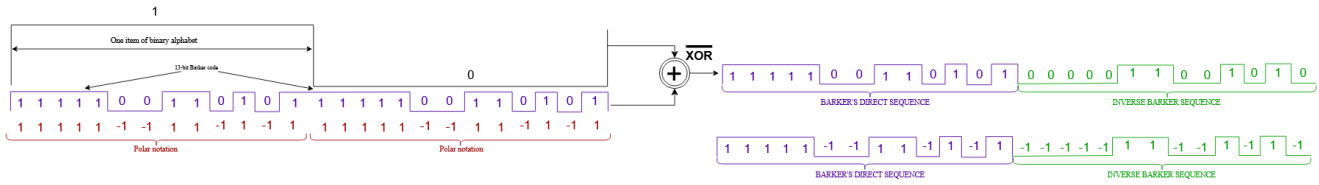


Рисунок 2.31 – Схема модуляції за допомогою кодів Баркера

Сигнал «1» модулюється прямим кодом Баркера, «0» інверсним кодом відповідно. З вихідного стану, коди переводяться у полярну форму при внесенні в сигнал. Корелятор має копію прямого коду Баркера та обчислює показник кореляції – згортку вихідного сигналу із еталоном.

3 ОПИС ПРОГРАМНОГО КОМПЛЕКСУ

3.1 Загальні положення

Стеганографічні моделі є елементом [2, 5] для реалізації систем впровадження ЦВЗн у мультимедійні носії та прихованого спілкування. Базові можливості функцій побудови стеганографічних систем планується реалізувати у комплексній програмній архітектурі. Пропонується модель (додаток В), яка буде взаємодіяти із акустичними об’єктами. Програма підтримує (рис. 3.1) сукупність модулів, які реалізують власний інструментарій безпеки.

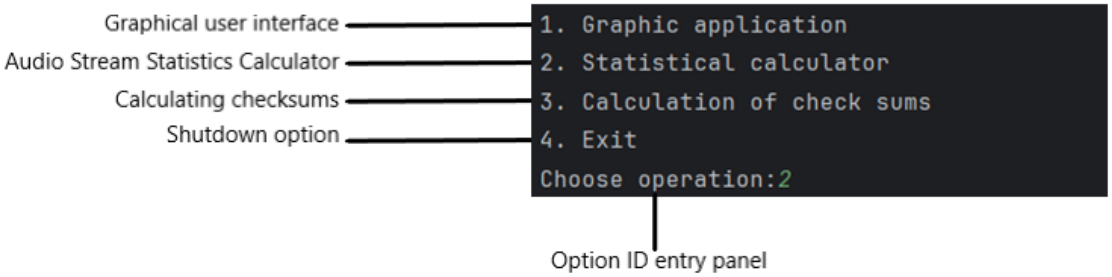


Рисунок 3.1 – Меню програмної системи

Програмна архітектура включатиме: графічний інтерфейс для стегановставки ЦВЗн у акустичний канал, статистичний калькулятор та розрахунок контрольної суми [3]. Встановлений шаблон у вигляді меню – списку для вибору опції. Графічний інтерфейс користувача охоплює реалізацію типових алгоритмів звукової стеганографії. Додаткові модулі інтегровані в систему для статистичного аналізу вибірки та контролю цілісності інформаційних відомостей. Реалізація (графічна частина) імітує мережеву систему, яка складається двох вузлів. Віртуальні пристрої взаємодіють між собою по локальній мережі за адресою оберненої петлі, яка вказує на власний комп’ютер. Доступна функція «Exit» (Вихід) для завершення роботи веб-додатку. Виведення області меню продовжується до тих пір поки не буде завершена робота системи. Мета побудови проекту

продемонструвати частковий спектр можливостей інструментів стеганографії для реалізації політики безпеки. Галузі експлуатації включають вбудування цифрового ідентифікатору в потоковий контейнер та організацію прихованого каналу спілкування. Статистичний аналізатор включає обчислення загальних показників статистики для кінцевої вибірки даних. Також побудови гістограми сигналу та обчислення часткових ймовірностей. Сфери застосування моделі стосуються політик та сценаріїв дослідження та забезпечення безпеки інформації.

3.2 Мережевий аналіз графічної частини

Розроблена графічна система симулює систему зв'язку [32]. У моделі є два віртуальні комп'ютери, які взаємодіють по КЗ. Вузл *А* виконує операцію безпеки та надсилає серверу (вузлу *Б*) виконати завдання – вилучення інформації. Обидва пристрої в пам'яті володіють правилом або ключем для відкриття контексту інформації. Концепція запропонованої системи базується (рис. 3.2) на загальній моделі «клієнт-сервер».

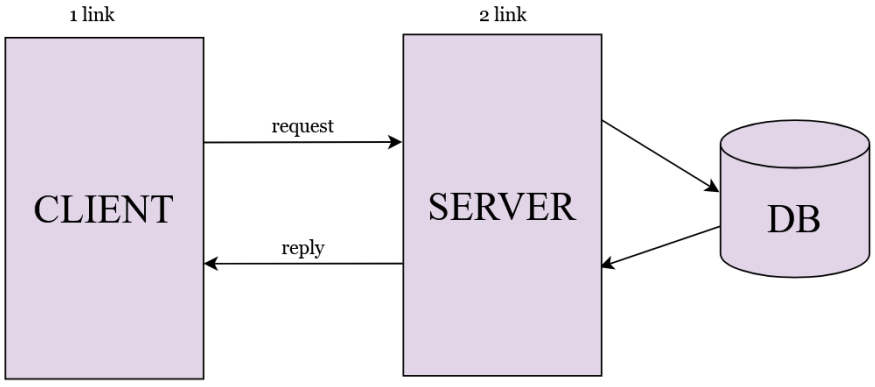


Рисунок 3.2 – Архітектура «клієнт-сервер»

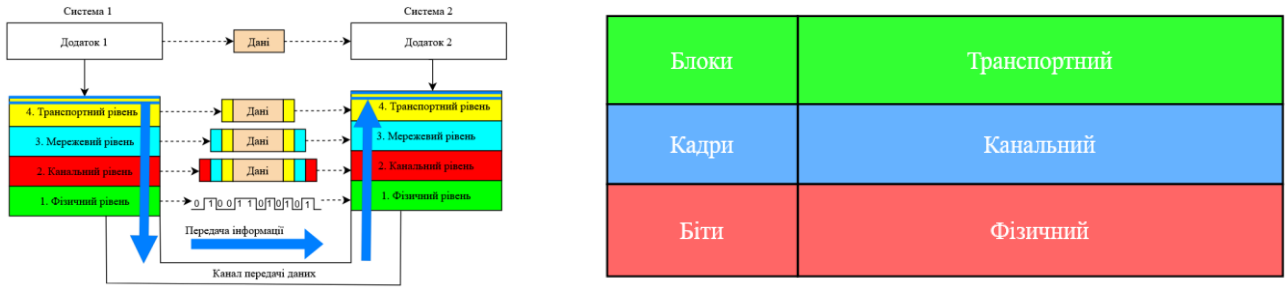
Сутність такої архітектури полягає в тому, що клієнтська сторона [32] відправляє запит на сервер. Вважається, що сервер знає, що спілкується саме із тим клієнтом, який до нього звертається. В реальних застосунках необхідний механізм криптографії, який дозволяє перевірити автентичність клієнту [19]. Стеганографічні моделі є хорошим прикладом для здійснення протоколу

верифікації суб'єкта. Запит обробляється і результат надсилається клієнту. Основні елементи моделі [32]:

1) Клієнт – комп'ютерний пристрій на стороні користувача, який надсилає запити серверу для обробки потоку даних або реалізації послідовності дій.

2) Сервер – комп'ютерна система, яка володіє потужними обчислювальними можливостями для вирішення комплексних завдань, надання доступу до цифрових ресурсів, управління даними.

Процес взаємодії регулюється мережевими протоколами [32, 33] – сукупність правил, які управляють процесом взаємодії вузлів мережі. Реалізована система з точки зору моделі OSI (Open Systems Interconnection) породжує три абстрактні рівні мережевої взаємодії (рис. 3.3).



а *б*

Рисунок 3.3 – Мережева модель взаємодії (а) функціональна модель (б) модель рівнів обміну

Загальна модель взаємодії вузлів проілюстрована на рис. 3.4. Канальний рівень включає функцію перевірки помилок [33]. В структуру кадру вбудований CRC код. Унікальний код реагує [3] на мікроскопічні модифікації контенту. Інструменти контролю цілісності є важливим елементом ефективної передачі інформації. Механізм дозволяє перевірити правильність отриманої посилки. Транспортний рівень відповідає [32, 33] за фрагментацію бітового потоку. Сегменти інформації циркулюють до пункту призначення. За фізичну передачу по середі відповідає фізичний рівень моделі OSI. В контексті запропонованої моделі можливий варіант імітації впливу природного шуму на потік даних. Сірою палітрою виділені рівні, які функціонують в границях програмного продукту. Помаранчеві рівні не є основними рівнями взаємодії.

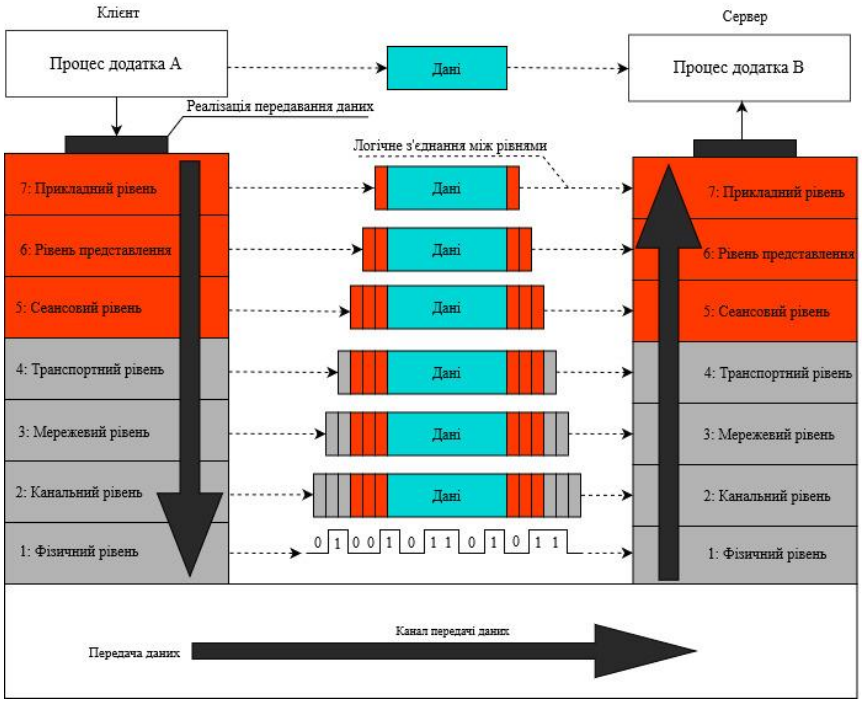


Рисунок 3.4 – Узагальнена модель взаємодії OSI програми

Імітація системи відбувається на локальному рівні, маршрутизація пакетів не відбувається в контексті глобальної мережі. Кожний рівень моделі відповідає за свою частину комунікаційної взаємодії систем та містить власний перелік протоколів. Віртуальні пристрої обмінюються потоковими даними, які містять корисну інформацію. В конкретному сценарії ЦВЗн непомітно монтується в звуковий потік та передається по КЗ. Згідно з моделлю на рис. 3.4 взаємодія відбувається в оберненому порядку на стороні адресата. Із пакетів вилучається потік цифрового сигналу. На основі наведеного сектору даних стеганографічний декодер вилучає дані на базі певного методу стеганографії. По суті, реалізується протокол прихованої передачі інформації по відкритому КЗ. Контент може містити сегменти шумів. Детальний опис функціональних рівнів [33] запропонованої моделі наведено в табл. 3.1.

Таблиця 3.1 – Опис функціональних рівнів обміну інформацією системи

Назва рівня	Тип даних	Характеристика
Фізичний	Біти	Реалізує передачу потоку бітів інформації по фізичному середовищу. Визначає тип фізичного середовища, фізичні та електричні характеристики інтерфейсів. Рівень працює із набором бітів інформації.

