НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ

«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ

імені ІГОРЯ СІКОРСЬКОГО»

Факультет електроніки
(повна назва інституту/факультету)

Звукотехніки та реєстрації інформації
(повна назва кафедри)

«На правах рукопису»

УДК 681.3.06

«До захисту допущено»

Завідувач кафедри

_____ Власюк А.Г.

(підпис) (ініціали, прізвище)

“___”_____2018р.

Магістерська дисертація

на здобуття ступеня магістра

зі спеціальності 171 Електроніка. Спеціалізація - Електронні та інформаційні системи і технології телебачення, кінематографії та звукотехніки
(код і назва)

на тему: Дослідження особливостей стеганографічних методів у разі використання відеоконтейнерів

Виконав (-ла): студент (-ка) __6__ курсу, групи ___ДВ-71мп_____
(шифр групи)

Гламаздін Владислав Владиславович _____ _____
(прізвище, ім’я, по батькові) (підпис)

Науковий керівник професор, д.т.н., Савченко Ю.Г _____ _____
(посада, науковий ступінь, вчене звання, прізвище та ініціали) (підпис)

Рецензент _____ _____
(посада, науковий ступінь, вчене звання, науковий ступінь, прізвище та ініціали) (підпис)

Засвідчую, що у цій магістерській дисертації немає запозичень з праць інших авторів без відповідних посилань.
Студент _____
(підпис)

Київ – 2018 року

НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ

«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ

імені ІГОРЯ СІКОРСЬКОГО»

Інститут (факультет)_____Факультет електроніки
(повна назва)

Кафедра_____Звукотехніки та реєстрації інформації
(повна назва)

Рівень вищої освіти – другий (магістерський) за освітньо-професійною програмою

Спеціальність 171 Електроніка. Спеціалізація - Електронні та інформаційні системи і технології телебачення, кінематографії та звукотехніки _____
(код і назва)

ЗАТВЕРДЖУЮ
Завідувач кафедри

_____ Власюк А.Г.

(підпис) (ініціали, прізвище)

“___”_____2018р

ЗАВДАННЯ
на магістерську дисертацію студенту
Гламаздіну Владиславу Владиславовичу
(прізвище, ім’я, по батькові)

1. Тема дисертації Дослідження особливостей стеганографічних методів у разі використання відеоконтейнерів _____,
науковий керівник дисертації Савченко Юлій Григорович, д.т.н., професор ,
(прізвище, ім’я, по батькові, науковий ступінь, вчене звання)

затверджені наказом по університету від «_07_»_листопада_ 2018 р. № 4114-с

2. Термін подання студентом дисертації 10.12.2018р._____

3. Об’єкт дослідження особливості стеганографічних методів у разі використання відеоконтейнерів _____

4. Предмет дослідження Методи та засоби стеганографії у разі використання відеоконтейнерів _____

5. Перелік завдань, які потрібно розробити: 1. Проаналізувати джерела цифрового шуму в файлах, які використовуються в якості контейнерів 2. Опрацювати основні методи стеганографії при використанні відеоконтейнерів.3.

Розглянути джерела шуму, які можуть виявитися корисними для збільшення корисного об'єму контейнера

6. Перелік ілюстративного матеріалу 17 рис., 22 табл., 1 перентація.
7. Орієнтовний перелік публікацій: Використання методу найменш значущого біта (НЗБ) для приховування інформаціїв відеофайлах.

8. Консультанти розділів дисертації

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв

9. Дата видачі завдання 10.09.2017

Календарний план

№ з/п	Назва етапів виконання магістерської дисертації	Термін виконання етапів магістерської дисертації	Примітка
1	Написання першого розділу	10.10.17	
2	Написання другого розділу	15.12.17	
3	Написання третього розділу	01.05.18	
4	Написання четвертого розділу	10.10.18	
5	Підготовка матеріалів до друку та оформлення пояснювальної записки	25.11.18	
6	Підготовка та оформлення презентації для доповіді	30.11.18	

Студент _____ В.В.Гламаздін
(підпис) (ініціали, прізвище)

Науковий керівник дисертації _____ Ю.Г.Савченко
(підпис) (ініціали, прізвище)

УДК 681.3.06

Реферат

Магістерська дисертація: 101 с., 17 рис., 22 табл., 1 додаток, 16 джерел.

СТЕГАНОГРАФІЯ; ПРИХОВУВАННЯ ІНФОРМАЦІЇ; СТЕГАНОКАНАЛ; ГЕНЕРАТОР ПСЕВДОВИПАДКОВИХ ЧИСЕЛ (ГПВЧ); ШТУЧНЕ ЗАШУМЛЕННЯ; СТЕГАНОАНАЛІЗ; ДИСКРЕТНО-КОСИНУСНОЕ ПЕРЕТВОРЕННЯ; МЕТОД НАЙМЕНШ ЗНАЧУЩОГО БІТА (НЗБ); ВЕЙВЛЕТ-ПЕРЕТВОРЕННЯ.

Актуальність роботи полягає у необхідності використовувати прихований інформаційний обмін в системах спеціального призначення, а також в ситуаціях, коли несанкціонований або небажаний доступ до інформації повинен бути закритий (наприклад, з огляду на лікарську таємницю). На сьогоднішній день комп'ютерна стеганографія пропонує нові методи захисту інформаційних ресурсів, застосовуються відомі і розробляються нові методи стеганографії, що базуються на результатах різноманітних областей науки. Стеганографічні системи переходять в нову фазу свого розвитку, сьогодні вже велика їх частина при приховуванні інформації враховує характеристики і природу стеганоконтейнерів.

Об’єктом дослідження є особливості стеганографічних методів у разі використання відеоконтейнерів.

Метою роботи є оцінка впливу штучного внесення шумовий складової для збільшення пропускної здатності стеганоканала та виявлення головних переваг і недоліків пропонованого підхода.

Для досягнення поставленої мети необхідно виконати такі завдання:

- проаналізувати джерела цифрового шуму в файлах, які використовуються в якості контейнерів;

- розглянути джерела шуму, які можуть виявитися корисними для збільшення корисного об'єму контейнера;

- провести аналіз відомих методів, з використанням різних контейнерів;

SUMMARY

Master's dissertation:101 p., 17 pick, 22 tabl, 1 supplement, 16 sources.

STEGANOGRAPHY; RESPONSIBILITY OF INFORMATION; STEGANOCANAL; GENERATOR OF PENALTY-BASED NUMBERS (GVVCH); ARTIFICIAL INTERVENTION; STEGANOANALIZE; DISCRETE-COROSS CONVERTER; METHOD TO DETERMINE A SIGNIFICANT BAT (NZB); WAVEEL-TRANSFORMATION.

The urgency of the work is the need to use hidden information exchange in special purpose systems, as well as in situations where unauthorized or unwanted access to information should be closed (for example, due to medical secret). To date, computer steganography offers new methods for the protection of information resources, known and developed new methods of steganography, based on the results of various fields of science. Steganography systems are moving into a new phase of their development, today their large part in concealing information takes into account the characteristics and nature of steganocontainers.

The object of research is the peculiarities of steganographic methods in the case of use of video containers.

The purpose of the work is to evaluate the effect of artificial noise pollution in order to increase the flow capacity of the steganokanal and to identify the main advantages and disadvantages of the proposed approach.

To achieve the goal you must accomplish the following tasks:

- analyze the sources of digital noise in the files used as containers;
- consider noise sources that may be useful for increasing the useful volume of the container;
- to carry out the analysis of known methods, using different containers;

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

ЦВЗ	цифровий водяний знак
ДКП	дискретне косинусне перетворення
НЗБ	найменший значущий біт
ЗСЛ	зорова система людини
ПВЧ	псевдо-випадкове число
ПВФ	псевдо-випадкова функція
ПВП	псевдо-випадкова послідовність
РСПП	розширення спектру (сигналу) прямою послідовністю

ВСТУП

Актуальність роботи полягає у необхідності використовувати прихований інформаційний обмін в системах спеціального призначення, а також в ситуаціях, коли несанкціонований або небажаний доступ до інформації повинен бути закритий (наприклад, з огляду на лікарську таємницю). На сьогоднішній день комп'ютерна стеганографія пропонує нові методи захисту інформаційних ресурсів, застосовуються відомі і розробляються нові методи стеганографії, що базуються на результатах різноманітних областей науки. Стеганографічні системи переходять в нову фазу свого розвитку, сьогодні вже велика їх частина при приховуванні інформації враховує характеристики і природу стеганоконтейнерів.

Об’єктом дослідження є особливості стеганографічних методів у разі використання відеоконтейнерів.

Метою роботи є оцінка впливу штучного внесення шумовий складової для збільшення пропускної здатністі стеганоканала та виявлення головних переваг і недоліків пропонованого підхода.

Для досягнення поставленої мети необхідно виконати такі завдання:

- проаналізувати джерела цифрового шуму в файлах, які використовуються в якості контейнерів;

- розглянути джерела шуму, які можуть виявитися корисними для збільшення корисного об'єму контейнера;

- провести аналіз відомих методів, з використанням різних контейнерів;

Наукова новизна роботи:

- Запропоновано методику обчислення побітової різниці між вихідним файлом і його модифікацією з вкладенням прихованої інформації;
- сформульовано рекомендації щодо використання та вибору найбільш раціонального методу в залежності від поставленого завдання.

Практичне значення роботи полягає в обгрунтованому підході до наявності у вихідних контейнерах шумових складових і оцінка збільшення пропускної здатності каналу за рахунок штучного внесення шумової складової в вихідне зображення, що збільшує пропускну здатність стеганоканала.

РОЗДІЛ 1 СТЕГАНОГРАФІЯ

Бурхливий розвиток комп’ютерних і телекомунікаційних мереж сприяв значному підвищенню обсягів передавання інформації, і проблема її захисту постала на перше місце. В даний час комп'ютери і комп'ютерні системи (КС) рідко використовуються автономно. Вони частіше утворюють локальну, корпоративну або глобальну мережі . У базі даних КС вже сформовані великі об'єми інформації, які мають меншу або більшу цінність. Її знищення, спотворення або несанкціоноване використання може привести до великих економічних втрат.

Однією з найбільш складних проблем, що стримує темпи інформатизації суспільства, є необхідність пріоритетного забезпечення питань державної безпеки (соціальної, економічної, екологічної і військово-стратегічної) в умовах широкого застосування засобів обчислювальної техніки для обробки цінної, конфіденційної і секретної інформації в державних і приватних підприємствах, в органах і установах державного управління, а також в банківській і біржовій інфраструктурах.

Інформаційна безпека має велике значення для забезпечення життєво важливих інтересів будь-якої держави. Створення розвиненого і захищеного середовища є неодмінною умовою розвитку суспільства та держави, в основі якого мають бути найновіші автоматизовані технічні засоби.

Останнім часом в Україні відбуваються якісні зміни у процесах управління на всіх рівнях, які зумовлені інтенсивним упровадженням новітніх інформаційних технологій. Швидке вдосконалення інформатизації, проникнення її в усі сфери життєво важливих інтересів зумовило, крім безперечних переваг, і появу низки стратегічних проблем. Посилюється небезпека несанкціонованого втручання в роботу комп'ютерних, інформаційних і телекомунікаційних систем.

Наскільки актуальна проблема захисту інформації від різних загроз, можна побачити на прикладі даних, опублікованих Computer Security Institute (Сан-Франциско, штат Каліфорнія, США), згідно з якими порушення захисту комп'ютерних систем відбувається з таких причин:

несанкціонований доступ — 2 %

укорінення вірусів — 3 %;

технічні відмови апаратури мережі — 20 %;

цілеспрямовані дії персоналу — 20 %;

помилки персоналу (недостатній рівень кваліфікації) — 55%.

Таким чином, однією з потенційних загроз для інформації в інформаційних системах слід вважати цілеспрямовані або випадкові деструктивні дії персоналу (людський фактор), оскільки вони становлять 75 % усіх випадків.

Відповідно до вимог законів України "Про інформацію", "Про державну таємницю" та "Про захист інформації в автоматизованих системах" основним об'єктом захисту в інформаційних системах є інформація з обмеженим доступом, що становить державну або іншу, передбачену законодавством України, таємницю, конфіденційна інформація, що є державною власністю чи передана державі у володіння, користування, розпорядження.

Загалом, об'єктом захисту в інформаційній системі є інформація з обмеженим доступом, яка циркулює та зберігається у вигляді даних, команд, повідомлень, що мають певну обмеженість і цінність як для її власника, так і для потенційного порушника технічного захисту інформації[1].

1.1 Криптографія

Тривалий час під криптографією розумілось лише шифрування - процес перетворення звичайної інформації (відкритого тексту) в незрозумілий набір символів (літер, цифр тобто, шифротекст). Дешифрування - зворотний процес відтворення інформації із шифротексту. Шифром називається пара алгоритмів шифрування/розшифрування. Дія шифру керується як алгоритмами, та, в кожному випадку, ключем. Ключ - секретний параметр (в ідеалі, відомий лише двом сторонам) для окремого контексту під час передачі повідомлення. Ключі мають велике значення, оскільки без змінних ключів алгоритми шифрування легко зламуються і непридатні для використання в більшості випадків. Історично склалось так, що шифри часто використовуються для шифрування та

дешифрування без виконання додаткових процедур, таких як аутентифікація або перевірка цілісності[2].

1.2 Інформаційна система як об'єкт захисту

Розвиток сучасних інформаційних технологій супроводжується зростанням числа комп'ютерних злочинів і пов'язаних з ними розкрадань інформації, а також матеріальних втрат. За результатами одного дослідження близько 58% опитаних постраждали від комп'ютерних зламів за останній рік. Приблизно 18% опитаних з цього числа заявляють, що втратили більше мільйона доларів в ході нападів, більше 66% зазнали збитків у розмірі 50 тис. доларів. Понад 22% атак були націлені на промислові секрети або документи, що представляють інтерес насамперед для конкурентів.

Інформаційні ресурси, тобто окремі документи або масиви документів, у тому числі і в інформаційних системах, будучи об'єктом відносин фізичних, юридичних осіб і держави, підлягають обов'язковому обліку та захисту, як будь-яке матеріальне майно власника. При цьому власникові надається право самостійно в межах своєї компетенції встановлювати режим захисту інформаційних ресурсів і доступу до них.

Норми, згідно яких відомості відносяться до категорії конфіденційних, встановлює і цілі захисту інформації:

- запобігання витоку, розкрадання, спотворення, підробки інформації;
- запобігання несанкціонованого знищення та блокування інформації;
- збереження державної таємниці, конфіденційності документованої інформації.

Стандарти і рекомендації статичні, причому статичні, принаймні, у двох аспектах. По-перше, вони не враховують постійної перебудови систем та їх оточення. По-друге, вони не містять практичних рекомендацій щодо формування режиму безпеки. Інформаційну безпеку не можна купити, її доводиться щодня підтримувати, взаємодіючи при цьому не тільки і не стільки з комп'ютерами, скільки з людьми.

Таким чином, стандарти і рекомендації не дають відповідей на два головні, з практичної точки зору, питання:

1. Як здобувати (комплектувати) інформаційну систему масштабу, наприклад, підприємства, щоб її можна було зробити безпечною?
2. Як практично сформувати режим безпеки і підтримувати його в умовах постійно мінливого оточення і структури самої системи?

Іншими словами, стандарти і рекомендації є лише відправною точкою на довгому і складному шляху захисту інформаційних систем організацій. Для підтримки режиму інформаційної безпеки особливо важливі апаратно-програмні заходи, оскільки основна загроза комп'ютерних систем виходить від самих цих систем (збої обладнання, помилки програмного забезпечення, промахи користувачів і адміністраторів і т.п.)[3].

1.3 Проблеми захисту інформації

Сьогодні інформацію розглядають як один з основних ресурсів розвитку суспільства, а інформаційні системи і технології як засіб підвищення продуктивності та ефективності роботи людей. Тому інформація є найціннішим і дорогим ресурсом. Інформаційна технологія визначає процеси передачі та розповсюдження, зберігання і обробки інформації, а так само її використання в певних цілях. Ясно, що ці процеси повинні бути швидкими, найменш витратними, максимально корисними, зручними і автоматизованими. З цієї причини основною тенденцією розвитку інформаційних технологій є їх представлення в цифровому вигляді, перехід до цифрових телекомунікаційно-інформаційних баз, що базуються на цифровій (розподіленій) взаємодії комп'ютерів, розроблених з найрізноманітніших функціональним алгоритмами. Впровадження персональних комп'ютерів в інформаційну сферу й застосування телекомунікаційних засобів зв'язку визначили новий етап розвитку інформаційної технології - нової (або сучасної) інформаційної технології. Комп'ютерні телекомунікації - тип інформаційних технологій, що використовують глобальні комп'ютерні мережі, зокрема Інтернет. Інтернет та інформаційна безпека несумісні по самій природі

мережі Інтернет. Ця мережа об'єднує поряд з мережами з обмеженим доступом (комерційних, освітніх, державних, військових та інших організацій) і рядових користувачів, які мають можливість отримати прямий доступ в Інтернет зі своїх домашніх комп'ютерів, використовуючи модем і телефонну мережу загального користування. Первісна простота доступу в Інтернет загрожує безпеці локальної мережі та конфеденційності інформації, що міститься в ній. За допомогою програмних портів, через які і здійснюється взаємодія комп'ютера з Інтернет, будь-хто теоретично може проникнути в саме серце комп'ютера і отримати над ним повний контроль. За результатами опитування, проведеного Computer Security Institute (CSI) серед 500 найбільш великих організацій, компаній і університетів з 1991 року число незаконних вторгнень зросло на 48,9%, а втрати, викликані цими атаками оцінюються в 66 млн. доларів США. Можливість доступу до комерційних архівними даними організації може їй дуже дорого коштувати, тому, підключаючись до мережі Інтернет, слід провести аналіз ризику і скласти план захисту інформаційної системи. Для запобігання несанкціонованого доступу до даних доцільно ставити фільтри (фейрволли) між внутрішньою мережею та Інтернет. Фейрволли (firewall) можуть бути реалізовані програмно або апаратно. Серед програм, що відносяться до класу фейрволлов або брандмауерів - міжмережевих екранів, популярністю користуються такі як ZoneAlarm, Outpost, KasherskyAntiHacker та інші. Таким чином, необхідний комплексний підхід до інформаційної безпеки організацій. Інформаційна безпека повинна розглядатися як складова частина загальної безпеки організації, причому як важлива і невід'ємна її частина. Необхідно розробити концепцію інформаційної безпеки, в якій слід передбачити не лише заходи, пов'язані з інформаційними технологіями (криптозахист, програмні засоби адміністрування прав користувачів, їхньої ідентифікації і аутентифікації, брандмауери для захисту входів-виходів мережі і т. п.), але і міри адміністративного і технічного характеру.

Уразливість інформації є стан, що виникає як результат такого збігу обставин, коли в силу якихось причин використовувані в автоматизованих системах обробки даних засоби захисту не в змозі надати достатньої протидії прояву дестабілізуючих факторів і небажаного їх впливу на інформацію, що

захищається. Модель уразливості інформації в мережах зв'язку в загальному вигляді показана на рис.1.1.

Дана модель деталізується при вивченні конкретних видів вразливості інформації: порушення фізичної або логічної цілісності, несанкціонованої модифікації, несанкціонованого отримання, несанкціонованого розмноження.

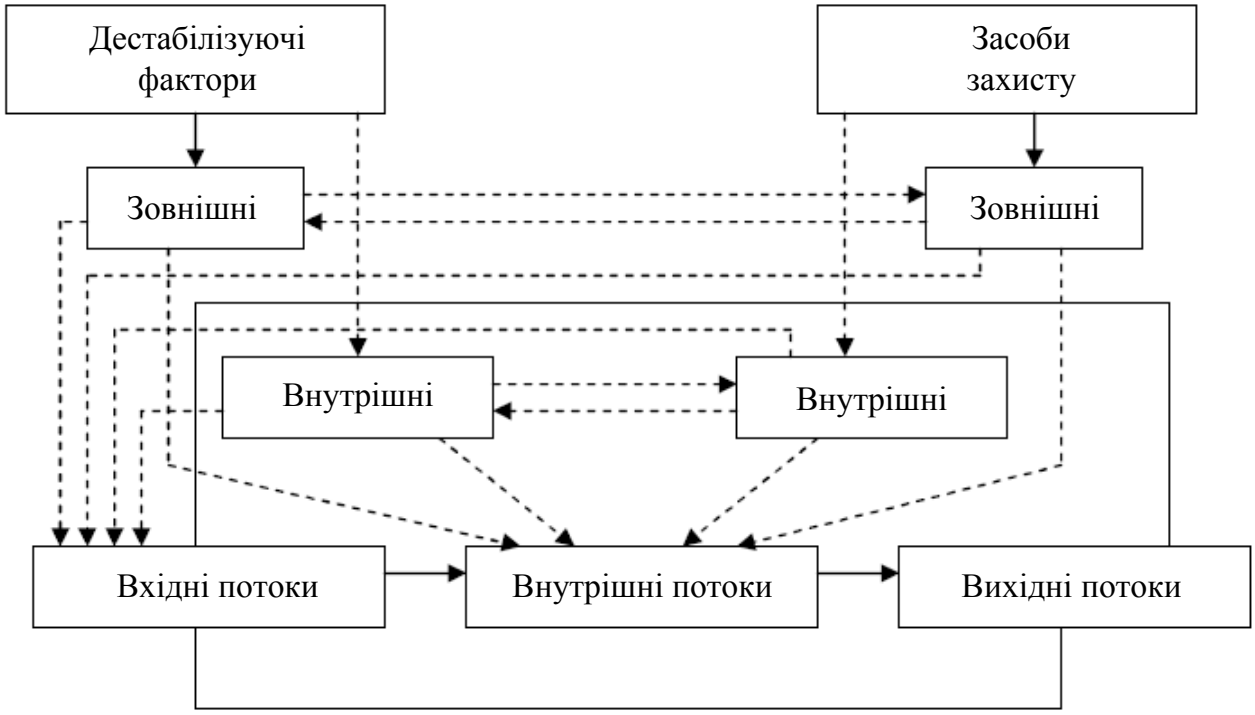

Рисунок 1.1 – Загальна модель впливу на інформацію

Сукупність методів і засобів захисту інформації включає програмні й апаратні засоби, захисні перетворення та організаційні заходи (рис. 1.2)

Апаратний, або схемний, захист полягає в тому, що в комп’ютерах та інших технічних засобах обробки інформації передбачається наявність спеціальних схем, що забезпечують захист і контроль інформації, наприклад, схеми контролю на парність, які контролюють правильність передачі інформації між різними приладами, а також екрануючими приладами, що локалізують електромагнітні випромінювання.

