Міністерство освіти і науки України
Сумський державний університет
Кафедра електроніки і комп’ютерної техніки

ПОЯСНЮВАЛЬНА ЗАПИСКА

до дипломного проекту

на тему:

«Пристрій захисту інформації на базі стеганографічного алгоритму»

Завідувач кафедри Опанасюк А.С.

Керівник проекту Бережна О. В.

Проектувала студентка Сиромля В. П.

Суми
2020 р.

Сумський державний університет

Факультет ЕлІТ **Кафедра** ЕКТ

Спеціальність 6.172 Телекомунікації та радіотехніка

ЗАТВЕРДЖУЮ**:**
Зав. кафедри Опанасюк А.С.

«___» _____20___ р.

Завдання
на дипломний проект студентові

Сиромлі Валерії Петрівні

(прізвище,ім'я,по батькові)

1. Тема проекту «Пристрій захисту інформації на базі стеганографічного алгоритму»

затверджено наказом по інституту від « 21 » квітня 2020 р. № 0544 - III

2. Термін здачі студентом закінченого проекту 05.06.2020

3. Вихідні дані до проекту: Тип стеганографічного алгоритму - вбудовування цифрових водяних знаків. Тип стеганографічного контейнеру – зображення. Розробити структурну та функціональну схеми пристрою.

4. Зміст розрахунково-пояснювальної записки (перелік питань, які підлягають розробці): 1. Аналітичний огляд методів стеганографії та створення водяних знаків; 2. Дослідження параметрів стеганоканалу; 3. Розробка структурних схем стеганографічної системи передачі даних; 4. Розробка структурної схеми пристрою захисту інформації на базі стеганографічного алгоритму; 5. Розробка схеми електричної функціональної пристрою вбудовування цифрового водяного знаку.

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень): 1. Схема електрична структурна стеганосистеми;

2. Схема електрична структурна стеганосистеми на базі протоколу RTP;

3. Схема електрична структурна стеганоканалу зв'язку;

4. Схема електрична структурна пристрою вбудовування цифрового водяного знаку;

5. Схема електрична функціональна пристрою вбудовування цифрового водяного знаку

Календарний план

№ п/п	Найменування етапів дипломного проекту (роботи)	Термін виконання етапів проекту (роботи)	Примітка
1	Затвердження теми та завдання бакалаврської роботи	21.04.20	
2	Огляд літератури та постановка завдання	30.04.20	
3	Дослідження прихованої пропускної здатності стеганографічного каналу передачі даних	07.05.20	
4	Розробка структурних схем стеганографічної системи передачі даних	14.05.20	
5	Розробка структурної схеми пристрою захисту інформації на базі стеганографічного алгоритму вбудовування цифрового водяного знаку	21.05.20	
6	Розробка схеми електричної функціональної пристрою вбудовування цифрового водяного знаку	28.05.20	
7	Оформлення пояснювальної записки, креслень	02.06.20	
8	Підготовка до захисту	05.06.20	

Студент-дипломник Сиромля В. П.

Керівник проекту Бережна О. В.

«____» _____ 20___ р.

РЕФЕРАТ

Пояснювальна записка містить: 58 аркушів, 18 рисунків, 2 таблиці.

Графічна частина роботи включає в себе: схеми електричні структурні стеганосистеми, стеганоканалу зв'язку, стеганосистеми на базі протоколу RTP та пристрою вбудовування цифрового водяного знаку, схему електричну функціональну пристрою.

Пояснювальна записка містить п'ять розділів: огляд літератури і постановку завдання проектування, дослідження прихованої пропускної здатності стеганоканалу, розробку структурних схем стеганографічної системи передачі даних, розробку структурної схеми пристрою захисту інформації на базі стеганографічного алгоритму, розробку схеми електричної функціональної пристрою.

Перший розділ містить розгляд проблеми забезпечення автентичності зображення, аналітичний огляд методів стеганографії, вибір на користь використання методу цифрових водяних знаків, варіації способів нанесення яких також описані в розділі, а також постановку завдання на проектування.

Другий розділ присвячений дослідженню прихованої пропускної здатності стеганографічного каналу передачі даних.

Третій розділ присвячений розробці структурних схем стеганографічної системи передачі даних.

Четвертий розділ присвячений розробці структурної схеми пристрою захисту інформації на базі стеганографічного алгоритму вбудовування цифрового водяного знаку.

П'ятий розділ присвячений розробці схеми електричної функціональної пристрою вбудовування цифрового водяного знаку.

ЗМІСТ

ВСТУП

Мультимедійний простір в сучасному світі представлено переважно цифровими форматами. Однак поширення інформації в інтернеті призводить до формування важливої проблеми: порушення авторського права стає неконтрольованим процесом. Захист цифрових даних, а також перевірку їх на оригінальність забезпечують нові розробки в області криптографії та стеганографії. Криптографія приховує вміст файлів шляхом шифрування. В стеганографії ж приховується сам факт існування прихованої інформації у файлі. "Можна виділити кілька причин популярності досліджень в області стеганографії в даний час: обмеження на використання криптозасобів в ряді країн світу і поява проблеми захисту прав власності на інформацію, яка представлена в цифровому вигляді. Перша причина викликала велику кількість досліджень у стилі класичної стеганографії (тобто приховування факту передачі інформації), друга причина - ще більш численні роботи в області цифрових водяних знаків. Цифровий водяний знак (ЦВЗ) - спеціальна мітка, яка приховано впроваджується в зображення або інший сигнал з метою тим чи іншим способом контролювати його використання" [8].

Актуальність роботи безпосередньо пов'язана зі зростанням потреби передачі прихованої інформації в загальнодоступних каналах зв'язку, так як стеганографічні системи дозволяють здійснити впровадження інформації у файл-контейнер без залучення уваги третіх сторін. Основними замовниками на системи впровадження цифрових водяних знаків в зображення є сучасні інтерактивні бібліотечні фонди, галереї образотворчого мистецтва, фотографи, ЗМІ, спецслужби та інші організації. Актуальність підтверджується необхідністю кожного окремого творця зображення відзначити авторське право на свій продукт, що розповсюджується в загальнодоступних мережах.

Метою роботи є розробка математичної моделі, алгоритму, а також пристрою, що здійснює впровадження та зчитування водяних знаків для забезпечення автентичності зображень.

1 ОГЛЯД ЛІТЕРАТУРИ

1.1 Проблеми забезпечення автентичності зображень

Для цифрових зображень, які знаходяться у вільному доступі, необхідний якийсь цифровий підпис, за допомогою якого автор зміг би контролювати публікації своїх робіт. В якості такої інформації може виступати текст або цифрове зображення, що розміщується в довільній області зображення. Мета даного знаку – однозначно ідентифікувати особу автора. "Вбудовування в цифрові фотографії невидимих міток, в якості яких можуть виступати послідовності символів або графічні зображення, є одним з поширених способів захисту інформаційного змісту фотографій.

Такі мітки були названі цифровими водяними знаками (ЦВЗ) за аналогією з широко відомим способом захисту цінних паперів від підробок. Метод захисту графічної інформації за допомогою ЦВЗ є складовою частиною цифрової стеганографії, науки про непомітне приховування одних даних в інших.

Впроваджуваний в захищену фотографію ЦВЗ повинен відповідати двом суперечливим критеріям: робастності (стійкості до різних зовнішніх впливів) і скритності (забезпечення найменших спотворень зображення в порівнянні з оригіналом). Для перевірки авторських прав на цифрове зображення здійснюють витягування вбудованої інформації" [7].

1.2 Методи стеганографії та створення водяних знаків

1.2.1 Напрямки цифрової стеганографії

Цифрова стеганографія як наука народилася буквально в останні роки. Вона включає наступні напрямки:

- вбудовування інформації з метою приховування факту передачі;
- вбудовування цифрових водяних знаків (ЦВЗ);
- вбудовування ідентифікаційних номерів;
- вбудовування заголовків (captioning) [8].

ЦВЗ можуть застосовуватися в основному для захисту від копіювання і несанкціонованого використання. У зв'язку з бурхливим розвитком технологій мультимедіа гостро постало питання захисту авторських прав та інтелектуальної власності у цифровому вигляді. Прикладами можуть бути фотографії, аудіо- та відеозаписи і так далі. Переваги, які дають представлення і передача повідомлень в цифровому вигляді, можуть виявитися перекреслені легкістю, з якою можливе їх крадіжка або модифікація. Тому розробляються різні заходи захисту інформації організаційного і технічного характеру. Один з найбільш ефективних технічних засобів захисту мультимедійної інформації і полягає у вбудовуванні в об'єкт, що захищається, невидимих міток ЦВЗ. Розробки в цій галузі ведуть найбільші фірми в усьому світі. Так як методи ЦВЗ почали розроблятися зовсім недавно, то тут є багато неясних проблем, що вимагають свого вирішення.

Назву цей метод отримав від всім відомого способу захисту цінних паперів, в тому числі і грошей, від підробки. Термін «digital watermarking» був вперше застосований у роботі [6]. На відміну від звичайних водяних знаків ЦВЗ можуть бути не тільки видимими, але і (як правило) невидимими. Невидимі ЦВЗ аналізуються спеціальним декодером, який виносить рішення про їх коректність. ЦВЗ можуть містити деякий автентичний код, інформацію про власника або яку-небудь керуючу інформацію. Найбільш придатними об'єктами захисту за допомогою ЦВЗ є нерухомі зображення, файли аудіо-та відеоданих.

Вбудовування заголовків (невидиме) може застосовуватися, наприклад, для підпису медичних знімків, нанесення легенди на карту та в інших випадках. Метою є зберігання різнорідно представленої інформації в єдиному цілому. Це, мабуть, єдиний додаток стеганографії, де в явному вигляді відсутній потенційний порушник.

Так як цифрова стеганографія є молодою наукою, то її термінологія не до кінця устоялася. Основні поняття були узгоджені на першій міжнародный конференції з приховування даних [12]. Тим не менше навіть саме поняття «стеганографія» трактується по-різному. Так, деякі дослідники розуміють під стеганографією тільки приховану передачу інформації. Інші відносять до стеганографії такі додатки, як, наприклад, метеорний радіозв'язок, радіозв'язок з псевдовипадковою перебудовою радіочастоти, широкосмуговий радіозв'язок.

Неформальне визначення того, що таке цифрова стеганографія, могло б виглядати наступним чином: «Наука про непомітне і надійне приховування одних бітових послідовностей в інших, що мають аналогову природу» Під це визначення якраз підпадають всі чотири вищенаведених напрямки приховування даних, а радіозв'язку немає. Крім того, у визначенні міститься дві основні вимоги до стеганографічного перетворення: надійність, тобто стійкість до різного роду спотворень. Згадка про аналогову природу цифрових даних підкреслює той факт, що вбудовування інформації проводиться в оцифровані безперервні сигнали. Таким чином, в рамках цифрової стеганографії не розглядаються питання впровадження даних в заголовки IP-пакетів і файлів різних форматів, в текстові повідомлення.

Як би не відрізнялись напрямки стеганографії, вимоги, що пред'являються ними, багато в чому збігаються, що буде показано далі. Найбільш істотна відмінність постановки завдання прихованої передачі даних від постановки завдання вбудовування ЦВЗ полягає в тому, що в першому випадку порушник повинен виявити приховане повідомлення, тоді як у другому випадку про його існування всі знають. Більше того, у порушника на законних підставах може бути пристрій виявлення ЦВЗ (наприклад, у складі DVD-програвача).

Слово «непомітним» в нашому визначенні цифрової стеганографії мається на увазі обов'язкове включення людини в систему стеганографічної передачі даних. Людина тут може розглядатися як додатковий приймач даних, що пред'являє до системи передачі досить важко формульовані вимоги.

1.2.2 Класифікація методів приховування інформації

Одними з найпоширеніших типів контейнерів в комп'ютерній стеганографії на даний момент є зображення, аудіодані, представлені в цифровій формі, та відеопослідовності. Це пояснюється тим, що подібні контейнери мають шумову складову, обумовлену їх утворенням, яка здатна замаскувати вбудоване повідомлення.

Всі методи, призначені для приховування даних, можна розділити за принципами, що лежать в їх основі:

– форматні методи приховування - це такі методи, які ґрунтуються на особливостях формату зберігання графічних даних. Розробка таких методів зводиться до аналізу формату з метою пошуку полів формату, зміна яких в конкретних умовах не позначиться на роботі з графічним зображенням;

– неформатні методи - це методи, що використовують безпосередньо самі дані, якими зображення представлено в цьому форматі. Застосування неформатних методів неминуче призводить до появи спотворень, що вносяться стеганографічною системою, однак при цьому вони є більш стійкими до атак як пасивних, так і активних супротивників.

Розглянемо класифікацію методів більш докладно.

Неформатні методи приховування:

– неформатні методи приховування в JPEG:
  1) метод приховування у вихідних даних зображення;
  2) метод приховування з використанням таблиць квантування;
  3) метод використання хибних таблиць квантування;
  4) метод приховування в спектрі зображення після квантування;
– методи приховування в графічних зображеннях з палітрою кольорів;
– метод приховування з використанням молодших бітів даних зображення;
– метод приховування з використанням молодших бітів елементів палітри;
– метод приховування, заснований на наявності однакових елементів палітри;
– метод приховування шляхом перестановки елементів палітри.

Форматні методи приховування в графічних зображеннях:

– форматні методи приховування у файлах BMP;
– форматні методи приховування в JPEG:
  1) дописування даних в кінець JPEG файлу;
  2) метод приховування в непрямих даних;
  3) метод приховування з використанням маркерів коментарів;
  4) метод приховування з використанням зменшеного зображення [8].

1.2.3 Класифікація стеганографічних систем на основі цифрових водяних знаків

Залежно від того, яка інформація потрібна детектору для виявлення ЦВЗ, стегосистеми ЦВЗ діляться на три класи: відкриті, напівзакриті і закриті. Ця класифікація наведена в табл. 1.1.

Таблиця 1.1 – Класифікація стегосистем на основі ЦВЗ

Вид стегосистеми цифрових водяних знаків		Вхідні дані, необхідні для детектування		Вихідні дані детектора	
		Вихідний сигнал	Вихідний ЦВЗ	Так/Ні	ЦВЗ
Закриті	Тип I	+	+	+	-
	Тип II	+	-	-	+
Напівзакриті		-	+	+	-
Відкриті		-	-	-	+

Найбільше застосування можуть мати відкриті стегосистеми ЦВЗ, які аналогічні системам прихованої передачі даних. Найбільшу стійкість по відношенню до зовнішніх впливів мають закриті стегосистеми I типу.

Розглянемо докладніше поняття «контейнера». До стегокодера - це пустий контейнер, після нього - заповнений контейнер, або стего. Стего повинно візуально відрізнятися від порожнього контейнера. Розрізняють два основних типи контейнерів: потоковий і фіксований.

Потоковий контейнер являє собою безперервно слідуючу по-послідовність біт. Повідомлення вкладається в нього в реальному масштабі часу, так що в кодері невідомо заздалегідь, чи вистачить розмірів контейнера для передачі всього повідомлення. В один контейнер великого розміру може бути вбудовано і кілька повідомлень. Інтервали між вбудованими бітами визначаються генератором псевдовипадкової послідовності з рівномірним розподілом інтервалів між відліками. Основна складність полягає у здійсненні синхронізації, визначенні початку та кінця послідовності. Якщо в даних

контейнера є біти синхронізації, заголовки пакетів і т. д., то прихована інформація може йти відразу після них. Складність забезпечення синхронізації перетворюється в перевагу з точки зору забезпечення скритності передачі. Крім того, потоковий контейнер має велике практичне значення: уявіть собі, наприклад, стегоприставку до звичайного телефону. Під прикриттям звичайної, незначної телефонної розмови можна було б передавати іншу розмову, дані і т. п., а не знаючи секретного ключа, не можна було б не тільки дізнатися зміст прихованої передачі, а й сам факт її існування. Не випадково, що відкритих робіт, присвячених розробці стегосистем з потоковим контейнером, практично не зустрічається.

У фіксованого контейнера розміри і характеристики заздалегідь відомі. Це дозволяє здійснювати вкладення даних оптимальним в деякому сенсі чином. Ми будемо розглядати в основному фіксовані контейнери (далі - контейнери).

