Міністерство освіти і науки України
Тернопільський національний технічний університет імені Івана Пулюя

Факультет прикладних інформаційних технологій та електроінженерії
(повна назва факультету)
Кафедра радіотехнічних систем
(повна назва кафедри)

КВАЛІФІКАЦІЙНА РОБОТА

на здобуття освітнього ступеня

магістр
(назва освітнього ступеня)

на тему: Дослідження системи 16-CPSK модуляції з хаотичними генераторами для бездротових комунікацій на FPGA

Виконав(ла): студент(ка) 6 курсу, групи РАм-62
спеціальності 172 Електронні комунікації та радіотехніка
(шифр і назва спеціальності)

(підпис) Федчишин В.Р. (прізвище та ініціали)

Керівник (підпис) Дунець В.Л. (прізвище та ініціали)

Нормоконтроль (підпис) Хвостівська Л.В. (прізвище та ініціали)

Завідувач кафедри (підпис) Дунець В. Л (прізвище та ініціали)

Рецензент (підпис) (прізвище та ініціали)

Тернопіль 2024

Міністерство освіти і науки України
Тернопільський національний технічний університет імені Івана Пулюя

Факультет прикладних інформаційних технологій та електроінженерії
(повна назва факультету)

Кафедра радіотехнічних систем
(повна назва кафедри)

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____ Дунець В. Л.
(підпис) (прізвище та ініціали)
« » 2024 р.

ЗАВДАННЯ

НА КВАЛІФІКАЦІЙНУ РОБОТУ

на здобуття освітнього ступеня магістр
(назва освітнього ступеня)

за спеціальністю 172 Електронні комунікації та радіотехніка
(шифр і назва спеціальності)

студенту Федчишину Віталію Руслановичу
(прізвище, ім'я, по батькові)

1. Тема роботи Дослідження системи 16-CPSK модуляції з хаотичними генераторами для зменшення завад у бездротових комунікаційних системах на базі FPGA

Керівник роботи Дунець Василь Любомирович, к.т.н., доц.
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

Затверджені наказом ректора від « 29 » листопада 2024 року № 4/7-1145.

2. Термін подання студентом завершеної роботи

3. Вихідні дані до роботи Об'єкт дослідження: Процес передачі енергії безпровідним шляхом
Предмет дослідження: Система безпровідної передачі енергії

4. Зміст роботи (перелік питань, які потрібно розробити)
1. Аналітична частина
2. Основна частина
3. Науково - дослідна частина
4. Охорона праці та безпека в надзвичайних ситуаціях

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень, слайдів)
1. Представлення
2. Актуальність теми
3. Розвиток і аналіз технології безпровідної передачі енергії
4. Принцип роботи і аналіз запропонованої технології
5. Наукова новизна
6. Загальні висновки

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Охорона праці	Зелінський І.М., доц. каф. ПВ		
Безпека в надзвичайних	Окіпний І.Б., зав. каф. МТ		
ситуаціях			

7. Дата видачі завдання _____

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів роботи	Термін виконання етапів роботи	Примітка
1	Отримання завдання на виконання роботи		виконано
2	Аналіз отриманого завдання		виконано
3	Виконання розділу 1		виконано
4	Виконання розділу 2		виконано
5	Виконання розділу 3		виконано
6	Виконання розділу 4		виконано
7	Оформлення пояснювальної записки		виконано
8	Оформлення графічного та презентаційного матеріалу		виконано
9	Перевірка кваліфікаційної роботи на антиплагіат		виконано
10	Попередній захист кваліфікаційної роботи		виконано
11	Захист кваліфікаційної роботи		

Студент _____ Федчишин В.Р.
(підпис) (прізвище та ініціали)

Керівник роботи _____ Дунець В.Л.
(підпис) (прізвище та ініціали)

АНОТАЦІЯ

Назва кваліфікаційної роботи: «Дослідження системи модуляції 16-CPSK з хаотичними генераторами для зменшення шумів у системах бездротового зв’язку на основі ПЛІС» // Кваліфікаційна робота // Федчишин Віталій Русланович // Тернопільський національний технічний університет імені Івана Пулюя, факультет приклад. Інформаційних технологій та електротехніки, група РАм-61 // Тернопіль, 2024 // стор. – 56, рис. – 12, табл. – 2, прим. – 1, вих. – 35.

Ключові слова: CPSK; шифрування; FPGA; модуляція; VHDL.

У дисертації представлено результати розробки та аналізу системи шифрування на основі модуляції 16-CPSK (Chaotic Phase Shift Keying), яка використовує хаотичні генератори для підвищення безпеки даних. Особливу увагу приділено реалізації синхронізованих генераторів у конфігурації «master–slave», що забезпечує високу ефективність передачі інформації.

Розроблено методику адаптації системи до мінливих умов роботи шляхом динамічного перенастроювання хаотичних генераторів. Математичне моделювання та апаратну реалізацію системи проводили на платформі FPGA з використанням мови VHDL. Було підтверджено, що використання хаотичних сигналів забезпечує низьку кореляцію між оригінальними та зашифрованими даними, значно покращуючи конфіденційність передачі.

Система демонструє високу адаптивність і стійкість до перешкод, забезпечуючи ефективне шифрування і передачу інформації як у форматах RGB, так і в відтінках сірого. Результати дослідження підкреслюють потенціал розробленої технології для застосування в телекомунікаціях, безпечних обчисленнях і конфіденційній передачі даних.

АНОТАЦІЯ

Title of the Qualification Thesis: "Investigation of a 16-CPSK Modulation System with Chaotic Generators for Noise Reduction in Wireless Communication Systems Based on FPGA" // Qualification Thesis // Vitalii Ruslanovych Fedchyshyn // Ternopil Ivan Puluj National Technical University, Faculty of Applied Information Technologies and Electrical Engineering, Group RAm-61 // Ternopil, 2024 // p. – 56, fig. – 12, tab. – 2, app. – 1, ref. – 35.

Ключові слова: CPSK; шифрування; FPGA; модуляція; VHDL.

The thesis presents the results of the development and analysis of an encryption system based on 16-CPSK (Chaotic Phase Shift Keying) modulation, utilizing chaotic generators to enhance data security. Particular attention is given to the implementation of synchronized generators in a master–slave configuration, ensuring high efficiency in information transmission.

A methodology for adapting the system to changing operational conditions through dynamic retuning of chaotic generators has been developed. Mathematical modeling and hardware implementation of the system were carried out on an FPGA platform using the VHDL language. It has been confirmed that the use of chaotic signals ensures low correlation between original and encrypted data, significantly improving transmission confidentiality.

The system demonstrates high adaptability and resilience to interference, providing efficient encryption and transmission of information in both RGB and grayscale formats. The research findings highlight the potential of the developed technology for applications in telecommunications, secure computing, and confidential data transmission.

ЗМІСТ

ВСТУП

Актуальність теми: У сучасному світі, де інформаційні технології забезпечують глобальну взаємодію між людьми, організаціями та пристроями, питання захисту переданих даних набуває вирішального значення. Розвиток телекомунікаційних систем, зокрема Інтернету, супроводжується підвищенням вимог до обсягу переданої інформації, швидкості передачі та рівня захищеності. У цьому контексті ключовими викликами залишаються ефективність шифрування, стійкість до атак і адаптивність систем до змін у середовищі передачі.

Зростаючі ризики кібератак підкреслюють необхідність розробки нових підходів до шифрування інформації. Існуючі методи, хоча й забезпечують базову безпеку, часто виявляються вразливими до сучасних загроз, таких як аналіз ключів, синхронізаційні атаки та відновлення псевдовипадкових послідовностей. У таких умовах використання хаотичних сигналів стає перспективним рішенням. Хаотичні системи мають низку унікальних властивостей: низьку автокореляцію, широкий спектр частот і детерміновану природу, що ускладнює їх розшифрування. Вони здатні генерувати складні та не повторювані сигнали, що підвищує рівень конфіденційності передачі.

У запропонованому дослідженні основну увагу приділено впровадженню технології 16-CPSK (Chaotic Phase Shift Keying) модуляції для передачі шифрованих зображень. Такий підхід базується на використанні хаотичних генераторів для створення носіїв інформації, які важко зламати через їхню непередбачуваність. Застосування 16-CPSK дозволяє ефективно сегментувати інформацію на 4-бітні пакети, що відповідають різним фазам сигналу, забезпечуючи високу стійкість до перешкод і завад.

Особливістю цього дослідження є реалізація системи на основі FPGA (Field Programmable Gate Array). Цей апаратний підхід забезпечує гнучкість і високу швидкість обробки, дозволяючи синхронізувати генерацію і демодуляцію сигналів у реальному часі. Використання FPGA сприяє оптимізації апаратних ресурсів і

забезпечує надійну синхронізацію за рахунок майстер–підлеглої конфігурації. Рішення продемонструвало високі показники кореляції при обробці RGB і grayscale зображень, підтвердивши свою ефективність у задачах захисту даних.

Практична значущість роботи полягає в її універсальності. Запропонована система може застосовуватись у різних сферах: від передачі конфіденційної інформації в телекомунікаціях до захищеного обміну медичними або науковими даними. Крім того, використання таких рішень дозволяє мінімізувати ризики несанкціонованого доступу та підвищити рівень безпеки в умовах сучасного інформаційного середовища.

Метою роботи є дослідження системи модуляції 16-CPSK для шифрування зображень із використанням хаотичних генераторів.

Об’єкт дослідження: процес шифрування зображень з допомогою модуляції 16-CPSK та хаотичних генераторів.

Предмет дослідження: процеси модуляції 16-CPSK.

Методи дослідження Методи дослідження базуються на основних принципах хаотичних систем, методах цифрового шифрування та модуляції, а також на теорії синхронізації хаотичних генераторів.

Наукова новизна полягає в розробці та реалізації системи шифрування зображень за допомогою модуляції 16-CPSK на основі хаотичних генераторів, що забезпечує високу стійкість до атак і перешкод.

Теоретичне та практичне значення здобутих результатів. Дослідження 16-CPSK модуляції для шифрування зображень із застосуванням хаотичних осциляторів, розрахунок основних параметрів системи з FPGA реалізацією, з врахуванням ефективності шифрування та стійкості до атак.

Публікації:

Струкура роботи: Робота складається із пояснювальної записки. Пояснювальна записка складається із вступу, чотирьох розділів, висновків, переліку використаних джерел. Обсяг роботи: пояснювальна записка - 45 аркушів формату А4.

РОЗДІЛ 1
АНАЛІТИЧНА ЧАСТИНА

1.1. Аналіз наявних систем хаотичного шифрування CPSK.

Використання телекомунікаційних систем забезпечує миттєве глобальне підключення, що дозволяє створювати групи екстреної координації у випадках природних катастроф та надавати віддалене медичне обслуговування. Завдяки передачі даних між людьми, організаціями та пристроями, а також забезпеченню доступу до ринків, ресурсів і інформації, глобальна торгівля стає більш ефективною. З розвитком комунікаційних технологій та Інтернету зростають вимоги до якості послуг, включаючи пропускну здатність та шифрування інформації [1,2].

Крім того, інформація повинна бути захищена від несанкціонованого доступу, що досягається за допомогою різноманітних методів шифрування або маскування, які демонструють високу стійкість у таких умовах [3]. Для підвищення потужності шифрування активно досліджуються носії на основі хаотичних генераторів. Сучасний стан досліджень свідчить, що комунікаційні схеми, засновані на хаосі, зазвичай менш схильні до розшифрування порівняно з традиційними схемами.

У 1963 році метеоролог Едвард Нортон Лоренц випадково відкрив одне з фундаментальних понять теорії хаосу під час роботи над моделями погоди. Завдяки теорії хаосу багато раніше незрозумілих явищ стали зрозумілими. Однією з ключових характеристик хаотичних систем є їхня детермінованість, що означає можливість опису їхньої поведінки за допомогою математичних моделей. Це вказує на те, що вони не є випадковими; однак навіть найменші зміни в початкових умовах або в процесі еволюції системи можуть призвести до експоненційних змін у її поведінці.

Через це бінарна арифметика є практично непередбачуваною, якщо невідомі її складові конфігурації, такі як числовий метод, параметри керування, початкові умови, фіксована чи плаваюча точка, розмір кроку і довжина слова. У літературі, втім,

запропоновано деякі підходи для зменшення втрати ентропії або досягнення максимальної ентропії в хаотичних системах під час їх реалізації [4].

Крім того, хаотичні системи характеризуються низькою автокореляцією, що означає, що сегменти одного й того ж сигналу в різні моменти часу мають різні форми хвиль. Шумоподібні характеристики схем модуляції на основі хаосу також сприяють їх нерегулярності, що може бути використано для досягнення вищого рівня конфіденційності передачі даних. До того ж, хаотичні носії мають широкий частотний діапазон, що робить їх ідеальними для багатоканальних комунікацій [5,6].

Однак у літературі досить обмежена кількість досліджень, присвячених шифруванню з використанням хаотичних послідовностей. У роботі [7] запропонована схема, яка включає чотири основні етапи шифрування зображень: генерацію хаотичної послідовності, шифрування методом Гілла, мережу Фейстеля та дифузію пікселів. У [8] представлено покращений метод захисту тексту ICIC-DNA (Improved Color Image Cipher DNA), заснований на простій структурі. Аналізуючи диференціально, спочатку порушується перестановка основ дезоксирибонуклеїнової кислоти (ДНК), потім знімається шифрування в ДНК-домені, і нарешті використовується еквівалентний ключ для повного дешифрування.

У роботі [9] використовується методологія шифрування за допомогою двох хаотичних генераторів, один із яких базується на квантовій моделі. У [10] автори пропонують алгоритм шифрування кольорових зображень із міжканальним перемішуванням (CCC-IE) на основі діагональної перестановки та двонаправленої послідовної дифузії з використанням 2D гіперхаотичної гібридної карти. Крім того, у [9] описано метод, що дозволяє отримати ключ перестановки шифрування. Потім за допомогою диференціальної атаки досягається повна перевага над системою шифрування з використанням алгоритму Quantum Chaotic Map із ДНК-кодуванням (QCMDC-IEA).

У [11] розроблена покращена двовимірна модульна логістична карта на основі техніки векторних операцій, яка дозволяє шифрувати зображення без необхідності генерації нових ключів або хаотичних послідовностей для кожного нового

зображення. У [12] запропонована дробова хаотична система, заснована на хаотичному генераторі Лоренца, а також двовимірний синусоїдальний хаотичний генератор (2D-SCPM), що став основою для алгоритму шифрування зображень (MIEA-FCSM).

У [13] автори пропонують метод, за яким спочатку звичайне зображення перетворюється в тривимірне (3D), а потім проводяться три етапи: перестановка на рівні площин, фільтрація пікселів на рівні площин і тривимірне хаотичне накладання зображення. Після виконання дискретного логарифмічного перетворення здійснюється випадкова перестановка пікселів для отримання зашифрованого зображення. У [3] описується алгоритм шифрування на основі перестановки, дифузії та фільтрації методом кубика Рубіка, що використовує нелінійні динамічні хаотичні системи для захисту високоякісних зображень, відновлених після стиснення в частотній області за допомогою дискретного косинусного перетворення (DCT).

У [14] представлено схему шифрування зображень, що використовує оптимізацію методом рою частинок (PSO) та модульну вбудовану логістичну експоненційну карту (MILE). Замість шифрування всього зображення, як у традиційних методах, ключ оптимізується для невеликої частини зображення. У [15] автори описують систему передачі зашифрованих зображень із використанням тривимірного хаотичного генератора з чотирма крилами. Система застосовує схему модуляції Chaos Shift Keying (CSK), яка добре задокументована та дозволяє передавати один біт на символ.

Існують також техніки дешифрування та відновлення інформації з хаотичних генераторів. У [16] показано вразливість систем генераторів випадкових чисел (RNG) на основі хаотичних генераторів. Майстер-система та атакуюча система успішно синхронізуються, і відновлюються псевдовипадкові послідовності. У [17] представлено метод криптоаналізу, який дозволяє дешифрувати 12 зображень, зашифрованих хаотичними методами. У [18] описано атакуючу систему, яка синхронізується із схемами хаотичної модуляції, демонструючи вразливості систем із каналом синхронізації.

У [4] запропоновано метод підвищення ефективності реалізації хаотичних систем, зокрема щодо проблем синхронізації, пов’язаних із помилками квантування та обмеженою точністю параметрів. Цей підхід базується на переході до закритих полів Галуа, операціях з системою залишків і скороченому перетворенні до вагової системи числення. У [19] оцінено стійкість комунікаційної схеми до диференціальних атак і атак методом перебору за допомогою показників NPCR (Number of Changing Pixel Rate) та UACI (Unified Averaged Changed Intensity), а також аналізу простору ключів.

Потреба в обробці великих обсягів даних призвела до пошуку нових альтернатив із кращою продуктивністю та меншою ймовірністю дешифрування, зокрема, за допомогою синхронізованих і несинхронізованих хаотичних схем. У [20] розглядаються синхронізовані комунікаційні системи, в яких передавальна система має головний (master) хаотичний генератор, що генерує сигнали для передачі повідомлення. Ці сигнали надсилаються до приймальної системи, яка містить ідентичний хаотичний генератор і синхронізується з головною системою для отримання інформації.

З іншого боку, у [21] описана несинхронізована комунікаційна система, в якій модульований сигнал містить інформацію, необхідну для відновлення переданого повідомлення. У [22] розроблена система, яка шифрує інформацію перед модуляцією і реалізується на FPGA-платформі. Для цього використовуються два хаотичні генератори, які виконують багаторазове шифрування інформації. Недоліком використання декількох хаотичних генераторів є підвищена потреба у логічних ресурсах.

Крім того, у [2] було розроблено генератор, що перемикається між двома різними хаотичними генераторами, використовуючи однакову систему рівнянь і змінюючи лише параметри. Це значно знижує потребу в логічних ресурсах архітектури. У [23] вивчається техніка Differential Chaotic Shift Keying (DCSK), яка використовується для багатокористувацького зв'язку. Її перевага полягає в тому, що для відновлення інформації не потрібна синхронізація між головною і

підпорядкованою системами. Модульований сигнал включає хаотичний опорний чип та інформаційний чип.

У цьому контексті у [24] пропонується багатокористувацька хаотична модуляційна техніка CPSK з синхронізацією "головний–підпорядкований". У передавачі та приймачі використовуються два генератори, і сегменти хаотичних генераторів передаються залежно від бітів інформації. Відновлення повідомлення здійснюється через процес кореляції між отриманим сегментом сигналу та сегментами, що генеруються на приймачі. Результати показали, що техніка CPSK досягла кращих показників ефективності порівняно з технікою Chaos Shift Keying (CSK), представленою в [25]. Перевага техніки CPSK над CSK полягає в фазових зсувів, що використовуються в CPSK, які дозволяють збільшити кількість символів, а отже, розмір кожного інформаційного пакету.