Програмні методи захисту — це сукупність алгоритмів і програм, які забезпечують розмежування доступу та виключення несанкціонованого використання інформації.

Сутність методів захисних перетворень полягає в тому, що інформація, яка зберігається в системі та передається каналами зв'язку, подається в деякому коді, що виключає можливість її безпосереднього використання.

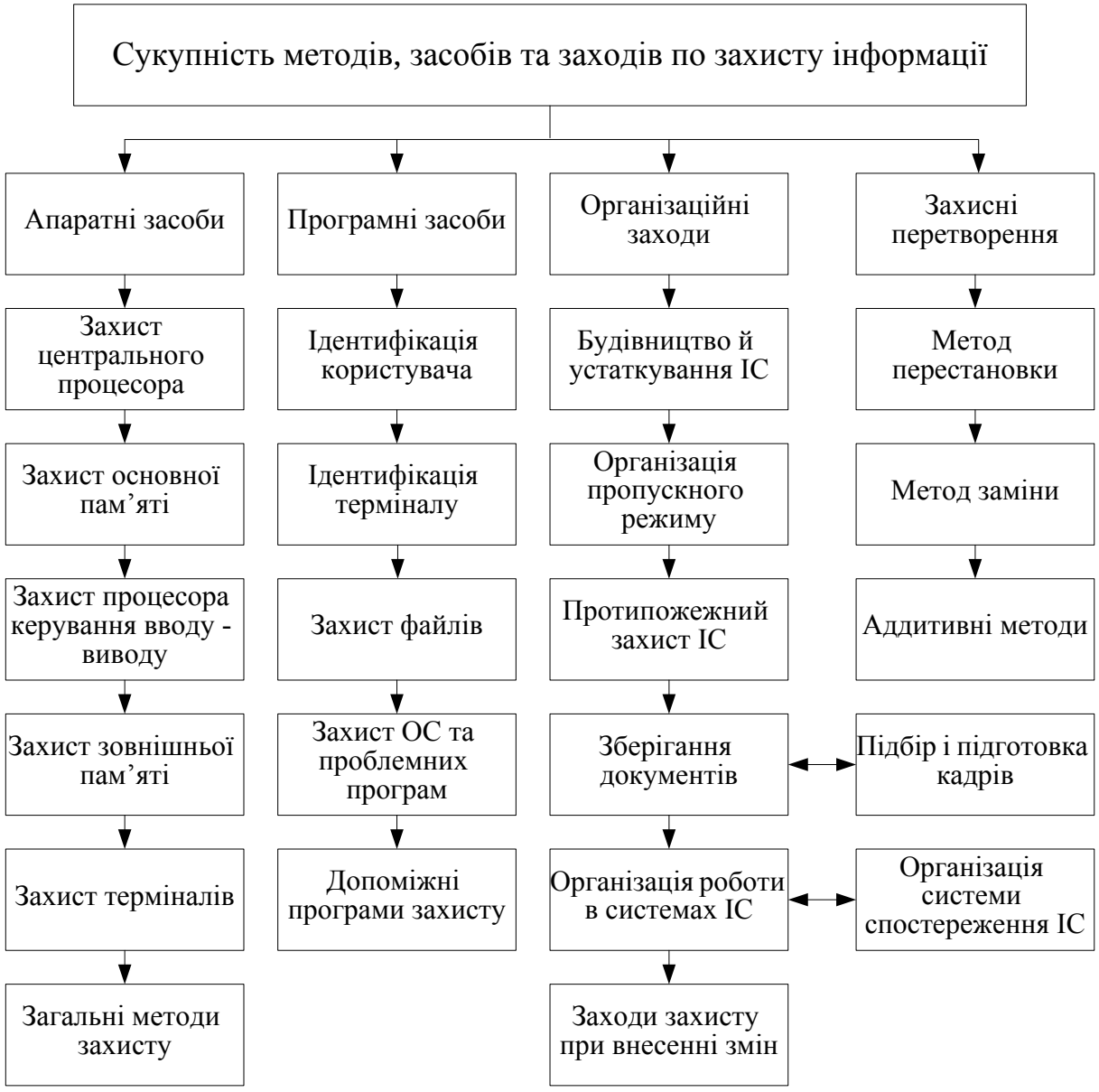

Рисунок 1.2 – Методи і засоби захисту інформації

Організаційні заходи із захисту інформації містять сукупність дій з підбору та перевірки персоналу, який бере участь у підготовці й експлуатації програм та інформації, чітке регламентування процесу розробки та функціонування інформаційної системи.

Лише комплексне використання різних заходів може забезпечити надійний захист інформації, тому що кожний метод або захід має слабкі та сильні сторони[4].

Виділяються наступні групи засобів захисту інформації:

- засоби захисту від несанкціонованого доступу;
- системи аналізу і моделювання інформаційних потоків;
- системи моніторингу мереж;
- аналізатори протоколів;
- антивірусні засоби;
- міжмережеві екрани;
- криптографічні засоби;
- стеганографічні засоби;
- системи резервного копіювання;
- системи безперебійного живлення;
- системи автентифікації;
- засоби запобігання зламу корпусів і крадіжок устаткування;
- засоби контролю доступу в приміщення;
- інструментальні засоби аналізу системи захисту.

Розглянемо детальніше методи захисту інформації за допомогою криптографічних та стеганографічних засобів.

1.4 Стеганографія та стеганоаналіз: різноманіття підходів

Стеганографія є техніка приховування конфіденційної інформації у будь-яких носіях інформації. Стеганографію часто плутають з криптографією, тому що ці дві техніки схожі в тому, що вони обидві використовуються для захисту конфіденційної інформації. Різниця між ними полягає у способі отримання кінцевих оброблених даних; результат стеганографічної операції не є очевидним, але в криптографії вихідні дані змінені так, що вони можуть привернути увагу.

Стегоаналіз є процес виявлення присутності стеганографії. Розглянемо детальніше підходи до використанні стеганографії у мультимедійних файлах, зокрема у статичних зображенням, а також мережі IP датаграм у якості прикриття.

Мета стеганографії полягає у приховуванні таємного повідомлення в медіа-носій таким чином, щоб сторонні були не в змозі розпізнати присутність

прихованого повідомлення. Простими словами "стеганографія означає приховування однієї частини даних в іншій". Сучасна стеганографія використовує можливість приховування інформації в цифрових мультимедійних файлах або на пакетних мережевих рівнях. Приховування інформації у носіях вимагає наявності наступних елементів:

- Медіа-носій (Н), що буде містити в собі приховані дані;
- Секретне повідомлення (П), може бути простим текстом, зашифрований текстом або будь-який інший тип даних;
- Стего-функція (Fe) та обернена до неї (Fe^{-1});
- Додатково можуть бути використані стего ключ (К) або пароль для захищення та вилучення повідомлення.

Стего-функція обробляє медіа-носій та повідомлення, що необхідно приховати, одночасно із стего ключем для отримання носія з прихованим повідомленням (Н+П).

Схематично стеганографічна операція показана на рис. 1.3:

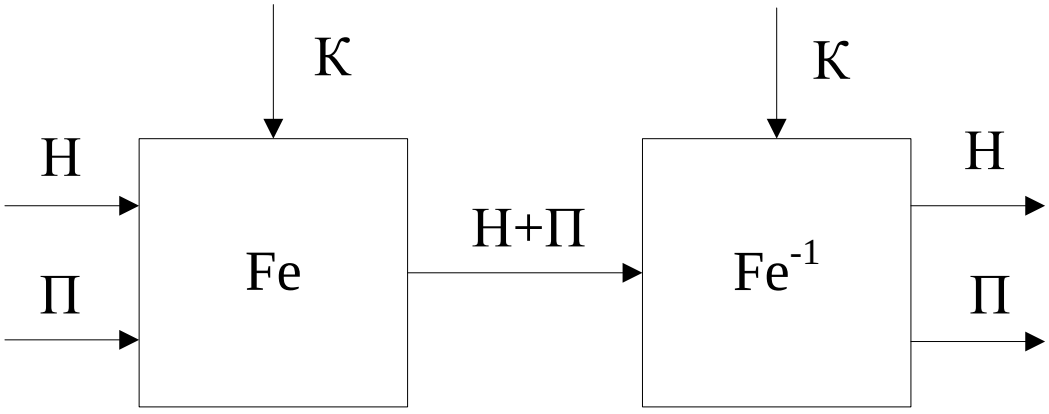

Рисунок 1.3 – Стеганографічний процес

1.4.1 Стегоаналіз

Стегоаналізом називають процес виявлення прихованого повідомлення шляхом перевірки різних параметрів контейнера. Першим і головним кроком є

виявлення підозрюваного контейнера. Після цього стеганоаналітичний процес виявляє, чи містить цей носій приховане повідомлення і намагається відтворити його.

При крипноаналізі очевидно, що перехоплене повідомлення зашифроване і безсумнівно містить приховане повідомлення, тому що повідомлення, наприклад, скрембльоване. Але у випадку стегоаналізу, це не обов'язково. Підозрюваний носій може з однаковими імовірностями містити чи не містити приховане повідомлення. Процес стеганоаналізу починається з набору потоків підозрюваної інформації. Згодом набір звужується за допомогою відповідних статистичних методів.

1.4.2 Стегоноаналітичні техніки.

Властивості електронних носіїв змінюються після приховування в них будь-якого об'єкту. Це може відобразитися як деградація з точки зору якості чи незвичних характеристиках носія: стеганографічні техніки базуються на незвичному вигляді шаблонів чи вузіальному огляді носія.

Наприклад, в випадку мережевої стеганографії це незвичний вигляд шаблону, представлений у заголовку TCP/IP пакета. Якщо техніка аналізу заголовка системи виявлення вторгнень мережі базується на так званому шаблоні чистого листа (white list pattern), тоді цей метод стеганографії може ефективним.

У випадку стеганоаналітичної техніки візуальної детекції набір стего зображень порівнюються з оригіналами та помічається видима різниця. Вміст прихованого повідомлення може бути отриманий порівнянням численних зображень. Обрізка та накладання зображення також є візуальною підказкою до прихованого повідомлення, тому що деякі із стегоінструментів обрізають та накладають пустий простір, щоб помістити стегозображення у фіксований розмір. Різниця у розмірі файлів між порожнім та завантаженим контейнером, збільшення чи зменшення унікальних кольорів у контейнерах також можуть бути використані у техніці візуальної детекції.

1.4.3 Сучасні техніки стеганографії

Сучасні поширені стеганографічні техніки використовують властивості самих медіа-носіїв для передачі повідомлень.

Наступні носії є кандидатами для внесення у них повідомлень:

- Звичайний текст;
- Статичні зображення;
- Аудіо та відео;
- IP датаграми;

На рис.1.4 представлена класифікація систем цифрової стеганографії.

Рисунок 1.4 – Класифікація систем цифрової стеганографії

На сьогоднішній день найбільш широко використовуваним є приховування секретних повідомлень саме у цифрові зображення. Це обумовлено наступними причинами:

- існуванням практичної необхідності захисту цифрових фотографій, зображень, відео від протизаконного тиражування та розповсюдження;
- відносно великим об’ємом цифрового представлення зображень, що дозволяє вбудовувати ЦВЗ значного об’єму або ж підвищувати стійкість цього вбудовування;
- заздалегідь відомим (фіксованим) розміром контейнера, відсутністю обмежень, що накладаються вимогами приховання в реальному часі;
- наявністю у більшості реальних зображень текстурних областей, що мають шумову структуру і найкращим чином підходять для вбудовування інформації;
- слабкою чутливістю людського ока до незначних змін кольору зображення, його яскравості, контрастності, вмісту в ньому шуму, спотворень поблизу контурів;
- добре розробленими в останній час методами цифрової обробки зображень.

Однак, остання причина викликає і значні труднощі в забезпеченні стійкості ЦВЗ: чим більш досконалими стають методи компресії, тим менше залишається можливостей для вбудовування сторонньої інформації.

Розвиток теорії і практики алгоритмів компресії зображень призвів до змін уявлень про техніку вбудування ЦВЗ. Якщо спочатку припускалось вбудовувати інформацію і незначущі біти для зменшення візуальної помітності, то сучасний підхід, навпаки, полягає у вбудуванні ЦВЗ у найбільш суттєві області зображень, руйнування яких будуть призводити до повної деградації самого зображення. Тому абсолютно зрозуміла необхідність врахування стеганоалгоритмами не тільки алгоритмів компресії зображення, але і властивостей зорової системи людини (ЗСЛ).

1.5 Стеганографічні атаки

Стеганографічні атаки складаються з виявлення, вилучення та знищення прихованих об’єктів контейнера. Стеганографічні атаки слідують за

стеганоаналізом. Існує кілька типів атак, що базуються на інформації, доступній для аналізу. Ось деякі з них:

- Атака з відомим носієм: порожній та завантажений контейнер обидва доступні для аналізу;
- Атака стеганографічна: у цьому типі відомий лише завантажений контейнер;
- Атака з відомим повідомленням: у цьому випадку приховане повідомлення відоме;
- Атака з відомим методом: порожній, завантажений контейнери та інструмент або алгоритм стеганографії відомі.

1.6 Прихована пропускна здатність стегоканалу

Дослідимо величину прихованої пропускної здатності (ПЗ) стегоканалів, призначених для прихованої передачі інформації. Сторона аналітика представлена пасивним порушником, що намагається встановити факт застосування стегосистеми. У цій задачі інформаційного приховування порушник не чинить на стего впливу завадами, отже, до розглянутої стегосистеми не висуваються вимоги щодо забезпечення стійкості до навмисного руйнування приховуваних повідомлень. Також будемо вважати, що в процесі передачі стего на нього не впливають ненавмисні завади, отже $Y = X$.

Під прихованою ПЗ в стегосистемах розуміється максимальна кількість інформації, яку потенційно можна вбудувати в один елемент контейнера таким способом, що зловмисник не зможе виявити, і потім витягти без помилок. В якості елементів контейнера можуть розглядатися вибірки звукового або мовного сигналу, дискретизовані відповідно до теореми Котельникова, або пікселі рухомого або нерухомо зображення.

Очевидно, що вимоги щодо непомітності та стійкості до видалення і руйнування є взаємно суперечливими, поліпшити одну характеристику можна

тільки за рахунок погіршення інших. Тому для систем ЦВЗ максимізується стійкість до видалення і руйнування водяного знака (максимізується допустиме спотворення D2) при забезпеченні порівняно невеликий пропускної здатності і достатньою непомітності, що характеризується максимально допустимою величиною спотворення кодування D1. У розглянутому класі максимізується прихована пропускна здатність при забезпеченні необхідної невиявленості стегоканала, а до завадостійкості висуваються мінімальні вимоги. Під невиявленістю розуміється здатність стегосистеми приховувати факт передачі інформації від порушника.

У ряді робіт величина прихованої ПЗ стегоканала визначається двома чинниками. По-перше, аналогічно тому, як в теорії зв'язку розглядається передача сигналів по каналу зв'язку, прихований зв'язок розглядається як передача приховуваних повідомлень по каналу із завадами. В якості завади розглядається контейнерний сигнал. Це дозволяє звести задачу передачі приховуваних повідомлень до добре дослідженої задачі передачі відкритих повідомлень по звичайному каналу із завадами. У цій задачі відношення потужності приховуваного сигналу до потужності шуму характеризує максимально досяжну швидкість передачі інформації, що приховується. У теорії відкритого зв'язку доцільно необмежено збільшувати відношення сигнал/шум, щоб максимізувати величину пропускної здатності каналу. У стеганографії, навпаки, це відношення необхідно суттєво обмежувати через вплив другого чинника, що проявляється в необхідності забезпечення невиявленості факту прихованого зв'язку. При порівнянних потужностях приховуваного сигналу і шуму кваліфікованим порушником легко виявляється факт наявності стегоканала. Отже, в стегосистемах доводиться ховати приховуваний сигнал під значно більшим за величиною шумом прикриття. Тому, з одного боку, для підвищення прихованої ПЗ стегоканала необхідно збільшувати відношення сигнал/шум, а з іншого боку, для підвищення захищеності стегоканала від його виявлення необхідно це відношення істотно зменшувати. Отже, необхідний баланс може бути досягнутий, якщо приховувані повідомлення безпомилково декодуються їх законним одержувачем, але залишаються невиявленими для порушника.

Зауважимо, що у відповідності з теорією оптимального прийому, якщо порушник і законний одержувач приховуваних сигналів мають однакову здатність до їх виявлення на тлі шумів контейнера, то величина прихованої ПЗ стегоканала дорівнює нулю. Отже, для існування невиявленого стегоканала порушник і одержувач приховуваних сигналів повинні перебувати в нерівних умовах. Канал передачі для них рівно є доступним, отже, одержувач повинен мати перевагу в знанні секретної інформації, що дозволяє йому виділити з суміші приховуваний сигнал + контейнер призначене для нього повідомлення, а порушник без знання цієї інформацію не повинен бути здатний відрізнити стего від порожнього контейнера.

Нехай по каналу передається корисний сигнал з потужністю S, а в каналі на нього діє гаусівський шум Z з потужністю N. Вихід адитивного каналу можна представити як X = M + Z. Спрощена схема такої системи передачі представлена на рис.1.5.

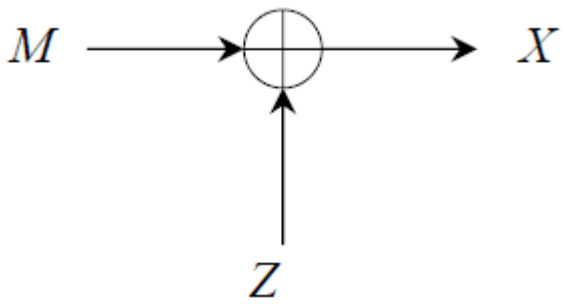

Рисунок 1.5 – Спрощена схема стеганоканалу

Для оцінки величини прихованої пропускної здатності адитивного стеганографічного каналу зіставимо її з величиною пропускної здатності каналу з адитивним білим гаусівським шумом. Якщо вихідний сигнал M та шум Z незалежні, то умовна ентропія вихідного сигналу X при заданому M рівна ентропії шумового сигналу. Використаємо цей результат для виявлення пропускної здатності адитивного каналу з шумом

$$C = \max_{p(x)} H(X) - H(Z)\,. \qquad (1.1)$$

Нехай шум Z має нормальне розподілення із середнім значенням 0 та дисперсією N. Тоді ентропія Z дорівнює

$$H(Z) = \frac{1}{2}\log 2\pi eN\,. \qquad (1.2)$$

Щоб досягти максимуму величини ПЗ по усім можливим розподілам, будемо вважати, що вхідний сигнал M має також нормальний розподіл з дисперсією S. Відповідно, X є сума двох гаусівскьих сигналів і має дисперсію S + N. Тоді пропускна здатність C_g гаусівського каналу виражається як

$$\tilde{N}_g = \frac{1}{2}\log_2[2\pi e(S+N)] - \frac{1}{2}\log_2(2\pi eN) = \frac{1}{2}\log_2\frac{S+N}{N}\,. \qquad (1.3)$$

З теорії зв'язку відомо, що величина ПР каналу мінімальна, коли шум у каналі гауссовский із середнім значенням 0. Отже, пропускна здатність інших адитивних негауссівських каналів обмежуються знизу величиною Cg (1.3). Рівняння (1.4) - (1.6) визначають пропускну здатность трьох таких каналів з різними розподілами шуму.

$$C_g \le C_{Uniform} \le C_g + 0{,}2546\,, \qquad (1.4)$$

$$C_g \le C_{Laplacian} \le C_g + 0{,}1044\,, \qquad (1.5)$$

$$C_g \le C_{Trianular} \le C_g + 0{,}0333 . \qquad (1.6)$$

Розглянемо стеганографічну систему, в якій прихована інформація додана деяким чином до контейнерних даних. Наприклад, приховуване повідомлення записується на місце найменш значущих біт (НЗБ) яскравості пікселів контейнерного зображення. У багатьох практичних стегосистемах приховуване повідомлення до вбудовування шифрується або стискається деяким архіватором даних. Це підвищує прихованість зв'язку та дозволяє описати зашифроване (стисле) повідомлення у вигляді послідовності з незалежно і рівноймовірністно розподіленими бітами. Величину прихованої пропускної здатності стегоканала оцінимо шляхом порівняння з пропускною спроможністю каналу з білим гауссовским шумом. Проте насправді сигнали реальних джерел інформації таких, як мова та відео, не можна описати гауссівськими сигналами, тому що в їх структурі висока залежність між сусідніми вибірками. Як і в інших випадках негауссівських каналів, прихована пропускна здатність стегоканалу, в якому приховувані повідомлення вбудовуються в негауссівські сигнали, обмежена знизу пропускною здатністю каналу з білим гаусівським шумом.