Контейнер може бути вибраним, випадковим або нав'язаним. Вибраний контейнер залежить від вбудовуваного повідомлення, а в граничному випадку є його функцією. Цей тип контейнера більше характерний для стеганографії. Нав'язаний контейнер може з'явитися в сценарії, коли особа, яка надає контейнер, підозрює про можливе приховане листування і бажає запобігти їй. На практиці ж найчастіше стикаються з випадковим контейнером.

Вбудовування повідомлення в контейнер може проводитися за допомогою ключа - одного або декількох. Ключ - псевдовипадкова послідовність (ПВП) біт, породжувана генератором, що задовольняє визначеним вимогам (криптографічно безпечний генератор). В якості основи генератора може використовуватися, наприклад, регістр зсуву з лінійним зворотним зв'язком. Тоді адресатам для забезпечення зв'язку може повідомлятися початкове заповнення цього регістра. Числа, породжувані генератором ПВП, можуть визначати позиції модифікованих відліків у разі фіксованого контейнера або інтервали між ними в разі потокового контейнера. Треба відзначити, що метод випадкового вибору величини інтервалу між вбудованими бітами не особливо хороший. Причин - дві. По-перше, приховані дані повинні бути розподілені по всьому зображенню. Тому рівномірний розподіл довжин (від найменшого до найбільшого) може бути досягнутий лише наближено: потрібно бути впевненим в тому, що все повідомлення

вбудовано, тобто «помістилося» в контейнер. По-друге, довжини інтервалів між відліками шуму розподілені не за рівномірним, а за експоненціальним законом. Генератор же ПВП з експоненціально розподіленими інтервалами складний в реалізації.

Інформація, що приховується, впроваджується відповідно до ключа в ті відліки, спотворення яких не призводить до суттєвих спотворень контейнера. Ці біти утворюють стегошлях. Залежно від додатка під істотним можна розуміти спотворення, що приводить як до неприйнятності для людини-адресата заповненого контейнера, так і до можливості виявлення прихованого повідомлення після стегоаналізу.

ЦВЗ можуть бути трьох типів: робастні, крихкі і напівкрихкі (semifragile). Під робастністю розуміється стійкість ЦВЗ до різного роду впливів на стего. Робастним ЦВЗ присвячено більшість досліджень.

Крихкі ЦВЗ руйнуються при незначній модифікації заповненого контейнера. Вони застосовуються для автентифікації сигналів. Відмінність від засобів електронного цифрового підпису полягає в тому, що ЦВЗ все ж допускають деяку модифікацію контенту. Це важливо для захисту мультимедійної інформації, так як законний користувач може, наприклад, побажати стиснути зображення. Інша відмінність полягає в тому, що крихкі ЦВЗ повинні не тільки відобразити факт модифікації контейнера, але також вид і місце розташування цієї зміни.

Напівкрихкі ЦВЗ стійкі по відношенню до одних впливів і не стійкі-до інших. Взагалі кажучи, всі ЦВЗ можуть бути віднесені до цього типу. Однак напівкрихкі ЦВЗ спеціально проектуються так, щоб бути нестійкими по відношенню до певного виду операцій. Наприклад, вони можуть дозволяти виконувати стиснення зображення, але забороняти вирізку з нього або вставку в нього фрагмента.

На рис. 1.1 представлена класифікація систем цифрової стеганографії.

Для того, щоб стегосистема була надійною, при її проектуванні необхідно виконання ряду вимог:

– Безпека системи повинна повністю визначатися секретністю ключа. Це означає, що порушник може знати всі алгоритми роботи стегосистеми та статистичні характеристики безлічі повідомлень і контейнерів, що, однак, не

дасть йому ніякої додаткової інформації про наявність або відсутність повідомлення в даному контейнері.

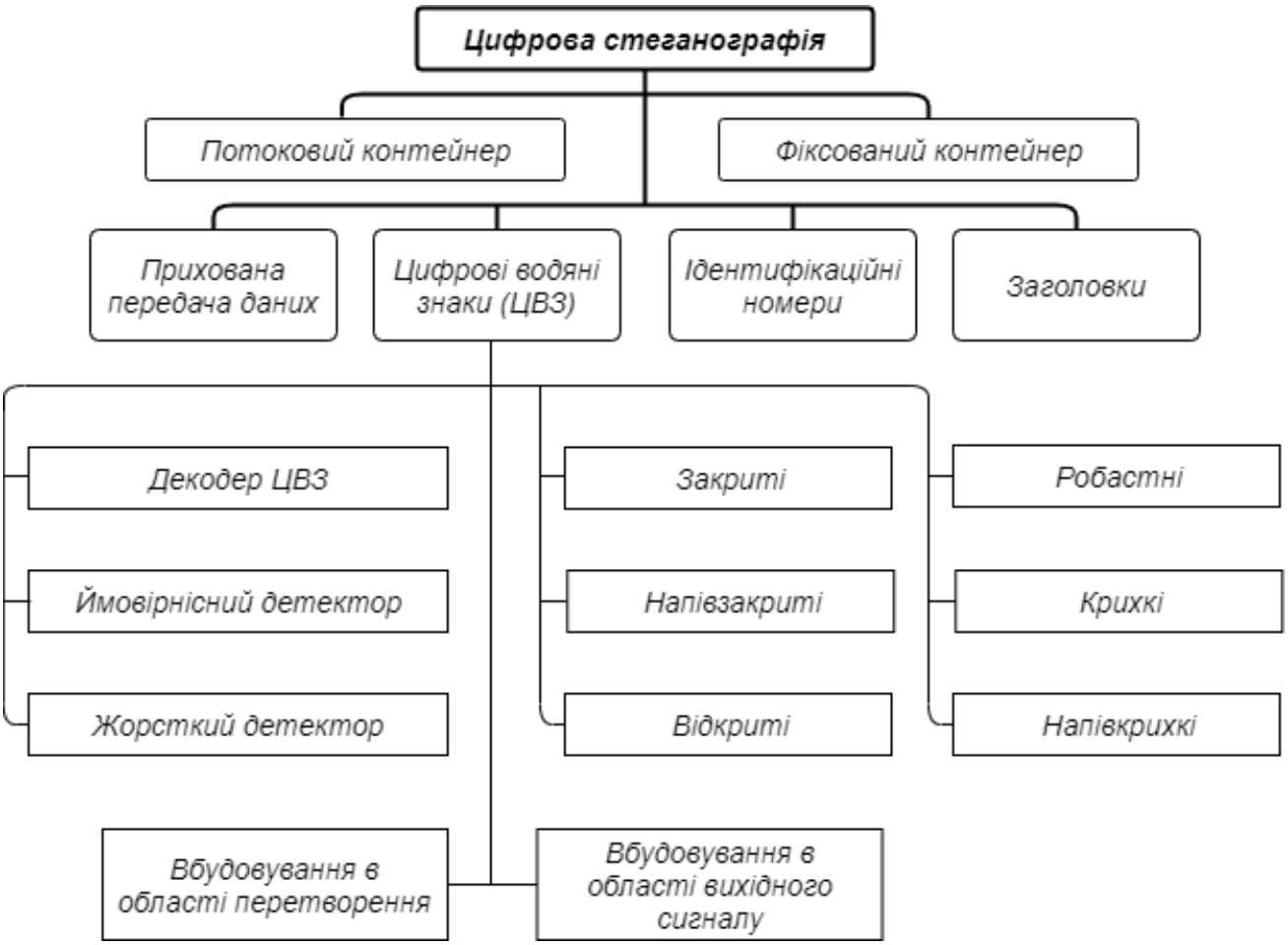

Рисунок 1.1 - Класифікація систем цифрової стеганографії

– Знання порушником факту наявності повідомлення в будь-якому контейнері не повинно допомогти йому при виявленні повідомлень в інших контейнерах.

– Заповнений контейнер повинен візуально не відрізнятися від незаповненого. Для цього треба, здавалося б, впроваджувати приховане повідомлення в візуально незначні області сигналу. Однак ці ж області використовують і алгоритми стиснення. Тому якщо зображення буде в подальшому піддаватися стисненню, то приховане повідомлення може зруйнуватися. Отож, біти повинні вбудовуватися в візуально значущі області, а відносна непомітність може бути досягнута за рахунок використання спеціальних методів, наприклад модуляції з розширенням спектру.

– Стегосистема ЦВЗ повинна мати низьку ймовірність помилкового виявлення прихованого повідомлення в сигналі, що його не містить. У деяких додатках таке виявлення призводить до серйозних наслідків. Наприклад, помилкове виявлення ЦВЗ на DVD-диску може викликати відмову від його відтворення плеєром.

– Повинна забезпечуватися необхідна пропускна здатність (ця вимога актуальна в основному для стегосистем прихованої передачі інформації). В подальшому ми введемо поняття прихованої пропускної здатності і розглянемо шляхи її досягнення.

– Стегосистема повинна мати прийнятну обчислювальну складність реалізації. При цьому можлива асиметрична за складністю реалізації система ЦВЗ, тобто складний стегокодер і простий стегодекодер.

До ЦВЗ пред'являються наступні вимоги:

– ЦВЗ повинен легко (обчислювально) витягуватися законним користувачем.

– ЦВЗ повинен бути стійким або нестійким до навмисних і випадкових впливів (залежно від програми). Якщо ЦВЗ використовується для підтвердження автентичності, то неприпустима зміна контейнера повинна призводити до руйнування ЦВЗ (крихкий ЦВЗ). Якщо ж ЦВЗ містить ідентифікаційний код, логотип фірми і т. п., то він повинен зберегтися при максимальних спотвореннях контейнера, що, звичайно, не призводять до істотного спотворення вихідного сигналу. Наприклад, у зображення можуть бути відредаговані колірна гамма або яскравість, у аудіозапису посилено звучання низьких тонів і т. д. крім того, ЦВЗ повинен бути робастним відносно до афінних перетворень зображення, тобто його поворотів, масштабування. При цьому треба розрізняти стійкість самого ЦВЗ та можливість декодера вірно його виявити. Скажімо, при повороті зображення ЦВЗ не зруйнується, а декодер може виявитися нездатним виділити його. Існують додатки, коли ЦВЗ повинен бути стійким по відношенню до одних перетворень і нестійким-до інших. Наприклад, може бути дозволено копіювання зображення (ксерокс, сканер), але накладено заборону на внесення в нього будь-яких змін [11].

– Повинна бути можливість додавання до стего додаткових ЦВЗ. Наприклад, на DVD-диску є мітка про допустимість одноразового копіювання. Після здійснення копіювання необхідно додати мітку про заборону

подальшого копіювання. Можна було б, звичайно, видалити перший ЦВЗ і записати на його місце другий. Однак це суперечить припущенню про складність видалення ЦВЗ. Кращим виходом є додавання ще одного ЦВЗ, після якого перший не буде братися до уваги. Але наявність декількох ЦВЗ на одному повідомленні може полегшити атаку зі сторони порушника, якщо не вжити спеціальних заходів.

Як видно з рис. 1.2, застосування ЦВЗ не обмежується додатками безпеки інформації. Основні галузі використання технології ЦВЗ можуть бути об'єднані в чотири групи: захист від копіювання (використання), прихована анотація документів, доказ автентичності інформації та прихований зв'язок.

Рисунок 1.2 - Потенційні галузі застосування стеганографії

1.2.4 Система стеганографічної передачі даних на основі цифрових водяних знаків

Розглянемо систему, що вбудовує водяний знак, представлений цифровим зображенням X, в інше цифрове зображення L, що називається контейнером. Заповнений контейнер H піддається різноманітним перетворенням з витяганням ЦВЗ. Введемо позначення K, J і P для опису процесів вбудовування ЦВЗ в контейнер, перетворення заповненого

контейнера і вилучення ЦВЗ, тоді схему стеганографічної системи можна представити у вигляді (рис.1.3).

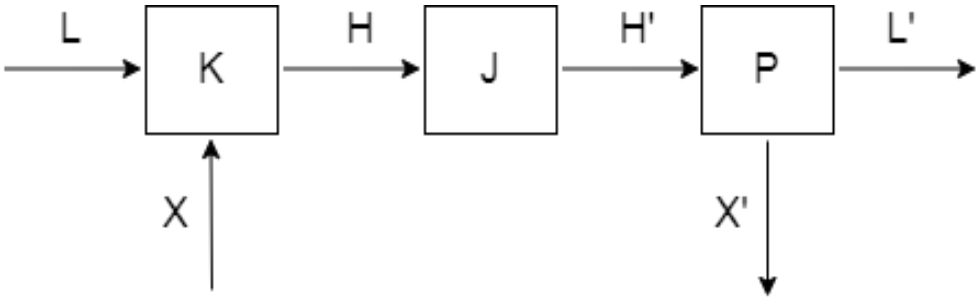

Рисунок 1.3 – Схема стеганографічної системи

За допомогою оператора J розглядаються перетворення, наприклад, передача по каналу зв'язку, атака на стегосистему, процес виведення зображень та ін.

Основною властивістю стеганографічної системи є умова візуальної схожості порожнього і заповненого контейнера:

$$L \approx H$$

1.2.5 Аналіз методів нанесення цифрових водяних знаків

Достатня кількість створених методів приховування даних в зображенні дозволяє провести їх класифікацію з виділенням декількох узагальнених груп:

- методи заміни в просторовій області;
- методи приховування в частотній області;
- широкосмугові методи;
- статистичні (стохастичні) методи;
- методи спотворення;
- структурні методи.

Розглянемо докладніше перші дві групи методів, так як розробки на їх основі є найбільш численними. Короткі описи методів для зручності зведені в табл. 1.2.

Таблиця 1.2 – Аналіз методів нанесення цифрових водяних знаків

Назва методу	Принцип дії методу. Переваги та недоліки
Просторові методи. Перевагою алгоритмів вбудовування даних в просторовій області є те, що ЦВЗ впроваджується в області вихідного зображення, і немає необхідності виконувати обчислювально громіздкі лінійні перетворення зображень. ЦВЗ впроваджується за рахунок маніпуляцій яскравістю або колірними складовими $l(x,y) \in \{1,\dots,L\}(r(x,y),g(x,y),b(x,y))$	
Метод заміни найменш значущого біту	Вбудовування інформації шляхом побітного запису в найменш значущі біти зображення. Переваги: швидкість (один крок-один біт), можливість запису великого обсягу інформації (до 1/8 від обсягу контейнера при якісному приховуванні). Недоліки: висока чутливість до спотворень.
Метод псевдовипадкової перестановки	Генератор псевдовипадкових чисел (ПСЧ) формує індекси $j_1 \dots j_M$ і зберігає К-й біт повідомлення в пікселі з індексом j_K. Далі псевдовипадкова функція перестановки розташовує біти в повідомленні випадковим чином. Переваги: біти прихованого повідомлення розташовані по зображенню хаотично, що підвищує рівень надійності. Недоліки: якщо кількість біт приховуваного повідомлення не набагато менша кількості молодших біт зображення, то велика ймовірність перетину індексів і як наслідок накладення одного біта повідомлення на інший.
Метод псевдовипадкового інтервалу	Полягає у випадковому розподілі бітів секретної інформації по контейнеру. При цьому відстань між вбудованими бітами псевдовипадкова. Переваги: метод ефективний у разі довжини секретного повідомлення набагато меншої кількості

Продовження табл. 1.2

	пікселів зображення. Недоліки: метод неефективний в разі великого обсягу прихованої інформації; біти повідомлення в контейнері розміщені в тій же послідовності, що і в секретному повідомлення.
Метод блочного приховування	Оригінальне зображення розбивається на l_M непересічних блоків $\Delta_i (l \leq i \leq l_M)$ довільної конфігурації, для кожного з яких формується біт парності $b(\Delta_i)$. У кожному блоці проводиться приховування одного секретного біта M_i. Переваги: можливість модифікації такого пікселя зображення, зміна якого призводить до мінімальної зміни статистики контейнера. Наслідок вбудовування секретних даних у файл можна знизити, збільшивши обсяг блока. Недоліки: нестійкість до спотворень.
Метод заміни палітри	Палітра з N кольорів представляється як список пар індексів (i, λ_i), що визначає відповідність між індексом i та його вектором кольоровості λ_i. Кожному пікселю зображення відповідає певний індекс таблиці. Переваги: так як зміна порядку кольорів не впливає на загальний вигляд зображення, можливе приховування інформації шляхом перестановки кольорів палітри. Недоліки: будь-яка атака, в основі якої лежить зміна палітри, призводить до знищення повідомлення.
Метод квантування зображення	Приховування інформації проводиться шляхом коригування різницевого сигналу Δ_i. Стеганоключ являє собою таблицю, яка кожному можливому значенню Δ_i ставить у відповідність певний біт. Для приховування і-го біта повідомлення обчислюється різниця Δ_i. Якщо при цьому b_i не відповідає секретному біту, то значення Δ_i змінюється на.