Додатково, у [26] пропонується варіант технік хаотичної модуляції CPSK і DCSK, що отримав назву Quadrature Differential Chaotic Phase Shift Keying (QDCPSK) для багатокористувацького зв'язку. Техніка QDCPSK має перевагу, оскільки може передавати кілька бітів, на відміну від техніки DCSK, описаної в [23], і виконувати кілька фазових зсувів на одному носії, на відміну від дослідження техніки CPSK, проведеного в [24], де кожен зсув відповідає пакету бітів. Основна різниця між техніками QDCPSK і CPSK полягає в тому, що фазові зсуви та сегмент опорного сигналу техніки QDCPSK знаходяться на тому ж носії, тоді як у техніках CPSK символи відповідають різним носіям. Однак техніки QDCPSK мають недолік: чим більше фазових зсувів, тим вища ймовірність перешкод між символами.

Що стосується технік CPSK, запропонованих у літературі, то є недолік: чим більше носіїв використовується для генерації символів, тим більше збільшується вимога до логічних ресурсів або елементів схем. Система, запропонована в цій статті, є попереднім етапом досліджень, які будуть проведені в майбутньому з хаотичними системами дробового порядку. Завдяки більшій кількості параметрів керування та складнішим динамікам хаотичні системи дробового порядку роблять схеми модуляції важчими для дешифрування зловмисниками [12]. Використання систем дробового

порядку дозволить оцінити та порівняти ефективність, точність і використання логічних ресурсів у порівнянні з хаотичними системами цілочисельного порядку, представленими в цій роботі.

1.2. Аналіз хаотичних генераторів та можливостей їх синхронізації.

У цій науковій роботі використовуються тривимірні (3D) генератори, а саме: Ванга та ін. [27], Ці та ін. [28], Чен-Лі та ін. [29], а також чотиривимірні (4D) генератори, а саме: Лая та ін. [30], Чжоу та ін. [31], Чен-Чжоу та ін. [32]. Таблиця 1 показує диференціальні формули, які моделюють ці 3D та 4D хаотичні генератори.

Таблиця 1.1

Моделі 3D хаотичних генераторів: Ванга, Ці, Чен-Лі; і 4D хаотичних генераторів: Лая, Чжоу та Чен-Чжоу.

Хаотичний осцилятор	Система рівнянь	Параметри	Початкові умови
	$\dot{x}=-x+y+yz$		
Ван [27]	$\dot{y}=-x-y+axz$	a=0.4, b=−0.3	
	$\dot{z}=z+bxy$		
	$\dot{x}=a(y-x)+eyz$		$x(1)$=1
Ци [28]	$\dot{y}=cx+dy-xz$	a=14, b=43, c=−1, d=16, e=4	$y(1)$=1
		c=−1, d=16, e=4	
	$\dot{z}=xy-bz$		$z(1)$=1
	$\dot{x}=ax-yz$		
Чен-Лі [29]	$\dot{y}=by+xz$	a=5, b=−10,c=−0.38, d=0.33	
	$\dot{z}=cz+dxy$		

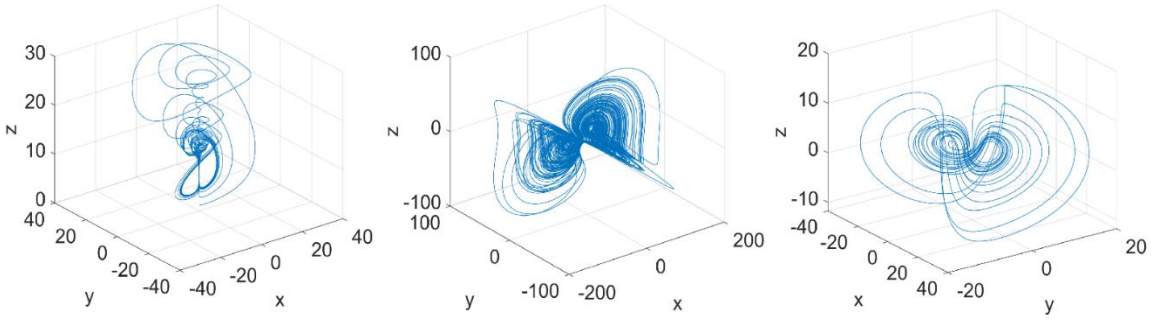
	$w^{\cdot}=ayz$		
Лая [30]	$x^{\cdot}=b(y-x)$	a=3, b=10, c=10	
	$y^{\cdot}=xz+w$		
	$z^{\cdot}=c-xy$		
	$w^{\cdot}=ax+byz$		$w(1)$=1
Чжоу [31]	$x^{\cdot}=c(y-x)$	a=8, b=0.1,c=10,d=20,e=8/3	$x(1)$=1

Продовж. табл. 1.1

	$y^{\cdot}=dx-y-xz+w$		$y(1)$=1
	$y^{\cdot}=dx-y-xz+w$		$z(1)$=1
	$w^{\cdot}=ax+byz$		
ЧенЧжоу[32]	$x^{\cdot}=c(y-x)$	a=8,b=0.1,c=10,d=20, e=8/3	
	$y^{\cdot}=dx-y-xz+w$		
	$z^{\cdot}=xy+ez+ywx$		

Рис. 1.1 показує хвильові форми (а) генератора Ванга, (б) генератора Ці та (в) генератора ван Вайка у їхніх площинах (x, y, z).

Рис. 1.2 показує хвильові форми генератора Лая, рисунок 1.3 (а) генератора Чжоу та (б) генератора Чен-Чжоу в різних площинах.



(а) (б) (в)

Рис. 1.1 Хвильові форми (а) генератора Ванга, (б) генератора Ці та (в) генератора ван Вайка у їхніх площинах (x, y, z).

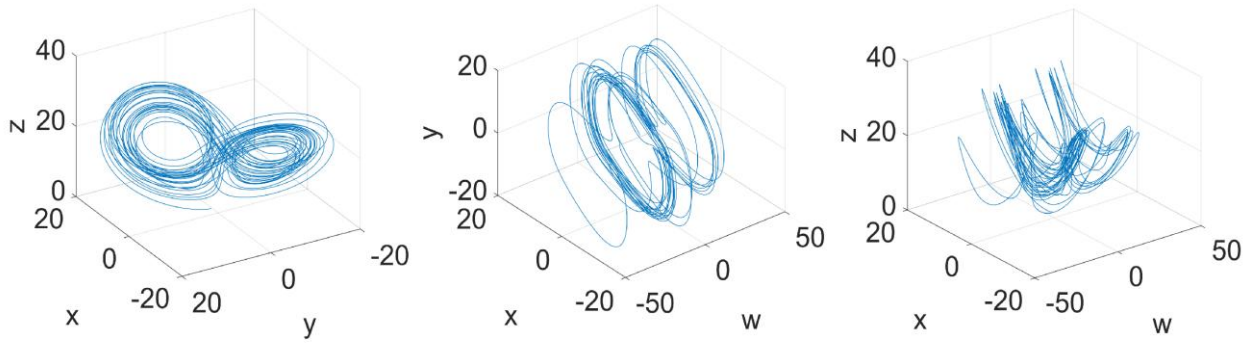


Рис. 1.2. Хвильові форми генератора Лая

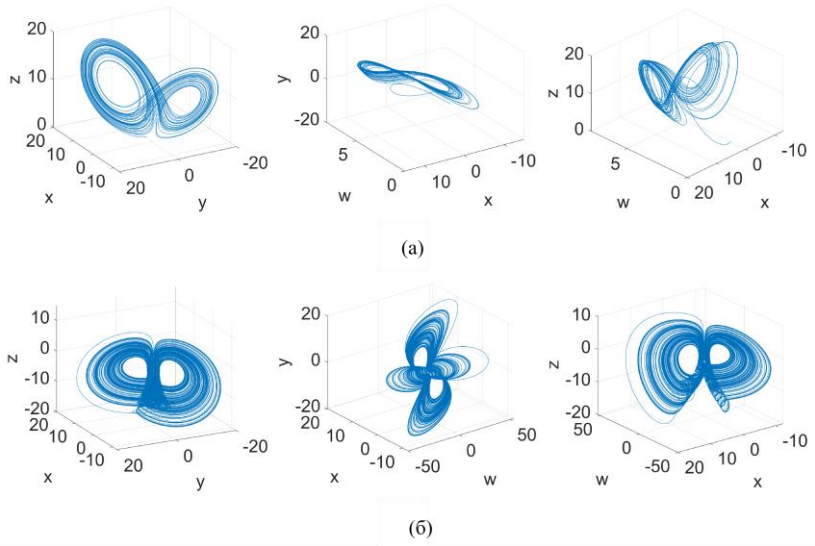
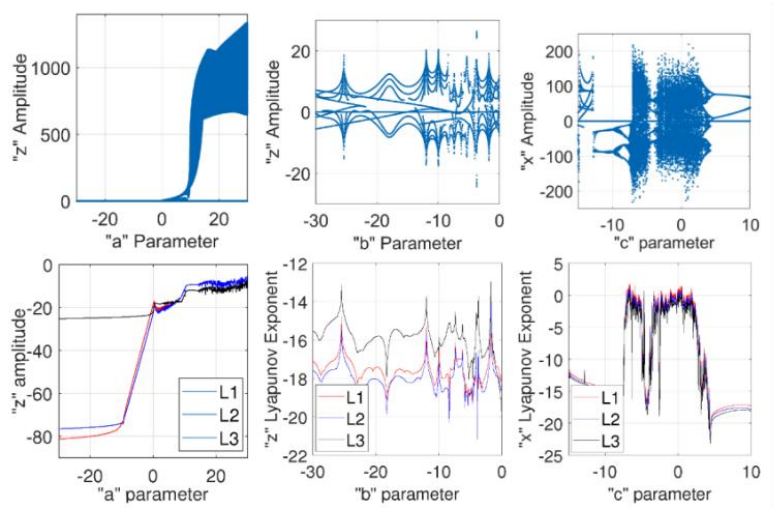


Рис. 1.3. Хвильові форми (а) генератора Чжоу та (б) генератора Чен-Чжоу в різних площинах

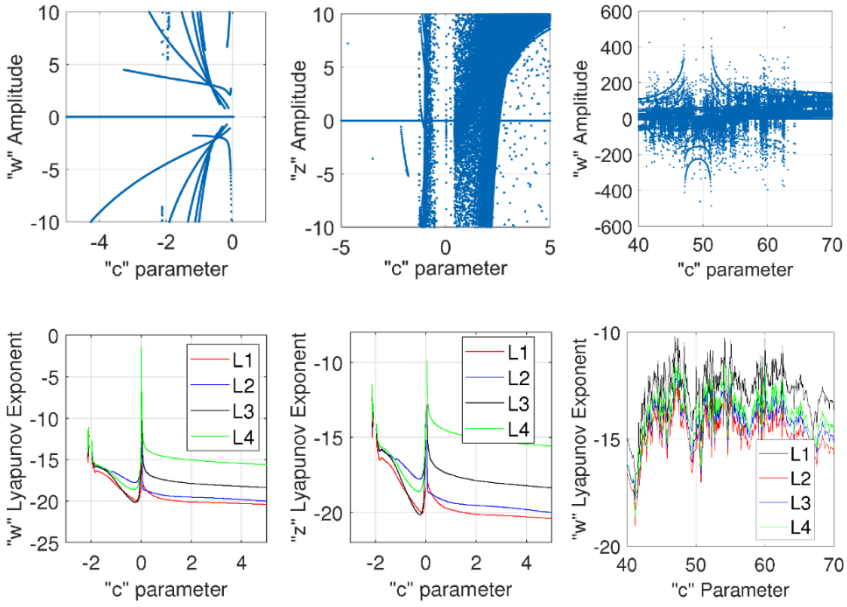
З іншого боку, діаграма розгалужень показує поведінку хаотичного генератора для різних значень контрольного параметра [33]. Рисунок 1.3 показує діаграми розгалужень генераторів із Таблиці 1.

Крім того, на рис. 1.4-1.5 наведені експоненти Ляпунова L_1, L_2, L_3, L_4 для хаотичних генераторів з Таблиці 1.1, які вказують на швидкість розбіжності двох початково близьких хаотичних траєкторій. Позитивні значення експоненти Ляпунова вказують на розбіжність між сусідніми траєкторіями, тоді як нульовий або від'ємний експонент вказує на відсутність експоненційної розбіжності [34,35,36].



(а) (б) (в)

Рис. 1.4. Діаграми розгалужень та спектри показників Ляпунова: (а) ван Вейк, (б) Ван, (в) Ці



(а) (б) (в)

Рис. 1.5. Діаграми розгалужень та спектри показників Ляпунова:(а) Чжоу, (б) Чень-Чжоу, (в) Лай.

1.3. 4D генератор з можливістю переналаштування.

Спостерігаючи за моделями диференціальних рівнянь, що представляють генератори, використані в цьому дослідженні (Таблиця 1.1), та іншими з літератури, пропонується розширена система рівнянь, яка враховує всі існуючі змінні та їх можливі комбінації. Таким чином, отримується узагальнена система рівнянь, яка називається перероблюваним генератором, з загальною кількістю 64 параметрів ($p_{1,1}$ … $p_{4,16}$) та 16 комбінаціями змінних стану w, x, y, z. формули (1.1) показує модель перероблюваного генератора з усіма комбінаціями параметрів і змінних.

$$F = \begin{bmatrix} p_{1,1} & p_{1,2} & p_{1,3} & p_{1,4} & p_{1,5} & p_{1,6} & p_{1,7} & p_{1,8} & p_{1,9} & p_{1,10} & p_{1,11} & p_{1,12} & p_{1,13} & p_{1,14} & p_{1,15} & p_{1,16} \\ p_{2,1} & p_{2,2} & p_{2,3} & p_{2,4} & p_{2,5} & p_{2,6} & p_{2,7} & p_{2,8} & p_{2,9} & p_{2,10} & p_{2,11} & p_{2,12} & p_{2,13} & p_{2,14} & p_{2,15} & p_{2,16} \\ p_{3,1} & p_{3,2} & p_{3,3} & p_{3,4} & p_{3,5} & p_{3,6} & p_{3,7} & p_{3,8} & p_{3,9} & p_{3,10} & p_{3,11} & p_{3,12} & p_{3,13} & p_{3,14} & p_{3,15} & p_{3,16} \\ p_{4,1} & p_{4,2} & p_{4,3} & p_{4,4} & p_{4,5} & p_{4,6} & p_{4,7} & p_{4,8} & p_{4,9} & p_{4,10} & p_{4,11} & p_{4,12} & p_{4,13} & p_{4,14} & p_{4,15} & p_{4,16} \end{bmatrix} \begin{bmatrix} 1 \\ w \\ x \\ y \\ z \\ wx \\ wy \\ wz \\ xy \\ xz \\ yz \\ wxy \\ wxz \\ wyz \\ xyz \\ wxyz \end{bmatrix}. \quad (1.1)$$

Тоді до формули (1.1) застосовується операція градієнта, представлена як $\nabla \cdot F \rightarrow$, для усунення змінних, які дестабілізують хаотичний генератор, як показано в формулі (2).

$$\nabla \cdot \vec{F} = \frac{\partial F_1}{\partial w} + \frac{\partial F_2}{\partial x} + \frac{\partial F_3}{\partial y} + \frac{\partial F_4}{\partial z}. \quad (1.2)$$

де $\frac{\partial F_1}{\partial w}, \frac{\partial F_2}{\partial x}, \frac{\partial F_3}{\partial y}, \frac{\partial F_4}{\partial z}$ відповідають частковим похідним змінних w, x, y та z відповідно. Розгортаючи члени формули (1.2), результат відображається в формулі (1.3).

$$\begin{aligned}\frac{\partial F_1}{\partial w} &= p_{1,2} + xp_{1,6} + yp_{1,7} + zp_{1,8} + xyp_{1,12} + xzp_{1,13} + yzp_{1,14} + xyzp_{1,16}\\ \frac{\partial F_2}{\partial x} &= p_{2,3} + wp_{2,6} + yp_{2,9} + zp_{2,10} + wyp_{2,12} + wzp_{2,13} + yzp_{2,15} + wyzp_{2,16}\\ \frac{\partial F_3}{\partial y} &= p_{3,4} + wp_{3,7} + xp_{3,9} + zp_{3,11} + wxp_{3,12} + wzp_{3,14} + xzp_{3,15} + wxzp_{3,16}\\ \frac{\partial F_4}{\partial z} &= p_{4,5} + wp_{4,8} + xp_{4,10} + yp_{4,11} + wxp_{4,13} + wyp_{4,14} + xyp_{4,15} + wxyp_{4,16}\end{aligned}. \quad (1.3)$$

Наступним кроком, з формули (1.1), змінні формули (1.3) усуваються, за винятком сталих членів $p_{1,1}$, $p_{2,1}$, $p_{3,1}$, $p_{4,1}$, і результат відображається в формулі (1.4).

$$\begin{aligned}\frac{\partial F_1}{\partial w} &= p_{1,2} + xp_{1,6} + yp_{1,7} + zp_{1,8} + xyp_{1,12} + xzp_{1,13} + yzp_{1,14} + xyzp_{1,16}\\ \frac{\partial F_2}{\partial x} &= p_{2,3} + wp_{2,6} + yp_{2,9} + zp_{2,10} + wyp_{2,12} + wzp_{2,13} + yzp_{2,15} + wyzp_{2,16}\\ \frac{\partial F_3}{\partial y} &= p_{3,4} + wp_{3,7} + xp_{3,9} + zp_{3,11} + wxp_{3,12} + wzp_{3,14} + xzp_{3,15} + wxzp_{3,16}\\ \frac{\partial F_4}{\partial z} &= p_{4,5} + wp_{4,8} + xp_{4,10} + yp_{4,11} + wxp_{4,13} + wyp_{4,14} + xyp_{4,15} + wxyp_{4,16}\end{aligned}. \quad (1.4)$$

де w, x, y та z — це залежні змінні системи, в той час як коефіцієнтна матриця $p_{i,j}$ змінюється залежно від вибраного хаотичного генератора.

1.4. Гамільтонівська синхронізація.