Продовження таблиці 3.1

Канальний	Кадри	Відповідає за надійну доставку інформаційної посилки, виправлення помилок, доступ до простору передачі. На прийомі дані із фізичного рівня вкладаються у кадри та проходять перевірку на цілісність. Якщо помилок немає кадр передається на наступний рівень. При наявності похибок кадр відкидається та формується запит на повторну пересилку.
Транспортний	Блоки	Забезпечує надійне та безпечне з'єднання між вузлами мережі. Прямий зв'язок між комп'ютерами, виконання надійної чи ненадійної доставки даних, керування потоком.

Симуляція мережі є елементом реалізації справжньої системи зв'язку. Модель реалізує обмін даними на локальному сегменті мережі. Мережеві пакети можуть мати ряд структурних комірок для вбудування. Даний аспект можна використати для внесення додаткової інформації про ЦВЗн або чутливої інформації. Пакет даних буде містити необхідну інформацію для правильного вилучення відомостей.

3.3 Характеристика графічного інтерфейсу продукту

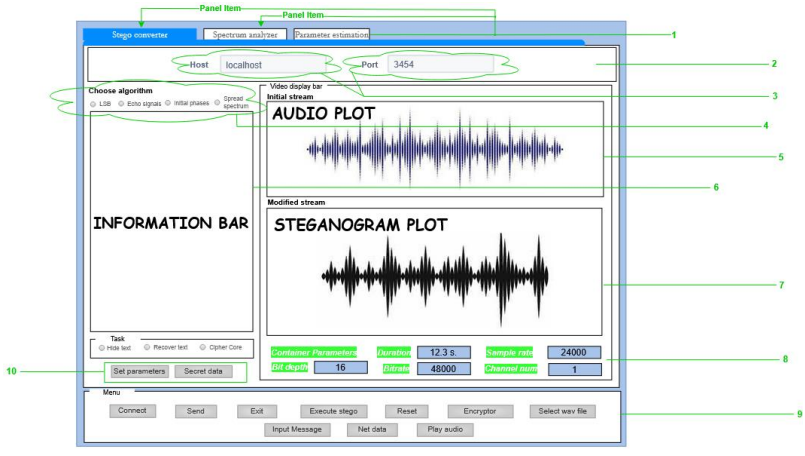
Графічний інтерфейс користувача включає інструменти управління: поля введення, кнопки, перемикачі тощо. Візуальні елементи призначені для керування поведінкою системи. Інструмент реалізований у вигляді фрейму. Ціль створення програми – це дослідження алгоритмів приховування інформації. Також здійснення процедури вбудування ЦВЗн в акустичний сигнал. В якості досліджень допускається виключно формат WAV. Графічні вікна при завантаженні файлу відображають ключові його атрибути. Графічна система містить меню для оперативного переходу між блоками схеми програми. Програмне рішення містить ряд секторів для оцінки вбудування. Здійснення процедур безпеки керується через блоки меню та спеціальні кнопки. В програму інтегровано загальні алгоритми парадигми звукового приховування. Надається можливість комплексування методів ІБ при реалізації подвійного шару безпеки [2, 6].

Стеганографічний блок [6] здійснює кодування інформації у відліках дискретного сигналу аудіо. Модуль стеганографії створений у вигляді програмної

реалізації. Конфіденційність даних [2] забезпечується через введення секретного ключа. Специфікація алгоритму визначає присутність чи відсутність ключа. Особливості його будови та необхідні атрибути. Тому встановлені додаткові вікна для налаштування. Параметр відомий лише сторонам спілкування й повинен зберігатися у таємниці. Викриття секретного ключа може спричинити компрометацію інформаційного повідомлення. Бітовий контент кодується в оболонці аудіотреку та пересилається по КЗ. Під час передачі на інформаційну суміш можуть впливати зовнішні чинники: шуми та деформуючі перетворення. Пасивний вплив може спотворити частину інформації або знищити чутливу інформацію. Декодування здійснює стеганографічний декодер на основі алгоритму декапсуляції за допомогою секретного ключа.

Результатом додавання інформаційного блоку є стеганограма. В контексті аудіообкладинки – це модифікований варіант аудіосигналу. Вбудований ЦВЗн повинен залишатися непомітним при різних видах аналізу контейнеру. Користувач встановлює вектор байтів в акустичний носій за допомогою інструментів веб-додатку. Після виконання монтування заповнений контейнер (стеганограма) – аудіосигнал передається на серверну сторону. У свою чергу, сервер має інструментарій для виділення медіаконтенту із шумової середи сигналу-переносника.

Як вже зазначалося програмне рішення поділено на дві базові частини. Інтерфейс фрейму (рис. 3.5) включає інформаційну панель та табло для графічного подання сигналу.



1 – Меню переходу
2 – Панель налаштування сеансу
3 – Параметри мережі
4 – Опції вибору методу стеганографії
5 – Графічне зображення аудіо потоку
6 – Інформаційне табло
7 – Графічне зображення стеганограми
8 – Інформаційна стрічка
9 – Меню кнопок
10 – Блокова панель меню

Рисунок 3.5 – Інтерфейс вікна програмного комплексу

Розроблена платформа представляє (рис. 3.6) стандартну програмну карту для навігації по функціональних блоках програми.

а) *б)*

Рисунок 3.6 – Конфігурація платформи (а) клієнту (б) серверу

Користувач може запустити будь-який блок через верхнє меню, яке не накладається на основний механізм системи вбудовування. У прототипі враховується концепція адаптивності додатку із його основними функціями. Доступні криптографічні пакети, що підтримують сучасні прийоми криптографічного захисту інформації. Програмна модель розроблена з урахуванням тенденцій сучасних додатків, що використовуються у різних галузях інформаційних послуг. В складі структури вбудовані механізми інформування користувача у разі дефектів. Стрічка кнопок встановлює взаємодію між модулями та зовнішнім користувачем. Інформаційна панель вказує на основні параметри звукового сигналу (частота дискретизації, тривалість сигналу, кількість каналів тощо).

На основі програмного рішення стеганографії планується комплексувати криптографічні коди. Для цього створено криптографічний модуль (рис. 3.7), який підтримує стандартні механізми. Функції гешування для отримання геш-образу, фіксуючи цілісність. Криптографічні примітиви, реалізуючи властивість конфіденційності. Комплексування методів [6] безпеки ініціює подвійний шар захисту. У веб-додатку підтримується три функції: «Зашифрування», «Розшифрування» та «Пошук гешу».

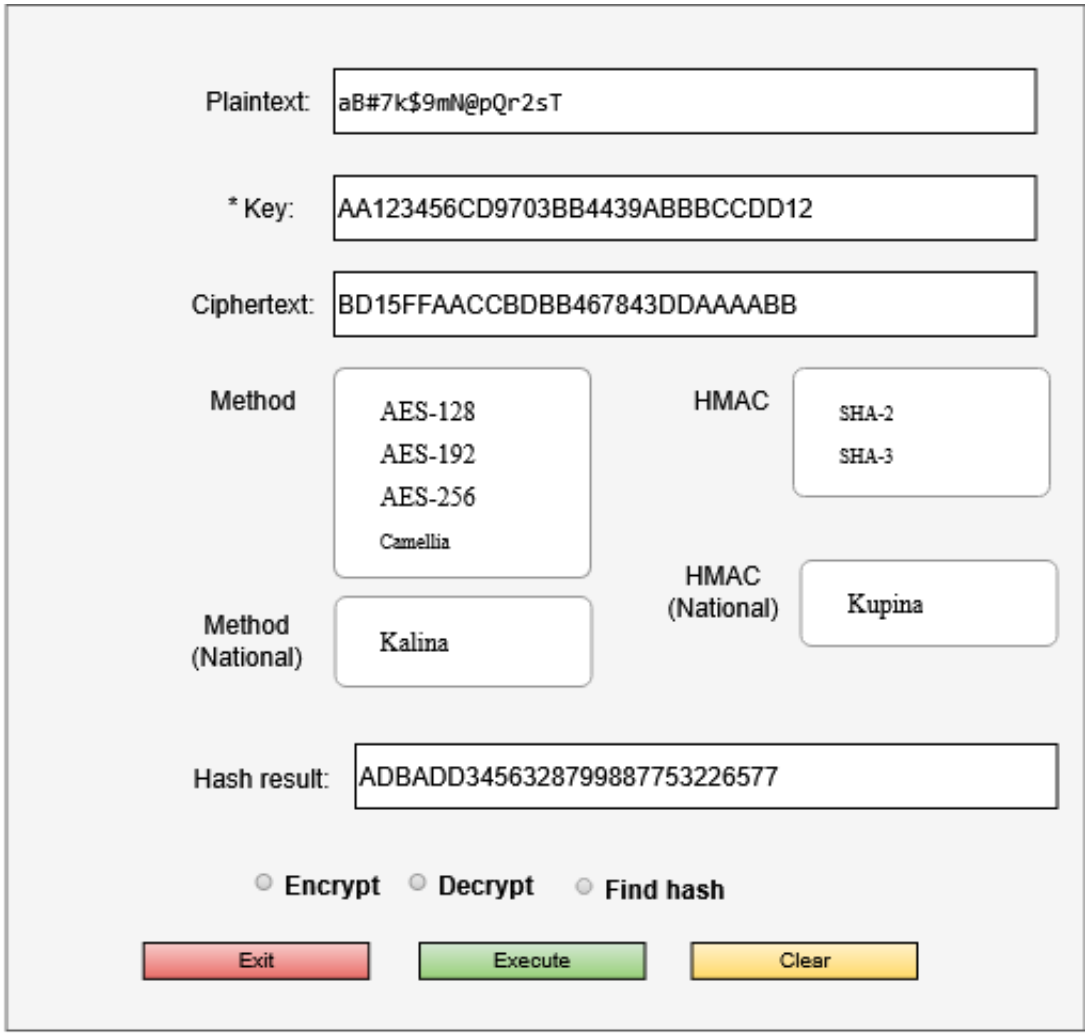
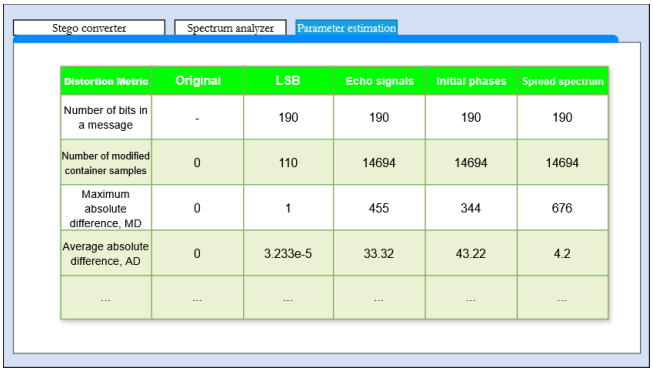


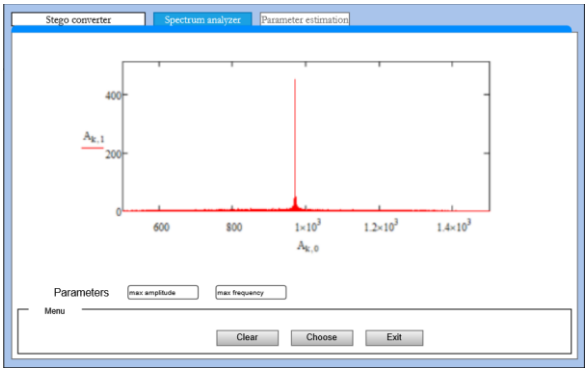
Рисунок 3.7 – Макет модуля криптографії

Опція «Clear» очищує всю встановлену інформацію. Обчислення геш-функції є засобом для забезпечення цілісності. Варіанти алгоритмів використовуються в мережевих системах та стандартизовані. Завдяки інструментам управління можливо керувати подіями веб-модуля. Функція «Execute» здійснює операцію криптографії в залежності від обраного стану. Процедура здійснюється на основі встановлених атрибутів. Розмірність параметрів повинна відповідати передбачені відповідним режимом.

