Форма № 24

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Національний університет «Запорізька політехніка»

Факультет інформаційної безпеки та електронних комунікацій
(повне найменування інституту, факультету)

Кафедра інформаційної безпеки та наноелектроніки
(повне найменування кафедри)

Пояснювальна записка

до дипломного проєкту (роботи)
магістра
(ступінь вищої освіти)

на тему: АЛГОРИТМ ШИФРУВАННЯ АНАЛОГОВОГО БЕЗДРОТОВОГО ВІДЕОСИГНАЛУ НА ОСНОВІ ХАОТИЧНИХ СИГНАЛІВ

Виконав: студент 2 курсу, групи БК-812м

Спеціальності

125 «Кібербезпека»
(код і найменування спеціальності)

Освітня програма (спеціалізація)

«Безпека інформаційних і комунікаційних систем»

ЯЦЕНКО Дмитро Юрійович
(прізвище та ініціали)

Керівник ЛІЗУНОВ С.І.
(прізвище та ініціали)

Рецензент
(прізвище та ініціали)

2023 рік

Форма № 25

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Національний університет «Запорізька політехніка»
(повне найменування закладу вищої освіти)

Інститут, факультет Факультет інформаційної безпеки та електронних комунікацій
Кафедра Інформаційна безпека та наноелектроніка
Ступінь вищої освіти магістр
Спеціальність 125 «Кібербезпека та захист інформації»
(код і найменування)
Освітня програма Безпека інформаційних і комунікаційних систем
(назва освітньої програми (спеціалізації)

ЗАТВЕРДЖУЮ
В.о. завідувача кафедри ІБтаН
Андрій КОРОТУН
_____
«_____» грудня 2023 року

З А В Д А Н Н Я
НА ДИПЛОМИНИЙ ПРОЄКТ (РОБОТУ) СТУДЕНТА(КИ)

ЯЦЕНКО Дмитра Юрійовича
(прізвище, ім'я, по батькові)

1. Тема проєкту (роботи) Алгоритм шифрування аналогового бездротового відеосигналу на основі хаотичних сигналів
Algorithm for encryption of analog wireless video signal based on chaotic signals
керівник проєкту (роботи) ЛІЗУНОВ Сергій Іванович, к.т.н., доцент,
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)
затверджені наказом закладу вищої освіти від «07» грудня 2023 року №493
2. Строк подання студентом проекту (роботи) 16 грудня 2023 р.
3. Вихідні дані до проєкту (роботи) Структура аналогового відеосигналу, що отримується з камер
4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити) Огляд переваг та недоліків аналогового відеосигналу, структура аналогового відеосигналу, огляд існуючих методів шифрування аналогового відео, хаотичне кодування як метод шифрування аналогового відеосигналу, розробка схеми шифратора та дешифратора, розробка конструкції шифратора та дешифратора, тестування розроблених методів та апаратних засобів
5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень)
Презентація роботи в PowerPoint

6. Консультанти розділів проєкту (роботи)

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	прийняв виконане завдання
1-3	ЛІЗУНОВ С.І., доц. каф. ІБтаН, к.т.н.,доцент		
Нормокон-	КОРОЛЬКОВ Р.Ю., доц. каф. ІБтаН, к.т.н., доцент		
троль			

7. Дата видачі завдання «02» вересня 2023 року.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів дипломного проєкту (роботи)	Строк виконання етапів проєкту (роботи)	Примітка
1	Пошук та вивчення наукових джерел	2.9-1.10	
2	Розробка методів шифрування аналогового відео	2.10-14.10	
3	Розробка схеми шифратора та дешифратора	14.10-24.10	
4	Розробка конструкції шифратору та дешифратору	24.10-2.11	
	Тестування розробленого методу та схемотехнчних рішень		
5	Оформлення пояснювальної записки	2.11-2.12	
6	Перевірка ПЗ на доброчесність	8.12	
7	Створення презентації у Power Point	10.12	
8	Захист	16.12	

Студент _____ Дмитро ЯЦЕНКО
(підпис) (прізвище та ініціали)

Керівник проєкту (роботи) _____ Сергій ЛІЗУНОВ
(підпис) (прізвище та ініціали)

РЕФЕРАТ

ПЗ: 78 сторінок, 39 рисунків, 7 джерел

КАДР, ВІДЕОСИГНАЛ, ПЕРЕДАВАЧ, ПРИЙМАЧ, СКРЕМБЛЕР, РЯДОК, ОПЕРАЦІЙНИЙ ПІДСИЛЮВАЧ

Мета роботи – розробка алгоритму шифрування аналогового відеосигналу при передаванні бездротовими передавачами з використанням хаотичних сигналів та розробка апаратного засобу перевірки запропонованого алгоритму.

Об’єкт дослідження – аналоговий відеосигнал і особливості його оборотного перетворення з метою шифрування при передаванні на відстані.

Предмет дослідження – пристрій на основі хаотичного кодування для шифрування аналогового відеосигналу при передаванні на відстань.

Здійснено огляд сучасної літератури з питань аналогового кодування відеозображення, існуючих методів шифрування аналогового відео. Проведено аналіз вразливостей відеопотоку при передаванні по радіоканалу та методів усунення цих вразливостей. Запропоновано метод шифрування аналогового відеосигналу за допомогою використання хаотичного кодування. Розроблено схему шифратора та дешифратора аналогового відеосигналу, розроблено конструкцію друкованих плат. Проведено тестування роботи розроблених шифратора та дешифратора яке показало можливість використання запропонованого методу для високоякісного шифрування аналогового відео. Розроблені на основі запропонованого методу шифратор та дешифратор надають можливість захистити від несанкціонованого доступу.

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ

БПЛА – Безпілотний літальний апарат

HD – High Definition (Висока роздільна здатність)

PAL – Phase Alternating Line (строкова зміна фази)

NTSC – National Television System Committee (Національний комітет з питань телевізійних систем)

FPV – First Person View (вид від першої особи)

SECAM – Séquentiel couleur à mémoire (послідовний колір із пам'яттю)

YUV – колірна модель, в якій колір складається з трьох компонентів - яскравість Y (Luma) і два кольорові компоненти UV (Chroma)

ЕПТ – електронно-променева трубка

РСІ – рядковий синхроімпульс

КСІ – кадровий синхроімпульс

КГІ – кадровий гасячий імпульс

ГПВП – генератор псевдовипадкових послідовностей

ВСТУП

Протягом багатьох десятиліть відео було важливим засобом передавання інформації для керування та контролю, а також спілкування та розваг. Відеозв’язок у реальному часі став потребою сучасності.

Бездроте передавання відеосигналу є одним з основних функціональних потреб для здійснення керування БПЛА, робототехнічними наземними та неводними системами, пристроями віддаленого візуального контролю виробництва. Для збільшення дальності передавання відеоінформації бездротовими передавачами необхідно застосовувати направлені антени та ретранслятори. Ретрансляція цифрового каналу зв’язку потребує складних пристроїв і до того ж через закриту структуру представлених на ринку цифрових передавачів унеможливлює самостійну реалізацію, що в свою чергу збільшує залежність від виробників та значно збільшує вартість побудови систем ретрансляції. Гарним рішенням здешевлення систем ретрансляції відеосигналу є використання аналогових прийомо-передавачів які мають відкриту документацію та через відсутність складних мікропроцесорних перетворень майже не будуть давати затримку в розповсюдженні сигналу. Основною проблемою бездротової передачі відеосигналу з використанням аналогових передавачів є відкритість каналу, що призводить до того, що будь хто з наявним приймачем може перехопити сигнал та отримати доступ до відеоінформації.

Шифрування аналогової передачі відеосигналу – це очевидний спосіб захисту, тобто спосіб не дозволяти дивитися їх колу осіб для яких воно не призначається.

До систем захисту відеоінформації висувається кілька критичних вимог. По-перше, це мінімальні спотворення зображення, що подається, по-друге, перешкодозахищеність і стійкість до зовнішніх впливів, і по-третє, звичайно

ж, захищеність від несанкціонованого перехоплення і передачі помилкової візуальної інформації.

Існуючі алгоритми шифрування аналогового відеосигналу не дозволяють бути на 100% впевненим, що зловмисник не зможу отримати доступ до відеоматеріалу в режимі реального часу, оскільки ці алгоритми використовують незначні зсуви та перестановки які можна відтворити з використанням навіть ненадшвидкісних мікропроцесорних систем. Отже виникає необхідність розробки нового алгоритму для захисту аналогового відеосигналу особливо в умовах необхідності його використання на безпілотних та робототехнічних засобах.

1 ОГЛЯД БЕЗДРОТОВОГО ПЕРЕДАВАННЯ ВІДЕОСИГНАЛУ ТА ПОСТАНОВКА ЗАДАЧ РОБОТИ

1.1 Бездротове передавання відео

Бездротова передача — це технологія, яка існує протягом тривалого часу, але вона стала широко доступною лише в останні кілька десятиліть. До того бездротова передача була можлива лише за дуже обмежених обставин. Якщо між двома точками відсутні фізичні з’єднання, можлива бездротова передача.

Бездротова передача відео – це можливість передавати відеосигнал від одного пристрою до іншого на певну відстань без будь-яких фізичних кабелів і без джерела живлення. Існують різні типи бездротової передачі відео, включаючи пряму бездротову передачу відео, бездротову передачу через HDMI, бездротову передачу через DisplayPort (DP) та інші.

Перевагами бездротової передачі відео є:

- простота (легке налаштування, універсальність);
- безпека;
- покращена мобільність (гнучкість);
- економія коштів.

Оновлення технологій для відеовиробництва на знімальному майданчику, оцінки обстановки на промисловому об’єкті чи майданчику чи навіть полі бою шляхом використання відеокамер, завжди корисне, але інколи може бути складно освоїти їх використання — так само, як навчитися використовувати будь-яку нову технологію. Чудова перевага бездротової передачі відео в тому, що вона спрощує, а не ускладнює процес налаштування відеообладнання.

Залежність від довжини дроту та розташування розеток може бути дуже напруженою. Порівняно з традиційною дротовою системою передачі відео, комплект бездротового відеопередавача та приймача, безсумнівно, зручний і

простий у налаштуванні, оскільки знадобиться лише кілька секунд, щоб об’єднати їх у пару та з’єднати за допомогою кнопок. Немає потреби прокладати довгі дроти та шукати правильні інтерфейси для встановлення з’єднання між джерелом відео та дисплеєм.

Набір бездротового відеопередавача та приймача можна широко використовувати в багатьох випадках. На робочому місці можна використовувати його для виведення відеопрезентації з ПК на телевізор у конференц-залі. На вулиці можна знімати відеоблог або вуличне інтерв’ю та передати зображення на приймач. На виробництві бездротова передача дозволить оперативно та віддалено контролювати промисловий процес. Удома може функціонувати як бездротова система відеоспостереження, яка буде контролювати обстановку всередині та зовні.

Чим менше проводів, тим краще не лише через вищезазначені причини, але й через небезпеку спотикання через проводи. Якщо хтось спіткнеться об дротовий відеопередавач або приймач, це може завдати як фізичної шкоди людині, так і шкоди майну. Навіть якщо ніхто не спіткнеться об дроти, пересуваючись поблизу дротових пристроїв, все одно є ризик зачепитися ними за сусідні предмети та зламати речі, що може призвести до пошкодження оточення. Крім того, перевірені та сертифіковані передавачі та приймачі забезпечують належну робочу температуру навіть під час тривалого запису на вулиці.

Бездротові системи передавання відео можна переміщати майже будь-де на майданчику, тому що їх не потрібно постійно підключати до розетки. Це дає змогу знімати відео з великою творчою свободою, а не прив’язуватися до найближчої точки живлення.

Відсутність кабелів підвищує гнучкість цих пристроїв. Бездротовий відеопередавач дає змогу знімати відео на відстані, яку підтримує система, навіть крізь натовп або на висоті. Навпаки, кабелі іноді обмежують відстані, а також можливості.

Система бездротової передачі відео може добре заощадити гроші, оскільки не доведеться купувати додаткові пристрої, такі як USB-диски та конвертери. Крім того, швидкий розвиток і високий попит на бездротову передачу приносять масову пропозицію бездротових відеопередавачів і роблять їхню вартість доступною.

Мінуси бездротової передачі відео:

- несправності;
- екологічні спотворення;
- крадіжка даних і втручання.

Бездротова передача погано працює в місцях із сильними електромагнітними полями, наприклад поблизу ліній електропередач і опор стільникового зв’язку.

Залежно від типу використовуваної передачі та середовища, в якому вона використовується, можуть виникати візуальні спотворення, шумові перешкоди тощо. Ці обмеження можуть вплинути на якість відеосигналів, які можуть передаватися між пристроями через такі фактори, як переривання, спричинені відбиттям світла.

Можуть виникнути перешкоди для передачі даних, якщо поблизу є інші бездротові мережі. Частоти Wi-Fi, які часто використовуються, стикаються з конкуренцією інших бездротових технологій, таких як бездротові телефони, радіоняні та камери безпеки. Оскільки потрібні передавач і приймач або пристрій із вбудованими функціями, це підвищує вартість виробництва.

1.2 Цифрова та аналогова передача відео. Переваги та недоліки

Оптичне зображення формується за допомогою об'єктива на світлочутливій матриці відео та телевізійних камер, телекінопроекторів, цифрових фотоапаратів, камерафонів або планшетів, веб-камер, камер систем

відеоспостереження та інших подібних пристроїв. За допомогою різних систем виробляється кольороподіл зображення для отримання монохромних напівтонових компонентів трьох основних кольорів.

Для запису та передачі цифрового відео, також як і аналогового, застосовують розкладання його на окремі рядки, тобто послідовне сканування та передача елементів кожного горизонтального рядка. Для відео та телебачення стандартної чіткості ці значення дорівнюють 480 або 576 рядків, з підвищеною чіткістю – 720. Для відео високої чіткості (англ. HD) – 1080.

Для скорочення потоку, що передається вдвічі застосовується черезрядкова розгортка, коли кожен кадр передається двома послідовними полукадрами — полями. Поле складається із телевізійних рядків. Одне поле містить парні рядки, друге – непарні. Такий режим розгортки позначається значком «і» від англ. interlace. Такий режим був розроблений в епоху аналогового телебачення, коли не було можливості передавати сигнали із широкою смугою пропускання. Також перші цифрові формати і навіть HD використовували цей режим зменшення відеопотоку. Недоліком такого режиму є наявність ефекту «гребінки» на об'єктах, що рухаються, при відтворенні на пристроях відображення з прогресивною (рядковою) розгорткою.

Переваги аналогової передачі відеосигналу:

- доступна ціна (дані типи пристроїв вже давно на ринку, а значить ціна на них відповідає кон'юнктурі, і не залежить від новизни технології);

- світлочутливість (більшість аналогових пристроїв добре реагують на зміну освітленості, знову ж таки причина в тому, що технологія знаходиться практично на своєму піку);

- не важлива ширина каналу (аналоговий сигнал не потребує великої пропускної спроможності каналу);

- якісна і плавна картинка об'єктів, що рухаються.

Основні недоліки аналогової передачі відеосигналу:

- обмежена 700 лініями якість відеосигналу (По суті аналоговий сигнал PAL – це те саме, що використовують у телемовленні. Низька якість відеосигналу не дозволить деталізувати зображення без оптичного збільшення);

- неконтрольована реакція на електромагнітні перешкоди (аналогові відеопередавачі здійснюють передачу відео без наявності зворотнього зв’язку – тобто передавач не контролює чи отримав приймач сигнал чи ні).

Цифрові відеосистеми

Основна відмінність між цифровою та аналоговою камерою полягає в тому, що цифрова передає потокове відео безпосередньо з матриці, без кодування його в аналоговий сигнал.

Звідси висока деталізація картинки. Ширина матриці у камері не має обмежень і відповідно можна досягти практично будь-якої якості картинки.

Цифрові відеосистеми мають більшу автономність роботи. За потреби цифрова відеосистема сама може записувати отримані дані на власний накопичувач.

Недоліки в цифрових відеосистем:

Вартість значно вища за аналогових конкурентів. Варто підкреслити, що йдеться про якісні камери, розраховані на тривалу службу та високу якість картинки.

Вимоги до ширини каналу. Чим більше якість картинки тим ширше необхідний канал, що пропускає (у аналогових відеосистемах ширина каналу завжди стала).

З точки зору використання систем передачі відео у БПЛА

Аналоговий зв'язок - це незашифрована передача відео без будь-яких кодеків та стискання відео . Принцип роботи як у старого телевізора. Має різні шуми і інші завади. Є багато різних частот (1.3/2.4/3.3/5.8) у всіх окулярів стандарт 5.8 . Великий плюс , що з сигналом можна робити будь що (ретранслятрувати зв‘язок або виносити приймач) без особливо складних апаратних засобів. Може літати далі ніж багато цифрових систем, крім того

відсутній зворотній сигнал, що по перше дає затримку відображення відеосигналу, по друге демаскує пілота, що вкрай не бажано в умовах використання БПЛА у військових цілях.

Цифровий відеозв’язок – має багато обмежень у використанні, але якість відео набагато краща і є шифрування сигналу у системі одразу. У деяких систем обмежена дальність через кодеки . У більшості тяжко зробити ретранслятор чи внести приймач або зовсім неможливо це зробити.

У цифрового зв’язку краща пробивна здатність через перешкоди ніж у аналога .Наприклад, якщо залетіти за дерева все буде добре , а на аналозі картинка може і повністю втратитись .Він краще втримує РЕБ , але неможливість зробити ретранслятор це нівелює.

Для використання БПЛА у військових цілях з метою збільшення відстані польоту краще використовувати аналоговий відеоканал через можливість зробити ретранслятор. На аналоговому каналі відеосигналу можна досягнути більшої дальності передачі, а відповідно польоту БПЛА та більш надійного зв’язку ніж у цифрового каналу.

1.3 Завдання, що ставляться в роботі

Оскільки з масовим використання БПЛА виникла необхідність роботи на великих відстанях при невеликій ціні реалізації використання аналогового відеоканалу є дуже актуальним, а оскільки за замовчуванням аналогова відеопередача є відкритою виникає необхідність розробки методів шифрування, що дозволять закрити відеоінформацію від несанкціонованого перегляду.

Отже в роботі пропонується розробка методів шифрування аналогового відеосигналу. Прості перетворення (типу інверсії) є стандартними методами закриття і швидко взламуються, до того ж є необхідність забезпечення

можливості реалізації унікальності за допомогою використання змінного сигналу, що буде накладатися на базовий відеопотік, що у свою чергу надасть можливість переналаштування на випадок якщо зловмисник буде мати схемотехнічну реалізацію (щоб не знаючи кодуючого сигналу він не міг зробити перехоплення).

Загалом пропонується реалізація двокомпонентної методики з використанням шифратору та дешифратору аналогового відеосигналу. Шифратор має встановлюватися після аналогової відеокамери (яка видає сигнал PAL або NTSC) і відповідно спотворювати сигнал який далі буде потрапляти на відеопередавач. Дешифратор має встановлюватись після приймача відеосигналу перед пристроєм відображення відео і відповідно перед тим як вивести на екран проводити зворотне спотворення. Структурна схема наведена на рис.1.1-1.2. При такій реалізації забезпечується уніфікація оскільки можна використовувати будь яку аналогову відеокамеру та будь які передавачі та приймачі відеосигналу оскільки запропонована схема ніяк не впливає на радіоканал та не залежить від схемотехніки інших компонентів системи передавання відео.

В роботі пропонується використання хаотичного кодування перевагами якого у порівнянні з цифровими схемами, або схемами з буферізацією є відсутність затримки для обробки з забезпеченням можливості зміни так званого «коду» (кодуючого сигналу).

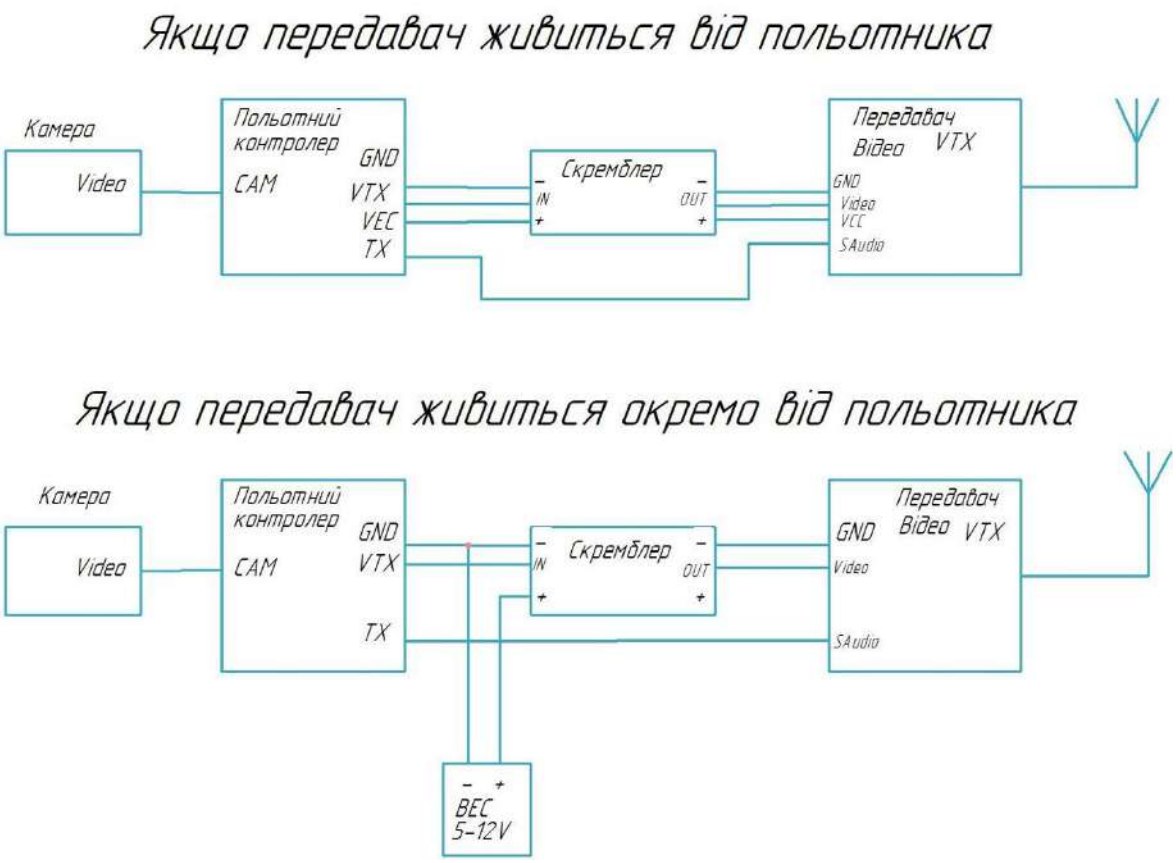

Рисунок 1.1 – Структура приєднання блоку шифрування

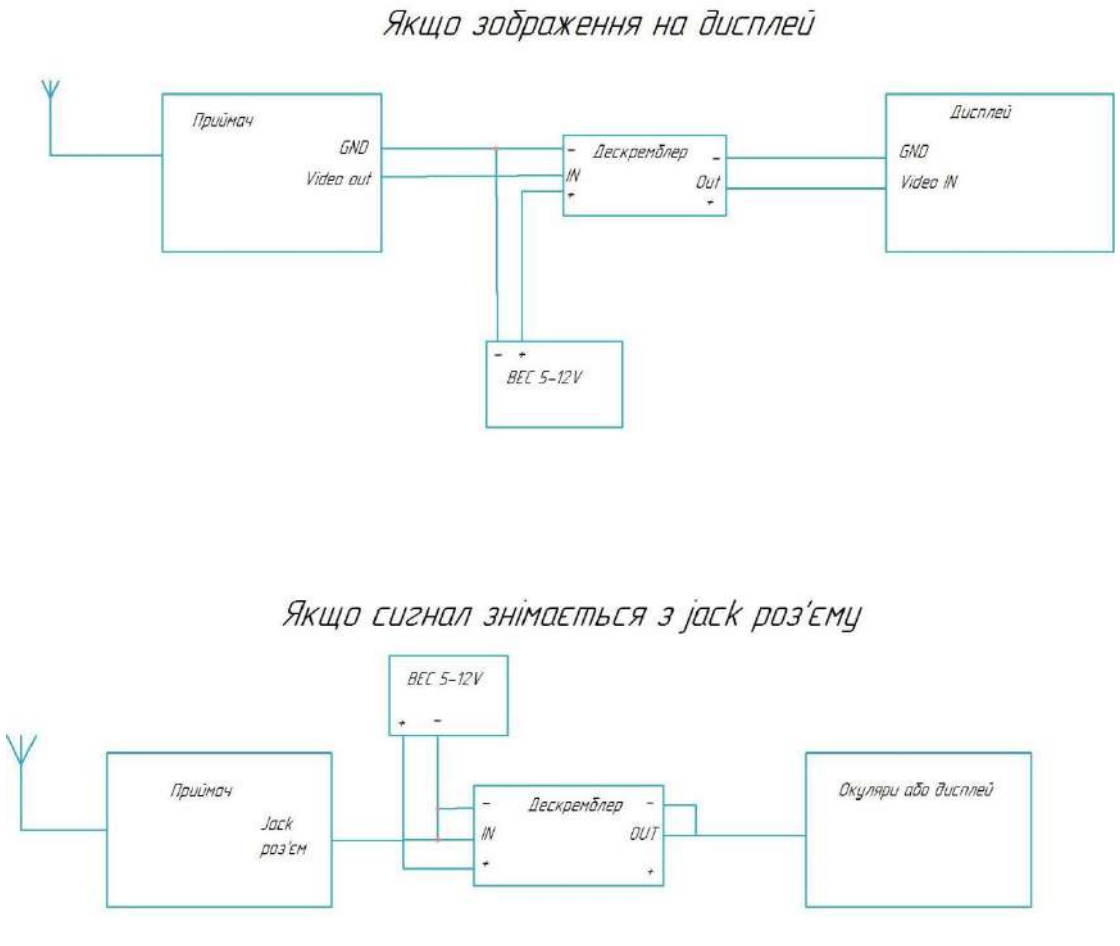

Рисунок 1.2 – Структура приєднання блоку дешифрування

Шифратор змінює параметри сигналу за псевдовипадковим законом (алгоритмом). Для відновлення сигналу дешифратор абонента повинен синхронно з шифратором виконати зворотне перетворення. У розподільчу мережу тим чи іншим способом вводиться інформація, що визначає права доступу (статуси) всіх дешифраторів системи. Обидва ці процеси повинні забезпечити такі вимоги:

- сигнал зображення повинен бути перекручений настільки, щоб переглядати його без дешифратора було неможливо;

- якість зображення, відновленого дешифратором, повинна хоч би суб'єктивно сприйматися не гірше, ніж якість зображення відкритих каналів;

- система має бути максимально захищена від злому, тобто створення піратського дешифратора має бути якомога складніше технічно та недоцільно економічно;

- система має бути повністю сумісною з існуючими відеокамерами та пристроями прийому-передавання аналогового відеосигналу (як мінімум в розрізі використання в БПЛА). Це означає, що шифрований сигнал за своїми радіочастотними параметрами (насамперед, по ширині займаної смуги частот) не повинен відрізнятися від нешифрованого сигналу, щоб можна було використовувати для його для передавання на існуючому обладнанні;

- вартість обладнання повинна бути якомога нижчою.

Неважко помітити, що ці вимоги багато в чому суперечать одна одній. Справді, з одного боку, щоб унеможливити несанкціонований перегляд, зображення треба максимально "зіпсувати". З іншого боку, необхідно зберегти якість зображення після відновлення дешифратором. При цьому дешифратор повинен являти собою недорогий, а отже, відносно нескладний пристрій. Тому використання хаотичного кодування є найбільш прийнятним для реалізації подібної системи через невелику вартість реалізації, збереження радіочастотних параметрів та відсутність затримки з можливістю відтворення начального відеосигналу.

2 ШИФРУВАННЯ АНАЛОГОВОГО ВІДЕОСИГНАЛУ

2.1 Структура аналогового відеосигналу

Для того щоб оцінити способи шифрування аналогового відеосигналу – треба спочатку провести аналіз особливостей цього сигналу з точки зору подання інформації і особливостей його кодування.

Передавання аналогового відео - це процес передачі відеосигналу у формі, яка не є цифровою. Це може відбуватися за допомогою аналогових технологій, таких як аналогове телебачення (PAL, NTSC, SECAM), композитний сигнал, компонентне відео, S-Video та інші.

Найбільший плюс стандартного аналогового відеосигналу, те, чого поки не може досягти HD-аналог (HD-TVI, HD-CVI, AHD), це повна сумісність з різними системами відображення (монітори, реєстратори, плати відеозахоплення, матричні комутатори та інше), не потрібно постійно пам'ятати, а чи буде моє обладнання від різних виробників сумісне.

Відеокамера на своєму виході формує спеціальний сигнал, який, будучи поданим на будь-який пристрій, монітор або відеовхід побутового телевізора, розгорне на екрані зображення. Це відбувається тому, що пристрої відображення працюють за єдиним алгоритмом, закладеним у структуру відеосигналу.

Цей алгоритм полягає у почерговому обході всіх елементів зображення у певному порядку та з певною швидкістю. Причому цей процес на передавальній (відеокамера) та приймальній стороні (пристрій відображення) має відбуватися абсолютно синхронно. Прийомо-передавачі лише забезпечують бездротове передавання з використанням власних методів модуляції.

Відеосигнал, який є основним електричним сигналом, який починається з камери та надходить до пристроїв відображення через систему передачі. У

аналогових відеосистемах цей сигнал називається композитним відео. Його максимальна амплітуда становить 1 вольт від піку до піку.

Як відомо із фізіології зору людини, відчуття кольору складається із трьох основних складових: червоного (R), зеленого (G) і синього (B) кольорів. Таку колірну модель позначають абревіатурою RGB. Через переважання у середньостатистичній телевізійній картинці зеленої складової кольору і для уникнення надлишкового кодування, як додатковий сигнал колірності використовують різницеві сигнали R-Y та B-Y (де Y — загальна яскравість монохромного телесигналу). У системі PAL використовують так звану колірну модель YUV (U = R-Y, V = B-Y).

Обидва додаткових сигнали кольоровості у стандартах PAL та NTSC передаються одночасно у квадратурній модуляції (різновид амплітудної модуляції), типова частота піднесучої сигналу — 4433618,75 Гц (4,43 МГц). При цьому кожен різницевий сигнал кольору повторяють у наступному рядку з поворотом фази з частотою 15,625 кГц на 180 градусів, завдяки чому декодер PAL повністю усуває фазові помилки (типові для системи колірності NTSC). Для усунення фазової помилки декодер складає поточний і попередній рядки із пам'яті (у аналогових телевізійних приймачах використовується лінія затримки). Таким чином, об'єктивно, кольорове телевізійне зображення у стандарті PAL має вдвічі меншу роздільну здатність по-вертикалі, ніж монохромне зображення. Суб'єктивно через більшу чутливість ока до яскравісної складової, на середньостатистичних телевізійних картинках таке погіршення майже не помітне. Застосування цифрової обробки сигналу ще більше згладжує цей недолік.

Коли світло падає на чіп матриці камери, воно створює заряд у пікселях, який прямо пропорційний кількості світла, що падає на них. Більше світла означає більший заряд. Потім цей заряд зчитується з мікросхеми матриці і перетворюється на відеосигнал. Методологія зчитування цього заряду з мікросхеми залежить від типу мікросхеми матриці. Чим більше світла на пікселі, тим більша амплітуда відеосигналу. У композитному відео

максимальна амплітуда відеосигналу становить 0,7 вольт. Іншими словами, біла або яскрава частина зображення матиме сигнал 0,7 вольт, тоді як чорна або темна частина матиме сигнал 0 вольт.

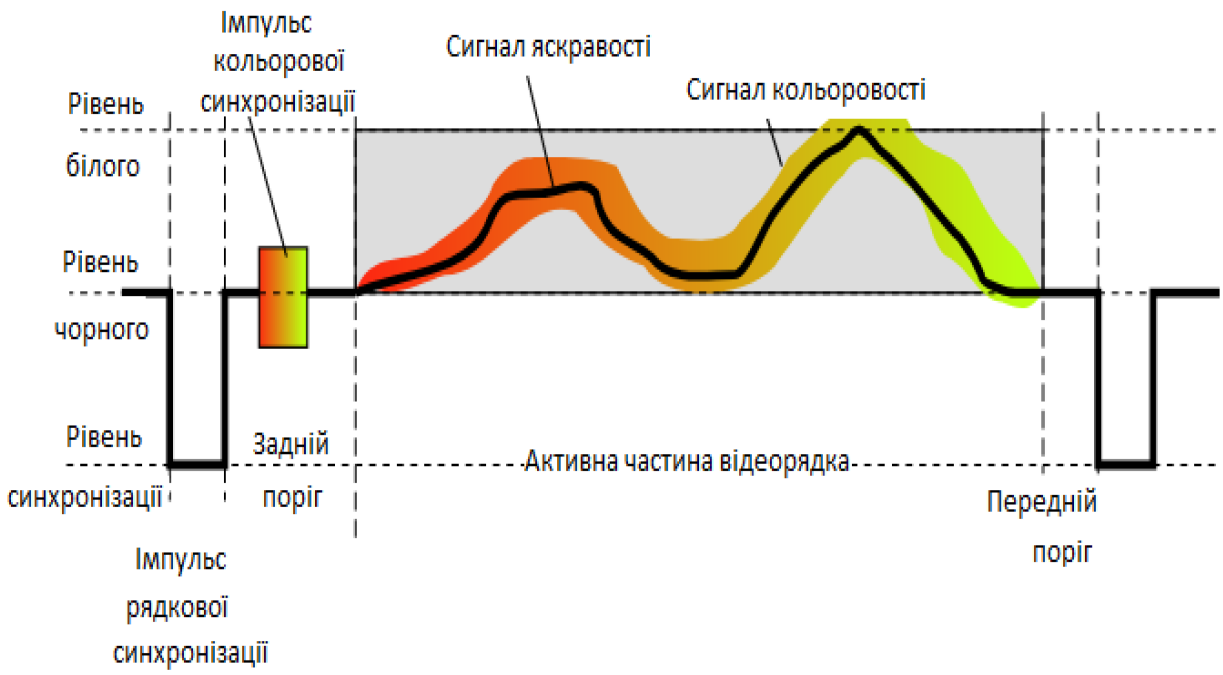

Рисунок 2.1 – Структура рядка аналогового відеосигналу

У аналоговому відеопакеті передається, крім відеосигналу, ще й набір імпульсів, що синхронізують. Повністю сформований відеосигнал складається з наступних компонентів:

- сигнал зображення, що переносить інформацію про яскравість елементів зображення;

– малі та кадрові імпульси синхронізації генераторів розгорток у моніторі;

– малі та кадрові імпульси гасіння електронного променя під час його зворотного ходу;

- зрівнювальні імпульси;

- імпульси колірної синхронізації.

Якщо розбирати сигнал рядку зображення

Передня частина - це короткий (близько 1,5 мікросекунди) період, вставлений між кінцем кожного переданого рядка зображення і переднім

фронтом наступного рядка синхроімпульсу. Його мета полягала в тому, щоб дозволити рівням напруги стабілізуватися в старих телевізорах, запобігаючи перешкодам між рядками зображення.

Переднє крильце - це перший компонент інтервалу гасіння по горизонталі, який також містить імпульс рядкової синхронізації та заднє крильце.

Заднє крильце - це частина кожного рядка розгортки між кінцем (наростаючий фронт) рядкового синхроімпульсу та початком активного відео. Він використовується для відновлення еталонного рівня чорного (300 мВ) в аналоговому відео. З погляду опрацювання сигналів, він компенсує час спаду і час встановлення після синхроімпульсу.

У системах кольорового телебачення, таких як PAL і NTSC, цей період також включає сигнал колірної синхронізації. У системі SECAM він містить опорну піднесучу для кожного послідовного кольоророзностного сигналу, щоб встановити опорний сигнал нульового кольору.

Рядкова та кадрова синхронізації

Рядкова синхронізація призначена для виведення зображення на монітор строчно в межах кожного кадру. Формування імпульсів малої синхронізації відбувається у відеокамері. Рядок відеосигналу з імпульсами синхронізації наведено на рис. 2.2. Вона складається з кількох видів імпульсів:

- малих синхроімпульсів, які визначають момент початку виведення зображення в рядку та запускають генератор малої розгортки в моніторі;

- малих гасящих імпульсів, які призначені для «гасіння» променя електронно-променевої трубки (ЕПТ – забезпечення зворотньої сумісності навіть попри те що зараз як правило матриці на екранах) під час його повернення на початок нового рядка. Термін "гасіння" означає, що промінь ЕПТ, повертаючись до початку нового рядка, не викликає свічення люмінофора на екрані кінескопа;

– імпульсів колірної синхронізації, в яких закладено інформацію про колір переданого зображення.

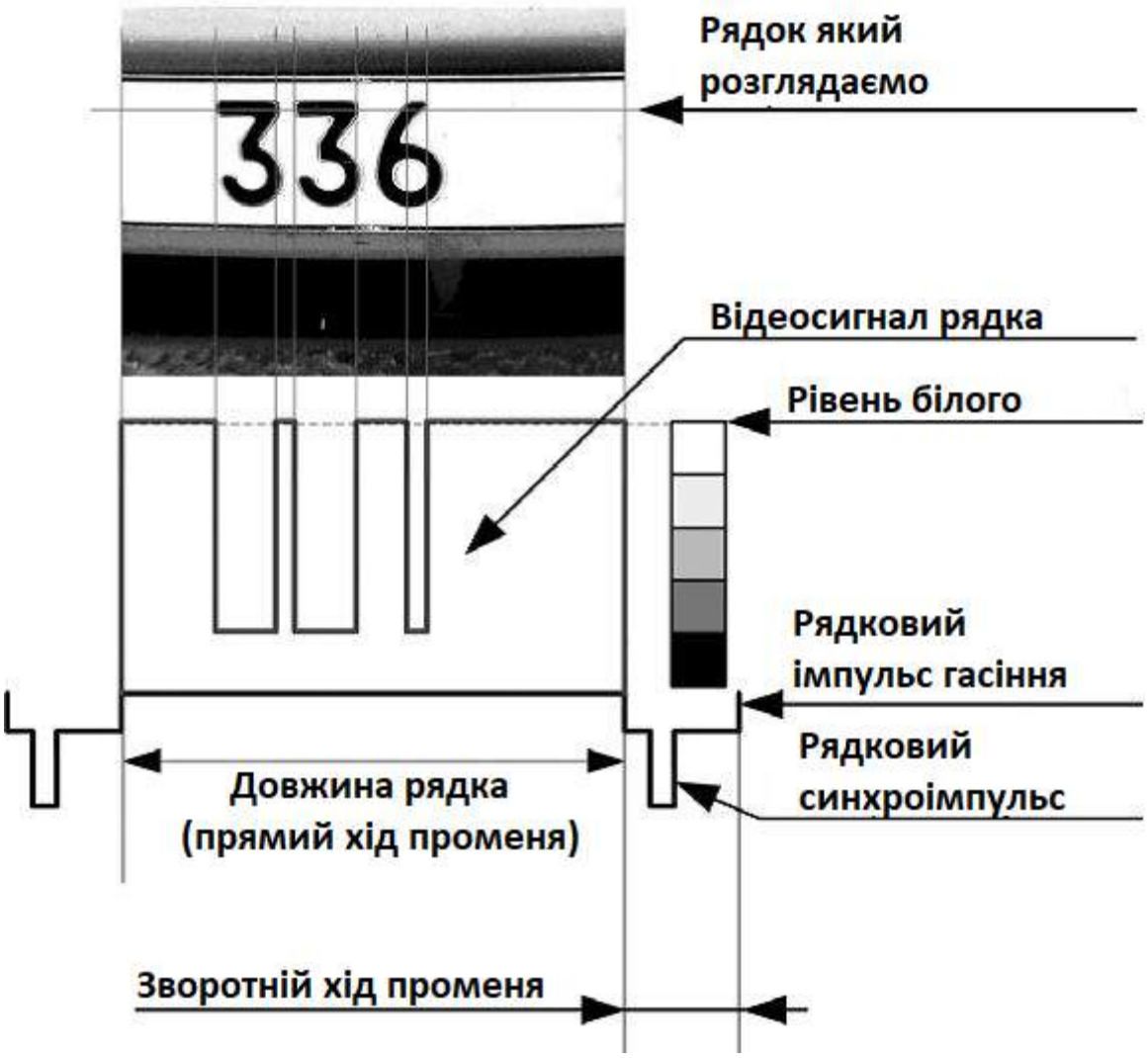

Рисунок 2.2 – Відеосигнал у межах тривалості рядка

У межах тривалості рядка (рис.2.2) виводиться відеосигнал. Інформація про зображення закладена у зміні рівня сигналу (яскравості). Найсвітліші ділянки зображення мають максимальну амплітуду, яка називається «рівнем білого». Темні ділянки зображення мають мінімальний рівень, що називається «рівнем чорного».

Відеозображення складається з відеокадрів. У NTSC є 30 кадрів в секунду, тоді як у PAL 25 кадрів в секунду.

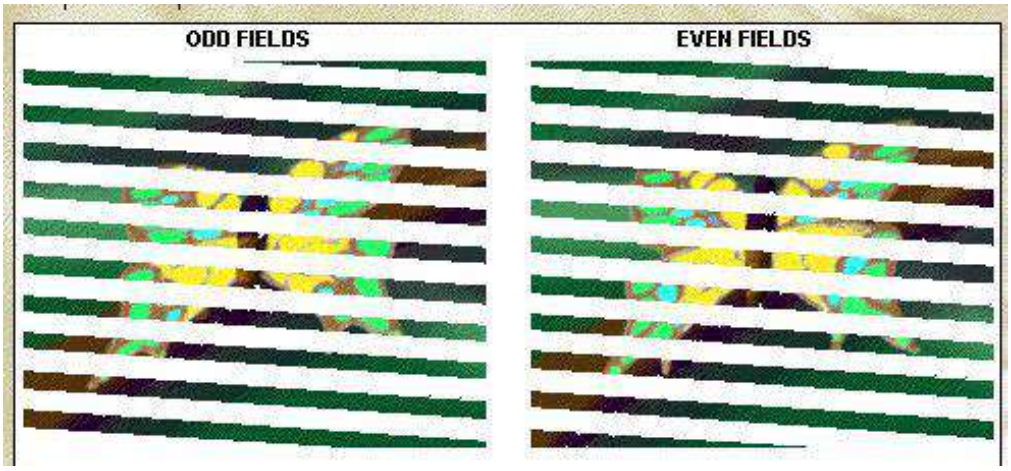

Рисунок 2.3 – Парний та непарний напівкадри

Щоб уникнути мерехтіння зображення в аналогових відеосистемах відеокадр розділений на 2 поля, тобто непарне та парне поля. Ці два поля відокремлюються в точці камери, а потім знову об’єднуються на стороні пристрою відображення. Це також називається переплетенням полів.

В кінці кожного кадру або поля додається імпульс вертикальної синхронізації. Цей імпульс синхронізації повідомляє електронним пристроям у камері та іншим компонентам аналогових відеосистем, що поле підійшло до кінця, і готує їх до прийому наступного кадру або напівкадру. Тривалість імпульсу залежить від часу, який потрібен електронним пристроям для отримання наступного нпівкадру. Амплітуда цього імпульсу становить 0,3 вольта. Коли це додається до відеосигналу, загальна амплітуда становить 1 вольт від піку до піку.

Відеокадр складається з ліній. У NTSC є 525 рядків на кадр, тоді як PAL має 625 рядків на кадр. Кожна точка в лінії відображає інтенсивність відеосигналу. У кінці кожного рядка додається горизонтальний синхроімпульс. Цей синхронізуючий імпульс повідомляє електронним пристроям у аналоговій відеосистемі, що лінія підійшла до кінця та підготуватися до початку наступної лінії. Він також має амплітуду 0,3 вольта.

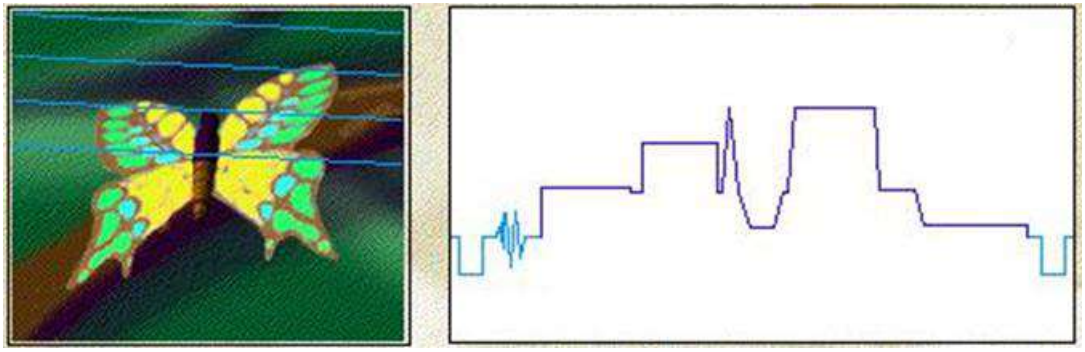

Рисунок 2.4 – Часова діаграма одного рядка зображення

Таблиця 2.1 – Кількісні та часові характеристики стандартів PAL та NTSC

	NTSC	**PAL**
Частота кадрів (в сек)	30	25
Тривалість кожного кадру	1/30 с	1/25 с
Кількість полів на кадр	2	2
Частота поля	60 Гц	50 Гц
Тривалість кожного поля	1/60 с	1/50 с
Кількість рядків на кадр	525	625
Кількість рядків на поле	262.5	312.5
Кількість рядків в секунду	525X30=15750	625X25=15625
Тривалість кожного рядка	1/15750 с або 63.5 мкс	1/15625 с або 64 мкс

Зворотний шлях або переліт назад – це час, необхідний для переходу від кінця одного рядка до початку наступного рядка або від кінця одного поля до початку наступного поля. Під час повторного відстеження інформація про зображення не сканується, тому її потрібно очистити. На телебаченні гасіння означає «перехід до рівня чорного».

Повернення повинно бути дуже швидким, оскільки це втрачає час з точки зору інформації про зображення.

Час, необхідний для горизонтального гасіння, становить приблизно 16% кожної горизонтальної лінії.

Час для вертикального гасіння становить приблизно 8% вертикального поля.

Таблиця 2.2 – Часові характеристики стандартів PAL та NTSC з врахуванням сигналів гасіння

	NTSC	**PAL**
Тривалість поля	1/60 с	1/50 с
Вертикальний сигнал гасіння	1/60 *0,08 = 1333 мкс	1/50* 0,08 = 1600 мкс
Кількість втрачених лінії через вертикальне гасіння	1333/63.5 = 21 лінія	1600/64 = 25 ліній
Тривалість рядка	63.5 мкс	64 мкс
Горизонтальне гасіння	63.5 * 0,16=10.2 мкс	64 * 0,16=10.25 мкс
Видимий час сліду	53.3 мкс	53.75 мкс

Імпульс гасіння ставить відеосигнал на рівень чорного, імпульс синхронізації починає фактичне відстеження під час сканування. Кожен імпульс горизонтальної синхронізації вставляється у відеосигнал протягом часу імпульсу горизонтального гасіння, а кожен імпульс вертикальної синхронізації вставляється у відеосигнал протягом часу вертикального гасіння. У табл.2.3 наведено частоту кожного імпульсу синхронізації.