У цьому підрозділі математично аналізується метод гамільтонівської синхронізації двох хаотичних систем в топології майстер–слейв, де майстер-систему спостерігає система-слейв. Якщо ми маємо динамічну систему у вигляді (1.1),

$$\dot{x} = f(x) \quad (1.5)$$

де $x^{\cdot} \in \mathbb{R}^n$ — це змінна стану, а f: $\mathbb{R}^n \longrightarrow \mathbb{R}^n$ — нелінійна функція. Динамічну систему формули (1.5) також можна записати як формули (1.6).

$$\dot{x} = A\frac{\partial H}{\partial x} + \mathcal{F}(x), \tag{1.6}$$

де $A = (A - A^{\mathrm{T}})/2 + (A + A^{\mathrm{T}})/2$, а $\mathscr{F}(x)$ представляє вектор поля нестабільності, де $H(x)$ описує глобально додатно визначену енергетичну функцію у вигляді $H(x) = 1/2\ x^{\mathrm{T}}\mathscr{M}x$, градієнт вектора H позначається як $\partial H/\partial x$, а $\mathscr{M}$ — це додатна симетрична й постійна матриця, так що формули (1.6) можна переписати у вигляді формули (1.7).

$$\dot{x} = \frac{A - A^T}{2}\frac{\partial H}{\partial x} + \frac{A + A^T}{2}\frac{\partial H}{\partial x} + \mathcal{F}(x)\,. \tag{1.7}$$

Якщо вирази $\mathcal{J}(x) = (A - A^{\mathrm{T}})/2$ і $\mathcal{S}(x) = (A + A^{\mathrm{T}})/2$ переписати, то формули (1.7) перетворюється на канонічну узагальнену гамільтонову систему, як показано формули (1.8).

$$\dot{x} = \mathcal{J}(x)\frac{\partial H}{\partial x} + \mathcal{S}(x)\frac{\partial H}{\partial x}, x \in \mathbb{R}^n, \tag{1.8}$$

Крім того, квадратні матриці $\mathcal{J}(x)$ і $\mathcal{S}(x)$ задовольняють умови $\mathcal{J}(x) + \mathcal{J}^{\mathrm{T}}(x) = 0$ та $\mathcal{S}(x) = \mathcal{S}^{\mathrm{T}}(x)$. З іншого боку, якщо ми розглянемо особливий клас узагальнених гамільтонових систем з дестабілізуючими векторними полями, ми отримаємо формули (1.9).

$$\begin{gathered}\dot{x}_m = J(y)\frac{\partial H}{\partial x_m} + (I + \mathcal{S})\frac{\partial H}{\partial x_m} + \mathcal{F}(y), y = \mathcal{C}\frac{\partial H}{\partial x_m}, \\ (x_m, y) \in \mathbb{R}^n\end{gathered} \tag{1.9}$$

де $\mathcal{C}$ відповідає сталою матриці, а I — сталою діагонально симетричною матрицею. Вибираючи змінні x_{m} та η як оцінювані вектор стану та вектор відповідно в системі-

слузі, вектор стану x представляється через x_e. З формули (1.9) генерується система-слуга, представлена формули (1.10) на виході.

$$\dot{x}_e = \mathcal{J}(y)\frac{\partial H}{\partial x_e} + (I + \mathcal{S})\frac{\partial H}{\partial x_e} + \mathcal{F}(y) + K(y - \eta), \eta = \mathcal{C}\frac{\partial H}{\partial x_e}, \quad (x_e, \eta) \in \mathbb{R}^n \tag{1.10}$$

З вектором K, який відомий як вектор посилення системи-слуги. З формули (1.9) і (1.10) процес синхронізації розвивається структуровано. Спочатку отримується енергетична функція шляхом вибору квадратичної енергетичної функції, яка показана в формули (1.11).

$$H(x) = \frac{1}{2}[aw^2 + bx^2 + cy^2 + dz^2]. \tag{1.11}$$

У свою чергу, вектор градієнта формули (1.11) показаний у формулі (1.12), де x відповідає вектору змінних осцилятора, а P — матричним коефіцієнтам:

$$\frac{\partial H}{\partial x} = \begin{bmatrix} aw \\ bx \\ cy \\ dz \end{bmatrix} = \begin{bmatrix} a & 0 & 0 & 0 \\ 0 & b & 0 & 0 \\ 0 & 0 & c & 0 \\ 0 & 0 & 0 & d \end{bmatrix} \begin{bmatrix} w \\ x \\ y \\ z \end{bmatrix} = Px. \tag{1.12}$$

Згодом, матриці J та S отримуються через матричне подання хаотичного осцилятора з формули (4), що дає формули (1.13):

$$Ax = \begin{bmatrix} \begin{vmatrix} p_{11}/w \\ p_{21}/x \\ p_{31}/y \\ p_{41}/z \end{vmatrix} \begin{vmatrix} p_{12} & p_{13} & p_{14} & p_{15} \\ p_{22} & p_{23} & p_{24} & p_{25} \\ p_{32} & p_{33} & p_{34} & p_{35} \\ p_{42} & p_{43} & p_{44} & p_{45} \end{vmatrix} \begin{vmatrix} \frac{p_{16}xy}{w} & p_{17}z & \frac{p_{18}xw}{y} & p_{19}y \\ \frac{p_{26}xy}{w} & p_{27}z & \frac{p_{28}xw}{y} & p_{29}y \\ \frac{p_{36}xy}{w} & p_{37}z & \frac{p_{38}xw}{y} & p_{39}y \\ \frac{p_{46}xy}{w} & p_{47}z & \frac{p_{48}xw}{y} & p_{49}y \end{vmatrix} \end{bmatrix} \begin{bmatrix} w \\ x \\ y \\ z \end{bmatrix}. \quad (1.13)$$

формули (1.13) переписується у термінах $\mathcal{J}$ та $\mathcal{S}$, як показано в формулі (1.14):

$$A = R\frac{\partial H}{\partial x} = [\mathcal{J}(y) + \mathcal{S}(y)]\frac{\partial H}{\partial x}, \quad (1.14)$$

де $R = AP^{-1}$ є допоміжною матрицею і виражається у формулі (1.15):

$$R = \begin{bmatrix} \frac{p_{11}}{aw} + \frac{p_{12}}{a} + \frac{p_{16}xy}{aw}, & \frac{p_{13}}{b} + \frac{p_{17}z}{b} + \frac{p_{11}}{aw}, & \frac{p_{14}}{c} + \frac{p_{11}}{aw} + \frac{p_{18}wx}{cy}, & \frac{p_{15}}{d} + \frac{p_{19}y}{d} + \frac{p_{11}}{aw} \\ \frac{p_{21}}{aw} + \frac{p_{22}}{a} + \frac{p_{26}xy}{aw}, & \frac{p_{23}}{b} + \frac{p_{27}z}{b} + \frac{p_{21}}{aw}, & \frac{p_{24}}{c} + \frac{p_{21}}{aw} + \frac{p_{28}wx}{cy}, & \frac{p_{25}}{d} + \frac{p_{29}y}{d} + \frac{p_{21}}{aw} \\ \frac{p_{31}}{aw} + \frac{p_{32}}{a} + \frac{p_{36}xy}{aw}, & \frac{p_{33}}{b} + \frac{p_{37}z}{b} + \frac{p_{31}}{aw}, & \frac{p_{34}}{c} + \frac{p_{31}}{aw} + \frac{p_{38}wx}{cy}, & \frac{p_{35}}{d} + \frac{p_{39}y}{d} + \frac{p_{31}}{aw} \\ \frac{p_{41}}{aw} + \frac{p_{42}}{a} + \frac{p_{46}xy}{aw}, & \frac{p_{43}}{b} + \frac{p_{47}z}{b} + \frac{p_{41}}{aw}, & \frac{p_{44}}{c} + \frac{p_{41}}{aw} + \frac{p_{48}wx}{cy}, & \frac{p_{45}}{d} + \frac{p_{49}y}{d} + \frac{p_{41}}{aw} \end{bmatrix}. \quad (1.15)$$

З формули (15) можна отримати співвідношення $\mathcal{S}(x) = 1/2(R + R^{\mathrm{T}})$, яке представлено у формулі (1.16):

$$\mathcal{S}(x) = \begin{bmatrix} \frac{p_{11}+p_{12}w+p_{16}xy}{aw} & S_5 & S_1 & S_4 \\ S_5 & \frac{p_{21}+p_{23}x+p_{27}xz}{bx} & S_3 & S_6 \\ S_1 & S_3 & \frac{p_{31}+p_{34}y+p_{38}wx}{cy} & S_2 \\ S_5 & S_5 & S_5 & \frac{p_{41}+p_{45}z+p_{49}yz}{dz} \end{bmatrix}, \quad (1.16)$$

де $\mathcal{S}_{\mathrm{n}}$ описується формули (1.17):

$$S_1 = \frac{p_{32}}{2a} + \frac{p_{14}}{2c} + \frac{p_{11}}{2aw} + \frac{p_{31}}{2cy} + \frac{p_{36}xy}{2aw} + \frac{p_{18}wx}{2cy}$$

$$S_2 = \frac{p_{44}}{2c} + \frac{p_{35}}{2d} + \frac{p_{39}y}{2d} + \frac{p_{31}}{2cy} + \frac{p_{41}}{2dz} + \frac{p_{48}wx}{2cy}$$

$$S_3 = \frac{p_{33}}{2b} + \frac{p_{24}}{2c} + \frac{p_{37}z}{2b} + \frac{p_{21}}{2bx} + \frac{p_{31}xy}{2cy} + \frac{p_{28}wx}{2cy}$$

$$S_4 = \frac{p_{42}}{2a} + \frac{p_{15}}{2d} + \frac{p_{19}y}{2d} + \frac{p_{11}}{2aw} + \frac{p_{41}}{2dz} + \frac{p_{46}xy}{2aw}. \quad (1.17)$$

$$S_5 = \frac{p_{22}}{2a} + \frac{p_{13}}{2b} + \frac{p_{17}z}{2b} + \frac{p_{11}}{2aw} + \frac{p_{21}}{2bx} + \frac{p_{26}xy}{2aw}$$

$$S_6 = \frac{p_{43}}{2b} + \frac{p_{25}}{2d} + \frac{p_{47}z}{2b} + \frac{p_{29}y}{2d} + \frac{p_{21}}{2bx} + \frac{p_{41}}{2dz}$$

$$S_7 = \frac{p_{31}}{2cy}, S_8 = \frac{p_{11}}{2aw}, S_9 = \frac{p_{41}}{2dz}, S_{10} = \frac{p_{21}}{2bx}$$

Крім того, $\mathcal{J}(x) = 1/2(R - R^{\mathrm{T}})$ виражено формули (1.18).

$$\mathcal{J}(x) = \begin{bmatrix} 0, & \frac{p_{13}}{2b} - \frac{p_{22}}{2a} + J_{16} + J_4 - J_3 - J_{10}, & \frac{p_{14}}{2c} - \frac{p_{32}}{2a} + J_4 - J_2 - J_9 + J_7, & \frac{p_{15}}{2d} - \frac{p_{42}}{2a} + J_{13} + J_4 - J_1 - J_8 \\ \frac{p_{22}}{2a} - \frac{p_{13}}{2b} - J_{16} - J_4 + J_3 + J_{10}, & 0, & \frac{p_{24}}{2c} - \frac{p_{33}}{2b} - J_{15} + J_3 - J_2 + J_6, & \frac{p_{25}}{2d} - \frac{p_{43}}{2b} - J_{14} + J_{12} + J_3 - J_1 \\ \frac{p_{32}}{2a} - \frac{p_{14}}{2c} - J_4 + J_2 + J_9 - J_7, & \frac{p_{33}}{2b} - \frac{p_{24}}{2c} + J_{15} - J_3 + J_2 - J_6, & 0, & \frac{p_{35}}{2d} - \frac{p_{44}}{2c} + J_{11} + J_2 - J_1 - J_5 \\ \frac{p_{42}}{2a} - \frac{p_{15}}{2d} - J_{13} - J_4 + J_1 + J_8, & \frac{p_{43}}{2b} - \frac{p_{25}}{2d} + J_{14} - J_{12} - J_3 + J_1, & \frac{p_{44}}{2c} - \frac{p_{35}}{2d} - J_{11} - J_2 + J_1 + J_5 & 0 \end{bmatrix}, \quad (1.18)$$

де $\mathcal{J}_{\mathrm{n}}$ описується формули (1.19).

$$J_1 = \frac{p_{41}}{2dz}, J_2 = \frac{p_{31}}{2cy}, J_3 = \frac{p_{21}}{2bx}, J_4 = \frac{p_{11}}{2aw}$$

$$J_5 = \frac{p_{48}wx}{2cy}, J_6 = \frac{p_{28}wx}{2cy}, J_7 = \frac{p_{18}wx}{2cy}, J_8 = \frac{p_{46}xy}{2aw}$$

$$J_9 = \frac{p_{36}xy}{2aw}, J_{10} = \frac{p_{26}xy}{2aw}, J_{11} = \frac{p_{39}y}{2d}, J_{12} = \frac{p_{29}y}{2d} \quad (1.19)$$

$$J_{13} = \frac{p_{19}y}{2d}, J_{14} = \frac{p_{47}z}{2b}, J_{15} = \frac{p_{37}z}{2b}, J_{16} = \frac{p_{17}z}{2b}$$

Крім того, матриця $\mathcal{C}$ = [1000]. Потім здійснюється синхронізація системи майстра–раба. Система майстра отримується шляхом розвитку формули (1.9), як показано в формулі (1.20):

$$\begin{bmatrix} \dot{w}_m \\ \dot{x}_m \\ \dot{y}_m \\ \dot{z}_m \end{bmatrix} = \begin{bmatrix} 0 & \frac{p_{13}}{2b} - \frac{p_{22}}{2a} + J_{16} + J_4 - J_3 - J_{10}, & \frac{p_{14}}{2c} - \frac{p_{32}}{2a} + J_4 - J_2 - J_9 + J_7, & \frac{p_{15}}{2d} - \frac{p_{42}}{2a} + J_{13} + J_4 - J_1 - J_8 \\ \frac{p_{22}}{2a} - \frac{p_{13}}{2b} - J_{16} - J_4 + J_3 + J_{10}, & 0, & \frac{p_{24}}{2c} - \frac{p_{33}}{2b} - J_{15} + J_3 - J_2 + J_6, & \frac{p_{25}}{2d} - \frac{p_{43}}{2b} - J_{14} + J_{12} + J_3 - J_1 \\ \frac{p_{32}}{2a} - \frac{p_{14}}{2c} - J_4 + J_2 + J_9 - J_7, & \frac{p_{33}}{2b} - \frac{p_{24}}{2c} + J_{15} - J_3 + J_2 - J_6, & 0, & \frac{p_{35}}{2d} - \frac{p_{44}}{2c} + J_{11} + J_2 - J_1 - J_5 \\ \frac{p_{42}}{2a} - \frac{p_{15}}{2d} - J_{13} - J_4 + J_1 + J_8, & \frac{p_{43}}{2b} - \frac{p_{25}}{2d} + J_{14} - J_{12} - J_3 + J_1, & \frac{p_{44}}{2c} - \frac{p_{35}}{2d} - J_{11} - J_2 + J_1 + J_5, & 0 \end{bmatrix} \begin{bmatrix} aw \\ bx \\ cy \\ dz \end{bmatrix} + \begin{bmatrix} \frac{p_{11}+p_{12}w+p_{16}xy}{aw} & S_5 & S_1 & S_4 \\ S_5 & \frac{p_{21}+p_{23}x+p_{27}xz}{bx} & S_3 & S_6 \\ S_1 & S_3 & \frac{p_{31}+p_{34}y+p_{38}wx}{cy} & S_2 \\ S_5 & S_5 & S_5 & \frac{p_{41}+p_{45}z+p_{49}yz}{dz} \end{bmatrix} \begin{bmatrix} aw \\ bx \\ cy \\ dz \end{bmatrix}. \quad (1.20)$$

Виконання операцій з матрицями в формулі (1.20) дає формули (1.21), яке відповідає системі рівнянь регульованого генератора:

$$\begin{aligned} \dot{w}_m &= p_{11} + wp_{12} + xp_{13} + yp_{14} + zp_{15} + xyp_{16} + xzp_{17} + xwp_{18} + yzp_{19} \\ \dot{x}_m &= p_{21} + wp_{22} + xp_{23} + yp_{24} + zp_{25} + xyp_{26} + xzp_{27} + xwp_{28} + yzp_{29} \\ \dot{y}_m &= p_{31} + wp_{32} + xp_{33} + yp_{34} + zp_{35} + xyp_{36} + xzp_{37} + xwp_{38} + yzp_{39} \\ \dot{z}_m &= p_{41} + wp_{42} + xp_{43} + yp_{44} + zp_{45} + xyp_{46} + xzp_{47} + xwp_{48} + yzp_{49} \end{aligned}. \quad (1.21)$$

Тому спостережувану систему можна представити, розв'язавши формули (1.10), як показано в формулі (1.22).

Помноживши матриці формули (1.22), ми отримуємо конфігурацію системи-підлеглого, як показано в формулі (1.23).

$$\begin{bmatrix}\dot{w}_e\\ \dot{x}_e\\ \dot{y}_e\\ \dot{z}_e\end{bmatrix}=\begin{bmatrix}0 & \frac{p_{13}}{2b}-\frac{p_{22}}{2a}+J_{16}+J_4-J_3-J_{10}, & \frac{p_{14}}{2c}-\frac{p_{32}}{2a}+J_4-J_2-J_9+J_7, & \frac{p_{15}}{2d}-\frac{p_{42}}{2a}+J_{13}+J_4-J_1-J_8\\ \frac{p_{22}}{2a}-\frac{p_{13}}{2b}-J_{16}-J_4+J_3+J_{10}, & 0, & \frac{p_{24}}{2c}-\frac{p_{33}}{2b}-J_{15}+J_3-J_2+J_6, & \frac{p_{25}}{2d}-\frac{p_{43}}{2b}-J_{14}+J_{12}+J_3-J_1\\ \frac{p_{32}}{2a}-\frac{p_{14}}{2c}-J_4+J_2+J_9-J_7, & \frac{p_{33}}{2b}-\frac{p_{24}}{2c}+J_{15}-J_3+J_2-J_6, & 0, & \frac{p_{35}}{2d}-\frac{p_{44}}{2c}+J_{11}+J_2-J_1-J_5\\ \frac{p_{42}}{2a}-\frac{p_{15}}{2d}-J_{13}-J_4+J_1+J_8, & \frac{p_{43}}{2b}-\frac{p_{25}}{2d}+J_{14}-J_{12}-J_3+J_1, & \frac{p_{44}}{2c}-\frac{p_{35}}{2d}-J_{11}-J_2+J_1+J_5, & 0\end{bmatrix}\begin{bmatrix}aw\\ bx\\ cy\\ dz\end{bmatrix}$$

$$+\begin{bmatrix}\frac{p_{11}+p_{12}w+p_{16}xy}{aw} & S_5 & S_1 & S_4\\ S_5 & \frac{p_{21}+p_{23}x+p_{27}xz}{bx} & S_3 & S_6\\ S_1 & S_3 & \frac{p_{31}+p_{34}y+p_{38}wx}{cy} & S_2\\ S_5 & S_5 & S_5 & \frac{p_{41}+p_{45}z+p_{49}yz}{dz}\end{bmatrix}\begin{bmatrix}aw\\ bx\\ cy\\ dz\end{bmatrix}. \quad (1.22)$$

$$+\begin{bmatrix}K_1\\ K_2\\ K_3\\ K_4\end{bmatrix}(y-\eta).$$

$$\begin{aligned}\dot{w}_e &= p_{11}+wp_{12}+xp_{13}+yp_{14}+zp_{15}+xyp_{16}+xzp_{17}+xwp_{18}+yzp_{19}+k_1(w_m-w_e)\\ \dot{x}_e &= p_{21}+wp_{22}+xp_{23}+yp_{24}+zp_{25}+xyp_{26}+xzp_{27}+xwp_{28}+yzp_{29}+k_2(x_m-x_e)\\ \dot{y}_e &= p_{31}+wp_{32}+xp_{33}+yp_{34}+zp_{35}+xyp_{36}+xzp_{37}+xwp_{38}+yzp_{39}+k_3(y_m-y_e)\\ \dot{z}_e &= p_{41}+wp_{42}+xp_{43}+yp_{44}+zp_{45}+xyp_{46}+xzp_{47}+xwp_{48}+yzp_{49}+k_4(z_m-z_e)\end{aligned}. \quad (1.23)$$

1.5. Хаотична модуляція типу CPSK

У модуляції 16-CPSK інформація сегментується на пакети по 4 біти, і кожен кадр відповідає різному блоку модуляції, що позначений як j, як показано в формулі (1.24):

$$cpsk_c(t) = x_m(snc + t(Sy + c - 1) : snc + t(Sy + c)), \quad (1.24)$$

де snc позначає затримку носія для завершення синхронізації; t відповідає періоду кожного символу; Sy позначає номер символу (у цьому випадку він змінюється від 1 до 16); а c — номер кадру, який необхідно передати, що змінюється від 1 до довжини повідомлення. Блок-схема процесу модуляції 16-CPSK показана на рисунку 1.4а. Варто зазначити, що 4-бітовий пакет буде відповідати символу каналу, який був попередньо збережений на хаотичному генераторі.