В структуру механізму веб-додатку (рис. 3.8) включені обчислювальні блоки. Вони включають ряд загальним метрик (рис. 3.8 (а)) для визначення рівня кореляції та спотворень контейнеру. Спектральний образ (рис. 3.8 (б)) будується на

основі частотних компонентів завантаженого сигналу. Програмний фундамент [5] містить віртуальний центр для лабораторних досліджень результатів монтування.





а) *б*)

Рисунок 3.8 – Програмно-обчислювальне забезпечення (а) аналізатор спектру (б) вимірювач спотворень

Розроблене програмне забезпечення (ПЗ) формує механізми безпеки для захисту від НСД та несанкціонованої модифікації. Основні показники оцінки в границях ПЗ включені із літературного джерела [3]. Метрики обчислюються для оцінки міри спотворень та кореляційних зв'язків. Кожний із блоків ПЗ представляє площину дослідження акустичного каналу. Аналізатор спектра використовує засоби ЦОС для розкладу дискретного сигналу на частоти. Спектр виділеного сигналу показує розподіл енергії по спектральним частотами сигналу. Опція «Choose» використовує проміжний компонент програми для зв'язування із файловою системою. У дереві файлової системи визначається файл для дослідження, що проходить обробку модуля. На основі аналізу будується графічне представлення спектра та його параметри. Спектрограма дозволяє побачити зміну сигналу в динаміці потоку. По осі абсцис позначаються частоти, а по осі ординат рівень амплітуди.

3.4 Подальші плани оптимізації

Описаний програмний комплекс не є кінцевою версією розробки. Планується інтегрувати механізми завадостійкого кодування [25]. Причому реалізувати різноманітні коректуючі коди у векторних просторах. Базовий принцип полягає у

інтеграції двійкового алфавіту у векторний простір та обчислення синдромів. Симптоми помилкових бітів встановлюється через ортогональні базиси. За специфікацію методології виправлення здійснюється коректування помилок. В контексті розширення спектра необхідно реалізувати різні варіанти ПВП для модуляції сигналів. Ортогональні АС Адамара-Уолша [13] є одним із можливих опцій. Хороші властивості автокореляції кодів Баркера [29-31] можуть стати еталоном для вибору ключа. Псевдовипадкові конструкції в залежності від властивостей можуть вплинути позитивно на динаміку правильності виведення інформації. Потужним інструментом є коди CRC для фіксування інформаційного контексту [3]. При верифікації можливо виявити мікроскопічні помилки в межах великих масивів даних. Додатковим модулем аналізу буде статистичний калькулятор, який визначатиме основні показники статистики. Будуватиме розподіл вибірки інтенсивності звуку та перевірятиме відношення до законів розподілу. Якщо спектральний аналіз показує, які частоти присутні в сигналі, то статистичний аналіз показує, яка природа самого сигналу (шум, мова, музика, детермінований сигнал) та наскільки якісно він оцифрований. Статистична оцінка є орієнтиром для плану внесення інформації. Які сектори сигналу можливо використати для інтеграції. Потрібно підкреслити, що математичний аналіз реалізовано в середовищі Mathcad.

Окремо потрібно виділити, перспективу реалізації вітчизняних криптопримітивів в границях комплексу. Симетричний шифр Kalyna, геш-функцію Kupyna. Які володіють достатнім рівнем стійкості проти квантових систем. Планується реалізувати потокове вбудування ЦВЗн в динамічному режимі. Причому монтування здійснюватиметься в випадкові зони сигналу. Пошук здійснюється на основі кореляції та механізмів синхронізації пакетів.

ВИСНОВКИ

Теоретичні дані та математичні перетворення парадигм захисту знаходять практичне застосування в програмно-апаратних комплексах. Актуальність механізмів захисту динамічно зростає на тлі потенційних загроз в цифровому просторі. Тактика гібридного захисту широко імплементується у системах зв'язку, що позитивно позначається на показниках стійкості. Підхід дозволяє впровадити подвійний рівень захисту [6] від атак. Популярними направленнями ІБ залишаються криптографія та стеганографія. Причому стеганографія є раціональною альтернативою криптографії. Особливо в системах з недостатньою обчислювальною здатністю [1, 5] для реалізації складних перетворень.

Стеганографічні кодери використовують мультимедійні об'єкти для внесення чутливої інформації. Гарантія конфіденційності залишається експлуатація елементів криптографії в алгоритмах. Основна мета стеганографічного кодування – досягти непомітності спотворень контейнеру необізнаним користувачем [6], програмно-апаратним аналізатором і ШІ.

Аудіостеганографія є прогресивною віткою науки стеганографії. Алгоритми маніпуляції над звуком інтегруються в системи розвідки, досліджень та управління правами для захисту інтелектуальної власності. Парадигма базується на застосуванні особливостей ССЛ. Особливості ССЛ дозволяють суттєво використати обсяг медіаоб'єкту. Технології аудіостеганографії формують прихований КЗ доступний лише для авторизованих сторін. Аудіостеганографія має потенціал у контексті приховування інформації [9]: аудіофайли більші за розміром ніж графічні зображення, незначна зміна амплітуди дозволяє зберігати великі масиви даних, людський слух можливо легко ввести в оману.

Комплекс призначений для симуляції реальної програмної архітектури у конфігурації розподіленої системи. Дослідження прикладної схеми з точки зору реального суб'єкта спілкування. Важливим етапом монтування даних є вибір алгоритму та підбір оптимального набору параметрів. Розроблений інструмент

дозволяє оцінити якість процедури вбудування контенту. Важливим аспектом є оцінка реакції інформаційного артефакту на модифікації звукового сигналу під впливом шумів. Математичні показники стеганографії та спектр доповненого сигналу є метрикою для аналізу. Система динамічних ЦВЗн активно інтегрується в системи медіаобробки даних. ЦВЗн може представляти як чутливу інформацію у вигляді напіввідкритої стеганосистеми, так і унікальний ідентифікатор для виявлення авторського права. Засоби стеганографії мають багатофункціональні властивості для реалізації політики безпеки.

Реалізований макет веб-додатку є прикладним варіантом реалізації стеганографічних інструментів у парадигмі мереж. Аналізована тематика активно досліджується у науковій призмі. Приховування інформації є доповнюючим механізмом до криптографічних кодів. Оптимальним фундаментом для реалізації системи безпеки. Літературні джерела [4, 7, 8, 13] пропонують варіації експлуатації методів інкапсуляції даних у потокові контейнери.

Стеганографічна парадигма [27] має широкий спектр застосувань. Механізми приховування даних охоплюють сектори [2, 6, 11] від розвідки та військових галузей до механізмів права інтелектуальної власності. Наука приховування [12] пропонує потужний арсенал для узгодження підходів безпеки ІзОД. Представляє додатковий механізм для комплексності захисту.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Стратегія кібербезпеки України (2021 – 2025 роки) : проект /Рада національної безпеки і оборони України. Режим доступу: https://www.rnbo.gov.ua/files/2021/STRATEGIYA KYBERBEZPEKI/proekt strategii_kyberbezpeki_Ukr.pdf (дата звернення: 27.10.2025).

2. Кузнецов О. О., Євсеєв С. П., Король О. Г. Стеганографія : навчальний посібник. Харків : ХНЕУ, 2011. 232 с.

3. Конахович Г. Ф., Прогонов Д. О., Пузиренко О. Ю. Комп'ютерна стеганографічна обробка й аналіз мультимедійних даних : підручник. Вінниця, 2018. 558 с.

4. Djebbar F., Ayad B., Meraim K. A. et al. Comparative study of digital audio steganography techniques. J AUDIO SPEECH MUSIC PROC. 2012. Issue 25. P. 2-16. DOI: 10.1186/1687-4722-2012-25. Режим доступу: https://doi.org/10.1186/1687-4722-2012-25 (Last accessed: 08.10.2025).

5. Хорошко В. О., Яремчук Ю. Є., Карпінець В. В. Комп'ютерна стеганографія: навчальний посібник. Вінниця, 2017. 155 с.

6. Bodnia M., Yesina M., Ponomar V. Researching the possibilities of using steganographic and cryptographic algorithms for information hiding // Computer Science and Cybersecurity. 2023. № 2. С. 43-57. DOI: https://doi.org/10.26565/2519-2310-2023-2-05. Режим доступу: https://ieeexplore.ieee.org/document/6398182 (Last accessed: 20.10.2025).

7. Singh P. A Comparative Study of Audio Steganography Techniques. International Research Journal of Engineering and Technology (IRJET). 2016. Vol. 3, №. 4. P. 580-585.

8. Hajer M., Anbar M. Identifying optimal message embedding location in audio steganography using generative adversarial networks. EEJET. Vol. 4, No. 9(118), P. 59–68. DOI: https://doi.org/10.15587/1729-4061.2022.263695. (Last accessed: 20.10.2025).

9. Введення в дискретне перетворення Фур'є: Studfile : веб-сайт. Режим доступу: https://studfile.net/preview/9576514/page:25/ (дата звернення: 10.11.2025).

10. Learn Discrete Fourier Transform (DFT). Medium : website. Режим доступу: https://medium.com/data-science/learn-discrete-fourier-transform-dft-9f7a2df4bfe9 (Last accessed: 20.10.2025).

11. Лімонов О. С. Цифрова обробка сигналів : конспект лекцій. Одеса: ОДЕКУ, 2011. 121 с.

12. Singh P., Singh H., Saroha K. A Survey on Steganography in Audio. Proceedings of the 3rd National Conference, INDIACo m-2009. 2015 P. 1-7. Режим доступу: https://www.researchgate.net/publication/266418653_A_Survey_on_Steganography_in_Audio (Last accessed: 10.11.2025).

13. Kuznetsov A., Onikiychuk A., Peshkova O., Gancarczyk T., Warwas K., Ziubina R. Direct Spread Spectrum Technology for Data Hiding in Audio. Sensors. 2022. Vol. 22(9), № 3115. P. 1-23. Режим доступу: https://doi.org/10.3390/s22093115 (Last accessed: 10.11.2025).

14. Kirovski D., Malvar H.Spread-Spectrum Watermarking of Audio. Signal Processing, IEEE Transactions on. 51. 2003. Vol. 51, № 1020-1033. P. 3-13. DOI: 10.1109/TSP.2003.809384.

15. Kuznetsov A., Smirnov O., Zhora V., Onikiychuk A., Pieshkova O. Hiding Messages in Audio Files Using Direct Spread Spectrum. 2021 11th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS). 2021. P. 414-418. DOI: 10.1109/IDAACS53288.2021.9660879.

16. Kuznetsov A., Smirnov O., Kiian A., Kuznetsova T. Data hiding based on noise-like signal addressing. Radiotekhnika. 2020. Vol. 4(203). P. 38–49. Режим доступу: https://doi.org/10.30837/rt.2020.4.203.04 (Last accessed: 10.11.2025).

17. Смірнов О., Арищенко А., Деменко Є., Онікійчук О., Кузнецов О. Pseudorandom Sequences for Spread Spectrum Image Steganography // Computer Science and Cybersecurity. 2020. № 4. С. 4-10.

18. Ipatov V.P. Spread Spectrum and CDMA: Principles and Applications. John Wiley & Sons, Ltd.: Chichester. UK. 2005. Режим доступу: https://content.e-bookshelf.de/media/reading/L-568753-8bd6d7891d.pdf (Last accessed: 13.11.2025).

19. Горбенко І. Д., Горбенко Ю. І. Прикладна криптологія: підручник. Форт, 1 та 2 видання. Харків, 2013. 878 с.

20. Горбенко І. Д., Замула О. О., Семенко А. Е., Морозов В. Л. Метод комплексного покращення характеристик ортогональних ансамблів на основі мультиплікативного об'єднання сигналів різних класів. Radiotekhnika. Вип. 187. С. 43–53.

21. Кузнецов О. О., Ботнов А. М., Лаптий П. О. Вбудування інформаційних даних в нерухомі зображення з використанням прямого розширення спектра. Прикладна радіоелектроніка: наук.-техн. журнал. 2010. № 3. Режим доступу: https://openarchive.nure.ua/server/api/core/bitstreams/e948d82c-734a-4844-9faf-b3a40d9d9e23/content (дата звернення: 16.11.2025).