Таблиця 2.3 – Частоти синхронізації для стандартів PAL та NTSC

	NTSC	**PAL**
Вертикальна	60 Гц	50 Гц
Горизонтальна	15750 Гц	15625 Гц

Кольоровий відеосигнал такий самий, як монохромний, за винятком того, що інформація про колір у кадрі також включається, і вона передається окремо. Наступні два сигнали передаються окремо:

- сигнал яскравості: відомий як сигнал Y, він містить варіації інформації про зображення, як у монохромному сигналі, і використовується для відтворення зображення в чорно-білому режимі;

- сигнал кольоровості: відомий як сигнал C, він містить інформацію про колір. Він передається як модуляція на допоміжній несучій.

Допоміжна несуча частота становить 3,58 МГц для NTSC і 4,43 МГц для PAL.

У кольоровому приймачі сигнал кольоровості відновлюється та поєднується з сигналом яскравості, щоб отримати кольорове зображення. У монохромному приймачі сигнал кольоровості не використовується і зображення відтворюється чорно-білим.

Оскільки кадр зображення (стандарт PAL) складається з 625 рядків, то розглянемо, як формується зображення у одному рядку. Наприклад візьмемо один кадр із зображеним у ньому автомобільним номером (рис. 2.2). Виберемо будь-який рядок. Як тільки закінчився рядковий імпульс, що гасить, інформація про яскравість зображення у вибраному рядку починає виводитися на монітор. У нашому випадку це білий колір, який відображається у відеосигналі максимальною амплітудою (білий рівень). "Дійшовши" до початку цифри "3", яскравість різко падає (колір чорний), і у відеосигналі ми бачимо аналогічне зменшення амплітуди сигналу до рівня чорного. Після цифри "3" яскравість знову зростає. Такий процес триває до кінця рядка і в результаті ми отримуємо один рядок повністю сформованого відеосигналу.

Оскільки відеокартинка на екрані монітора складається з 625 рядків (PAL), то для послідовного виведення на монітор у потрібних місцях існує кадрова синхронізація. Структура кадрових синхроімпульсів наведено на рис. 2.5.

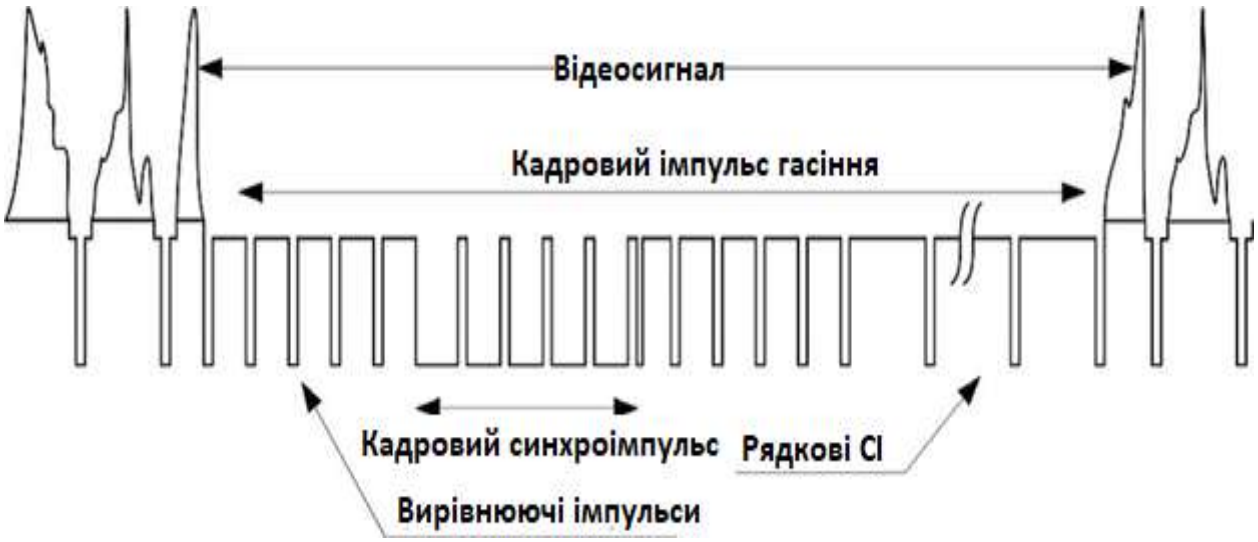

Рисунок 2.5 - Структура кадрових синхроімпульсів

Кадровий синхроімпульс призначений для запуску нового напівкадра.

Кадровий імпульс, що гасить - призначений для гасіння променя під час зворотного ходу кадрової розгортки.

Вирівнюючі імпульси (передні та задні) – призначені для отримання стійкої роботи через рядкову розгортки.

Врізання малих синхроімпульсів - призначені для утримання малої синхронізації під час кадрового імпульсу, що гасить. Найчастіше у цих місцях передається додаткова інформація.

Інформацію про те, який напівкадр «приходить», монітор отримує з відеосигналу по кадровому синхроімпульсу та рядковому синхроімпульсу. Перший напівкадр – той, у якого передні фронти кадрового синхроімпульсу та рядкового синхроімпульсу збігаються.

Слід звернути увагу, що в кожному новому полі після синхроімпульсу рядок відеосигналу починається то з початку рядка, то з його середини. Це дозволяє електронному променю малювати рядки, не накладаючи їх один на одного, а виводити зі зміщенням по вертикалі на один рядок.

Якщо відеокамера, формуючи відеосигнал, не створює інформацію про те, яке поле передається (відсутня черезрядкова розгортка), то кожен напівкадр починається з нового рядка, і замість вертикальної роздільної

здатності 625 рядків ми маємо 312,5, тобто якість картинки погіршується вдвічі.

Якщо прийняти весь розмах аналогового відеосигналу Umax за 100%, то згідно зі стандартом амплітуда синхронізуючих імпульсів (СІ) завжди має становити 30% від цього максимуму незалежно від змісту зображення. Ця сталість амплітуди забезпечує надійне їх відокремлення від відеосигналу в пристроях відображення. Рівень білого відеосигналу при позитивній полярності відстань від максимального рівня повного відеосигналу (контрольного рівня білого) на 10-15% від Umax, а між рівнем чорного та рівнем горизонтального імпульсу розташовується охоронна смуга, що становить від 0 до 7% від Umax. Ця охоронна смуга необхідна для захисту синхронізуючих імпульсів від потрапляння імпульсних перешкод з області відеосигналу.

Рядки кадру нумеруються послідовно цифрами від 1 до 625, починаючи з передачі фронту КСІ у першому полі. Першим вважається те поле, біля якого фронти КСІ та РСІ збігаються. При надрядковій розгортці перше поле включає рядки з 1 по 312 і половину 313 рядка, а друге поле включає другу половину рядка 313 і рядки з 314 по 625. Для виключення порушень малої синхронізації РСІ слід передавати і під час КДМ та КСІ. ССІ під час передачі КСІ поміщаються всередині нього у вигляді врізок, з яких у пристроях відображення формуються звичайні РСІ. Перед КСІ розміщена перша, а після нього друга послідовності імпульсів, що зрівнюють. Необхідність зрівнюючих імпульсів, а також врізок у КСІ, що прямують з подвійною рядковою частотою 2fz=31250 Гц, викликана особливістю побудови схем синхронізації блоків розгортки в старих ТВ приймачах.

Амплітуда модуляції пропорційна кількості кольору (насиченості), а інформація про фазу означає відтінок кольору. Частина горизонтального гасіння містить горизонтальний синхроімпульс. Горизонтальна частина гасіння сигналу розташована в часі так, що її не видно на екрані системи відображення (моніторі).

2.2 Огляд існуючих систем шифрування аналогового відеосигналу

Після огляду структури відеосигналу, який, згідно завдань магістерської роботи, має шифруватися за допомогою спотворення, розглянемо найпоширеніші існуючі методи та засоби шифрування аналогового відеосигналу для аналізу їх переваг та недоліків.

Оскільки шифрування аналогового відеосигналу до цього використовувалось лише у телебаченні для шифрування кабельних та супутникових каналів – було зроблено аналіз саме цих систем шифрування.

2.2.1 Загальна класифікація підходів до шифрування аналогового відеосигналу

При шифруванні/дешифруванні необхідно зберегти якість зображення після відновлення дешифратором. При цьому дешифратор має бути недорогим, а значить, відносно нескладним пристроєм. Тому в найбільш популярних кабельних системах адресного кодування використовуються спрощені технології скремблювання. Змінюються лише окремі елементи відеосигналу (як правило, сигнали синхронізації) та/або використовуються прості лінійні перетворення сигналу (наприклад, інверсія). Такі системи кодування прийнято називати "аналоговими", хоча, безумовно, у них використовуються елементи цифрової техніки. Устаткування аналогових систем порівняно дешеве, проте такі системи легко зламуються. Відновлення спотворених елементів відеосигналу здійснюється за іншими елементами того ж сигналу, що залишилися незашифрованими. Піратський декодер, побудований за таким принципом, використовує для декодування лише інформацію, що міститься у самому сигналі, ігноруючи дані управління.

У складніших системах сигнал піддається нелінійним перетворенням, у результаті порушується його тимчасова структура. Як правило, зміщуються за часом або змінюються місцями рядки всередині поля або частини рядків усередині самих рядків. Для відновлення такого сигналу декодер повинен містити пристрій буферної пам'яті на рядок або поле. У процесі декодування аналоговий сигнал спочатку перетворюється на цифрову послідовність, потім обробляється цифровими методами і знову перетворюється на аналогову форму. Такі системи отримали назву "цифрових" - не плутати із системами кодування цифрових каналів! Обладнання цифрових систем кодування значно дорожче, а стійкість до злому значно вища. Відновити сигнал, кодований "цифровими" методами, використовуючи лише інформацію, що міститься в самому сигналі, набагато складніше.

Однак і цифрові системи не гарантують стовідсоткового захисту від зламу. По-перше, сам кодований сигнал залишається аналоговим, і при будь-якій "глибині" кодування просторова кореляційна залежність різних елементів зображення залишається. Простіше кажучи, сусідні елементи зображення (наприклад, послідовні рядки одного поля) менші різняться між собою, ніж елементи, розташовані не поруч. Аналіз елементів зображення на "схожість" (кореляцію) для сучасних комп'ютерів не є складним завданням, і відновлення картинки за принципом мозаїки залишається як мінімум можливим. Це підтверджується фактом злому системи Nagravision-Syster.

По-друге, у зловмисників залишається другий шлях злому – аналіз даних управління декодерами. Як правило, тими хто зламує використовується один із трьох способів. Перший - зміна електричної схеми декодера (установка "перевірочних чіпів", "перевірочних плат", перемичок тощо). Другий - створення зовнішнього пристрою ("кубика"), що вносить зміни до потоку даних управління. І, нарешті, третій спосіб – копіювання (клонування) вмісту ППЗП декодера чи електронної карти.

Стійкість системи тим вища, що більше довжина ключа. А пропускна здатність каналу передачі даних дуже низька. Зрозуміло, ключ може бути

переданий у відкритому вигляді, він кодується за спеціальним алгоритмом, у якому, своєю чергою, ключем є постійний " секретний номер " декодера. Це означає, що черговий ключ для кожного декодера має бути переданий окремо. Через зазначені причини процес роздачі чергового ключа може зайняти досить тривалий час. Для відновлення "картинки" не можна використовувати ключ, отриманий безпосередньо з ефіру - до моменту переходу на новий ключ всі авторизовані декодери повинні його мати. Тому ключ змінюється досить рідко (зазвичай раз на місяць). Отже, будь-який ключ, і постійний і завантажуваний, тривалий час зберігається в незалежній пам'яті декодера (мікросхемі EEPROM). Активація (деактивація) декодерів провадиться не передачею власне ключа, а передачею команди на включення (вимкнення).

І те, й інше знижує стійкість системи, відкриваючи другий шлях для злому. Якщо ключ тривалого використання зберігається в пам'яті декодера, його можна скопіювати. Захист від копіювання здійснюється лише конструктивними методами. У найпростішому випадку - при розтині корпусу відключається батарейка "підживлення" пам'яті, у складніших пристроях (у тому числі в пластикових картах) використовуються спеціальні мікросхеми із захистом від зчитування EEPROM. Якщо декодер управляється командами, отже, команду включення можна імітувати, а команду вимкнення - блокувати. Як правило, піратами використовується один із трьох способів. Перший - зміна електричної схеми декодера (установка "перевірочних чіпів", "перевірочних плат", перемичок тощо). Другий - створення зовнішнього пристрою ("кубика"), що вносить зміни до потоку даних управління. І, нарешті, третій спосіб - копіювання (клонування) вмісту ППЗУ декодера чи електронної карти

2.2.2 Технологія Sync Suppression

Технологія Sync Suppression — подавлення сигналів синхронизації

Суть процесу скремблювання – до відеосигналу додається маскуючий сигнал у вигляді послідовності прямокутних імпульсів, що збігаються за часом із синхронізуючими імпульсами рядків.

В результаті кодованого сигналу рівень малих синхроімпульсів виявляється в зоні розмаху сигналу яскравості (на рівні "сірого"). Маскований синхроімпульс сприймається телевізором як елемент зображення, темні елементи зображення, навпаки, сприймаються як синхроімпульси. В результаті повністю порушується горизонтальна синхронізація, рядки безладно зміщуються по горизонталі, малий синхроімпульс і частина рядкового імпульсу, що гасить, стають видимими (ламана вертикальна лінія в центрі екрану).

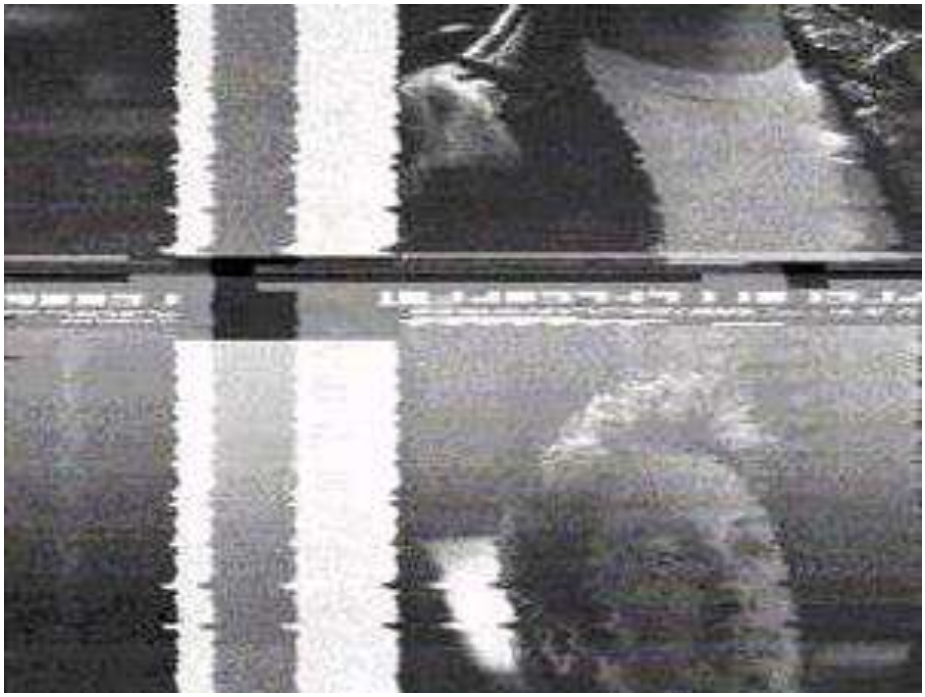

Рисунок 2.6 – Вид екрана при прийомі сигналу з скремлюванням Sync Suppression

Цей метод реалізовували декілька систем.

Система ACS-500 вироблялась НВК "Телевідео", Київ. За кордоном система відома під торговою маркою UNIVERSAL-500. У ACS-500 описаний вище принцип використовується без будь-яких модифікацій. Рівень синхроімпульсів змінений, проте самі імпульси в сигналі присутні, їх фронти залишаються стабільними за часом (див. рис. 2.7 б). Крім того, для забезпечення коректного читання даних і синхронної роботи з кодером, сам декодер повинен синхронізуватися за часом, тому синхроімпульси рядків, що припадають на кадровий інтервал, що гасить, взагалі залишаються без змін. Ці обставини дозволяють легко відновити пригнічені синхроімпульси. Як опорний сигнал піратським декодером можуть використовуватися незамасковані синхроімпульси КДІ, синхроімпульси інших рядків відновлюються по їх фронтах генератором, що задає, з системою автопідстроювання частоти і фази. АПЧФ дозволяє генератору спрацьовувати на фронт імпульсу, тільки якщо він знаходиться у потрібному проміжку часу.

Система CryptOn вироблялась НВФ "Кріптон", м. Антрацит. Організація та можливості системи аналогічні ACS-500, однак, передбачається більш високий рівень захисту. У базовій модифікації у системі CryptOn синхроімпульси рядків не зміщуються за рівнем, а повністю видаляються з сигналу, заміщаючись сигналом постійного рівня (рівень "сірого", див. рис. 2.7 в). Весь малий інтервал гасіння заповнюється квазицветовой піднесучою, таким чином, не залишається жодних явних "слідів" синхроімпульсу. Декодувати такий сигнал дещо складніше, оскільки синхроімпульси потрібно не відновити, а синтезувати.

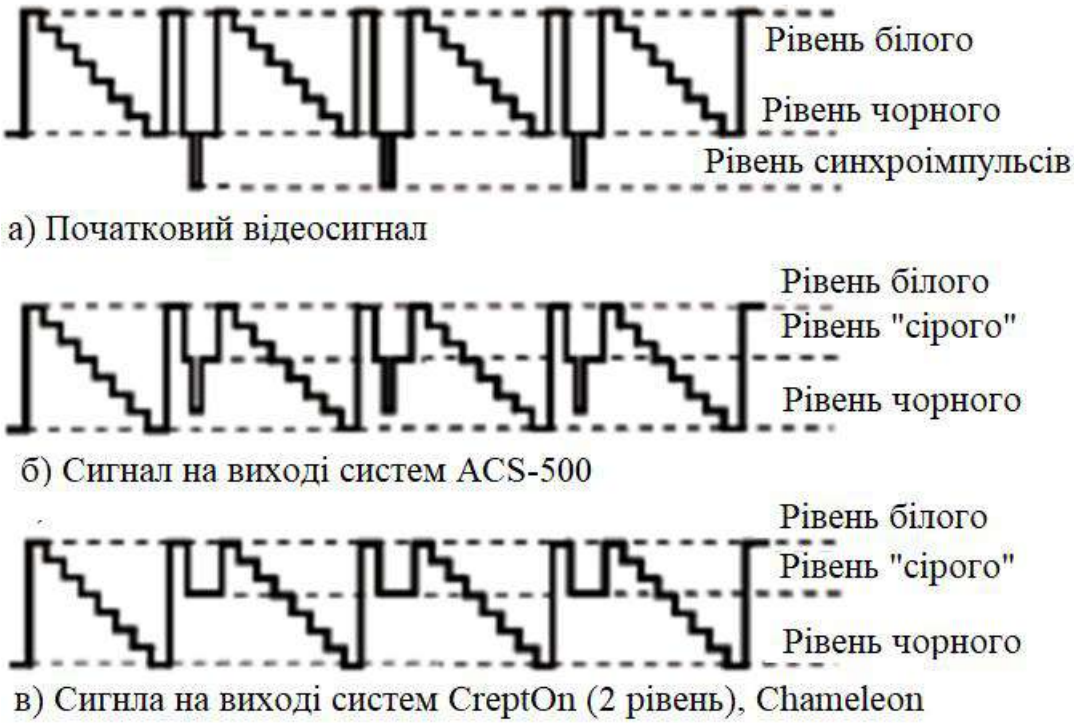

Рисунок 2.7 – Осциллограми сигналів виідео на виході скремблерів Sync Suppression

Розроблено та випробувано модифікацію системи, що забезпечує ще більш високий ступінь захисту. Суть її в тому, що на головній станції до кодера додається кадровий синхронізатор. Це пристрій, що має цифровий буферний блок і дозволяє робити запис сигналу відео з однією тактовою частотою, а відтворення (зчитування) - з іншого. Штатно воно використовується як коректор часових спотворень для джерел сигналу, часові характеристики якого нестабільні (відеомагнітофони). В описуваній системі, навпаки, за допомогою кадрового синхронізатора сигнал навмисно вносяться часові спотворення.

Під керуванням кодера кадровий синхронізатор періодично змінює тактову частоту зчитування деяку малу величину.

В результаті на деяку малу величину змінюється тривалість рядків і, отже, частота слідування малих синхроімпульсів. Зміна досить мала, щоб на екрані телевізора не було помітних спотворень і щоб система автопідстроювання частоти і фази (АПЧФ) генераторів розгорток телевізора,

що задають, могла відстежити і компенсувати зміни. Однак якщо на приймальному кінці синхроімпульси рядків синтезуються не фірмовим декодером, а стабільним незалежним генератором, то через різницю частот PCI сигналу, обробленого веденим кадровим синхронізатором, і генератора, синтезований PCI виявиться зрушеним по фазі щодо "розрахункового" положення. Набіг різниці фази від рядка до рядка збільшуватиметься і неминуче призведе до зриву синхронізації.

Фірмові декодери за командою кодера миттєво перемикають частоту синтезатора PCI, завдяки чому на виході авторизованих декодерів синхронізація зберігається. Декодери CryptOn спочатку здатні працювати як у системі зі стабільними синхроімпульсами, так і в модернізованому, тому введення додаткового захисту не потребує заміни декодерів - достатньо дообладнати головну станцію.

Технологію Chameleon™ розроблено NCA Microelectronics. Системи, що використовують цю технологію та базовий набір IMC виробництва MCA, також випускалися фірмами Megavision Video Industries Ltd. під торговою маркою Megacrypt-2001 та Telelynx Inc. під торговою маркою TeleCipher™.

Система поєднує простий і надійний спосіб скремблювання зображення Sync Suppression із високо захищеним методом передачі інформації для відновлення сигналу. Зі сигналу відео видаляються (заміщаються постійним рівнем) всі синхроімпульси - і малі, і кадрові. Дані, необхідні для їх відновлення, передаються не в рядках кадрового інтервалу, що гасить, а на додатковій звуковій піднесучій. Таким чином, у сигналі відео не залишається взагалі ніяких імпульсів, які можна було б використовувати як позначки часу для відновлення синхронізації. Дані передаються у вигляді пакетів, один пакет на полі (60 разів на секунду в NTSC, 50 разів - у PAL і SECAM). Тимчасове положення кожного пакета щодо початку поля змінюється за псевдовипадковим законом. Це означає, що пакети даних неможливо використовувати для тимчасової "прив'язки" сигналу. Самі дані є псевдовипадковою послідовністю. Мікропроцесор декодера аналізує цю

послідовність, використовуючи один із 128 алгоритмів (ключів), що зберігаються в його енергонезалежній пам'яті, і отримує послідовність даних, що визначають тимчасове положення синхроімпульсів. Псевдовипадкове двійкове слово, що передається 60 (50) разів на секунду, має довжину 32 біти, тобто може приймати одне з 2 мільярдів значень. Період повторення послідовності становить кілька років, тому підібрати часові інтервали між пакетом даних та синхроімпульсом, або записати такі на виході авторизованого декодера і потім відтворити практично неможливо. Якщо оператор має підстави вважати, що використовуваний ключ все ж таки скомпрометований, він просто перемикає канальний кодер на інший алгоритм. Оскільки всі 128 алгоритмів зберігаються спочатку в ППЗУ декодерів, перехід відбувається миттєво. ППЗУ фізично розміщується на кристалі мікропроцесора та захищено від зчитування замовною логічною схемою. На відміну від примітивних систем, в яких функції декодування та аналізу даних розділені, у мікропроцесорі декодера Chameleon™ вони невіддільні один від одного, таким чином, немає можливості змусити вузол декодування працювати "обхід" вузла авторизації. Адресне поле системи складає понад 16 мільйонів адрес. Крім індивідуальної адреси, у пам'ять декодера під час виготовлення може бути записаний ідентифікатор мережі. Виробники гарантують, що для кожної більш-менш великої мережі буде поставлено партію декодерів зі своїм унікальним ідентифікатором. Це повністю виключає можливість використання мережі декодерів, проданих іншому оператору.