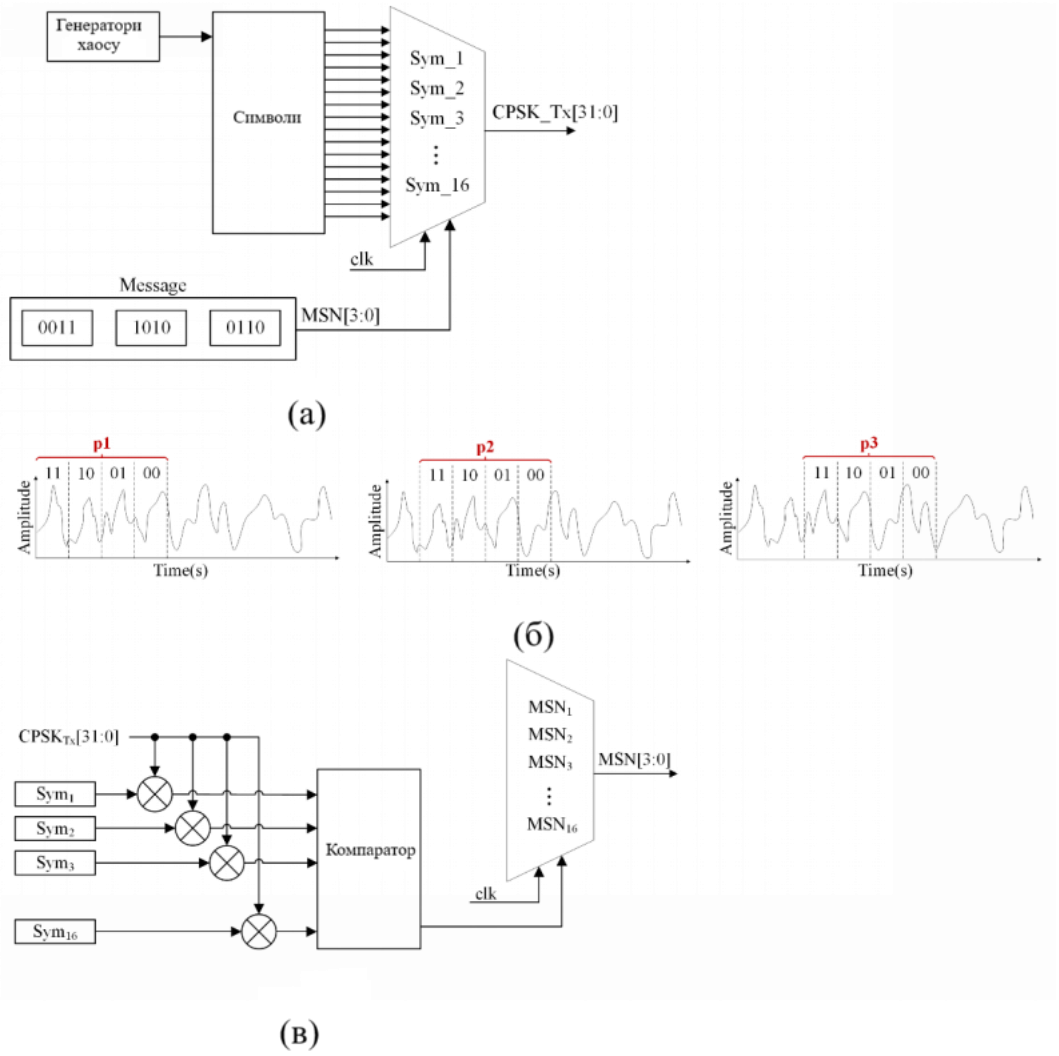


Рис. 1.4. Схема процесу 16-CPSK: (а) Модуляція; (б) Оновлення символу в періодах 1–2; (в) Демодуляція.

Модульовані символи 16-CPSK модифікації передаються за допомогою зміщень фази в їхніх хвильових формах. Кожне зміщення фази генерує блок модулюючих символів, де кожен символ відповідає певному набору бітів. У випадку 16-CPSK кожен символ несе 4 біти інформації. У цьому дослідженні використано носій, складений з кількох хаотичних генераторів. Композитний носій сегментувався, і кожен фрагмент сигналу призначався для певного символу. На рис. 1.4а (зліва) показано перший сегмент символу, позначений як $p1$. Також показано відповідні біти для кожного символу. Після цього стан усіх символів оновлюється для генерації $p2$, показаного на рис. 1.4б (по центру) з їхніми відповідними парами бітів. І наостанок,

рис. 1.4б (праворуч) показує третій блок символів, позначений як $p3$. Як видно з рисунка 1.4б, блоки $p1$, $p2$ і $p3$ зберігають пари бітів, але їхні відповідні сегменти сигналу змінюються. Процес демодуляції передбачає кореляцію отриманого модуляційного сигналу з кожним із 16 збережених символів. Схему демодуляції 16-CPSK показано на рис. 1.4в.

1.6. Висновки до Розділу 1

Існуючі системи хаотичного шифрування CPSK, такі як техніки на основі хаотичних генераторів, показують значний потенціал для підвищення захищеності передачі даних. Однак вони стикаються із проблемами реалізації, зокрема потребою у складних алгоритмах синхронізації та значному обсязі обчислювальних ресурсів.

Хаотичні генератори, такі як 3D і 4D системи, демонструють унікальні характеристики, включаючи низьку автокореляцію та широкий спектр частот. Проте можливості їхньої адаптації до складних умов середовища передачі, включаючи дестабілізаційні фактори, ще недостатньо досліджені.

Метод гамільтонівської синхронізації в конфігурації "майстер–підлеглий" дозволяє досягти високої точності синхронізації та підвищити ефективність системи, однак його застосування вимагає подальшої оптимізації для зменшення впливу помилок квантування та забезпечення стійкості до атак.

Таким чином, результати аналітичного огляду підтверджують необхідність удосконалення хаотичних систем шифрування CPSK шляхом впровадження більш складних генераторів, адаптивних алгоритмів синхронізації та використання мультиканальних технологій. Це створить основу для подальшої розробки ефективних рішень у сфері захисту даних.

РОЗДІЛ 2
ОСНОВНА ЧАСТИНА

2.1. Теоретична реалізація системи модуляції-демодуляції на VHDL

Система модуляції-демодуляції 16-CPSK демонструє високу ефективність у задачах передачі даних, забезпечуючи надійну синхронізацію та мінімізацію помилок під час демодуляції. Завдяки використанню хаотичних сигналів та їх обробці у цифровій формі, система має підвищену стійкість до перешкод і зберігає конфіденційність переданої інформації.

Система модуляції-демодуляції 16-CPSK була реалізована за допомогою мови VHDL у програмному забезпеченні Vivado, версії 2020.2. Система складається з трьох основних компонентів, що включають 14 різних апаратних модулів. Модулі позначені як gen_caos, Tx, Rx, error_sinc, ctrl_RAM_Tx, ctrl_RAM_Rx, RAM_1_Tx, RAM_2_Tx, RAM_16_Tx, RAM_1_Rx, RAM_2_Rx, RAM_16_Rx, CPSK_mod та CPSK_demod, як показано на блок схемі на Рис. 2.1.

Для представлення та обробки підписаних згенерованих хаотичних сигналів використовувалася довжина слова 32 біти в арифметиці двійкових чисел зі знаком. Основні входи системи: clk та MSN[3:0], де clk — це тактовий сигнал системи, а MSN[3:0] — це 4-розрядний цифровий сигнал, що несе повідомлення.

Повідомлення може бути у вигляді інформації зображення, що передається у вигляді чотирибітних пакетів. Хоча сигнал CPSK_Tx є входом системи, він відповідає вихідному модуляційному сигналу повідомлення, отриманому з модуля $CPSK\_demod$. Цей самий сигнал, $CPSK\_Tx$, разом з сигналом MSN[3:0] на приймальній стороні, складає вихід системи, який представляє модуляційне повідомлення та відновлене повідомлення відповідно.

Детальніше буде розглянуто процес реалізації системи модуляції-демодуляції 16-CPSK у наступних підрозділах.

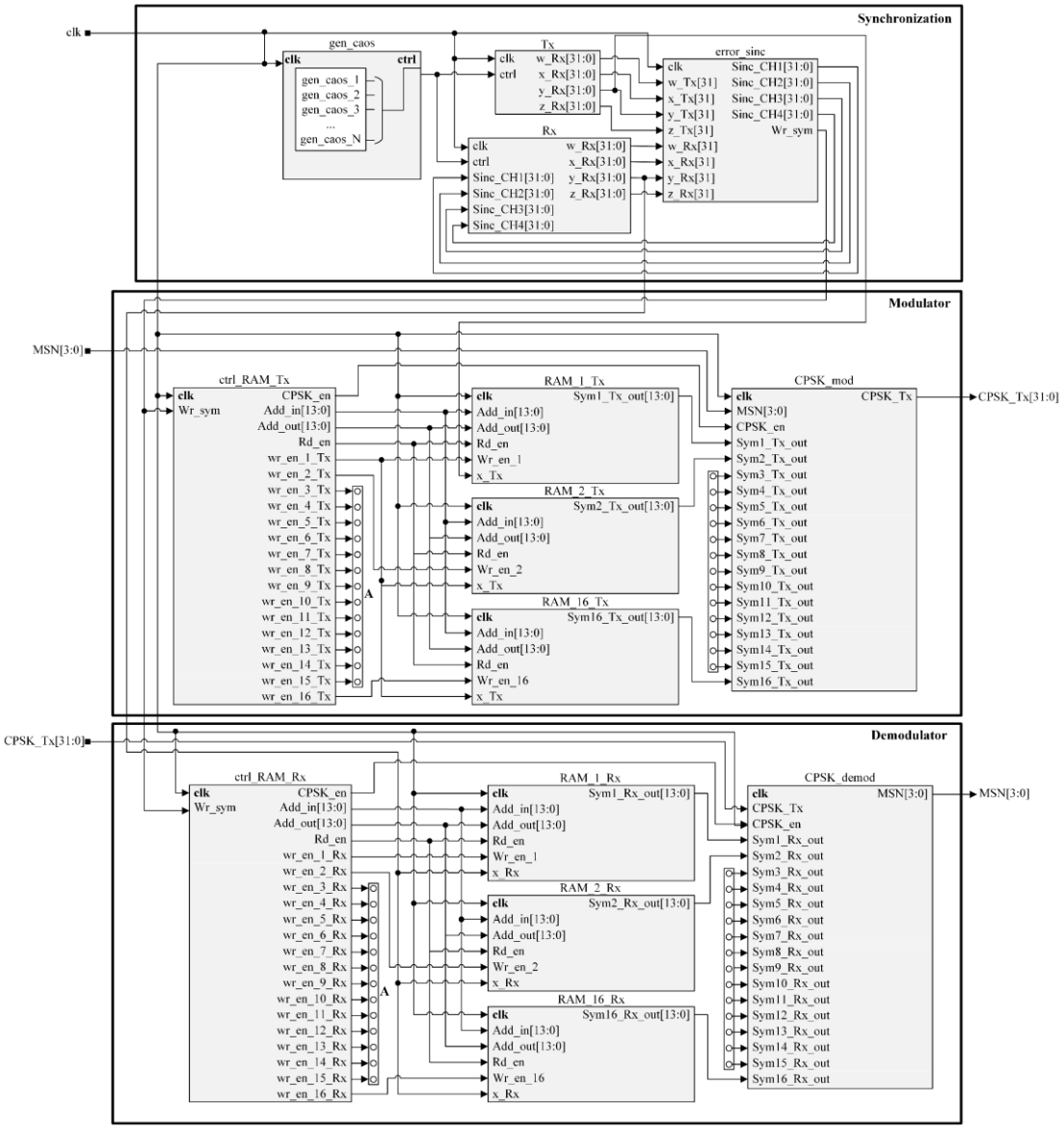


Рис. 2.1. Блок схема системи модуляції-демодуляції 16-CPSK

2.2. Переналаштовувані генератори хаосу типу майстер–підлеглий.

Основною особливістю системи модуляції–демодуляції 16-CPSK, реалізованої в цьому дослідженні, що сприяє її стійкості, є переналаштовуваність генератора хаосу та синхронізація в конфігурації майстер–підлеглий. Пам'ятна схема в системі періодично перемикається між різними параметрами для генерації різноманітних хаотичних сигналів. Інтегруючи генератори хаосу Wang 3D, Qi 3D, van Wyk 3D, Lai 4D, Zhou 4D та Chen-Zhou 4D для формування складеного носія, отриманий сигнал

відображає поведінку всіх шести генераторів, переходячи між ними на заданих тимчасових інтервалах. Цей підхід дозволяє сигналу плавно поєднувати характеристики кожного генератора в межах визначеного часу. Вхідні сигнали clk і $ctrl$ визначають, який генератор буде генеруватися в межах сегментованого тимчасового інтервалу. Виходи wTx, xTx, yTx і zTx відповідають каналам генератора хаосу, що відображають стан динамічної поведінки системи. Коли генератор генерує 3D хаотичні сигнали, канал wTx тимчасово вимикається. Крім того, модуль підлеглої системи, показаний на рисунку 2.1, також має реалізований генератор за формули (1.1), а сигнали clk і $ctrl$ представляють головний такт та контрольний сигнал відповідно, що перемикають синхронізовані підлеглі генератори хаосу на той самий сегмент основних систем, що використовуються для генерації складених носійних сигналів. Сигнали wRx, xRx, yRx і zRx представляють канали підлеглого генератора, а сигнали $SincCH1$, $SincCH2$, $SincCH3$ і $SincCH4$ є зворотними сигналами для коригування помилок шляху підлеглого генератора. На рисунку 2.2а показано канал w складених носійних сигналів для передавача, а канал w для приймача показано на рисунку 2.2б. Рисунок 2.2в показує канал x передавача, а рис. 2.2г — канал x приймача, тоді як рисунок 2.2д показує ті самі сигнали в програмному забезпеченні Vivado після 3 мс.

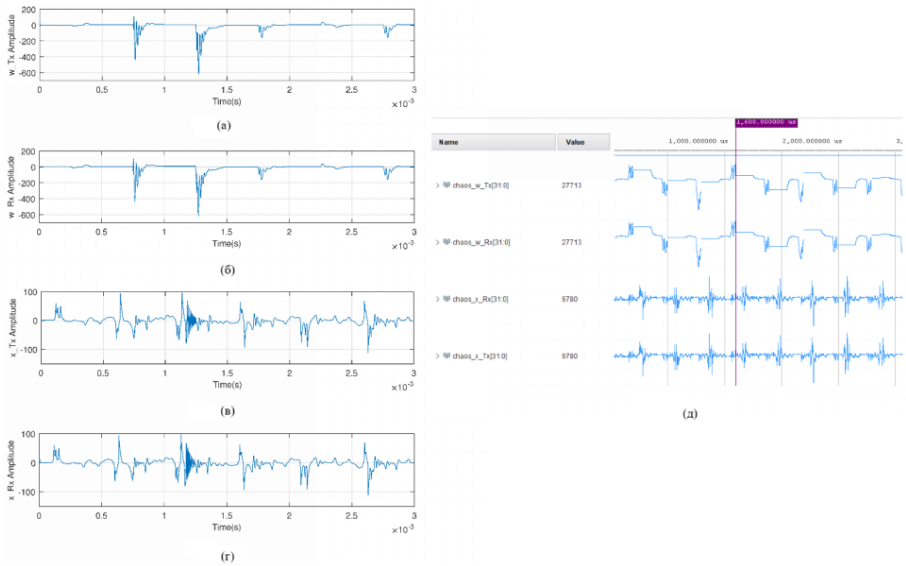


Рис. 2.2. Канали w і x переналаштовуваного генератора хаосу для складеного носія. (а) w_Tx, (б) w_Rx, (в) x_Tx, (г) x_Rx, (д) канали w, x майстра та підлеглого в Vivado.

Для теоретичної перевірки використовувалась проста архітектура пам'яті RAM з подвійними портами. Схеми мали єдиний тактовий сигнал для читання та запису, синхронізований з основним тактовим сигналом. Шістнадцять елементів пам'яті було використано для підлеглого генератора хаосу та ще шістнадцять для майстер-генератора хаосу.

Кожен з цих елементів тимчасово зберігала хаотичні символи. На рисунку 2.1 зображено елементи пам'яті RAM, де clk позначає основний тактовий сигнал. $Rden$ і $Wren1$ — це сигналі модулі, які, якщо вони високі, дозволяють читання та запис у пам'ять відповідно. Якщо вони низькі, читання та запис неможливі. $Addin$ — це адреса запису, а $Addout$ — адреса читання.

Нарешті, сигнали $Sym1Txin$ і $Sym1Txout$ представляють дані, які потрібно записати і прочитати з пам'яті відповідно.

