Міністерство освіти і науки, молоді та спорту України
Тернопільський національний економічний університет
Факультет комп'ютерних інформаційних технологій
Кафедра комп'ютерної інженерії

До захисту допущено
Завідувач кафедри
комп'ютерної інженерії
к.т.н., доц. О.М.Березький
_____
"___" _____ 20___ р.

ДИПЛОМНА РОБОТА

освітньо-кваліфікаційного рівня "Магістр"
зі спеціальності 8.05010201 "Комп'ютерні системи та мережі"
на тему:

АНАЛІЗ СТІЙКОСТІ СТЕГАНОГРАФІЧНИХ СИСТЕМ В МОДЕЛЯХ ПАСИВНОГО ТА АКТИВНОГО СУПРОТИВНИКІВ

Студент групи КСМм - 51
Квасниця О.В.

_____
підпис
Науковий керівник
к.ф.-м.н., доцент Касянчук М.М.

_____
підпис
Консультант з нормоконтролю
Березький О. В.
_____
Прізвище, ініціали Підпис

2012

Міністерство освіти і науки, молоді та спорту України
Тернопільський національний економічний університет
Факультет комп'ютерних інформаційних технологій
Кафедра комп'ютерної інженерії

"Затверджую"

Зав. кафедри
комп'ютерної інженерії
к.т.н., доц. О.М. Березький
_____
"____"_____20__ р.

З А В Д А Н Н Я

НА ДИПЛОМНУ РОБОТУ СТУДЕНТА

Квасниці Олега Васильовича

1. **Тема дипломної роботи** "Аналіз стійкості стеганографічних систем в моделях пасивного та активного супротивників" затверджена наказом університету № 475 від 14 жовтня 2011 року.

2.**Термін здачі** закінченої дипломної роботи _____

3. **Об'єкт дослідження**: Дослідження стійкості стеганографічних систем в різних моделях супротивників.

4. **Предмет дослідження**: Стеганографічні системи в моделях активного і пасивного супротивників.

5. **Перелік задач, які мають бути вирішені**:

1. Детальний аналіз стеганографічних методів захисту інформації, стегоаналітичних атак та критеріїв визначення стеганографічної стійкості.
2. Дослідження методів та алгоритмів оцінки стеганографічної стійкості в моделях активного і пасивного супротивників.
3. Побудова моделей стеганографічних перетворень з врахуванням пасивних та активних атак.
4. Розробка методу адаптивного вбудовування даних у сегменти зображень з використанням поліноміальних моделей.

6. **Перелік ілюстративного матеріалу:**

- загальна схема криптографічного перетворення;
- загальна схема стеганографічного перетворення;
- загальна схема побічної стеганографії;
- структурна модель стеганографічних перетворень;
- схема визначення поліноміальної моделі прогнозування положення точки;
- схема відновлення даних;
- зміна коефіцієнта кореляції для відновленого та оригінального повідомлень;
- зміна пікового відношення сигнал/шум при різних коефіцієнтах стиску контейнера.

7.**Консультанти** по роботі

Розділ	Консультант	Підпис
1		
2		
3		

КАЛЕНДАРНИЙ ПЛАН

№	Назва структурних частин ДР	Термін виконання	Примітка
1	Стеганографічні методи захисту інформації та стеганографічна стійкість	15.09.2011 – 5.11.2011	
2	Дослідження методів та алгоритмів оцінки стеганографічної стійкості в моделях активного і пасивного супротивників	6.11.2011 – 31.01.2012	
3	Моделі стеганографічних перетворень з врахуванням пасивних та активних атак	1.02.2012 – 23.04.2012	

Завдання прийняв до виконання _____
(підпис)

Керівник дипломної роботи _____
(підпис)

РЕФЕРАТ

Дипломна робота на тему “Аналіз стійкості стеганографічних систем в моделях пасивного та активного супротивників” на здобуття освітньо-кваліфікаційного рівня “Магістр” зі спеціальності “Комп’ютерні системи та мережі” написана обсягом 77 сторінок і містить 27 ілюстрацій, 4 таблиці, 2 додатки та 26 джерел за переліком посилань.

Метою роботи є системний аналіз стійкості різних стеганографічних систем при умові існування активного та пасивного супротивників.

Методи досліджень базуються на математичних методах дослідження стійкості стеганографічних систем, а також математичних методах стеганографії

Здійснено системний аналіз оцінки стійкості стеганографічних систем в моделях активного і пасивного супротивників. Розроблено та досліджено моделі стеганографічних перетворень з врахуванням пасивних та активних атак. Розроблено алгоритм побічної стеганографії для активного і пасивного супротивників, який має більшу стійкість до стеганоаналізу. Показано, що при організації стеганографічного каналу передачі інформації отримані у роботі результати дозволяють обґрунтовано вибирати параметри алгоритму Коха–Жао, які забезпечують необхідний рівень стійкості системи одночасно з максимально можливою «непомітністю» вбудованого повідомлення.

Результати роботи можуть бути використані при побудові стеганографічних систем захисту інформації.

Можливими напрямками подальших досліджень є продовження роботи по дослідженню існуючих стеганографічних методів приховування інформації та розробці нових.

Ключові слова: СТІЙКІСТЬ, СТЕГАНОГРАФІЧНА СИСТЕМА, СТЕГОАНАЛІТИЧНА АТАКА, МОДЕЛЬ ЗАГРОЗ, АКТИВНИЙ І ПАСИВНИЙ СУПРОТИВНИКИ, ВБУДОВУВАННЯ ІНФОРМАЦІЇ.

ABSTRACT

The diploma work on theme "Analysis of stability steganography systems in models of passive and active opponents" on education and qualification of "Master" specialty "Computer systems and networks" written up 77 pages and contains 27 figures, 4 tables, 2 applications and 26 sources for references.

The aim of work is a systematic analysis of the stability of different systems of steganography, provided the existence of active and passive opponents.

The methods of research based on on mathematical methods of studying the stability of Stenography systems and mathematical methods of steganography.

With systematic evaluation of the stability analysis steganography systems in models of active and passive opponents. Research and development model steganography changes with regard to passive and active attacks. The algorithm adverse steganography for active and passive opponents, which is more resistant to stegoanalized. It is shown that the organization steganographic channel information obtained in the results can reasonably choose the parameters of the algorithm Koch–Zhao, providing the necessary level of system stability at the same time as possible "unremarkability" embedded message.–

The results may be used in the construction of steganography information security systems.

Possible directions for further research is continuing work on the study of existing methods Stenography withholding information and developing new ones.

Keywords: STABILITY, STEGANOGRAPHICAL SYSTEM, STEHOANALITYCAL ATTACK, THREAT MODEL, ACTIVE AND PASSIVE OPPONENT EMBEDDED INFORMATION.