Продовження табл. 1.2

	найближче Δ_j, що відповідає умові. Переваги: стійкість методу до стиснення. Недоліки: обов'язковою умовою методу є наявність ключа і проведення коригування яскравості змінених бітів.
Метод Куттера-Джордана-Боссена	Секретний біт M_i вбудовується в зображення $C = \{RGB\}$ в канал синього кольору шляхом модифікації яскравості $\lambda_{x,y} = 0{,}29890 * R_{x,y} + 0{,}58662 * G_{x,y} + 0{,}11448 * B_{x,y}$ Переваги: алгоритм стійкий до НЧ фільтрації, обрізання країв зображення, компресії (стиснення). Недоліки: метод зчитування водяних знаків, створених цим методом, відмінний від методу вбудовування. Велика ймовірність помилок при зчитуванні.
Метод Дармстедтера-Делейгла-Квісквотера-Макка	Інформація перетворюється на двійковий вектор, кожен біт якого вбудовується в окремий блок, розміром 8*8 пікселів. Блок попередньо розбивається на зони яскравості, в відповідності до яких біт інформації записується в блок. Переваги: метод заснований на чутливому сприйнятті людини і стійкий до стиснення. Недоліки: громіздкість програмної реалізації, тривалість роботи програм.
Частотні методи вбудовують водяний знак в частотну область зображення з використанням ортогональних перетворень файлу-контейнера і перерозподілом його енергії. В результаті застосування перетворення max енергія зображення зосереджується в НЧ області, min - у високочастотній.	
Метод відносної заміни величин коефіцієнтів	Первинне зображення розбивається на блоки 8 * 8 пікселів. Дискретне косинусне перетворення (ДКП) застосовується до кожному блоку. В результаті чого утворюються матриці коефіцієнтів ДКП. Кожен блок приховує один біт даних.

Продовження табл. 1.2

	Приховування починається з випадкового вибору блоку. Для приховування 0 прагнуть, щоб різниця абсолютних значень коефіцієнтів ДКП перевищувала певну величину >0, а для приховування 1 різниця робиться меншою за деяку величину <0. Переваги: стійкість до компресії. Недоліки: візуальне погіршення якості зображення.
Метод Бенгама-Мемона-Ео-Юнг	Удосконалення методу Коха і Жао шляхом накладення умов на вибір блоків (блоки не повинні мати різкі перепади яскравості або бути занадто монотонними) та збільшення числа коефіцієнтів ДКП з 2 до 3. Переваги: зменшення похибки зчитування водяного знаку. Недоліки: мала пропускна здатність.
Метод Фрідріх	Зображення-контейнер конвертується в сигнал з нульовим математичним очікуванням і певним відхиленням для того, щоб НЧ-коефіцієнти ДКП потрапляли в попередньо заданий незмінний діапазон. При обчисленні коефіцієнтів ДКП для модифікації відбираються тільки низькочастотні. Переваги: стійкість до стегоатак. Недоліки: складність читання ЦВЗ, а також його детектування.

Складено за: [8].

1.3 Системи цифрової стеганографії

1.3.1 Структура цифрової стеганографічної системи

Відзначимо в даному підрозділі стеганографічне повідомлення як ЦВЗ. Розглянемо структуру цифрової стеганографічної системи (рис. 1.4).

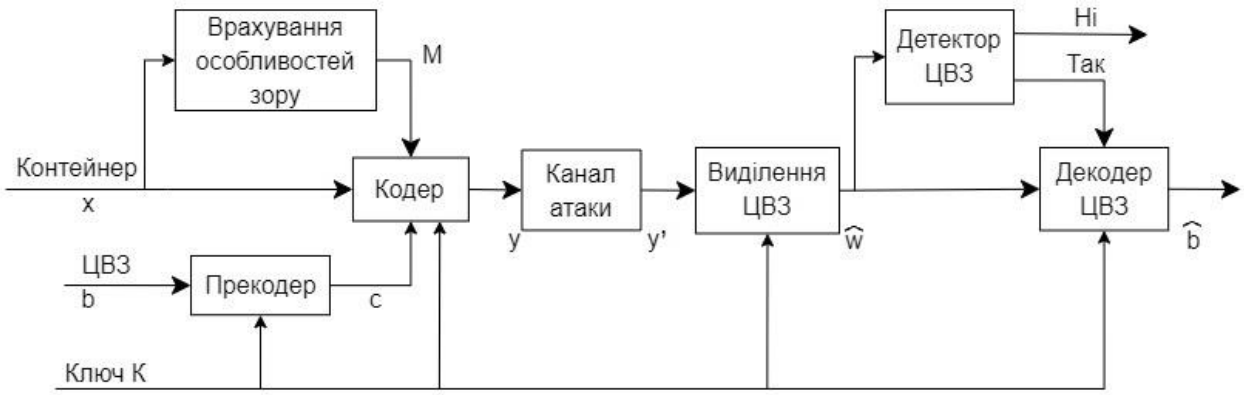

Рисунок 1.4 – Структурна схема типової стегосистеми ЦВЗ

Стегосистема, представлена на рис. 1.4, виконує задачу вбудовування та виділення повідомлень з іншої інформації та складається з наступних основних елементів:

– прекодер - пристрій, призначений для перетворення приховуваного повідомлення у вигляд, зручний для вбудовування в сигнал-контейнер (контейнером називають інформаційну послідовність, в якій приховується повідомлення);

– стеганокодер – пристрій, призначений для здійснення вкладення прихованого повідомлення в інші дані з урахуванням їх моделі;

– пристрій виділення вбудованого повідомлення;

– стеганодетектор – пристрій, призначений для визначення наявності стегоповідомлення. Можуть бути з м’яким та жорстким рішенням;

– декодер – пристрій, що відновлює приховане повідомлення. Цей вузол може бути відсутній.

Дані, що містять приховане повідомлення, можуть піддаватися навмисним атакам або випадковим завадам, опис яких представлено в підрозділі 1.3.2.

Як показано на рис. 1.4, в стегосистемі відбувається об’єднання двох типів інформації так, щоб їх можна було відрізнити двома принципово різними детекторами. В якості одного з них виступає система виділення ЦВЗ, в якості другого – людина.

Перш ніж здійснити вкладення ЦВЗ в контейнер, ЦВЗ повинен бути перетворений в деякий відповідний вигляд. Наприклад, якщо в якості

контейнера виступає зображення, то і послідовність ЦВЗ зазвичай представляється як двовимірний масив біт. Для того, щоб підвищити стійкість ЦВЗ до спотворень, нерідко виконують його завадостійке кодування або застосовують широкосмугові сигнали. Початкову обробку прихованого повідомлення виконує показаний на рис. 1.4 прекодер.

В якості найважливішої попередньої обробки ЦВЗ (а також і контейнера) назвемо вирахування його узагальненого перетворення Фур'є. Це дозволяє здійснити вбудовування ЦВЗ в спектральній області, що значно підвищує його стійкість до спотворень. Попередня обробка часто виконується з використанням ключа К для підвищення секретності вбудовування. Далі ЦВЗ «вкладається» в контейнер, наприклад шляхом модифікації молодших значущих біт коефіцієнтів. Цей процес можливий завдяки особливостям системи сприйняття людини. Добре відомо, що зображення володіють великою психовізуальною надлишковістю. Око людини подібне низькочастотному фільтру, що пропускає маленькі деталі. Особливо непомітні спотворення в високочастотній області зображення. Ці особливості людського зору використовуються, наприклад, при розробці алгоритмів стиснення зображень та відео.

Процес впровадження ЦВЗ також повинен враховувати властивості системи сприйняття людини. Стеганографія використовує наявну в сигналах психовізуальну надмірність, але іншим, ніж при стисненні даних, чином.

Наведемо простий приклад. Розглянемо напівтонове зображення з 256 градаціями сірого, тобто з питомою швидкістю кодування 8 біт/піксел. Добре відомо, що око людини не здатне помітити зміну молодшого значущого біту. Ще в 1989 році був отриманий патент на спосіб прихованого вкладення інформації в зображення шляхом модифікації молодшого значущого біту. В даному випадку детектор стего аналізує тільки значення цього біту для кожного пікселя, а око людини, навпаки, сприймає тільки старші 7 біт. Цей метод простий в реалізації і ефективний, але не задовольняє деяким важливим вимогам до ЦВЗ.

У більшості стегосистем для впровадження і виділення ЦВЗ використовується ключ. Ключ може бути призначений для вузького кола осіб або ж бути загальнодоступним. Наприклад, ключ повинен міститися у всіх DVD-плеєрах, щоб вони могли прочитати вміст дисків ЦВЗ. Іноді за аналогією

з криптографією стегосистеми ділять на два класи: з відкритим і з секретним ключем. Та ця аналогія невірна, так як поняття відкритого ключа в даному випадку значно відрізняється. Правильним виразом був би «загальнодоступний ключ», причому ключ вбудовування збігається з ключем виділення. Не існує, наскільки відомо, стегосистеми, в якій би при виділенні ЦВЗ була потрібна інша інформація, ніж при його вкладенні. Хоча і не доведена гіпотеза про неможливість існування подібної системи. В системі із загальнодоступним ключем досить складно протистояти можливим атакам з боку зловмисників. Насправді, в даному випадку порушнику точно відомі ключ і місце розташування ЦВЗ, а також його значення.

В стеганодетекторі відбувається виявлення ЦВЗ в захищеному (зміненому, модифікованому) ЦВЗ зображенні. Зміни можуть бути обумовлені можливим впливом операцій обробки сигналу, помилок в каналі передачі даних, навмисних атак порушників (стиснення, стегоаналіз).

В стегодетекторі відбувається виявлення ЦВЗ в (можливо, зміненому) захищеному ЦВЗ зображенні. Ця зміна може бути зумовлена впливом помилок в каналі зв'язку, операцій обробки сигналу, навмисних атак порушників. У багатьох моделях стегосистем сигнал-контейнер вихід детектора розглядається як адитивний шум [8]. Тоді задача виявлення і виділення стегоповідомлення є класичною для теорії зв'язку. Однак такий підхід не враховує двох факторів: невипадкового характеру сигналу контейнера і вимог щодо збереження його якості. Ці моменти не зустрічаються у відомій теорії виявлення і виділення сигналів на тлі адитивного шуму. Їх облік дозволить побудувати більш ефективні стегосистеми.

Розрізняють стегодетектори, призначені для виявлення наявності ЦВЗ та пристрої для виділення цього ЦВЗ (стегодекодери). У першому випадку можливі детектори з жорсткими (так/ні) або м'якими рішеннями. Для винесення рішення про наявність/відсутність ЦВЗ зручно використовувати такі заходи, як відстань по Хеммінгу або взаємну кореляцію між наявним сигналом і оригіналом (при наявності останнього, зрозуміло). А що робити, якщо у нас немає вихідного сигналу? Тоді в справу вступають більш тонкі статистичні методи, засновані на побудові моделей досліджуваного класу сигналів.

Стеганографія з відкритим ключем спирається на досягнення криптографії останніх 25 років. Поняття «відкритий ключ» означає, що для дешифрування повідомлення використовується інший ключ, ніж при його шифруванні. Один з ключів робиться загальнодоступним, відкритим. Криптографічна система з відкритим ключем використовується, наприклад, при нанесенні цифрового підпису. Повідомлення підписується закритим ключем, і будь-хто, хто має відповідний відкритий ключ, може упевнитися в її справжності. При шифруванні використовують зворотний порядок: повідомлення підписується відкритим ключем, а прочитати його може лише той, хто має відповідний закритий ключ. Зрозуміло, що з відкритого ключа ніякими способами не можна отримати закритий ключ (в обчислювальному сенсі).

Нагадаємо, що стеганографічний ключ не шифрує дані, а приховує місце їх знаходження в контейнері. Заховані дані можуть бути додатково зашифровані звичайними методами, але це питання не відноситься до стеганографії. Щоб була можливість організації стегоканалу, сторони повинні, як правило, мати перед початком сеансу деяку інформацію.

Розглянемо часто використовувану схему побудови системи ЦВЗ, представлену на рис. 1.5. У даній схемі враховується, що повідомлення M зазвичай не належить множині **X** і має довжину, відмінну від довжини контейнера $\widetilde{X^N}$. Наприклад, якщо ЦВЗ являє собою зображення фірмового знаку виробника інформаційної продукції, то такий водяний знак за формою представлення та за своїми характеристиками істотно відрізняється від контейнера, що завіряється. Тому приховане повідомлення (ЦВЗ) M перетворюється в кодову послідовність U^N довжиною N символів, $U^N(M) \in X^N$. Ця операція приводить водяний знак M до вигляду, зручного для вбудовування в контейнер $\widetilde{X^N}$. Зауважимо, що на рис. 1.5 показаний випадок, коли це перетворення незалежно від контейнерного сигналу.

Завірене водяним знаком стего в загальному випадку формується за правилом $x_N = f_N(\widetilde{x^N}, u^N, k^N)$ x, де f_N - функція вбудовування за ключем k^N.В значенні функції вбудовування неявно вказується, що вона виконує перетворення над блоком довжини N. У найпростішому прикладі вбудовування може виконуватися за правилом $x_i = \widetilde{x_i} + u_i$ для $1 \le i \le N$, де змінні $\widetilde{x_i}, x_i$ та u_i належать кінцевому алфавіту $\widetilde{0}$.

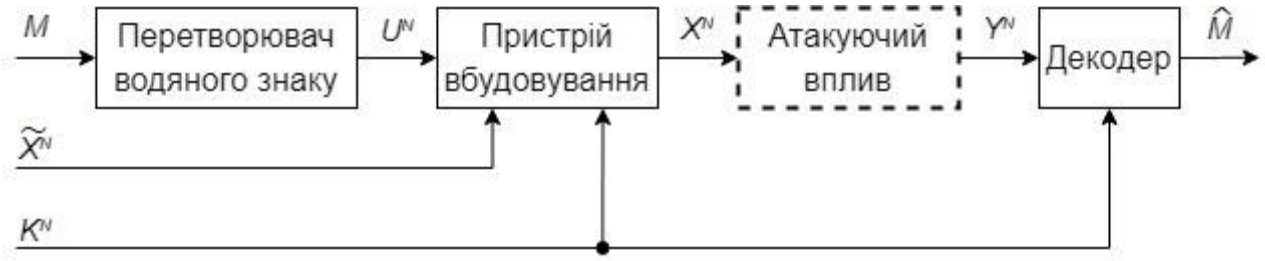

Рисунок 1.5 – Структурна схема стегосистеми водяного знаку при при активній протидії порушника

В сучасних системах водяного знаку застосовуються складні побудови функції f_N, які враховують характеристики чутливості органів зору або слуху людини і не є адитивними [12]. Перетворення f_N має бути зручним для того, хто приховує інформацію, а також має мінімізувати спотворення, що вносяться в контейнер за умови забезпечення необхідної стійкості до атак порушника. Оптимальна побудова таких функцій представляє складну задачу.

Формально визначимо спотворення, що вносяться, в стратегіях того, хто приховує інформацію, та порушника. Це завершує математичний опис стегосистеми і дозволяє визначити швидкість безпомилкової передачі для стегосистеми.

Нехай спотворення в стегосистемі оцінюються відповідно до обмеженої невід'ємної функції виду $d(x,y)$, де $x,y \in X$. Міра спотворення, що використовується, симетрична: $d(x,y) = d(y,x)$, виконання рівності $d(x,y) = 0$ означає збіг $x = y$. Отже, використовувана міра спотворення є метрикою. Метрика спотворень розширюється на послідовності довжиною N символів $x^N = (x_1, x_2, \dots, x_N)$ та $y^N = (y, y_2, \dots, y_N)$ наступним чином: $d^N(x^N, y^N) = \frac{1}{N}\sum_{k=1}^{N} d\,(x_k, y_k)$. Теорія інформаційного приховування використовує класичні метрики спотворення, такі, як метрики Хеммінга і Евкліда, а також метрики, що враховують особливості слухової або зорової чутливості людини [13].

1.3.2 Класифікація атак на стеганографічні системи на основі цифрових водяних знаків

Можлива різна класифікація атак на стегосистеми, та в цій роботі буде

розглянуто атаки, специфічні для систем ЦВЗ.