22. Стасєв Ю.В. Основи теорії побудови сигналів: навч. посіб. Харків: ХВУ, 1999. 87с.

23. Стасєв Ю. В., Сійчук А. Ю., Костиленко К. Ю., Манакова О. В. Алгоритми побудови дискретних ортогональних сигналів на основі матриць Адамара. Системи озброєння і військова техніка. 2021. Вип. 67, № 3. С. 113-118. DOI: 10.30748/soivt.2021.67.15.

24. Приховування даних в аудіо сигналах, основні методи. Studfile : веб-сайт. Режим доступу: https://studfile.net/preview/9650052/page:12/ (дата звернення: 17.11.2025).

25. Майданюк В. П. Кодування та захист інформації: навчальний посібник. Вінниця: ВНТУ, 2009. – 164 с.

26. Взаємні та автокореляційні функції сигналу. UM.CO : веб-сайт. Режим доступу: http://www.um.co.ua/4/4-16/4-163414.html (дата звернення: 21.11.2025).

27. Fridrich J. Steganography in Digital Media. Cambridge University Press. 2014. Режим доступу: https://doi.org/10.1017/CBO9781139192903 (Last accessed: 22.11.2025).

28. Смірнов О., Горбачова Л., Кузнецов О. Hiding information in images using pseudo-random sequences // Computer Science and Cybersecurity. 2020. № 1 (1). С. 4-13. DOI: 10.26565/2519-2310-2020-1-01.

29. Дворников С.В., Дворников С.С., Марков Е.В. Модифіковані імпульсні послідовності на основі кодів Баркера. Праці навчальних закладів зв'язку. 2022. Вип. 8, № 1. С. 8–14. DOI:10.31854/1813-324X-2022-8-1-8-14.

30. Barker R.H. Ground synchronizing of binary digital system. Communication theory. 1953. Vol.7, №2. P.273 –287.

31. Банкет В.Л., Токарь М.С. Композитні коди Баркера. Цифрові технології. 2007. № 2. С. 1-17.

32. Клієнт-серверна архітектура. QATestLAB : веб-сайт Режим доступу: https://training.qatestlab.com/blog/technical-articles/client-server-architecture/ (дата звернення: 22.11.2025).

33. Еталонна модель OSI. Urpylka`s blog : веб-сайт Режим доступу: https://urpylka.com/posts/post-39/ (дата звернення: 22.11.2025).

ДОДАТОК А

ПЕРЕЛІК ВЛАСНИХ ПУБЛІКАЦІЙ

УДК 004.056.5 **DOI:10.30837/rt.2023.3.214.02**

М. О. БОДНЯ, М. В. ЄСІНА, канд. техн. наук, В. А. ПОНОМАР, канд. техн. наук

ОСНОВНІ ОСОБЛИВОСТІ ІНФРАСТРУКТУРИ ВІДКРИТИХ КЛЮЧІВ

Вступ

На сьогодні широко застосуються засоби мережевої інфраструктури та інформаційно-комунікаційні системи для організації спілкування та обміну даними між користувачами. Внаслідок цього виникло питання – як забезпечити автентифікацію всіх авторизованих користувачів. Сучасні криптографічні протоколи автентифікації базуються на криптографії з відкритим ключем. Системи захисту інформації та технічні засоби захисту не можуть повністю гарантувати запобігання несанкціонованому доступу до каналу зв'язку, внаслідок цього реалізовуються різноманітні протоколи та системи автентифікації, що грунтуються на асиметричній криптографії. Застосування технологій та процедур, що засновані на криптографії з відкритим ключем, широко впроваджуються в системи комерційних організацій та урядових установ, тому що вони забезпечують надійний механізм, який дозволяє підтвердити, що особа є тим, за кого себе видає, та реалізувати конфіденційність, цілісність, неспростовність та автентичність інформації.

Як показує практика, застосування асиметричної криптографії є недостатнім комплексом методів та технологій для забезпечення процедури достовірної автентифікації та обміну інформацією між авторизованими користувачами. Суб'єкти комунікації гіпотетично можуть використовувати паперові документи, які містять персональні дані та відкриті ключі авторизованих користувачів, підписані рукописним підписом та завірені нотаріусом. Але в такому випадку виникає проблема масштабності: проведення нотаріального завірення документів для великої множини суб'єктів спілкування потребує великої кількості аркушів паперу та займає багато часу. Інфраструктура відкритих ключів (ІВК) є надійним інструментом для розв'язання задач, пов'язаних з автентифікацією користувачів та визначенням легітимності, справжності відкритих ключів користувачів у цифровому середовищі.

Структура ІВК складається зі спеціалізованих компонентів, кожен з яких має власний напрям діяльності та фіксований спектр задач. При цьому забезпечуються всі процеси відносно управління цифровими сертифікатами, які включають: видачу, перевипуск, відкликання сертифікатів, управління життєвим циклом та ключами сертифікатів тощо. Такі сертифікати підтверджують факт належності певного відкритого ключа конкретному суб'єкту та наявності у відповідного суб'єкта секретного ключа. Завдяки цифровим сертифікатам всі сторони можуть ідентифікувати один одного та безпечно обмінюватись інформацією через мережу. Фальсифікувати облікові дані цифрового сертифіката, видані центром сертифікації, дуже важко, адже цифровий сертифікат підписується особистим ключем центру сертифікації, який відомий лише йому. Цифровий підпис забезпечує цілісність, автентичність та неспростовність відповідного сертифікату.

ІВК є комплексною системою, яка має раціональну структуру та широкий набір функцій, які спрощують процедуру автентифікації та забезпечують її справжність на підставі цифрових сертифікатів. Суб'єкти комунікації можуть повністю не довіряти один одному, але довіряти третій незалежній стороні, яка регулює механізм встановлення довіри між ними. Цей механізм базується на використанні цифрових сертифікатів і криптографії з відкритим ключем та є важливим елементом для забезпечення безпеки та конфіденційності інформації в Інтернеті та інших цифрових середовищах.

ІВК широко застосовується для проведення безпечних електронних транзакцій, банківських операцій, цифровізації та трансформації уряду, державних установ та організацій задля підвищення рівня якості надання послуг та організації комунікації між суспільством та державними органами. Міжнародна спільнота розгортає та модернізує ІВК у вигляді надійного механізму для забезпечення процесу обміну інформацією та комунікації.

Рисунок А.1 – Матеріал публікації

ISSN 2519-2310 Computer Science &Cyber Security, Issue 2(24) 2023

DOI : 10.26565/2519-2310-2023-2-05
УДК 004.056.5

ДОСЛІДЖЕННЯ МОЖЛИВОСТЕЙ ЗАСТОСУВАННЯ СТЕГАНОГРАФІЧНИХ ТА КРИПТОГРАФІЧНИХ АЛГОРИТМІВ ДЛЯ ПРИХОВУВАННЯ ІНФОРМАЦІЇ

Микита Бодня[1], Марина Єсіна[1,2], Володимир Пономар[1,2]

[1]Харківський національний університет імені В. Н. Каразіна, майдан Свободи, 4, Харків, 61022, Україна
bodnia2020kb12@student.karazin.ua, m.v.yesina@karazin.ua ORCID: https://orcid.org/0000-0002-1252-7606
[2]АТ «ІІТ», вулиця Коломенська, 15, Харків, 61166, Україна
Laedaa@gmail.com ORCID: https://orcid.org/0000-0001-5271-2251

Надійшла до редакції 17 листопада 2023 р. Переглянута 18 грудня 2023 р. Прийнята 25 грудня 2023 р.

Анотація: Організація захисту інформації завжди було актуальною задачею особливо після появи інформаційно-комунікаційних систем. Базисними напрямленнями в області захисту інформації, які прийшли зі стародавніх часів є криптографія та стеганографія. Криптографія реалізує захист інформації шляхом перетворення інформації у нечитабельний вигляд. Стеганографія дозволяє приховати інформацію в різних контейнерах, при цьому факт наявності інформації залишається непоміченим для випадкових спостерігачів. У статті розглядаються підходи до криптографії та стеганографії, концепція гібридного застосування криптографічних та стеганографічних методів для забезпечення подвійного рівня захисту даних, загальна архітектура криптографічних та стеганографічних систем. Традиційними криптографічними системами, які застосовуються в сучасних системах захисту інформації є симетричні та асиметричні криптосистеми. Хоча симетричні системи еволюціонували з появою нових математичних перетворень, але вони мають суттєвий недолік. Він полягає в потребі додаткової передачі секретного ключа отримувачу. Така стратегія вимагає використання захищеного каналу зв'язку, оснащеного технічними системами захисту. При цьому існує ризик несанкціонованого доступу, який може спричинити компрометацію секретного ключа. Виходячи з вищенаведених проблем симетричних криптосистем, при розробці механізмів захисту, перевагу віддають асиметричним алгоритмам. Проведено аналіз криптосистеми RSA, яка грунтується на асиметричному підході шифрування. Ця система використовується в сучасних протоколах автентифікації та забезпечення конфіденційності в інформаційних системах та Інтернеті. Проведено дослідження швидкодії програмних модулів генерації ключової пари, шифрування та розшифрування для системи RSA, шляхом зміни загальних параметрів алгоритму (модуля перетворень, розміру вихідних даних). Результати часових вимірювань наведені в таблиці, на базі яких побудовані залежності часу від модифікації конкретних параметрів. Досліджено стеганографічний алгоритм модифікації найменш значущого біту (НЗБ), який застосовується для приховування даних в зображеннях. Нині існує широкий спектр стеганоалгоритмів, які розробляються на базі особливостей сенсорних систем людини (системи зору або слуху). Розглядаються властивості зорової системи людини, які використовуються в стеганографії.

Ключові слова: *криптографія, стеганографія, ключ, інформаційне повідомлення, асиметрична криптосистема, симетрична криптосистема, криптограма, стеганограма..*

1.Вступ

Інформація завжди займала провідне місце в житті людини. Поняття «інформація» [1] можна інтерпретувати як сукупність публічно оголошених або документованих відомостей, які охоплюють явища природи, навколишнього середовища та різноманітні області діяльності соціуму й держави. Вагомість і класифікація інформації визначається її вмістом. Поява інформаційно-комунікаційних систем і глобальних мереж спрощує доступність й обмін інформацією. Стрімкий технологічний прогрес призвів до появи загроз несанкціонованого доступу, порушення конфіденційності, цілісності інформації, фальсифікації даних тощо. Поряд з цим питання забезпечення інформаційної безпеки (ІБ) завжди було актуальним, починаючи зі стародавніх часів і до теперішнього моменту. Основними напрямами, що впроваджують надійні механізми забезпечення ІБ є криптографія і стеганографія [2].

Для розв'язання проблем ІБ широко використовуються відповідні алгоритми криптографії і стеганографії. Сучасні системи ІБ розробляються з реалізацією перспективних криптографічних і стеганографічних методів захисту. Система інформаційної безпеки (СІБ) [1]

Рисунок А.2 – Матеріал публікації

УДК 004.056.5 **СЕКЦІЯ 2**

БОДНЯ М. О., НАРЄЖНІЙ О. П.

ПРОГРАМНО-АПАРАТНА ПЛАТФОРМА ДЛЯ ДОСЛІДЖЕННЯ ШУМОВИХ ТОНАЛЬНИХ КАНАЛІВ

Subject of work. Development of a software and hardware complex for researching covert communication methods in acoustic channels.
Goal. Investigation of the application of steganographic technologies for building a defense strategy.
Investigation methods. The key methods are the analysis and comparison of various tools and techniques, as well as literary sources related to steganographic principles of protection building. The comparison is based on a dataset and theoretical information.
The results. The developed model simulates a communication system that incorporates modern security mechanisms. The cybersecurity strategy of the web application involves the integration of various algorithms. Next steps include the implementation of the hardware component and the enhancement of the prototype's functional capabilities. The software product simulates the formation of a secure communication system for researching acoustic channels. The web application architecture is supplemented with a steganographic device containing cryptographic elements. An option for selecting a steganographic encoding method within the container is supported. The graphical diagram of the steganographic apparatus reveals the essence of the developed technology. The application of acoustic steganography methods has demonstrated high efficiency and promise in the information protection paradigm.
Conclusions. Improving security policy is a sensitive issue. This fact is confirmed by the formation of the updated Cybersecurity Strategy of Ukraine. The defense strategy includes a symbiosis of cyber defense vectors. Steganographic architecture, as a reliable communication system, is an additional layer to cryptographic ciphers. The effectiveness of a steganographic procedure is determined by the quality of embedding and the impossibility of detecting the embedded media content. Acoustic channels offer a number of advantages over other steganographic systems. Steganographic technologies are being actively applied in innovative models. The choice of algorithm and procedure parameters are determining aspects in the embedding process.