Технологія SSAVI (Sync Suppression & Active Video Inversion)

Це найбільш уживана технологія скремблювання аналогового відео. З тими чи іншими модифікаціями вона використовувалась в системах відомих виробників, як Pioneer, Jerrold, Scientific Atlanta. У країнах Скандинавії, США та багатьох інших країнах ця технологія де-факто є стандартом для платних кабельних аналогових мереж.

На рис.2.8 показаний екран пристрою відображення при прийомі кодованого SSAVI відеосигналу. Систему легко впізнати за "картинкою".

Кадровий імпульс, що гасить, стає видимим (темна горизонтальна смуга у верхній частині) і на ньому чітко видно пакети даних, що передаються в рядках КГІ (яскраві чорні і білі горизонтальні штрихи різної довжини).

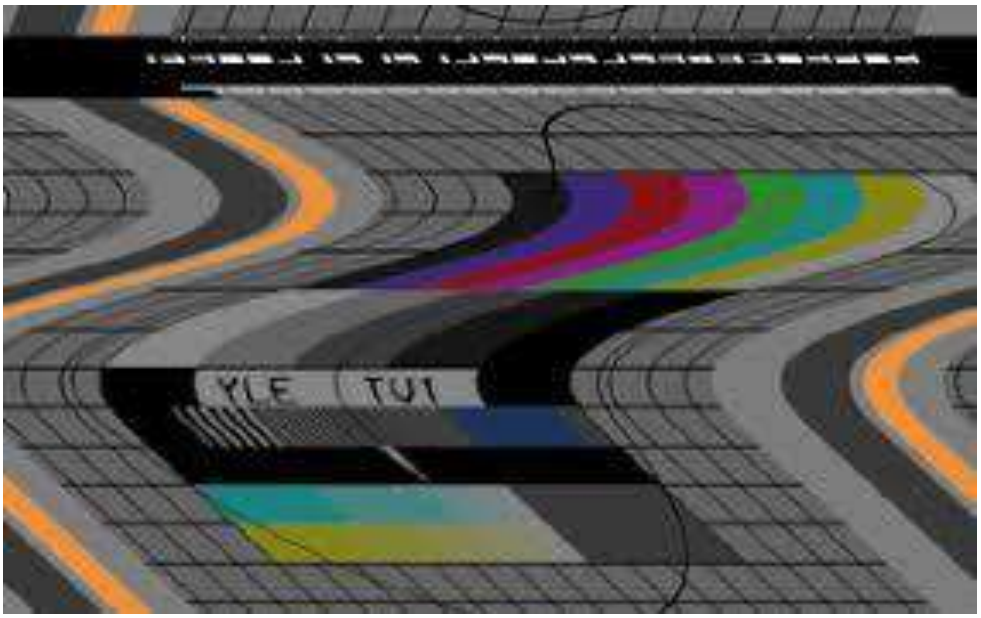

Рисунок 2.8 – Екран пристрою відображення при подачі на нього відеосигналу з SSAVI скремблюванням

Синхроімпульси рядків не видаляються, але зміщуються за рівнем рівня "чорного". Крім того, в деяких рядках сигнал зображення (активна частина рядка) інвертується – рівень "білого" стає рівнем "чорного" і навпаки. Можливі наступні комбінації (режими): пригнічені синхроімпульси / нормальне відео; нормальні синхроімпульси / інвертований відео; пригнічені синхроімпульси / інвертований відео; і, нарешті, нормальні синхроімпульси/нормальний відео. Комбінації змінюються від поля до поля у псевдовипадковому порядку. Ознака інверсії відео передається у вигляді спеціального імпульсу (прапора) у рядках 22 та 335 КГІ (парного та непарного поля відповідно). Дані управління декодерами передаються у вигляді імпульсів з амплітудою від рівня "чорного" до рівня "білого" чотирма пакетами в активній частині рядків КДМ - у рядках 6-9 першого поля та 319-322 другого поля. Крім даних управління доступом, передається спеціальний біт - ознака " вірити/не вірити прапору інверсії " . Наявність такої ознаки

додатково ускладнює завдання піратів. Синхроімпульси рядків, розташовані в кадровому гасячому інтервалі, і імпульси, що зрівнюють, передаються без спотворень. Вони використовуються декодером як опорний сигнал відновлення зміщених синхроимпульсов активної частини поля.

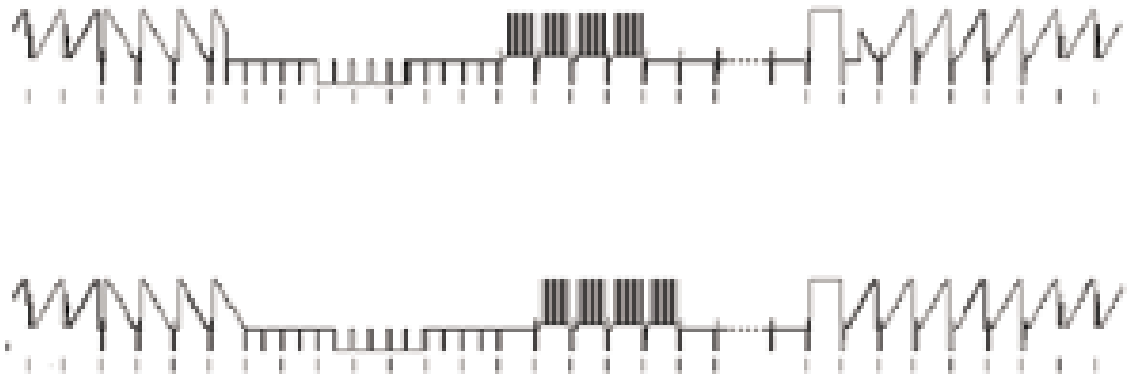

Рисунок 2.9 – Осцилограми відеосигналу з SSAVI

Усі системи, що використовують технологію SSAVI, "надійно" зламані, методи злому докладно описані у піратській літературі. Піратські "універсальні" декодери, "куби" та "тестові" чіпи виробляються серійно та широко рекламуються.

2.2.3 Line Shear

Суть процесу скремблювання: цифровими методами активна частина рядка зміщується за часом щодо свого нормального становища деяку величину, а сигнали синхронізації у своїй залишаються незмінними. Усунення може бути як позитивним (затримка), так і негативним (випередження), а величина його змінюється в деяких межах від рядка до рядка псевдовипадковим чином. Зображення кожного рядка виявляється зміщеним щодо сусіднього рядка і вертикальна структура "картинки" руйнується. Для

того, щоб неможливо було "виміряти" час зміщення та відновити зображення, використовуючи лінію затримки на рядок, "рідні" початок та кінець рядка маскуються. Якщо рядок передається із затримкою, то часовий інтервал від місця, де має бути початок "нормального" рядка, і до фактичного початку затриманого рядка заповнюється псевдовипадковим сигналом. Кінець же затриманого рядка, "що стирчить" далі місця, де має знаходитися кінець "нормального" рядка, обрізається. Якщо рядок передається з випередженням, то, навпаки, початок рядка піддається обрізанню, а кінець - дописуванню (рис.2.10). Таким чином, структура кодованого сигналу не відрізняється від структури вихідного, і відновити зображення, використовуючи тільки інформацію, що міститься в самому сигналі, неможливо. Так як малі синхроімпульси не видозмінюються, немає необхідності видаляти або маскувати сигнали колірної синхронізації, які використовуються декодерами кольоровості телевізорів. Тому основна перевага технології Line Shear перед аналоговими технологіями Sync Suppression і SSAVI - якісніші кольори зображення (принаймні так стверджують виробники). Побічний ефект технології Line Shear – невелике зменшення розміру зображення по горизонталі.

Типова система – PhaseKrypt® – розроблена американською компанією Macrovision Corparation. Сама Macrovision виробляє лише базовий набір IMC та програмне забезпечення, обладнання випускається за її ліцензіями компаніями Eastern Electronics CO Ltd. (Тайвань), Pacific Satellite International Ltd. (Гонконг) та Off Air Electronics (Ірландія) під торговими марками Eastern, Pacific та PhraseKrypt® відповідно.

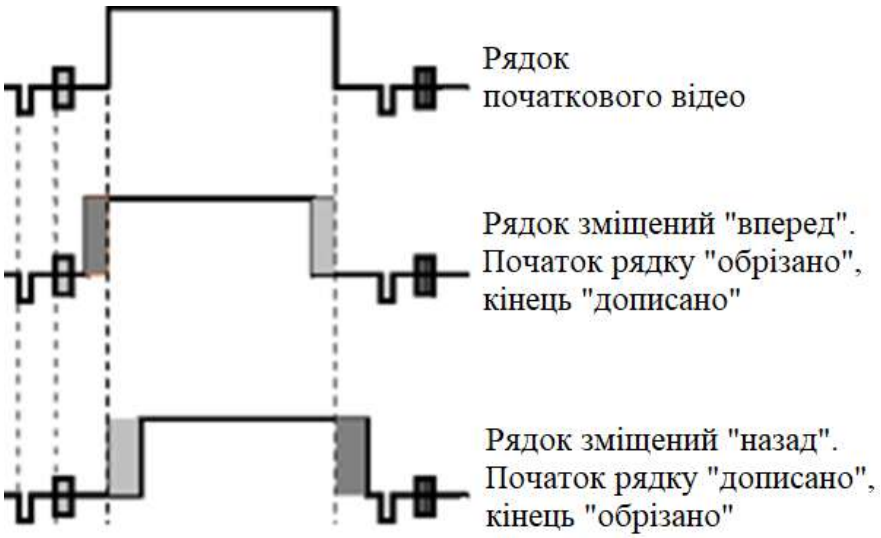

Рисунок 2.10 – Принцип технологии PhaseKrypt

2.2.4 Line Cut & Rotate

Суть процесу скремблювання: кожен рядок видимої частини поля ділиться на дві нерівні частини, потім ці частини змінюються місцями – спочатку передається кінцева частина рядка, потім – початкова. Положення точки "розрізу" змінюється від рядка до рядка псевдовипадковим чином (рис.2.12).

Рисунок 2.11 – Екран пристрою відображення при подаванні відеосигналу спотвореного по принципу Line Cut & Rotate

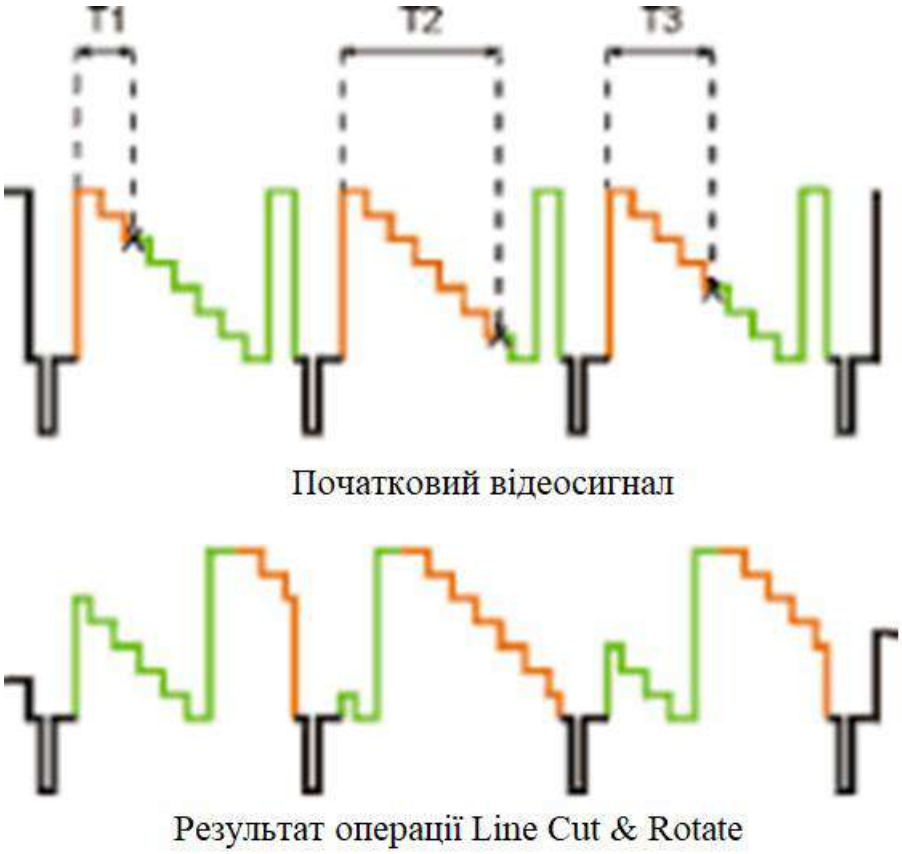

Рисунок 2.12 – Принцип технологии Line Cut & Rotate

Більшість систем, що використовують Cut & Rotate, передбачають 256 можливих положень цієї точки, тобто її положення всередині кожного рядка однозначно визначається двійковим словом (ключом) із 8 біт. Ключ не передається окремо для кожного рядка, а синтезується генератором псевдовипадкових послідовностей (ГПВП) усередині декодера. У випадку ГПВП є зсувний регістр зі зворотними зв'язками. З періодичністю від часток секунди до декількох секунд проводиться початкова установка регістру завантаженням "стартового" ключа, який виділяється з сигналу, що приймається. Для відновлення кодований сигнал кожного рядка перетворюється декодером на цифрову послідовність, потім за допомогою цифрових ліній затримки рядок "розрізається" в "точці склеювання" і "склеюється" в "точці розрізу". На малюнку 6 показані зображення на екрані телевізора прийому відкритого сигналу і сигналу, кодованого за технологією Line Cut & Rotate. Неважко помітити, що, на відміну від аналогових

технологій, за "картинкою" кодованого сигналу неможливо навіть здогадуватися про зміст вихідної "картинки". Відновити зображення, аналізуючи лише сам сигнал відео, практично неможливо, тому технологія Cut & Rotate вважається однією з найзахищеніших.

Типові системи - VTech та Dalvi. Система кодування, що випускається VTech Communications Ltd., використовує лише технологію Line Cut & Rotate. Система Dalvi, розроблена компанією Technetix PLC, передбачає 4 рівні кодування. На рівнях 1 - 3 використовується технологія Line Shear з невеликим, середнім та великим максимальним зміщенням рядків відповідно. На рівні 4 використовується технологія Line Cut&Rotate. В обох системах дані управління декодерами передаються в послідовному вигляді в рядках кадрового інтервалу, що гасить.

2.2.5 Line Shuffle

Сигнал кожного рядка передається без змін, але самі рядки всередині поля змінюються місцями (перемішуються) в псевдовипадковому порядку. Така технологія забезпечує більш високу якість зображення, так як "точки розрізу" розташовуються на невидимій частині відеосигналу - в малих інтервалах, що гасять. Системи Line Shuffle набагато стійкіші, ніж аналогові, але менш стійкі, ніж системи з Line Cut & Rotate. Одна із систем, у якій реалізована технологія Line Shuffle – Nagravision-Syster. Ентузіастам супутникового прийому відомий спосіб піратського декодування цих каналів за допомогою IBM PC з картою ТБ-тюнера та відповідним програмним забезпеченням (MoreTV та подібними).

Підсумовуючи, можна сказати, що абсолютно захищених систем адресного кодування немає. Відповідно випливає питання використання нових принципів шифрування аналогового відеосигнала ніж ті що

використовувались для шифрування телевізійного сигналу кабельних та супутникових систем. В роботі пропонується використання хаотичних сигналів для шифрування аналогового відеосиганлу.

2.3 Хаотичне кодування як метод шифрування аналогового відеосигналу

Хаотичне кодування жодного разу не використовувалось для шифрування аналогового відеосигнала не в одній з відомих систем. Оскільки водо дозволяє накладати власний «код» на початковий сигнал і не мало використання – в роботі пропонується розробити метод кодування аналогового відео на основі хаотичних сигналів.

Хаотичні системи виглядають як динамічні системи, які не піддаються синхронізації. Дві ідентичні автономні хаотичні системи, що почалися майже в однакових початкових точках у фазовому просторі, мають траєкторії, які швидко стають некорельованими, навіть якщо кожна відображає той самий атрактор у фазовому просторі. Таким чином, практично неможливо побудувати ідентичні, хаотичні, синхронізовані системи в лабораторії.

Останнім часом зростає кількість літератури, яка підтримує можливість практичного спілкування за допомогою хаотичних сигналів. Зокрема, нещодавні досягнення в розумінні нелінійних схем показали, що хаотичні осцилятори можуть синхронізуватися або захоплюватися.

Здатність проектувати системи синхронізації в нелінійних і, особливо, хаотичних системах може відкрити цікаві можливості для застосування хаосу в комунікаціях, використовуючи унікальні особливості хаотичних сигналів. Тепер є можливість мати дві віддалені системи з багатьма внутрішніми сигналами, які поводяться хаотично, але все ще синхронізовані один з одним через один зв’язуючий сигнал приводу.

Як повідомляється в літературі, синхронізація хаотичних систем припускає можливість для зв'язку з використанням хаотичних сигналів як носіїв, можливо, із застосуванням для безпечного зв'язку. Очевидний підхід використовує хаотичний осцилятор як передавач і синхронну хаотичну систему для приймача, і було запропоновано кілька конструкцій, які відповідають цій методиці.

Розглянено підхід, який використовує для досягнення безпечного зв’язку хаотичний сигнал для маскування сигналу конфіденційної інформації. У цьому підході синхронна хаотична система використовується в приймачі для ідентифікації хаотичної частини сигналу, яка потім віднімається для виявлення інформаційного сигналу.

Підхід для аналогового зв’язку досягається шляхом виявлення невідповідності параметрів між передавачем і приймачем. Неузгодженість, яка навмисно вводиться в передавач, виявляється шляхом порівняння отриманого сигналу з реплікою, сформованою за допомогою каскадних синхронних підсистем. Ця схема визнає, що величина різниці в цих сигналах пропорційна невідповідності параметрів, забезпечуючи таким чином грубий метод демодуляції. Однак цей підхід страждає, коли в каналі зв’язку присутній шум.

Кілька дослідників використовували інверсний системний підхід для комунікації з використанням хаосу. У цьому підході інформаційний сигнал змішується з хаотичною формою сигналу за допомогою операції функціонального кодування. Приймач складається з синхронного хаотичного генератора, з якого інформаційний сигнал відновлюється шляхом ефективного інвертування операції кодування, що використовується в передавачі.

Загальний опис нашого підходу складається у наступному. У передавачі аналоговий інформаційний сигнал кодується на несучій за допомогою модуляції параметра в хаотичному генераторі. У приймачі синхронна хаотична підсистема доповнена фільтром, розробленим спеціально для безперервного вилучення сигналу з модульованої форми сигналу. Правильний

вибір каналу приводу та параметра модуляції забезпечує синхронізацію в приймачі незалежно від модуляції.

Розглянемо модель шифрування за допомогою внутрішньосмугового хаотичного скремблера для захисту бездротового аналогового відео. У цій системі аналоговий відеосигнал подається на хаотичний генератор, а вихідний сигнал передається через стандартний бездротовий відеоканал. На приймачі дескремблер відокремлює відео від хаотичного сигналу в режимі реального часу. Експериментальні результати показують, що зашифрований сигнал ефективно приховує оригінальне відеозображення, проте дескремблер відновлює оригінальне кольорове відео з достатньою чіткістю і деталізацією. У порівнянні з цифровим шифруванням, хаотичне скремблювання пропонує ефективну, недорогу альтернативу для маскування критично важливого за часом аналогового зв'язку.

Поєднання цифрового відео та сучасних технологій шифрування практично гарантує, що наступне покоління бездротових відеозв'язків буде безпечним. Однак, незахищені аналогові бездротові відеосистеми все ще широко використовуються в багатьох існуючих системах. Для багатьох із цих застарілих систем перехід на захищений цифровий канал зв'язку може бути недоцільним через надмірну вартість і високі вимоги до енергоспоживання. Фактично, сигнали в цих системах продовжуватимуть передаватися у відкритому вигляді, де їх легко виявити і перехопити.

Рисунок 2.13 – Подібності та відмінності між хаотичними системами та криптографічними алгоритмами

На рис.2.13 узагальнено подібності та відмінності між хаотичними картами та криптографічними алгоритмами. Хаотичні карти та криптографічні алгоритми (або загальніше карти, визначені на скінченних множинах) мають деякі подібні властивості: чутливість до зміни початкових умов і параметрів, випадкова поведінка та нестабільні періодичні орбіти з великими періодами. Раунди шифрування криптографічного алгоритму призводять до бажаних

властивостей дифузії та плутанини алгоритму. Ітерації хаотичної карти поширюють початкову область на весь фазовий простір. Параметри хаотичної карти можуть являти собою ключ алгоритму шифрування. Важлива відмінність між хаосом і криптографією полягає в тому, що перетворення шифрування визначаються на кінцевих наборах, тоді як хаос має значення лише на дійсних числах. Крім того, на даний момент поняття криптографічної безпеки та продуктивності криптографічних алгоритмів не мають аналогів у теорії хаосу.

Два загальні принципи, якими керується розробка практичних алгоритмів, - це дифузія та плутанина. Дифузія означає поширення впливу однієї цифри відкритого тексту на багато цифр зашифрованого тексту, щоб приховати статистичну структуру відкритого тексту. Розширенням цієї ідеї є поширення впливу однієї цифри ключа на багато цифр зашифрованого тексту. Плутанина означає використання перетворень, які ускладнюють залежність статистики зашифрованого тексту від статистики відкритого тексту. Властивість змішування хаотичних карт тісно пов'язана з властивістю дифузії в шифрувальних перетвореннях (алгоритмах). Система F має властивість змішування (або просто є змішуванням), якщо для будь-яких двох вимірних множин A1 і A2 маємо $\lim n \to \infty \mu(F - nA1 \cap A2) = \mu (A1) \mu(A2)$ [10] . Іншими словами, будь-який набір початкових умов ненульової міри з часом буде поширюватися на весь фазовий простір у міру еволюції системи [10]. Якщо ми думаємо про набір можливих (чуттєвих) відкритих текстів як про початкову область у фазовому просторі карти (перетворення), то це властивість змішування (або, іншими словами, чутливість до початкових умов), яка передбачає «розповсюдження вплив однієї цифри відкритого тексту на багато цифр зашифрованого тексту».

Системи змішування мають також таку корисну властивість [10]: якщо $\mu 0$ є довільною мірою (нормованою та абсолютно неперервною відносно μ), і $\mu n = \mu 0(F- n A)$, то $\mu n(A) \to \mu(A)$ для будь-який вимірний A. Таким чином, можна сказати, що в динамічних системах з властивістю змішування будь-

який нерівноважний розподіл прагне до рівноваги. Іншими словами, в межі, коли кількість ітерацій прагне до нескінченності, статистика шифротексту (обчислена за допомогою інваріантної міри) не залежить від статистики відкритого тексту (який відповідає початковій області у фазовому просторі карта).

Хороший алгоритм шифрування також поширює вплив однієї цифри ключа на багато цифр зашифрованого тексту. Ключі алгоритму шифрування представляють його параметри. Тому ми повинні розглядати лише такі перетворення, в яких і параметри, і змінні залучені чутливим чином, тобто «невелика варіація будь-якого» (змінної, параметра) «суттєво змінює результати». Іншими словами, свого роду «властивість змішування» також має зберігатися в просторі параметрів карти, якщо ми хочемо використовувати хаотичні карти як алгоритм шифрування. Це означає, що ми розглядаємо тільки ті карти, для яких хаос є стійким при малих збуреннях параметрів (ключів).