Елемент $ctrlRAMTx$ визначає, в яких елементах пам'яті будуть збережені сегменти символів модуляції. Процес збереження символів починається, коли сигнал $Wrsym$ стає високим.

На рис. 2.1 зображено елемент контролера читання та запису пам'яті RAM. В архітектурі є два таких модуля: один для майстер-генератора хаосу та інший для підлеглого генератора хаосу.

Процес залежить від лічильника, який скидається після десяти тисяч тактових циклів, що відповідає ширині кожного символу. Ці модулі зберігають символи кожного бітового кадру.

Сигнали $CPSKen$ та $Rden$ є сигналами модуляції. Коли ці сигнали високі, процес модуляції починає кодувати повідомлення, і читання в пам'ять дозволяється відповідно. $Addin$ відповідає адресі запису, а $Addout$ — адресі читання. Нарешті,

сигнали $wren1Tx$ - $wren16Tx$ є сигналами модуляції. Коли їхній стан високий, вони дозволяють запис в відповідну пам'ять.

Ці сигнали активуються по черзі через рівні періоди в десять тисяч ітерацій або 50 мікросекунд. На рисунку 2.1 блок A представляє з'єднання з $Wren$ для блоків пам'яті 3 до 15.

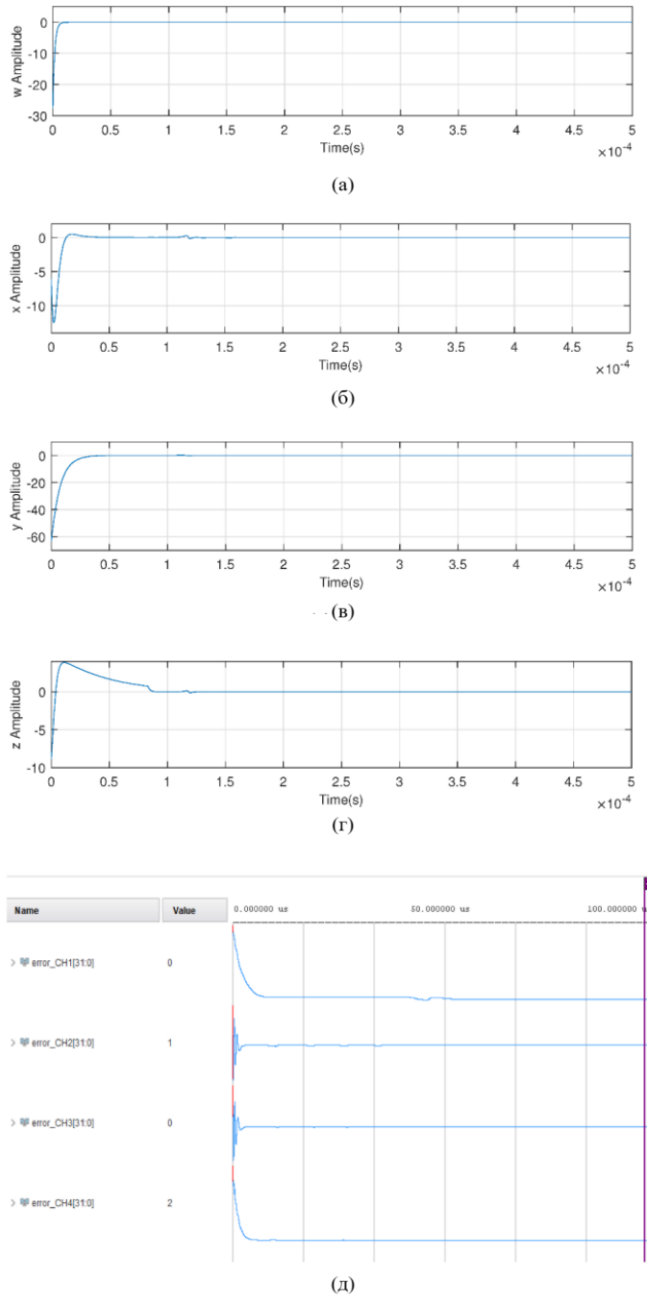


Рис. 2.3. Помилка синхронізації техніки 16-CPSK для каналів: (а) w, (б) x, (в) y та (г) z. (д) Помилка синхронізації у Vivado.

Зберігання кожного з символів завершується наступним чином:

- Синхронізація. Майстер- і підлеглі генератори хаосу синхронізуються, і сигнал wr_sym стає високим, що активує елемент $ctrlRAMTx$. Цей елемент починає зберігати сигнал $RAM1Tx$ в xTx майстер-генератора хаосу.

- Зберігання символу. Після десяти тисяч ітерацій завершується зберігання першого символу, і елемент $ctrlRAMTx$ починає зберігати вміст xTx у наступній пам'яті, $RAM2Tx$. Вже завантажені дані в пам'яті зберігають свій вміст до початку процесу оновлення символів. Процес заповнення пам'яті символами триває 700 мікросекунд від початку процесу з першою пам'яттю.

- Оновлення символів. Після того як всі 16 елементів пам'яті заповнені, процес повторюється, замінюючи вміст першої пам'яті, $RAM1Tx$, новим символом каналу xTx. Потім замінюється наступна пам'ять, $RAM2Tx$.

- Кінець зберігання символу. Коли зберігання символу 15 завершується, сигнал $CPSKen$ стає високим, що активує процес модуляції через елемент $CPSKmod$.

Елемент модулятора 16-CPSK зображений на рис. 2.1.

Процес модуляції починається, коли сигнал $CPSKen$ високий, і інформація, надана цифровим сигналом MSN, групується в 4-бітні пакети. Залежно від стану бітів вибирається символ з пам'яті модуля: $Sym1Txout - Sym16Txout$. Блок B відповідає за з'єднання $SymTxout$ пам'ятей RAM з 3 по 15. На рисунку 2.4 зображено модуляцію цифрового сигналу MSN[3:0] за допомогою техніки 16-CPSK. Окрім того, рисунки 8a–d відповідають повідомленню. Також рис. 8e відповідає 16-CPSK модуляційному сигналу в MATLAB, а рисунок 8f — повідомленню, модуляційному за допомогою 16-CPSK у Vivado. У цьому випадку модуляційний сигнал $CPSKTx$[13:0] починається після 1600 мікросекунд, коли завершено зберігання символів.

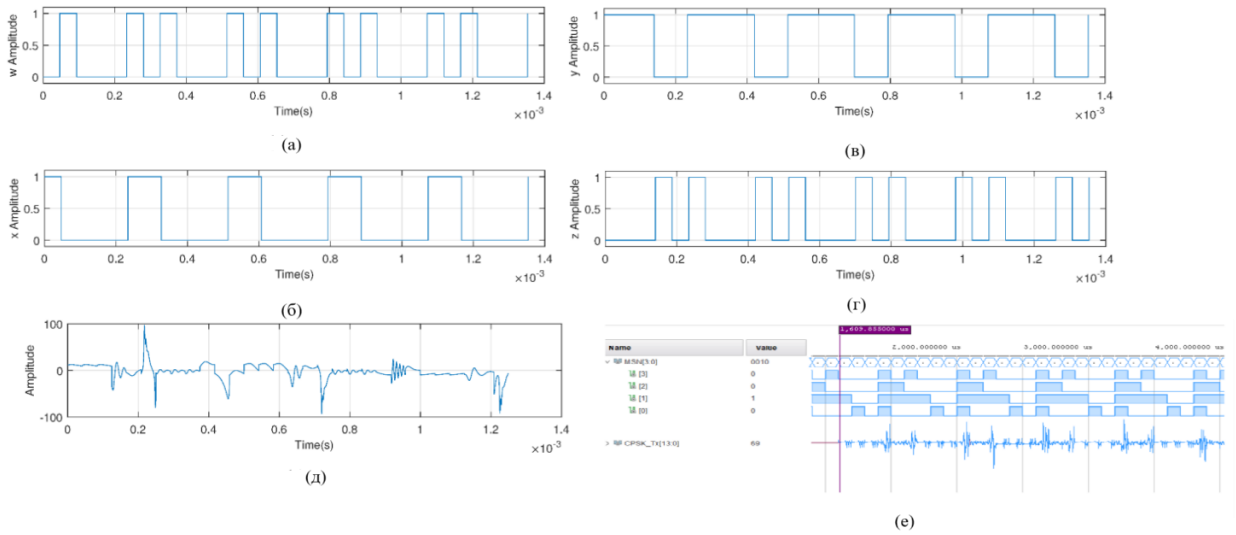


Рис. 2.4. Симуляція в Vivado 16-CPSK хаотичного модулятора. (а–г) Повідомлення, (д) 16-CPSK модуляція, (е) модуляція повідомлення у Vivado.

Робота 16-CPSK демодулятора показана на рис. 2.1. Процес демодуляції починається, коли сигнал $CPSKDen$ встановлюється в високий стан. У цей момент модульований сигнал $CPSKTx$ порівнюється з кожним з символів, збережених у пам'яті, які мають назви $Sym1Rxout$ до $Sym16Rxout$. Цей процес синхронізується з основним годинниковим сигналом clk. На основі кореляції між отриманим символом і символом, збереженим у пам'яті, повертається результат демодуляції, що відповідає повідомленню MSN.

2.3. Висновки до Розділу 2

У другому розділі було виконано теоретичну реалізацію системи модуляції-демодуляції 16-CPSK на основі хаотичних генераторів. Використання мови VHDL дозволило створити ефективну апаратну реалізацію із застосуванням FPGA.

Основними результатами стали:

- Розробка та реалізація системи переналаштовуваних генераторів хаосу в конфігурації "майстер–підлеглий". Цей підхід забезпечив стійкість до перешкод і адаптацію системи до змінних умов передачі.

- Використання шести типів генераторів (3D і 4D) для формування складеного носія, що дозволило досягти високої ефективності в задачах передачі та синхронізації.
- Розробка алгоритмів зберігання символів у пам’яті RAM з подвійними портами для передачі даних у форматі 16-CPSK. Це дозволило зберігати синхронізовані символи й мінімізувати помилки під час передачі.
- Виконано симуляцію роботи модуляторів і демодуляторів у середовищі Vivado, що підтвердило їхню ефективність для задач шифрування й передачі даних.

Отримані результати показали, що розроблена система забезпечує високу надійність, стійкість до перешкод і адаптивність у сучасних інформаційних середовищах.

РОЗДІЛ 3
НАУКОВО-ДОСЛІДНА РОБОТА

3.1. Дослідження продуктивності техніки 16-CPSK у передачі даних

У цьому дослідженні запропоновано методику хаотичної модуляції з використанням гамільтонової синхронізації. Техніка передбачає використання 4-канального переналаштовуваного генератора хаосу як у ведучій, так і у веденій системах. Під час процесу передачі генератор змінює свій режим від одного типу хаотичного генератора до іншого. Схема процесу шифрування та дешифрування інформації представлена на рисунку 3.1. У цьому процесі використовуються X-OR шифрування для файлів зображень у форматі RGB та градаціях сірого перед модуляцією 16-CPSK.

Етапи процесу шифрування в модуляторі:

- Хаотичний сигнал отримується з ведучої переналаштовуваної системи.
- Цифровий сигнал генерується з хаотичного сигналу.

- Шифрований сигнал формується за допомогою операції X-OR між цифровим хаотичним сигналом і цифровим сигналом даних.

Для шифрування використовуються хаотичні носії, які змінюються через регулярні інтервали, задані користувачем. Ці носії імітують форми хвиль, отримані від генераторів хаосу Ванга, Ці, ван Вайка, Лая, Чжоу та Чен-Чжоу [27,28,29,30,31,32].

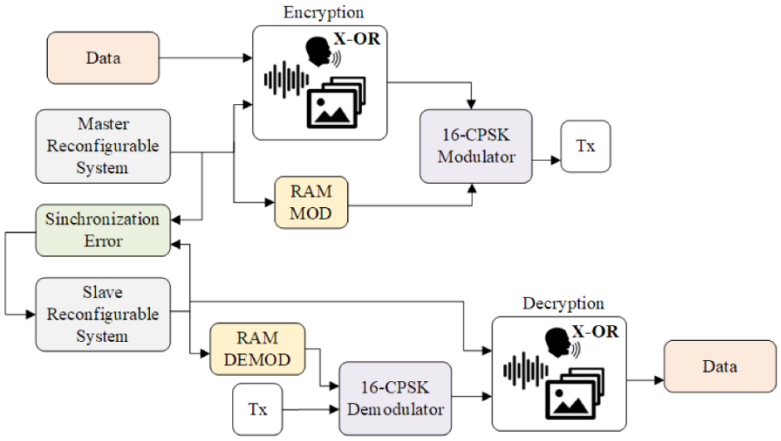


Рис. 3.1. Схема модуляції та демодуляції 16-CPSK

Процес демодуляції 16-CPSK включає: (1) синхронізацію, (2) генерацію символів, (3) кореляцію символів і (4) демодуляцію.

Для демодуляції 16-CPSK необхідно виконати кілька кроків у правильній послідовності. Ці кроки охоплюють синхронізацію, генерацію символів, кореляцію символів та, зрештою, демодуляцію. Важливо, щоб кожен етап виконувався коректно для успішної демодуляції.

Перші 16 символів генератора хаосу тимчасово зберігаються у елементі пам’яті. Ці символи прив’язуються до відповідних наборів бітів. Процес синхронізації, генерації та оновлення символів ілюстровано на рис. 3.2. Як показано, для синхронізації знадобилося близько 500 ітерацій. Генерація 16 символів зайняла 8000 ітерацій, оскільки кожен символ має довжину 500 ітерацій. Після цього символи оновлюються безперервно до завершення довжини повідомлення.

Для ідентифікації символів, отриманих приймачем, використовується техніка кореляції. Ця техніка дозволяє відновити оригінальну інформацію навіть за наявності

перешкод. Хаотичний режим роботи генератора хаосу полегшує ідентифікацію відповідного символу на основі поточного періоду, оскільки згенеровані символи є унікальними та ніколи не повторюються.

Відновлення оригінального інформаційного сигналу здійснюється шляхом визначення сегментів сигналу з найвищою кореляцією серед отриманих пакетів даних.

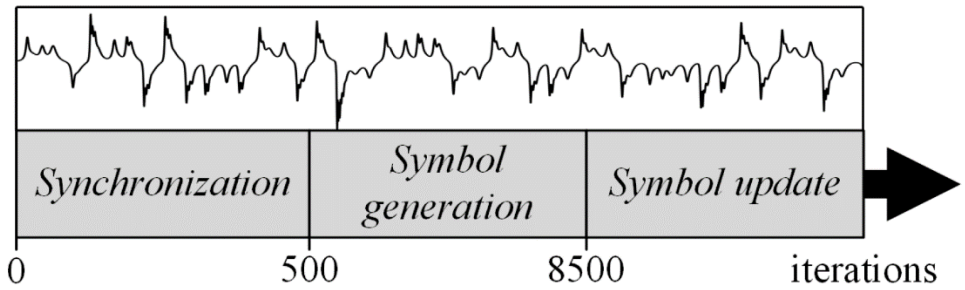


Рис. 3.2. Схема таймінгу процесу синхронізації, генерації та оновлення символів

Для оцінки продуктивності модулятора було використано програмне забезпечення MATLAB версії 2020b для тестування різних зображень у форматах RGB і відтінків сірого.

Під час тестів шифрування використовувалися різні зображення в обох форматах, щоб продемонструвати, що результати шифрування залежать від таких факторів, як генератор хаосу, канал генератора хаосу та інформація, яка шифрується. Запропонована в цьому дослідженні система застосовувалася для шифрування зображень із використанням різних генераторів хаосу та для шифрування різних зображень з кожним із цих генераторів.

Для моделювання використовувалися кілька зображень розміром 256×256 пікселів із бази даних USC-SIPI, серед яких: Airplane, Tree, Mandrill і Peppers у форматі RGB, а також Couple, Male, Stream і Boat у відтінках сірого. Ця інформація взята із джерела [37].

Рис. 3.3 і Рис. 3.4 демонструють результати шифрування для зображень у форматах RGB і відтінків сірого відповідно. Ці рисунки показують, що зашифровані зображення не мають жодної схожості з оригінальними, що підтверджує ефективний захист модульованої інформації. Крім того, було оцінено різні аспекти запропонованого процесу шифрування та модуляції.

(а) (б) (в) (г)

Рис. 3.3. Зображення у форматі RGB: оригінальні та зашифровані. (а) Літак, (б) Дерево, (в) Мандрил, (г) Перець.

(а) (б) (в) (г)

Рис. 3.4. Відтінки сірого, оригінальні зображення та зашифровані. (а) Пара, (б) Чоловік, (в) Потік, (г) Човен.

3.2. Дослідження чутливості для методу шифрування

Аналіз чутливості є метрикою, яка використовується для оцінки точності відновлення початкового сигналу за умови використання некоректних ключів. У цьому випадку були проведені зміни параметрів c та e, а також змінних шифрування x, y та z з відхиленням 1×10^{-13}. На рис. 3.5 показано початкове зображення та зображення, розшифровані з використанням некоректних ключів. Аналіз чутливості також є тестом на стійкість системи шифрування до криптографічних атак методом повного перебору.

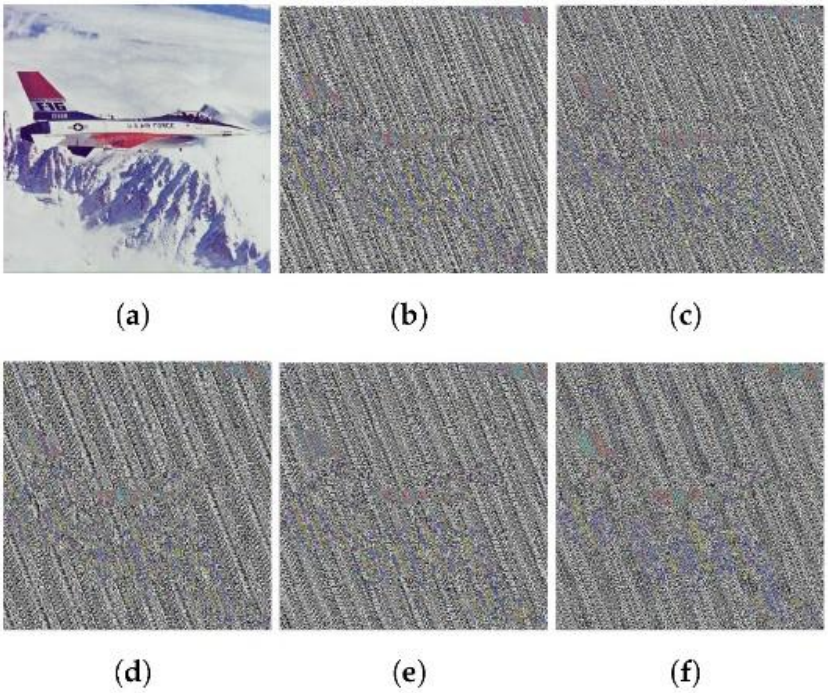


Рис. 3.5. Чутливість до змін параметрів запропонованої системи: (а) без змін; (б) c=1.0000000000001; (в) e=−43.0000000000001; (г) x=1.0000000000001; (д) y=1.0000000000001; (е) z=1.0000000000001.