Key words: *audiosteganography, signal, acoustic channel, human auditory system, software and hardware complex, information security.*

Вступ

Вдосконалення технологій захисту інформації обумовлене [1] зростанням експлуатації Інтернету серед соціуму. Інтеграція технічних систем динамічно протікає у критичні сектори життєдіяльності. На тлі міжнародного протистояння, кібербезпека стає пріоритетом національного масштабу.

Безпечність інформаційного простору є актуальним питанням у системі національної безпеки України. Формування оновленої Стратегії кібербезпеки України [2], направлене на посилення здатності національної парадигми кіберзахисту протидіяти потенційним загрозам. Розширення технічного інструментарію кібератак негативно впливає на ключові сфери функціонування. Цифровий простір класифікується як один з ландшафтів ведення військових конфліктів, тому концепція кібербезпеки грає стратегічне значення. Нині, базовими напрямленнями інформаційного захисту [1] є криптографія, стеганографія та цифрові водяні знаки.

Стеганографія – це наука, що вивчає методи та способи [3, 4] приховування даних в медіа об'єктах. При цьому приховується факт існування інформації в контейнері для необізнаних спостерігачів. Стеганографія доповнює криптографічні алгоритми [4] для посилення ефективності моделі захисту. Методи конструювання акустичних каналів динамічно розвиваються у схемі прихованого зв'язку. Звукові контейнери мають багато переваг [3-6], що виділяють їх поміж інших медіа об'єктів. Акустична стеганографія трансформує звуковий потік, доповнюючи його інформаційним шумом неномітним чином.

Постановка задачі та теоретична база

Контейнер, який використовується для монтування інформації – акустичний сигнал. Аудіооб'єкти мають позитивні властивості, які дозволяють вбудовувати великі обсяги інформації. Секретне повідомлення підмішується в аудіопотік, що передається по каналу зв'язку. Неможливість виявлення інформації повинна залишатися при обробці та аналізі заповненого контейнеру. Незначний запис інформаційного контенту імітує природний шум.

Рисунок А.3 – Результати конференції

Секція 1

АЛГОРИТМ РОЗШИРЕННЯ СПЕКТРУ ДЛЯ ПРИХОВАНОГО ЗАПИСУ ЦИФРОВИХ ВОДЯНИХ ЗНАКІВ В АУДІОСИГНАЛИ

Бодня М. О.
Харківський національний університет ім. В. Н. Каразіна
Науковий керівник: Нарежній О. П.

Актуальність. На тлі порушення авторського права реалізація механізмів цифрових водяних знаків (ЦВЗн) є необхідним напрямом. Даний механізм є гарантією забезпечення захисту інтелектуальної власності. Вектор приховування інформації є оптимальною альтернативою криптографічним кодам [1] в умовах обмежених обчислювальних потужностей. Стеганографічна функція монтує цифровий ідентифікатор в структурну збитковість медіа об'єктів. Застосування базових операцій для маніпуляції над контейнером є перевагою технологій приховування. Інженери кібербезпеки досліджують технології модернізації моделей стеганографії для інтеграцію їх в автоматизовані системи. Моделі приховування мають варіаційні вектори застосування в парадигмі інформаційної безпеки. Принцип стеганографії активно досліджується у науковому просторі. Динаміка експериментів стеганографічних засобів набула революційного імпульсу.

Метою даної роботи є особливості та ідея методу розширення спектру для непомітного запису ЦВЗн або іншого інформаційного контенту в звуковий потік.

Основні положення. Методи стеганографічного кодування базуються [1-3] на особливостях слухової системи людини (ССЛ). Експлуатація властивостей ССЛ застосовується для побудови правильної структури методу приховування. Технологія розширення спектру призначена для модуляції передавального сигналу шляхом його розсіювання по частотному спектру. Вилучення сигналу можливе навіть при існуванні завад. Основна концепція технології спектрального розширення – розчинити інформаційний артефакт по частотному спектру в допустимих межах. Застосування технології позитивно впливає на цілісність посилки. Оскільки за рахунок рознесення інформаційного сигналу по частотній смузі підвищується складність знищення. Перевага розширення спектру полягає в реалізації одночасної передачі декількох біт інформації в межах часового інтервалу. Підхід породжує ортогональну систему [3], що організує модель багатокористувацького доступу. Множинний доступ із кодовим поділом заснований на розширенні спектру кодовою

Рисунок А.4 – Результати конференції

ДОДАТОК Б

ДИНАМІКА ДОСЛІДЖЕННЯ НАУКОВОЇ ПРОБЛЕМИ

Зростання перспективи застосування [4] технічних систем викликало потребу в побудові моделей захисту. В силу високих обчислювальних вимог та масивних ресурсних потреб [27] криптографічних комплексів виникла потреба в альтернативі. Стеганографічна парадигма [2] вивчається як оптимальна заміна алгоритмам криптографії, так і резервний механізм захисту інформації. Методологія розширення спектра породжує багатоканальну систему комунікації на основі кодового поділу. Система зв'язку [15] реалізується в структурній надмірності медіаоб'єкту та призначена для прихованого зв'язку. В джерелі [13] розглядаються основні аспекти застосування такого сценарію стеганографії в середі звукового файлу. Методологія розширення спектра [11, 13, 15] використовується в системах передачі інформації, радіозв'язку, глобального призначення та бездротових мережах. Підхід гарантує надійність та конфіденційність інформаційних пакетів. Технологія передбачає модуляцію двійкового алфавіту [13-16] в слабокорельованих сигналах, що надає повідомленню шумоподібний вигляд. Алгоритм є популярний в призмі наукових досліджень, оскільки застосований до систем воєнного призначення та авторського права. Він також придатний для впровадження у широкий перелік мультимедійних об'єктів (відеофайли, звукові потоки, цифрові зображення тощо). Дискретні сигнали, які виступають в якості секретного ключа та є ідентифікатором окремого каналу володіють властивостями випадковості. Висуваються високі вимоги до генерації таких дискретних послідовностей. Фахівці у сфері захисту інформації розглядають похідні реалізації технології із різними способами генерації кодових послідовностей. Також розробляється [4] інструмент реалізації методології розширення спектра в технічних системах прихованого запису. Завдання приховування [13] даних інтерпретується як передача сигналу по каналу спілкування з шумом, де у ролі шуму виступає сам мультимедійний контейнер.

Особливий інтерес проявляється в структурі кодових послідовностей [15, 20], які використовуються в процедурі. Основна мета досягти низького рівня BER для відправленої інформації. При цьому забезпечити властивість непомітності та оптимальну пропускну спроможність стегаканалу. Актуальність дослідження [4] зумовлена необхідністю захисту авторських прав та забезпечення прихованої передачі даних у відкритих КЗ. А також високою потребою в інноваційних підходах до захисту даних. Ключова проблема, виявлена авторами [13-17], полягає в тому, що реальні мультимедійні дані (на відміну від «білого шуму») мають високу внутрішню кореляцію і надмірність. Це порушує базову умову ортогональності сигналу та шуму [15], що при використанні стандартних псевдовипадкових послідовностей призводить до високого рівня помилок при вилученні даних. Основна мета оптимізації [13] дискретних сигналів направлена на зниження рівня помилок бітів даних. Зниження рівня помилок досягається через вибір правильного методу формування розширюючих послідовностей. В якості перспективного напрямку оптимізації розглядається використання адаптивних дискретних послідовностей [13-17], які враховують статистичні властивості конкретного контейнера. Це дозволяє ще суттєвіше знизити BER або навіть отримати практично безпомилкову передачу. Підбір послідовностей здійснюється з розрахунком на наближення до нуля рівня кореляції з цифровим об’єктом.

На відміну від криптографії, яка шифрує вміст, або ЦВЗн, які захищають авторські права, стеганографія забезпечує таємну комунікацію. Арсенал стеганографії [6] породжує канал спілкування між абонентами, що непомітний для необізнаних спостерігачів. Стеганографічні кодери [2, 4] є проміжним шаром в системі спілкування. При динамічному формуванні потокового контенту [4] встановлена приставка стеганографії (рис. Б.1) здійснює вбудування інформації. Монтування даних здійснюється в просторовій області мультимедійних носіїв. Концепція вбудування формується на основі фізіологічних та психологічних особливостей систем сприйняття людини.

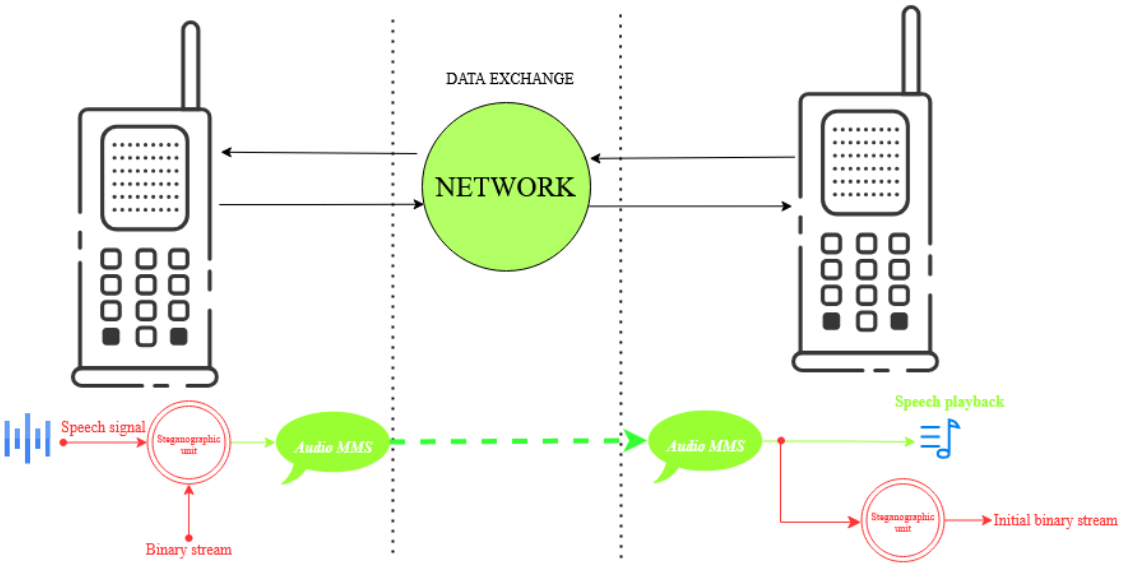


Рисунок Б.1 – Модель системи прихованого зв’язку

Позитивними сторонами методу розширення спектра є високий рівень надійності в умовах шумів та зовнішніх впливів. Алгоритм стійкий проти шумового впливу та інтерференції. Володіє стійкістю [13] проти навмисного та природного спотворення потокового носія. На основі розширення спектра формується багатоканальна архітектура зв’язку, яка використовується кількома абонентами. Застосування ПВП [13-17] як елемента зберігання інформації робить складним процес виявлення прихованих відомостей. При цьому впроваджується резервний механізм захисту на основі секретного ключа. На основі вихідних способів розробляються похідні методи, які направлені на збереження конфіденційності інформації.

Існує необхідність забезпечення авторського права у цифрових об’єктах. Технологія розширення спектра унеможливлює видалення ЦВЗн без помітного спотворення сигналу. Такі мітки [2] можуть використовуватися для підтвердження права власності. Технології приховування в акустичних каналах використовуються для таємного спілкування та механізмів автентифікації.