Динамічна система є структурно стабільною, коли невеликі збурення C1 дають топологічно еквівалентну систему. Іншими словами, структурно стабільна або надійна система перенавчає свої якісні властивості при невеликих збуреннях. Надійні або структурно стабільні хаотичні атрактори можуть, зрештою, забезпечити властивість дифузії в ключовому просторі. Алгоритми, засновані на ненадійних системах, можуть мати слабкі ключі. Проте більшість хаотичних атракторів є структурно нестабільними [11]. Тому до вибору хаотичних карт слід підходити дуже обережно. Відомо, що робастний хаос не може виникнути в гладких системах, тоді як структурно стійкий хаос може виникнути в кусково-гладких відображеннях [12].

Слід розглядати лише системи, які мають стійкий хаос для великого набору параметрів (ключів). Ентропія криптосистеми є мірою розміру ключового простору і зазвичай апроксимується $\log_2 K$, де K є кількістю ключів. Отже, більший простір параметрів динамічної системи означає, що її дискретизована версія матиме більший K.

2.4 Алгоритм шифрування з використанням хаотичних сигналів

Теорія хаосу, як розділ теорії нелінійних динамічних систем, звернула нашу увагу на дещо дивовижний факт: низькорозмірні динамічні системи здатні до складної та непередбачуваної поведінки.

Для простоти ми розглядаємо тут динамічну систему з дискретним часом, визначену ітерацією функції F: X → X, X ∈ RN. Набір точок {x, F(x), F2(x), …} називається траєкторією (або орбітою) початкової умови x. Припустимо, що F має хаотичний атрактор. Неофіційно атрактор називають хаотичним, якщо рух на ньому є непередбачуваним: два сусідні стани на атракторі мають різну та непов’язану поведінку в атракторі.

Еволюція детермінованої системи повністю визначається векторним полем F і початковою умовою x. Однак, щоб повністю визначити початковий стан, необхідна нескінченна кількість інформації та вимірювальна система з нескінченною точністю, які є важкорозв’язними. Які наслідки кінцевої точності вимірювальної системи? Вимірювання початкового (і майбутнього) стану еквівалентно розділенню простору станів на кінцеву кількість областей і спостереженню за еволюцією в цьому макроскопічному світі. Будь-який набір із кінцевого числа непересічних областей, які охоплюють простір станів, називається розбиттям системи. Процес поділу простору станів, присвоєння символів кожній області з поділу та результуюча макроскопічна динаміка називається символьною динамікою.

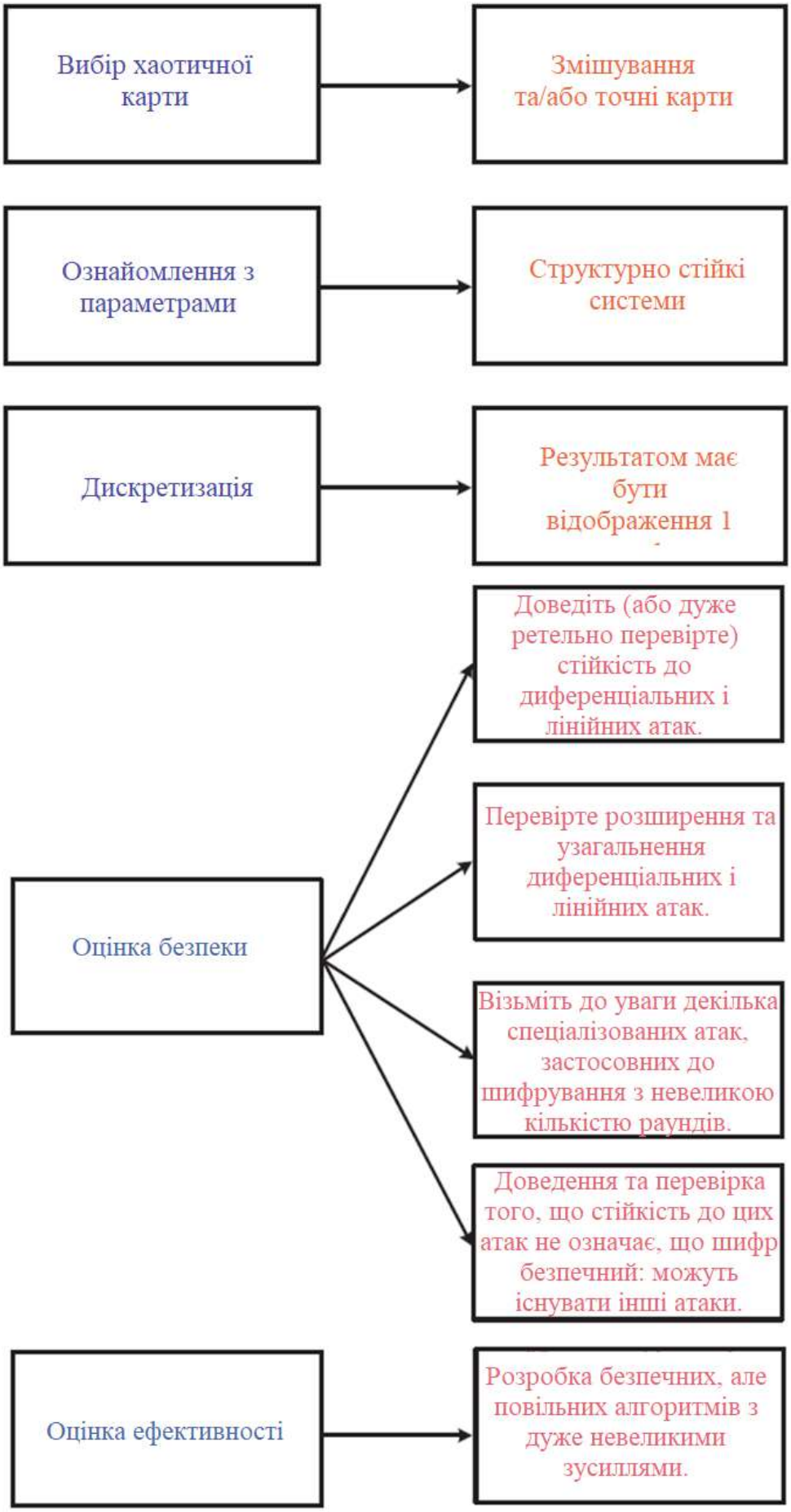

Рисунок 2.14 – Алгоритм блочного шифрування на основі хаосу

Якщо система є хаотичною, то різні початкові стани, що належать одній області, призведуть до різних спостережень пізніше. З точки зору нашої системи, ідентичні макроскопічні початкові стани розвиваються по-різному. Відбулася втрата детермінізму, і переходи між областями розбиття можна вказати лише за допомогою ймовірностей. Поділ простору станів перетворює детерміновану хаотичну систему на ергодичне джерело інформації, яке можна аналізувати з точки зору теорії інформації. Ентропія Колмогорова-Сіная (позначається hKS) є мірою асимптотичної швидкості створення інформації шляхом ітерації F. Системи з позитивною ентропією зазвичай вважаються хаотичними. Непередбачуваність хаотичних траєкторій зумовлена експоненціальним рознесенням найближчих точок. Непередбачуваність означає невизначеність; тому слід очікувати, що ентропія динамічної системи пов'язана з її додатними показниками Ляпунова. Цей глибокий математичний результат (відомий як теорема Песіна) строго доведено лише для так званої міри Сіная-Рюелля-Бовена.

З точки зору будь-якого вимірювального пристрою, якщо динамічна система виробляє непередбачувані послідовності, то динамічна система називається хаотичною. Тоді як рух динамічної системи в безперервному (мікроскопічному) просторі станів є детермінованим, її рух у розділеному (макроскопічному) просторі є стохастичним, а траєкторії є послідовностями символів. На основі знання минулої грубозернистої траєкторії системи ми можемо передбачити її майбутні макроскопічні стани лише в імовірнісних термінах. Перетворення детермінованої хаотичної системи на джерело інформації через поділ простору станів не суперечить зауваженню Шеннона [14] про те, що детермінована система не може генерувати інформацію. Насправді хаотична система не породжує інформацію, тобто її еволюція повністю визначається початковим станом. Хаотична система просто перетворює інформацію про свій початковий стан у форму, видиму для вимірювальної системи. Кожна літера в крупнозернистої траєкторії, яка є

послідовністю літер, приносить додаткову кількість інформації про початковий стан.

Слово випадковий у детермінованих динамічних системах пов’язане з нестисливістю інформації: траєкторія системи називається випадковою, коли найкоротша програма, яка її генерує, має (по суті) такий самий розмір, як і сама траєкторія. Траєкторія руху точки x називається випадковою, якщо її алгоритмічна складність позитивна. Суттєве значення в цьому випадку має наступна теорема [15]: для хаотичних систем траєкторії майже всіх точок стану $x \in X$ є випадковими і їх алгоритмічна складність дорівнює ентропії Колмогорова-Сіная hKS. Як тривожний наслідок, жодна кінцева комп’ютерна програма не може створити або передбачити хаотичну траєкторію, або, кажучи мовою Джозефа Форда [16], для будь-якого додаткового біта початкового стану, комп’ютерна програма може вивести лише один додатковий біт про хаотична траєкторія.

Очевидно, що позитивної алгоритмічної складності майже всіх початкових станів недостатньо для випадковості траєкторій динамічної системи; наприклад, динамічна система зі стабільною рівновагою суперечить такій гіпотезі. Що є джерелом непередбачуваності та інформаційної генерації хаотичної поведінки? Кінцева точність будь-якої реальної вимірювальної системи та чутлива залежність хаотичної еволюції від зміни початкових станів поєднуються з нездатністю довгострокового передбачення хаотичної поведінки.

Сподіваємось, цей розділ розв’язує зіставлення трьох, здавалося б, суперечливих термінів: «випадковий», «детермінований» і «хаос». Детермінованість визначальних рівнянь передбачає наявність і єдиність розв’язків, але не припускає обчислюваності розв’язків. Хаотичність поведінки передбачає випадкові траєкторії, які не піддаються обчисленню жодною кінцевою комп’ютерною програмою. Більше про цей зв’язок можна знайти в натхненних статтях Джозефа Форда [16].

Хаос є необхідною, але недостатньою властивістю алгоритмів шифрування. Згідно з приписами Шеннона [7], кожен алгоритм шифрування має властивості плутанини, дифузії, змішування та чутливості до змін у відкритому тексті та секретному ключі. Це майже гарантує, що розширення області алгоритму шифрування від решітки до континууму призведе до хаотичної карти.

Хаотичні системи характеризуються позитивним показником Ляпунова, позитивною ентропією та позитивною алгоритмічною складністю. З іншого боку, відображення та/або системи з дискретним часом, які були запропоновані для використання в криптографії, визначені на кінцевих наборах цілих чисел. У таких системах найбільший показник Ляпунова і складність нескінченної послідовності тривіально дорівнює 0, тому що кожна орбіта врешті-решт є періодичною і буде повторюватися. Тому центральною проблемою тут є оцінка властивостей (LE, ентропія, складність і так далі) типової орбіти за час, що не перевищує її період.

Хороший криптографічний алгоритм пропонує оптимальний компроміс між безпекою та продуктивністю. Властивості хаотичних систем є асимптотичними, однак криптографічні алгоритми зазвичай побудовані на властивостях дуже швидкої дифузії та/або плутанини.

Можна чисельно перевірити дифузійну властивість алгоритму простим способом: через скільки ітерацій (раундів) маленька хмара початкових точок (відкритий текст) рівномірно поширюється по всьому простору так, що середня кількість нулів (або одиниць) у блоці 2p бітів є p. Це число дає силу властивості дифузії в алгоритмі подібно до того, як вимірюють силу хаосу в безперервних системах.

Головне припущення в інформатиці полягає в тому, що модель машини Тюрінга є відповідною моделлю цифрового комп’ютера та комп’ютерного моделювання. Однак нещодавно було стверджено, що інша модель обчислень, заснована на дійсних числах, також є відповідною і в деяких випадках більш корисною як модель комп’ютера. Обидві моделі, звичайно, є абстракціями

(машина Тьюрінга використовує тип необмеженої нескінченної довжини, тоді як для представлення одного дійсного числа потрібна нескінченна кількість бітів). Мені здається, що також доцільно, принаймні на теоретичному рівні, розглянути неперервну (дійсне число) модель для вирішення деяких проблем у криптографії. Ця модель, якщо її використовувати в криптографії, буде невід'ємно пов'язана з теорією хаосу.

2.5 Реалізація принципу шифрування на основі запропонованого алгоритму

Щоб унеможливити випадкове прослуховування допустиме застосування малопотужного аналогового відеоскремблера на основі синхронізованого хаосу. Ця внутрішньосмугова скремблерна система сумісна з існуючими бездротовими каналами передачі відео, при цьому вона відповідає мінімальним вимогам до вартості та енергоспоживання. Хоча ця технологія не може забезпечити таку ж безпеку, як цифрове шифрування, хаотичне скремблювання забезпечує ефективну модернізацію для критично важливого зв'язку в застарілих системах, де низька вартість і низьке енергоспоживання є критично важливими.

Як показано на рисунку 2.15, хаотичний скремблер розташований між джерелом відеосигналу і радіопередавачем в аналоговому бездротовому відеозв'язку.

Відеосигнал базової смуги пропускається через хаотичний генератор, який перекриває спектральну смугу відеосигналу.

В результаті сигнал нелінійно змішується з випадковими, непередбачуваними хаотичними коливаннями, в результаті чого на виході отримуємо зашумлений скрембльований сигнал. Оскільки скрембльований сигнал міститься в межах смуги пропускання відеосигналу, його можна

передавати стандартним аналоговим відеорадіоканалом. Дескремблер розташований відразу після радіоприймача і містить другий хаотичний генератор. Якщо дескремблер узгоджений зі скремблером, генератори синхронізуються і процес модуляції може бути інвертований, відновлюючи вихідний відеосигнал. Без синхронізації хаотичний сигнал не може бути легко розшифрований, а оригінальна форма відеосигналу залишається прихованою. Хаотичне скремблювання використовує властивості синхронізації зв'язаних нелінійних генераторів.

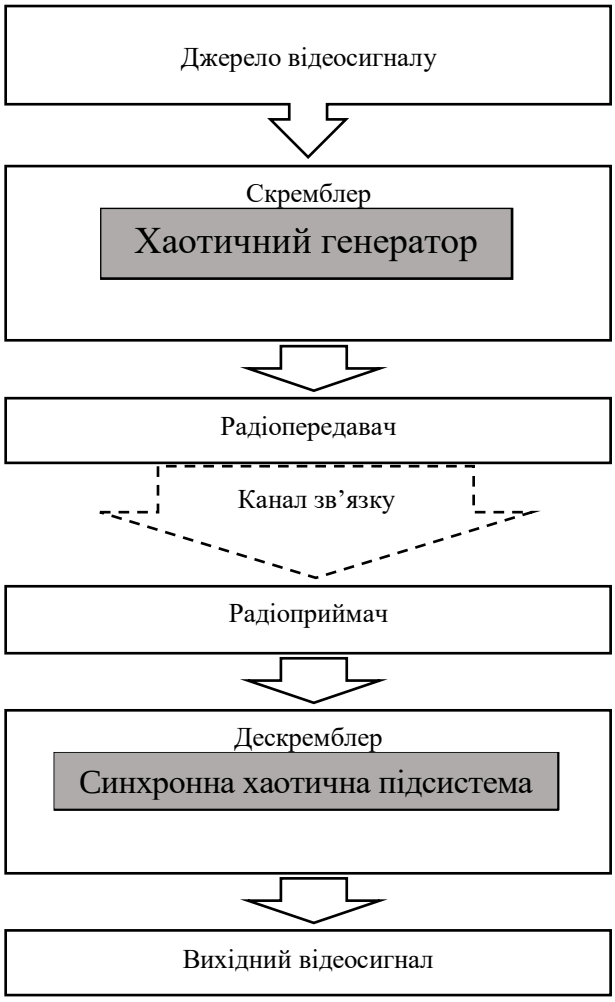

Рисунок 2.15 – Структура роботи хаотичної аналогової системи скремблювання

Відеосигнал керує першим генератором, який знаходиться в передавачі. Типовий хаотичний генератор може бути змодельований нелінійною системою третього порядку за формулою:

$$\frac{dx}{dt} = f(x, y, z) + s(t)$$

$$\frac{dy}{dt} = g(x, y, z)$$

$$\frac{dz}{dt} = h(x, y, z)$$

де x, y і z - динамічні стани скремблера;

s(t) - вхідний відеосигнал;

f, g і h - функції, що визначають хаотичний потік.

Результуюче коливання є складною, нелінійною комбінацією непередбачуваного хаосу та вхідного відеосигналу. Стан x(t) - це зашифрований сигнал, який передається замість відеосигналу s(t). Для підслуховувача переданий сигнал не схожий на оригінальний вхідний відеосигнал.

Другий генератор розташований на приймачі і формує дескремблер. Він спеціально підібраний так, щоб відповідати першому генератору, і моделюється за формулою:

$$\frac{dY}{dt} = g(x, Y, Z)$$

$$\frac{dZ}{dt} = h(x, Y, Z)$$

$$S(t) = \frac{dx}{dt} - f(x, Y, Z)$$

де Y і Z - стани відгуку;

f, g і h - ті самі функції, що й у скремблерному генераторі.

Дескремблер утворює інверсну систему для відновлення модульованого сигналу.

Перші два з цих рівнянь представляють синхронну підсистему, яка відтворює стани скремблера як Y(t) → y(t) і Z(t) → z(t). Останнє рівняння "інвертує" процес скремблювання, відновлюючи відеосигнал у вигляді S(t) → s(t).

Якщо дескремблер не відповідає скремблеру, схеми не синхронізуються і відео залишається прихованим. Таким чином, синхронізація покладається на дескремблер, який використовує точно такі ж нелінійні функції f, g і h, як і скремблер, а параметри цих функцій складають ключ безпеки. Без відповідного дескремблера зловмисник, швидше за все, буде змушений вдатися до складної і дорогої цифрової обробки сигналу, щоб витягти корисну відеоінформацію.

Вперше теоретично зв'язок за допомогою хаотичного шифрування було запропоновано на початку 1990-х років. Однак практична реалізація таких систем для аналогового відео була ускладнена відсутністю відповідних схем високочастотних хаотичних генераторів.

В основі скремблера лежить хаотична радіочастотна схема, яка підходить для скремблювання відеосигналів і більш швидких сигналів.

Варіант цього генератора використовується в системі скремблера відеосигналів.

Схему хаотичного генератора показано на рисунку 2.16.

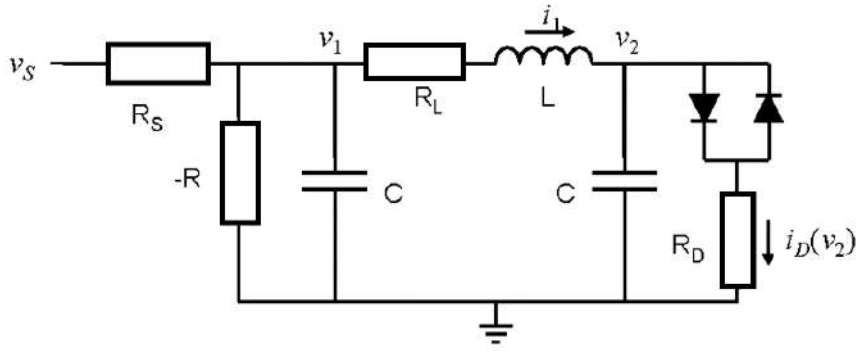

Рисунок 2.16 - Схема хаотичного скремблера з вхідним відеосигналом *v*S та скремблерним виходом *v*1

Ця схема складається з низки стандартних лінійних компонентів, а також двох діодів, які забезпечують нелінійність, необхідну для хаосу.

Для цієї моделі типовими значеннями, які дають хаотичну динаміку, є конденсатори C = 1 нФ, котушка індуктивності L = 22 нГн, опори Rl = 25 Ом, Rs = 510 Ом і R = 150 Ом. Ці елементи використовуються як номінальні значення при проектуванні скремблерної системи. Для моделі діода використовуються значення V_D = 0,3 В і R_D = 40 Ом.

Єдиним активним компонентом є від'ємний резистор. Схема моделюється за формулою:

$$C\frac{d_v}{dt} = \frac{v_1}{R} - i_1 + \frac{v_S - v_1}{R_S}$$

$$L\frac{di_1}{dt} = v_1 - v_2 - i_1 R_L$$

$$C\frac{dv_2}{dt} = i_1 - i_D(v_2)$$

де v_1 і v_2 – напруги;

i_1 - струм.

Струм діода i_D є нелінійною функцією напруги v_2, яку можна моделювати за допомогою дискретно-лінійної апроксимації, яка виражається формулою:

$$i_D(v) = \begin{cases} \frac{v + V_D}{R_D} & v < -V_D \\ 0 & |v| \le V_D \\ \frac{v - V_D}{R_D} & v > V_D \end{cases}$$

де V_D - напруга перемикання для окремого діода.

Важливим компонентом у схемі є від'ємний резистор. Цей активний пристрій забезпечує підсилення для підтримки хаотичних коливань. Від'ємний резистор реалізується за допомогою схеми підсилювача зі зворотним зв'язком, як показано на рис. 2.17.

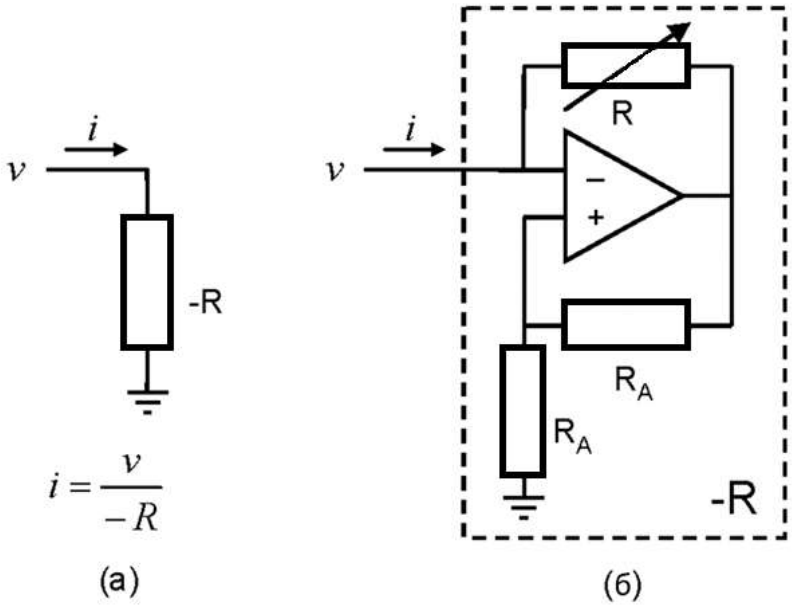

Рисунок 2.17 - Схеми, що показують залежність струм-напруга (а) і практичну реалізацію схеми для пристрою з від'ємним резистором (б)

У цій реалізації величина від'ємного опору задається безпосередньо змінним резистором R.

Типова форма сигналу отриманого за допомогою чисельного моделювання при vS = 0, показано на рис. 2.18.