3.3. Перевірка відновлюваності зображення

Аналіз приховування RGB-зображення представлений на рис. 3.6, де видалено 6.25%, 12.5% та 25% зашифрованого зображення. Цей аналіз дає змогу перевірити

відновлюваність оригінального зображення за допомогою сутності демодуляції 16-CPSK. Дослідження ефективно демонструє здатність відновити оригінальне зображення після видалення частини зашифрованого зображення.

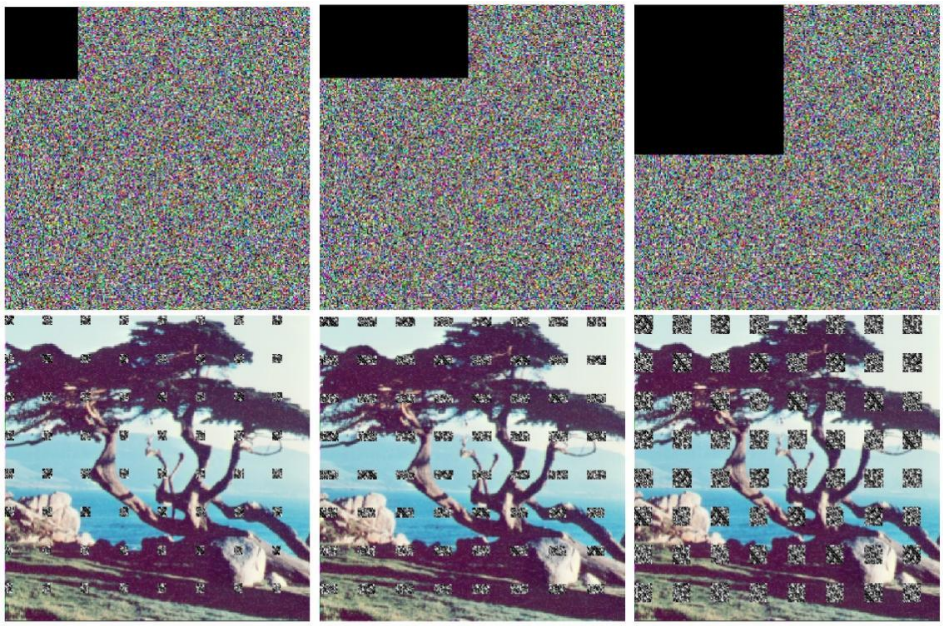


Рис. 3.6. Дешифрування із втратою інформації. (a) Втрата 6.25%, (b) втрата 12.5%, (c) втрата 25%

3.4. Аналіз коефіцієнта кореляції

Коефіцієнт кореляції є важливою мірою схожості між двома векторами. Коефіцієнт кореляції, близький до нуля, вказує на відсутність схожості, тоді як коефіцієнт, близький до одиниці, свідчить про високу схожість. Зворотно, коефіцієнт, близький до мінус одиниці, вказує на високу зворотну схожість між двома векторами. У цьому дослідженні наша мета полягає в забезпеченні хорошої процедури шифрування шляхом підтримання коефіцієнтів кореляції близькими до нуля. У таблицях 2, 3, 4 та 5 наведені результати коефіцієнтів кореляції для шифрування зображень у форматах RGB і grayscale, використовуючи змінні x, y і z для 3D генераторів хаосу та w, x, y і z для 4D генераторів хаосу. Коефіцієнти кореляції демонструють ефективність запропонованого методу шифрування зображень. Крім

того, для зображень у форматі RGB найнижчий коефіцієнт кореляції серед зображень отримано для зображення Airplane, при використанні змінної x генератора хаосу Qi для червоної матриці, який склав -15.9×10^{-6}. Для зображень у форматі grayscale найнижчий коефіцієнт кореляції був отриманий для зображення Male і складав 0.13×10^{-3}, при використанні змінної шифрування z.

Таблиця 3.2

Коефіцієнти кореляції та ентропії при шифруванні зображень RGB за допомогою 3D генераторів хаосу.

Зображення	Змінна шифрування	Червоний	Осцилятор Ван Зелений	Синій	Ентропія Зашифр. оригінал	
Літак	x	3.56×10-3	2.33×10-3	2.3×10-3	7.9912	6.799
	y	−3.09×10-3	−0.74×10-3	2.48×10-3	7.994	
	z	−0.39×10-3	−3.56×10-3	0.41×10-3	7.8894	
Дерево	x	5.6×10-3	4.92×10-3	1.84×10-3	7.997	7.4136
	y	−7.83×10-3	3.27×10-3	2.32×10-3	7.9974	
	z	−8.16×10-3	0.48×10-3	−6.59×10-3	7.9719	
Мандрил	x	3.17×10-3	3.12×10-3	3.77×10-3	7.9995	7.4744
	y	1.44×10-3	−0.46×10-3	3.97×10-3	7.9998	
	z	0.3×10-3	−2.7×10-3	−4.93×10-3	7.9971	
Перці	x	−2.07×10-3	0.6×10-3	0.18×10-3	7.999	7.4963
	y	1.04×10-3	−0.9×10-3	0.59×10-3	7.9994	
	z	2.88×10-3	−3.24×10-3	−0.28×10-3	7.9874	
Зображення	Змінна шифрування	Червоний	Осцилятор Ци Зелений	Синій	Ентропія оригінал	Зашифр.
Літак	x	−15.9×10-3	3.54×10-3	3.11×10-3	7.9916	6.799
	y	−3.19×10-3	−1.66×10-3	−0.7×10-3	7.9863	
	z	0.78×10-3	2.39×10-3	−1.35×10-3	7.9577	

Дерево	x	4.36×10-3	2.63×10-3	0.47×10-3	7.9977	7.4136
	y	−0.3×10-3	2.59×10-3	4.49×10-3	7.9964	
	z	5.83×10-3	2.08×10-3	2.58×10-3	7.9926	

Продовж. табл. 3.2

Мандрил	x	1.23×10-3	2.16×10-3	8.38×10-3	7.9996	7.4744
	y	−2.04×10-3	−0.69×10-3	−0.48×10-3	7.9996	
	z	2.28×10-3	1.26×10-3	−1.67×10-3	7.9988	
Перці	x	−3.17×10-3	−1.49×10-3	−0.24×10-3	7.999	7.4963
	y	−0.35×10-3	1.22×10-3	2.24×10-3	7.9987	
	z	−3.36×10-3	1.23×10-3	3.6×10-3	7.9958	
Зображення	Змінна шифрування	Червоний	Осцилятор Ван Вик Зелений	Синій	Ентропія Зашифр. оригінал	
Літак	x	−3.3×10-3	−0.39×10-3	0.56×10-3	7.8384	6.799
	y	−2.52×10-3	−0.54×10-3	−0.36×10-3	7.8165	
	z	2.52×10-3	−2.08×10-3	−0.9×10-3	7.4404	
Дерево	x	−2.05×10-3	3.47×10-3	2.27×10-3	7.9405	7.4136
	y	2.68×10-3	3.21×10-3	4.6×10-3	7.9358	
	z	−7.78×10-3	−0.16×10-3	−2.89×10-3	7.7387	
Мандрил	x	3.32×10-3	1.55×10-3	2.97×10-3	7.9959	7.4744
	y	1.61×10-3	0.58×10-3	3.18×10-3	7.9949	
	z	−2.99×10-3	−4.92×10-3	−5.28×10-3	7.9801	
Перці	x	−2.71×10-3	2.51×10-3	2.36×10-3	7.9816	7.4963
	y	−2.89×10-3	3.42×10-3	3.41×10-3	7.9773	
	z	7.8×10-3	−7.11×10-3	−2.63×10-3	7.9112	

Таблиця 3.3

Коефіцієнти кореляції та ентропії при шифруванні чорно-білих зображень за допомогою 3D генераторів хаосу.

Ци осцилятор				
Зображення	Змінна шифрування	Кореляція Коефіцієнт	Ентропія Зашифровано	оригінал

Продовж. табл. 3.3

Пара	x	-1.69×10^{-3}	7.9990	7.201
	y	-1.7×10^{-3}	7.9920	
	z	1.03×10^{-3}	7.9949	
Чоловік	x	2.7×10^{-3}	7.9969	7.5237
	y	1.97×10^{-3}	7.9987	
	z	-6.59×10^{-3}	7.9463	
Потік	x	0.48×10^{-3}	7.9982	5.7056
	y	-4.79×10^{-3}	7.9978	
	z	7.86×10^{-3}	7.9644	
Човен	x	-0.64×10^{-3}	7.9975	7.1914
	y	-3.31×10^{-3}	7.9978	
	z	6×10^{-3}	7.9741	
Осцилятор Ван				
Зображення	Змінна шифрування	Кореляція Коефіцієнт	Ентропія Зашифровано	оригінал
Пара	x	-1.69×10^{-3}	7.9990	7.201
	y	-1.7×10^{-3}	7.9920	
	z	1.03×10^{-3}	7.9949	
Чоловік	x	2.7×10^{-3}	7.9969	7.5237
	y	1.97×10^{-3}	7.9987	
	z	-6.59×10^{-3}	7.9463	
	x	0.48×10^{-3}	7.9982	5.7056

Потік	y	-4.79×10^{-3}	7.9978	
	z	7.86×10^{-3}	7.9644	
Човен	x	-0.64×10^{-3}	7.9975	7.1914
	y	-3.31×10^{-3}	7.9978	
	z	6×10^{-3}	7.9741	

Продовж. табл. 3.3

Осцилятор ван Вика				
Зображення	Змінна шифрування	Кореляція Коефіцієнт	Ентропія Зашифровано оригінал	
Пара	x	-4.01×10^{-3}	7.9924	7.201
	y	-2.81×10^{-3}	7.9905	
	z	4.81×10^{-3}	7.9534	
Чоловік	x	10.19×10^{-3}	7.9273	7.5237
	y	10.32×10^{-3}	7.9178	
	z	-14.74×10^{-3}	7.8185	
Потік	x	-7.56×10^{-3}	7.9489	5.7056
	y	-10.26×10^{-3}	7.9336	
	z	13.34×10^{-3}	7.7585	
Човен	x	-6.17×10^{-3}	7.9573	7.1914
	y	-6.84×10^{-3}	7.9504	
	z	10.7×10^{-3}	7.794	

Таблиця 3.4

Коефіцієнти кореляції та ентропії при шифруванні RGB зображень за допомогою 4D генераторів хаосу.

Осцилятор Лай

Зображення	Змінна шифрування	Червоний	RGB зображення зелений	Синій	Ентропія Зашифр. оригінал	
Літак	w	7.26×10^{-3}	3.36×10^{-3}	-1.13×10^{-3}	7.9451	6.799
	x	0.49×10^{-3}	1.25×10^{-3}	0.49×10^{-3}	7.9332	
	y	1.66×10^{-3}	2.28×10^{-3}	16.56×10^{-3}	7.9185	

Продовж. табл. 3.4

	z	-4.46×10^{-3}	0.29×10^{-3}	0.93×10^{-3}	7.9398	
Дерево	w	0.87×10^{-3}	-5.24×10^{-3}	-0.89×10^{-3}	7.9511	7.4136
	x	4.45×10^{-3}	-3.92×10^{-3}	-3.09×10^{-3}	7.9775	
	y	2.11×10^{-3}	-5.1×10^{-3}	-2.68×10^{-3}	7.9782	
	z	2.75×10^{-3}	4.55×10^{-3}	6.01×10^{-3}	7.9862	
Мандрил	w	1.22×10^{-3}	5.6×10^{-3}	4.87×10^{-3}	7.9992	7.4744
	x	1.93×10-3	4.07×10^{-3}	1.26×10^{-3}	7.9983	
	y	1.7×10^{-3}	2.39×10^{-3}	1.43×10^{-3}	7.9978	
	z	0.95×10^{-3}	2.21×10^{-3}	3.93×10^{-3}	7.9985	
Перці	w	-3.12×10^{-3}	19.9×10^{-3}	4.73×10^{-3}	7.9959	7.4963
	x	-3.65×10^{-3}	10.45×10^{-3}	2.1×10^{-3}	7.993	
	y	-4.68×10^{-3}	10.6×10^{-3}	2.02×10^{-3}	7.9909	
	z	-1.27×10^{-3}	5.62×10^{-3}	3.66×10^{-3}	7.9936	
Осцилятор Чжоу						
Зображення	Змінна шифрування	Червоний	RGB зображення зелений	Синій	Ентропія Зашифр. оригінал	
Літак	w	-0.82×10^{-3}	-1.71×10^{-3}	-0.94×10^{-3}	7.7295	6.799
	x	2.85×10^{-3}	-2.37×10^{-3}	-1.43×10^{-3}	7.4823	

	y	2.58×10^{-3}	-2.42×10^{-3}	-1.53×10^{-3}	7.4980	
	z	0.66×10^{-3}	4.52×10^{-3}	8.44×10^{-3}	7.8355	
Дерево	w	-3×10^{-3}	9.91×10^{-3}	11×10^{-3}	7.8381	7.4136
	x	-7.34×10^{-3}	0.74×10^{-3}	-0.70×10^{-3}	7.7603	
	y	-7.11×10^{-3}	0.79×10^{-3}	-0.22×10^{-3}	7.7682	

Продовж. табл. 3.4

	z	2.17×10^{-3}	1.23×10^{-3}	0.60×10^{-3}	7.8555	
Мандрил	w	-2.84×10^{-3}	-7.88×10^{-3}	-6.42×10^{-3}	7.921	7.4744
	x	-3.02×10^{-3}	-4.99×10^{-3}	-5.48×10^{-3}	7.9819	
	y	-3.35×10^{-3}	-5.22×10^{-3}	-6.28×10^{-3}	7.9826	
	z	1.52×10^{-3}	-2.09×10^{-3}	-3.09×10^{-3}	7.9969	
Перці	w	6.14×10^{-3}	-11.9×10^{-3}	-1.69×10^{-3}	7.9642	7.4963
	x	7.30×10^{-3}	-7.87×10^{-3}	-3.45×10^{-3}	7.9191	
	y	7.23×10^{-3}	-8.30×10^{-3}	-3.62×10^{-3}	7.9219	
	z	9.32×10^{-3}	-10.7×10^{-3}	0.525×10^{-3}	7.983	
Осцилятор Чень-Чжоу						
Зображення	Змінна шифрування	Червоний	RGB зображення зелений	Синій	Ентропія Зашифр. оригінал	
Літак	w	-2.52×10^{-3}	2.08×10^{-3}	0.9×10^{-3}		
	x	1.27×10^{-3}	4.41×10^{-3}	2.98×10^{-3}	7.7314	6.799
	y	-1.14×10^{-3}	3.46×10^{-3}	1.84×10^{-3}	7.5566	

	z	1.06×10^{-3}	7.14×10^{-3}	2.31×10^{-3}	7.8285	
Дерево	w	7.78×10^{-3}	0.16×10^{-3}	2.89×10^{-3}	7.7387	7.4136
	x	6.69×10^{-3}	-6.89×10^{-3}	-5.51×10^{-3}	7.8539	
	y	8.56×10^{-3}	2.04×10^{-3}	3.53×10^{-3}	7.7940	
	z	4.93×10^{-3}	6.22×10^{-3}	10.49×10^{-3}	7.8539	
Мандрил	w	2.99×10^{-3}	4.92×10^{-3}	5.28×10^{-3}	7.9801	7.4744

Продовж. табл. 3.4

	x	4.37×10^{-3}	7.61×10^{-3}	5.86×10^{-3}	7.9920	
	y	4.13×10^{-3}	5.27×10^{-3}	4.27×10^{-3}	7.9847	
	z	7.16×10^{-3}	5.67×10^{-3}	0.71×10^{-3}	7.9971	
Перці	w	-7.8×10^{-3}	7.11×10^{-3}	2.63×10^{-3}	7.9112	7.4963
	x	-4.20×10^{-3}	13.89×10^{-3}	3.06×10^{-3}	7.9635	
	y	-7.54×10^{-3}	10.36×10^{-3}	3.68×10^{-3}	7.9323	
	z	2.30×10^{-3}	11.55×10^{-3}	13.46×10^{-3}	7.9792	

Таблиця 3.5

Коефіцієнти кореляції та ентропії при шифруванні зображень у градаціях сірого за допомогою 4D генераторів хаосу.

Осцилятор Лай				
Зображення	Змінна шифрування	Кореляція Коефіцієнт	Ентропія Зашифровано	оригінал
Пара	w	7.28×10^{-3}	7.9968	7.201
	x	-51.45×10^{-3}	7.9972	

	y	-0.82×10^{-3}	7.9961	
	z	-3.76×10^{-3}	7.9974	
Чоловік	w	-0.85×10^{-3}	7.9918	7.5237
	x	-1.2×10^{-3}	7.9931	
	y	-0.71×10^{-3}	7.9935	
	z	7.98×10^{-3}	7.9689	
Потік	w	9.77×10^{-3}	7.9878	5.7056
	x	6.47×10^{-3}	7.9863	
	y	6.1×10^{-3}	7.9851	

Продовж. табл. 3.5

	z	-4.43×10^{-3}	7.984	
Човен	w	7.04×10^{-3}	7.9894	7.1914
	x	2.51×10^{-3}	7.9883	
	y	2.11×10^{-3}	7.1914	
	z	-6.45×10^{-3}	7.9874	
Осцилятор Чжоу				
Зображення	Змінна шифрування	Кореляція Коефіцієнт	Ентропія Зашифровано	оригінал
Пара	w	-3.52×10^{-3}	7.9833	7.201
	x	4.81×10^{-3}	7.9534	
	y	2.71×10^{-3}	7.9614	
	z	-9.4×10^{-3}	7.9885	
Чоловік	w	-10.2×10^{-3}	7.8919	7.5237
	x	-14.74×10^{-3}	7.8151	
	y	-14.24×10^{-3}	7.8304	
	z	0.13×10^{-3}	7.9797	
Потік	w	0.53×10^{-3}	7.8930	5.7056

	x	13.34×10^{-3}	7.7585	
	y	11.99×10^{-3}	7.7872	
	z	-8.35×10^{-3}	7.9414	
Човен	w	9.77×10^{-3}	7.9116	7.1914
	x	10.7×10^{-3}	7.794	
	y	10.7×10^{-3}	7.8194	
	z	-12.93×10^{-3}	7.95	
Осцилятор Чень-Чжоу				
Зображення	Змінна шифрування	Кореляція Коефіцієнт	Ентропія Зашифровано	оригінал

Продовж. табл. 3.5

Пара	w	-4.81×10^{-3}	7.9534	7.201
	x	-1.60×10^{-3}	7.9841	
	y	-4.37×10^{-3}	7.9668	
	z	-10.61×10^{-3}	7.9888	
Чоловік	w	14.74×10^{-3}	7.8151	7.5237
	x	9.86×10^{-3}	7.8921	
	y	13×10^{-3}	7.8429	
	z	9.33×10^{-3}	7.9556	
Потік	w	-13.34×10^{-3}	7.7585	5.7056
	x	-3.76×10^{-3}	7.8926	
	y	-9.33×10^{-3}	7.8127	
	z	2.66×10^{-3}	7.9441	
Човен	w	-10.7×10^{-3}	7.794	7.1914
	x	-10.12×10^{-3}	7.109	
	y	-9.64×10^{-3}	7.8397	
	z	-15.93×10^{-3}	7.9539	

Метрика ентропії використовується для вимірювання ступеня розподілу пікселів у зображенні. Значення «8» відповідає випадковому розподілу значень пікселів. У цьому дослідженні максимальна ентропія становила 7.9998 для зображення Mandrill у форматі RGB при використанні змінної шифрування "y" та хаотичного осцилятора Ванга. Для зображень у градаціях сірого зображення Couple досягло ентропії 7.9991 при використанні змінної шифрування "x" хаотичного осцилятора Qi. Розрахунок ентропії базується на формулі (3.1).

$$E(N) = -\sum_{i=1}^{255} \quad p(u_i) log_2(p(u_i)). \tag{3.1}$$

Формулою визначає ймовірність кожного значення пікселя (ui) в зображенні, де $p(ui)$ є відповідною ймовірністю. Значення пікселів у зображенні варіюються від 0 до 255. Таблиці 3.2, 3.3, 3.4 та 3.5 надають результати ентропії для зображень у форматі RGB та градаціях сірого при використанні 3D та 4D генераторів.