Можна виділити наступні категорії атак проти таких систем:

– атаки проти вбудованого повідомлення – направлені на видалення або псування ЦВЗ шляхом маніпулювання стего (секретною інформацією). Методи, що входять до цієї категорії атак, не намагаються оцінити та виділити водяний знак. Прикладами таких атак можуть бути лінійна фільтрація, стиснення зображення, додавання шуму, вирівнювання гістограми, зміна контрастності (рис. 1.6) та ін.;
– атаки проти стеганодетектора – направлені на те, щоб ускладнити або зробити неможливою правильну роботу детектора. При цьому водяний знак в зображенні залишається, але втрачається можливість його прийому. В цю категорію входять такі атаки, як афінні перетворення (повороти, зсуви, масштабування), кадрування зображення, перестановка пікселів та ін. (рис. 1.6);
– атаки проти протоколу впровадження ЦВЗ – здебільшого пов'язані зі створенням хибних ЦВЗ, хибних стего, інверсією ЦВЗ, додаванням декількох ЦВЗ;
– атаки проти самого ЦВЗ – направлені на оцінювання та вилучення ЦВЗ із стегоповідомлення, по можливості без спотворення контейнера. В цю групу входять такі атаки, як атаки змови, методи очищення сигналів від шумів, статистичного усереднення, деякі з видів нелінійної фільтрації та ін.

Треба відмітити, що розглянута класифікація атак не є єдино можливою та повною. Крім того, деякі атаки (наприклад, видалення шуму) можуть бути віднесені до декількох категорій.

Враховуючи різні класифікації всі атаки на системи вбудовування ЦВЗ можуть бути розділені на чотири групи:

– атаки, направлені на видалення ЦВЗ;
– геометричні атаки, направлені на спотворення контейнера;
– криптографічні атаки;
– атаки проти використовуваного протоколу вбудовування та перевірки ЦВЗ.

Розглянемо деякі типи геометричних перетворень, які можуть виявитись як умисними, так і ненавмисними атаками:

– дзеркальне відображення. Більшість комп'ютерних зображень можна дзеркально відобразити відносно вертикальної або горизонтальної осі. Однак небагато СЦВЗ можуть зберегти вбудований знак після такого перетворення. При цьому основна проблема - розсинхронізація стеганодекодера (рис. 1.6);
– поворот. Поворот зображення на невеликий кут часто застосовується до відсканованого зображення, щоб вирівняти картинку по горизонталі або вертикалі, але може застосовуватися і для того, щоб не виявлявся ЦВЗ. Зазвичай поворот поєднується з кадруванням;
– кадрування (обрізка та нарощування зображення). В деяких випадках порушники зацікавлені «центральною» частиною матеріалу, захищеного авторським правом. Тоді вони вирізають центральний сегмент зображення. Однак розсіювання (розмноження) ЦВЗ по всій площі зображення запобігає вирізанню вбудованого знака (рис. 1.6);
– стиснення JPEG. В даний час JPEG - один із широко використовуваних алгоритмів стиснення зображення, тому будь-яка СЦВЗ повинна бути стійкою до стиснення. Важливим є показник рівня стиснення, рекомендований рівень стійкості до стиснення до 70% [1];
– видалення рядків та/або стовпців. Видалення кількох рядків або стовпців зображення, обраних псевдовипадковим чином з усієї картинки, вважається ефективною атакою проти впровадження ЦВЗ.

Технічні прийоми редагування:

– фільтрація. Вона включає в себе лінійні і нелінійні фільтри, що застосовуються з метою редагування зображення. Часто використовують медіанний і гауссівський фільтри. Фільтрацією за допомогою згладжування образу можна видалити ЦВЗ. Сучасні системи маркування не дозволяють відфільтрувати ЦВЗ без значних пошкоджень самого образу;
– збільшення різкості. Функція збільшення різкості належить до стандартних можливостей ПЗ для обробки зображень. Це перетворення ефективно визначає шуми в високих частотах, що

вводяться програмами впровадження ЦВЗ, і тому може бути використано для атак на СЦВЗ;

– додавання шуму і очищення від шумів. Багато СЦВЗ ефективно протистоять додаванню завад (адитивний шум або некорельована мультипликативна завада) в зображення. Даний вид перетворень широко розглянуто в теорії зв'язку та теорії обробки сигналів, де і розроблені алгоритми захисту від шуму. При цьому важливим є допустимий рівень шуму щодо рівня сигналу самого маркованого зображення;
– атака «Мозаїка». При цій атаці картинка розбивається на фрагменти, які є окремими, але зістикованими в єдине ціле. Такі сегментовані зображення можуть використовуватися при оформленні інтернет-сайтів. Якщо зловмисникові вдасться розбити марковане зображення на немарковані фрагменти, то він зможе обдурити автоматичну систему пошуку файлів з впровадженими ЦВЗ;
– атака усереднення і атака змови. Маючи кілька копій одного і того ж зображення, але з різними знаками, можна видалити ЦВЗ шляхом усереднення цих зображень (атака усереднення) або шляхом поділу всіх копій зображення на невеликі частини з подальшим складанням оригінальної картинки, але вже з відповідних частин різних копій (атака змови);
– атаки на протокол СЦВЗ. Зазначені атаки спрямовані проти функціонування самого протоколу вироблення і перевірки ЦВЗ. Однією з таких атак є атака, заснована на інверсії послідовності дій при впровадженні мітки, в результаті чого в разі незворотності ЦВЗ зловмисникові вдається промаркувати вже захищене зображення. При розробці всієї системи необхідно аналізувати слабкості не тільки ЦВЗ, але і стеганографічні протоколи взаємодії учасників комунікаційного процесу.

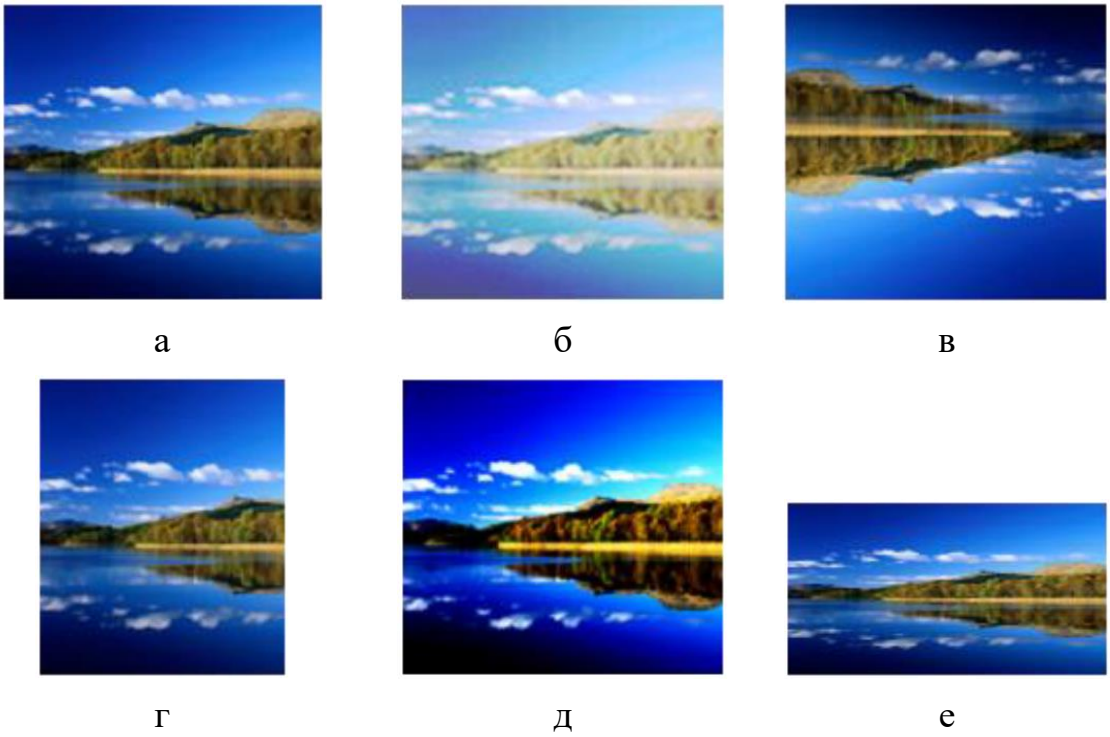

Рисунок 1.6 – Приклади атак на стеганодетектор та вбудоване повідомлення (а – оригінальне зображення, б – зміна яскравості, в – дзеркальне відображення, г – кадрування, д – зміна контрастності, е – масштабування)

1.3.3 Методи протидії атакам на стеганографічні системи на основі цифрових водяних знаків

Причиною нестійкості систем ЦВЗ з розширенням спектру до атак подібних атаці змови є те, що послідовність, яка використовується для вкладення, зазвичай має нульове середнє. Після усереднення за достатньо великою кількістю реалізацій ЦВЗ видаляється. Відомий спеціальний метод побудови водяного знаку, направлений проти подібної атаки. При цьому коди розробляються таким чином, щоб при будь-якому усередненні завжди залишалась не рівна нулю частина послідовності. Недоліком запропонованих кодів є те, що їх довжина збільшується експоненціально зі зростанням числа розповсюджуваних захищених копій. Можливим виходом з цього положення є застосування ієрархічного кодування, тобто призначення кодів для групи

користувачів. Деякі аналогії тут є з системами стільникового зв'язку з кодовим розподіленням користувачів (CDMA) [4].

Різні методи протидії пропонувались для вирішення проблеми прав власності. Перший спосіб полягає в побудові незворотного алгоритму ЦВЗ. ЦВЗ повинен бути адаптивним до сигналу та вбудовуватись за допомогою одно направленої функції, наприклад, хеш-функції. Хеш-функція перетворює 1000 біт вихідного зображення V в бітову послідовність $b_i, i = \overline{1 \dots 1000}$. Далі, в залежності від значення b_i використовується дві функції вбудовування ЦВЗ. Якщо $b_i = 0$, то використовується функція $v_i(1 + \alpha w_i)$, якщо $b_i = 1$, то функція $v_i(1 - \alpha w_i)$, де v_i – і-й коефіцієнт зображення, w_i – і-й біт вбудовуваного повідомлення. Припускається, що такий алгоритм формування ЦВЗ перешкодить фальсифікації.

Другий спосіб вирішення проблеми прав власності полягає у вбудовуванні в ЦВЗ деякої тимчасової мітки, яка надається третьою, довіреною стороною.

Для захисту від атак типу афінного перетворення можна використовувати додатковий (опорний) ЦВЗ. Цей ЦВЗ не несе в собі інформації, але використовується для «реєстрації» виконуваних порушником перетворень. В детекторі ЦВЗ є схема передспотворення, що виконує зворотне перетворення. Тут є аналогія з використанням в зв'язку тестових послідовностей. Однак, в цьому випадку атака може бути направлена саме проти опорного ЦВЗ. Іншою альтернативою є вкладення ЦВЗ у візуально значимі області зображення, які не можуть бути видалені з нього без істотної його деградації. Нарешті, можна розмістити стего в інваріантних до перетворення коефіцієнтах. Наприклад, амплітуда перетворення Фур'є інваріантна до зсуву зображення (при цьому змінюється тільки фаза) [3].

Другим методом захисту від подібних атак є блочний детектор. Модифіковане зображення розбивається на блоки розміром 12x12 або 16x16 пікселів, та для кожного блоку аналізуються всі можливі спотворення. Тобто пік селі в блоці піддаються поворотам, перестановкам і т. д. Для кожної зміни визначається коефіцієнт кореляції ЦВЗ. Перетворення, після якого коефіцієнт кореляції виявився найбільшим, вважається реально виконаним порушником. Таким чином з'являється можливість, так би мовити, обернути внесені порушником спотворення. Можливість такого підходу заснована на

припущенні про те, що порушник не буде значною мірою спотворювати контейнер (це не в його інтересах).

1.4 Постановка завдання

Метою роботи є розробка пристрою захисту інформації на базі стеганографічного алгоритму, який повинен забезпечити прихованість та автентичність інформації при її передачі по каналах зв’язку.

Для досягнення цієї мети необхідно виконати наступне:

1. Визначити основні функції та завдання, які повинен виконувати пристрій, який реалізує стеганографічний алгоритм вбудовування цифрового водяного знаку з достатньою прихованою пропускною здатністю.
2. Розробити структурну схему стеганосистеми.
3. Розробити структурну схему пристрою захисту інформації на базі стеганографічного алгоритму вбудовування цифрового водяного знаку.
4. Розробити функціональну схему пристрою вбудовування цифрового водяного знаку.

2 ДОСЛІДЖЕННЯ ПРИХОВАНОЇ ПРОПУСКНОЇ ЗДАТНОСТІ СТЕГАНОГРАФІЧНОГО КАНАЛУ ПЕРЕДАЧІ ДАНИХ

Прихованою пропускною здатністю є верхня межа швидкості безпомилкової передачі приховуваних повідомлень, при якій спотворення контейнера, викликані вкладенням в нього даних повідомлень і діями порушника по руйнуванню цих повідомлень, не перевищують заданих величин. Як і ПЗ каналів передачі відкритих повідомлень, ПЗ каналів передачі прихованих повідомлень визначається в ідеалізованих умовах, в яких затримка кодування/декодування нескінченна ($N \to \infty$), статистика контейнерів, приховуваних повідомлень, стего і ключів точно відома, складність побудови стегосистеми необмежена.

Визначимо величину прихованої пропускної здатності стегосистеми, в якій алфавіт прихованих повідомлень, контейнерів, ключів і стего є двійковим алфавітом $X = \{0,1\}$. Нехай контейнер $\widetilde{X}$ формується джерелом Бернуллі, тобто символи послідовності контейнера є незалежними один від одного і рівноймовірними. Функція спотворення описується відстанню Хеммінга: $d = (x, y) = 0$, якщо $x = y$ і $d(x, y) = 1$ d в іншому випадку. Опис контейнера є секретним ключем стегосистеми ($K = \widetilde{X}$) і відомий декодеру. Нехай двійкова послідовність $\widetilde{X}$ формується незалежно і рівноймовірно. Стегограми формуються у вигляді $X = \widetilde{X} \oplus Z$, де операція $\oplus$ є підсумовуванняv по модулю 2. Змінна Z має бернуліївський розподіл і відображає приховане повідомлення M зі спотворенням D_1. Спотворення D_1 означає, що кожен символ двійкової послідовності Z відрізняється від відповідного символу двійковій послідовності M із ймовірністю D_1. Перетворення повідомлення M в послідовність Z виконується тим, хто приховує інформацію, з використанням кодера з викривленням D_1. Порушник обробляє стего накладенням на нього двійкової шумової послідовності W, в якій одиничний символ породжується з імовірністю D_2. Одержувач підсумовує спотворене стего з двійковою послідовністю $\widetilde{X}$ по модулю 2 і з отриманої таким чином двійкової послідовності $\hat{Z}$ декодує прийняте приховане повідомлення $\widehat{M}$. Особливістю цієї стегосистеми є те, що в ній приховане повідомлення при вбудовуванні спотворюється з ймовірністю спотворення D_1і це спотворення дорівнює спотворенню кодування стего. Така стегосистема показана на рис. 2.1.

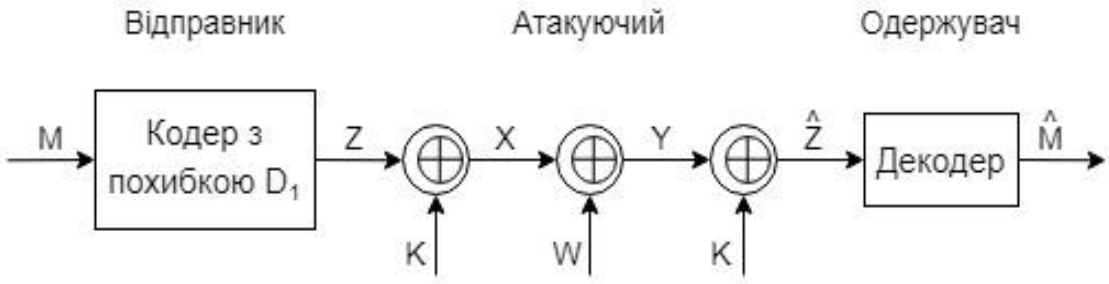

Рисунок 2.1 – Структурна схема двійкової стегосистеми

Випадок малих величин спотворень D_1 і D_2 типовий для багатьох інформаційно-приховуючих завдань. Цей випадок для стегосистем аналогічний випадку малих спотворень в теорії залежності швидкості передачі відкритих повідомлень від величини їх спотворення [7]. Малими спотвореннями в стегосистемах вважаються ті спотворення контейнера, при яких величини D_1 і D_2 у багато разів менші за дисперсію σ^2. В більшості реальних стегосистем величини спотворень D_1 і D_2 є малими. У стегосистемах, орієнтованих на невиявлення факту наявності прихованого зв'язку, це зумовлено вимогами скритності зв'язку, в системах ЦВЗ формувач водяного знака і атакуючий змушені обмежувати спотворення D_1 і D_2, зберігаючи споживчі та інші якості контейнера.