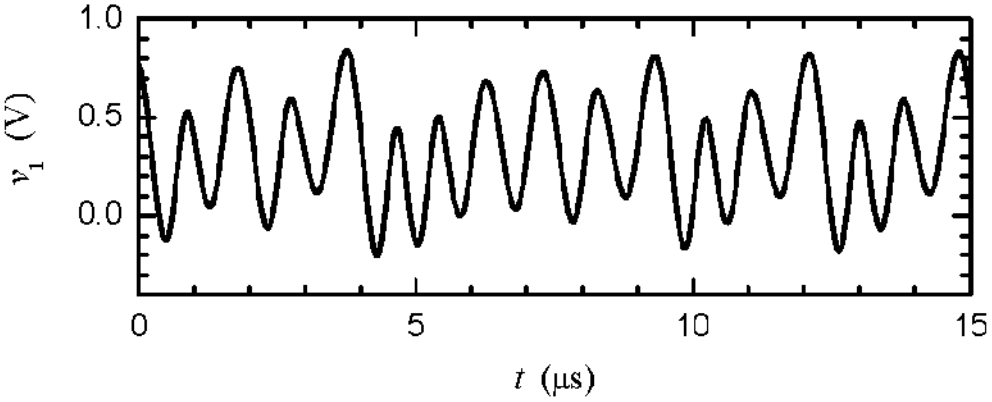

Рисунок 2.18 - Типовий хаотичний сигнал v_1(t), отриманий за допомогою чисельного моделювання моделі осцилятора з v_S = 0

Форма сигналу демонструє синусоїдальні коливання з коливаннями амплітуди від циклу до циклу. Середній час повернення від піку до піку становить 0,92 мс, що відповідає середній частоті 1,1 МГц. Проекція фазового простору v_1-v_2 показана на рисунку 2.19.

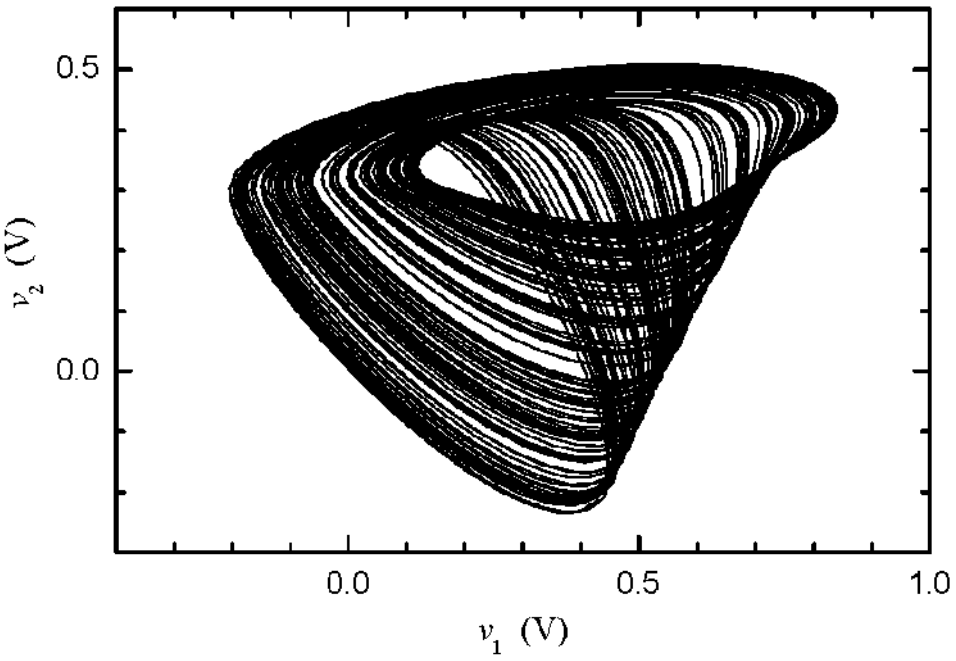

Рисунок 2.19 - Хаотичний атрактор, спроектований на площину v_1- v_2, отриманий з чисельного моделювання моделі генератора з $v_S = 0$

Для номінальних значень параметрів генератор має два атрактори пов'язані симетрією (v_1, i_1, v_2)→(-v_1, -i_1, -v_2). Фізично кожен з цих атракторів відповідає коливанням навколо робочої точки для симетричних діодів. Атрактор, який спостерігається в симуляції, залежить від використаних початкових умов.

Для роботи в якості скремблера генератор модулюється вхідним відеосигналом v_S, причому сила модуляції задається підлаштуванням резистора R_S. На виході скремблера отримуємо сигнал напруги v_1. Для $v_s \neq 0$ зв'язок такий, що вхідна модуляція є лише невеликим збудженням природної динаміки генератора, і хаотичний характер генератора зберігається. В результаті скрембльований вихідний сигнал v_1 є складною, нелінійною комбінацією непередбачуваного хаосу та вхідного відеосигналу.

Відповідна схема дескремблера показана на рис. 2.20.

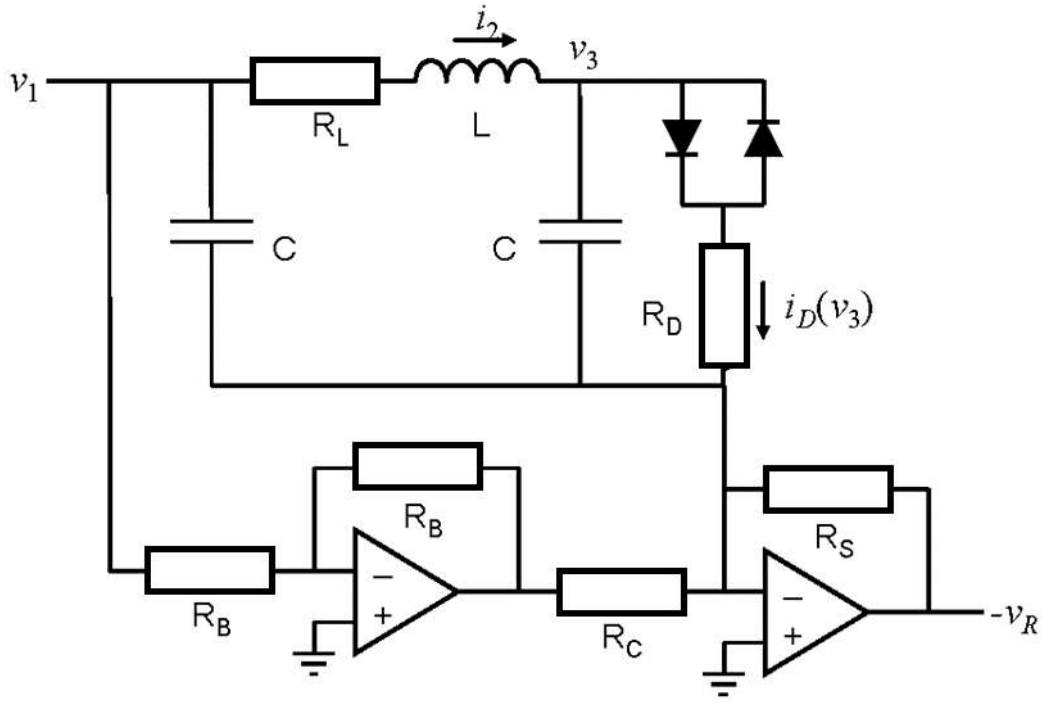

Рисунок 2.20 - Схема дескремблера зі скрембльованим входом v_1 та відновленим відео виходом v_R

Ця схема розроблена таким чином, щоб задовольняти зворотні рівняння:

$$L\frac{di_2}{dt} = v_1 - v_3 - i_2 R_L$$

$$C\frac{dv_3}{dt} = i_2 - i_D(v_3)$$

$$v_R = R_S\left\{C\frac{dv_1}{dt} + \left(\frac{1}{R_S} - \frac{1}{R}\right)v_1 + i_2\right\}$$

де $v_R \rightarrow v_S$ - відновлений сигнал.

В оберненій системі перші два рівняння утворюють синхронну підсистему, яка відтворює інші стани генератора скремблера, що не передаються. Зокрема, стани дескремблера асимптотично наближаються до $i_2 \rightarrow i_1$ і $v_3 \rightarrow v_2$. Останнє рівняння інвертує рівняння невикористаного скремблера і розв'язує його для модуляції.

У схемі дескремблера обмеження проектування повинні відповідати моделі дескремблера, що виражається за формулою:

$$\frac{1}{R_C} = \frac{1}{R} - \frac{1}{R_S}$$

Однак на практиці змінний резистор R_C треба просто підлаштовувати для оптимального відновлення сигналу.

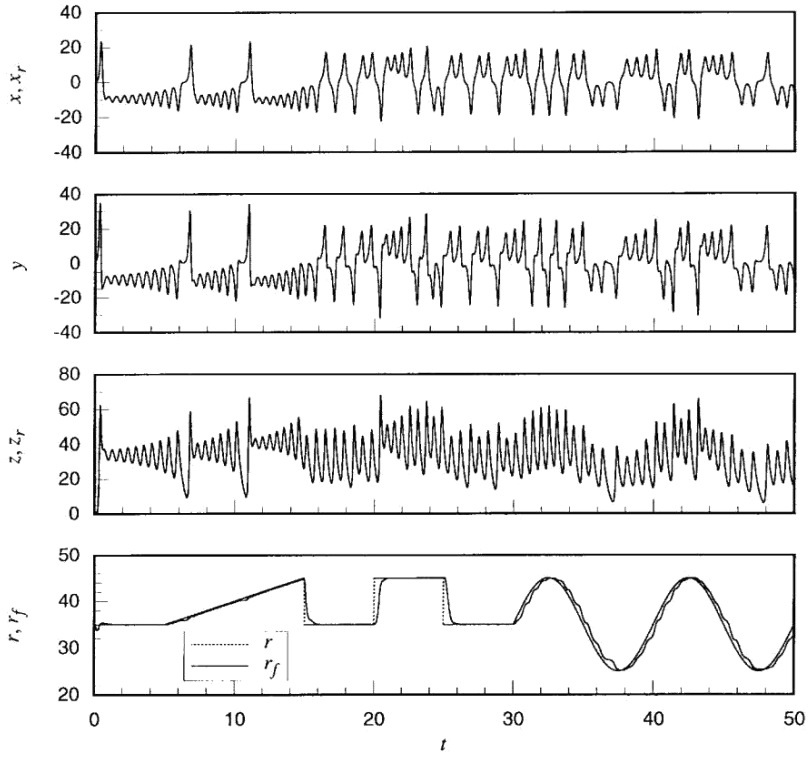

Рисунок 2.21 – Результати моделювання для системи зв’язку на основі хаотичного осцилятора Лоренца

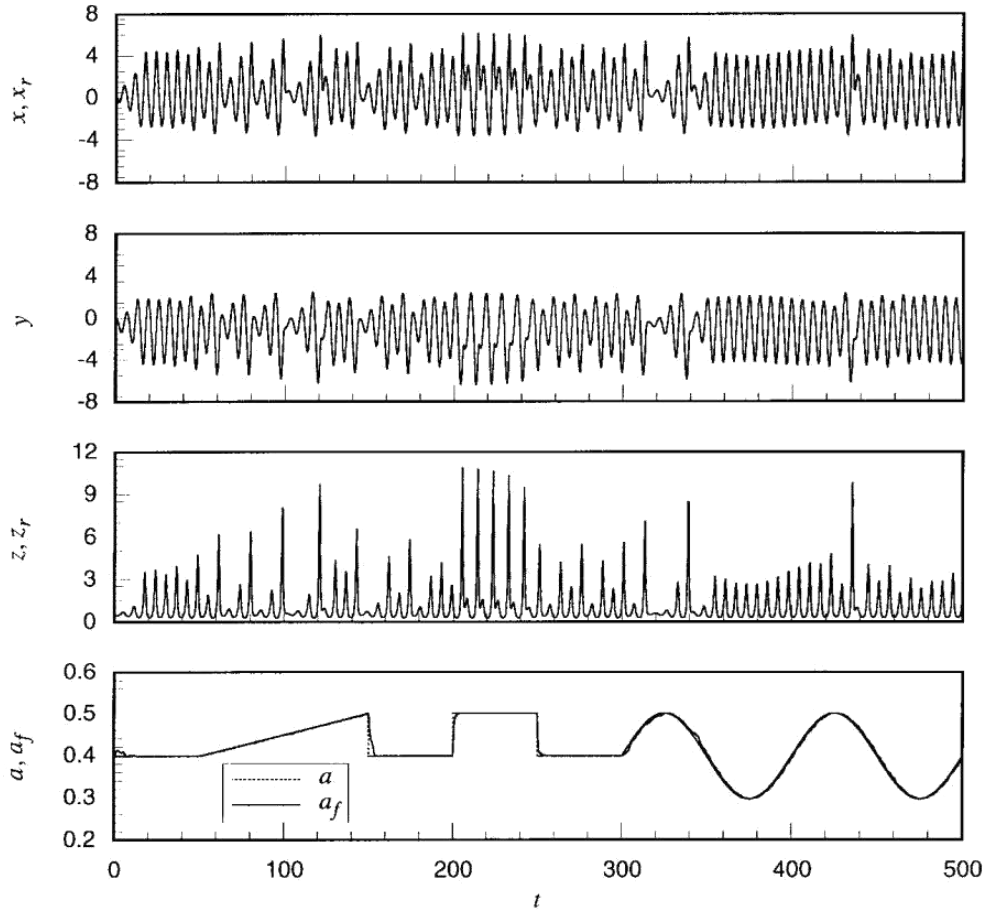

Рисунок 2.22 – Результати моделювання для системи зв’язку на основі хаотичного осцилятора Росслера

Однією з важливих переваг цієї комунікаційної архітектури є те, що синхронізація підтримується в приймачі навіть за наявності модуляції. Теорія передбачає, що приймач не збивається, оскільки передавач модулюється. Це випливає з вибору параметра модуляції, який не відображається в синхронній підсистемі. Ця конструкція забезпечує постійну якість сигналу навіть для помірно великих сигналів модуляції.

Динаміка хаосу не повинна бути спектрально відокремлена від інформаційного сигналу для роботи нелінійного фільтра. Зокрема, припущенням у виведенні фільтра є те, що інформаційний сигнал повільно змінюється відносно постійної часу, що міститься в першій постійній фільтру, однак ця вимога не обмежує спектральний вміст хаосу. Тому при правильному виборі динаміки інформаційний сигнал і хаос можуть значно перекриватися, тим самим підвищуючи аспекти безпеки системи зв'язку.

3 РЕАЛІЗАЦІЯ ТА ТЕСТУВАННЯ СИСТЕМИ ШИФРУВАННЯ АНАЛОГОВОГО ВІДЕОСИГНАЛУ НА ОСНОВІ МЕТОДА ХАОТИЧНОГО КОДУВАННЯ

3.1 Розробка схеми шифратора та дешифратора

Схема хаотичного скремблера відеосигналу була побудована з використанням стандартних комерційно доступних компонентів.

Детальна схема хаотичного скремблера показана на рис. 3.1. Значення компонентів було підібрано таким чином, щоб отримати хаотичні коливання з широким спектром, який перекриває смугу пропускання 4,5 МГц базового відеосигналу NTSC. Аналогове відео надходить на скремблер через роз'єм X1.

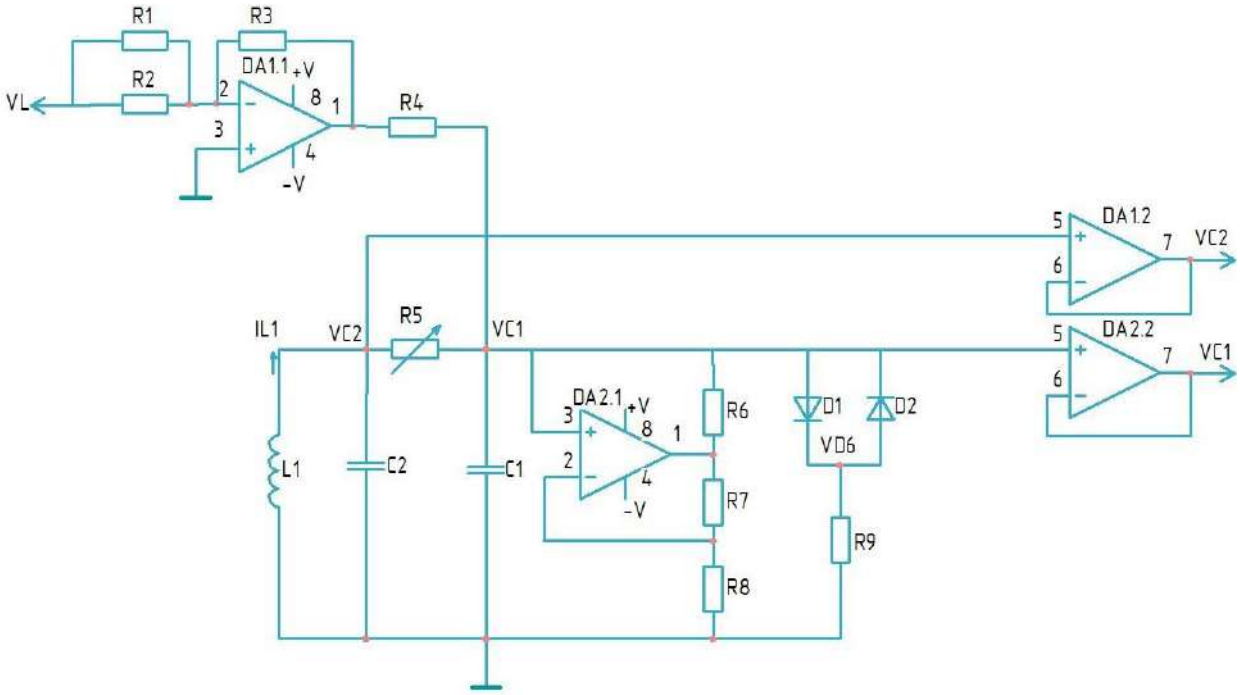

Рисунок 3.1 – Схема скремблера

Схема хаотичного дескремблера відеосигналу була побудована з використанням стандартних комерційно доступних компонентів. Детальна схема дескремблера показана на рисунку 3.2.

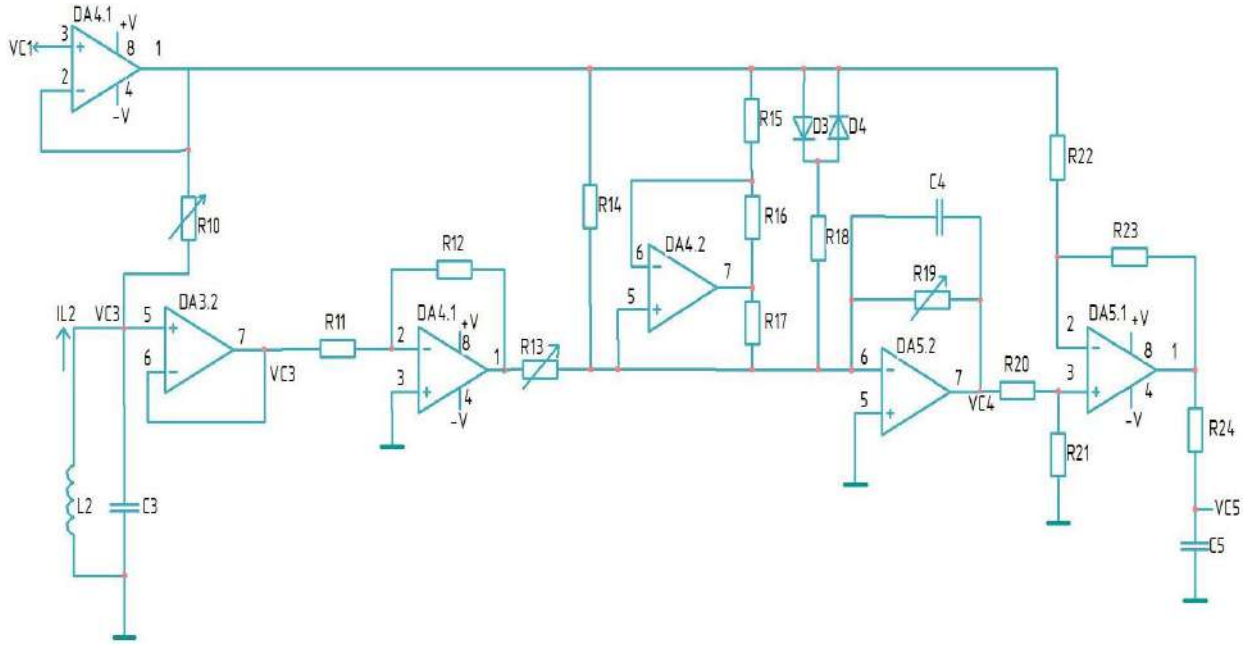

Рисунок 3.2 – Схема дескремблера

На практиці R5 регулюється для отримання відповідної форми хаотичної несучої; отже R5, реалізується в схемі за допомогою потенціометра. Таким чином, подібні потенціометри використовуються для R10, R13 та R19. Ці три потенціометри дозволяють налаштувати приймач для отримання оптимальної якості вихідного відео та забезпечують можливість компенсувати, до певної міри, неточності в інших узгоджених компонентах схеми. Зручні номінали резисторів вибираються для узгоджених пар R11=R12, R20=R21 і R22=R23, а постійна часу R24C5 вибирається для встановлення параметра фільтра g_f

В таблиці 3.1 наведено номінали елементів схеми для реалізації системи зв’язку. Значення всіх компонентів у цій таблиці вказані як номінальні, а всі резистори мають номінальне відхилення 5%. Конкретні операційні підсилювачі та діоди, зазначені в цій таблиці, не є критичними, їх можна замінити аналогічними пристроями.

Для цих значень компонентів схему було налаштовано для отримання відповідної хаотичної несучої з R5=1,315 кОм

Таблиця 3.1 – Значення номіналів компонентів схеми

Компонент	Номінальне значення
L1, L2	1,8мГн
C1,C4	0,001 мкФ
C2, C3	0,01 мкФ
C5	0,1 мкФ
R1,R2,R20,R21	10 кОм
R3,R4,R11, R12, R14, R22, R23	12кОм
R5, R10, R13, R19	5 кОм (змінний)
R6,R7,R16,R17	220 Ом
R8,R15	750 Ом
R9,R18	1,2 кОм
R24	3,3 кОм
DA1…DA5	LMH6723
VD1…VD4	1N914

В якості операційного підсилювача застосовано мікросхему LMH6723. Схема підключення LMH6723 зображена на рисунку 3.3.

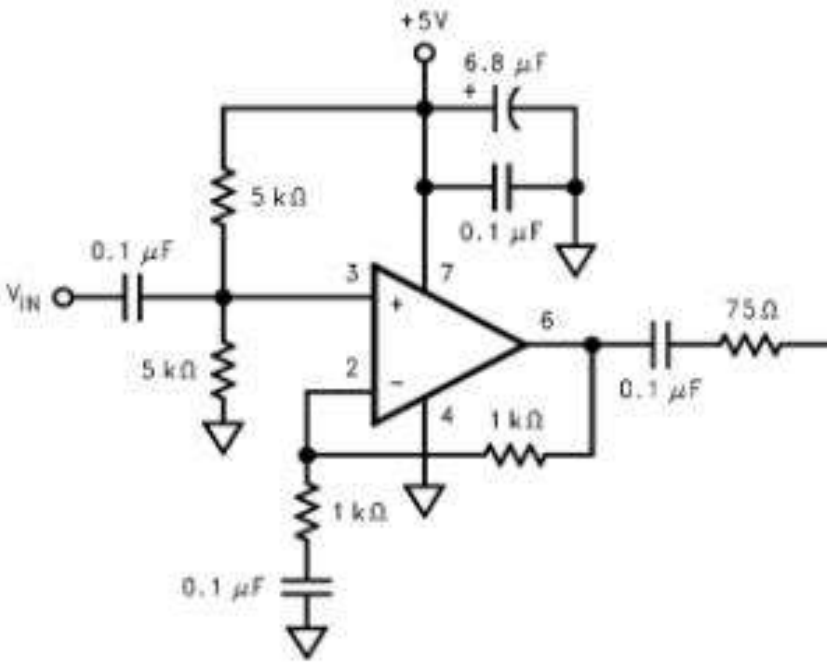

Рисунок 3.3 - Схема підключення мікросхеми LMH6723 згідно документації

LMH6723 - це високошвидкісний операційний підсилювач, який зазвичай використовується в вимірювальних системах, швидкісних драйверах, а також у високочастотних приладах.