ДОДАТОК В

МОДЕЛІ РОЗРОБОК ТА ДОСЛІДЖЕНЬ

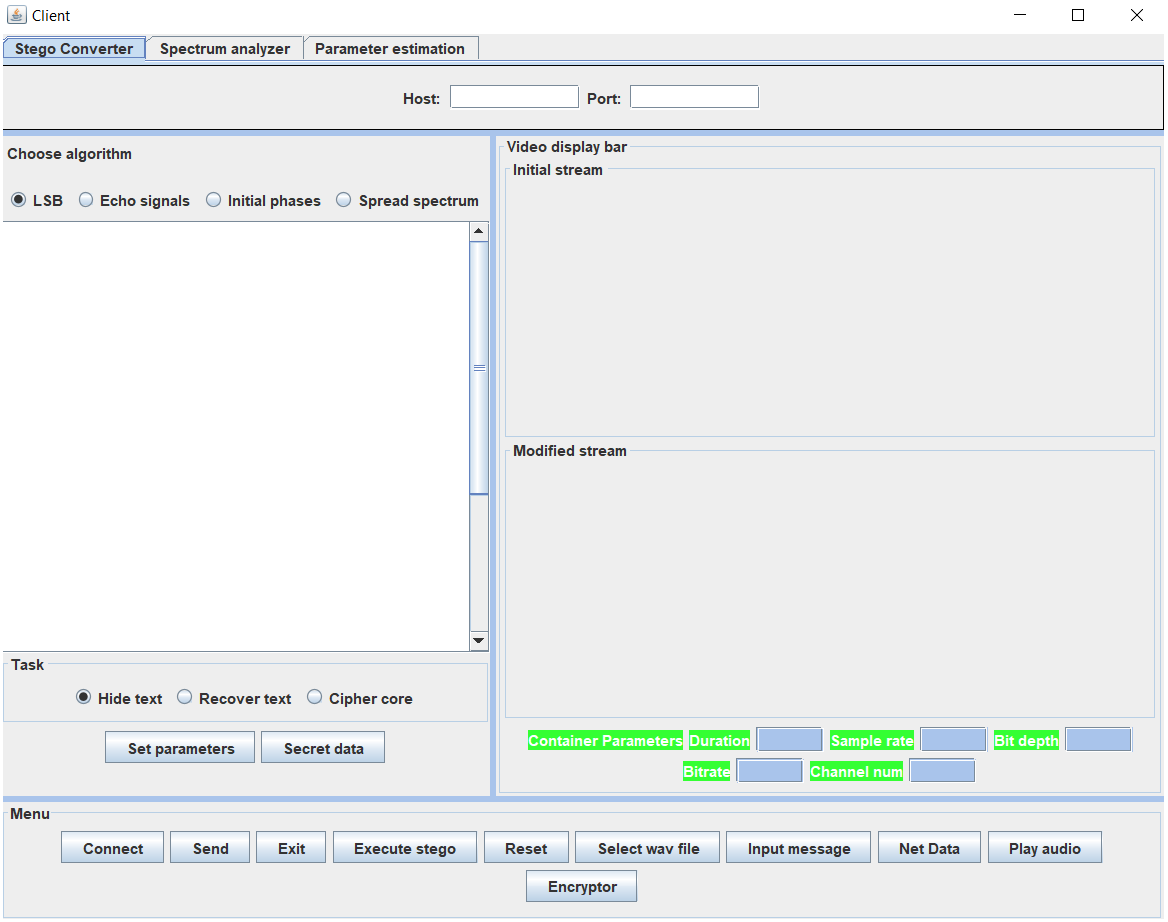


Рисунок В.1 – Інтерфейс веб-додатку

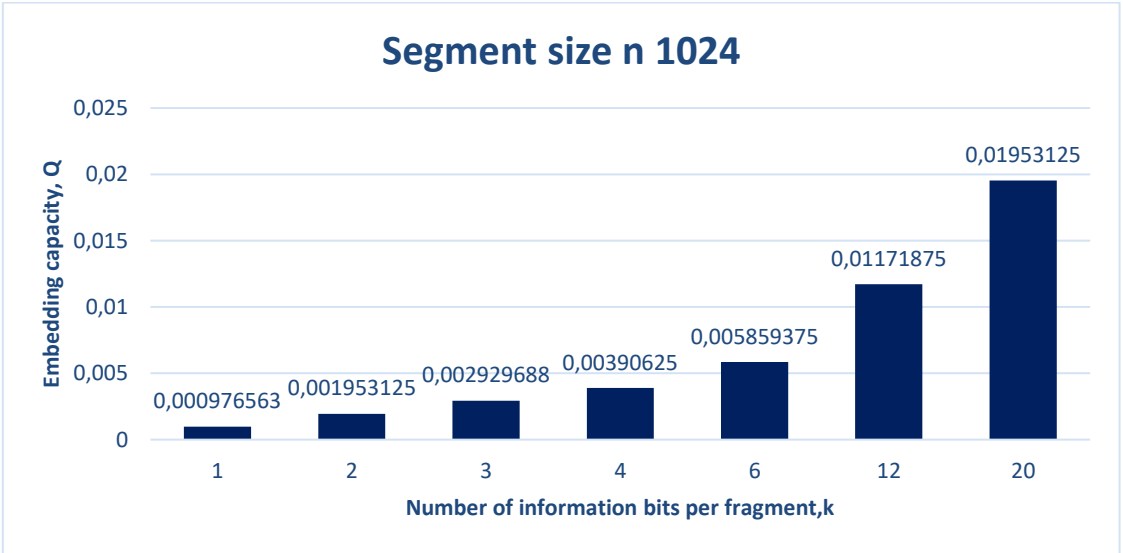


Рисунок В.2 – Пропускна спроможність стегаканалу для *n* 1024 біт

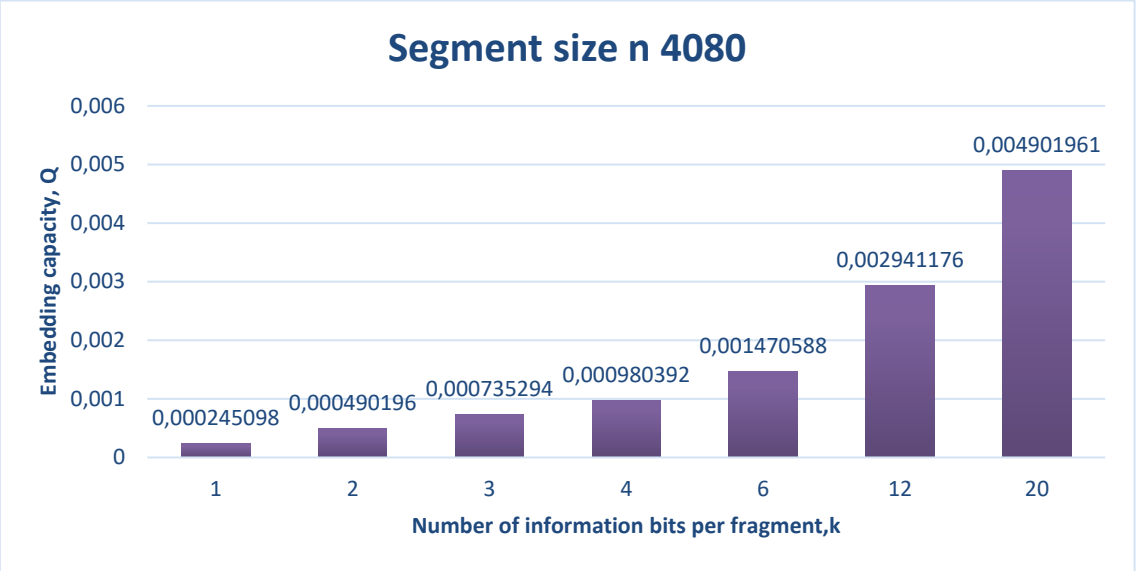


Рисунок В.3 – Пропускна спроможність стегаканалу для *n* 4080 біт

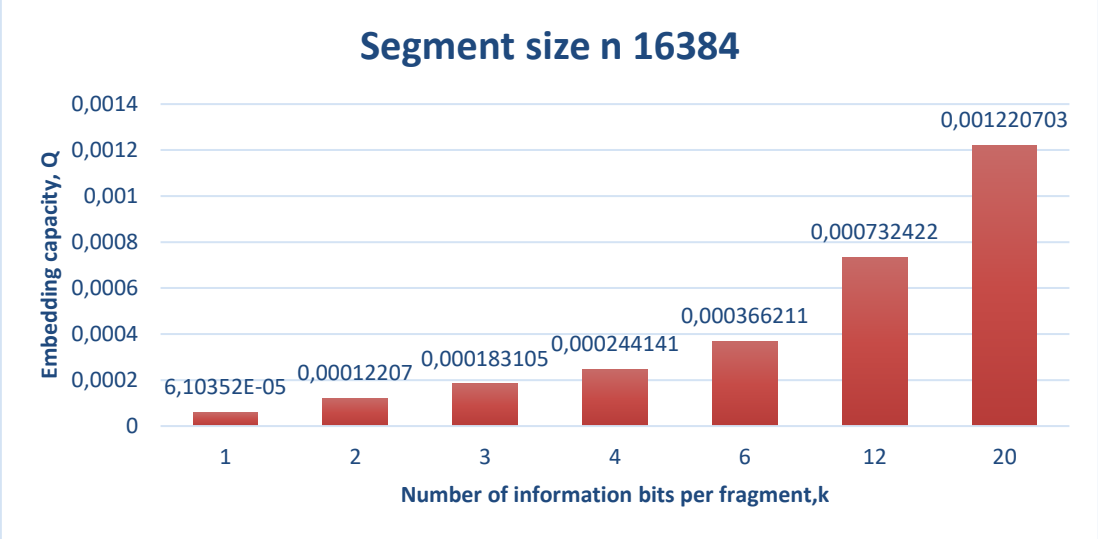


Рисунок В.4 – Пропускна спроможність стегаканалу для *n* 16384 біт

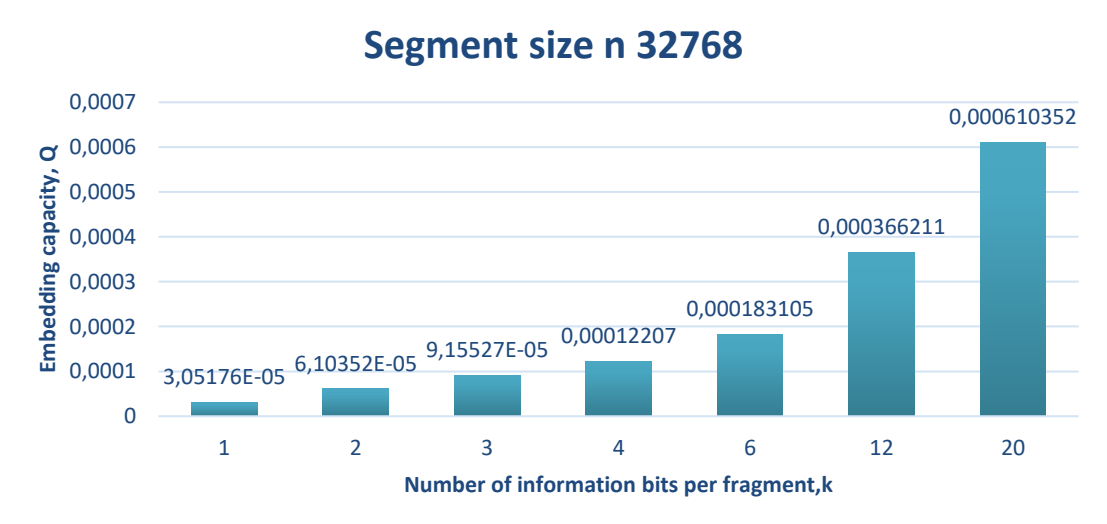


Рисунок В.5 – Пропускна спроможність стегаканалу для *n* 32768 біт

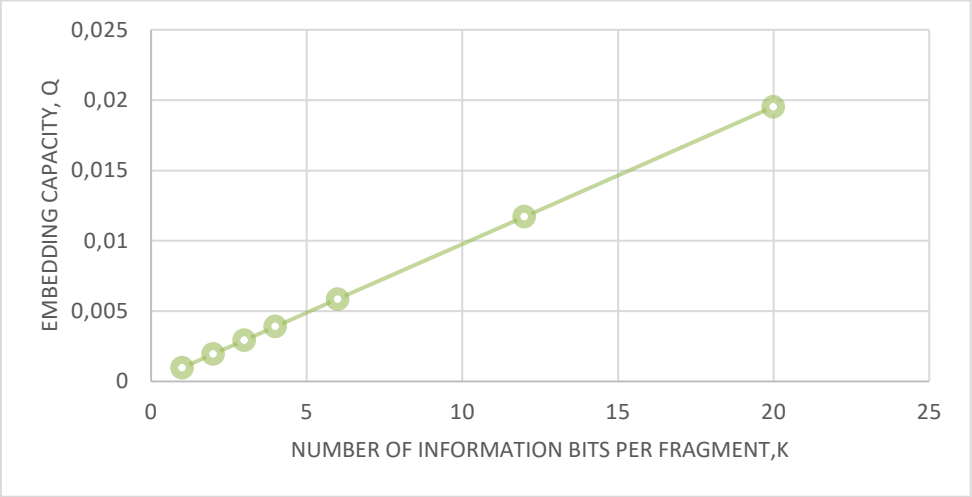


Рисунок В.6 – Залежність $Q(k)$