Невизначеність шуму з довільним розподілом може бути порівняна з білим гауссовским шумом, використовуючи вимір ентропійної потужності N_e. Якщо довільний шум Z має ентропію $H(Z)$, то його середня шумова потужність дорівнює потужності гауссівського шуму, який має таку ж ентропію і визначається як

$$N_e(Z) = \frac{1}{2\pi e} e^{2H(Z)} . \qquad (1.7)$$

об'єднуючи (1.7) з оцінкою пропускної здатності каналу з аддитивним шумом, отримаємо, що прихована пропускну здатність C стегоканала обмежена

$$C_g \le C \le \frac{1}{2}\log_2 \frac{S+N}{N_e}. \qquad (1.8)$$

де N_e - ентропійна потужність контейнера. Так як величина N_e строго менше, ніж N для всіх негауссівських сигналів, то величина C_g є нижньою межею для прихованої ПЗ стегоканалів, що використовують довільні контейнери. Верхня межа прихованої ПЗ визначається максимумом взаємної інформації між прихованим повідомленням і стего, вважаючи, що стего має нормальний розподіл з дисперсією S + N і шум у каналі є гаусівським з потужністю N_e. Отже

$$\tilde{N}_g \le \frac{1}{2}\log_2 \frac{S+N_e}{N_e} \le C \le \frac{1}{2}\log_2 \frac{S+N}{N_e}. \qquad (1.9)$$

очевидно, що якщо контейнер можна представити у вигляді білого гаусівського шуму, то його ентропійна потужність зменшується до величини N і прихована ПЗ приймає мінімальне значення, рівне C_g.

1.7 Контейнери

Істотний вплив на надійність стегосистеми і можливість виявлення факту передачі прихованого повідомлення надає вибір контейнера. Наприклад, досвідчене око експерта з художньою освітою легко виявить зміну колірної гами при впровадженні повідомлення в репродукцію «Мадонни» Рафаеля або "Чорного квадрата" Малевича.

За об’ємом контейнери можна поділити на два типи: безперервні (потокові) і обмеженою (фіксованою) довжиною. Особливістю потокового контейнера є те, що неможливо визначити його початок або кінець. Більш того, немає можливості дізнатися заздалегідь, якими будуть наступні шумові біти, що

призводить до необхідності включати приховують повідомлення біти в потік в реальному масштабі часу, а саме приховані біти вибираються за допомогою спеціального генератора, що задає відстань між послідовними бітами в потоці.

У безперервному потоці даних найбільші труднощі для одержувача - визначити, коли починається приховане повідомлення. При наявності в потоковому контейнері сигналів синхронізації або границь пакета, приховане повідомлення починається відразу після одного з них. У свою чергу, для відправника можливі проблеми, якщо він не впевнений в тому, що потік контейнера буде достатньо довгим для розміщення цілого таємного повідомлення.

При використанні контейнерів фіксованої довжини відправник заздалегідь знає розмір файлу і може вибрати приховані біти в підходящої псевдовипадкової послідовності. З іншого боку, контейнери фіксованої довжини, як це вже зазначалося вище, мають обмежений обсяг і іноді вбудоване повідомлення може не помістится в файл-контейнер.

Інший недолік полягає в тому, що відстані між прихованими бітами рівномірно розподілені між найбільш коротким і найбільш довгим заданими відстанями, в той час як справжній випадковий шум буде мати експоненціальний розподіл довжин інтервалу. Звичайно, можна створити псевдовипадкові експоненціально розподілені числа, але цей шлях зазвичай занадто трудомісткий. Однак на практиці найчастіше використовуються саме контейнери фіксованої довжини, як найбільш поширені і доступні.

Можливі такі варіанти контейнерів:

- Контейнер генерується самою стегосистемою. Прикладом може служити програма MandelSteg, в якій в якості контейнера для вбудовування повідомлення генерується фрактал Мандельброта. Такий підхід можна назвати конструюючою стеганографією.

- Контейнер вибирається з множини контейнерів. В цьому випадку генерується велика кількість альтернативних контейнерів, щоб потім вибрати найбільш підходящий для приховування повідомлення. Такий підхід можна назвати вибірковим. В даному випадку при виборі оптимального контейнера з множини згенерованих, найважливішою вимогою є природність контейнера. Єдиною ж проблемою залишається те, що навіть оптимально організований контейнер дозволяє заховати незначну кількість даних при дуже великому обсязі самого контейнера.
- Контейнер надходить ззовні. В даному випадку відсутня можливість вибору контейнера і для приховування повідомлення береться перший-ліпший контейнер, який не завжди підходить до вбудовуваного повідомлення. Назвемо це безваріантна стеганографія[5].

Висновки до першого розділу

Таким чином, об'єктом захисту в інформаційній системі є інформація з обмеженим доступом, яка циркулює та зберігається у вигляді даних, команд, повідомлень, що мають певну обмеженість розповсюдження і цінність як для її власника, так і для потенційного порушника технічного захисту інформації.

Застосування стеганографії як техніки приховування конфіденційної інформації дозволяє виконати задачу захисту у будь-яких носіях інформації.

В стегосистемах доводиться приховувати сигнал під значно більшим за величиною шумом прикриття. Тому, з одного боку, для підвищення прихованої ПЗ стегоканала необхідно збільшувати відношення сигнал/шум, а з іншого боку, для підвищення захищеності стегоканала від його виявлення необхідно це відношення істотно зменшувати.

РОЗДІЛ 2 ПРИХОВУВАННЯ ДАНИХ В НЕРУХОМИХ ЗОБРАЖЕННЯХ

Більшість проаналізованих в роботі досліджень присвячено використанню в якості стеганоконтейнерів саме зображень. Це обумовлено наступними причинами:

- Існуванням практичної необхідності захисту цифрових фотографій, зображень, відео від протизаконного тиражування та розповсюдження.
- Відносно великим об'ємом цифрового представлення зображень, що дозволяє вбудовувати ЦВЗ значного обсягу або ж підвищувати стійкість цього вбудовування.
- Заздалегідь відомим (фіксованими) розміром контейнера, відсутністю обмежень, які накладаються вимогами приховування в реальному часі.
- Наявністю в більшості реальних зображень текстурних областей, що мають шумову структуру і найкращим чином підходять для вбудовування інформації.
- Слабкою чутливістю людського ока до незначних змін кольорів зображення, його яскравості, контрастності, вмісту в ньому шуму, спотворень поблизу контурів.
- Добре розробленими останнім часом методами цифрової обробки зображень.

Проте, як зазначається остання причина викликає і значні труднощі в забезпеченні стійкості ЦВЗ: чим більш досконалими стають методи компресії, тим менше залишається можливостей для вбудовування сторонньої інформації.

Розвиток теорії і практики алгоритмів компресії зображень призвело до зміни уявлень про техніку вбудовування ЦВЗ. Якщо спочатку пропонувалося вбудовувати інформацію в незначущі біти для зменшення візуальної помітності, то сучасний підхід, навпаки, полягає у вбудовуванні ЦВЗ в найбільш істотні області зображень, руйнування яких буде приводити до повної деградації самого зображення. Тому абсолютно зрозуміла необхідність врахування

стеганоалгоритмами не тільки алгоритмів компресії зображень, а й властивостей зорової системи людини (ЗСЛ) [6].

2.1 Основні властивості ЗСЛ, які необхідно враховувати при побудові стеганоалгоритмів

Властивості ЗСЛ можна розділити на дві групи: низькорівневі ("фізіологічні ") і високорівневі ("психофізіологічні"). Майже до середини 1990-х р.р. дослідники брали до уваги, головним чином, низькорівневі властивості зору. В останні роки намітилася тенденція побудови стеганоалгорітмів з урахуванням і високорівневих характеристик ЗСЛ.

Виділяють три найважливіші низькорівневі властивості, що впливають на помітність стороннього шуму в зображенні:

1. Чутливість до зміни яскравості (контрастності) зображення.
2. Частотна чутливість.
3. Ефект маскування.

На рис. 2.1 зображена залежність мінімального контрасту ΔI/I від яскравості I.

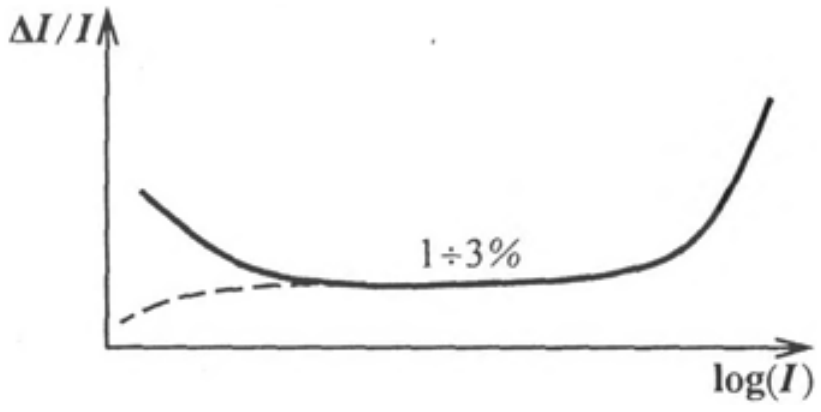

Рис. 2.1 Чутливість до зміни контрасту і поріг нерозрізненості ΔI.

Як видно, для середнього діапазону зміни яскравості, контраст приблизно постійний, тоді як для малих і великих яскравостей значення порогу

нерозрізненості (ΔI) зростає. Встановлено, що $\Delta I \approx (0.01/0.03) \cdot I$ для середніх значень яскравості.

Крім того, зазначено, що результати новітніх досліджень суперечать "класичній" теорії і показують, що при малих значення яскравості поріг нерозрізненості зменшується, тобто ЗСЛ більш чутлива до шуму в цьому діапазоні.

Частотна чутливість ЗСЛ проявляється в тому, що людина набагато більш сприйнятлива до низькочастотного (НЧ), ніж до високочастотного (ВЧ) шуму. Це пов'язано з нерівномірністю амплітудно-частотної характеристики ЗСЛ.

Елементи ЗСЛ поділяють відеосигнал, що надходить на окремі складові, кожна з яких збуджує нервові закінчення ока через ряд підканалів. Виділені оком складові мають різні просторові і частотні характеристики, а також різну просторову орієнтацію (горизонтальну, вертикальну, діагональну).

У разі одночасного впливу на око двох складових зі схожими характеристиками збуджуються одні й ті ж підканали. Це призводить до ефекту маскування, який полягає у збільшенні порогу виявлення зорового сигналу в присутності іншого сигналу, що має аналогічні характеристики. Тому, адитивний шум набагато помітніший на НЧ (однотонних) ділянках зображення в порівнянні з ВЧ ділянками, тобто, в останньому випадку спостерігається маскування. Найбільш сильно даний ефект проявляється, коли обидва сигнали мають однакову орієнтацію і місце розташування.

Частотна чутливість тісно пов'язана з яскравістю. Відомо також і вираз для визначення порогу маскування на основі відомої чутливості до яскравості, що дозволяє знайти метрику спотворення зображення, яка враховувала б властивості ЗСЛ. Математичні моделі такого типу добре розроблені для випадку квантування коефіцієнтів дискретного косинусного перетворення (ДКП), оскільки саме воно застосовується в стандарті JPEG.

Ефект маскування в просторовій області може бути пояснений шляхом побудови стохастичних моделей зображення. При цьому зображення

представляється у вигляді марківського випадкового поля, розподіл ймовірностей якого описується, наприклад, узагальненим законом Гаусса.

Пропонується наступна узагальнена схема вбудовування даних у зображення:

1. Виконується фільтрація зображення за допомогою орієнтованих смугових фільтрів. При цьому отримується розподіл енергії за частотно-просторовими компонентами.
2. Розраховується поріг маскування на основі знання локальної величини енергії.
3. Масштабується значення енергії впроваджуваної інформації в кожному компоненті таким чином, щоб воно було менше порога маскування.

Високорівневі властивості ЗСЛ поки що рідко враховуються при побудові стеганоалгорітмів. Вони відрізняються від низькорівневих тим, що проявляються "вторинно" - обробивши первинну інформацію від ЗСЛ, мозок видає команди на "підлаштування" зорової системи під зображення[6].

Перерахуємо основні з цих властивостей:

1. Чутливість до контрасту — висококонтрастні ділянки зображення і перепади яскравості звертають на себе більше уваги.
2. Чутливість до розміру — великі ділянки зображення більш "помітні" у порівнянні з меншими за розміром, причому існує поріг насиченості, коли подальше збільшення розміру не грає ролі.
3. Чутливість до форми — довгі і тонкі об'єкти викликають більше уваги, ніж закруглені і однорідні.
4. Чутливість до кольорів — деякі кольори (наприклад, червоний) більш "помітні", ніж інші. Цей ефект посилюється, якщо фон заднього плану відрізняється від кольорів фігур на ньому.
5. Чутливість до місця розміщення — людина схильна в першу чергу розглядати центр зображення. Також уважніше розглядаються фігури переднього плану, ніж заднього.

6. Чутливість до зовнішніх подразників — рух очей спостерігачів залежить від конкретної обстановки, від отриманих ними перед переглядом або під час його інструкцій, додаткової інформації.

2.2 Приховування даних у просторовій області

Алгоритми, описані в даному підрозділі, вбудовують приховувані дані в області первинного зображення. Їх перевага полягає в тому, що для вбудовування немає необхідності виконувати складні обчислювально та тривалі перетворення зображень.

Загальний принцип цих методів полягає в заміні надлишкової, малозначимої частини зображення бітами секретного повідомлення. Для вилучення повідомлення необхідно знати алгоритм, за яким розміщувалась по контейнеру прихована інформація[6].

2.2.1 Метод найменш значущого біта (НЗБ)

ЗСЛ не може виявляти варіації яскравість векторів кольорів на області високих частот видимого спектру. Окремі пікселі можуть бути представлені своїми оптичними характеристиками, такими як яскравість, кольоровість та ін. Кожна з цих характеристик може бути представлена у цифровому вигляді одиниць і нулів.

Наприклад, 24-х бітова карта має 8 бітів, що представляють кожен з трьох кольорових складових (червоний, зелений та блакитний) кожного пікселя. Якщо розглядати тільки блакитний, отримаємо 2^8 різних значень блакитного. Різниця між 11111111 та 11111110 значеннями блакитного скоріше всього не буде виявлена людським оком. Отже, якщо кінцевий приймач даних ніщо інше як людська зорова система (ЗСЛ), то Найменш Значущий Біт (НЗБ) може бути використаний для чогось іншого, ніж інформація про кольори.

Ця техніка може бути напряму використана на цифрових зображеннях у форматі бітової карти, так само як і для формату стиснення зображень, як, наприклад, JPEG. У форматі JPEG кожний піксель зображення закодований з використанням дискретного косинусного перетворення (ДКП). НЗБ декодованих компонентів ДКП можуть бути використані як носії для приховуваних повідомлень.

2.2.2 Модифікація НЗБ зображення-носія у bitmap форматі

У цьому методі бінарний еквівалент повідомлення (яке необхідно приховати) розподілений поміж молодшими бітами кожного пікселя. Наприклад, спробуємо сховати літеру "A" в 8-бітове кольорове зображення.

Беремо вісім послідовних пікселів з верхнього лівого кутка зображення. Бінарний еквівалент бітової таблиці цих пікселів може виглядати наступним чином:

00100111 11101001 11001000 00100111 11001000 11101001 11001000 00100111

Після цього кожний біт бінарного еквіваленту літери "A", а саме **01100101** копіюється періодично (з лівого боку) до бінарного еквіваленту бітової таблиці пікселів. Результат отримаємо наступний:

00100110 11101001 11001001 00100110 11001000 11101001 11001000 00100111

Одна з головних проблем цієї техніки полягає в тому, що вона дуже вразлива до таких атак, як стиснення зображень та форматування.

2.2.3 Застосування технології НЗБ під час дискретного косинусного перетворення (ДКП) на зображенні-носії

У цьому випадку виконуються наступні кроки:

1. Зображення розбивається на блоки даних, кожний з яких складається з 8x8 блоків пікселів.
2. Переміщуючись з лівого верхнього до правого нижнього кутка, ДКП застосовується до кожного пікселя кожного блока даних.
3. Після застосування ДКП, для кожного пікселя у блоці даних генерується ДКП коефіцієнт.
4. Кожний ДКП коефіцієнт кантується у відповідності до таблиці квантизації.
5. НЗБ бінарного еквіваленту квантованого ДКП коефіцієнта може бути замінений бітом з секретного повідомлення.
6. До кожного модифікованого ДКП коефіцієнта застосовується декодування для отримання стисненого стегозображення.

Рисунок 2.2 – Приклад статичного зображення. Зображення ліворуч є оригіналом, зображення праворуч містить у собі приховане повідомлення.

2.2.4 Метод псевдовипадкового інтервалу

У розглянутому вище найпростішому випадку виконується заміна НЗБ всіх послідовно розміщених пікселів зображення. Інший підхід - метод випадкового

інтервалу, полягає у випадковому розподілі бітів секретного повідомлення по контейнеру, в результаті чого відстань між двома вбудованими бітами визначається псевдовипадковою функцією. Цей метод особливо ефективний у випадку, коли бітова довжина секретного повідомлення є істотно меншою за кількість пікселів зображення.

Найпростіший випадок цього методу: коли інтервал між двома послідовними вбудовування бітів повідомлення є функцією координат попереднього модифікованого пікселя. (наприклад: кількістю одиниць у двійковому представлення індексу переднього пікселя) [7].

2.2.5 Метод блочного приховування

Метод блочного приховування — це ще один підхід до реалізації методу заміни і полягає в наступному. Зображення-оригінал розбивається на l_M непересічних блоків Δ_i $(1 \le i \le l_M)$ довільної конфігурації, для кожного з яких обчислюється біт парності $b(\Delta_i)$:

$$b(\Delta_i) = \sum_{j \in \Delta_i}^{\mathrm{mod}2} LSB(C_j). \qquad (2.1)$$

У кожному блоці виконується приховування одного секретного біта M_i. Якщо біт парності $b(\Delta_i) \neq M_i$, то відбувається інвертування одного з НЗБ блоку Δ_i, в результаті чого $b(\Delta_i) = M_i$. Вибір блоку може відбуватися псевдовипадково з використанням стеганоключа.

Хоча цей метод має таку ж низьку стійкість до спотворень, як і всі попередні, у нього є ряд переваг. По-перше, існує можливість модифікувати значення такого пікселя в блоці, зміна якого приведе до мінімального зміни статистки контейнера. По-друге, вплив наслідків вбудовування секретних даних у контейнер можна зменшити за рахунок збільшення розміру блоку[8].

2.2.6 Метод заміни палітри

Щоб приховати дані можна також скористатися палітрою кольорів, присутніх у форматі зображення. Палтіра з ***N*** кольорів визначається як список пар індексів (i, Δ_i), що визначає відповідність між індексом ***i*** та його вектором кольоровості Δ_i (так звана таблиця кольорів). Кожному пікселю зображення ставиться у відповідність певний індекс в таблиці. Оскільки порядок кольорів у палітрі не важливий для відновлення загального зображення, конфіденційна інформація може бути прихована шляхом перестановки кольорів у палітрі.

Існує ***N!*** різних способів перестановки ***N***-кольорової палітри, чого цілком достатньо для приховування невеликого повідомлення. Проте методи приховування, в основі яких лежить порядок формування палітри, також є нестійкими: будь-яка атака, пов'язана зі зміною палітри, знищує вбудоване повідомлення.

Найчастіше сусідні кольори в палітрі не обов'язково схожі, тому деякі стеганометоди перед вбудовуванням даних впорядковують палітру таким чином, що суміжні кольори стають подібними. Наприклад, значення кольору може бути впорядковано по відстані ***d*** у RGB-просторі, де $d = \sqrt{R^2 + G^2 + B^2}$.

Оскільки ЗСЛ більш чутлива до змін яскравості кольору, то доцільно сортувати вміст палітри саме по значеннях яскравості сигналу. Після сортування палітри можна змінювати НЗБ індексів кольору без надмірного спотворення зображення.

Деякі стеганометоди передбачають зменшення загальної кількості значень кольорів (до $N/2$) шляхом "розмивання" зображення. При цьому елементи палітри дублюються таким чином, щоб значення кольорів для них розрізнялося неістотно. У результаті кожне значення кольору розмитого зображення відповідає двом елементам палітри, які вибираються у відповідності з бітом приховуваного повідомлення[8,9].