Для відновлення оригінальної інформації без втрат, цей аналіз визначає рівень шуму, який може витримати техніка модуляції. Одне з зображень було забруднене шумом різної величини для перевірки його відновлення. Додавання гаусового шуму моделюється формули (3.2):

$$I_N = I + gN, \tag{3.2}$$

I_N представляє зашифроване зображення з доданим шумом, I — початкове зашифроване зображення, g — коефіцієнт інтенсивності шуму, N — змінна гаусового адитивного білого шуму з дисперсіями 0.1, 0.01, 0.001, 0.0001. Рис. 3.7 показує результати додавання шуму та відновлення зображення, а Таблиця 3.6 демонструє вплив шуму на основі коефіцієнта кореляції.

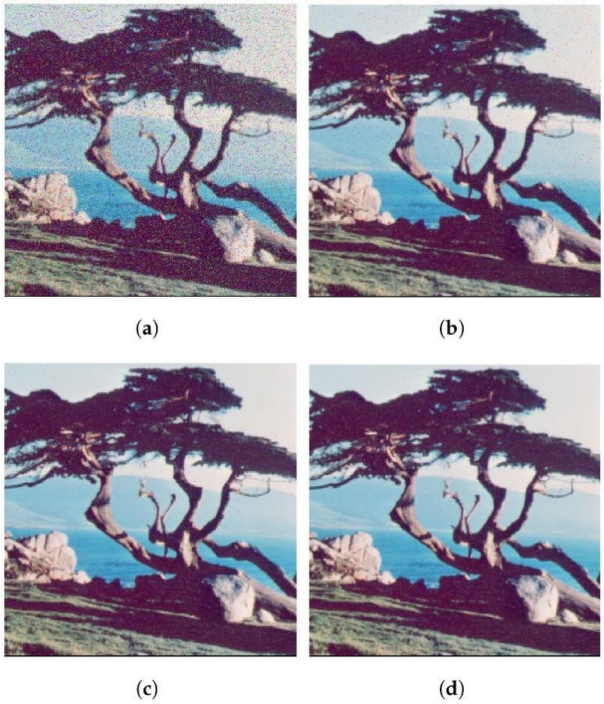


Рис. 3.7. Зображення, відновлені після введення гаусового білого шуму з нульовим середнім: (a) при дисперсії 0.1, (b) при дисперсії 0.01, (c) при дисперсії 0.001, та (d) при дисперсії 0.0001.

Таблиця 3.6

Вплив гаусового білого шуму з нульовим середнім при різних значеннях дисперсії на відновлені зображення.

Метрика	Відхилення 0,1	Відхилення 0,01	Відхилення 0,001	Відхилення 0,0001
Коефіцієнт кореляції	0.7587	0.9707	0.9969	0.9997
Відсоток відновлення	75%	97%	99.6%	99.9%

Логічні ресурси на FPGA

Таблиця 3.7 показує апаратні ресурси, необхідні для системи модуляції-демодуляції 16-CPSK. Модулі передавача та приймача використовують системи головного та підлеглого осцилятора для генерації хвильових форм різних хаотичних осциляторів. Модулятор та демодулятор кодують і шифрують повідомлення у

передавачі, а також дешифрують та декодують інформацію в приймачі. Система синхронізації захоплює сигнал носія передавача та приймача для їх синхронізації. Контролери RAM для Tx та Rx зберігають символи модуляції 16-CPSK як для модулятора, так і для демодулятора. Останнім елементом є схема x32 RAM, яка зберігає пам'ять для символів модуляції та демодуляції 16-CPSK.

Однією з потенційних проблем, яку може зустріти запропонована система, є вимоги до логічних ресурсів системи модуляції 16-CPSK, зокрема у використанні пам'яті.

Запропонованим рішенням є оптимізація системи для більш ефективного розподілу елементів пам'яті плати FPGA та зменшення частоти дискретизації збережених сигналів. Це допоможе зменшити навантаження на пам'ять, при цьому зберігаючи продуктивність і дозволяючи системі функціонувати ефективно в різних FPGA-конфігураціях.

Таблиця 3.7

Логічні ресурси, що використовуються системою модуляції-демодуляції 16-CPSK, з використанням карти ARTIX-7 AC701

Сутність	LUTs (134,600)	РЕЄСТРИ (269 200)	BRAM (365)	DSP (740)	I/O (400)	BUFF (32)
Головна сутність	24,472 (18.8%)	2684 (0.95%)	224 (61.35%)	562 (75.95%)	0 (0%)	2(6.25%)
Головний осцилятор	6402	503	0	280	0	
Підлеглий осцилятор	6640	539	0	282	0	0
Демодулятор	1782	520	0	0	0	0
Модулятор	447	78	0	0	0	0

Синхронізація	145	128	0	0	0	0
RAMTx Контроллер	167	500	0	0	0	0
RAMRx Контроллер	122	416	0	0	0	0
RAMx32 Контроллер	672	0	224	0	0	0

3.5. Висновки до Розділу 3

У третьому розділі було проведено науково-дослідну роботу, спрямовану на оцінку ефективності системи модуляції 16-CPSK для задач шифрування і передачі даних.

Основні результати:

Виконано дослідження продуктивності техніки 16-CPSK у передачі даних. Показано, що використання гамільтонової синхронізації та переналаштовуваних генераторів хаосу дозволяє забезпечити високу точність передачі навіть за умов змінних параметрів середовища.

Проведено аналіз чутливості методу шифрування до змін параметрів та ключів. Встановлено, що запропонована система демонструє високу стійкість до криптографічних атак методом повного перебору.

Виконано перевірку відновлюваності зображень після часткової втрати даних. Дослідження показало здатність системи до ефективного відновлення інформації за допомогою демодуляції 16-CPSK.

Проведено аналіз коефіцієнтів кореляції між оригінальними та зашифрованими даними. Отримані результати підтвердили високий рівень безпеки шифрування, оскільки коефіцієнти кореляції залишаються близькими до нуля.

Результати науково-дослідної роботи підтвердили ефективність запропонованої системи для задач захисту даних і передачі інформації. Система

забезпечує високу точність, стійкість до перешкод і криптографічних атак, що робить її перспективною для практичного застосування.

РОЗДІЛ 4

ОХОРОНА ПРАЦІ ТА БЕЗПЕКА В НАДЗВИЧАЙНИХ СИТУАЦІЯХ

4.1. Електробезпека при роботі з шифрувальними системами FPGA

Робота з FPGA (Field-Programmable Gate Array) у шифрувальних системах передбачає використання складних апаратних компонентів, які працюють під високою напругою та можуть створювати значну кількість небезпечних ситуацій для користувачів. Основні ризики пов’язані з ураженням електричним струмом, пошкодженням обладнання через статичну електрику або перевантаження, а також перегрівом компонентів. Кожен із цих факторів вимагає ретельного аналізу та запровадження заходів для мінімізації небезпеки[58].

Одним із найсерйозніших ризиків під час роботи з FPGA є ураження електричним струмом. Цей ризик виникає внаслідок неправильної експлуатації обладнання або порушення стандартів електробезпеки. Типові ситуації, які можуть призвести до ураження струмом:

- Прямий контакт зі струмопровідними частинами. Це трапляється, якщо оператор випадково торкається відкритих елементів плати, які перебувають під напругою. У таких випадках напруга навіть у 12-24 В, яка вважається низькою, може бути небезпечною залежно від опору тіла, а напруга понад 50 В може спричинити серйозні травми[56].
- Пошкодження ізоляції. Кабелі живлення або з’єднувальні дроти, що втратили ізоляційний шар, створюють ризик витоку струму[55]. Це може бути наслідком зношення матеріалу, фізичних пошкоджень під час монтажу або використання неякісних компонентів.
- Високовольтні компоненти. У шифрувальних системах FPGA часто використовуються блоки живлення, які працюють на високих напругах (від 220 В у мережі до понад 400 В у схемах перетворення). Контакт із такими джерелами струму може спричинити опіки, м’язові спазми або навіть зупинку серця.

- Несправне або ненадійне обладнання. Використання старих або пошкоджених блоків живлення, перетворювачів чи адаптерів підвищує ймовірність аварій. Наприклад, нестабільність напруги в джерелі живлення може створити перевантаження або пробій компонентів.

Наслідки ураження струмом варіюються від короткочасного дискомфорту до серйозних травм, включаючи опіки шкіри, порушення роботи серцево-судинної системи чи навіть летальний випадок. Тому першочерговим завданням є забезпечення ефективних систем захисту та дотримання правил безпеки[56].

FPGA-плати є чутливими до різних впливів, які можуть знизити їхню працездатність або повністю вивести з ладу. Основними причинами пошкодження обладнання є:

- Електростатичні розряди (ESD). Ці розряди виникають під час контакту з матеріалами, що мають різний електричний потенціал. Навіть розряд із напругою у 10 В, невідчутний для людини, може зруйнувати напівпровідникові елементи FPGA. У результаті мікросхема може стати частково або повністю непридатною для використання[55].

- Перевантаження по струму. FPGA-плати та їхні компоненти (пам’ять, регістри, буфери) мають чітко визначені параметри споживання струму. Використання блоків живлення із завищеними параметрами або підключення неправильних навантажень може призвести до перегріву або короткого замикання в ланцюгах живлення.

- Коротке замикання. Це явище виникає при замиканні струмопровідних частин через помилку монтажу, фізичне пошкодження або несправність компонентів. Окрім пошкодження плати, коротке замикання може стати причиною пожежі.

- Нестабільна робота джерела живлення. Перепади напруги або стрибки струму можуть спричинити пошкодження логічних елементів FPGA або викликати збої в роботі системи. Це особливо критично для шифрувальних систем, де збій може призвести до втрати даних або помилок у процесі шифрування.

Для уникнення цих проблем необхідно дотримуватись строгих правил експлуатації обладнання, використовувати стабільні джерела живлення з вбудованим захистом, а також регулярно перевіряти стан кабелів та з’єднань.

FPGA у шифрувальних системах працюють із високими навантаженнями, що може призводити до значного тепловиділення. Якщо система охолодження не справляється, компоненти можуть перегрітися, що спричиняє:

- Зниження продуктивності. Занадто високі температури призводять до уповільнення роботи FPGA через активацію захисних механізмів, таких як троттлінг.
- Пошкодження компонентів. Постійна робота при підвищених температурах викликає деградацію матеріалів, що використовуються у транзисторах, і може призвести до їх виходу з ладу.
- Потенційна пожежна небезпека. Перегрівання може спричинити займання ізоляції, кабелів або навіть самої плати.

Для боротьби з перегрівом використовуються активні та пасивні системи охолодження: вентилятори, теплові радіатори, а також спеціальні корпуси з підвищеною вентиляцією. Крім того, необхідно стежити за чистотою вентиляційних отворів, оскільки накопичення пилу значно знижує ефективність охолодження.

4.2. Безпека при аварійному вимкненні системи FPGA

Аварійне вимкнення системи FPGA є важливим аспектом забезпечення безпеки під час роботи. Воно дозволяє швидко припинити роботу обладнання в разі виникнення критичних ситуацій, таких як коротке замикання, перегрів компонентів, неконтрольовані електричні розряди або інші непередбачувані ситуації. Ефективна організація процедури аварійного вимкнення забезпечує безпеку як персоналу, так і обладнання.

Аварійне вимкнення в системах FPGA — це процес, при якому система автоматично вимикається або зупиняється, коли виявляється, що подальша робота може призвести до серйозних наслідків. Це може бути як повне вимкнення всіх

функцій системи, так і зупинка лише певних її компонентів або відновлення в безпечний стан. Механізм аварійного вимкнення часто включає використання додаткових сенсорів, контролерів та програмних алгоритмів, що виявляють небезпечні умови для подальшої роботи[58].

Основні елементи аварійного вимкнення наступні

Моніторинг є першочерговим елементом для виявлення загроз, що можуть вимагати аварійного вимкнення. Для цього використовуються різні апаратні та програмні засоби, які регулярно перевіряють ключові параметри роботи FPGA та пов'язаних з ним компонентів. Основні показники, що підлягають моніторингу, включають кілька параметрів.

Одним із основних факторів, що можуть призвести до помилок, є перегрів. Багато FPGA-систем мають вбудовані температурні датчики, які допомагають відслідковувати температуру чипа та інших важливих компонентів. Якщо температура перевищує безпечний рівень, система може ініціювати аварійне вимкнення.

Нестабільність або аномалії в напрузі можуть призвести до пошкодження чипа або збоїв в роботі логіки FPGA. Моніторинг напруги і споживаної потужності дозволяє швидко виявити такі проблеми і активувати відключення або перезавантаження системи[59].

Відсутність коректної роботи програмних або апаратних компонентів може призвести до втрати синхронізації. Watchdog таймери — це спеціальні таймери, які регулярно перевіряють, чи виконуються певні функції системи. Якщо ці функції не виконуються вчасно, таймер спрацьовує і запускає процес аварійного вимкнення.

FPGA-система зазвичай інтегрує численні входи та виходи для комунікації з іншими частинами системи. Моніторинг стану цих сигналів може виявити короткі замикання або інші проблеми, що загрожують безпеці, і спричинити аварійне вимкнення.

Ідентифікація критичних ситуацій — це етап, на якому система вирішує, чи потребує ситуація аварійного вимкнення. Це зазвичай відбувається після того, як

моніторинг виявив відхилення від нормального стану, і на основі певних алгоритмів система робить висновок про необхідність відключення або зупинки.

У разі виявлення серйозної помилки в програмному забезпеченні (наприклад, неправильний алгоритм або збій коду), система може визначити ситуацію як критичну і ініціювати аварійне вимкнення[60].

Якщо температура або напруга перевищують допустимі межі, це може призвести до деградації або пошкодження апаратних компонентів. Тому система може зупинити роботу FPGA, щоб уникнути більш серйозних наслідків.

У разі виявлення дефектів на рівні апаратного забезпечення, таких як збої в роботі пам'яті, логіки, або вихід з ладу критичних компонентів, система може автоматично вимкнути частину функцій або всю систему.

Якщо сигнали між модулями FPGA починають бути нестабільними або перериваються, це може свідчити про пошкодження апаратної частини або втрату зв'язку з іншими компонентами, що також викликає активацію аварійного вимкнення.

Після того, як виявлено критичну ситуацію, наступним етапом є активація аварійного вимкнення. Існують кілька варіантів того, як може бути реалізоване вимкнення:

У разі виявлення дуже серйозної проблеми (наприклад, коротке замикання чи критичне перевищення температури) система може бути вимкнена моментально, щоб уникнути подальших пошкоджень.

У деяких випадках аварійне вимкнення може відбуватися поетапно, коли система спочатку зупиняє менш критичні функції, а потім виконує відключення всіх компонентів для забезпечення безпеки.

В деяких системах після виявлення критичної помилки FPGA може бути перезавантажена або скинута для відновлення працездатності. Це дозволяє системі почати роботу знову, якщо помилка є тимчасовою або коригується за допомогою повторного запуску.

Якщо аварія стосується лише частини FPGA-системи, можна вимкнути лише певні модули або підсистеми, залишаючи інші функції працездатними. Це дозволяє мінімізувати вплив збоїв і зберегти частину працездатності.

4.3. Висновки до розділу 4

Визначено основні аспекти забезпечення електробезпеки при роботі з шифрувальними системами на основі FPGA. Показано, що використання високоякісного обладнання, дотримання стандартів безпеки та проведення регулярних інструктажів суттєво знижують ризики електротравматизму.

Обґрунтовано важливість інтеграції сучасних методів моніторингу напруги, температури та інших параметрів у системи на базі FPGA, що дозволяє своєчасно виявляти і запобігати потенційним аварійним ситуаціям.

Розглянуто вимоги до технічного обслуговування систем, включаючи регулярні перевірки та сертифікацію обладнання, що сприяє підвищенню надійності системи і зменшенню ймовірності виникнення небезпечних ситуацій.

ЗАГАЛЬНІ ВИСНОВКИ

У роботі представлені результати дослідження системи шифрування на основі 16-CPSK модуляції з використанням хаотичних генераторів. Проведено аналіз існуючих методів хаотичного шифрування та показано їхні переваги у забезпеченні захисту даних, а також виявлено недоліки, що стосуються складності реалізації та необхідності високих обчислювальних ресурсів.

Розроблено систему модуляції-демодуляції, засновану на переналаштовуваних генераторах хаосу, що працюють у конфігурації «майстер–підлеглий». Застосування шести типів генераторів (3D і 4D) дозволило забезпечити високий рівень ефективності, стійкість до перешкод та адаптивність системи до змін умов передачі. Використання VHDL і FPGA дозволило створити апаратно-ефективне рішення з високою продуктивністю.

Проведено дослідження ефективності системи у завданнях передачі зашифрованих даних, включаючи шифрування RGB та grayscale зображень. Аналіз результатів підтвердив надійність і високу стійкість запропонованої системи до атак, зокрема до методів повного перебору та перешкод. Досліджено чутливість системи до змін параметрів шифрування та продемонстровано здатність відновлювати дані навіть за втрати частини зашифрованої інформації.