У разі малих спотворень при використанні оптимальних приховуючих перетворень величина прихованої пропускної здатності згідно з виразом:

$$\underline{C} = \overline{C} = C\begin{cases} {}^1\!/_2 \log(1 + \dfrac{D_1}{\beta D_2}), & \text{при } D_2 < \sigma^2 + D_1, \\ 0, & \text{при } D_2 \geq \sigma^2 + D_1, \end{cases}$$

близька до величини 1/2 біта на відлік контейнера при $D_1 = D_2$.

На рис. 2.2 показана залежність прихованої ПЗ в бітах на відлік гауссівського контейнера від величини спотворення D_2 при фіксованому спотворенні кодування $D_1 = 1$ і дисперсії контейнера $\sigma^2 = 10$. З графіка видно, що зі зростанням величини спотворення D_2 значення прихованої ПЗ експоненціально швидко зменшується як для оптимального приховуючого перетворення, так і при виборі при побудові стегосистеми випадку $U = X$. При малих величинах D_2 прихована ПЗ незначно програє оптимальному випадку,

але і при $D_2 = D_1$ для таких систем приховано передавати інформацію не можна (обрив стегоканалу). Для більшості застосувань стегосистем в умовах активної протидії порушник може спотворювати контейнер на величину, порівнянну з величиною спотворення кодування. Наприклад, така ситуація характерна для атак на систему ЦВЗ за умови збереження необхідної якості контейнера. Або коли порушник подавляє загороджувальною перешкодою передбачуваний канал передачі приховуваних повідомлень. В другому випадку порушник не обмежений необхідністю збереження контейнера і може застосувати перешкоду більш потужну, ніж перешкода, що вноситься при кодуванні відправником повідомлень. Відзначимо, що в обох випадках стегосистема, побудована за принципом $U = X$, непридатна для практичного використання.

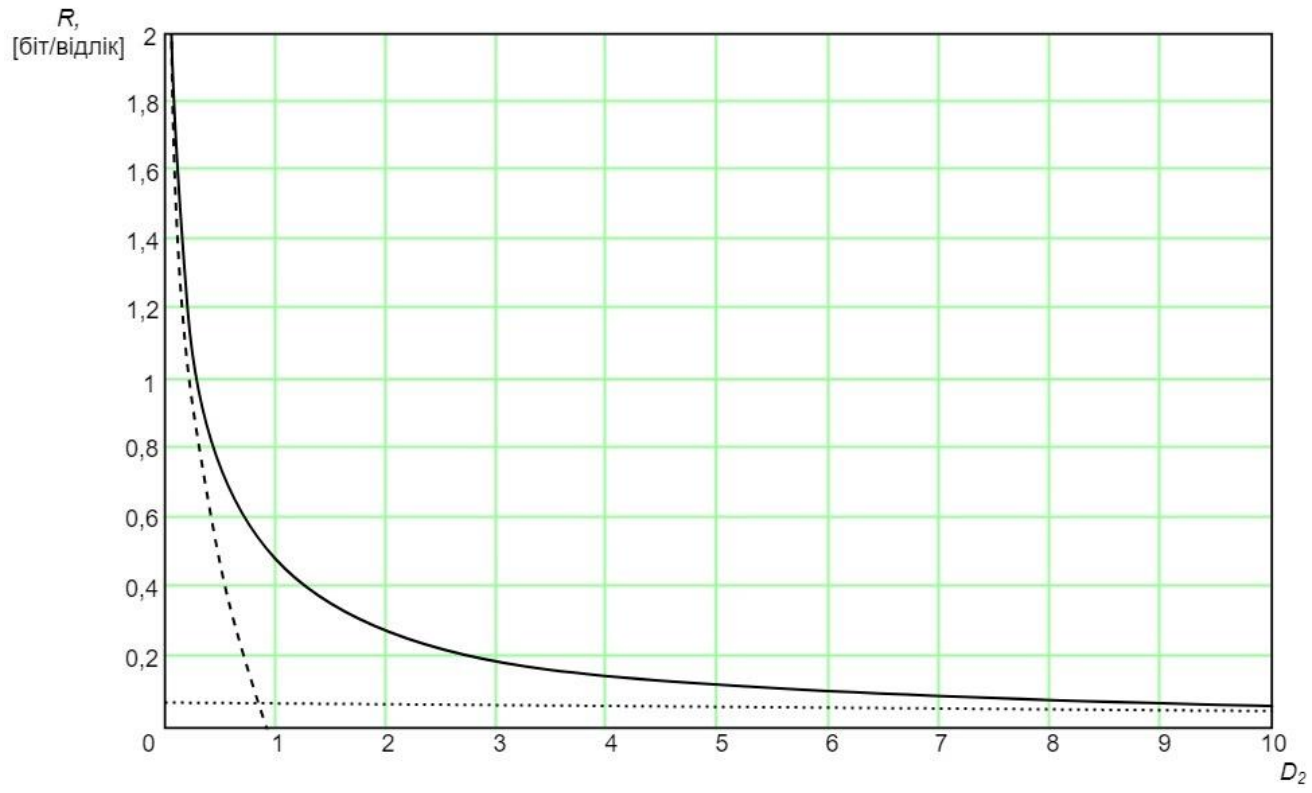

Рисунок 2.2 – Залежність прихованої ПЗ в бітах на відлік гаусівського контейнеру при $\mathbf{D_1 = 1}$ та $\boldsymbol{\sigma^2 = 10}$: оптимальне приховуючи перетворення (суцільна лінія), при виборі $\mathbf{U = X}$ (пунктирна лінія), при виборі $\mathbf{U = Z}$ (пунктирна лінія)

На рис. 2.2 також показана залежність прихованої ПЗ для вибору $U = Z$ при вбудовуванні прихованого повідомлення. Видно, що такий принцип побудови стегосистеми в порівнянні з іншими варіантами побудови забезпечує істотно меншу величину прихованої ПЗ. Коли величина спотворення D_2 наближається до величини енергії контейнера, значення прихованої ПЗ при оптимальному приховуючому перетворенні і при виборі $U = Z$ стають зіставними. Однак настільки великі величини спотворення D_2 не характерні для стегосистем. При використанні в якості контейнерів звукових (мовних) сигналів або зображень допустима ступінь спотворення таких контейнерів практично обмежується значно меншими величинами. Наприклад, якщо завіряти мовні або музичні файли водяними знаками, то для збереження мінімально прийнятної їх якості потрібно забезпечити відношення потужності сигналу до потужності завади не гірше 10-20 дБ. Для зображень, що завіряються, відношення сигнал/завада повинно бути не гірше 30 дБ. Якщо до стегосистеми пред'являються вимоги невиявлення факту існування стегоканалу, то необхідне відношення сигнал/завада має бути істотно вище. Отже, для найбільш використовуваних в стеганографії контейнерів потрібно забезпечити відношення $D_2/\sigma^2 < 0.1, \ldots, 0.001$. Зауважимо, що аналогічним чином на практиці доводиться зменшувати і відношення D_1/σ^2. Таким чином, для стегосистем практично цікавий випадок, коли величини спотворення D_1 і D_2 істотно менші за енергію контейнера.

Особливий інтерес викликає питання, як співвідносяться між собою величини прихованої ПЗ стегоканалу передачі приховуваних повідомлень і звичайної пропускної здатності відкритого каналу передачі. Нехай по відкритому каналу передається сигнал з нормальним розподілом. На передаваний сигнал впливає гауссівський шум з потужністю D_2. З теорії зв'язку відомо, що максимальна швидкість передачі по відкритому каналу дорівнює:

$$R_0 = \begin{cases} {}^1\!/_2 \log(1 + \dfrac{\sigma^2}{D_2}), & \text{при } 0 \le D_2 \le \sigma^2, \\ 0, & \text{при } D_2 > \sigma^2. \end{cases}$$

Нехай в стегосистемі в якості контейнера використовується розглянутий сигнал з нормальним розподілом. В нього вбудовується приховане

повідомлення, при цьому в контейнер вноситься спотворення кодування величиною D_1. На стего накладається такий же шум з потужністю D_2 як і у відкритому каналі. Таким чином, для стегосистеми розглядається випадок гауссівського приховуючого перетворення і гауссівського атакуючого впливу. Стегосистема і система відкритої передачі поставлені в однакові умови (за винятком спотворення кодування, відсутнього для системи відкритої передачі).

На рис. 2.3 показані залежності величин ПЗ відкритого каналу передачі гауссівського сигналу і прихованої ПЗ стегоканалу при оптимальному приховуючому перетворенні цього ж гауссівського контейнера з дисперсією $\sigma^2 = 10$. Пропускна здатність виражена в бітах на відлік гауссівського сигналу (контейнера). Для стегосистеми розглянуто випадок фіксованої величини спотворення кодування $D_1 = 1$ (суцільна лінія) і випадок $D_1 = 0{,}1$ (пунктирна лінія). З рис. 2.2 видно, що ПЗ відкритого каналу передачі істотно перевищує приховану ПЗ стегоканалу, причому при зменшенні спотворення кодування D_1 величина прихованої ПЗ становить все меншу частина величини ПЗ відкритого каналу. Отже, для випадку малих спотворень D_1 і D_2, що становить найбільш практично важливий випадок застосування стегосистем, за скритність передачі інформації доводиться платити зменшенням швидкості захищеної передачі в порівнянні зі швидкістю відкритої передачі в десятки разів. Можна зробити висновок, що при утворенні стегоканалу всередині відкритого каналу передачі основний ресурс цього відкритого каналу витрачається не на передачу прихованого повідомлення, а на передачу контейнера, який виступає в ролі сигналу прикриття прихованого повідомлення.

Використовуючи середньоквадратичну метрику, покажемо, що величина прихованої ПЗ незалежно від статистики контейнера $\tilde{X}$ при асимптотичному зменшенні величин спотворень D_1 і D_2. Прихована ПЗ істотно залежить від геометрії областей малих спотворень, збільшуючись при таких малих областях, в яких розподіл $p(\tilde{x})$ рівномірний.

Нехай в стегосистемі з безперервним алфавітом X використовується середньоквадратична міра спотворень виду $d(x, y) = (x - y)^2$. В стегосистемі розподіл контейнерів $p(\tilde{x})$ має нульове середнє значення і дисперсію σ^2, воно обмежене і безперервне. Тоді при $D_1,\ D_2 \to 0$ величина $C(D_1, D_2)$ прагне до значення прихованої ПЗ при гауссівському контейнері, рівній $\frac{1}{2}\log(1 + \frac{D_1}{D_2})$.

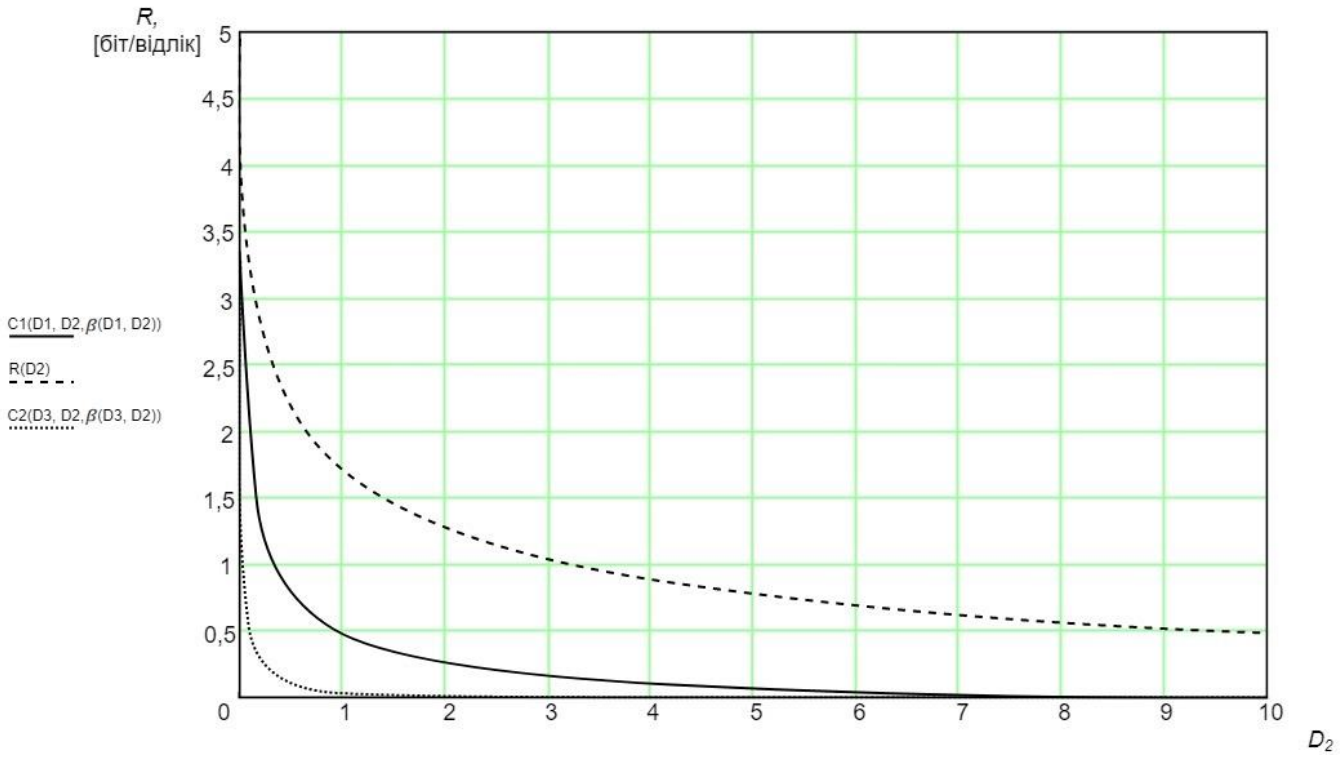

Рисунок 2.3 – Залежність ПЗ прихованого каналу передачі гауссівського сигналу від спотворення $\mathbf{D_2}$ (пунктирна лінія) та прихованої ПЗ стегоканалу з оптимальним приховуючим перетворенням гауссівського контейнеру при $\mathbf{D_1 = 1}$ та $\boldsymbol{\sigma^2 = 10}$ (суцільна лінія), при $\mathbf{D_1 = 0,1}$ та $\boldsymbol{\sigma^2 = 10}$ (пунктирна лінія)

Побудова стегосистеми, при якій асимптотично досягається максимальне значення прихованої ПЗ, збігається з гауссівським випадком: $X = \tilde{X} + Z,\ U = Z + \alpha\tilde{X}$, де $\alpha = \frac{D_1}{D_1 + D_2}$, послідовність Z має нульове математичне очікування, дисперсію D_2 і є незалежною від контейнера X, а розподіл $Q(y/x)$ описує гауссівський атакуючий вплив виду $H(C) + D(P_C \parallel P_S) = log|X|$ при $\beta = 1$.

Розглянуті результати мають дуже важливе практичне значення. Вони визначають, що при використанні таких контейнерів. як відео або аудіо, характеристики яких не розподілені за нормальним законом, при малих величинах D_1 і D_2 величина прихованої ПЗ практично не зменшується в порівнянні з випадком гауссівських контейнерів. Для цього інформація. Що

вбудовується, повинна впроваджуватися в такі малі ділянки контейнера, для яких розподіл $p(\tilde{x})$ наближений до рівномірного.

3 РОЗРОБКА СТРУКТУРНИХ СХЕМ СТЕГАНОГРАФІЧНОЇ СИСТЕМИ ПЕРЕДАЧІ ДАНИХ

3.1 Розробка схеми електричної структурної стеганосистеми

Стегосистема може бути розглянута як система зв'язку. Схема стеганосистеми зображена на рис. 3.1.