2.2.7 Метод квантування зображення

До методів приховування в просторовій області можна також віднести метод квантування зображення, що базується на міжпіксельній залежності, яку можна описати деякою функцією Θ. У найпростішому випадку можна обчислити різницю ε_i між суміжними пікселями c_i та c_{i+1} (або c_{i-1} та c_i) і задати її як параметр функції $\Theta: \Delta_i = \Theta(c_i - c_{i+1})$, де Δ_i — дискретна апроксимація різниці сигналів $c_i - c_{i+1}$.

Оскільки Δ_i — ціле число, а реальна різниця $c_i - c_{i+1}$ — дійсне число, то виникають помилки квантування $\delta_i = \Delta_i - \varepsilon_i$. Для сильно корельованих сигналів ця помилка близька до нуля: $\delta_i \approx 0$.

При цьому методі [10] приховування інформації проводиться шляхом коригування сигналу різниці Δ_i. Стеганоключ представляє собою таблицю, яка кожному можливому значенню Δ_i ставить у відповідність певний біт, наприклад:

Δ_i	-4	-3	-2	-1	0	1	2	3	4
b_i	1	0	1	1	0	0	1	0	1

Для приховування ***i***-го біта повідомлення обчислюється різниця Δ_i. Якщо при цьому b_i не відповідає секретному біту, який необхідно приховати, то значення Δ_i замінюється найближчим Δ_j, для якого така умова виконується. При цьому відповідним чином коректуються значення інтенсивностей пікселів, між якими обчислювалася різниця Δ_i. Вилучення секретного повідомлення здійснюється за значенням $b*_i$, що відповідає різниці $\Delta*_i$.

2.2.8 Метод Дармстедтера-Делейгла-Квісквотера-Макка

Незвичайний блоковий метод вбудовування в просторову область контейнера запропонували Дармстедтер (V. Darmsteadter), Делейгл (J.-F. Delaigle), Квісквотер (JJ Quisquater) і Макк (B. Macq). Розроблений ними метод дозволяє досягти компромісу між стійкістю стеганосистеми до спотворень, якістю вбудовування і, звичайно ж, обчислювальною складністю алгоритму. Метод базується на елементарному перцепційному (відчуваємому) сприйнятті і дозволяє пристосовувати вбудовування щодо поточного вмісту блоків контейнера.

Перед вбудовуванням, конфіденційна інформація перетворюється у вектор двійкових даних. Кожен біт вбудовується в окремий блок. У розглянутому авторами варіанті розмірність блоків становила 8×8 пікселів. Головна причина такого вибору, очевидно, - співрозмірність з блоками, які використовуються при JPEG-компресії. Таким чином, дія компресії буде однаково поширюватися на кожен вбудований біт. Крім того, при цьому інформація вбудовується з надлишковістю, що збільшує загальну стійкість стеганосистеми.

У загальному випадку процес вбудовування біт повідомлення виконується в чотири етапи:

1. Розбиття масиву зображення-контейнера на блоки 8×8 пікселів.
2. Класифікація пікселів окремого блоку на зони з приблизно однорідними значеннями яскравості.
3. Розбиття кожної зони на категорії відповідно до індивідуальної (псевдовипадкової) маски.
4. Вбудовування біту в залежності від співвідношення між середніми значеннями категорій кожної зони шляхом модифікації значень яскравості кожної категорії в кожній зоні.

Розглянемо останні три етапи більш докладно.

Класифікація на зони

Мета полягає в тому, щоб розбити пікселі всередині блоку на групи, які мали б приблизно однакову яскравість. Така класифікація бере до уваги особливості блоку, що представляють інтерес з точки зору невидимості і стійкості. При класифікації автори виділяють три типи контрасту:

1. Різко виражений контраст (рис. 2.3 а), коли можна розрізнити дві зони, розділені помітним стрибком яскравості;
2. Поступовий контраст (рис. 2.3 б), коли дві однорідні зони розділені ділянкою з поступовою зміною яскравості;
3. Шумовий (нечіткий) контраст (рис. 2.3 в) з яскравістю, що розподілена на зразок випадкового шуму (в граничному випадку шумовий контраст вироджується в однотонне зображення — контраст відсутній, всі пікселі блоку мають однакову яскравість).

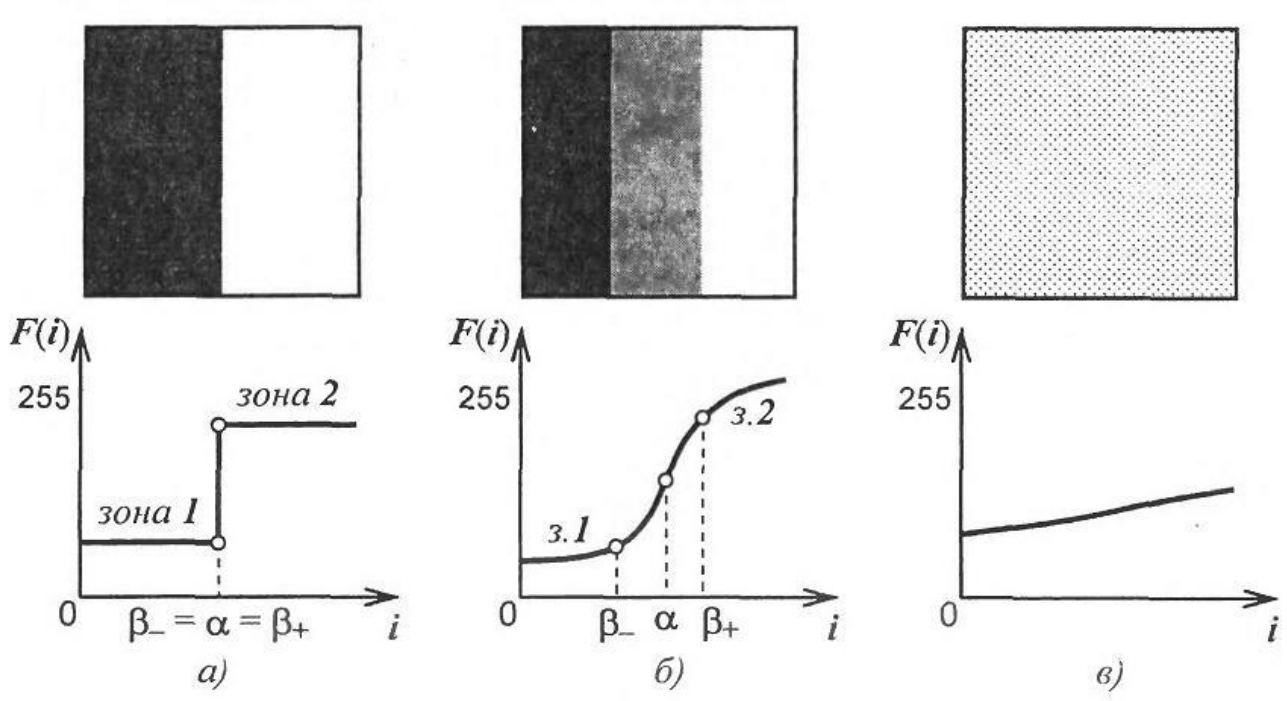

Рис.2.3 - Класифікація на зони: а - різко виражений контраст;

б - поступовий контраст; в - шумовий контраст

Відсортовані за зростанням значення яскравості пікселів блоку можна уявити зростаючою функцією $F(i)$, де $F(1)$ — найменше значення яскравості серед всіх присутніх у цьому блоці, а $F(N^2)$ — найбільше серед присутніх у блоці значень яскравості (N — розмірність квадратного блоку). Тип контрасту блоку визначає крутизна функції $F(i)$, яку позначимо через $S(i)$.

Нехай $S_{\max}$ — максимальна крутизна функції F при $i = a$. Якщо $S_{\max}$ нижче заданого порогу T_1, вважається, що блок має шумовий контраст. Якщо $S_{\max}$ перевищує поріг T_1, блок має або поступовий, або різко виражений контраст. У цьому випадку додатково визначають параметри β_+ та β_- — індекси в найближчому околі точки a (відповідно вище і нижче її), які задовольняють нерівностям:

$$S(a) - S(\beta_+) > T_2 \quad \text{і} \quad S(a) - S(\beta_-) > T_2,$$

де T_2 — ще одне задане значення порогу.

Якщо контраст різко виражений, то $\beta_+ \approx a$ і $\beta_- \approx a$. Якщо контраст поступовий, то інтервал $[\beta_+, \beta_-]$ являє собою перехідну зону поступового контрасту.

Класифікація пікселів $p(x, y)$ на дві зони визначається наступними правилами:

1.Для поступового і різко вираженого контрастів:

1.1 Якщо $p(x, y) \le F(\beta_-)$, то піксель $p(x, y)$ належить до зони 1;

1.2 Якщо $p(x, y) \ge F(\beta_+)$, то піксель $p(x, y)$ належить до зони 2;

1.3 Якщо $F(\beta_-) < p(x, y) < F(\beta_+)$, то піксель $p(x, y)$ належить до перехідної зони.

2.Для шумового контрасту пікселі розподіляють на дві зони однакової розмірності:

2.1 Якщо $p(x,y) < F(N^2/2)$, то піксель $p(x,y)$ належить до зони 1;

2.2 Якщо $p(x,y) > F(N^2/2)$, то піксель $p(x,y)$ належить до зони 2.

У блоках першого і другого типів зони з різною яскравістю не обов'язково повинні розміщуватися впритул один до одного і не обов'язково повинні містити рівну кількість пікселів. Більше того, деякі пікселі взагалі можуть не належати до жодної з цих зон. У блоках третього типу класифікація більш складна.

Розбиття зон на категорії

Після розбиття на зони необхідно передбачити вбудовування біта шляхом модифікації певних характеристик зон. На жаль, як зазначають автори, безпосередній вплив на зони призводить до результатів, які або недостатньо стійкі до перетворень, або ж є незадовільними, виходячи з показників візуальних спотворень вихідного зображення.

Пошук оптимального для вбудовування пікселя полягає в розділенні зони на дві категорії (A та Z). Для сортування пікселів по цим категоріям на блоки зображення накладаються маски, причому бажана індивідуальність масок для кожного конкретного блоку. Призначення масок полягає в забезпеченні таємності вбудовування.Приклади масок для двох зон представлені на рис 2.4

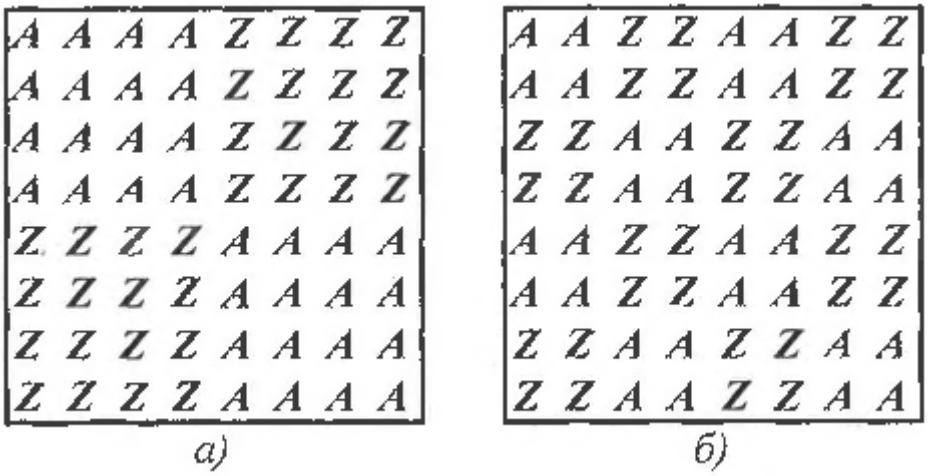

Рис. 2.4 - Приклади масок, що використовуються:

$а$ — розмірами 4×4, $б$ — розмірами 2×2.

Рекомендується використовувати більш складні комбінації і змінювати маску при переході до приховування кожного наступного біта повідомлення. Категорія, до якої буде віднесено той чи інший піксель; залежить від двох чинників:

1. Простір розміщення пікселя в масиві блоку;
2. Номери зони, до якої був віднесений піксель.

Важливо зазначити, що алгоритм формування масок повинен триматися в секреті, оскільки знання конфігурації останніх істотно знижує стійкість стеганосистеми в цілому.

Правила вбудовування біт повідомлення

За результатами виконання перших трьох етапів отримані чотири різні групи пікселів в певних блоках: залежно від зони (1 або 2) і категорій (***A*** або ***Z***). Слід зазначити, що існує ще й п'ята група пікселів: ті, які не ввійшли в жодну із зон. Однак останні не беруть участі в подальшому аналізі.

Для зазначених чотирьох підмножин можуть бути обчислені шість параметрів:

- Чотири середніх значення яскравості $\lambda_{1A}, \lambda_{1Z}, \lambda_{2A}$ та λ_{2Z} для груп, які містять відповідно n_{1A}, n_{1Z}, n_{2A} та n_{2Z} пікселів;
- Два середніх значення яскравості відповідних зон: Λ_1 і Λ_2.

Середні значення яскравості однакових зон об'єднуються разом. Таким чином, один біт повідомлення вбудовується в кожну із зон. Це збільшує стійкість системи і дозволяє вбудовувати біт без надмірного спотворення блоку.

Вбудовування біта b в блок виконується у відповідності зі зв'язками між категоріями середніх значень яскравості. Правило вбудовування наступне:

$$\begin{cases} \lambda^*_{1Z} - \lambda^*_{1A} = E; \\ \lambda^*_{2Z} - \lambda^*_{2A} = E, \end{cases} \quad npu\, b = 0; \qquad (2.2\,a)$$

$$\begin{cases} \lambda^*_{1A} - \lambda^*_{1Z} = E; \\ \lambda^*_{2A} - \lambda^*_{2Z} = E, \end{cases} \quad при\, b = 1; \qquad (2.2\ б)$$

де $\lambda^*_{1A}, \lambda^*_{1Z}, \lambda^*_{2A}$ та λ^*_{2Z} — середні значення яскравості, необхідні для приховування біта b; E — рівень вбудовування, тобто, необхідна різниця між вказаними середніми значеннями.

Для того щоб зробити результат вбудовування якомога більш непомітним, повинні бути збережені низькі частоти (до них найбільш чутлива ЗСЛ). Збереження середніх значень інтенсивностей кожної зони забезпечується виконанням наступних умов:

$$\frac{n_{1A} \cdot \lambda^*_{1A} + n_{1Z} \cdot \lambda^*_{1Z}}{n_{1A} + n_{1B}} = \Lambda_1; \qquad (2.3\ а)$$

$$\frac{n_{2A} \cdot \lambda^*_{2A} + n_{2Z} \cdot \lambda^*_{2Z}}{n_{2A} + n_{2B}} = \Lambda_2 \qquad (2.3\ б)$$

Формули (2.2) і (2.3) дозволяють визначити значення $\lambda^*_{1A}, \lambda^*_{1Z}, \lambda^*_{2A}$ та λ^*_{2Z}. Яскравість пікселів кожної зони повинна бути адаптована для збереження значень Λ_1 і Λ_2. При цьому вважається, що зміна яскравості всіх пікселів, які належать до однієї зони, однакова.

Нехай $\Delta_{1A}, \Delta_{1Z}, \Delta_{2A}$ та Δ_{2Z} — зміни яскравості. Тоді маємо:

$$\Delta_{ij} = \lambda^*_{ij} - \lambda_{ij},$$

де $i = \{1,2\}; \; j = \{A, Z\}$.

Вилучення вбудованої інформації

Вилучення вбудованої інформації з контейнера вимагає наявності відомостей про розмірності блоків, на які розбивається зображення, а також про

конфігурацію масок, які використовувались при вбудовуванні. Процес вилучення складається з наступних етапів:

1. Розбиття зображення на блоки розмірністю $N \times N$.
2. Класифікація пікселів окремого блоку на зони.
3. Розподіл кожної зони на категорії.
4. Порівняння середніх значень яскравості для визначення значення вбудованого біта даних.

Перші три етапи ідентичні відповідним етапам алгоритму вбудовування. Четвертий етап заслуговує більш докладного розгляду.

Нехай Σ_1 і Σ_2 — значення, отримані шляхом порівняння середніх значень яскравості:

$$\Sigma_1 = \lambda_{1A} - \lambda_{1B}; \quad (2.4\ а)$$

$$\Sigma_2 = \lambda_{2A} - \lambda_{2B}. \quad (2.4\ б)$$

Знак обчислених Σ_1 і Σ_2 дозволяє зробити припущення щодо істинного значення прихованого біта. Крім того, абсолютні значення Σ_1 і Σ_2 несуть інформацію про рівень достовірності такого припущення.

Можливі три випадки:

1. $\Sigma_1 \cdot \Sigma_2 > 0$. При цьому $b^* = 1$, якщо $\Sigma_1 > 0$, і $b^* = 0$, якщо $\Sigma_2 < 0$.
   Рівень достовірності:
   - Дуже високий, якщо $|\Sigma_1|$ і $|\Sigma_2| > 2$;
   - Дуже високий, якщо $|\Sigma_1|$ або $|\Sigma_2| > 2.5$;
   - Низький, якщо $|\Sigma_1|$ і $|\Sigma_2| < 0.7$;
   - Високий у всіх інших випадках.
2. $\Sigma_1 \cdot \Sigma_2 < 0$. Додатково обчислюється наступний параметр:

$$\Sigma' = \Sigma_1 \cdot (n_{1A} + n_{1Z}) + \Sigma_2 \cdot (n_{2A} + n_{2Z}).$$

При цьому $b^* = 1$, якщо $\Sigma' > 0$, і $b^* = 0$, якщо $\Sigma' < 0$. Рівень достовірності при цьому низький.

3. $\Sigma_1 \cdot \Sigma_2 \approx 0$. Обчислюється параметр $\Sigma' = \max(|\Sigma_1|, |\Sigma_2|)$. При цьому $b^* = 1$, якщо $\Sigma' > 0$, і $b^* = 0$, якщо $\Sigma' < 0$. Рівень достовірності при цьому низький. Якщо $\Sigma' = 0$, то значення біта невизначене.

Для підвищення завадостійкості автори пропонують використовувати циклічний код корекції помилок БЧХ (Боуза-Чоудхурі-Хоквенгема).

2.3 Інші методи приховування даних у просторовій області

Незвичним є алгоритм, заснований на копіюванні блоків з однієї випадково вибраної текстурної області в іншу, яка має подібні статистичні характеристики, що призводить до появи в зображенні повністю ідентичних блоків. Ці блоки можуть бути виявлені таким чином:

1. Аналіз автокореляційної функції стеганозображення і визначення її піків;
2. Зсув зображення у відповідності з цими піками і вираховування зображення з його зрушеної копії;
3. Відмінність в місцях розміщення зкопійованих блоків повинна бути близькою до нуля. Тому можна вибрати якийсь поріг і значення, що не перевищують цей поріг за абсолютною величиною, вважати шуканими блоками.

Оскільки копії блоків ідентичні, вони змінюються однаково при перетвореннях всього зображення. Якщо зробити розмір блоків досить великим, алгоритм буде стійким до більшості негеометричних спотворень. У проведених авторами експериментах була підтверджена стійкість алгоритму до фільтрації, компресії, обертанню зображення.

Основним недоліком алгоритму, є виняткова складність знаходження достатньої кількості областей, блоки з яких можуть бути замінені без помітного

погіршення якості зображення. Крім того, в даному алгоритмі в якості контейнера можуть використовуватися тільки досить текстуровані зображення.

Алгоритм, дозволяє вбудовувати інформацію в блоки 8×8 зображення-контейнера. На початку алгоритму створюється маска $\mu(x,y)$, розмірність якої відповідає розмірності масиву контейнера, а елементами є псевдовипадково розподілені 0 і 1: $\mu(x,y)\in\{0;1\}$. Кожен блок $Б$ в залежності від значення елементів маски ділиться на два підмасива $Б_1$ і $Б_2$ для кожного з яких обчислюються середні значення яскравості — λ_1 і λ_2. Біт приховуваного повідомлення вбудовується наступним чином:

$$s(x,y)=\begin{cases}1, \text{при } \lambda_1-\lambda_2>E;\\ 0, \text{при } \lambda_1-\lambda_2<-E,\end{cases} \qquad (2.5)$$

де E — деяке значення порогу (необхідна відмінність між зазначеними середніми значеннями яскравості).

У тих випадках, коли умови (2.4) не виконуються, відповідним чином модифікують значення яскравості пікселів одного з підмасивів ($Б_1$ або $Б_2$). Для вилучення біта прихованого повідомлення проводиться обчислення відповідних середніх значень яскравості під масивів — λ_1^* і λ_2^*. Відмінність між ними дозволяє визначити значення прихованого біта:

$$b_i=\begin{cases}1, \text{ при } \lambda_1^*-\lambda_2^*>0;\\ 0, \text{ при } \lambda_1^*-\lambda_2^*<0;\\ ?, \text{ при } \lambda_1^*-\lambda_2^*=0.\end{cases}$$

2.3.1 Приховування даних в частотній області зображення

Як вже було зазначено вище, стеганографічні методи приховування даних у просторовій області зображення є нестійкими до більшості видів спотворень. Так, наприклад, використання операції компресії з втратами (щодо зображення,

це може бути JPEG-компресія) призводить до часткового або, що більш ймовірно, повного знищення вбудованої в контейнер інформації. Більш стійкими до різноманітних спотворень, в тому числі і компресії, є методи, які використовують для приховування даних не просторову область контейнера, а частотну.