Результати моделювання підтверджують, що запропонований метод забезпечує високу кореляційну відповідність, що мінімізує ризик розшифрування. Система може знайти широке застосування у сферах, що потребують високого рівня захисту інформації, включаючи телекомунікації, медичну діагностику та наукові дослідження.

ПЕРЕЛІК ПОСИЛАНЬ

1. Rawat, D.B.; Doku, R.; Garuba, M. Cybersecurity in Big Data Era: From Securing Big Data to Data-Driven Security. *IEEE Trans. Serv. Comput.* **2021**, *14*, 2055–2072. [**Google Scholar**] [**CrossRef**]

2. Lu, H.; Tang, W.K. Chaotic Phase Shift Keying in Delayed Chaotic Anticontrol Systems. Int. J. Bifurc. Chaos 2002, 12, 1017–1028. [Google Scholar] [CrossRef]

3. Lin, Y.; Xie, Z.; Chen, T.; Cheng, X.; Wen, H. Image privacy protection scheme based on high-quality reconstruction DCT compression and nonlinear dynamics. Expert Syst. Appl. 2024, 257, 124891. [Google Scholar] [CrossRef]

4. Michaels, A.J. A maximal entropy digital chaotic circuit. In Proceedings of the 2011 IEEE International Symposium of Circuits and Systems (ISCAS), Rio de Janeiro, Brazil, 15–18 May 2011; IEEE: Piscataway NJ, USA, 2011; pp. 717–720. [Google Scholar] [CrossRef]

5. Vali, R.; Berber, S.M.; Nguang, S.K. Effect of Rayleigh fading on non-coherent sequence synchronization for multi-user chaos based DS-CDMA. Signal Process. 2010, 90, 1924–1939. [Google Scholar] [CrossRef]

6. Liang, X.; Zhang, J.; Xia, X. A chaos-based CDMA scheme with a chaos-based encryption algorithm. IFAC Proc. Vol. 2009, 42, 110–115. [Google Scholar] [CrossRef]

7. Feng, W.; Qin, Z.; Zhang, J.; Ahmad, M. Cryptanalysis and Improvement of the Image Encryption Scheme Based on Feistel Network and Dynamic DNA Encoding. IEEE Access 2021, 9, 145459–145470. [Google Scholar] [CrossRef]

8. Wen, H.; Lin, U. Cryptanalyzing an image cipher using multiple chaos and DNA operations. J. King Saud-Univ.-Comput. Inf. Sci. 2023, 35, 101612. [Google Scholar] [CrossRef]

9. Wen, H.; Lin, Y. Cryptanalysis of an image encryption algorithm using quantum chaotic map and DNA coding. Expert Syst. Appl. 2024, 237, 121514. [Google Scholar] [CrossRef]

10. Toktas, F.; Erkan, U.; Yetgin, Z. Cross-channel color image encryption through 2D hyperchaotic hybrid map of optimization test functions. Expert Syst. Appl. 2024, 249, 123583. [Google Scholar] [CrossRef]

11. Li, H.; Yu, S.; Feng, W.; Chen, Y.; Zhang, J.; Qin, Z.; Zhu, Z.; Wozniak, M. Exploiting Dynamic Vector-Level Operations and a 2D-Enhanced Logistic Modular Map for Efficient Chaotic Image Encryption. Entropy 2023, 25, 1147. [Google Scholar] [CrossRef]

12. Feng, W.; Wang, Q.; Liu, H.; Ren, Y.; Zhang, J.; Zhang, S.; Qian, K.; Wen, H. Exploiting Newly Designed Fractional-Order 3D Lorenz Chaotic System and 2D Discrete Polynomial Hyper-Chaotic Map for High-Performance Multi-Image Encryption. Fractal Fract. 2023, 7, 887. [Google Scholar] [CrossRef]

13. Feng, W.; Zhao, X.; Zhang, J.; Qin, Z.; Zhang, J.; He, Y. Image Encryption Algorithm Based on Plane-Level Image Filtering and Discrete Logarithmic Transform. Mathematics 2022, 10, 2751. [Google Scholar] [CrossRef]

14. Kocak, O.; Erkan, U.; Toktas, A.; Gao, S. PSO-based image encryption scheme using modular integrated logistic exponential map. Expert Syst. Appl. 2024, 237, 121452. [Google Scholar] [CrossRef]

15. Estudillo-Valdez, M.A.; Adeyemi, V.A.; Tlelo-Cuautle, E.; Sandoval-Ibarra, Y.; Nuñez-Perez, J.C. FPGA realization of four chaotic interference cases in a terrestrial trajectory model and application in image transmission. Sci. Rep. 2023, 13, 12969. [Google Scholar] [CrossRef]

16. Tastan, I.; Ergün, S. Experimental Cryptanalysis of A Chaos-Based Random Number Generator. In Proceedings of the IEEE Asia Pacific Conference on Circuits and Systems (APCCAS), Chengdu, China, 26–30 October 2018; pp. 283–286. [Google Scholar] [CrossRef]

17. Chen, J.; Chen, L.; Zhou, Y. Cryptanalysis of Image Ciphers with Permutation-Substitution Network and Chaos. IEEE Trans. Circuits Syst. Video Technol. 2021, 31, 2494–2508. [Google Scholar] [CrossRef]

18. Ergün, S. Cryptanalysis of a chaos-based encryption scheme. In Proceedings of the International Symposium on Intelligent Signal Processing and Communication Systems (ISPACS), Xiamen, China, 6–9 November 2017; pp. 474–479. [Google Scholar] [CrossRef]

19. Xu, L.; Zhang, J. A novel four—Wing chaotic system with multiple attractors based on hyperbolic sine: Application to image encryption. Integration 2022, 87, 313–331. [Google Scholar] [CrossRef]

20. Xu, Y.; Zhang, M.; Li, C. Multiple attractors and robust synchronization of a chaotic system with no equilibrium. Optik 2016, 127, 1363–1367. [Google Scholar] [CrossRef]

21. Kaddoum, G.; Tadayon, N. Differential Chaos Shift Keying: A Robust Modulation Scheme for Power-Line Communications. IEEE Trans. Circuits Syst. II Express Briefs 2017, 64, 31–35. [Google Scholar] [CrossRef]

22. Rezk, A.A.; Madian, A.H.; Radwan, A.G.; Soliman, A.M. Reconfigurable chaotic pseudo random number generator based on FPGA. AEU-Int. J. Electron. Commun. 2019, 98, 174–180. [Google Scholar] [CrossRef]

23. Kaddoum, G.; Soujeri, E. NR-DCSK: A Noise Reduction Differential Chaos Shift Keying System. IEEE Trans. Circuits Syst. II Express Briefs 2016, 63, 648–652. [Google Scholar] [CrossRef]

24. Sandhu, G.S.; Berber, S.M. Investigation on operations of a secure communication system based on the chaotic phase shift keying scheme. In Proceedings of the Third International Conference on Information Technology and Applications (ICITA’05), Sydney, Australia, 4–7 July 2005; pp. 1–4. [Google Scholar] [CrossRef]

25. Hasan, M.; Idris, I.; Nokib Uddin, A.F.M.; Shahjahan, M. Performance analysis of a coherent chaos-shift keying technique. In Proceedings of the 2012 15th International Conference on Computer and Information Technology (ICCIT), Chittagong, Bangladesh, 22–24 December 2012; pp. 249–254. [Google Scholar] [CrossRef]

26. Zhu, S.; Xu, Y.; Yin, K. Design of a Quadrature Differential Chaotic Phase Shift Keying Communication System. In Proceedings of the 2009 International Conference

on Networks Security, Wireless Communications and Trusted Computing, Wuhan, China, 25–26 April 2009; pp. 518–521. [Google Scholar] [CrossRef]

27. Wang, Z.; Qi, G.; Sun, Y.; van Wyk, B.J.; van Wyk, M.A. A new type of four-wing chaotic attractors in 3-D quadratic autonomous systems. Nonlinear Dyn. 2010, 60, 443–457. [Google Scholar] [CrossRef]

28. Qi, G.; Chen, G. A spherical chaotic system. Nonlinear Dyn. 2015, 81, 1381–1392. [Google Scholar] [CrossRef]

29. Liu, L.; Guo, R. Control problems of Chen–Lee system by adaptive control method. Nonlinear Dyn. 2016, 87, 503–510. [Google Scholar] [CrossRef]

30. Lai, Q.; Nestor, T.; Kengne, J.; Zhao, X.W. Coexisting attractors and circuit implementation of a new 4D chaotic system with two equilibria. Chaos Solitons Fractals 2018, 107, 92–102. [Google Scholar] [CrossRef]

31. Zhou, L.; Chen, Z.; Wang, Z.; Wang, J. On the analysis of local bifurcation and topological horseshoe of a new 4D hyper-chaotic system. Chaos Solitons Fractals 2016, 91, 148–156. [Google Scholar] [CrossRef]

32. Zhou, L.; Chen, Z. Local Bifurcation Analysis and Global Dynamics Estimation of a Novel 4-Dimensional Hyperchaotic System. Int. J. Bifurc. Chaos 2017, 27, 1750021. [Google Scholar] [CrossRef]

33. Wang, M.; Deng, Y.; Liao, X.; Li, Z.; Ma, M.; Zeng, Y. Dynamics and circuit implementation of a four-wing memristive chaotic system with attractor rotation. Int. J. Bifurc. Chaos 2019, 111, 149–159. [Google Scholar] [CrossRef]

34. Wu, G.C.; Baleanu, D. Jacobian matrix algorithm for Lyapunov exponents of the discrete fractional maps. Commun. Nonlinear Sci. Numer. Simul. 2015, 22, 95–100. [Google Scholar] [CrossRef]

35. Zhou, S.; Wang, X. Simple estimation method for the largest Lyapunov exponent of continuous fractional-order differential equations. Physica A Stat. Mech. Its Appl. 2021, 563, 125478. [Google Scholar] [CrossRef]

36. Zhang, S.; Zeng, Y.; Li, Z.; Wang, M.; Xiong, L. Generating one to four-wing hidden attractors in a novel 4D no-equilibrium chaotic system with extreme multistability. Chaos 2018, 28, 013113. [Google Scholar] [CrossRef]

37. Kumlu, D. USC-SIPI Report 422. 2012. Available online: https://sipi.usc.edu/database/database.php?volume=misc (accessed on 11 October 2024).

38. Njitacke, Z.T.; Tsafack, N.; Ramakrishnan, B.; Rajagopal, K.; Kengne, J.; Awrejcewicz, J. Complex dynamics from heterogeneous coupling and electromagnetic effect on two neurons: Application in images encryption. Chaos Solitons Fractals 2021, 153, 111577. [Google Scholar] [CrossRef]

39. Dong, W.; Li, Q.; Tang, Y.; Hu, M.; Zeng, R. A robust and multi chaotic DNA image encryption with pixel-value pseudorandom substitution scheme. Opt. Commun. 2021, 499, 127211. [Google Scholar] [CrossRef]

40. Demirtas, M. A new RGB color image encryption scheme based on cross-channel pixel and bit scrambling using chaos. Optik 2022, 265, 169430. [Google Scholar] [CrossRef]

41. Yildirim, M. DNA encoding for RGB image encryption with memristor based neuron model and chaos phenomenon. Microelectron. J. 2020, 104, 104878. [Google Scholar] [CrossRef]

42. Trujillo, D.A.; Lopez, O.R.; García, E.E.; Tlelo, E.; López, D.; Guillen, O.; Inzunza, E. Real-time RGB image encryption for IoT applications using enhanced sequences from chaotic maps. Chaos Solitons Fractals 2021, 153, 111506. [Google Scholar] [CrossRef]

43. Sabir, S.; Guleria, V.; Mishra, D.C. Security of multiple RGB images in the time domain and frequency domain. J. Inf. Secur. Appl. 2021, 63, 103005. [Google Scholar] [CrossRef]

44. Liu, X.; Tong, X.; Wang, Z.; Zhang, M. A new n-dimensional conservative chaos based on Generalized Hamiltonian System and its' applications in image encryption. Chaos Solitons Fractals 2022, 154, 111693. [Google Scholar] [CrossRef]

45. Yang, C.H.; Huang, S.J. Secure color image encryption algorithm based on chaotic signals and its FPGA realization. Int. J. Circuit Theory Appl. 2018, 46, 2444–2461. [Google Scholar] [CrossRef]

46. Louzzani, N.; Boukabou, A.; Bahi, H.; Boussayoud, A. A novel chaos based generating function of the Chebyshev polynomials and its applications in image encryption. Chaos Solitons Fractals 2021, 151, 111315. [Google Scholar] [CrossRef]

47. Lai, Q.; Zhang, H.; Kuate, P.D.K.; Xu, G.; Zhao, X.W. Analysis and implementation of no-equilibrium chaotic system with application in image encryption. Appl. Intell. 2021, 52, 11448–11471. [Google Scholar] [CrossRef]

48. Peng, X.; Zeng, Y. Image encryption application in a system for compounding self-excited and hidden attractors. Chaos Solitons Fractals 2020, 139, 110044. [Google Scholar] [CrossRef]

49. Yu, F.; Shen, H.; Zhang, Z.; Huang, Y.; Cai, S.; Du, S. A new multi-scroll Chua's circuit with composite hyperbolic tangent-cubic nonlinearity: Complex dynamics, Hardware implementation and Image encryption application. Integr. VLSI J. 2021, 81, 71–83. [Google Scholar] [CrossRef]

50. Khymych, H., Dunets, V., Duda, S., Palaniza, Y., Kornieiev, K. Dual-Polarization Yagi Antenna for Meter Wavelength Range. Radioelectronics and Communications Systems, 66(11), pp. 609–615. 2023

51. Дунець В.Л., Хвостівська Л.В., Паляниця Ю.Б. Математичне, алгоритмічне та програмне забезпечення оцінювання завадозахищеності каналів зв'язку з балансною модуляцією. Збірник наукових праць Вісник НУ nВГП, серія технічні науки, випуск 4 (104), 2023. - С. 95-107. ISSN: 2306-5478.

52. Palianytsia, Yurii, Vasyl Dunets, and Liliia Khvostivska. "Modeling of Phased Array Antenna for Data Transmission in Urban Environment." Proceedings of the 3rd International Workshop on Information Technologies: Theoretical and Applied Problems, 22-24 November 2023, Ternopil, Ukraine, edited by Lytvynenko I.V. and Lupenko S.A., ITTAP-2023, 2023, pp. 370-381. (Scopus);

53. Khvostivska L., Khvostivskyi M., Dunets V., Dediv I. Mathematical, algorithmic and software support of synphase detection of radio signals in electronic communication networks with noises. Scientific Journal of TNTU (Tern.), vol 111, no 3, 2023. pp. 48–57;

54. Liliya Khvostivska, Mykola Khvostivskyy, Vasyl Dunets, Iryna Dediv. “Mathematical and Algorithmic Support of Detection Useful Radiosignals in Telecommunication Networks”. Proceedings of the 2nd International Workshop on Information Technologies: Theoretical and Applied Problems, 22-24 November 2022, Ternopil, Ukraine, ITTAP 2022, 2022, pp. 314-318. ISSN 1613-0073 (Scopus);

55. НПАОП 32.0-1.02-14 “Правила охорони праці під час виробництва радіо- та електронної апаратури”

56. ДСН 3.3.6.037 – 99 „Державні санітарні норми виробничого шуму, ультразвуку та інфразвуку”.

57. ДСН 3.3.6.039 – 99 „Державні санітарні норми виробничої загальної та локальної вібрації”.

58. ДСН 3.3.6.042 – 99 „Санітарні норми мікроклімату виробничих приміщень”.

59. Атаманчук П.С. Безпека життєдіяльності. Навчальний посібник. - К.: Основа, 2017, с.437.

60. Запорожець О.І. Основи охорони праці. – К.: ВД Центр навчальної літератури (ЦНЛ), 2019, с. 560.

ДОДАТОК А
Копія тези

УДК 621.311.6

В.Р. Федчишин, В.Л. Дунець, канд. техн. наук, доцент
(Тернопільський національний технічний університет імені Івана Пулюя, Україна)

ПРОДУКТИВНІСТЬ ТЕХНІКИ 16-CPSK У ПЕРЕДАЧІ ДАНИХ

V.R. Fedchyshyn, V.L. Dunets, PhD

PERFORMANCE OF 16-CPSK TECHNIQUE IN DATA TRANSMISSION

Сучасні бездротові системи зв'язку стикаються з проблемами завад, які знижують якість передачі даних. Використання 16-CPSK модуляції з хаотичними генераторами дозволяє значно підвищити стійкість сигналу до завад, забезпечуючи кращу безпеку та надійність зв'язку. Реалізація цих систем на базі FPGA додає гнучкості та продуктивності, що важливо для задач реального часу.

Метою дослідження є розробка та аналіз системи 16-CPSK модуляції в поєднанні з хаотичними генераторами для підвищення стійкості бездротових комунікацій до завад. Використання FPGA як основи забезпечує високу швидкість обробки, гнучкість та адаптивність, що є критично важливими для сучасних систем зв'язку. Такий підхід дозволяє реалізувати складні алгоритми у реальному часі, зберігаючи компактність і енергоефективність апаратури. Однак, поряд із перевагами, виникають певні недоліки:

1. Складність розробки:

Інтеграція хаотичних генераторів із модуляційною схемою на FPGA потребує глибокого математичного моделювання і точного налаштування, оскільки хаотичні сигнали мають нелінійну природу.

2. Ресурсозатратність:

Для реалізації системи на FPGA необхідна велика кількість логічних блоків, DSP-модулів та пам'яті, що може обмежувати використання менш потужних FPGA у проєкті.

3. Складність синхронізації:

Для успішної передачі та прийому даних необхідно забезпечити ідеальну синхронізацію між передавачем і приймачем, оскільки будь-які похибки можуть призводити до значних втрат сигналу.

4. Обмежена масштабованість:

Хоча FPGA забезпечують гнучкість, у системах із дуже високою пропускною здатністю їхня продуктивність може виявитися менш ефективною у порівнянні з ASIC-реалізаціями.

Незважаючи на ці виклики, система 16-CPSK модуляції з хаотичними генераторами має значний потенціал для створення стійких до завад комунікаційних технологій, що можуть бути адаптовані до вимог сучасних і майбутніх бездротових мереж.

Література

1. Wang, Z.; Qi, G.; Sun, Y.; van Wyk, B.J.; van Wyk, M.A. A new type of four-wing chaotic attractors in 3-D quadratic autonomous systems. Nonlinear Dyn. 2010, 60, 443–457.

2. Liu, L.; Guo, R. Control problems of Chen–Lee system by adaptive control method. Nonlinear Dyn. 2016, 87, 503–510.