ЗМІСТ

ВСТУП

Актуальність теми. Проблема інформаційної безпеки вирішується на протязі всієї історії людства [1]. Ще в давнину виділилося два основні напрямки захисту інформаційних ресурсів: криптографія та стеганографія [2]. Криптографія блокує несанкціонований доступ до даних шляхом їх шифрування [3]. Стеганографія ж іде принципово далі – її мета приховати сам факт існування конфіденційної інформації [4].

Хоча стеганографія має дуже довгу і багату історію [5], однак тільки останнім часом у зв'язку з бурхливим розвитком інформаційних технологій, зокрема з появою комп'ютерних мереж [6], а також через наявність обмежень на використання криптозасобів та надзвичайну актуальність проблеми захисту інтелектуальної власності, стеганографія стає предметом зростаючого інтересу й активних наукових досліджень. Стеганографічні методи, які приховують інформацію у потоках оцифрованих сигналів та реалізуються на базі комп'ютерної техніки і програмного забезпечення в рамках окремих обчислювальних систем, корпоративних чи глобальних мереж, складають предмет вивчення цифрової стеганографії.

На сьогодні цифрова стеганографія є досить наукоємкою дисципліною, інструментами для розвитку якої є методи теорії ймовірностей та математичної статистики, теорії швидких ортогональних перетворень, теорії апроксимації, теорії кодування, теорії складності, теорії похибок, цифрової обробки сигналів та зображень тощо. Разом з тим, зважаючи на її молодість, чимало проблем поки що знаходяться на початковій стадії свого вирішення.

Так, більшість існуючого програмного забезпечення побудовано на основі модифікацій відомого стеганографічного методу – методу найменшого значущого біту. Цифрові контейнери, створені таким програмним забезпеченням, характеризуються низькою стійкістю і не можуть забезпечити прийнятного рівня захисту інформації. Порушення наявних у контейнері кореляційних зв'язків, обумовлене "вкрапленням" у нього додаткових даних, легко виявити візуальною атакою на молодші біти або застосуванням до контейнера серії статистичних атак.

Крім того, інформація може бути знищена активним супротивником.

Більш стійкими є спектральні алгоритми [7]. Але ті, що відомі на сьогодні, розроблялися насамперед, виходячи з потреб захисту інтелектуальної цифрової власності, і тому характеризуються малою пропускною здатністю створюваного стегоканалу, достатньою для передачі в сигналі–контейнері лише мінімуму інформації: логотипу фірми, імені та координат власника контейнера, певної бітової послідовності невеликої довжини і т. п.

Вирішення науково–технічної задачі з вдосконалення методів та цифрових засобів стеганографічного захисту інформації в комп'ютеризованих системах являється ключовим завданням для багатьох наукових центрів. Значний вклад в розвиток даної теорії внесли відомі зарубіжні та вітчизняні вчені І.Кох, В.Жао, Дж. Фрідріх, Є.Разінков, Р.Латипов, Н.Кошкіна, Н. Алішов, В.Задірака та ін.

За цей час було опубліковано немало якісних алгоритмів стеганографічного приховування даних в зображеннях як в зарубіжній, так і вітчизняній літературі [8-10]. Однак значно менше уваги було присвячено аналізу стійкості запропонованих алгоритмів до різних атак. Стеганографічних методів, однаково стійких до всіх видів атак, на сьогоднішній день не існує [11]. Тому при виборі стеганоалгоритма важливо мати в наявності якомога детальніший аналіз стійкості цих алгоритмів до різних видів атак.

Іншою важливою вимогою до стеганосистем є «непомітність» вбудованого повідомлення, для забезпечення якого спотворення, внесені в контейнер під час приховування в ньому інформації, повинні бути мінімальними, але забезпечувати при цьому необхідну стійкість до певних видів атак [12].

Крім того, на даний час не виявлено стеганографічних алгоритмів, що поєднують у собі високі стійкість та пропускну здатність за прийнятної обчислювальної складності своєї реалізації. Таким чином, задача надійної прихованої передачі великих об'ємів інформації на сьогодні вирішується недостатньо ефективними шляхами. Усе вищесказане і визначає актуальність обраної проблеми дослідження.

Мета роботи. Метою даної роботи є системний аналіз стійкості різних стеганографічних систем при умові існування активного та пасивного супротивників.

Для досягнення мети необхідно вирішити наступні **завдання**:

1. Детальний аналіз стеганографічних методів захисту інформації, стегоаналітичних атак та критеріїв визначення стеганографічної стійкості.

2. Дослідження методів та алгоритмів оцінки стеганографічної стійкості в моделях активного і пасивного супротивників.

3. Побудова моделей стеганографічних перетворень з врахуванням пасивних та активних атак.

4. Розробка методу адаптивного вбудовування даних у сегменти зображень з використанням поліноміальних моделей.

Об’єкт дослідження. Дослідження стійкості стеганографічних систем в різних моделях супротивників.

Предмет дослідження. Стеганографічні системи в моделях активного і пасивного супротивників.

Методи дослідження. Математичні методи дослідження стійкості стеганографічних систем, а також математичні методи стеганографії.

Наукова новизна одержаних результатів.

1. Здійснено системний аналіз оцінки стійкості стеганографічних систем в моделях активного і пасивного супротивників.

2. Розроблено та досліджено моделі стеганографічних перетворень з врахуванням пасивних та активних атак.

3. Розроблено алгоритм побічної стеганографії для активного і пасивного супротивників, який має більшу стійкість до стеганоаналізу.

4. Показано, що при організації стеганографічного каналу передачі інформації отримані у роботі результати дозволяють обґрунтовано вибирати параметри алгоритму Коха−Жао, які забезпечують необхідний рівень стійкості системи одночасно з максимально можливою «непомітністю» вбудованого повідомлення.

Практичне значення отриманих результатів.

Побудовано узагальнені структурні моделі стеганографічних перетворень інформації з урахуванням пасивних і активних стегоаналітичних атак. Розроблено методи адаптивного вбудовування даних у сегменти зображень з використанням поліноміальних моделей. Наведено практичні рекомендації по вибору відповідного параметра алгоритму Коха–Жао із заданою стеганографічною стійкістю до компресії контейнера.