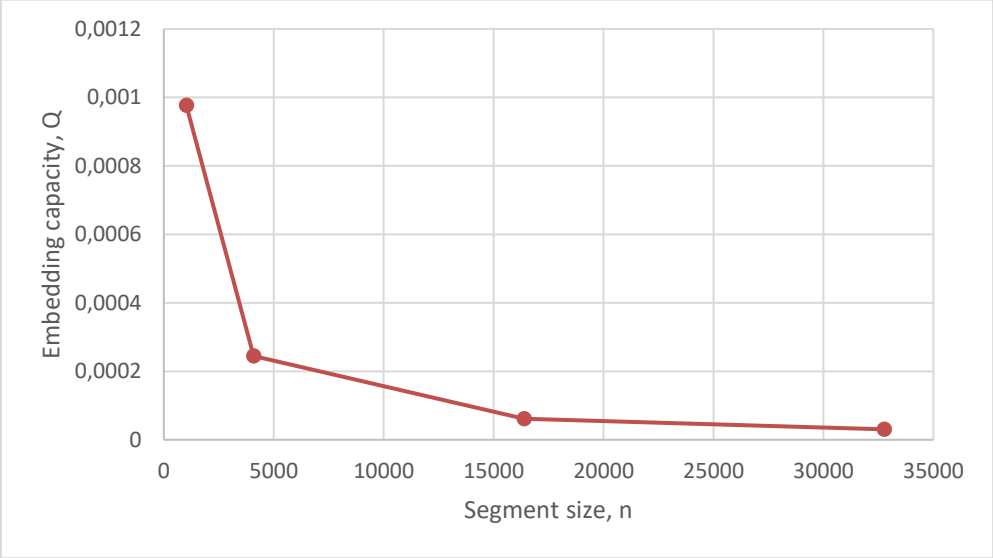
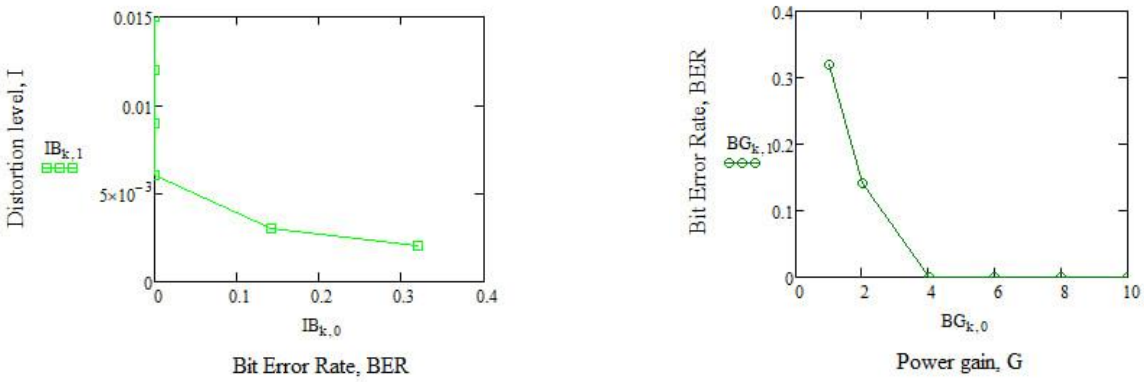


Рисунок В.7 – Залежність $Q(n)$



а *б*

Рисунок В.8 – Залежності (а) $I(BER)$ (б) $BER(G)$

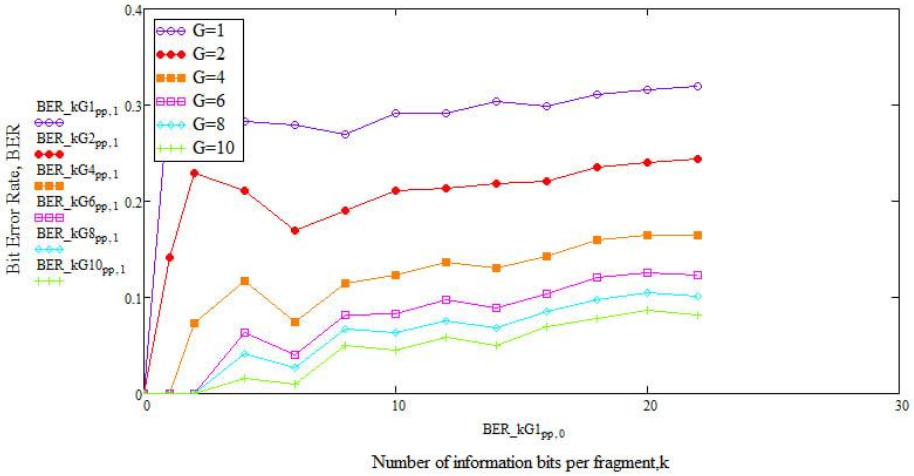


Рисунок В.9 – Графік емпіричної оцінки BER(k)

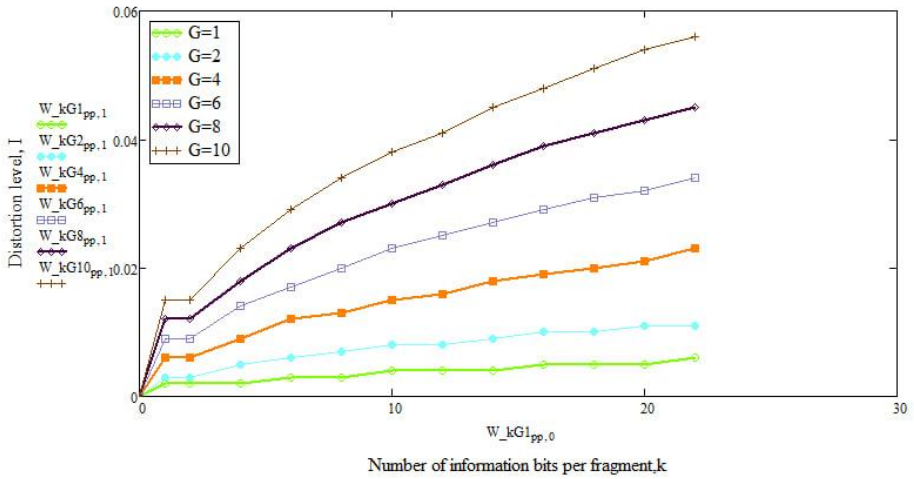


Рисунок В.10 – Графік емпіричної оцінки $I(k)$

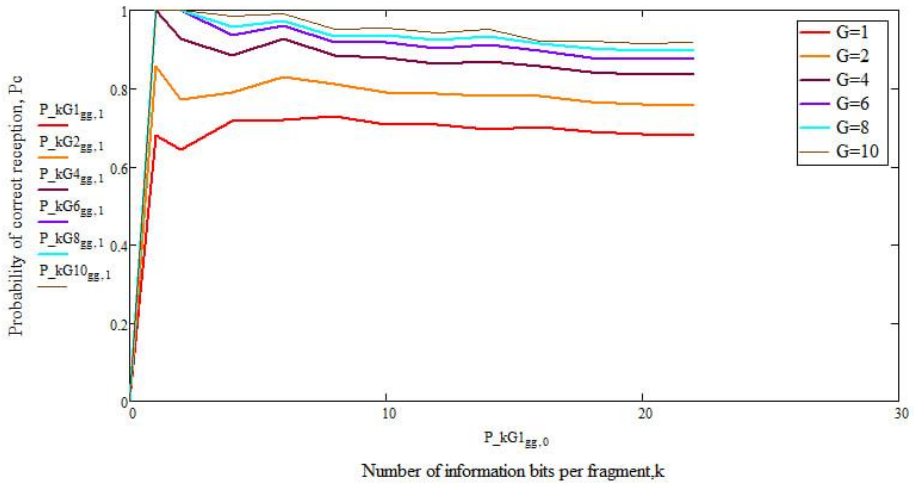


Рисунок В.11 – Графік емпіричної оцінки $P_{б.п.}(k)$

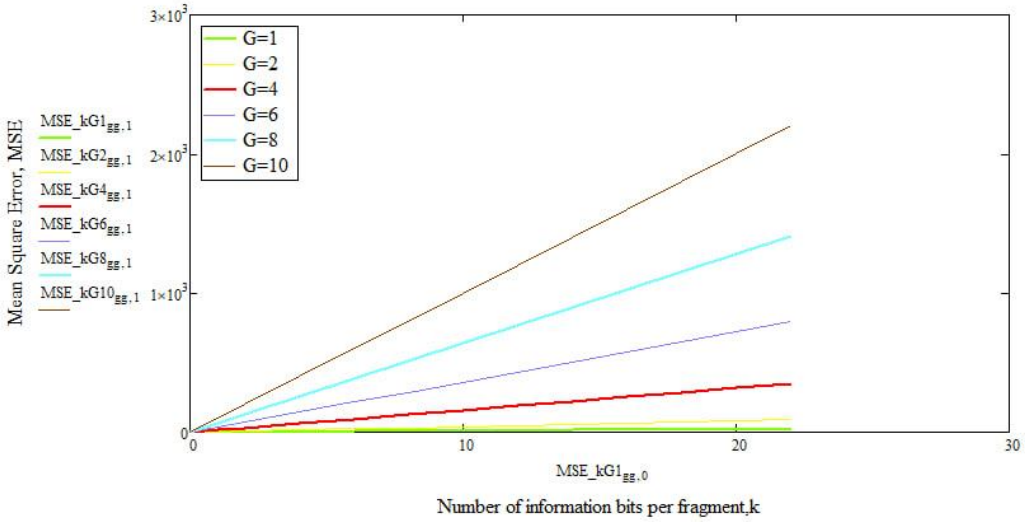


Рисунок В.12 – Графік емпіричної оцінки *MSE*(*k*)

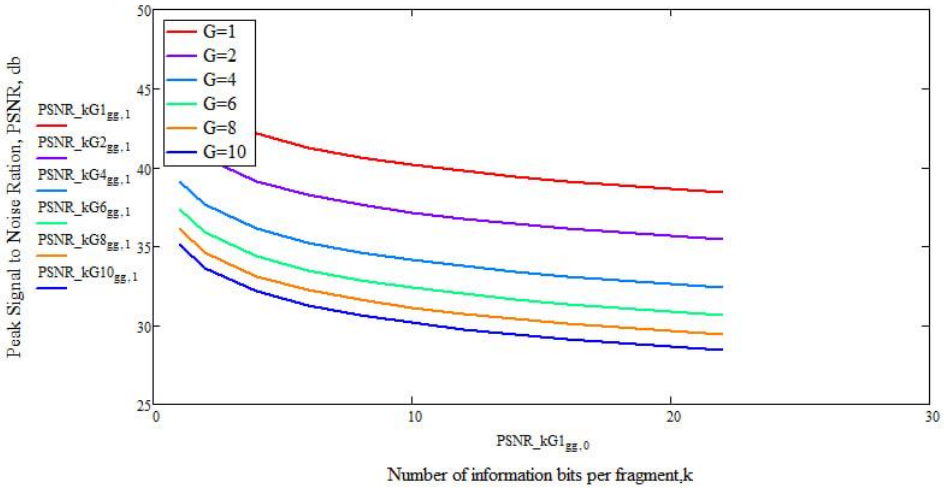


Рисунок В.13 – Графік емпіричної оцінки *PSNR*(*k*)