Існує декілька способів представлення зображення в частотній області. При цьому використовується та чи інша декомпозиція зображення, використовуваного як контейнер. Наприклад, існують методи на основі використання дискретного косинусного перетворення (ДКП) [11], дискретного перетворення Фур'є (ДПФ), вейвлет-перетворення, перетворення Карунена-Лоєва і деякі інші. Подібні перетворення можуть застосовуватися або до окремих частин зображення, або до зображення в цілому.

Найбільшого поширення серед всіх ортогональних перетворень в стеганографії отримали вейвлет-перетворення та ДКП, що певною мірою пояснюється значним поширенням їх використання при компресії зображень. Крім того, для приховування даних доцільно застосовувати саме то перетворення зображення, якому останнє буде піддаватися з часом при можливій компресії. Наприклад, відомо, що алгоритм ДКП є базовим у стандарті JPEG, а вейвлет-перетворення — в стандарті JPEG2000.

Стеганоалгоритм може бути досить стійким до подальшої компресії зображення, тільки якщо він буде враховувати особливості алгоритму перспективного стиснення. При цьому, звичайно, стеганоалгоритм, в основу якого закладено вейвлет-перетворення, зовсім не обов'язково буде стійким до ДКП алгоритму стиснення, і навпаки. Ще більші труднощі виникають при виборі методу стеганоперетворення під час приховування даних в потоковому відео. Причина цього — однією із складових алгоритмів компресії відеоінформації (на додаток до компресії нерухомого кадру), є кодування векторів компенсації руху. При компресії нерухомого зображення ця компенсація відсутня за непотрібністю. Щоб бути в достатній мірі стійким, стеганоалгоритм повинен враховувати даний чинник.

Залишається також відкритим питання про існування стійкого стеганоперетворення, яке було б незалежним від застосовуваного в подальшому алгоритму компресії. Розгляд різних ортонормованих перетворень, таких як ДПФ. ДКП, перетворення Хартлі, субсмугове перетворення та інших з позиції теорії інформації проведено авторами.

На сьогоднішній день відомо досить багато моделей, що дозволяють оцінити пропускну здатність каналу передачі прихованих даних. Нижче наведена одна з них, представлена в роботах.

Нехай C — первинне зображення (контейнер-оригінал), M — повідомлення, яке підлягає приховуванню. Тоді модифіковане зображення (стеганоконтейнер) $S = C + M$. Також передбачається, що модифіковане зображення S візуально неможливо відрізнити від первинного і воно може бути піддано в стеганоканалі компресії з втратами: $S^{\nabla} = \Theta(S)$, де $\Theta(\bullet)$ — оператор компресії.

Задача адресата — вилучити з отриманого контейнера S^{∇} вбудовані на попередньому етапі біти даних M_i.

Основне, що буде при цьому цікавити нас, — відповідь на питання: яку кількість біт можна ефективно вбудовувати в зображення і згодом витягти з нього за умови задовільно низької ймовірності помилок на останньому етапі. Іншими словами, яка пропускна здатність каналу передачі прихованих даних за умови наявності в каналі зв'язку певного алгоритму компресії? Блок-схема такого стеганоканалу представлена на Рис.2.5.

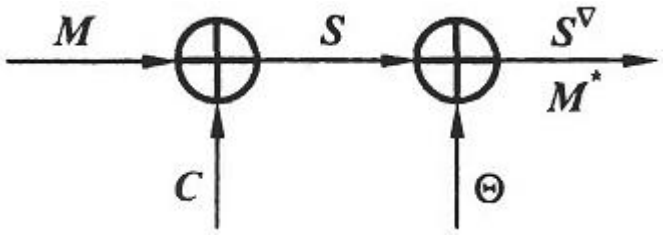

Рис.2.5 - Блок-схема стеганоканала з атакою у вигляді компресії

Повідомлення M передається по каналу, який має два джерела "шуму": C — зображення-контейнер і "шум" Θ, що виникає в результаті операції компресії/декомпресії. При цьому S^{∇} і M^{*} — можливо спотворені стеганоконтейнер і, як результат, — оцінка корисного повідомлення.Структурна схема стеганосистеми наведена на Рис.2.6.

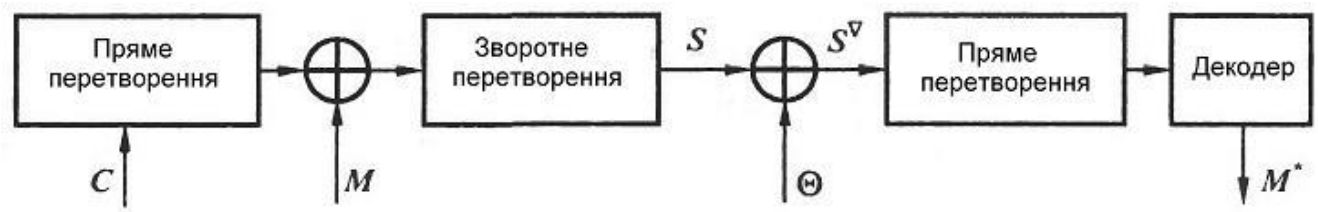

Рис.2.6 - Структурна схема стеганосистеми за наявності в стеганоканалі атаки компресії.

Зображення C розкладається на D субсмуг (пряме перетворення), в кожну з яких вбудовується приховувана інформація M. Після зворотного перетворення виходить модифіковане зображення S. Після компресії/декомпресії Θ в каналі зв'язку отримується зображення S^{∇}, яке на приймаючій стороні знову піддається прямому перетворенню і з кожної субсмуги D незалежно витягується приховане повідомлення — оцінка M^{*}.

Реальні зображення не являють собою випадкові процеси з рівномірно розподіленими значеннями величин. Відомо, і даний факт використовується в алгоритмах компресії, що більша частина енергії зображень зосереджена в низькочастотній (НЧ) області спектра. Звідси і виникає необхідність у здійсненні декомпозиції зображення на субсмуги, до яких додається стеганоповідомлення. НЧ субсмуги містять основну частину енергії зображення і, таким чином, носять шумовий характер. Високочастотні (ВЧ) субсмуги спектра зображення найбільшим чином піддаються впливу з боку різноманітних алгоритмів обробки, таких як, наприклад, компресія або НЧ-фільтрація. Таким чином, можна зробити висновок, що для вбудовування повідомлення найоптимальнішими є

середньочастотні (СЧ) субсмуги спектра зображення. Типовий розподіл шуму зображення та шуму обробки за спектром частоти зображено на Рис. 2.7

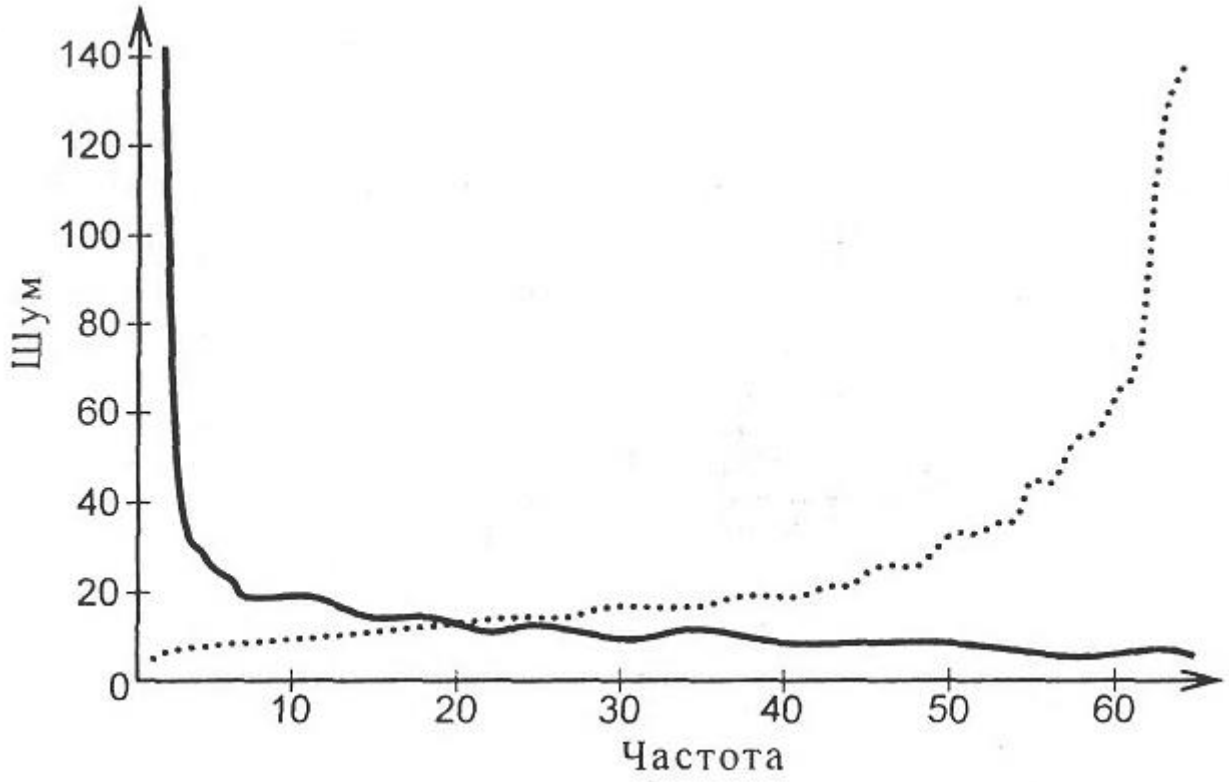

Рис.2.7 - Залежність шуму зображення (суцільна лінія) і шуму обробки (пунктирна лінія) від частоти.

Стеганографічний канал можна розкласти на ряд незалежних підканалів. Таке розкладання відбувається за рахунок виконання прямого і зворотного перетворень. У кожному з D підканалів існує по два джерела шуму. Нехай $\sigma^2_{\overline{N},\Theta_j}$, при $j = 1,\ldots,D$ — дисперсія коефіцієнтів перетворення (шум зображення) в кожному з підканалів. Тоді вираз для пропускної здатності каналу стеганосистеми набуде вигляду:

$$B = \frac{X \cdot Y}{2 \cdot D} \cdot \sum_{j=1}^{D} \log_2 \left(1 + \frac{\nu_j^2}{\sigma_{C_j}^2 + \sigma_{\Theta_j}^2} \right) \text{ біт}, \qquad (2.6)$$

Де ν_j — візуальний поріг для ***j-ї*** субсмуги (ν_j^2 — максимально допустима енергія стеганоповідомлення, виходячи з вимог збереження візуальної якості зображення); ***X*** і ***Y*** піксельний розмір зображення-контейнера.

Вибір значення візуального порогу базується на врахуванні властивостей ЗСЛ. Відомо, що шум у ВЧ областях зображення більш прийнятний, ніж в НЧ областях. Можна ввести деякі вагові коефіцієнти: $\nu_j^2 = \kappa \cdot \sigma_{\overline{N},\Theta_j}^{2\cdot\alpha}$, де $0 \le \alpha \le 1$, а $\kappa << \sigma_{\overline{N},\Theta_j} \ \forall\ j$ — константа.

Випадок, коли $\alpha = 0$, відповідає рівномірному розподілу стеганограмми по всім субсмугам. Випадок $\alpha = 1$ відповідає розподілу стеганограмми у відповідності з дисперсією субсмуг.

Після деяких спрощень можна отримати вираз для пропускної здатності каналу передачі прихованих даних:

$$B = \frac{X \cdot Y}{2 \cdot D} \cdot \sum_{j=1}^{D} \log_2 \left(1 + \frac{\kappa_1 \cdot \sigma_{\overline{N}_j}^{2\cdot\alpha}}{\sigma_{C_j}^2} \right) \approx \frac{X \cdot Y}{2 \cdot D} \cdot \log_2 \left(1 + \sum_{j=1}^{D} \frac{\kappa_1}{\sigma_{C_j}^{2\cdot(1-\alpha)}} \right).$$

Знак наближення у виразі є справедливим, оскільки $\kappa_1 \cdot \sigma_{\overline{N}_j}^{2\cdot\alpha} \Big/ \sigma_{C_j}^2 << 1$ для будь-якого значення j.

Очевидно, що при $\alpha = 1$ декомпозиція жодним чином не буде впливати на пропускну здатність стеганоканалу. При $\alpha < 1$ пропускна здатність буде зростати за рахунок того, що в області з низькою дисперсією (високочастотній області) стеганосигналу додається відносно більше енергії.

Відомо, що перетворення можна впорядкувати за можливими виграшами від алгоритму кодування. Рис.2.8.

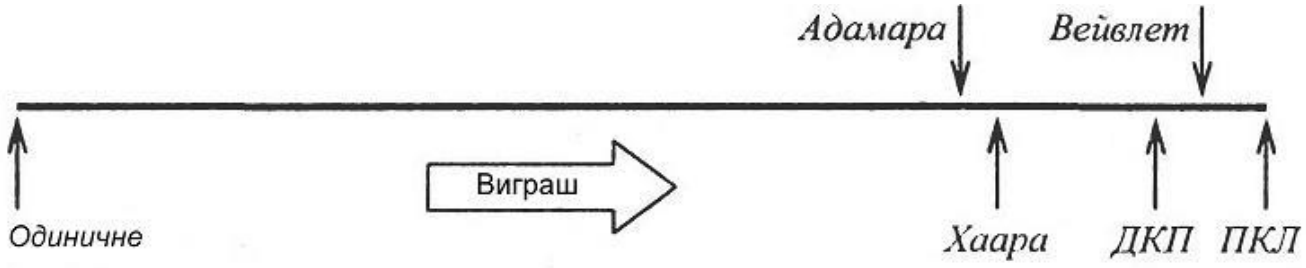

Рис.2.8. Види перетворень, впорядковані за можливими виграшами від використання алгоритму кодування.

Під виграшем від кодування мається на увазі ступінь перерозподілу дисперсій коефіцієнтів перетворення. Найбільший виграш дає перетворення Карунена-Лоєва (ПКЛ), найменший — розкладання за базисом одиничного імпульсу (тобто відсутність перетворення).

Перетворення, які характеризуються високими значеннями виграшу від кодування, такі як ДКП, вейвлет-перетворення, характеризуються різко нерівномірним розподілом дисперсій коефіцієнтів субсмуг. Високочастотні субсмуги не підходять для вбудовування через великий шум обробки, а низькочастотні через високий шум. Тому, як зазначалося , доводиться обмежуватися середньочастотними смугами, у яких шум зображення приблизно дорівнює шуму обробки. Оскільки таких смуг небагато, то пропускна здатність стеганоканалу є порівняно малою.

У разі застосування перетворення з більш низьким виграшем від кодування, наприклад, перетворення Адамара або Фур'є, існує більше блоків, у яких шум зображення приблизно дорівнює шуму обробки, а, отже, і пропускна здатність вище. Висновок, до якого прийшли автори зазначеної роботи, досить несподіваний: для підвищення пропускної здатності стеганографічного каналу доцільно застосовувати перетворення з меншими виграшами від кодування, які погано підходять для компресії сигналів.

Ефективність застосування вейвлет-перетворення та ДКП для компресії зображень пояснюється тим, що вони добре моделюють процес обробки зображення в ЗСЛ, відокремлюючи суттєві деталі від другорядних. Таким чином, дані перетворення більш доцільно використовувати у разі присутності активного

порушника, оскільки модифікація значимих коеффіцієнтв може призвести до неприйнятного спотворення зображення.

При застосуванні перетворень з низькими значеннями виграшу від кодування існує значна небезпека руйнування вбудованих даних, внаслідок того, що коефіцієнти перетворення менш стійкі до модифікацій. Однак при цьому існує велика гнучкість у виборі перетворення, і якщо останнє невідомо порушнику, то модифікувати стеганограмму буде значно складніше.

Під час цифрової обробки зображення часто застосовується двовимірна версія дискретного косинусного перетворення:

$$\Omega(\upsilon,\nu)=\frac{\zeta(\upsilon)\cdot\zeta(\nu)}{\sqrt{2\cdot N}}\cdot\sum_{x=0}^{N-1}\sum_{y=0}^{N-1}C(x,y)\cdot\cos\left[\frac{\pi\cdot\upsilon\cdot(2\cdot x+1)}{2\cdot N}\right]\cdot$$
$$\cdot\cos\left[\frac{\pi\cdot\nu\cdot(2\cdot y+1)}{2\cdot N}\right];\quad(2.7\,\text{а})$$

$$S(x,y)=\frac{1}{\sqrt{2\cdot N}}\cdot\sum_{\upsilon=0}^{N-1}\sum_{\nu=0}^{N-1}\zeta(\upsilon)\cdot\zeta(\nu)\cdot\Omega(\upsilon,\nu)\cdot\cos\left[\frac{\pi\cdot\upsilon\cdot(2\cdot x+1)}{2\cdot N}\right]\cdot$$
$$\cdot\cos\left[\frac{\pi\cdot\nu\cdot(2\cdot y+1)}{2\cdot N}\right],\quad(2.7\,\text{б})$$

де $C(x,y)$ і $S(x,y)$ — відповідно, елементи оригінального і відновленого за коефіцієнтами ДКП зображення розмірністю $N\times N$; x,y — просторові координати пікселів зображення; $\Omega(\upsilon,\nu)$ — масив коефіцієнтів ДКП; υ,ν — координати в частотній області; $\zeta(\upsilon)=1/\sqrt{2}$, якщо $\upsilon=0$, і $\zeta(\upsilon)=1$, якщо $\upsilon>0$.

Розглянемо існуючі методи, які базуються на алгоритмі ДКП[11].

2.3.2 Метод відносної заміни величин коефіцієнтів ДКП (метод Коха і Жао)

Один з найбільш поширених на сьогодні методів приховування конфіденційної інформації в частотній області зображення полягає у відносній заміні величин коефіцієнтів ДКП. Метод свого часу описали Кох (E. Koch) і Жао (J. Zhao).

На початковому етапі первинне зображення розбивається на блоки розмірністю 8×8 пікселів. ДКП застосовується до кожного блоку — формула (1.6 а), в результаті чого отримують матриці 8×8 коефіцієнтів ДКП, які часто позначають $\Omega_b(\upsilon,\nu)$, де b — номер блоку контейнера C, а (υ,ν) — позиція коефіцієнта в цьому блоці. Кожен блок при цьому призначений для приховування одного біта даних.

Було запропоновано дві реалізації алгоритму: псевдовипадково можуть вибиратися два або три коефіцієнти ДКП. Розглянемо перший варіант.

Під час організації секретного каналу абоненти повинні попередньо домовитися про два конкретні коефіцієнти ДКП з кожного блоку, які будуть використовуватися для приховування даних. Задамо дані коефіцієнти їх координатами в масивах коефіцієнтів ДКП: (υ_1,ν_1) і (υ_2,ν_2). Крім цього, зазначені коефіцієнти повинні відповідати косинус-функціям з середніми частотами, що забезпечить прихованість інформації в суттєвих для ЗСЛ областях сигналу, до того ж інформація не буде спотворюватися при JPEG-компресії з малим коефіцієнтом стиснення.

У зв'язку з низькою чутливістю ЗСЛ до каналу синього кольору секретне повідомлення вбудовують саме в нього.

Безпосередньо процес приховування починається з вибору випадкового блоку C_b зображення, призначеного для кодування b-го біта повідомлення. Вбудовування інформації здійснюється таким чином: для передачі біта "0" прагнуть, щоб різниця абсолютних значень коефіцієнтів ДКП перевищувала

деяку позитивну величину, а для передачі біта "1" ця різниця робиться меншою в порівнянні з деякою від'ємною величиною:

$$\begin{cases} \left| \Omega_b(\upsilon_1,\nu_1) \right| - \left| \Omega_b(\upsilon_2,\nu_2) \right| > P, \text{при } m_b = 0; \\ \left| \Omega_b(\upsilon_1,\nu_1) \right| - \left| \Omega_b(\upsilon_2,\nu_2) \right| < -P, \text{при } m_b = 1. \end{cases} \quad (2.8)$$

Коефіцієнт в лівому верхньому куті матриці Ω_b — $(\Omega_b)_{1.1}$ містить інформацію про яскравість всього сегменту (його називають DC-коефіцієнтом). Інші коефіцієнти називаються AC-коефіцієнтами. Зазначимо, що коефіцієнти НЧ компонентів розміщені ближче до лівого верхнього кута, а ВЧ компонентів ближче до правого нижнього кута. (Рис.2.9).

Таким чином, первинне зображення спотворюється за рахунок внесення змін до коефіцієнтів ДКП, якщо їх відносна величина не відповідає приховуваному біту. Чим більше значення P, тим стеганосистема, створена на основі даного методу, є більш стійкою до компресії, проте якість зображення при цьому значно погіршується.

Після відповідного внесення корекції в значення коефіцієнтів, які повинні задовольняти нерівностям (2.8), проводиться зворотне ДКП[12].