1 СТЕГАНОГРАФІЧНІ МЕТОДИ ЗАХИСТУ ІНФОРМАЦІЇ ТА СТЕГАНОГРАФІЧНА СТІЙКІСТЬ

1.1 Методи захисту інформації в каналах зв’язку

Сучасні інформаційні системи мають розподілену архітектуру, що часто використовують загальні мережі, (Intranet, Internet, мережі комунікаційних операторів) у якості транспортної інфраструктури для корпоративної мережі [13]. З однієї сторони це дозволяє значно скоротити витрати на розробку та підтримку таких систем, а з іншої − доступ до такої загальної транспортної мережі мають особи, що не є членами відповідної інформаційної системи. З огляду на це, питанням контролю даних, що циркулюють у таких мережах, приділяється особлива увага як з боку експлуатуючих подібні системи, так і з сторони дослідників. Розкриття або доступність цих даних сторонньому користувачу може привести до непередбачених наслідків, значних матеріальних та нематеріальних втрат. Одним з основних напрямків у інформаційних технологіях, що дозволяють вирішити поставлене завдання, є застосування різних алгоритмів та методів криптографії [14]. Вони дозволяють контролювати та обмежувати доступ до переданих даних тільки для осіб, які мають на це право. У сучасних інформаційних системах використовується багато різних алгоритмів і методів шифрування інформації й наступної її передачі одержувачеві [15]. Всі вони відносяться до двох основних напрямків досліджень в області, пов'язаній із захистом комп’ютерної інформації від несанкціонованого використання: комп'ютерної криптографії та комп'ютерної стеганографії.

При застосуванні комп’ютерної криптографії інформація, яку потрібно захищати, шифрується з допомогою числових ключів, причому із збільшенням розрядності ключів обчислювальна складність перетворення збільшується. Загальна схема криптографічного шифрування показана на рисунку 1.1.

При застосуванні комп’ютерної стеганографії інформація, яку потрібно захищати, змішується з визначеним видом мультимедійної інформації (мова, аудіо, відео, зображення та ін.) і передається до законного користувача. В комп’ютерній стеганографії важко реалізувати передачу великого об’єма

інформації, що дуже важливо для сучасних комп'ютерних мереж. Загальна схема стеганографічного перетворення показана на рисунку 1.2.

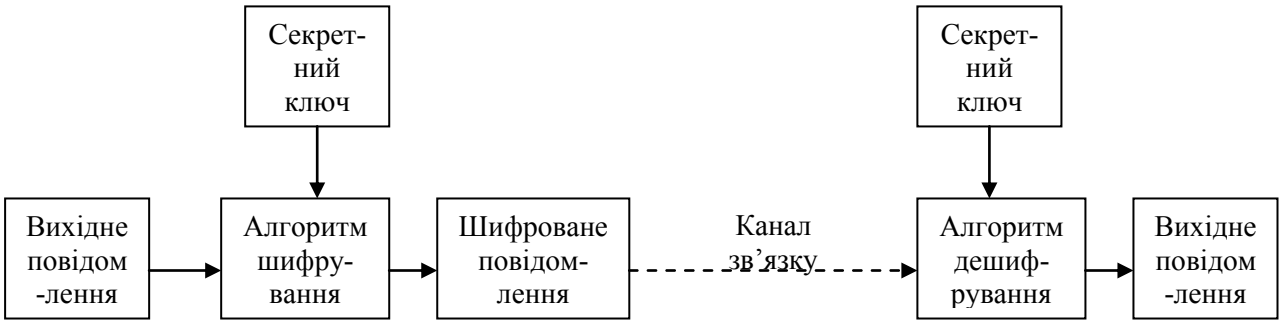

Рисунок 1.1 – Загальна схема криптографічного перетворення

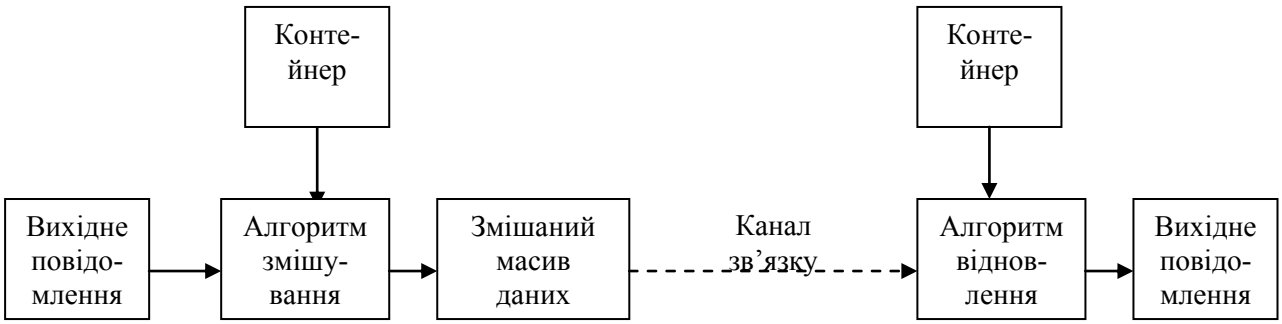

Рисунок 1.2 – Загальна схема стеганографічного перетворення

Як в комп'ютерній криптографії, так і в комп'ютерній стеганографії, в кінцевому підсумку захищена інформація передається по каналу зв'язку в шифрованому або змішаному вигляді, що дозволяє крипто– або стеганоаналітику провести відповідний аналіз для зламу шифра і/або виділення корисної інформації.

1.2 Огляд стеганографічних методів захисту інформації

Серед усього спектру систем захисту інформації від несанкціонованого доступу особливе місце займають стеганографічні системи [16]. На відміну від інших систем, вони опираються не лише на властивості самої інформації, а й на

властивості її матеріальних носіїв, особливості вузлів її обробки, передачі й зберігання.

У даний час важко переоцінити необхідність приховування наявності самого факту передачі інформації, що захищається у діяльності більшості як державних, так і комерційних установ. Адже, криптографічні засоби на даний час можуть лише затягнути процес дешифрування даних зловмисником, але навряд чи зупинять його. Операції з важливими даними завжди пов'язані з підвищеним ризиком, особливо якщо інформація надзвичайно важлива, наприклад, ведення секретних переговорів, передача номерів рахунків, кодів доступу і т.п.

Питаннями захисту конфіденційної інформації займається стеганографія – наука про приховування інформації шляхом збереження в таємниці самого факту передачі. Тобто приховування одних повідомлень в інших повідомленнях. У якості контейнера (звичайного повідомлення, придатного для вбудовуваної інформації, що захищається) використовуються типові документи, мультимедійні дані та звичайний текст.

Стеганографічні методи захисту інформації в останні роки розвиваються досить активно, постійно з'являються нові методи приховування інформації і нові методи стеганоаналізу.

Зростає і загальне число як зарубіжних, так і вітчизняних публікацій. Разом з тим, аналіз останніх дозволяє говорити про те, що переважна більшість досліджень [17] спрямована на мультимедійний контент. Хоча на даний момент величезна кількість інформації представлена в текстовому вигляді: книги, статті, електронне листування, документи, звіти і багато іншого, і всі ці матеріали можуть бути ефективно використані в якості контейнерів для прихованої передачі інформації. Недарма величезною популярністю в процесі приховування інформації зараз користується лінгвістична стеганографія, яка дозволяє приховати кодовану довільну інформацію у тексти, спираючись на особливості мови та лінгвістичні ресурси.