LMH6723 може бути застосований у вимірювальних системах, які вимагають високої швидкості передачі даних і точності у вимірюваннях. Також він може використовуватися для підсилення слабких сигналів у високочастотних пристроях, таких як високочастотні комунікаційні системи або радіоприймачі.

Цей операційний підсилювач має широкосмугову характеристику і високу швидкодію, що робить його корисним для застосувань, де потрібна обробка високочастотного сигналу з високою точністю.

Підсилювач може працювати в діапазоні номінальних напруг живлення від 4,5 В до 12 В і споживає лише 1 мА струму спокою при напрузі живлення 10 В (зазвичай ±5 В). LMH6723 не мають внутрішньої точки заземлення, тому однакові конфігурації з одним або двома джерелами живлення є однаково корисними.

Вибір резистора зворотного зв'язку

Однією з ключових переваг операційного підсилювача зі зворотним зв'язком за струмом є можливість підтримувати оптимальну частотну характеристику незалежно від коефіцієнта підсилення, використовуючи відповідні значення резистора зворотного зв'язку (R_F). Електричні характеристики та графіки типових характеристик були згенеровані з резистором зворотного зв'язку 1200 Ом, коефіцієнтом підсилення +2 В/В і живленням ±5 В або ±2,5 В (рис. 3.7).

Як правило, зниження R_F від рекомендованого значення призводить до піку частотної характеристики і розширення смуги пропускання частотної характеристики і розширить смугу пропускання; однак збільшення значення R_F призведе до того, що частотна характеристику швидше спадатиме. Зменшення значення R_F занадто сильно нижче рекомендованого значення призведе до перерегулювання, дзвін і, зрештою, коливання.

На рисунку 3.7 показано частотну характеристику LMH6723 при зміні радіочастоти (R_L = 100 Ом, A_V = +2). Цей графік показує, що при R_F 800 Ом спостерігається пік. Значення R_F 1200 Ом дає майже максимальну смугу пропускання і рівність коефіцієнта підсилення з хорошою стабільністю.

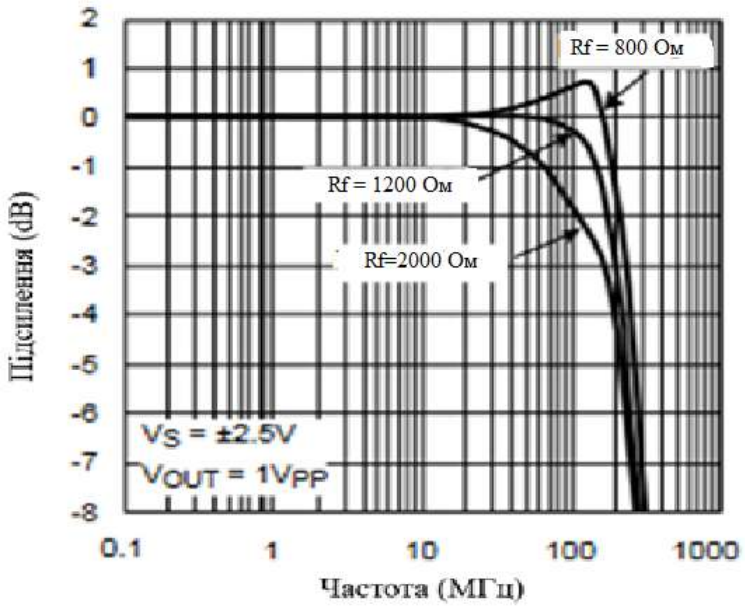

Рисунок 3.4 - Частотна характеристика в залежності від радіочастоти

Оскільки кожне застосування дещо відрізняється, варто поекспериментувати, щоб знайти оптимальний R_F для даної схеми. Загалом, значення R_F, яке дає ~0,1 дБ піку, є найкращим компромісом між стабільністю і максимальною смугою пропускання.

Не можна використовувати підсилювач зі зворотним зв'язком за струмом з виходом, замкненим безпосередньо до інвертуючого входу. Буферна конфігурація LMH6723 вимагає резистора зворотного зв'язку на 2000 Ом для стабільної роботи. Для інших коефіцієнтів підсилення див. графіки на рис.3.5-3.6. Ці діаграми забезпечують гарне місце для початку при виборі найкращого значення резистора зворотного зв'язку для різних значень коефіцієнта підсилення.

LMH6723 розроблений для оптимальної роботи при коефіцієнтах підсилення від +1 до +5 В/В і від -1 до -4 В/В. Конфігурації з вищим

коефіцієнтом підсилення все ще корисні; однак, смуга пропускання буде падатиме зі збільшенням коефіцієнта підсилення, подібно до типового підсилювача зі зворотним зв'язком за напругою.

На рисунку 6 і рисунку 7 показано залежність ВЧ від коефіцієнта підсилення.

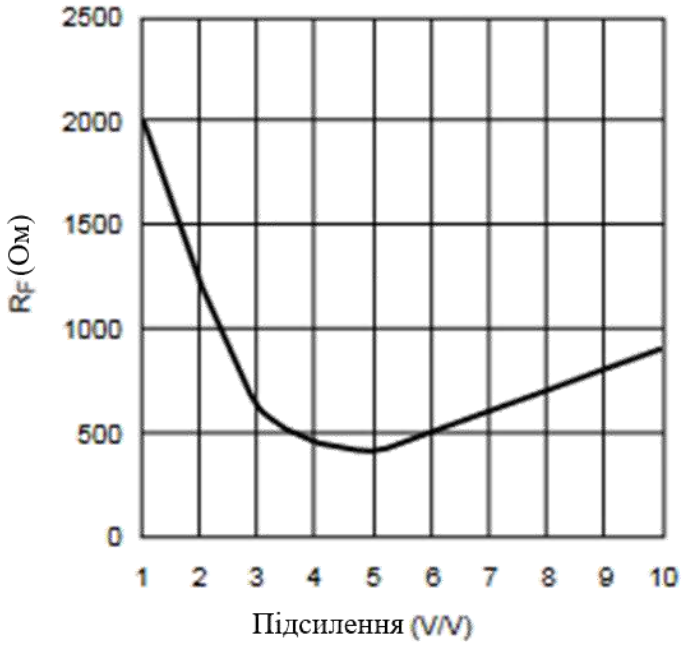

Рисунок 3.5 - R_F та неінвертуючий коефіцієнт підсилення

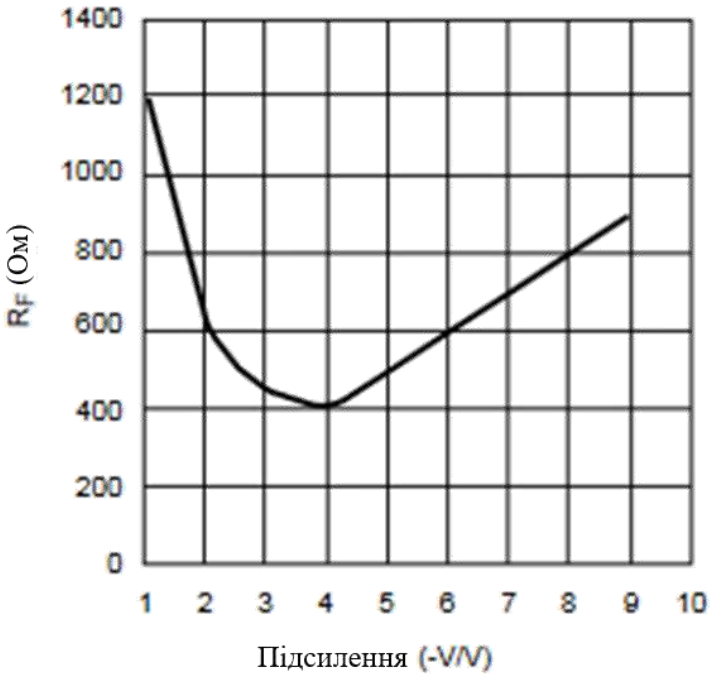

Рисунок 3.6 - R_F та інвертуючий коефіцієнт підсилення

Для того, щоб утримати R_F від зниження нижче опору інвертуючого входу, потрібен вищий R_F при вищому коефіцієнті підсилення щоб не зменшувався занадто сильно нижче вхідного опору інвертуючого входу. Це обмеження застосовується як до інвертуючих так і до неінвертуючих конфігурацій.

Для LMH6723 вхідний опір інвертуючого входу становить приблизно 500 Ом, а 100 Ом є практичною нижньою межею для R_G. LMH6723 починає працювати в режимі з обмеженою смугою пропускання в області, де для отримання більшого коефіцієнта підсилення необхідно збільшити частоту.

Зверніть увагу, що підсилювач працюватиме зі значеннями R_G значно нижче 100 Ом; проте результати будуть істотно відрізнятися від прогнозованих ідеальними моделями.

При використанні LMH6723 в якості фільтра нижніх частот значення R_F може бути істотно зменшено від значення, рекомендованого на графіках залежності частоти від коефіцієнта підсилення. Перевагою зменшення R_F є збільшення коефіцієнта підсилення на більш високих частотах, що покращує загасання в смузі зупинки.

Проблем зі стабільністю можна уникнути, оскільки в смузі зупинки додаткова смуга пропускання пристрою використовується для гасіння вхідного сигналу, а не для його посилення.

Перевага цієї зміни залежить від особливостей схеми. У разі використання фільтра високих частот зменшення R_F ймовірно, призведе до нестабільності пристрою і не рекомендується.

3.2 Розробка конструкції системи шифрування аналогового відеосигналу

Після розробки схеми та її перевірки у ПЗ MultiSim було розроблено конструкцію плат шифратора та дешифратора з метою експерементальної перевірки працездатності методу та схеми. Розробка проводилась в програмному забезпеченні KiCAD.

На рис 3.7 представлена розроблена конструкція схеми скремблера побудована на друкованій платі з розводкою, розрахованою на високочастотну роботу.

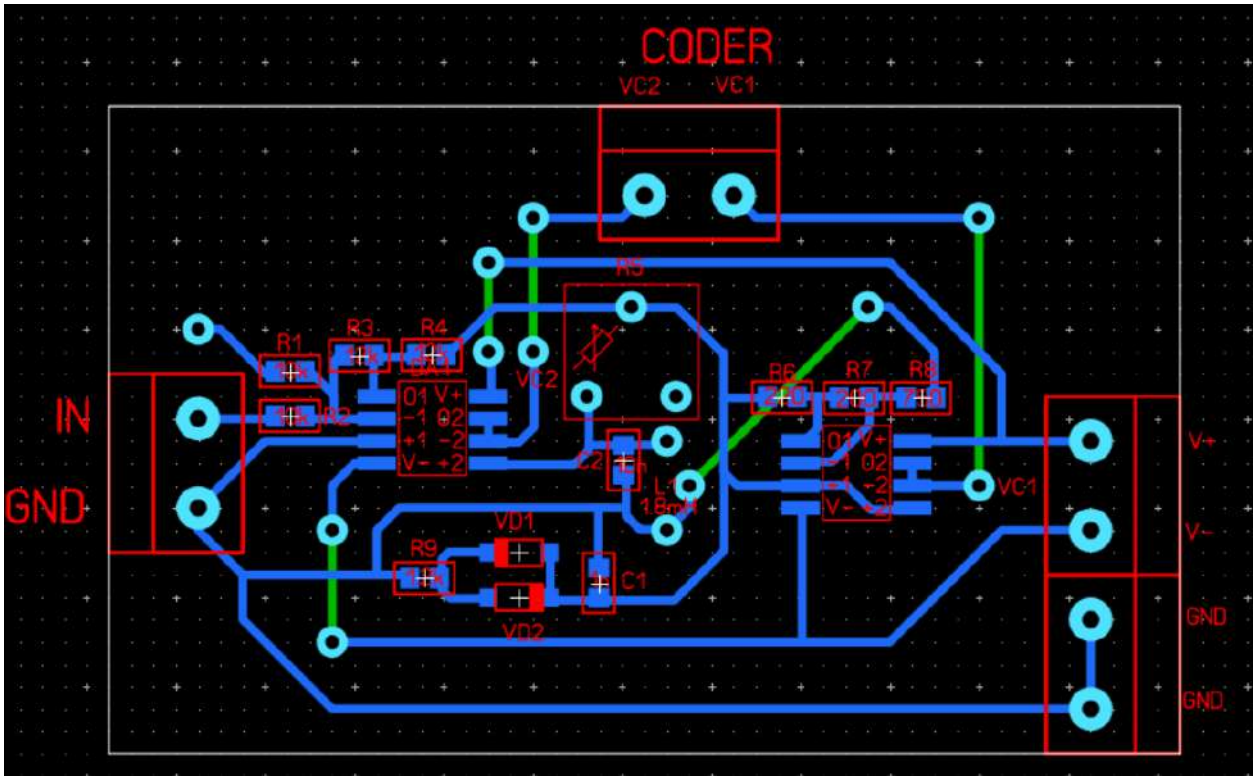

Рисунок 3.7 – Розроблена конструкція друкованої плати хаотичного скремблера

На рис 3.8 представлена розроблена конструкція схеми дескремблера побудована на друкованій платі з розводкою, розрахованою на високочастотну роботу.

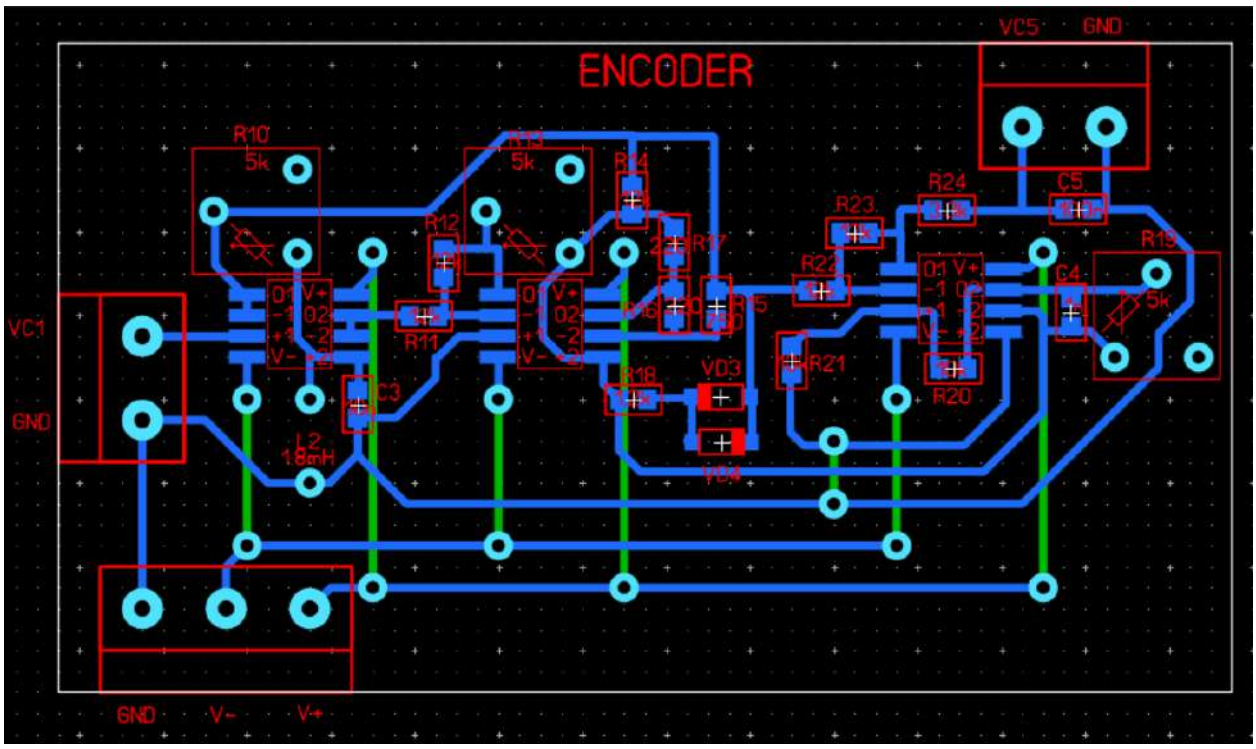

Рисунок 3.8 – Розроблена конструкція друкованої плати хаотичного дескремблера

Для мінімізації паразитного реактивного опору використано поверхневий монтаж і корпусні компоненти. Для забезпечення механічного та електричного екранування, плати рекомендується розміщувати у металевих корпусах. Підключення до ланцюгів здійснюється через коаксіальні прохідні роз'єми, що встановлюються на корпусах. Електричне живлення доступне від будь-якого джерела з напругою від +5 до +12 Вольт постійного струму.

Переваги конструкції:

- нульова затримка між вхідним і вихідним сигналом;

- конструкція Plug and Fly, не потрібно налаштовувати.

- підтримує усі види камер з аналоговим виходом, не потребує приєднання узгоджувального навантаження.

Наступним етапом було виготовлення друкованих плат методом ЛУТ. Отримані плати наведені на рис. 3.9-3.10.

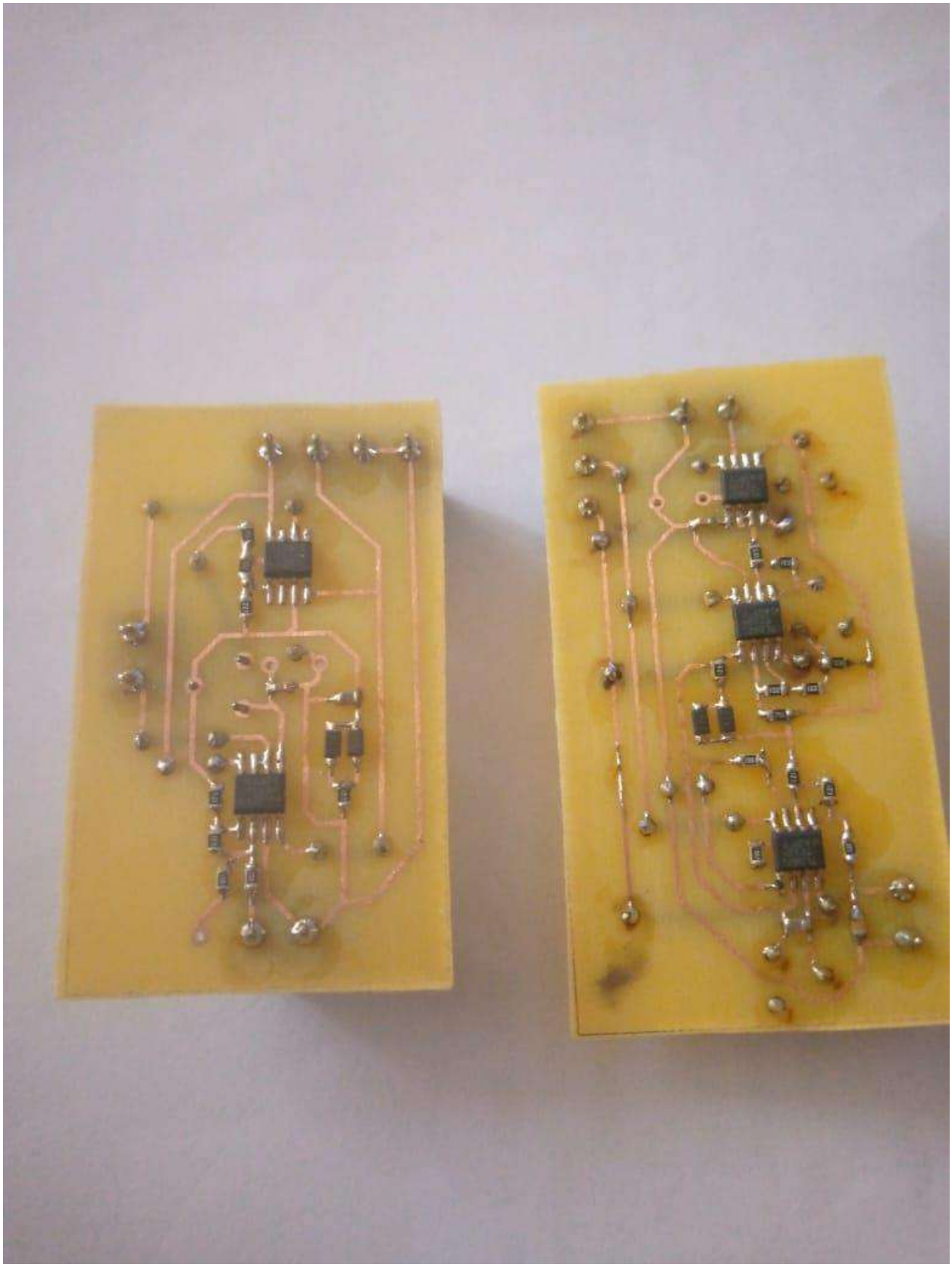

Рисунок 3.9 – Виготовлені плати шифратора та дешифратора (сторона встановлення елементів)

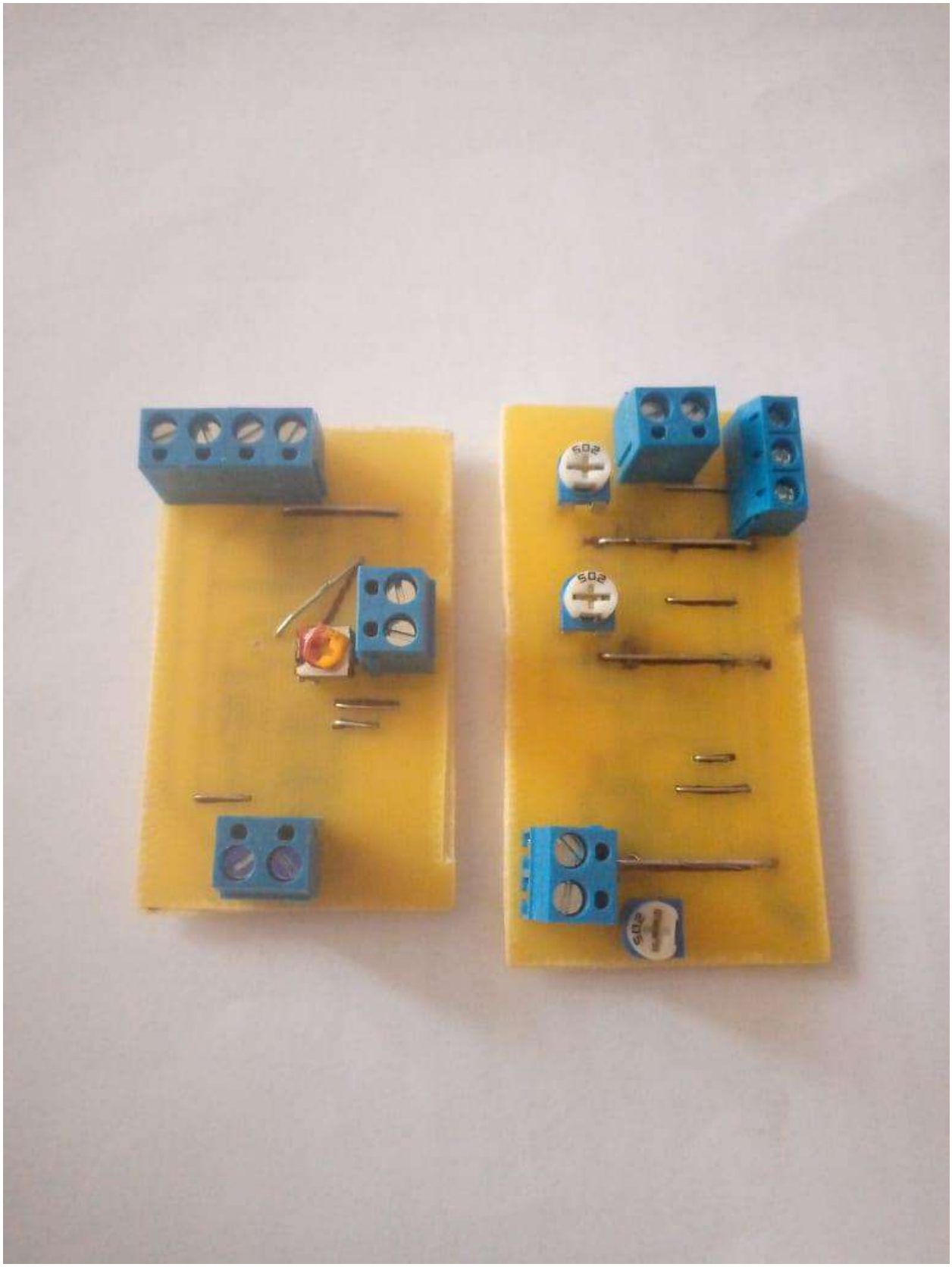

Рисунок 3.10 – Виготовлені плати шифратора та дешифратора (сторона встановлення розємів)

3.3 Тестування розробленої системи шифрування

Після розробки конструкції плати були виготовлені методом ЛУТ (через неможливість ручного виготовлення двошарових плат з метолізацію отворів) та проведено тестування роботи системи шифрування аналогового відео.