Для вилучення даних, в декодері виконується аналогічна процедура вибору коефіцієнтів, а рішення про переданий біт приймається у відповідності з наступним правилом:

$$\begin{cases} m_b^* = 0, \ при \ \left| \Omega_b^*(\upsilon_1,\nu_1) \right| > \left| \Omega_b^*(\upsilon_2,\nu_2) \right|; \\ m_b^* = 1, \ при \ \left| \Omega_b^*(\upsilon_1,\nu_1) \right| < \left| \Omega_b^*(\upsilon_2,\nu_2) \right|. \end{cases} \quad (2.9)$$

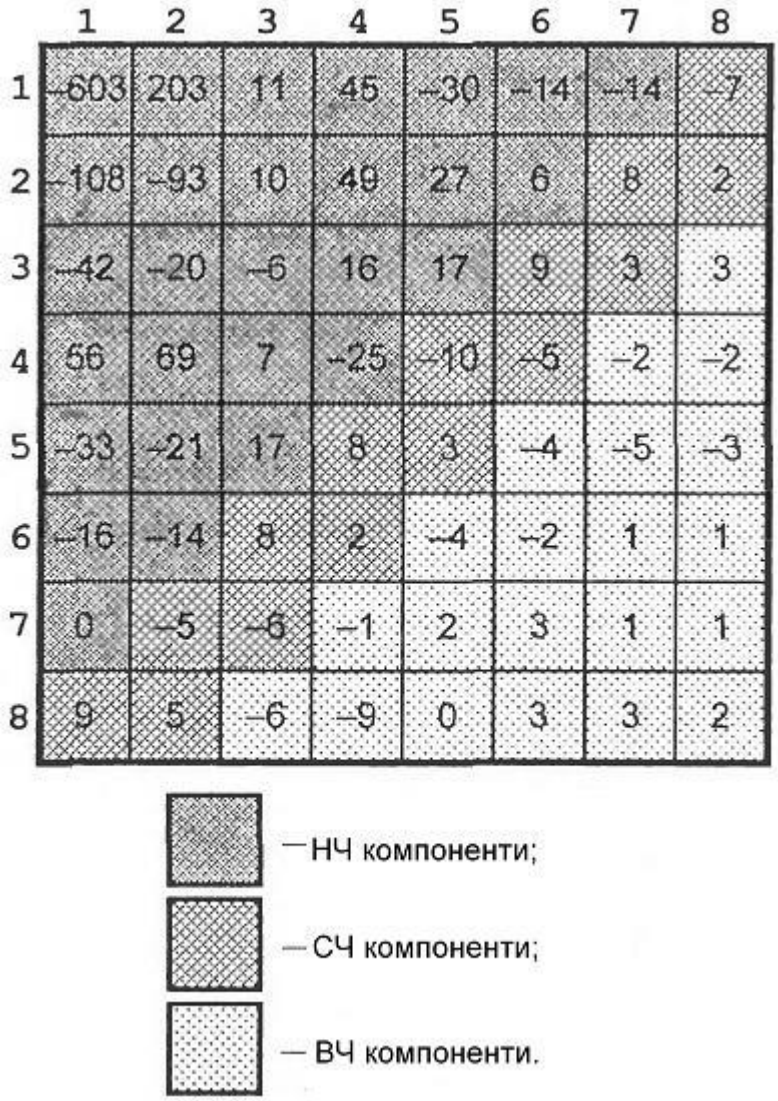

Рис.2.9. Приклад масиву Ω коефіцієнтів ДКП.

2.3.3 Метод Бенгама-Мемона-Ео-Юнг

Бенгам (D. Benham), Мемон (N. Memon), Ео (B.-L. Yeo) і Юнг (Minerva Yeung) запропонували оптимізовану версію описаного вище методу. Причому оптимізація була проведена за двома напрямками: по-перше, було запропоновано для вбудовування використовувати не всі блоки, а тільки найбільш придатні для цього, по-друге, в частотній області блоку для вбудовування вибираються не два, а три коефіцієнти ДКП, що, як буде показано далі, істотно зменшує візуальні спотворення контейнера. Розглянемо зазначені удосконалення більш докладно[12].

Придатними для вбудовування інформації вважаються такі блоки зображення, які одночасно задовольняють наступним двом вимогам:

1. Блоки не повинні мати різких переходів яскравості;
2. Блоки не повинні бути занадто монотонними.

Блоки, які не відповідають першій вимозі, характеризуються наявністю занадто великих значень низькочастотних коефіцієнтів ДКП, співставних по своїй величині з DC-коефіцієнтом. Для блоків, які не задовольняють другій вимозі, характерна рівність нулю більшості високочастотних коефіцієнтів. Зазначені особливості є критерієм відкидання непридатних блоків.

Зазначені вимоги відкидання враховуються використанням двох порогових коефіцієнтів: P_L (для першої вимоги) та P_H (для другої вимоги), перевищення (P_L) або недосягнення (P_H) яких буде вказувати на те, що даний блок не придатний для модифікації в частотній області.

Вбудовування в блок біта повідомлення здійснюється наступним чином. Вибираються (для більшої стійкості стеганосистеми — псевдовипадково) три коефіцієнти ДКП блоку із середньочастотної області з координатами (υ_1, ν_1), (υ_2, ν_2) і (υ_3, ν_3). Якщо необхідно провести вбудовування "0", ці коефіцієнти змінюються таким чином (якщо, звичайно, це необхідно), щоб третій коефіцієнт став менше будь-якого з перших двох; якщо необхідно приховати "1", він стає більшим у порівнянні з першим і другим коефіцієнтами:

$$\begin{cases} \left.\begin{array}{l} |\Omega_b(\upsilon_3,\nu_3)| < |\Omega_b(\upsilon_1,\nu_1)|; \\ |\Omega_b(\upsilon_3,\nu_3)| < |\Omega_b(\upsilon_2,\nu_2)|. \end{array}\right\}, \text{при } m_b = 0; \\ \left.\begin{array}{l} |\Omega_b(\upsilon_3,\nu_3)| > |\Omega_b(\upsilon_1,\nu_1)|. \\ |\Omega_b(\upsilon_3,\nu_3)| > |\Omega_b(\upsilon_2,\nu_2)|. \end{array}\right\}, \text{при } m_b = 1. \end{cases} \qquad (2.10)$$

Як і в попередньому методі, для прийняття рішення про достатність розрізнення зазначених коефіцієнтів ДКП, у вираз (2.10) вводиться значення порогу розрізнення P:

$$\begin{cases} |\Omega_b(\upsilon_3,\nu_3)| < \min(|\Omega_b(\upsilon_1,\nu_1)|,|\Omega_b(\upsilon_2,\nu_2)|) - P, \text{ при } m_b = 0; \\ |\Omega_b(\upsilon_3,\nu_3)| > \max(|\Omega_b(\upsilon_1,\nu_1)|,|\Omega_b(\upsilon_2,\nu_2)|) + P, \text{ при } m_b = 1. \end{cases} \quad (2.11)$$

У тому випадку, якщо така модифікація призводить до занадто великої деградації зображення, коефіцієнти не змінюють, і блок в якості контейнера не використовується.

Використання трьох коефіцієнтів замість двох і, що найголовніше, відмова від модифікації блоків зображення у випадку неприйнятних їх спотворень, зменшує похибки, які вносяться повідомленням. Одержувач завжди може визначити блоки, в які не проводилося вбудовування, просто повторивши аналіз, аналогічний виконаному на стороні передачі.

У процесі домовленості між сторонами прихованого обміну щодо алгоритму псевдовипадкового вибору трьох пар координат коефіцієнтів ДКП і значень порогів відбраковування обов'язково повинна бути присутня фаза перевірки обраного в якості контейнера зображення (набору зображень) на достатність його пропускної здатності. Іншими словами, після встановлення певних значень порогів P_L і P_H, обчислюється кількість блоків, визнаних придатними для вбудовування, і виконується оцінка візуального спотворення контейнера. За отриманими результатами приймається рішення про достатність обраних значень порогів або ж про необхідність їх зміни.

Наведемо результати обчислення кількості придатних блоків $N_{C_{opt}}$ у залежності від параметрів P_L і P_H. (Рис.2.10).

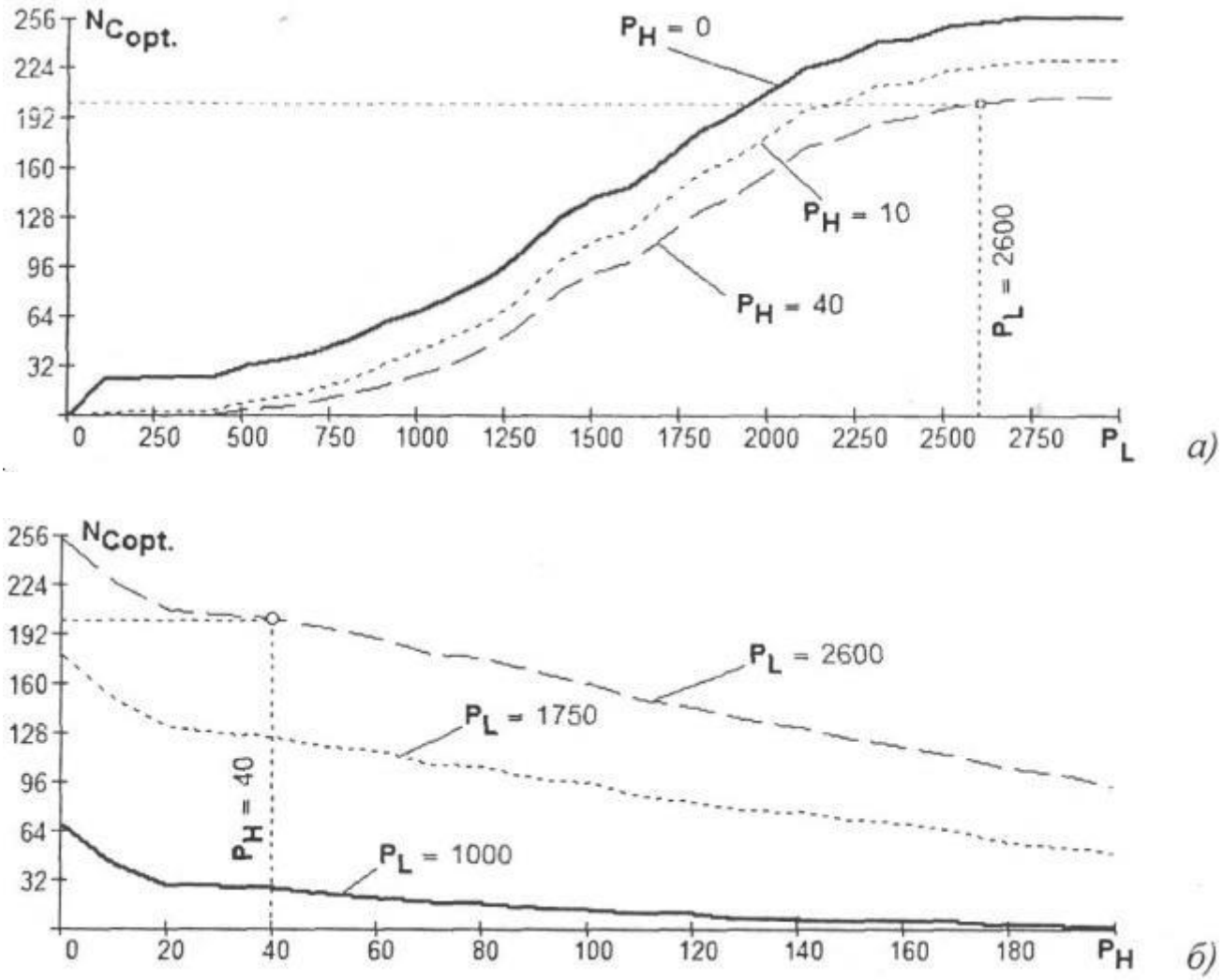

Рис.2.10. Залежність кількості придатних для вбудовування блоків від значень порогів P_L і P_H: $P_L = \text{var}$, $P_H = const(a)$; $P_L = const$, $P_H = \text{var}(б)$

2.3.4 Метод Хсу і Ву

Хсу (Chiou-Ting Hsu) і Ву (Ja-Ling Wu) [26] було запропоновано алгоритм вбудовування цифрового водяного знака у масив коефіцієнтів ДКП блоків зображення-контейнера. Наведемо основні положення, закладені авторами в основу алгоритму.

Нехай C — напівтонове зображення розміром $X \times Y$, а W — ЦВЗ, який представляє собою бінарне зображення розміром $A \times Z$. У ЦВЗ піксель може приймати значення або «1», або «0». Зрозуміло, що безпосереднє спостереження

такого зображення неможливо, оскільки інтенсивності 0 і 1 відповідають чорному кольору (остання в деякому наближенні). Зображення ЦВЗ можна створити чорно-білим, а перед утаєнням замінити інтенсивність білих пікселів (255) на одиницю, наприклад, шляхом поділу всього масиву ЦВЗ на 255. Під час вилучення, навпаки, для візуального спостереження масив ЦВЗ необхідно помножити на 255.

Оскільки, як буде показано в подальшому, під час вбудовування ЦВЗ буде оброблятися тільки середньочастотний діапазон сигналу-контейнера, необхідною передумовою є те, що ЦВЗ повинен мати менший у порівнянні з контейнером розмір. Так, наприклад, для контейнера, розбитого на блоки 8×8, при вбудовуванні ЦВЗ оптимальним буде використання $64\cdot A\cdot Z/(X\cdot Y)$ коефіцієнтів ДКП. Відношення $A\cdot Z/(X\cdot Y)$ в даному випадку визначає ту кількість інформації, яка може бути вбудована в обране в якості контейнера зображення (в наведеному прикладі — до 64 коефіцієнтів блоку 8×8). Для більшої стійкості і прихованості результатів використання розглянутого стеганометода кількість вбудованої інформації на практиці намагаються зменшити.

Зображення-контейнер C і ЦВЗ W представимо як:

$$C=\{c(x,y);\ 1\le x\le X;\ 1\le y\le Y\},$$

$$W=\{w(a,z);\ 1\le a\le A;\ 1\le z\le Z\},$$

де $c(x,y)\in\{0,\ldots,2^L-1\}$ — інтенсивність пікселя (x,y); L — кількість біт, що використовується для квантування інтенсивностей; $w(a,z)\in\{0,1\}$ — двійкові значення пікселя (a,z) ЦВЗ.

Контейнер C можна розбити на $\frac{X}{8}\times\frac{Y}{8}$ блоків розмірністю 8×8. Для отримання цієї ж кількості блоків, ЦВЗ розбивається на блоки розмірністю

$\frac{8 \cdot A}{X} \times \frac{8 \cdot Z}{Y}$. Наприклад, якщо $A = X/2$ і $Z = Y/2$, розмірність блоку ЦВЗ складе 4×4, якщо ж $A = X/4$ і $Z = Y/4$, — 2×2 і т.д.

Для створення контейнера або ЦВЗ необхідної розмірності, до останніх можуть бути додані додаткові стовпці або рядки.

Висновки до другого розділу

Результатом анализу таких стеганографічних методів як:

- метод найменш значущого біта (НЗБ);
- метод псевдовипадкового інтервалу;
- метод блочного приховування;
- метод заміни палітри;
- метод квантування зображення;
- метод Дармстедтера-Делейгла-Квісквотера-Макка;
- метод відносної заміни величин коефіцієнтів ДКП (метод Коха і Жао);
- метод Бенгама-Мемона-Ео-Юнга;
- метод Хсу і Ву.

можна вважати висновок про доцільність для приховування у відео файлах саме методу найменш значущого біта. Такий висновок базується на можливості застосування цього методу як для графічних, так і аудіо файлах приблизно за однаковою методикою.

РОЗДІЛ 3 ШУМИ

В даний час проблема захисту інформаційних ресурсів стає все більш гострою в зв'язку з широким використанням електронного документообігу, оскільки передача інформації здійснюється в основному через незахищені телекомунікаційні канали. У той же час застосування криптографічного шифрування, щоб запобігти несанкціонованому доступу, не завжди вирішує проблему, оскільки привертає небажану увагу до самого факту передачі важливої інформації. Як альтернативний шлях останнім часом використовують стеганографічні методи, коли факт інформаційного обміну залишається прихованим. Однак пропускна здатність такого каналу вельми обмежена.

Основні (але не єдині) методи вбудовування прихованих повідомлень базуються на аналогової природі вихідних файлів, використовуваних як контейнери для «транспортування» прихованого повідомлення. Мова, перш за все, йде про аудіо і графічні файли, призначені для прослуховування або перегляду. З огляду на недосконалість слуховий і зорової системи людини з точки зору роздільної здатності, частина інформації, що міститься в файлах, може бути без шкоди для сприйняття модифікована або видалена. Саме ця частина, яка сприймається людиною як шум, є корисною для організації прихованого інформаційного обміну і визначає потенційну пропускну здатність стеганоканала. Виходячи з експериментальних даних, роздільна здатність слуховий і зорової системи людини не перевищує 0,4 ... 0,8%, тобто людина розрізняє не більше 64 ... 128 рівнів гучності або відтінків червоного, блакитного або зеленого кольору на зображенні. Це означає, що після деякого значення подальше збільшення рівнів квантування при оцифруванні аналогових сигналів і, відповідно, кількість пікселів матриці цифрової фотокамери для людини не призводить до помітного поліпшення якості, тобто непомітно.

Іншими словами, якщо цей рівень перевищений при передачі відповідних файлів по реальному каналу, то має місце надлишкова і прихована пропускна

здатність каналу передачі Cγ. У загальному випадку оцінити величину Cγ досить складно, оскільки на неї істотно впливає спосіб перетворення аналогового сигналу в цифровий. Наприклад, при аналогово-цифровому перетворенні аудіо сигналу необхідно враховувати частоту дискретизації та вимоги до якості передачі (смугу відтворюваних частот або смугу про-пускання використовуваного каналу передачі).

Так, в традиційних мережах багатоканального телефонного зв'язку частота дискретизації df = 8кГц, і необхідну якість досягається при 8-бітовом кодуванні кожного відліку. Реально без помітного для користувача погіршення якості можна зменшити розрядність кожного відліку до семи біт, а молодший, найменш значущий біт (НЗБ) використовувати для прихованого вкладення. По суті, це і є основна ідея методу НЗБ, який багаторазово описаний в різних літературних джерелах [13,14]. З іншого боку, цей «найменш значущий біт» можна інтерпретувати як шум каналу.

3.1 Постановка завдання

З точки зору кінцевого користувача, для якого призначена інформація контейнера, цей «шум» не відрізняється від шуму, створюваного завадами в каналі, або шуму, накладеного на первинний аналоговий сигнал при записі від мікрофона (шум в приміщенні) або нерівномірності освітлення при зйомці. Але цей шум незалежно від його походження або джерела для створення стеганоканала є корисним - чим більше такого «шуму», тим краще. Тому може бути виправданим штучне внесення шумової складової, що збільшує пропускну здатність стеганоканала (зрозуміло, кількість інформації, переносний контейнером, відповідно зменшиться). Необхідно, очевидно, проаналізувати джерела цифрового шуму в файлах, які використовуються в якості контейнерів.

3.2 Джерела шуму

Розглянемо джерела шуму, які можуть виявитися корисними для збільшення корисного об'єму контейнера.

3.2.1 Цифровий шум

Цифровий шум - це дефекти зображення, які вносяться матрицею цифрового фотоапарата. Вони проявляються як дрібні елементи зображення у вигляді світлих, темних або кольорових крапок, що заповнюють цілі області. Цей шум помітний на однотонних областях. Розрізняють яскравості і хроматичний шум. У першому випадку це невеликі ділянки зображення, які мають відмінності в яскравості, у другому - в кольорі. Рівень цифрового шуму залежить від моделі камери і може бути знижений при використанні спеціальних програм шумозаглушення. Не зупиняючись тут на детальному аналізі фізичних і навіть хімічних чинників, що впливають на рівень шуму, відзначимо, що цифровий шум присутній практично у всіх зображеннях, отриманих за допомогою цифрових фотокамер. Найбільш істотними факторами, що впливають на рівень шуму, є світлочутливість сенсора (матриці) і експозиція. Наприклад, на затемнених недоекспонованих ділянках зображення, а також на фотографіях, знятих з великою експозицією при недостатньому освітленні, можна побачити невеликі різнокольорові точки прямокутної або невизначеної форми. На ділянках, які добре освітлені, як правило, шум не проявляється. Інший важливий параметр - експозиція. Чим більше експозиція, тим вище рівень шуму. Це проявляється під час нічної зйомки і зйомки без спалаху при слабкому освітленні.

3.2.2 Шуми, що виникають при скануванні зображень

Ще один поширений вид цифрового шуму - це завади, які виникають, наприклад при використанні сканерів. Виявляється цей шум при збільшенні зображень у вигляді точок (кластерів). Крім того, рівень шуму залежить,

очевидно, від якості підкладки (паперу), на якій надруковано (намальовано) зображення.