Розглядаючи роботи зарубіжних фахівців [9, 18], присвячені текстовій та лінгвістичній стеганографії, можна помітити, що автори цих робіт чітко розмежовують методи та алгоритми стеганографії із захисту інформації, що

приховується від “роботів” і від людей. Перші спрямовані на захист інформації при тотальному скануванні всієї кореспонденції програмними пошуковими роботами і аналізаторами, другі спрямовані на захист інформації при уважному перегляді тексту людиною.

1.3 Основна задача стеганографії, моделі супротивників, формальне визначення стегосистем та їх класифікація

Стеганографія − це наука та мистецтво прихованої передачі інформації. Приховується сам факт наявності обміну інформацією. Це досягається шляхом вбудовування повідомлень у невикликаючий підозр об'єкт, який називається стеганографічним контейнером. У цифровий стеганографії в якості контейнера використовуються цифрові зображення, цифрове аудіо та відео.

Основне завдання стеганографії сформульоване у вигляді так званої «проблеми ув'язнених», яка схематично зображена на рисунку 1.3. Двоє ув'язнених, Аліса й Боб, сидять у різних камерах. Для того, щоб спланувати втечу, їм необхідно обмінюватися інформацією по відкритому каналу зв'язку, контрольованому порушником Євою. Для того, щоб передати повідомлення Бобові, Аліса вбудовує його в стеганографічний контейнер і передає результат вбудовування (стего) по каналу зв'язку.

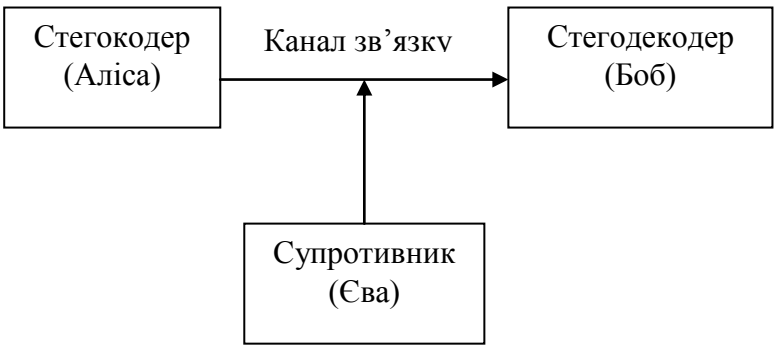

Рисунок 1.3 – Схема «проблеми ув’язнених»

У стеганографії розглядаються три моделі супротивника:

1) Єва – пасивний супротивник. В цьому випадку її основне завдання полягає у виявленні самого факту наявності прихованої передачі інформації, модифікувати стего у Єви немає можливості. Єва досліджує перехоплене стего на предмет наявності прихованої інформації. Якщо інформація нею не виявляється, Єва пересилає стего Бобові. У противному випадку канал зв'язку блокується;

2) Єва − активний супротивник. У цьому випадку Єва модифікує кожний перехоплений цифровий об'єкт, щоб знищити можливе приховане повідомлення. В якості атак можуть застосовуватися такі, наприклад, перетворення стего, як стиск із втратами або низькочастотна фільтрація;

3) супротивник називається зловмисником (malicious), якщо його дії ґрунтуються на властивостях конкретного стеганографічного алгоритму і спрямовані на таємне втручання в комунікацію Аліси та Боба. Наприклад, Єва може спробувати видавати себе за Алісу або Боба.

Як правило, у завданнях прихованої передачі інформації передбачається присутність пасивного або активного супротивника.

Вбудовування інформації в стеганографічний контейнер полягає в незначній його модифікації [11]. Внесені зміни не повинні виявлятися статистично або за допомогою органів чуття людини. Якщо, приміром, інформація вбудовується в цифрове зображення, то елементами контейнера, що модифікуються при вбудовуванні інформації, можуть бути інтенсивність колірних компонентів пікселів, коефіцієнти різних перетворень тощо.

Виходячи з вищесказаного, загальне формальне визначення стегосистеми можна дати таким чином. Нехай k – стеганографічний ключ із множини K можливих стеганографічних ключів, $k \in K$, M − множина можливих приховуваних повідомлень, C − множина можливих стеганографічних контейнерів. Стеганографічна система складається із двох відображень: вбудовуючого Emb та відновлюючого Ext:

$$\text{Emb: } C \times K \times M \to \text{C}, \tag{1.1}$$

$$\text{Ext: } C \times K \to M, \tag{1.2}$$

таких, що Ext (Emb (c, k, m), k) = m для всіх $c \in C$, $k \in K$, $m \in M$. Вбудовуюче перетворення Emb на основі контейнера c, ключа k і повідомлення m генерує стегоповідомлення s = Emb(c, k, m).

В [7, 8, 19] даються такі формальні визначення відомих сучасних стегосистем:

1) сукупність Y=(C, M, D, E), де C – множина контейнерів, M – множина секретних повідомлень, $|C| \geq |M|$; E: $C \times M \to C$, D: $C \to M$ – функція приховування та відновлення повідомлення з контейнера C, причому $D(E(c, m))=m$ для будь – яких $m \in M$ і $c \in C$, являє собою безключову стегосистему;

2) сукупність Y=(C, M, K, D, E), де C – множина контейнерів, M – множина секретних повідомлень, $|C| \geq |M|$; K– множина секретних ключів E_k: $C \times M \times K \to C$, D_k: $C \times K \to M$ – стеганографічне перетворення з властивістю $D_k(E_k(c, m, k), k)=m$ для будь – яких $m \in M$, $c \in C$ і $k \in K$, являє собою стегосистему з секретним ключем;

3) сукупність Y=(C, M, K, D, E), де C – множина контейнерів, M – множина секретних повідомлень, $|C| \geq |M|$; K=(K_1, K_2)– множина пар стегоключів E_k: $C \times M \times K_1 \to C$, D_k: $C \times K_2 \to M$ – стеганографічне перетворення з властивістю $D_k(E_k(c, m, k_1), k_2)=m$ для будь – яких $m \in M$ і $c \in C$, являє собою стегосистему з відкритим ключем.

Стегосистеми класично розрізняють по таких критеріях:

1) виконуваному завданню:

– стегосистеми прихованої передачі даних;

– стегосистеми цифрових водяних знаків;

– інші;

2) природі сигналу, який використовується в якості контейнера:

– аналогова природа сигналу;

– цифрова природа сигналу;

3) необхідності наявності у стегодетектора вихідного сигналу:

– для добування вбудованої інформації потрібен вихідний сигнал;

– для добування вбудованої інформації вихідного сигналу не потрібно;

3) типу присутнього супротивника:

– пасивний супротивник;

– активний супротивник.

1.4 Класифікація стегоаналітичних атак

Стегоаналіз – це наука й мистецтво виявлення прихованої інформації або визначення яких–небудь параметрів стегосистеми. У цьому випадку розглядаємо атаки Єви.