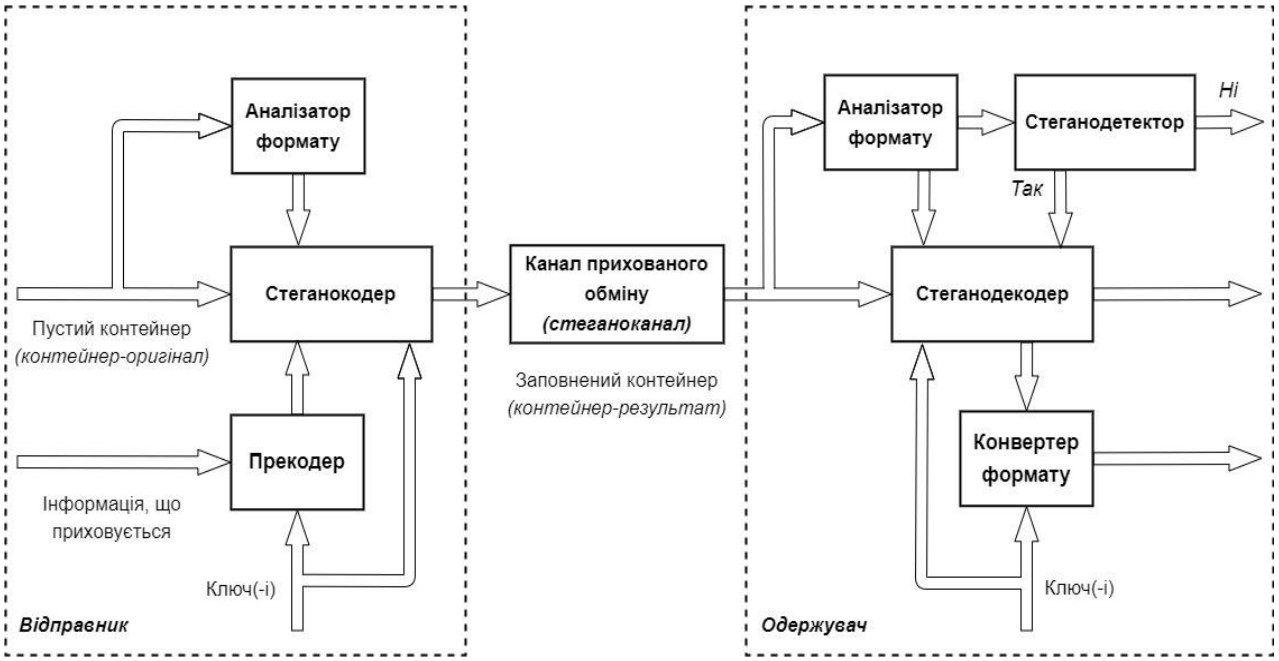

Рисунок 3.1 – Схема електрична структурна стеганосистеми як системи зв'язку

Алгоритм вбудовування ЦВЗ складається з двох основних етапів: 1) генерації ЦВЗ та 2) вбудовування ЦВЗ в кодері.

1. Нехай W*, K*, I*,B* є безлічі можливих ЦВЗ, ключів, контейнерів і приховуваних повідомлень, відповідно. Тоді генерація ЦВЗ може бути представлена у вигляді:

$$F: I^* \times K^* \times B^* \to W^*, W = F(I, K, B),$$

де W, K, I, B - представники відповідних множин. Взагалі кажучи, функція F може бути довільною, але на практиці вимоги робастності ЦВЗ накладають на неї певні обмеження. Так, в більшості випадків, $F(I, K, B) \approx F(I + \varepsilon, K, B)$,

тобто незначно змінений контейнер не призводить до зміни ЦВЗ. Функція F зазвичай є складовою:

$$F = T \text{о } G, \text{де } G: K^* \times B^* \to C^* \text{ та } T: C^* \times I^* \to W,$$

тобто ЦВЗ залежить від властивостей контейнера. Функція G реалізується за допомогою криптографічно безпечного генератора ПВП з К в якості початкового значення.

Для підвищення робастності ЦВЗ можуть застосовуватися завадостійкі коди, наприклад коди БЧХ, згорткові коди [12]. У ряді публікацій відмічені хороші результати, що досягаються при вбудовуванні ЦВЗ в області вейвлет-перетворення з використанням турбо-кодів. Відліки ЦВЗ приймають зазвичай значення з множини {-1,1}, при цьому для відображення $\{0,1\} \to \{-1,1\}$ може застосовуватися двійкова відносна фазова модуляція (BPSK).

Оператор T модифікує кодові слова C*, в результаті чого отримуємо ЦВЗ W*. На цю функцію можна не накладати обмеження необоротності, так як відповідний вибір G вже гарантує незворотність F. Функція T повинна бути обрана так, щоб незаповнений контейнер I_0, заповнений контейнер I_W і незначно модифікований заповнений контейнер Γ_W , породжували б один і той же ЦВЗ:

$$T(C, I_0) = T(C, I_W) = T(C, \Gamma_W),$$

тобто вона повинна бути стійкою до малих змін контейнера.

2. Процес вбудовування ЦВЗ $W(i,j)$ у вихідне зображення $I_0(i,j)$ може бути описаний як суперпозиція двох сигналів:

$$\varepsilon: I^* \times W^* \times L^* \to I_W^*, I_W(i,j) = I_0(i,j) \oplus L(i,j) W(i,j) p(i,j),$$

де $L(i,j)$ - маска вбудовування ЦВЗ, що враховує характеристики зорової системи людини; служить для зменшення помітності ЦВЗ; $p(i,j)$ - проектуюча функція, що залежить від ключа; знаком $\oplus$ позначений оператор суперпозиції, що включає в себе, крім складання, усічення і квантування.

Проектуюча функція здійснює «розподіл» ЦВЗ по області зображення. Її використання може розглядатися, як реалізація рознесення інформації по паралельних каналах. Крім того, ця функція має певну просторову структуру і кореляційні властивості, що використовуються для протидії геометричним атакам (див. 1.3.3).

Інший можливий опис процесу впровадження отримаємо, представивши стегосистему як систему зв'язку з передачею додаткової інформації (рис. 3.2) [8]. У цій моделі кодер і декодер мають доступ, крім ключа, до інформації про канал (тобто про контейнер і про можливі атаки). У залежності від положення перемикачів А і Б виділяють чотири класи стегосистем (мається на увазі, що ключ завжди відомий кодеру і декодеру).

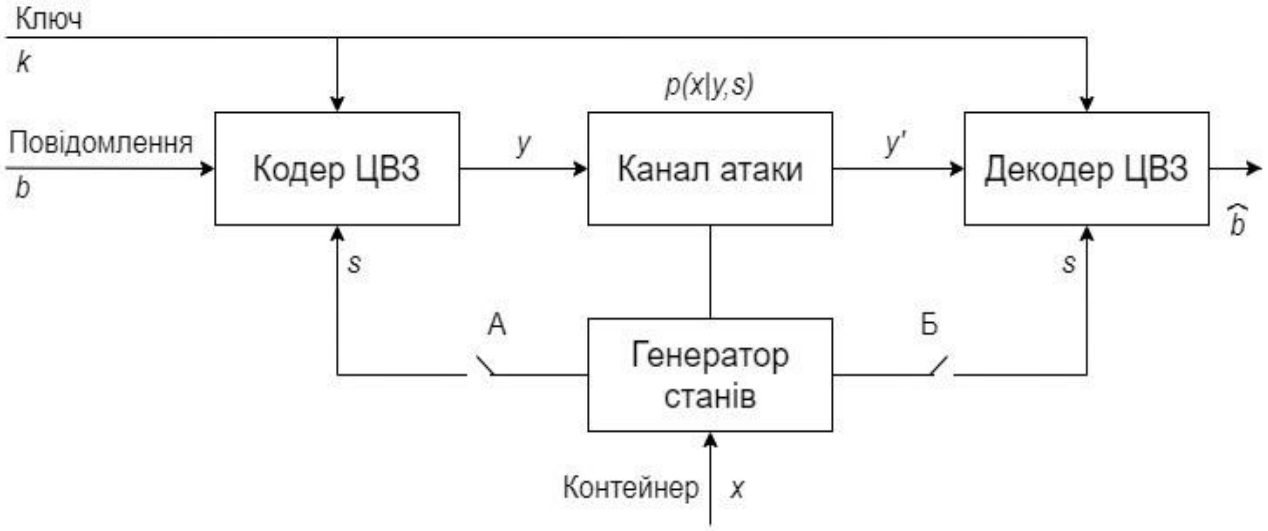

Рисунок 3.2 – Представлення стегосистеми як системи зв’язку з передачею додаткової інформації

І клас: додаткова інформація відсутня (перемикачі розімкнені) - "класичні" стегосистеми. У ранніх роботах по стеганографії вважалося, що інформація про канал недоступна кодеку. Виявлення ЦВЗ здійснювалося шляхом обчислення коефіцієнта кореляції між прийнятим стего і обчисленим за ключем ЦВЗ. Якщо коефіцієнт перевищував деякий поріг, виносилося рішення про присутність ЦВЗ. Відомо, що кореляційний приймач оптимальний лише в разі адитивної гауссової перешкоди. При інших атаках

(наприклад, геометричних спотвореннях) ці стегосистеми показували гірші результати.

II клас: інформація про канал відома тільки кодеру (А замкнутий, Б розімкнутий). Цікавою особливістю схеми є те, що, будучи сліпою, вона має ту ж теоретичну пропускну здатність, що і схема з наявністю вихідного контейнера в декодері. До недоліків стегосистем II класу можна віднести високу складність кодера (необхідність побудови кодової книги для кожного зображення), а також відсутність адаптації схеми до можливих атак. Останнім часом запропоновано ряд практичних підходів, що долають ці недоліки. Зокрема, для зниження складності кодера пропонується використовувати структуровані кодові книги, а декодер розраховувати на випадок найгіршої атаки.

III клас: додаткова інформація відома тільки декодеру (А розімкнутий, Б замкнутий). У цих схемах декодер будується з урахуванням можливих атак. В результаті виходять робастні до геометричних атак системи. Одним з методів досягнення цієї мети є використання так званого опорного ЦВЗ (аналог пілот-сигналу в радіозв'язку). Опорний ЦВЗ - невелике число біт, що впроваджуються в інваріантні до перетворення коефіцієнти сигналу. Наприклад, можна виконати вбудовування в амплітудні коефіцієнти перетворення Фур'є, які інваріантні до афінних перетворень. Тоді опорний ЦВЗ «покаже», яке перетворення виконав зі стего атакуючий. Іншим призначенням пілотного ЦВЗ є боротьба з завмираннями за аналогією з радіозв'язком. Завмираннями в даному випадку можна вважати зміну значень відліків сигналу при вбудовуванні даних, атаках, додаванні негауссівського шуму і т. д. В радіозв'язку для боротьби з завмираннями використовується метод рознесеного прийому (за частотою, часом, простором, кодом). У стеганографії ж використовується рознесення ЦВЗ по простору контейнера. Пілотний ЦВЗ генерується в декодері на основі ключа.

IV клас: додаткова інформація відома і в кодері і в декодері (обидва ключа замкнуті). Очевидно, всі перспективні стегосистеми повинні будуватися за цим принципом. Оптимальність цієї схеми досягається шляхом узгодження кодера з сигналом-контейнером, а також адаптивним управлінням декодером в умовах спостереження каналу атак.

3.2 Розробка схеми електричної структурної стеганосистеми на базі протоколу RTP

Метод вбудовування стеганоповідомлення базується на передачі бінарної послідовності довжини N у вигляді послідовності RTP-пакетів: переданий пакет відповідає одиничному біту, фантомний (навмисно пропущений) – нульовому (рис. 3.3). Часові проміжки t між RTP-пакетами вважаються рівними один одному.

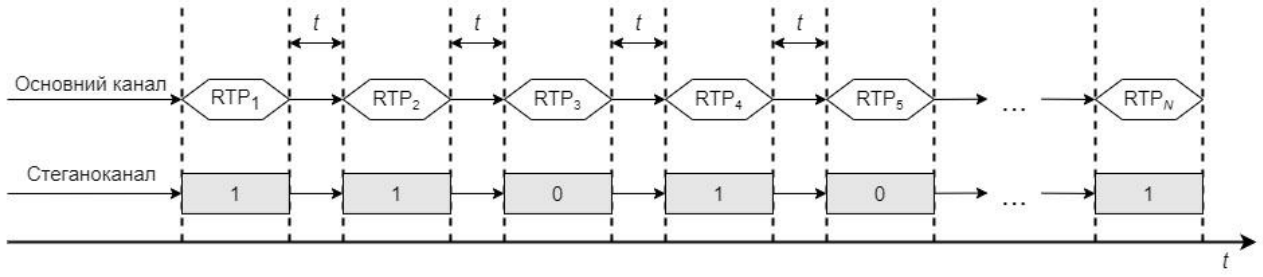

Рисунок 3.3 - Стеганоканал на базі RTP-потоку

Для ефективної передачі стеганоповідомлень подібним способом їх необхідно підготувати до передачі, додавши засоби контролю цілісності. Крім того, необхідно забезпечити прийнятну «зашумленість» RTP-потоку, щоб його характеристики змінювалися незначно. Дані вимоги реалізовані в запропонованій стеганосистемі.

Структурна схема побудови стеганосистеми, представлена на рис. 3.4, є практично класичною для мережевої стеганографії [10]. Відмінність полягає в тому, що, крім основного каналу передачі інформації - передавач-приймач, схема включає в себе і додатковий-керуючий канал зв'язку передавач-приймач, за допомогою якого здійснюється конфігурування стеганосистеми. Цим керуючим каналом може бути, наприклад, канал для управління пристроєм, з якго ведеться широкомовна передача.

Основним елементом передавача стеганосистеми є модулятор, який, використовуючи вихідні значення з таймера і генератора псевдовипадкових чисел (ГПВЧ), модулює стеганокодером основний канал-потік RTP-даних у відповідності з передаваним стеганоповідомленням. Зміни в основному каналі

виробляються передавачами стеганосистеми таким чином, щоб приймач, що має дзеркальну будову, мав можливість витягти стеганоповідомлення [9].

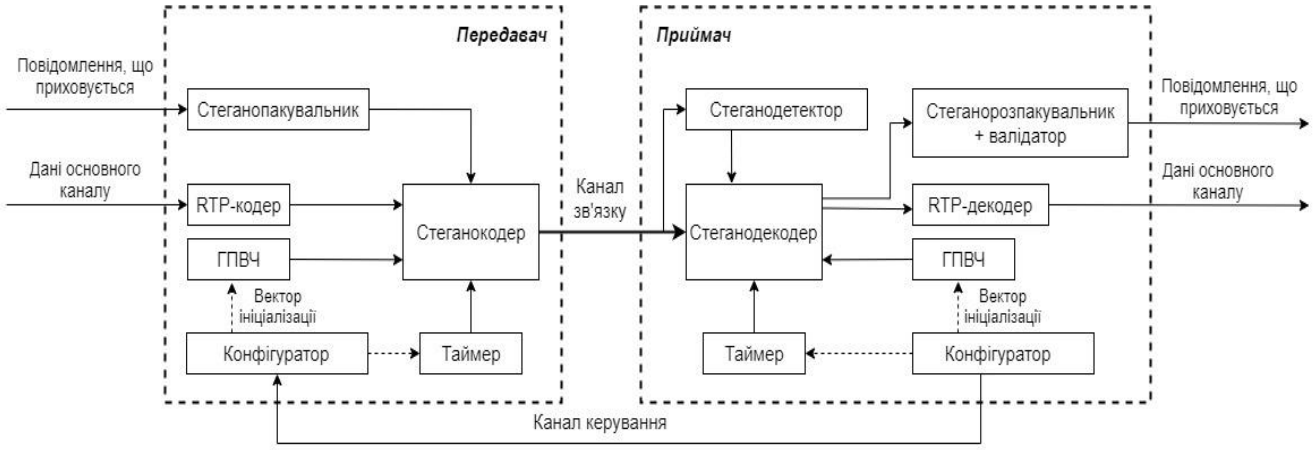

Рисунок 3.4 - Схема електрична структурна стеганосистеми на базі протоколу RTP

Стеганокодер в процесі модулювання RTP-потоку визначає, який пакет слід в дійсності передати, а який навмисно пропустити (зробити фантомним). Таймер на стороні передавача використовується для підтримки стабільності тимчасових затримок між усіма переданими RTP-пакетами (реальними і фантомними) - це необхідно для однозначної інтерпретації потоку на стороні приймача за допомогою синхронізованого з передавачем таймера. За допомогою конфігуратора на стороні передавача і приймача ініціалізується ГПВЧ і налаштовується таймер. Застосування в стеганосистемі ГПВЧ підвищує скритність каналу, так як забезпечує псевдовипадковість появи фантомних пакетів, а також збільшує конфіденційність, ускладнюючи витяг стеганоповідомлення з уже розкритого стеганоканалу. В якості ГПВЧ може бути використаний будь-який генератор, що має великий період.