Ясно, що дефекти підкладки також будуть перенесені в файл при скануванні і еквівалентні шумовий складової. Не потрібно також забувати, що певний рівень шуму завжди присутній в будь-якому електричному сигналі як результат зовнішніх завад і наведень від сторонніх джерел електромагнітного випромінювання. Такий шум стає особливо помітним при передачі аналогових сигналів по кабелю або через ефір. Слід також виділити в окремий клас шуму, що виникає при квантуванні та оцифрування аналогового сигналу. Такий шум проявляється у вигляді «снігу», гранулювання або безладно розташованих точок на зображенні. Це результат нестабільності роботи електроніки при зміні температури. Такий же шум може з'явитися при надмірно великій розрядності АЦП при перетворенні аналогового сигналу (так зване «тремтіння» молодшого біта).

Шум найбільш помітний на темних ділянках зображення, оскільки при сталості абсолютного рівня шумовий складової рівень сигналу зменшується і відповідно зменшується відношення сигнал\шум. На світлих ділянках це не проявляється. Саме для мінімізації такого шуму перед скануванням виконують калібрування для корекції базового напруги світлочутливих елементів. Регулярний шум, який є результатом перехресних завад і взаємних наведень, проявляється у вигляді смуг на зображенні і не представляє інтересу з точки зору можливості використання в якості корисного об'єму для прихованих вкладень. Крім перерахованих джерел і причин виникнення шумової складової будь-яка обробка сигналів електронними приладами супроводжується присутністю так званого дробового шуму. Виникає він як результат флуктуацій внаслідок дискретності зарядів, які створюють струм в електронних і напівпровідникових приладах. Оскільки електрони починають свій рух в випадкові моменти часу і ці моменти незалежні один від одного, спектральна щільність дробового шуму не залежить від частоти, то цю складову можна віднести до білого шуму.

3.2.3 Тепловий шум

Ще один різновид шуму - тепловий шум. Електричний струм крім спрямованого руху електронів містить складову, яка визначається їх хаотичним (ненаправленим) тепловим рухом, що призводить до випадкових коливань щільності струму і, відповідно, напруги на вході, наприклад, сенсора.

Дисперсія теплового шуму визначається формулою Найквіста

$$U_ш \times U_ш = 4KTRB$$

де K - постійна Больцмана, R = 1,38 ·10-23 Дж / К, Т - абсолютна температура, В – ефективна смуга частот, в якій проводять вимірювання рівня теплового шуму.

Ця формула визначає теплові шуми активних опорів при будь-яких температурах, за винятком наднизьких. Наведена формула показує, що спектральна щільність теплового шуму, тобто потужність, віднесена до одиночного інтервалу частоти, не залежить від частоти. Такий шум можна вважати «білим» і в першому наближенні моделювати рівномірно розподіленими різнокольоровими точками на зображенні.

Перераховані та деякі інші різновиди шуму є природними в тому розумінні, що шумова складова присутня в контейнері незалежно від бажання користувача і для звичайного (традиційного) інформаційного обміну є небажаною. Але для організації прихованого обміну ця складова виявляється корисною, оскільки дозволяє (принаймні, потенційно) збільшити корисне навантаження контейнера.

3.2.4 Цілеспрямоване штучне введення шумовий складової

Найбільш простим і очевидним способом збільшення шумовий компоненти (і, тим самим, і пропускної здатності стеганоканала) є додавання шумовий е.р.с. ще на електричному рівні, додавши її до аналогового сигналу. Те ж саме можна реалізувати і на акустичному рівні, записуючи файл-контейнер від мікрофона в зашумлення штучно приміщенні (студії). Аналогічно для зображень штучний шум може бути доданий на рівні освітлення (наприклад, зйомці в умовах слабкого освітлення і, відповідно, тривалої експозиції або скануванні зображень, надрукованих на папері невисокої якості). Шум може бути внесений і шляхом цілеспрямованої корекції або модифікації файлу-контейнера.

3.3 Графічні файли фотознімків

У цьому випадку шум може бути внесений програмно за допомогою інструментів програми Photoshop [15]. При кодуванні в комп'ютерній графіці зображення розуміється комп'ютером як таблиця, яка складається з маленьких осередків одного і того ж розміру, кожному у тому числі присвоюється колірне значення в залежності від займаної їй площі. Коли обробляється зображення, комп'ютер запам'ятовує ідентифіковану таблицю зображення, осередки в якій є інформація про колір елементів цього зображення. Практично всі ефекти, що застосовуються до вихідного зображення, збільшують його бітовий обсяг. Наприклад, застосувавши до зображення кілька ефектів, пов'язаних з шумами, оцінимо зміна обсягу зображень. Початковий розмір зображення 2,8 Мб.

Ефект	Розмір (Мб)	Коментарі
+ 10% гауссовский шуму	4,1 Мб	Внесення дрібних деталей істотно збільшує розмір.
+ 50% гауссовский шуму	5,9 Мб	Внесення дрібних деталей істотно збільшує розмір
+ 100% гауссовский шуму	6,3 Мб	Слід зауважити відсутність лінійної залежності між рівнем шуму і розміром оскільки пікселі шуму все більше і більше перекривають один одного
Зменшення шуму з максимальними значеннями різкості і колірного шуму	1,4 Мб	Зменшення розміру в 2 рази пояснюється зменшенням деталізації об'єкту, і так само зниженням кількості колірних тонів
Гауссовского розмиття в 1 піксель	611 Кб	Зменшення розміру пояснюється зменшенням деталізації об'єкта
Гауссовское розмиття в 5 пікселів	340 Кб	Пояснюється тим, що один піксель приймають на себе значення п'яти, і тому знижується кількість інформації

Таблиця 3.1 - Залежність розміру картинки від застосовуваного ефекту

3.4 Аудіофайли

Перетворення аналогового звуку в цифровий при використанні формату WAV в максимальному ступені зберігає вихідний звук з певним ступенем точності, але розмір файлу виявляється досить великим. Наприклад, при частоті дискретизації 44 кГц (16 бітів на відлік, стерео) розмір файлу буде складати $44 \cdot 16 \cdot 2 = 1408$ кбіт в одній секунді звучання або 1408/8 = 176 кбайт.

Використання формату MP3. Цей спосіб дозволяє істотно зменшити розмір файлу. Досягти цього можна, якщо прибрати деякі частоти, поза частотного діапазону чутності людини. Аудіостеганографія приховує повідомлення в області частот, які не сприймаються людським вухом [16] На слух результат анітрохи не відрізняється від оригіналу за якістю звучання.

а) б)

Рис.3.1 - Частотна діаграма оригінального звукового фрагмента (а) і той же фрагмент, але з прихованим повідомленням (б)

Існує кілька методів аудіостеганографії: Ехо-методи застосовуються в цифровий аудіостеганографії і використовують нерівномірні проміжки між ехо-сигналами для кодування послідовності значень. При накладенні ряду обмежень дотримується умова непомітності для людського сприйняття. Відлуння характеризується трьома параметрами: початкової амплітудою, ступенем загасання, затримкою. При досягненні певного порогу між сигналом і луною вони змішуються. У цій точці людське вухо не може вже відрізнити ці два сигнали. Відлуння-методи стійкі до амплітудних і частотних атак, але нестійкі до атак по часовим характеристикам. Фазове кодування - також застосовується в

цифровий аудіостеганографії. Відбувається заміна вихідного звукового елемента на відносну фазу, яка і є секретним повідомленням.

Фазовий кодування є одним з найбільш ефективних методів приховування інформації. Метод розширеного спектра полягає в тому, що спеціальна випадкова послідовність вбудовується в контейнер, потім, використовуючи узгоджений фільтр, ця послідовність детектирується. Даний метод дозволяє вбудовувати велика кількість повідомлень в контейнер, і вони не будуть створювати завади один одному. Метод запозичений з широкосмугового зв'язку.

Ефект	Розмір (Мб)	Коментарі
Початковий файл	7,7	Довжина аудіо-доріжки 3 хв 24 сек
Внесення даних в тег метаданих	7,9	Тег ID3v1 не дозволить зберегти багато даних і жорстко регламентований, але ось ID3v2.4, як видно зі збільшення розміру здатний зберігати більшу кількість інформації СТКО регламентований, але ось ID3v2.4, як видно зі збільшення розміру здатний зберігати більшу кількість інформації
Внесення фазових змін	8,3	Розмір файлу збільшився, але все залежить від кількості змін
Вбудовування спеціальних випадкових послідовності	8,9	обсяг файлу безпосередньо залежить від обсягу внесених послідовностей

Таблиця 3.2 - Залежність розміру аудіо-файлу від застосовуваного методу

Таким чином, самий звичайний на перший погляд (і слух) формату MP3-файл може містити в собі великий обсяг прихованої інформації.

3.5 Відео файли

Незважаючи на те, що існує велика кількість відео форматів, на практиці для приховування інформації використовуються формати MPEG-2 і MPEG-4. Розглянемо три способи впровадження інформації в файли формату MPEG-2 Метод вбудовування інформації на рівні коефіцієнтів. Біти вбудовуються в коефіцієнти дискретного косинусного перетворення (ДКП). Головною проблемою модифікації коефіцієнтів ДКП в стисненому потоці відео є накопичення зсуву або помилок. Спотворення, викликані зміною коефіцієнтів ДКП, можуть поширюватися в часовій і просторовій областях. Тому для компенсації спотворень додають спеціальний сигнал. В силу обмеження на бітову швидкість, при впровадженні змінюються лише 10-20% коефіцієнтів ДКП. При використанні даного методу приховувана інформація зберігається при фільтруванні,

Метод вбудовування інформації на рівні бітової площині. Цей метод відрізняється високою пропускною здатністю і невеликої обчислювальної складністю. Але є і істотний недолік: інформація, вбудована таким чином, може бути легко видалена. При повторному накладення послідовності біт якість відео погіршиться, а прихована інформація буде знищена. Метод вбудовування інформації за рахунок енергетичної різниці між коефіцієнтами. В основі цього методу лежить диференціальне вбудовування енергії. Складність алгоритму незначно вище складності методу вбудовування на рівні бітової площини і значно нижче складності методу, заснованого на кореляції з компенсацією помилок передбачення. Метод може бути застосований не лише до відеоданих MPEG, але і до інших алгоритмам стиснення відео. Інформація вбудовується шляхом видалення декількох коефіцієнтів ДКП, і це має свої переваги. По-друге, в стислий потік відеоданих не треба нічого додавати, можна обійтися без повторного стиснення відновленого потоку відео. По-друге, видалення

високочастотних коефіцієнтів буде зменшувати розмір стегообраза потоку стиснених відеоданих в порівнянні з вихідним потоком. Алгоритм вносить в відео кілька менше спотворень, ніж метод вбудовування інформації на рівні бітової площині. Для видалення прихованої інформації потрібне проведення більш складних обчислювальних операцій, ніж вбудовування нової довільної бітової послідовності. видалення високочастотних коефіцієнтів буде зменшувати розмір стегообраза потоку стиснених відеоданих в порівнянні з вихідним потоком. Алгоритм вносить в відео кілька менше спотворень, ніж метод вбудовування інформації на рівні бітової площині. Для видалення прихованої інформації потрібне проведення більш складних обчислювальних операцій, ніж вбудовування нової довільної бітової послідовності. Видалення високочастотних коефіцієнтів буде зменшувати розмір стегообраза потоку стиснених відеоданих в порівнянні з вихідним потоком. Алгоритм вносить в відео менше спотворень, ніж метод вбудовування інформації на рівні бітової площині. Для видалення прихованої інформації потрібне проведення більш складних обчислювальних операцій, ніж вбудовування нової довільної бітової послідовності.

ефект	Розмір (Мб)	Коментарі
Початковий файл	45,5	
Вбудовування в ДКП	47,2	Тільки 10-20% коефіцієнтів ДКП використовуються, тим не менш, інформація зберігається при дискретизації, зашумлення і фільтруванні
Вбудовування на рівні бі товой площині	48,9	Висока пропускна здатність, але невелика надійність
метод	46,75	Більш низький обсяг файлу досягається за рахунок видалення «зайвих» коефіцієнтів ДКП

Таблиця 3.3 - Залежність розміру відео-файлу від застосовуваного методу

На закінчення слід зазначити, що крім методу НЗБ можуть бути використані і інші підходи, які не передбачають первинної аналогової природи файлу контейнера і недосконалості слуховий або зорової системи людини. Для пояснення можна задати собі питання: чи так уже необхідна візуальна (слухова) непомітність різниці між заповненим і порожнім контейнером? Уявімо, що в якості контейнера використовується файл записаного музичного твору. Навіть якщо змінити оркестровку виконання, навряд чи для пересічного слухача, який

вперше прослуховує файл, це буде дивним і підозрілим. У той же час зміною оркестровки можна істотно збільшити обсяг файлу і, відповідно, потенційні можливості збільшення корисного об'єму для прихованого інформаційного обміну. Аналогічно при зміні вихідного зображення шляхом корекції яскравості, контрастності, колірного балансу і т.п. в значних межах не викличе підозр. Можна піти далі. А якщо взагалі замість одного файлу передавати по каналу інший файл (контейнер)? Наприклад, замість однієї картинки іншу, замість однієї пісні іншу, або замість одного тексту інший? А бітову різницю між ними використовувати для вкладення СВ?

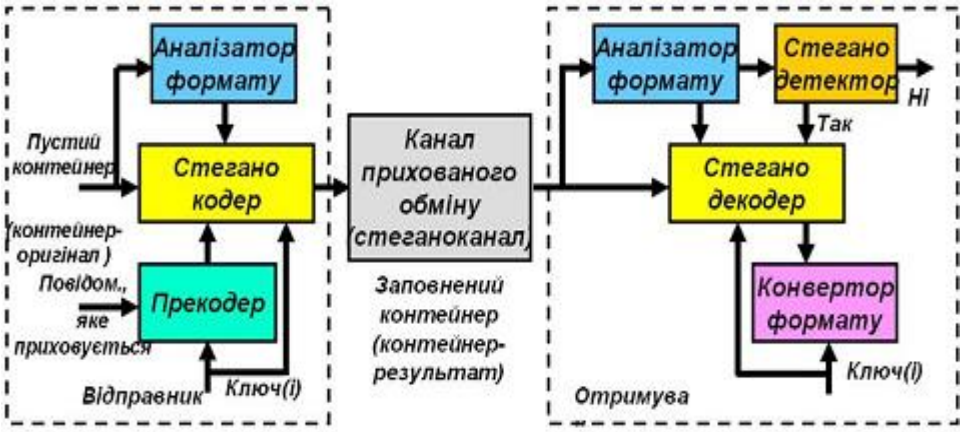

Рис. 3.2 - Загальна схема організації стеганоканала

У загальному випадку розглянутий підхід передбачає процедуру створення стеганоканала шляхом попередньої корекції файлу контейнера, обчислення побітової різниці між вихідним файлом і його модифікацією і завантаженням СВ (рис.2). На цій схемі показаний також блок формування адрес завантаження СВ за допомогою генератора псевдовипадкових чисел (ГПВЧ). Точно такий же генератор повинен бути в складі засобів (апаратних або програмних) одержувача СВ. Крім того необхідна синхронізація генераторів шляхом обміну стартовими числами (бітовими комбінаціями), наприклад, за допомогою протоколу Діффі-Хеллмана.

Висновки до третього розділу

На основі існуючих підходів до застосування стеганографії з різними контейнерами був проведений аналіз відомих методів та з використанням різних контейнерів. Проведено дослідження впливу наявності у вихідних контейнерах шумових складових і оцінка збільшення пропускної здатності каналу за рахунок штучного внесення шумової складової в вихідне зображення, що збільшує пропускну здатність стеганоканала (зрозуміло, кількість інформації, що переноситься контейнером, відповідно зменшиться). Наведено загальну схему організації стеганоканала шляхом попередньої корекції файлу контейнера, обчислення по бітової різниці між вихідним файлом і його модифікацією з вкладенням прихованої інформації. Сформульовано рекомендації щодо використання та вибору найбільш раціонального методу в залежності від поставленого завдання.

РОЗДІЛ 4 РОЗРОБЛЕННЯ СТАРТАП - ПРОЕКТУ

4.1 Опис ідеї проекту

Проаналізовано та подано у вигляді таблиць:

- зміст ідеї (що пропонується);
- можливі напрямки застосування;
- основні вигоди, що може отримати користувач товару (за кожним напрямком застосування);
- чим відрізняється від існуючих аналогів та замінників.

Зміст ідеї	Напрямки застосування	Вигоди користувача
Збільшення пропускної здатності каналу за рахунок штучного внесення шумової складової в відеоконтейнер, що збільшує пропускну здатність стеганоканалу	Прихований інформаційний обмін при використанні каналів загальног призначення	Інформаційний обмін є прихованим і не викликає підозри при застосуванні шифрування

Таблиця 4.1 – Опис ідеї стартап-проекту

4.2 Технологічний аудит ідеї проекту

В межах даного підрозділу проведено аудит технології, за допомогою якої можна реалізувати ідею проекту. Визначення технологічної здійсненності ідеї проекту передбачає аналіз таких складових (табл.4.2):

- за якою технологією буде виготовлено товар згідно ідеї проекту;
- чи існують такі технології чи їх потрібно розробити/допрацювати;
- чи доступні такі технології авторам проекту.

№ п/п	Ідея проекту	Технології її реалізації	Наявність технологій	Доступність технологій
1	Збільшення пропускної здатності каналу за рахунок штучного внесення шумової складової в відеоконтейнер, що збільшує пропускну здатність стеганоканалу	Хостинг	Наявні	Доступно
		Спеціальне програмне забезпечення для ПК	Потребує розробки	Доступно

Таблиця 4.2 – Технологічна здійсненність ідеї проекту

4.3 Аналіз ринкових можливостей запуску стартап-проекту

Визначення ринкових можливостей, які можна використати під час ринкового впровадження проекту, та ринкових загроз, які можуть завадити реалізації проекту, дозволяє спланувати напрями розвитку проекту із урахуванням стану ринкового середовища, потреб потенційних клієнтів та пропозицій проектів- конкурентів. Спочатку проводиться аналіз попиту: наявність попиту, обсяг, динаміка розвитку ринку (табл. 4.3).

Таблиця 4.3 – Попередня характеристика потенційного ринку стартап-проекту

№ п/п	Показники стану ринку (найменування)	Характеристика
1.	Кількість головних гравців, од	2
2.	Загальний обсяг продаж, ум.од/місяць	5
3.	Динаміка ринку (якісна оцінка)	Зростаюча
4.	Наявність обмежень для входу	Немає
5.	Специфічні вимоги до стандартизації та сертифікації	Немає
6.	Середня норма рентабельності в галузі або по ринку,%	140%

Середня норма рентабельності в галузі (або по ринку) порівнюється із банківським відсотком на вкладення. За результатами попереднього оцінювання ринок є привабливим для входження.

Надалі визначаються потенційні групи клієнтів, їх характеристики, та формується орієнтовний перелік вимог до послуги для кожної групи (табл. 4.4).

Після визначення потенційних груп клієнтів проведений аналіз ринкового середовища: складені таблиці факторів, що сприяють ринковому впровадженню проекту, та факторів, що йому заважають (табл. № 4.5…4.6). Фактори в таблиці подані в порядку зменшення значущості.

Таблиця 4.4 – Характеристика потенційних клієнтів стартап-проекту

№ п/п	Потреба, що формує ринок	Цільова аудиторія (цільові сегменти ринку)	Відмінності у поведінці різних потенційних цільових груп клієнтів	Вимоги споживачів до товару
1	Збільшення пропускної здатності каналу за рахунок штучного внесення шумової складової в відеоконтейнер, що збільшує пропускну здатність стеганоканалу	Служба безпеки країн	Поведінку клієнта формують потреби; особливостей купівлі та експлуатації товару немає	Товар має забезпечувати якісне збільшення пропускної здатності каналу за рахунок штучного внесення шумової складової в відеоконтейнер, що збільшує пропускну здатність стеганоканалу .

Таблиця 4.5 – Фактори загроз

№ п/п	Фактор	Зміст загрози	Можлива реакція компанії
1.	Наявність кваліфікованих кадрів	Для створення продукту потрібен спеціяліст по шифруванню данних	Пошук персоналу у навчальних закладах даного спрямування
2.	Потреба в ресурсах	-	-

Таблиця 4.6 – Фактори можливостей

№ п/п	Фактор	Зміст можливості	Можлива реакція компанії
1.	Конкуренція	Спонукає покращувати фільтр підбору та розширювати базу даних	Поглиблений аналіз ринку ПЗ моделювання ЕМС
2.	Попит	Існування стійкого попиту означає, що більшість клієнтів зацікавлені у введенні інновацій	Рекламна діяльність, SEO оптимізація сайту

Надалі проведений аналіз пропозиції: визначені загальні риси конкуренції на ринку (табл. 4.7)

Таблиця 4.8 – Ступеневий аналіз конкуренції на ринку

Особливості конкурентного середовища	В чому проявляється дана характеристика	Вплив на діяльність підприємства
1. Вказати тип конкуренції: олігополія	На ринку присутня невелика кількість фірм, які займаються шифруванням данних	Підвищувати якість послуг за рахунок використання передових технологій
2. За рівнем конкурентної боротьби: національний	Сервіси знаходяться в інтернеті і користувачі мають до них доступ з будь-якої точки країни	Безпека Країн
3. За галузевою ознакою:	Економічна боротьба між різними сервісами, які діють в одній галузі економіки, надають однакові послуги,	Слідкувати за продуктами конкурентів

Особливості конкурентного середовища	В чому проявляється дана характеристика	Вплив на діяльність підприємства
внутрішньогалузева	що задовольняють одну й ту саму потребу, але мають відмінності у виробничих затратах, якості, ціні, тощо	
4. Конкуренція за видами товарів: товарно-видова	Конкуренція між сервісами одного виду	Покращувати якість сервісу
5. За характером конкурентних переваг: цінова	Передбачає продаж продукції за нижчими цінами, ніж конкуренти.	Надавати послуги за доступною ціною, нижчою ніж конкуренти.
6. За інтенсивністю: марочна	Боротьба носить явно виражений марочний характер, велике значення набуває брендинг	Реклама послуг, створення символіки продукту

Після аналізу конкуренції, було проведено більш детальний аналіз умов конкуренції в галузі (за моделлю 5 сил М. Портера) (табл. 4.8).