Стегоаналітичні атаки розрізняються по використовуваних методах, по наявній у стегоаналітика інформації, по одержуваній у результаті атаки інформації. Є два основних підходи до побудови пасивних стегоаналітичних атак: стегоаналіз, що грунтується на контрольованому навчанні, та статистичний стегоаналіз.

1.4.1 Стегоаналіз, що грунтується на контрольованому навчанні

Цей вид стегоаналізу полягає у навчанні класифікатора на основі вибірки, що складається з великої кількості стего та порожніх стеганографічних контейнерів. На вхід класифікатора подається вектор значень, обчислених на основі стего й контейнерів з навчальної вибірки.

Плюси цього виду стегоанализа:

– показує гарні результати при правильному підборі параметрів, що подаються на вхід класифікатора;

– при навчанні класифікатора для будь–якого конкретного алгоритму може бути досягнуте досить точне виявлення інформації;

– немає необхідності в розробці статистичних моделей – використовється навчальна вибірка;

– машинне навчання – досить добре вивчена область.

Мінуси цього виду стегоаналізу:

– для кожного окремого стеганографічного алгоритму потрібно навчити окремий класифікатор, що непросто реалізувати на практиці;

– критично важливий правильний вибір параметрів, які подаються на хід класифікатора, у той час як чітка системна схема підбору цих параметрів не розроблена;

– деякі параметри самого класифікатора і параметри процесу навчання повинні бути підібрані стегоаналітиком, а цей підбор часто може бути здійснений тільки методом проб і помилок;

– стеганоаналітик не має можливості контролювати ймовірності помилок першого та другого роду;

– методи, які відносяться до цього виду стегоагалізу, як правило, не здатні оцінити стеганографічний ключ або довжину повідомлення.

1.4.2 Статистичний стегоаналіз

Статистичний стегоаналіз спрямований на виявлення прихованого повідомлення на основі всебічного дослідження відповідних статистичних закономірностей, що порушуються приховуючим перетворенням. Атаки, які відносяться до цього виду стегоаналізу, можуть бути досить різноманітними і використовують різні властивості стеганографічних контейнерів та алгоритмів.

Плюси статистичного стегоаналізу:

– необхідний для статистичного стегоаналізу математичний апарат добре розроблений і може бути прямо застосований при побудові стегоаналітичних атак;

– стегоаналітик має можливість контролювати ймовірності помилок першого або другого роду;

– є можливість оцінки стеганографічного ключа, довжини прихованого повідомлення, місцезнаходження прихованої інформації у вибраному стегоконтейнері.

Мінуси статистичного стегоаналізу:

– ефективність статистичного стегоаналізу значно зменшується при наявності неточностей у статистичних моделях, які використовуються для вбудовування інформації;

– статистична нестаціонарність цифрових зображень викликає значні практичні труднощі.

1.5 JPEG–стеганографія та її межа

Поширеність зображень у форматі JPEG стала причиною особливої актуальності алгоритмів JPEG–стеганографії та відповідних стегоаналітичних атак.

Всі алгоритми JPEG–стеганографії вбудовують інформацію, яку треба приховати шляхом модифікації AC–коефіцієнтів відповідного JPEG–перетворення. Більшість існуючих алгоритмів JPEG–стеганографії використовують в якості контейнерів візуальні зображення у форматі JPEG. Існують алгоритми, які використовують нестиснуті зображення, вбудовуючи інформацію в процесі проведення JPEG–перетворення, враховуючи відкинуту інформацію.

Використання нульових JPEG–коефіцієнтів повинно приводити до досить значного зниження стійкості будь-якої стегосистеми проти взламу, тому для вбудовування приховуваної інформації використовуються тільки ненульові AC–коефіцієнти.

Дослідження показують, що на даний момент кращі алгоритми JPEG–стеганографії можуть забезпечити стійку до пасивних атак передачу інформації при пропускній здатності каналу, що не перевищує 0,05 біт на ненульовий AC–коефіцієнт (стійкою вважається стегосистема, для якої напівсума ймовірностей помилок першого та другого роду перевищує 0,4).

1.6 Стеганографічна стійкість

1.6.1 Інформаційно–теоретичне визначення стійкості

Нехай стеганографічні контейнери *c* мають імовірнісний розподіл P_C, де $P_C(c)$ – імовірність того, що Алісою буде обраний контейнер *c* для вбудовування інформації. Ця інформація відома Єві.

Вважається, що і стеганографічний ключ *k* з множини *K*, і повідомлення *m* з множини *M* вибираються рівноймовірно. На основі цієї інформації та розподілу P_C за допомогою формул повної ймовірності можна отримати P_S – імовірнісний розподіл отриманих в результаті вбудовування інформації стегоповідомлень, $P_S(s)$ – імовірність того, що приховуючим перетворенням буде згенероване стегоповідомлення *s*.

Порівняння розподілів P_C і P_S відбувається на основі відстані Кульбака – Лейблера (відносної ентропії), що визначається у такий спосіб:

$$D(P_C \| P_S) = \sum_{c \in C} P_C(c) \log \frac{P_C(c)}{P_S(c)} \qquad (1.3)$$

Відносна ентропія завжди невід'ємна і може дорівнювати нулю тоді і тільки тоді, коли $P_C = P_S$. Відносна ентропія не є відстанню у строгому математичному змісті (тому що вона асиметрична і не задовільняє нерівності трикутника).

Якщо $D(P_C \| P_S) = 0$, тобто розподіл створюваних Алісою стего P_S співпадає з розподілом стеганографічних контейнерів P_C, відомим зловмиснику, то стегосистема являється абсолютно стійкою, оскільки зловмисник немає можливості розрізнити стего та контейнери.

Якщо $D(P_C \| P_S) \le \varepsilon$, то стегосистема визначається як ε–стійка (епсилон-стійка). Чим менше значення ε, тим більш стійкою до пасивних стегоаналітичних атак є система.

1.6.2 Практична стійкість

Оцінити стійкість стегосистеми в теоретико−інформаційному змісті на практиці не представляється можливим, тому вводиться поняття стеганографічної стійкості в практичному змісті.

Стеганографічна система називається стійкою в практичному змісті, якщо не існує стегоаналітичного алгоритму, що був би здатний виявляти наявність прихованої інформації. Таким чином, практична стійкість стегосистеми залежить від розвитку стегоаналітичних методів і може знижуватися з розвитком методів стегоаналізу.

Відзначимо фактори, що істотно впливають на стійкість стеганографічних систем:

– вибір стеганографічного контейнера;

– спосіб зміни елементів контейнера;

– кількість змінених елементів;

– правило вибору змінюваних елементів контейнера.

1.6.3 Вибір стеганографічного контейнера

Від вибору контейнера для вбудовування інформації істотно залежить імовірність виявлення порушником прихованого повідомлення.