Стеганодетектор призначений для ідентифікації передачі прихованого повідомлення в RTP-потоці. Стеганодекодер встановлює відповідність між бінарною послідовністю прихованого повідомлення, переданого по стеганоканалу, і потоком RTP-пакетів основного каналу [5].

Функціональна модель пропонованої стеганосистеми являє собою сукупність наступного виду:

$$\sum = (M, FC, SP, SUP, SV, Enc, Dec, PR, PC),$$

де M – множинність переданих прихованих повідомлень; FC - потоковий стеганоконтейнер (RTP-пакети); $SP: M \to GP$ - відображення прихованого повідомлення в бінарному вигляді в групи метапакетів (стеганопакувальник); $SUP: GP \to M$ - відображення груп метапакетів в приховане повідомлення в бінарному вигляді (стеганорозпакувальник); SV - валідатор, що забезпечує перевірку цілісності отриманого стеганоповідомлення; $Enc: GP \to FC$ - відображення груп метапакетів в потоковий стеганоконтейнер (стеганокодер); $Dec: FC \to GP$ - відображення потокового стеганоконтейнера в групи метапакетів; $PR = \{pr_1, pr_2, pr_3, pr_4\}$ - стек протоколів передачі стеганоповідомлення; PC - протокол керування.

У пропонованій моделі стеганосистеми взаємодію між приймачем і передавачем забезпечує оверлейний стек протоколів - PR, реалізований над протоколом RTP. На рис. 3.5 проілюстрована аналогія відповідності внутрішнього стека протоколів PR стеганосистеми та стека протоколів моделі OSI (вибраним її рівнями: 1, 3, 4, 6). Протокол pr_4, будучи протоколом верхнього рівня, представляє стеганоповідомлення у відкритому, бінарному вигляді. Протокол pr_3призначений для упаковки стеганоповідомлення в мета пакети - абстрактні сутності, призначені для передачі декількох біт стего з можливістю виявлення двох помилок і виправлення однієї. Протокол pr_2 організує групу метапакетів із заданою їх надмірністю (дублюванням в межах групи від 1 до n разів) і контролем цілісності, готової до подальшої передачі. Протокол pr_1 забезпечує передачу груп метапакетів за допомогою модулювання RTP –потоку [2].

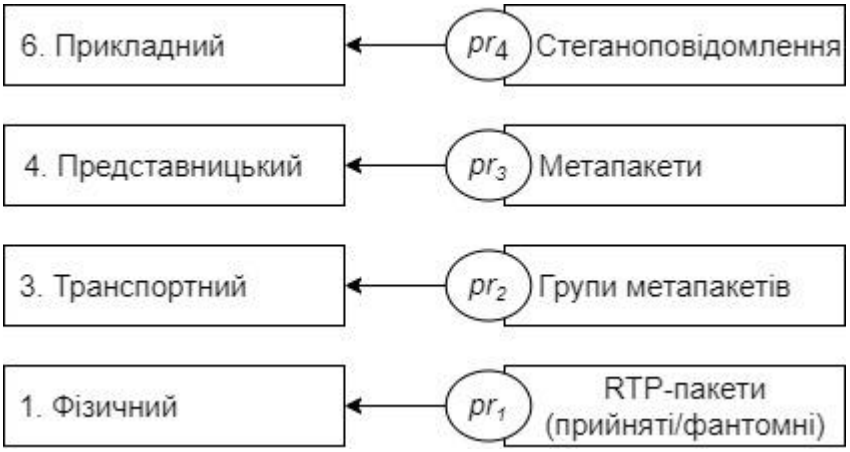

Рисунок 3.5 – Аналогія відповідності стеку протоколів стеганосистеми моделі OSI

Запропонуємо спрощений алгоритм взаємодії передавача та одержувача (рис. 3.6).

Рисунок 3.6 – Блок-схема алгоритму взаємодії передавача та приймача стеганосистеми на базі протоколу RTP

4 РОЗРОБКА СТРУКТУРНОЇ СХЕМИ ПРИСТРОЮ ЗАХИСТУ ІНФОРМАЦІЇ НА БАЗІ СТЕГАНОГРАФІЧНОГО АЛГОРИТМУ ВБУДОВУВАННЯ ЦИФРОВОГО ВОДЯНОГО ЗНАКУ

4.1 Розробка схеми електричної структурної стегоканалу зв’язку

Пристрій, показаний на рис. 4.1, складається з передавальної сторони першого пристрою і приймальної сторони другого пристрою, які взаємодіють через канал передачі. Передавальна сторона першого пристрою призначена для вирахування з електронного зображення (ЕЗ), що завіряється, цифрового водяного знака з використанням секретного ключа автентифікації і вбудовування його в це ж зображення з використанням секретного ключа вбудовування, а також передачі сформованого таким чином завіреного цифровим водяним знаком електронного зображення по каналу передачі. На передавальну сторону першого пристрою надходять електронне зображення, що завіряється, секретний ключ автентифікації і секретний ключ вбудовування. Вихід передавальної сторони 1-го пристрою через канал передачі з'єднаний з входом приймальної сторони другого пристрою. У каналі передачі порушником може здійснюватися перехоплення переданого відправником завіреного цифровим водяним знаком ЕЗ.

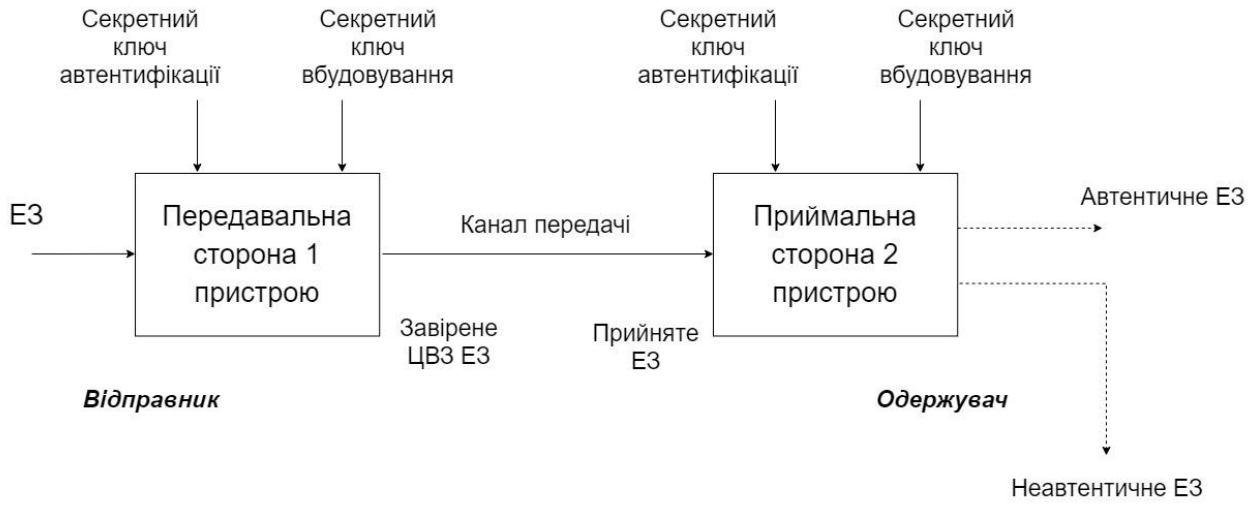

Рисунок 4.1 - Схема електрична структурна стегоканалу зв’язку

Порушник намагається витягти цифровий водяний знак із завіреного ЕЗ і витягнутий цифровий водяний знак вбудувати в помилкове ЕЗ, після чого порушник помилкове ЕЗ передає одержувачу по каналу передачі. Приймальна сторона другого пристрою призначена для прийому з каналу передачі ЕЗ, вилучення з прийнятого ЕЗ цифрового водяного знака з використанням секретного ключа вбудовування і перевірки його автентичності з використанням секретного ключа автентифікації. На приймальну сторону другого пристрою надходять секретний ключ автентифікації і секретний ключ вбудовування. Результат перевірки автентичності прийнятого електронного зображення зчитують з виходів приймальної сторони другого пристрою «автентичне ЕЗ» та «неавтентичне ЕЗ».

4.2 Розробка схеми електричної структурної пристрою вбудовування цифрового водяного знаку

Передавальна сторона першого пристрою (рис .4.2) складається з блоку розділення ЕЗ - 1, блоку перетворення Фур'є - 2, першого квантувача - 3, кодера Хаффмана - 4, першого виділювача співпадаючих послідовностей - 5, першого блоку пам'яті пар послідовностей - 6, першого лічильника співпадаючих послідовностей - 7, другого квантувача - 8, формувача послідовності блоку - 9, формувача автентифікатора блоку - 10, першого блоку пам'яті ключа автентифікації - 11, формувача ЦВЗ блоку - 12, суматора - 13, першого блоку пам'яті ключа вбудовування - 14, блоку вбудовування ЦВЗ - 15 та блоку передачі - 16.

М-розрядний вхід блоку перетворення Фур'є підключений до М-розрядного виходу блоку розділення ЕЗ, де $M \geq 2$, інформаційний вхід якого є інформаційним входом пристрою. Інформаційний вхід «ключ автентифікації» і вихід формувача автентифікатора блоку підключені відповідно до виходу першого блоку пам'яті ключа автентифікації і до інформаційного входу «автентифікатор блоку» формувача ЦВЗ блоку, вихід якого підключений до входу «ЦВЗ блоку» суматора, вихід якого підключений до інформаційного входу «підсумований ЦВЗ» блоку вбудовування цифрового водяного знака, вихід якого підключений до входу блоку передачі, вихід якого є виходом передавальної сторони пристрою.

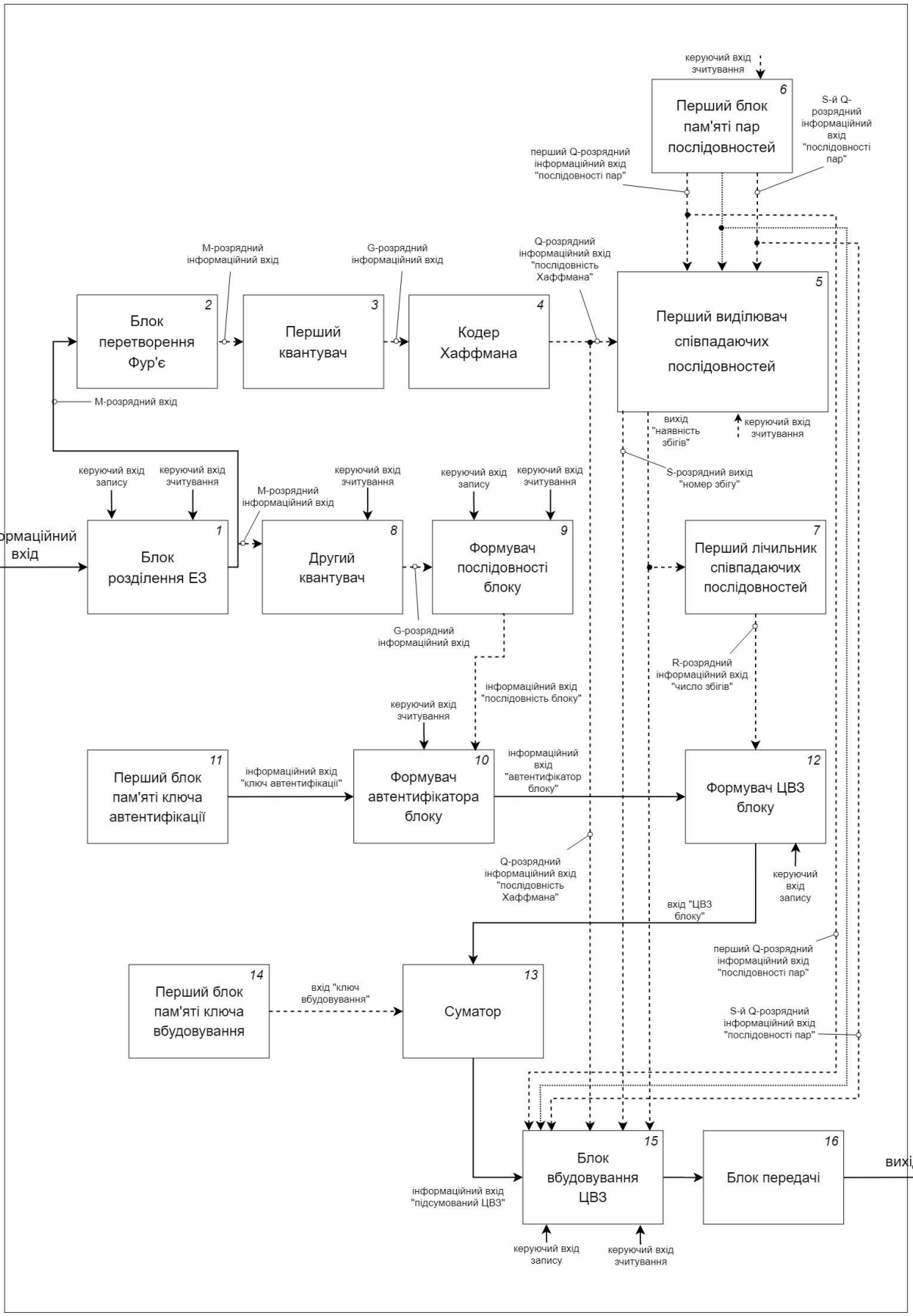

Рисунок 4.2 - Схема електрична структурна пристрою вбудовування цифрового водяного знаку

Вихід першого блоку пам'яті ключа вбудовування підключений до входу «ключ вбудовування» суматора. Вихід першого блоку пам'яті ключа вбудовування підключений до входу «ключ вбудовування» суматора.

М-розрядний вихід блоку розділення ЕЗ підключений до М-розрядного інформаційного входу другого квантувача, G-розрядний вихід якого підключений до G-розрядного інформаційного входу формувача послідовності блоку, де $\mathbf{2 \leq G \leq M}$, вихід якого підключений до інформаційного входу «послідовність блоку» формувача автентифікатора блоку. М-розрядний вихід блоку перетворення Фур'є підключений до М-розрядного інформаційного входу першого квантувача, G-розрядний вихід якого підключений до G-розрядного інформаційного входу кодера Хаффмана, Q-розрядний вихід якого підключений до Q-розрядного інформаційного входу «послідовність Хаффмана» першого виділювача співпадаючих послідовностей і до однойменного інформаційного входу блоку вбудовування ЦВЗ, де $\mathbf{Q \geq 2}$. S-розрядний вихід «номер збігу» першого виділювача співпадаючих послідовностей підключений до однойменного S-розрядного інформаційного входу блоку вбудовування ЦВЗ, де $\mathbf{S \geq 2}$. Вихід «наявність збігу» першого виділювача співпадаючих послідовностей підключений до однойменного інформаційного входу блоку вбудовування ЦВЗ і до входу першого лічильника співпадаючих послідовностей, R-розрядний вихід якого підключений до R-розрядного інформаційного входу «число збігів» формувача ЦВЗ блоку, де $\mathbf{R \geq \log_2(N \times N)}$. З першого по S-й Q-розрядні виходи першого блоку пам'яті пар послідовностей 6 підключені до відповідних Q-розрядних інформаційних входів «послідовності пар» першого виділювача співпадаючих послідовностей 5 і блоку вбудовування ЦВЗ. Причому блок розділення ЕЗ 1, перший кантувач 3, кодер Хаффмана 4, перший виділювач співпадаючих послідовностей 5, перший блок пам'яті пар послідовностей 6, другий кантувач 8, формувач послідовності блоку 9, формувач автентифікатора блоку 10 і блок вбудовування ЦВЗ 15 забезпечені керуючими входами зчитування, формувач ЦВЗ блоку 12 забезпечений керуючим входом запису, а блок розділення ЕЗ 1, формувач послідовності блоку 9 і блок вбудовування ЦВЗ 15 - забезпечені також керуючими входами запису, на які надходять відповідні сигнали керування від блоку керування (на схемі не показаний).