Таблиця 4.8 – Аналіз конкуренції в галузі за М. Портером

	Прямі конкуренти в галузі	Потенційні конкуренти	Постачальники	Клієнти	Товари-замінники
Складові аналізу	Методи стеганографії	Можливі	-	Вимоги до якості (зручність користування та багатий функціонал)	Замінників немає
Висновки:	Інтенсивність Середня	Моніторинг ринку	-	Послуги мають бути якісними та дешевими	Обмежень немає

Для того, щоб бути конкурентоспроможним на ринку для надання послуг, потрібно залучати висококваліфікованих спеціалістів у галузі маркетингу та програмування.

На основі аналізу конкуренції, наведеного в табл. 4.8, а також із урахуванням характеристик ідеї проекту (табл. 4.1), вимог споживачів до послуги (табл. 4.4) та факторів маркетингового середовища (табл. №№ 4.5-4.6) визначається та обґрунтовується перелік факторів конкурентоспроможності. Аналіз оформлюється за табл. 4.9.

Таблиця 4.9 – Обґрунтування факторів конкурентоспроможності

№ п/п	Фактор конкурентоспроможності	Обґрунтування
1.	Ступінь задоволення потреб користувача	Послуга має мати інтуїтивно зрозумілий інтерфейс для керування, щоб користувач без зайвих зусиль міг використовувати обладнання
2.	Якість розробки з точки зору оптимальності показників надійності	Продукт має працювати стабільно
3.	Наявність наукових ресурсів	Для створення високоякісного та стабільно працюючого шифрування потрібні програмісти
4.	Економічний	Ціна послуги не має бути занадто висока, щоб знайти потенційних користувачів та сформувати імідж сервісу

За визначеними факторами конкурентоспроможності (табл. 4.9) проводиться аналіз сильних та слабких сторін стартап-проекту (табл. 4.10).

Таблиця 4.10 – Порівняльний аналіз сильних та слабких сторін проекту

№ п/п	Фактор конкурентоспроможності	Бали 1-20	-3	-2	-1	0	+1	+2	+3
1.	Ступінь задоволення потреб користувача	15						+	
2.	Якість розробки з точки зору оптимальності показників надійності	20					+		
3.	Наявність профресурсів	10				+			
4.	Економічний	20		+					

Фінальним етапом ринкового аналізу можливостей впровадження проекту є складання SWOT-аналізу (матриці аналізу сильних (Strength) та слабких (Weak)

сторін, загроз (Troubles) та можливостей (Opportunities) (табл. 4.11) на основі виділених ринкових загроз та можливостей, та сильних і слабких сторін (табл. 4.10).

Перелік ринкових загроз та ринкових можливостей складається на основі аналізу факторів загроз та факторів можливостей маркетингового середовища. Ринкові загрози та ринкові можливості є наслідками (прогнозованими результатами) впливу факторів, і, на відміну від них, ще не є реалізованими на ринку та мають певну ймовірність здійснення. Наприклад: зниження доходів потенційних споживачів – фактор загрози, на основі якого можна зробити прогноз щодо посилення значущості цінового фактору при виборі товару та відповідно, – цінової конкуренції (а це вже – ринкова загроза).

Таблиця 4.11 – SWOT- аналіз стартап-проекту

Сильні сторони: економічна (ціна послуги).	Слабкі сторони: ступінь задоволення потреб користувача, конкуренція, якість розробки з точки зору зручності та надійності.
Можливості: знижувати витрати на надання послуг, покращувати якість продукту; формування попиту у користувачів за рахунок рекламної діяльності.	Загрози: потрібно розширювати ринки надання послуг (зробити версії сервісу на різних мовах); технічне забезпечення та певні умови для тестування працездатності продукту.

На основі SWOT-аналізу розробляються альтернативи ринкової поведінки (перелік заходів) для виведення стартап-проекту на ринок та орієнтовний оптимальний час їх ринкової реалізації з огляду на потенційні проекти конкурентів, що можуть бути виведені на ринок (див. табл. 4.8, аналіз потенційних конкурентів). Визначені альтернативи аналізуються з точки зору строків та ймовірності отримання ресурсів (табл. 4.12).

Таблиця 4.12 – Альтернативи ринкового впровадження стартап-проекту

№ п/п	Альтернатива (орієнтовний комплекс заходів) ринкової поведінки	Ймовірність отримання ресурсів	Строки реалізації
1.	Дослідження поведінки споживачів, пошук наукових ресурсів, розробка обладнання, створення реклами, взаємодія з покупцями для перевірки працездатності обладнання	90%	1рік
2.	Дослідження поведінки споживачів, пошук інвесторів, пошук наукових ресурсів, створення обладнання, тестування	70%	2 роки

Обрано альтернативу № 1.

4.4 Розроблення ринкової стратегії проекту

Розроблення ринкової стратегії першим кроком передбачає визначення стратегії охоплення ринку: опис цільових груп потенційних споживачів (табл. 4.13).

Таблиця 4.13 – Вибір цільових груп потенційних споживачів

№ п/п	Опис профілю цільової групи потенційних клієнтів	Готовність споживачів сприйняти продукт	Орієнтовний попит в межах цільової групи (сегменту)	Інтенсивність конкуренції в сегменті	Простота входу у сегмент
1.	Наукові інститути, університети	Готові	Середній	Низька	Висока
2.	Державні підприємства	Готові	Середній	Низька	Висока
Які цільові групи обрано цільову групу №1 та №2.					

Для роботи в обраних сегментах ринку необхідно сформувати базову стратегію розвитку (табл. 4.14).

Таблиця 4.14 – Визначення базової стратегії розвитку

№ п/п	Обрана альтернатива розвитку проекту	Стратегія охоплення ринку	Ключові конкурентоспроможні позиції до обраної альтернативи	Базова стратегія розвитку*
1.	1	За рахунок великих можливостей по об’ємах надання послуг (розширення ринку), компанія зможе отримувати більше доходів	Витрати на маркетинг (реклама на нових ринках)	Стратегія розвитку ринку
2.	2	Покращення надання послуг за рахунок оптимізації роботи сервісу	Витрати на оптимізацію роботи сервісу	Стратегія захисту частки ринку

Обрано стратегію розвитку ринку. Наступним кроком є вибір стратегії конкурентної поведінки (табл. 4.15).

Таблиця 4.15 – Визначення базової стратегії конкурентної поведінки

№ п/п	Чи є проект "першопр охідцем" на ринку?	Чи буде компанія шукати нових споживачів, або забирати існуючих у конкурентів?	Чи буде компанія копіювати основні характеристики товару конкурента, і які?	Стратегія конкурентної поведінки*
1.	Ні	Так	Так, основний функціонал	Наслідування лідера

На основі вимог споживачів з обраних сегментів до постачальника (стартап-компанії) та до продукту (табл. 4.4), а також в залежності від обраної базової стратегії розвитку (табл. 4.14) та стратегії конкурентної поведінки (табл. 4.15) розробляється стратегія позиціонування (табл. 4.16). що полягає у формуванні ринкової позиції (комплексу асоціацій), за яким споживачі мають ідентифікувати торгівельну марку/проект.

Таблиця 4.16 – Визначення стратегії позиціонування

№ п/п	Вимоги до товару цільової аудиторії	Базова стратегія розвитку	Ключові конкурентоспромо жні позиції власного стартап- проекту	Вибір асоціацій, які мають сформувати комплексну позицію власного проекту (три ключових)
1.	Сервіс має надавати якісне збільшення пропускної здатності каналу за рахунок штучного внесення шумової складової в відеоконтейнер, що збільшує пропускну здатність стеганоканалу	розвитку ринку	Низька ціна, простий та інтуітивно зрозумілий інтерфейс керування, базовий функціонал	Доступність, надійність, співпраця

4.5 Розроблення маркетингової програми стартап-проекту

Першим кроком є формування маркетингової концепції товару, який отримає споживач. Для цього у табл. 4.17 наведені результати попереднього аналізу конкурентоспроможності товару.

Таблиця 4.17 – Визначення ключових переваг концепції потенційного товару

№ п/п	Потреба	Вигода, яку пропонує товар	Ключові переваги перед конкурентами (існуючі або такі, що потрібно створити)
1.	Якісние збільшення пропускної здатності каналу	Зручність та ефективність	Ціна, простота у роботі
2.	Надійність	Використання надійного хостингу	Стабільність роботи

Надалі розробляємо трьохрівневу маркетингову модель товару: уточнюємо ідею продукту та/або послуги, його фізичні складові, особливості процесу його надання (табл. 4.18).

Таблиця 4.18 – Опис трьох рівнів моделі товару

<table>
<tr><td>Рівні товару</td><td colspan="3">Сутність та складові</td></tr>
<tr><td>I. Товар за задумом</td><td colspan="3">Багатоканальна аудіо система побудована на основі мережного обладнання</td></tr>
<tr><td rowspan="4">II. Товар у реальному виконанні</td><td>Властивості/характеристики</td><td>М/Нм</td><td>Вр/Тх /Тл/Е/Ор</td></tr>
<tr><td>1. Низька ціна 10 у.о./місяць
2. Висока надійність
3. Безпечно для користування</td><td>М
М
М</td><td></td></tr>
<tr><td colspan="3">Якість: стабільна робота та надійний функціонал</td></tr>
<tr><td colspan="3">Пакування: -</td></tr>
<tr><td rowspan="2">III. Товар із підкріпленням</td><td colspan="3">До продажу гарантія</td></tr>
<tr><td colspan="3">Після продажу техпідтримка</td></tr>
<tr><td colspan="4">За рахунок чого потенційний товар буде захищено від копіювання: захист інтелектуальної власності</td></tr>
</table>

Після формування маркетингової моделі товару слід особливо відмітити – чим саме проект буде захищено від копіювання. Захист може бути організовано за рахунок захисту ідеї товару (захист інтелектуальної власності), або ноу-хау, чи комплексне поєднання властивостей і характеристик, закладене на другому та третьому рівнях товару.

Наступним кроком є визначення цінових меж, якими необхідно керуватись при встановленні ціни на потенційний товар (остаточне визначення ціни відбувається під час фінансово-економічного аналізу проекту), яке передбачає аналіз ціни на товари-аналоги або товари субститути, а також аналіз рівня доходів цільової групи споживачів (табл. 4.19). Аналіз проводиться експертним методом.

Таблиця 4.19 – Визначення меж встановлення ціни

№ п/п	Рівень цін на товари-замінники	Рівень цін на товари-аналоги	Рівень доходів цільової групи споживачів	Верхня та нижня межі встановлення ціни на товар/послугу
1.	–	15…20 у.о./місяць	1000 у.о. і вище	9 – 11 у.о./місяць

Наступним кроком є визначення оптимальної системи збуту. Оптимальною системою збуту є надання послуги шляхом платної підписки користувача на сервіс на певний термін (1, 3, 6 або 12 місяців).

Висновки до четвертого розділу

На сьогодні збільшення пропускної здатності каналу за рахунок штучного внесення шумової складової в відеоконтейнер, що збільшує пропускну здатність стеганоканалу є дуже важливим та затребуваним.

Компанії, що займаються шифруванням даних, наукові установи чи освітні заклади є потенційними користувачами сервісу, тому безперечно існує можливість ринкової комерціалізації проекту, бо в майбутньому прогнозується лише зростання ринку в цій галузі.

Подальша розробка проекту безперечно є доцільною.

ВИСНОВКИ

Стеганографія включає в себе методи приховування секретних повідомлень всередині контейнера. Як правило, приховування інформації з використанням електронних носіїв вимагає модифікації властивостей контейнера, що, в свою чергу, може викликати його спотворення. Наприклад, в разі комп'ютерної графіки можлива деградація зображення, помітна оком, що може вказувати на специфічні методи, використані для приховування повідомлення, а також може нейтралізувати саму мету стеганографії - приховати існування повідомлення. Тому завданнями стегоаналізу є виявлення і знищення прихованого повідомлення.

Будь-який файл може бути оброблений з метою знищити потенційне приховане повідомлення, незалежно від його наявності, але попереднє виявлення заощадить час на етапі знищення. Залежно від наших цілей, можна вибрати тип контейнера для передачі і метод стеганографії для того, щоб приховати її. Щоб гранично ускладнити аналіз зловмисником файлу-контейнера зі стеганографічної інформацією, сам контейнер повинен бути рівномірно заповнений, а впроваджуваний об'єкт повинен мати рівномірний розподіл, близький до випадкового, тобто шумоподібного.

Ця вимога може бути принаймні частково виконана за рахунок попереднього штучного «зашумлення» контейнера. У цьому випадку, як можна сподіватися, досягаються дві цілі: 1) поліпшується «прихованість» таємного повідомлення та 2) збільшується потенційна пропускна спроможність стегокананалу. Саме це є головним результатом дисертаційної роботи.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. Стаття «Захист інформаційних ресурсів від несанкціонованого доступу», URL: https://textbook.com.ua/informatika/1473447592/s-9 (дата звернення 10.10.2017р.)
2. Стаття «Криптографія»,URL: https://uk.wikipedia.org/wiki?curid=21421 (дата звернення 10.10.2017р.)
3. Стаття «Захист інформації в компютерних системах»,
URL: http://zahyst-informatsiyi-v-kompyuternyh-systemah/ (дата звернення 10.10.2017р.)
4. Стаття «Система захисту облікової інформації»,
URL: http://refpin.ru/ref_polmerotrpol.html (дата звернення 10.10.2017р.)
5. Стаття «Захист інформації в автоматизованих системах управління», URL:https://learn.ztu.edu.ua/pluginfile.php/37099/mod_resource/content/1/ЗІАСУ_версія2_2.pdf (дата звернення 10.10.2017р.)
6. Стаття «Приховування даних в нерухомих зображеннях»,URL: https://revolution.allbest.ru/programming/00553679_0.html (дата звернення 15.12.2017р.)
7. Стаття «Підвищення пропускної здатності методу приховування інформації у растрових зображеннях», URL:http://inmad.vntu.edu.ua/portal/static/E18E93CC-36E5-4FF9-8CEB-73FADAC3D277.pdf (дата звернення 15.12.2017р.)
8. Стаття « Стеганографія »,
URL: https://pns.hneu.edu.ua/mod/resource/view.php?id=132667 (дата звернення 15.12.2017р.)
9. Стаття «Назвіть вимоги для надійності стегосистеми»,
URL: https://lektsii.org/2-88932.html (дата звернення 15.12.2017р.)
10. Стаття «Стеганографічний захист інформації»,
URL: https://edudocs.net/4316473/ (дата звернення 15.12.2017р.)
11. Стаття «Аналіз ефективності застосування вейвлет-перетворення в стеганографічних системах передавання даних»,
URL:http://science.lpnu.ua/sites/default/files/journal-paper/2018/jun/12922/3-9-17.pdf (дата звернення 15.12.2017р.)
12. Стаття «Створення системи покращення індексу цитування інформаційного порталу»,URL: http://www.academia.edu/25619695/Курсова (дата звернення 15.12.2017р.)
13. В.Г.Грибунин, И.Н.Оков, И.В.Туринцев, – Цифровая стеганографія. – М.,Солон-Пресс, 2002. – 272с
14. Г.Ф.Коханович, А.Ю.Пузыренко, Компъютерная стеганография, – «МК-Пресс»,Киев, 2006 – 284с.
15. Г.В.Кугушина, Ю.Г.Савченко, Использование инструментов программы Photoshop для организации скрытого информационного обмена, ВісникДУІКТ,том10, No4, 2012, с.24-28
16. Gary C. Kessler , Null Ciphers. An Overview of Steganography for the Computer Forensics Examiner, Forenic Science Communications, vol. 4, No5, 2004, p.27

Додаток А

ABSTRACT

Steganography or Stego as it often referred to in the IT community, literally means, “Covered writing” which is derived from the Greek language. Steganography is defined as follows, “Steganography is the art and science of communicating in a way which hides the existence of the communication. The goal of Steganography is to hide messages inside other harmless messages in a way that does not allow any enemy to even detect that there is a second message present”.

In a digital world, Steganography and cryptography are both intended to protect information from unwanted parties. Both Steganography and Cryptography are excellent means by which to accomplish this but neither technology alone is perfect and both can be broken. It is for this reason that most experts would suggest using both to add multiple layers of security.

The term Steganography means, “cover writing” whereas cryptography means “secret writing”. Cryptography is the study of methods of sending messages in distinct form so that only the intended recipients can remove the disguise and read the message. The message we want to send is called plain text and disguised message is called cipher text. The process of converting a plain text to a cipher text is called enciphering or encryption, and the reverse process is called deciphering or decryption. Encryption protects contents during the transmission of the data from sender to receiver. However, after receipt and subsequent decryption, the data is no longer protected and is the clear. Steganography hides messages in plain sight rather than encrypting the message; it is embedded in the data (that has to be protected) and doesn’t require secret transmission. The message is carried inside data.

Steganography can be used in a large amount of data formats in the digital world of today. The most popular data formats are .bmp, .doc, .gif, .jpeg,mp3, .txt and .wav. Steganographic technologies are a very important part of the future of Internet security and privacy on open systems such as Internet.

Watermarking in the frequency domain involves selecting the pixels to be modified based on the frequency of occurrence of that particular pixel. This is to

overcome the greatest disadvantage of techniques operating in the spatial domain i.e. susceptibility to cropping. The mosaic attack (In a mosaic attack, the attacker breaks up the entire watermarked image into many small parts. For example, a watermarked image on a web page can be cut up and reassembled as a whole using tables in HTML. The only defence against this attack is to tile a very small watermark all over the image, and allow retrieval of the watermark from any of the small subsections of the fragmented image. However, the attacker can always create smaller blocks, and the watermarked image also has to be large enough to be distinguishable), defeats most implementations of digital watermarking operating in the spatial domain but the frequency domain watermarking is less susceptible.

The LSB technique can also be applied in the frequency domain selecting the pixels according to frequency, though not robust. Common transforms, such as Fast Fourier Transforms, alter the value of pixels within the original image based on their frequencies. The watermark is more commonly applied to the lower frequencies within an image as higher frequencies are usually lost when an image is compressed or to frequencies considered to contain perceptually significant information. Frequency based techniques result in a watermark that is dispersed throughout the image, therefore, less susceptible to attack by cropping. However these techniques are susceptible to standard frequency filters and lossy compression algorithms, which tend to filter out less significant frequencies.

Digital audio watermarking involves the concealment of data within a discrete audio file. Applications for this technology are numerous. Intellectual property protection is currently the main driving force behind research in this area. To combat online music piracy, a digital watermark could be added to all recording prior to release, signifying not only the author of the work, but the user who has purchased a legitimate copy. Newer operating systems equipped with digital rights management software (DRM) will extract the watermark from audio files prior to playing them on the system. The DRM software will ensure that the user has paid for the song by comparing the watermark to the existing purchased licenses on the system.From the

above spectral analysis of each frame, we have calculated the low frequency component, which can now be removed by subtraction from each frame.

The process of extracting the digital watermark from the audio file is similar to the technique for inserting the watermark. The computer processing requirements for extraction are slightly lower. A marked audio file in wave format is fed into the system, where it is subsequently framed, analysed, and processed, to remove the embedded data which exists as a digital watermark.Subsequent to the framing of the watermarked audio signal, we perform spectral analysis on the signal, consisting of a fast Fourier transform, which again allows us to calculate the low frequency components of each frame, as well as the overall frame power.

From the spectral analysis completed previously, we calculated the spectral power for each frame, which allows us to examine the low frequency power in each frame and subsequently extract the watermark.

In order to attain higher hidden data density in the watermarked signal, more advanced techniques must be used such as spread spectrum, phase encoding, or echo hiding.

In this tutorial, we take an introductory look at information hiding techniques. Historical detail is discussed. Several methods for hiding data in text, image, and audio are described, with appropriate introductions to the environment of each medium, as well as the strengths and weaknesses of each method. Most data hiding systems take advantage of human perceptual weaknesses, but have weaknesses of their own. In areas where cryptography and strong encryption are being outlawed, citizens are looking at steganography to circumvent such policies and pass messages covertly. Commercial applications of steganography in the form of digital watermarks are currently being used to track the copyright and ownership of electronic media. We conclude that for now, it seems that no system of data hiding is totally immune attack. However, steganography has its place in security. It in no way can replace cryptography, but is intended to supplement it. Its application in watermarking for use in detection of unauthorised, illegally copied material is continually being realised and developed.