Розглянемо в якості контейнерів випадок використання цифрових зображень. Не слід використовувати для вбудовування інформації зображення з невеликою кількістю кольорів, а також зображення, створені в стандартних графічних редакторах. Для вбудовування інформації у просторовій області варто також уникати використання зображення, що раніше було у форматі JPEG, оскільки JPEG − компресія залишає «слід» у зображенні, який може бути виявлений. Після вбудовування інформації цей «слід» збережеться, але існує спосіб визначити те, що дане зображення не могло бути отримане лише в результаті декомпресії JPEG−зображення. Це, звичайно ж, може викликати підозри.

1.6.4 Спосіб зміни елементів контейнера

При вбудовуванні інформації деякі елементи контейнера (байти інтенсивності колірних компонентів пікселів, JPEG–коефіцієнти та ін.) змінюються відповідно до бітів приховуваного повідомлення.

Розглянемо розповсюджений випадок, коли в результаті вбудовування повідомлення міститься в молодших бітах відповідних елементів контейнера.

Є два основних підходи до зміни молодшого біта, якщо він не збігається із вбудованим:

1) змінити молодший біт на протилежний (01000111 – 01000110, 00111010 – 00111011). Використовується, наприклад, в алгоритмі Jsteg [6];

2) відняти одиницю із числа (01000111 – 01000110, 00111010 – 00111001).

Використовується, наприклад, в алгоритмі F5 [20].

Варто відмітити, що використання першого способу в багатьох випадках істотно знижує стійкість стеганографічної системи. В [21] описана гістограмна атака на алгоритм Jsteg, що використовує саме цю його властивість.

1.6.5 Кількість змінених елементів

Очевидно, що чим менше спотворень внесено приховуючим перетворенням, тим нижча ймовірність виявлення прихованої інформації.

Відношення кількості переданих біт до кількості внесених спотворень називається ефективністю вбудовування (embedding efficiency). Високе значення цього параметра свідчить про можливість невиявлення передачі порівняно великого обсягу інформації.

Як приклад розглянемо спосіб підвищення ефективності вбудовування, який називається матричним (matrix embedding). Він був запропонований в [21] як частина алгоритму F5, що приховує інформацію в зображеннях формату JPEG.

Застосування цього способу дозволяє вмонтувати k біт в n коефіцієнтів, де $n = 2^k - 1$, шляхом зміни тільки одного із цих коефіцієнтів.

Нехай H – матриця $k \times n$, стовпці якої являють собою всі ненульові вектори довжини k. Нехай x – вектор довжини n з молодших біт використовуваних

коефіцієнтів, а m – вектор довжини k, що містить біти приховуваного повідомлення.

Якщо $Hx=m$, то зміни вносити не потрібно – повідомлення вже міститься в молодших бітах коефіцієнтів. У протилежному випадку обчислюється вектор $z=Hx-m$. Очевидно, що z збігається з одним із стовпців матриці H, наприклад, з j–м. Тоді повідомлення m може бути вбудоване шляхом зміни j–го елемента. Отримувач, який відновив послідовність x з прийнятого стего обчислює повідомлення наступним чином: $m = Hy$.

Матричне вбудовування дозволяє вбудовувати k біт в $n=2^k-1$ коефіцієнтів із внесенням у середньому $(1 - l/2^k)$ змін.

1.6.6 Правило вибору.

Один зі способів підвищення стійкості стеганографічної системи – адаптивний вибір елементів стегоконтейнера для вбудовування інформації. Приміром, інформація може вбудовуватися в найбільш зашумлені ділянки зображення, що ускладнює її виявлення зловмисником.

Однак, варто відмітити, що адаптивне правило вибору елементів контейнера найчастіше не залежить або слабко залежить від секретного ключа. Ця властивість дозволяє зловмисникові успішно застосувати це правило вибору, що може дати можливість йому провести досить успішну атаку на стегосистему.

Ця проблема може бути вирішена, якщо при вбудовуванні повідомлення використовується інформація, доступ до якої порушник одержати не може. Такий підхід до приховування, дозволяючи використовувати переваги адаптивного стеганографічного перетворення, не знижує стійкості системи, тому що порушник не має можливості застосувати правило вибору елементів стегоконтейнера. Добування повідомлення одержувачем можливо завдяки "wet paper codes", запропонованим в [22].

Крім того, в [22] запропонована стегосистема з адаптивним вибором елементів контейнера. Відомо, що людське око не чутливе до спотворень на границях об'єктів, тому для вбудовування інформації в цьому методі використовуються пікселі, що перебувають на границях об'єктів зображення.

1.7 Теоретико−інформаційний критерій оцінки стійкості

У роботі [11] представлений теоретико−інформаційний метод оцінки стійкості симетричних одноразових стеганосистем з наявністю пасивного супротивника. Метод ґрунтується на відомій моделі стеганографічного каналу і використовує теорію інформації та перевірки гіпотези для аналізу розподілів імовірностей появи контейнерів і наступного одержання оцінки стійкості. Вважаємо за необхідне перелічити основні недоліки даного методу.

Передбачається, що супротивник знає точні імовірнісні характеристики порожніх контейнерів, стеганографічних контейнерів, приховуваних повідомлень і ключів. У підсумку будь−яке відхилення статистики при спостереженні супротивником трактується як виявлення стеганографічного повідомлення/каналу. У підсумку, будь−яке незначне відхилення спостережуваної супротивником статистики від середньостатистичних характеристик порожніх контейнерів кваліфікується як виявлення схованого каналу. Очевидно, що:

− на практиці будь−який канал вносить перекручування в передані повідомлення, тобто відхилення від очікуваних значень неминучі;

− у супротивника в найкращому разі в наявності можуть бути усереднені характеристики по перерахованим вище сутностях;

− відправник вільний підбирати або створювати такі контейнери, для яких характеристики стеганографічних контейнерів незначно відрізнялися від середньостатистичних характеристик порожніх контейнерів.

Часто користувачеві потрібно оцінити стійкість декількох різнотипних методів приховання, щоб зробити обґрунтований вибір на користь одного з них. Важко представити відправника й одержувача, які обмінюються відкритим текстом з випадковим розподілом символів. Важко знайти супротивника (наглядача), що допускає передачу безглуздих повідомлень (з випадковим розподілом символів).

Очевидно, що така ідеалізована модель неадекватна реальним системам тайнопису і не може бути застосована на практиці. Вона становить теоретичний інтерес і використовується для:

– доказу абсолютної стійкості теоретичних стегосистем на зразок одноразового стеганографічного блокнота [11];

– одержання нижньої оцінки для ймовірності помилки другого роду (стеганографічний контейнер був неправильно визначений як порожній), використовуючи теорему Неймана–Пірсона, маючи верхню оцінку для ймовірності помилки першого роду (порожній контейнер був неправильно визначений як стеганографічний) і стійкість стеганосистеми по даній моделі.