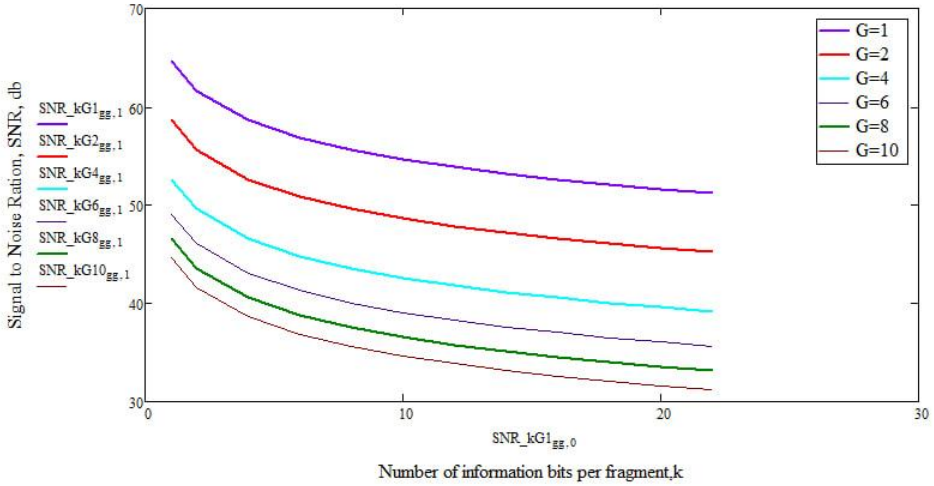
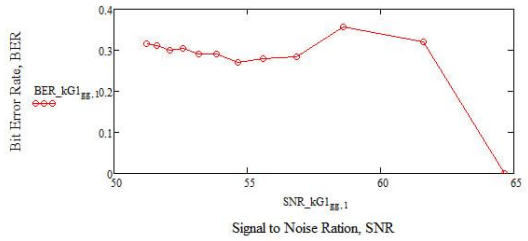
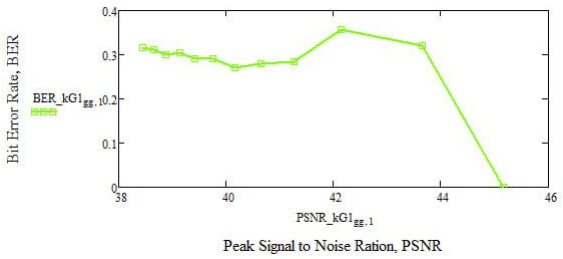


Рисунок В.14 – Графік емпіричної оцінки *SNR*(*k*)



а)



б)

Рисунок В.15 – Графік емпіричної оцінки (а) *BER*(*SNR*) (б) *BER*(*PSNR*)

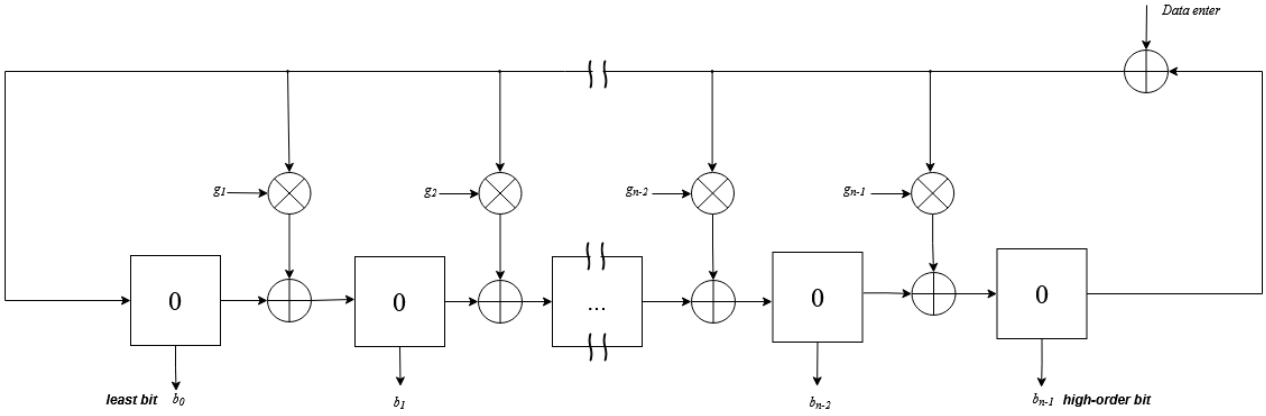
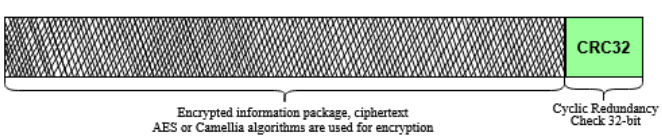
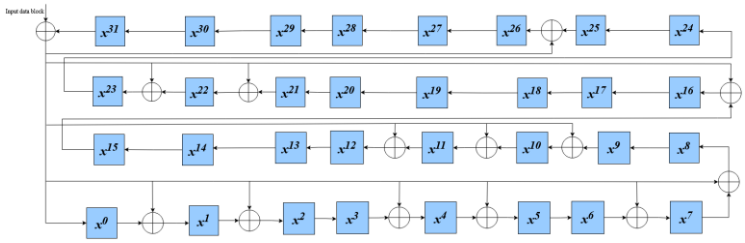


Рисунок В.16 – Правило генерації CRC





а) *б)*

Рисунок В.17 – Структурні схеми (а) інформаційного пакету (б) регістру зсуву з лінійним зворотним зв'язком CRC-32

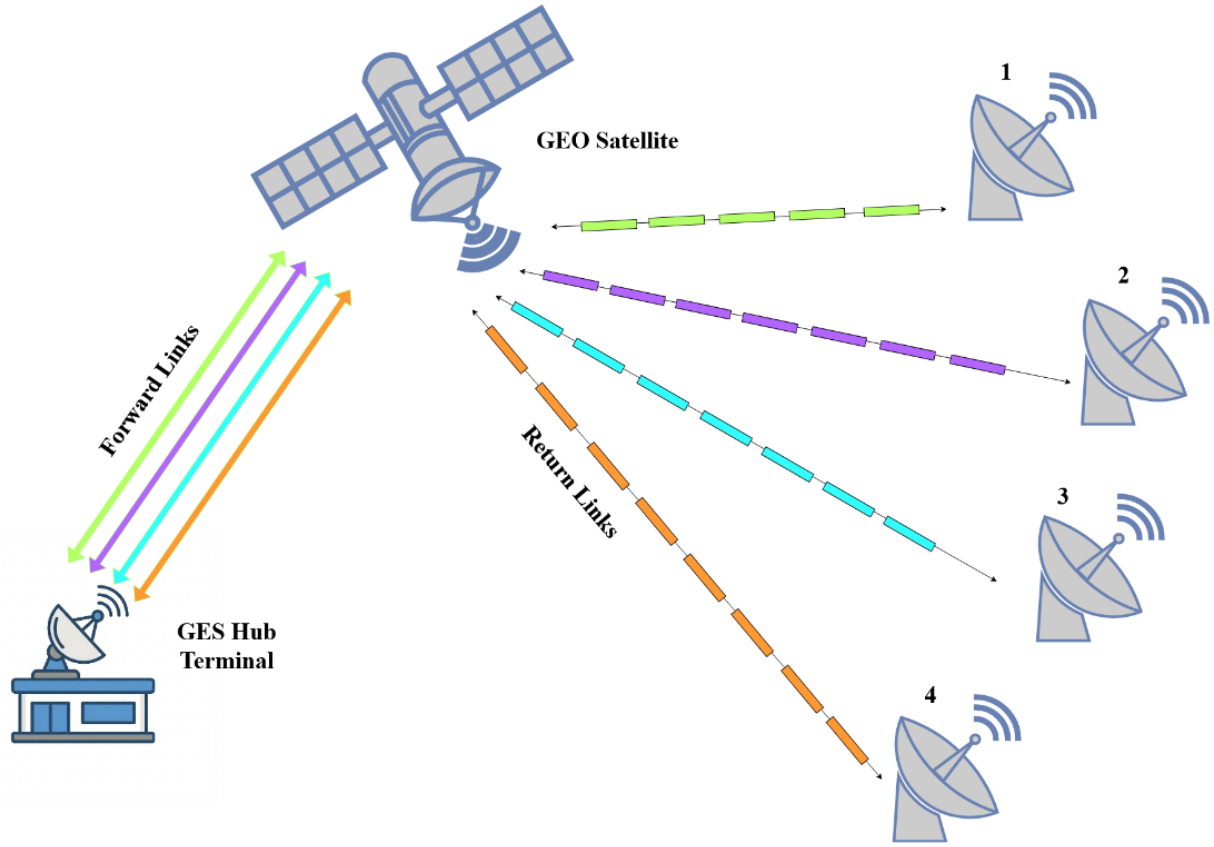
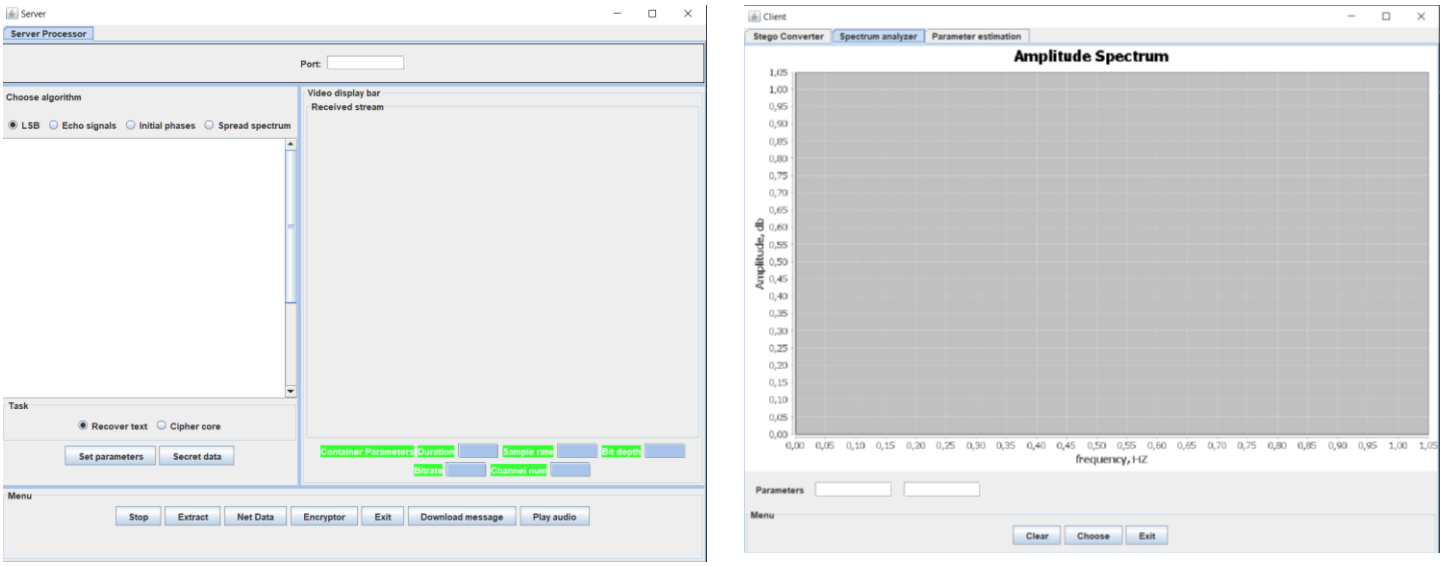


Рисунок В.18 – Сутність кодового розділення каналів



а *б*

Рисунок В.19 – Веб-сервіси програмно-апаратного комплексу (а) серверна частина (б) спектральний аналізатор