Функціональність скремблерної системи була успішно продемонстрована з використанням кольорового відеосигналу від стандартної аналогової відеокамери.

Для тестування використовувались наступні пристрої:

- відеокамера з аналоговим виходом PAL/NTSC RunCam Phoenix 2 SP 1500TVL
- комплект FPV 1.2Ghz Tarot 600mW для передачі відеосигналу (складається з бездротових передавача та приймача аналогових відеосигналів);
- автомонітор LCD 4,3", для камери заднього виду автомобіля (у якості пристрою відображення, що має входи для аналогового відеосигналу);
- розроблені та виготовлені плати шифратора та дешифратора.

Рисунок 3.11 – Відеокамера RunCam Phoenix 2 SP 1500TVL

Рисунок 3.12 – Комплект FPV 1.2Ghz Tarot 600mW

Рисунок 3.13 – Автомонітор LCD 4,3" у якості пристрою відображення

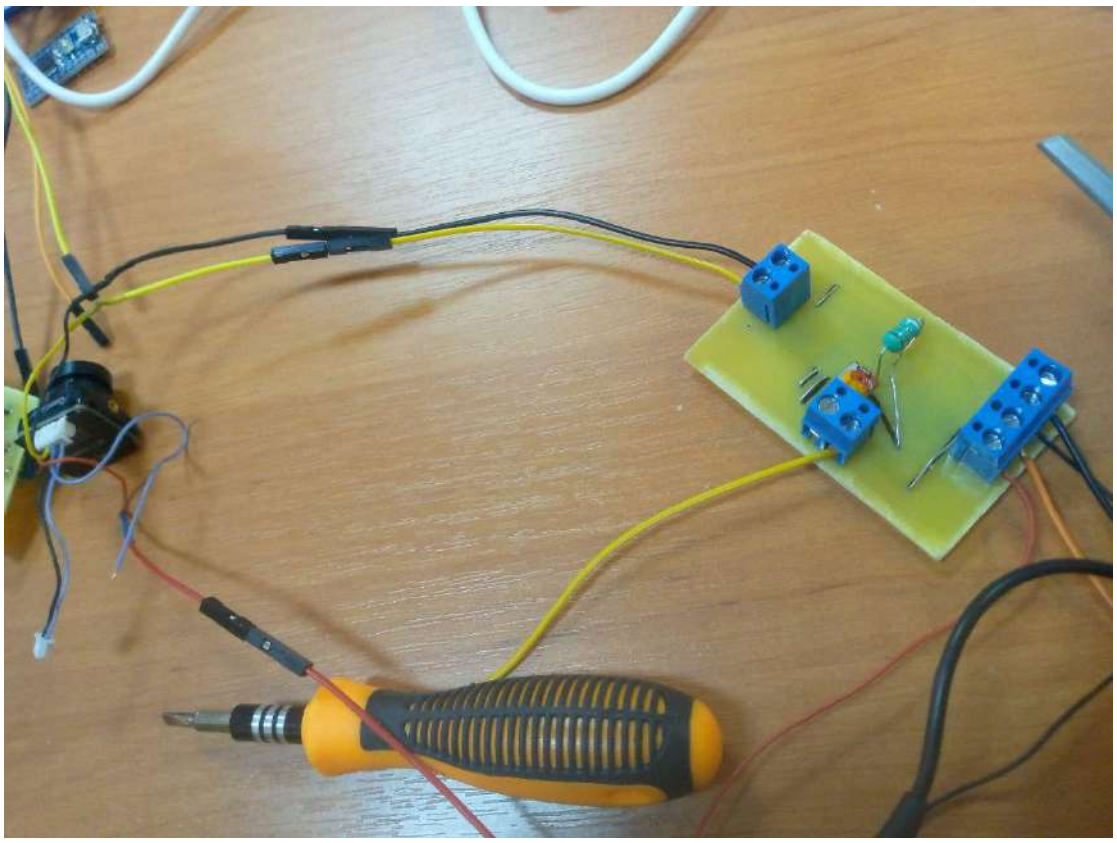

Рисунок 3.14 – Тестування роботи системи бездротової передачі відео з наявним шифруванням розробленим методом (передавальна сторона)

Рисунок 3.15 – Тестування роботи системи бездротової передачі відео з наявним шифруванням розробленим методом (приймальна сторона)

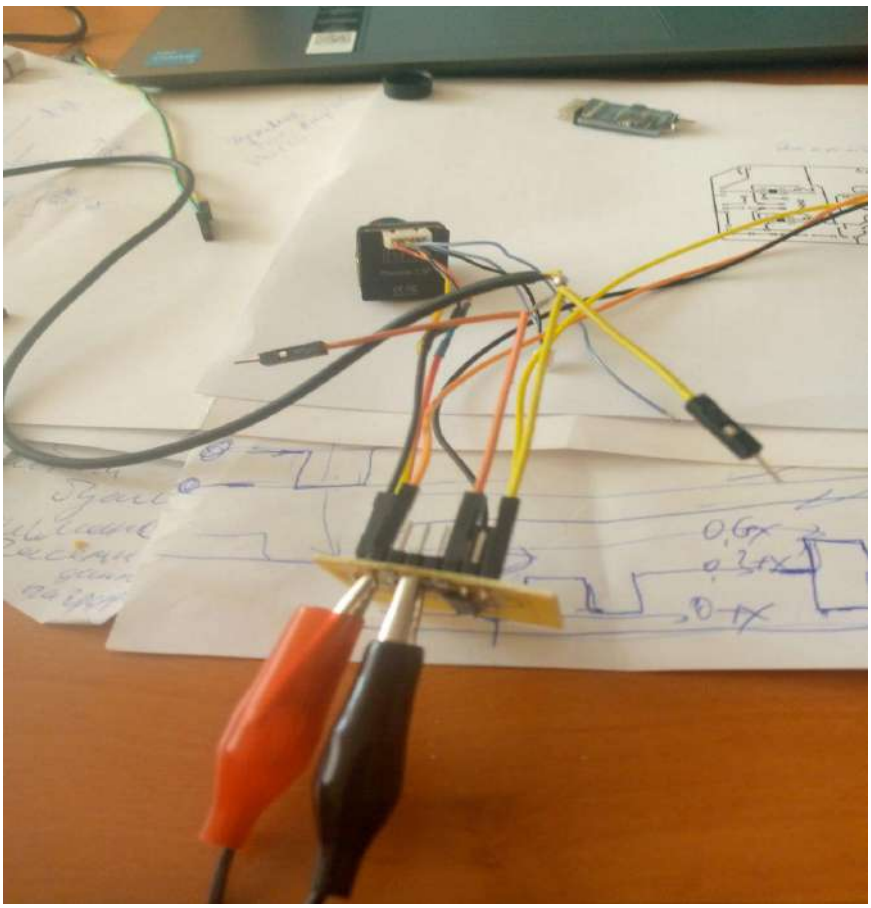

Рисунок 3.16 – Знімання сигналів з розроблених плат

Рисунок 3.17 – Перевірка системи шифрування з використанням бездротової передачі

Типова форма сигналу, що генерується хаотичним скремблером за відсутності вхідного відеосигналу і зафіксована за допомогою цифрового осцилографа, показана на рис.3.18.

Рисунок 3.18 - Осцилограма, знята з виходу хаотичного скремблера на роз'ємі X3 за відсутності вхідного відеосигналу.

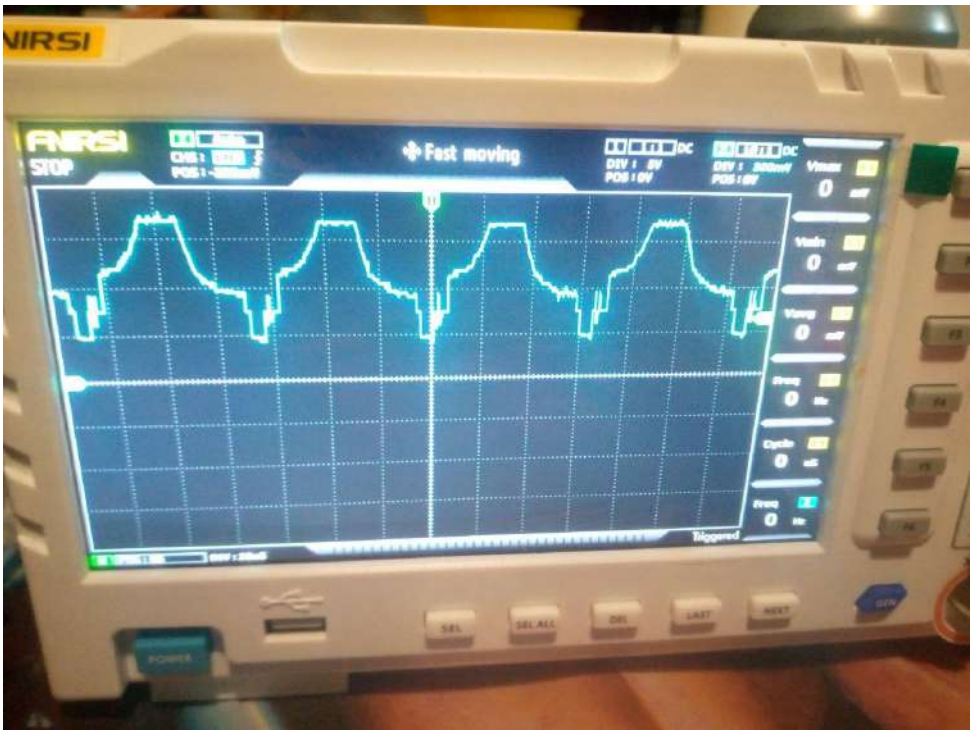

Рисунок 3.19 – Осцилограма вхідного відеосигналу

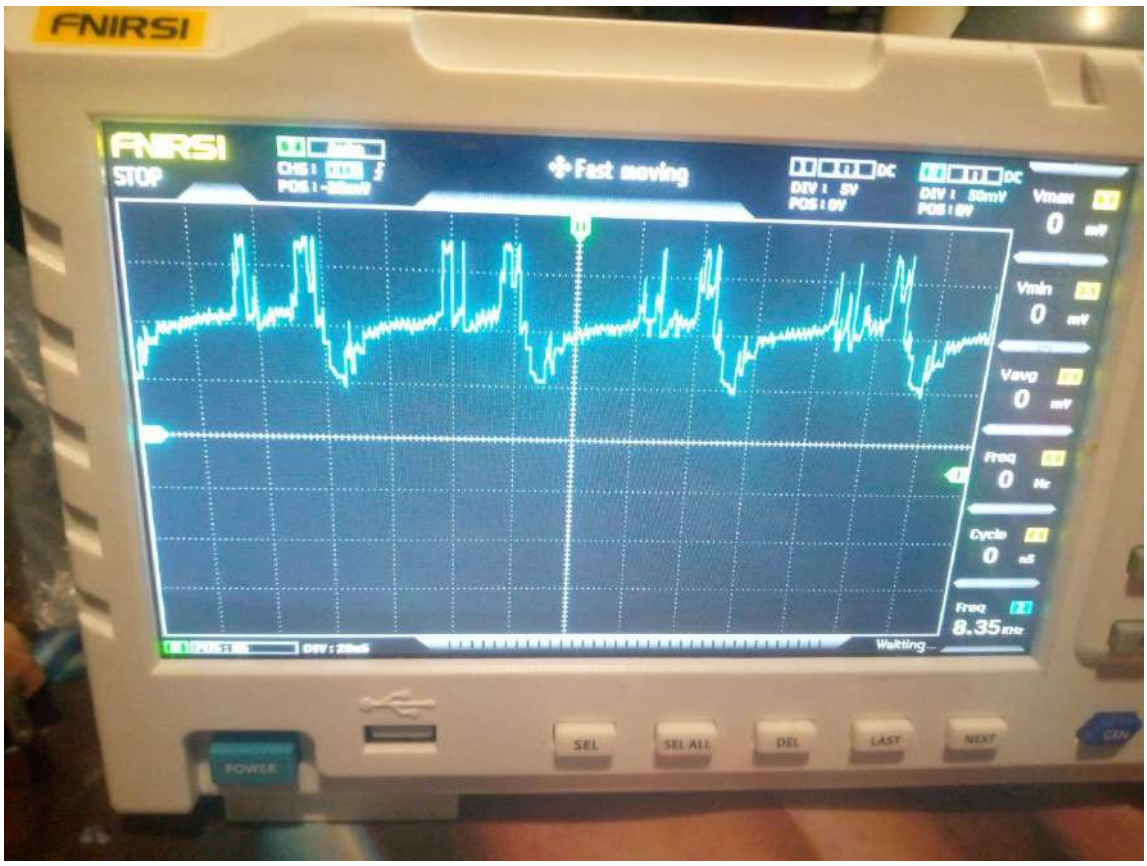

Рисунок 3.20 – Осцилограма шифрованого сигналу

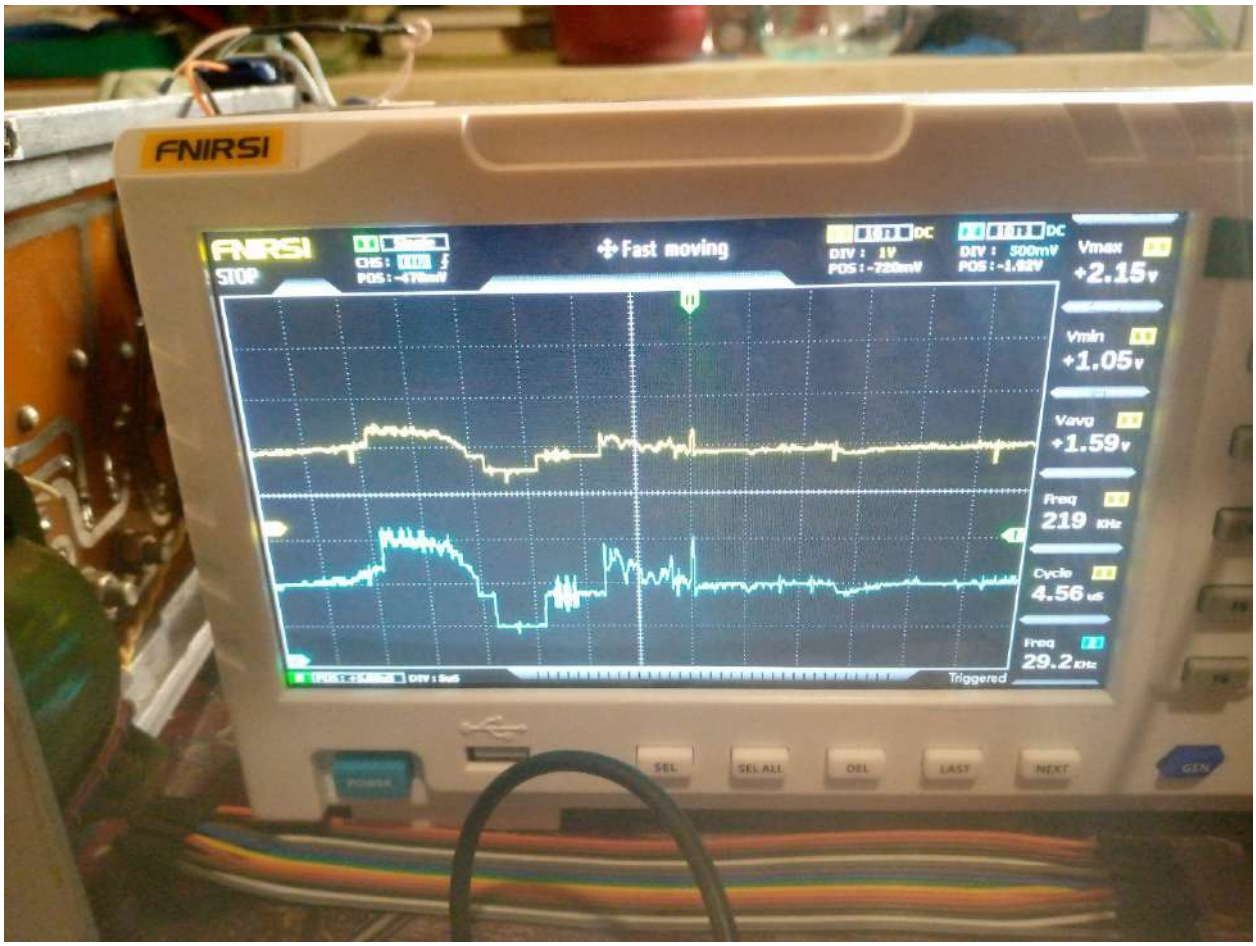

Рисунок 3.21 – Осцилограми початкового та розшифрованого сигналів

Отриманий розшифрований сигнал переглядався в реальному часі на пристрої відображення.

Зашифрований рядок відеосигналу виглядає просто як шум, тим самим заперечуючи будь-яку корисну інформацію для підслуховувача, в той час як дешифрований сигнал відновлює оригінальне зображення.

ВИСНОВКИ

В роботі розроблено алгоритм шифрування відеосигналів на основі хаотичних сигналів та проведено його перевірку шляхом реалізації хаотичного скремблеру та дескремблеру для захисту бездротового аналогового відео. Згідно розробленого алгоритму аналоговий відеосигнал вводиться в хаотичний генератор, а вихідний сигнал передається через стандартний бездротовий радіозв’язок. У приймачі дескремблер відокремлює відео від хаотичного сигналу в реальному часі. Експериментальні результати розробленого та виготовленого на основі алгоритму пристрою шифрування показують, що закодований сигнал ефективно приховує оригінальне відеозображення, але дешифратор відновлює оригінальне кольорове відео з достатньою чіткістю та деталізацією. У порівнянні з цифровим шифруванням використання алгоритму шифрування з використанням хаотичного скремблування пропонує ефективну недорогу альтернативу для маскування критичних за часом аналогових комунікацій.

Перевагою хаотичного скремблювання відеосигналів перед більш складними методами цифрового шифрування є його проста аналогова реалізація яка виключає затримки часу необхідні цифровим методам для перетворень. Запропонований алгоритм та технологія на його основі має високу функціональність, незважаючи на неймовірну простоту схем скремблювання і дескремблювання. Кожен компонент складається з невеликої кількості звичайних аналогових компонентів. Конструктивні та схемотехнічні елементи хаотичної схеми складають "ключ" шифратору. До недоліків можна віднести, що ця інформація може бути вилучена з переданого сигналу без відповідної схеми дескремблювання, але лише за допомогою складних методів нелінійної цифрової обробки сигналів, які вимагають порівняно дорогих технологій оцифрування та обчислень, а також достатньо великого сховища даних і нереальні в умовах реального часу, а відповідно отримання

відеозображення можливе лише постфактум після довгої обробки. Отже цей недолік невелюється при використанні розробленого алгоритму та технології при передаванні бездротового відеосигналу на БПЛА під час польоту.

Асиметрія вартості і складності перехоплення зашифрованої передачі означає, що все ще існує ефективний рівень безпеки, який забезпечується хаотичним шифруванням. Хоча це не справжнє шифрування, воно може забезпечити достатній рівень захисту від підслуховувачів для критично важливих комунікацій.

Розроблений алгоритм та технологія на його основі прокладає шлях до повноцінного використання хаотичного скремблювання у військових цілях, де бюджетні витрати і потужність виключають використання цифрового шифрування. Майбутні розробки з використанням цієї технології включатимуть програмований ключ і покращену стійкість до атак. Одним з підходів може бути використання хаотичних генераторів вищої розмірності. Технологія також може бути масштабована за частотою для використання при ще більшій пропускній здатності інформації.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. Xia Weguo, Cao Jinde, Chaos, 18, 2, 2008.

2. https://uk.wikipedia.org/wiki/Відеосигнал

3. https://ru.wikibrief.org/wiki/Analog_television

4. Nalini Bagal, Shivani Pandita ,“A Review: Real-Time Wireless Audio-Video Transmission”, IJETAE, vol. 5,issue 4, April 2015.

5. Z. He, Y. Liang, L. Chen, I. Ahmad, and D. Wu, “Power-rate-distortion analysis for wireless video communication under energy constraints,” IEEE Transactions on Circuits and Systems for Video Technology, vol. 15, no. 5, pp. 645-658, May 2005.

6. P. Iscold, G. A. S. Pereira, and L. A. B. Torres, “Development of a hand-launched small uav for ground reconnaissance,” Aerospace and Electronic Systems, IEEE Transactions on, 2010. – 348 c

7. C. E. Shannon, “Communication Theory of Secrecy Systems”, The Bell System Technical Journal, vol. 28, no. 4, pp. 656– 715, October 1949.

8. T. Kruger and S. Troubetzkoy, “Complexity, Randomness, Discretization: Some Remarks on a Program of J. Ford”, Physica D, vol. 105, pp. 97–104, 1997.

9. B. V. Chirikov and F. Vivaldi, “An Algorithmic View of Pseudochaos”, Physica, D 129, pp. 223–235, 1999.

10. I. P. Cornfeld, S. V. Fomin, and Ya. G. Sinai, Ergodic Theory. Berlin: Springer, 1982.

11. J. Palis and F. Takens, Hyperbolicity and Sensitive Chaotic Dynamics at Homoclinic Bifurcations. Cambridge: University Press, 1993.

12. S. Banerjee, J. A. Yorke, and C. Grebogi, “Robust Chaos”, Physical Review Letters, vol. 80, no. 14, pp. 3049–3052, 1998.

13. D. Ruelle, Chaotic Evolution and Strange Attractors. Cambridge: University Press, 1989.

14. C. E. Shannon, “A Mathematical Theory of Communication”, The Bell System Technical Journal, vol. 27, no. 3, pp. 379– 423, July 1948.

15. A. A. Brudno, “The Complexity of the Trajectories of a Dynamical System”, Russian Mathematical Surveys, vol. 33, no. 1, pp. 197–198, 1978.

16. J. Ford, “What Is Chaos, That We Should be Mindful of It?”, in The New Physics, P.Davies, ed., Cambridge University Press, 1992.

17. Зайцев С. В. Математична модель оцінки достовірності передачі інформації в безпровідних мережах за умов впливу структурних завад / С.В. Зайцев // Молода наука України. Перспективи та пріоритети розвитку : матеріали XIV Всеукр. наук.- практ. конф. з міжнар. участю, (Київ, 26–27 грудня 2013р.). – К.:, 2014. – С. 174 – 175