1.8 Постановка задачі

Аналіз найбільш популярних стеганографічних програм, які дозволяють вбудовувати інформацію в текстові файли (FFENCODE, SecureEngine, Центуріон), а також аналіз відповідних статистичних даних вказують на нестійкість таких стегосистем (таємність забезпечується за рахунок збереження в таємниці алгоритму вбудовування інформації, що суперечить принципу Керкхофа). Звідси виникає необхідність створення лінгвістичної стегосистеми, яка б була стійкою до атак стегоаналітиків (активних та пасивних супротивників).

Хоча історія стеганографії нараховує тисячоліття, комп’ютерна стеганографія досить молода наука. Час її створення відносять до 1996 року. Розвиток засобів обчислювальної техніки та зв’язку дав поштовх розвитку комп’ютерної стеганографії. Повідомлення тепер «вкраплюється» в цифрові образи – фотографії, графічні зображення, відео, звукові, текстові файли, файли програм та інше.

Актуальність досліджень у галузі комп’ютерної стеганографії витікає з обмежень на використання криптографічних засобів та з необхідності розв’язування задач захисту прав власності на інформацію, яка представлена у цифровому вигляді. На сьогодні в якості інструментів для розвитку цієї дисципліни широко використовуються методи теорії ймовірностей та математичної статистики, теорії швидких ортогональних перетворень, теорії апроксимації, теорії кодування, теорії складності, теорії похибок, цифрової

обробки сигналів та зображень тощо. Тобто, як бачимо, це вже досить наукоємна дисципліна.

Незважаючи на молодість комп'ютерної стеганографії, до теперішнього часу вже чітко сформовано її основні поняття та принципи. Так в роботах [4, 5] наведено базову систему означень та математичні моделі стеганографічних систем. Велика кількість вітчизняних та зарубіжних публікацій присвячена аналізу головної характеристики стегосистеми – її стійкості. В [7, 11] наведено комплексний огляд теоретико–інформаційного, теоретико–складнісного та теоретико–ігрового підходу до оцінки стійкості стеганографічних систем. Не менш активно розвиваються і стеганографічні методи захисту інтелектуального капіталу.

Разом з тим чимало проблем поки що знаходяться на початковій стадії свого вирішення. Наведемо деякі з них:

– побудова стійких стеганографічних систем в рамках моделей пасивного та активного супротивників;

– отримання оцінок стійкості стеганографічних систем;

– отримання оцінок складності стеганографічних алгоритмів та їх порівняльний аналіз;

– розробка критеріїв оптимальності стеганоалгоритмів;

– побудова стеганоалгоритмів з мінімальною довжиною ключа при заданій стеганостійкості та інші.

Дана робота присвячена вирішенню деякиз з цих проблем, зокрема, аналізу стійкості стеганографічних систем в моделях пасивного [11] та активного супротивників.

Висновки до розділу I

1. Проведено огляд методів захисту інформції в каналах зв'язку та стеганографічних методів захисту інформації.

2. Проаналізовано поняття стеганографічної стійкості, розглянуто теоретико-інформаційний критерій стійкості та здійснено постановку задачі.

3. Проаналізовано структури стеганографічних систем та здійснено системний аналіз методик оцінки їх стійкості, що дає змогу обгрунтувати вибір типу стеганографічного перетворення в моделях пасивного та активного супротивників.

2 ДОСЛІДЖЕННЯ МЕТОДІВ ТА АЛГОРИТМІВ ОЦІНКИ СТЕГАНОГРАФІЧНОЇ СТІЙКОСТІ В МОДЕЛЯХ АКТИВНОГО І ПАСИВНОГО СУПРОТИВНИКІВ

2.1 Метод теоретико−статистичної оцінки стійкості стеганографічних систем

При побудові теоретико−статистичної оцінки потрібно ґрунтуватися на наступних принципах:

1) відштовхуватися від відомих методів організації атак на стеганосистеми, оскільки стійкість визначає можливість пасивних супротивників виявити прихований канал зв'язку застосуванням комплексних заходів аналізу (атак) системи тайнопису;

2) мати можливість порівнювати стійкість різнотипних стеганосистем;

3) мати можливість побудови практичної оцінки стійкості на основі розробленої теоретичної оцінки;

4) уміти чітко розпізнавати абсолютно стійкі стеганосистеми.

Отже, припустимо, що є стеганосистема, яка працює за схемою, представленою на рисунку 1.2. Відправник відсилає контейнер одержувачеві через канал загального користування. Контейнери, що відсилаються, можуть бути або порожніми, або містити приховане повідомлення, тобто бути стеганографічними контейнерами. Якщо передається стеганографічний контейнер, то говорять, що існує прихований канал зв'язку між відправником і одержувачем. Супротивник має доступ до всіх переданих повідомлень. Завданням супротивника є виявлення факту передачі прихованого повідомлення (виявлення прихованого каналу). Супротивник може застосувати власні методи аналізу контейнера, які допоможуть йому вирішити поставлене перед ним завдання.

Нас буде цікавити випадок, коли повідомлення, послане відправником, містить якусь інформацію, що зменшить ентропію на стороні одержувача як тільки останній розшифрує та прочитає повідомлення.

Одержувач, при виявленні прихованого каналу, використовуючи закритий ключ, застосовує стеганографічний алгоритм і отримує відкрите повідомлення.

При побудові даної моделі нас не буде цікавити, яким саме чином одержувач довідається про існування прихованого каналу на даний момент часу. Вважаємо, що існує оракул, за допомогою якого отримувач взнає про існування прихованого каналу.

Почнемо із простого випадку. Нехай по каналу загального користування можуть відсилатися контейнери одного типу K і для цього типу контейнерів існує один−єдиний параметр T, що має відомий (зокрема − відомий всім трьом учасникам у нашій моделі) середньостатистичний розподіл значень: $Y=(Y_1, Y_2, \ldots, Y_k)$, де k − кількість категорій для параметра T. Випадковою подією назвемо визначення значення параметра T супротивником і, відповідно, визначення приналежності до однієї з k категорій. Ясно, що для Y мають місце аксіоми Колмогорова. Супротивник, аналізуючи статистичну характеристику параметра T у контейнері, вирішує, або він містить приховані дані, або він порожній. Вважається, що супротивник буде використовувати множину статистичних критеріїв для оцінки відхилень закономірностей у значеннях параметра T для аналізованого контейнера. Пропонується використовувати критерій Хі−квадрат для оцінки стійкості стеганосистеми проти атак пасивного та активного супротивників, ґрунтуючись на наступних твердженнях:

1) критерій Хі−квадрат один з найвідоміших статистичних критеріїв [23];

2) успішно використовується при аналізі систем тайнопису на виявлення прихованого каналу;

3) є основним методом перевірки порушення закономірностей, які використовуються у поєднанні з іншими методами [24];

4) припускає використання скінченого числа категорій, що робить більш практичним його використання, у порівнянні з безперервними критеріями, що припускають нескінченну множину категорій;

5) грунтується на загальному принципі найменших квадратів, що знову−таки робить його більш практичнішим [24].