5 РОЗРОБКА СХЕМИ ЕЛЕКТРИЧНОЇ ФУНКЦІОНАЛЬНОЇ ПРИСТРОЮ ВБУДОВУВАННЯ ЦИФРОВОГО ВОДЯНОГО ЗНАКУ

Пристрій вбудовування цифрового водяного знаку (ПВЦВЗ), представлений на рис. 5.1, призначений для вбудовування підсумованого цифрового водяного знака блоку електронного зображення в цей же блок.

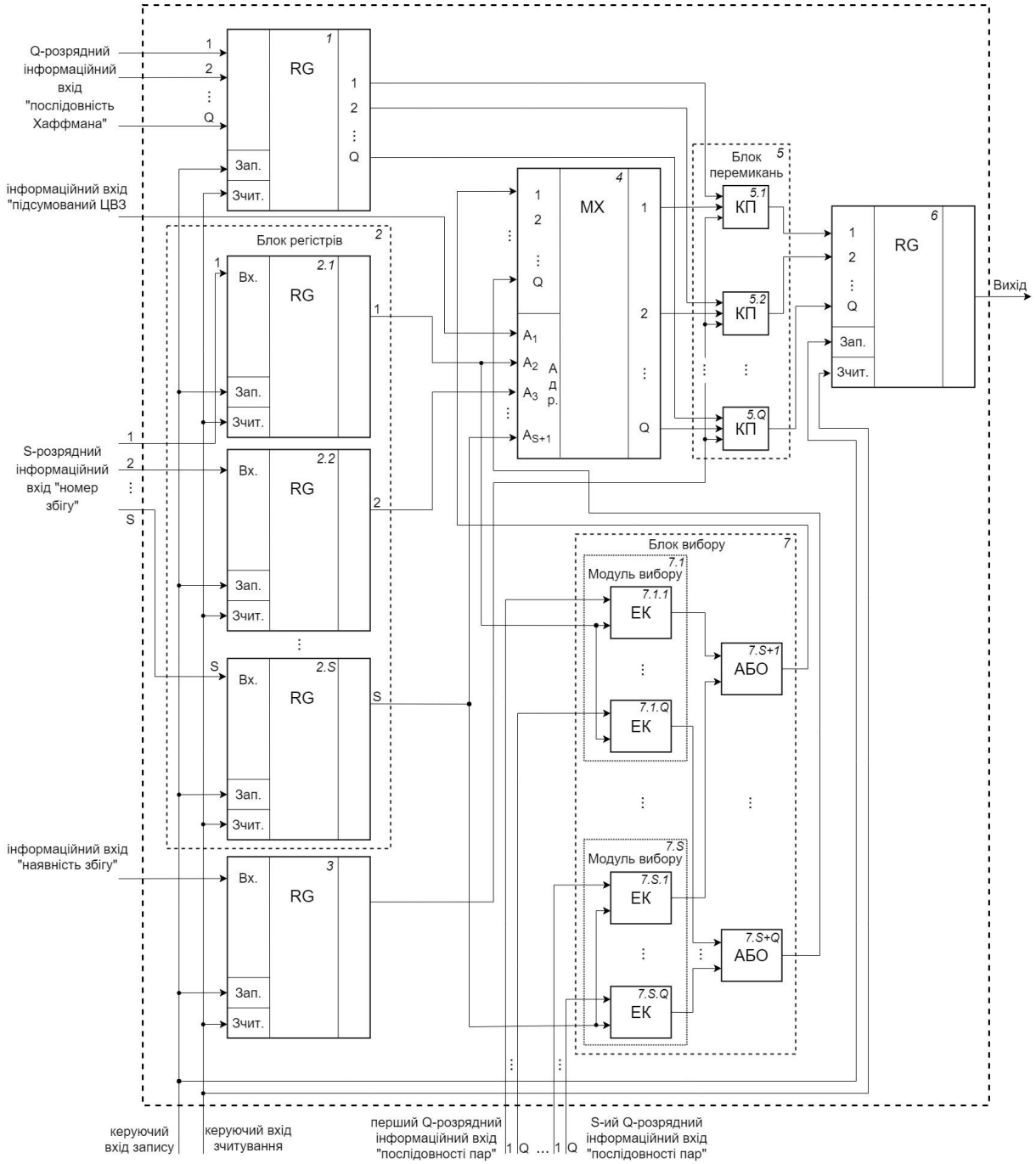

Рисунок 5.1 – Схема електрична функціональна пристрою вбудовування цифрового водяного знаку

ПВЦВЗ складається з регістрів зсуву (RG) - 1 і 3, блоку регістрів - 2, мультиплексора (МХ) - 4, блоку перемикань - 5, паралельно/послідовного регістра (RG) - 6 і блоку вибору - 7. Вхід регістра зсуву 1, реалізований у вигляді Q-розрядної шини з паралельною передачею, є Q-розрядним інформаційним входом «послідовність Хаффмана» ПВЦВЗ. Інформаційний вхід блоку регістрів, реалізований у вигляді S-розрядної шини з паралельною передачею, є S-розрядним інформаційним входом «номер збігу» ПВЦВЗ. Інформаційний вхід регістра зсуву 3 є інформаційним входом «наявність збігу». S Q-розрядних інформаційних входів блоку вибору 7 є відповідними Q-розрядними інформаційними входами «послідовності пар» ПВЦВЗ. Керуючий вхід «вибір молодшого розряду адреси» (A1) мультиплексора МХ є інформаційним входом «підсумований ЦВЗ». Керуючий вхід «вибір старших розрядів адреси» мультиплексора МХ (A2, A3,..., A_{S+1}), реалізований у вигляді S-розрядної шини з паралельною передачею, підключений до S-розрядного виходу блоку регістрів 2. Перший інформаційний вхід блоку перемикань 5, реалізований у вигляді Q-розрядної шини з паралельною передачею, підключений до виходу регістра зсуву 1. Вихід мультиплексора МХ, реалізований у вигляді Q-розрядної шини з паралельною передачею, підключений до другого інформаційного входу блоку перемикань 5. Вихід блоку вибору 7, реалізований у вигляді Q-розрядної шини з паралельною передачею, підключений до Q-розрядного інформаційного входу мультиплексора МХ. Керуючий вхід блоку перемикань 5 підключений до виходу регістра зсуву 3. Вихід блоку перемикань, реалізований у вигляді Q-розрядної шини з паралельною передачею, підключений до інформаційного входу паралельно/послідовного регістра 6, вихід якого є виходом ПВЦВЗ. Керуючий вхід запису ПВЦВЗ є керуючим входом запису регістрів зсуву 1, 3, блоку регістрів і паралельно/послідовного регістра 6. Керуючий вхід зчитування ПВЦВЗ є керуючим входом зчитування регістрів зсуву 1, 3, блоку регістрів 2 і паралельно/послідовного регістра 6.

Регістр зсуву 1 призначений для запису двійкових послідовностей коду Хаффмана блоку електронного зображення, що надходять на його інформаційний вхід, і подальшого їх зчитування на виході. Запис здійснюється при надходженні на його керуючий вхід запису керуючого сигналу запису,

зчитування здійснюється при надходженні на його керуючий вхід зчитування керуючого сигналу зчитування.

Блок регістрів 2 призначений для запису номерів послідовностей коду Хаффмана, що збіглися, блоку електронного зображення, які надходять на його інформаційний вхід, і подальшого їх зчитування на виході. Запис здійснюється при надходженні на його керуючий вхід запису сигналу запису, зчитування здійснюється при надходженні на його керуючий вхід зчитування сигналу зчитування. Блок регістрів складається з S однакових регістрів зсуву (RG) 2.1, 2.2, ..., 2.S. Керуючі входи запису та керуючі входи зчитування регістрів зсуву 2.1, 2.2, ..., 2.S підключені до відповідних керуючих входів блоку регістрів 2. Схема регістрів зсуву 2.1, 2.2, ..., 2.S аналогічна, наприклад, схемі регістра зсуву 1, описаній раніше.

Регістр зсуву 3 призначений для запису послідовності двійкових значень, що надходять на його інформаційний вхід «наявність збігу», з однойменного виходу першого виділювача послідовностей, що збіглися, і подальшого її зчитування на виході. Запис здійснюється при надходженні на його керуючий вхід запису керуючого сигналу запису, зчитування здійснюється при надходженні на його керуючий вхід зчитування керуючого сигналу зчитування.

Мультиплексор МХ призначений для вибору двійкової послідовності з пар двійкових послідовностей, що надходять на його Q-розрядний інформаційний вхід. Вибір здійснюється у відповідності з адресними сигналами, що складаються з сигналу вибору молодшого розряду адреси (A1), що надходить на керуючий вхід «вибір молодшого розряду адреси» мультиплексора 4, і сигналів вибору старших розрядів адреси (A2, A3, ..., A_{S+1}), що надходять на керуючий вхід «вибір старших розрядів адреси» цього мультиплексора. Обрана двійкова послідовність з виходу мультиплексора 4, реалізованого у вигляді Q-розрядної шини з паралельною передачею, надходить на другий інформаційний вхід блоку перемикань 5.

Блок перемикань 5 призначений для підключення одного зі своїх двох інформаційних входів на вихід відповідно до значення керуючого сигналу, що надходить на його керуючий вхід. Якщо керуючий сигнал має нульове двійкове значення, то на вихід підключається перший інформаційний вхід блоку перемикань 5. Якщо керуючий сигнал має одиничне двійкове значення,

то на вихід підключається другий інформаційний вхід. Блок перемикань складається з Q однакових керуючих перемикачів (КП) 5.1, 5.2, ..., 5.Q.

Паралельно/послідовний регістр 6 призначений для перетворення паралельно зчитуваних двійкових сигналів на його Q-розрядному інформаційному вході в послідовний двійковий сигнал на його виході. Запис в паралельно/послідовний регістр 6 виконується при надходженні на його керуючий вхід запису керуючого сигналу запису, а зчитування - при надходженні на його керуючий вхід зчитування керуючого сигналу зчитування.

Блок вибору 7 призначений для вибору з S Q-розрядних інформаційних входів «послідовності пар» ПВЦВЗ у відповідності з сигналом на S-розрядному виході блоку регістрів 2 і підключення обраного Q-розрядного інформаційного входу «послідовності пар» ПВЦВЗ до Q-розрядного інформаційного входу мультиплексора 4. Блок вибору складається з S однакових модулів вибору 7.1, ..., 7.S і Q однакових схем об'єднання 7.S+1, …, 7.S+Q. Q-розрядний інформаційний вхід модуля вибору 7.1 підключений до першого Q-розрядного інформаційного входу «послідовності пар» ПВЦВЗ і так далі, Q-розрядний інформаційний вхід модуля вибору 7.S підключений до S-го Q-розрядного інформаційного входу «послідовності пар» ПВЦВЗ і т.д. Керуючий вхід модуля вибору 7.1 підключений до виходу регістра зсуву 2.1 блоку регістрів і так далі, керуючий вхід модуля вибору 7.S підключений до виходу регістра зсуву 2.S блоку регістрів. Перші виходи модулів вибору 7.1, ..., 7.S підключені до однойменних входів схеми об'єднання 7.S+1 і так далі, Q-і виходи модулів вибору 7.1,..., 7.S підключені до однойменних входів схеми об'єднання 7.S+Q.

Кожен модуль вибору 7.1, ..., 7.S складається з Q електронних ключів (ЕК) 7.1.1, ..., 7.1.Q, …, 7.S.1, …, 7.S.Q, призначених для підключення відповідного розряду відповідного Q-розрядного інформаційного входу «послідовності пар» ПВЦВЗ. Інформаційні входи електронних ключів 7.1.1, ..., 7.1.Q є Q-розрядним інформаційним входом модуля вибору 7.1 і т.д. З'єднані між собою керуючі входи електронних ключів 7.1.1, ..., 7.1.Q є керуючим входом модуля вибору 7.1 і т. д.

Схема об'єднання 7.S+1 призначена для об'єднання сигналів з виходів електронних ключів 7.1.1, ..., 7.S.1 і підключення вихідного сигналу на перший

розряд Q-розрядного інформаційного входу мультиплексора 4 і так далі, схема об'єднання 7.S+Q призначена для об'єднання сигналів з виходів Q в своєму модулі вибору електронних ключів 7.1.Q, …, 7.S. Q і підключення вихідного сигналу на Q розряд Q-розрядного інформаційного входу цього ж мультиплексора.

ВИСНОВОК

В процесі виконання роботи був здійснений огляд та проведений аналіз існуючих методів впровадження ЦВЗ, а також дослідження особливостей зорової системи людини, що дозволив розробити пристрій для вбудовування та зчитування цифрового водяного знаку. Підіб'ємо підсумки виконання даної роботи:

- розглянуто проблему захисту авторського права на електронне зображення, що підтверджує актуальність робіт, пов'язаних з методами впровадження секретної інформації в зображення;
- описано загальний принцип побудови стегосистеми;
- проведено аналіз сучасних методів забезпечення автентичності зображень, що включає їх класифікацію і короткий опис;
- на основі проведеного аналізу виявлено найбільш ефективні методи вбудовування цифрового водяного знаку в нерухоме електронне зображення та RTP-потік для розробки власного пристрою, засновані на відкритій стегосистемі;
- проведено дослідження параметрів стегосистеми;
- ґрунтуючись на отриманих даних, розроблено структурні електричні та функціональні схеми пристрою захисту інформації на базі стеганографічного алгоритму.

Запропонований пристрій відноситься до області електрозв'язку та інформаційних технологій, а саме до техніки захисту автентичності електронних зображень, переданих відправником одержувачу по загальнодоступних каналах передачі, в яких порушник може здійснювати дії по нав'язуванню одержувачу помилкових електронних зображень. Заявлені структурні електричні та функціональні схеми можуть бути використані для подальшої технічної реалізації пристрою для встановлення автентичності електронних зображень, що передаються в сучасних інформаційно-телекомунікаційних системах.

СПИСОК ЛІТЕРАТУРИ

1. Mazurczyk W., Wendzel S., Zander S., Houmansadr A., Szczypiorski K. Information Hiding in Communication Networks: Fundamentals, Mechanisms, Applications, and Countermeasures. Wiley, 2016, 296 p.
2. Janicki A., Karas M., Mazurczyk W., Szczypiorski K. YouSkyde: information hiding for Skype video traffic // Multimedia Tools and Applications. 2016. V. 75. N 21. P. 13521–13540.
3. Gutierrez-Cardenas J.M. Steganography and data loss prevention: an overlooked risk? // International Journal of Security and Its Applications. 2017. V. 11. N 4. P. 71–84.
4. Nayak MR, Tudu B, Basu A, Sarkar SK (2015) On the implementation of a secured digital watermarking frame work. Inf Secur J Glob Perspect 24(1):1–9.
5. S. M. Sakthivel and A. Ravi Sankar, “A real time watermarking of grayscale images without altering it's content,” in Proceedings of the 2015 International Conference on VLSI Systems, Architecture, Technology and Applications, VLSI-SATA 2015, IEEE, January 2015.
6. D. Kahn, The Code-Breakers: The Story of Secret Writing. MacMillan Publishing Company, New York, USA, 1996.
7. Грибунин В.Г., Оков И.Н., Туринцев И.В. Цифровая стеганография М.: Солон-Пресс, 2009.
8. Конахович Г. Ф., Пузыренко А. Ю. Компьютерная стеганография. Теория и практика.— К.: "МК-Пресс", 2006. — 288 с, ил.
9. Шипулин П.М., Козин В.В., Шниперов А.Н. Метод организации скрытого канала передачи информации на основе протокола потоковой передачи данных // Научно-технический вестник информационных технологий, механики и оптики. 2018. Т. 18. № 5. С. 834–842.
10. Белкина Т. А. Аналитический обзор применения сетевой стеганографии для решения задач информационной безопасности. «Молодой ученый» № 11, 2018.
11. Белобокова Ю.А. Метод встраивания цифровых водяных знаков для доказательства подлинности фотоизображений./Белобокова Ю.А.

//Известия Тульского государственного университета. / Тула: «Известия ТулГУ» Технические науки, выпуск 3 , 2013.

12. Хорошко В.О., Азаров О.Д., Шелест М.Є., Яремчук Ю.Є. Основи комп’ютерної стеганографії : Навчальний посібник для студентів і аспірантів. — Вінниця:ВДТУ, 2003. — 143 с.
13. Голубєв В.О., Гавловський В.Д., Цимбалюк В.С. Інформаційна безпека: проблеми боротьби зі злочинами у сфері використання комп’ютерних технологій.— Запоріжжя: Просвіта, 2001. — с.198-201.