Стійкість представленої стеганосистеми до атак пасивних та активних супротивників є значення дистанції Хі−квадрат між очікуваним і спостережуваним розподілом імовірностей параметра T:

$$V = \sum_{s=1}^{k} \frac{(Y_s - np_s)^2}{np_s}, \qquad (2.1)$$

де Y_s – спостережуване число належності значення параметра T категорії s, p_s– очікувана ймовірність потрапляння T в категорію s, n – кількість проведених експериментів.

При порівнянні різнотипних стеганосистем треба враховувати той факт, що значення критерію Хі–квадрат залежить від вибору кількості категорій – чим більше категорій, тим більше значення критерію Хі–квадрат (див. таблиці по процентних точках Хі–квадрат розподілу) [23-24]. Ті ж таблиці видають однакові значення для конкретної процентної точки розподілу Хі–квадрат при рівній кількості категорій. Звідси слідує, що при порівнянні стеганосистем з різними параметрами T_i потрібно вибирати однакову кількість категорій.

Розглянемо основні властивості критерію оцінки стійкості стеганосистеми. Стійкість згідно теоретико–статистичного методу завжди більша, ніж стійкість по теоретико–інформаційній моделі. Іншими словами, дистанція Хі–квадрат завжди не менша, ніж відносна ентропія.

Стійкість, визначена в (2.1), завжди невід'ємна і дорівнює нулю тоді і тільки тоді, коли спостережуваний розподіл дорівнює очікуваному.

Перша частина цього твердження, а також достатність другої частини, випливають із попереднього твердження і з аналогічної властивості відносної ентропії. Доказ останнього можна знайти в [18]. Необхідність другої частини леми очевидна – підставляючи $Y_s=np_s$ у вираз (2.1), отримаємо нульове значення стійкості.

Випадок, коли ймовірності появи значення параметра T у кожної з категорій рівні, тобто $p_1= p_2=\ldots=p_k=\frac{1}{k}$, називається випадком з рівноймовірними категоріями.

Стійкість стеганосистеми, визначеної в (2.1), при рівноймовірних категоріях можна обчислити, використовуючи наступну спрощену формулу:

$$V = \frac{k}{n}\sum_{s=1}^{k} Y_s^2 - n, \qquad (2.2)$$

Доведення (2.2) здійснюється за допомогою наступних рівностей: $\sum_{s=1}^{k} Y_s = n$ і $\sum_{s=1}^{k} p_s = 1$, згідно яких очевидні наступні перетворення:

$$V = \sum_{s=1}^{k} \frac{(Y_s - np_s)^2}{np_s} = \sum_{s=1}^{k} \frac{\left(Y_s - \frac{n}{k}\right)^2}{\frac{n}{k}} = \frac{k}{n}\sum_{s=1}^{k} (Y_s)^2 - 2\sum_{s=1}^{k} Y_s + \sum_{s=1}^{k} \frac{n^2}{k^2} = \frac{k}{n}\sum_{s=1}^{k} Y_s^2 - n. \qquad (2.3)$$

Стеганосистема, абсолютно стійка по Качину, є також абсолютно стійкою по вищеозначеній теоретико–статистичній оцінці, а також навпаки, стеганосистема, що не є абсолютно стійкою по Качину, також не є абсолютно стійкою по теоретико–статистичній оцінці. Це пояснюється тим, що відповідно до моделі стеганосистеми, супротивникові відомі обидва розподіли ймовірностей появи конкретного контейнера в каналі зв'язку – і у випадку звичайної взаємодії, і у випадку створення прихованого каналу.

Розходження цих двох розподілів дає шанс супротивникові взламати систему. Відповідно до теоретико–інформаційної оцінки, при однакових розподілах імовірностей порожніх та стеганографічних контейнерів, супротивник не зуміє розпізнати стеганографічний контейнер, якщо такий з'явиться в каналі зв'язку, і, отже, така стеганосистема буде абсолютно стійкою до атак пасивних супротивників.

Виберемо в якості параметра для аналізу появу конкретного контейнера в каналі зв'язку. Середня статистика появи порожнього контейнера є нічим іншим, як очікуваною статистикою появи контейнерів у нестеганографічній системі.

Спостережуваною статистикою є імовірнісний розподіл появи стеганографічних контейнерів у каналі зв'язку. Оцінюючи стійкість такої системи до атак пасивних супротивників, використовуючи теоретико−статистичну оцінку, одержимо необхідний результат.

2.2 Загальна практична оцінка стійкості для складних систем тайнопису

Вищевикладений метод оцінки дає можливість оцінювати стійкість стеганосистем, які, із точки зору розроблювача системи, мають один вразливий параметр, відхилення якого може бути виявлене при статистичному аналізі контейнера. До таких систем, в основному, відносяться класичні методи приховування інформації в цифрових контейнерах і протоколи передачі прихованих даних. Для більш складних методів і протоколів, а також для складних підсистем стеганографічного захисту інформації, необхідно мати більше загальний метод оцінки стійкості,який не тільки дасть можливість оцінювати їх стійкість, але й порівнювати зі стеганосистемами іншого типу. Для складних систем існує множина взаємозалежних параметрів, істотне відхилення яких може мати вирішальне значення для даної системи і провокувати взлам такої системи. Прикладом для простих систем може бути випадок, коли користувачеві необхідно приховати дані в якому−небудь часто використовуваному контейнері. Для нього несуттєво, чи буде цим контейнером JPEG−файл або MP3−файл. Його цікавить тільки стійкість обраної системи і, відповідно, його перевага буде на боці більш стійкої системи.

Приклад для складних систем: користувачеві необхідна система тайнопису для приховування великої кількості даних. Існує дві альтернативи − або це буде стеганографічна файлова система, або стеганографічна база даних. Знову−таки, для користувача істотна тільки стійкість і йому необхідно мати під рукою метод порівняння стійкостей цих двох систем.

Перейдемо до визначення більше загальної й більше зручної, з практичної точки зору, оцінки стійкості на основі вищеописаного методу оцінки стійкості стеганосистем. Допустимо, що для стеганосистемы Ψ існує множина параметрів

$T=\{T_1, T_2, \ldots, T_m\}$, які можуть бути проаналізовані супротивником на предмет виявлення відхилень розподілу їх значень від очікуваних. Метою розробника системи є:

1) виявлення всіх тих параметрів, які мають істотні відхилення від середньостатистичних значень при створенні прихованого каналу;

2) розробка методів приховування, при яких в супротивника, при відомому статистичному аналізі контейнера, не з'явиться серйозних підстав для припущення про існування прихованого каналу в системі.

Отже, припустимо, що параметр T_i, як випадкова величина, має функцію щільності розподілу $f(T_i)$. Розіб'ємо інтервал $(-\infty, +\infty)$ на k частин: $(-\infty, a_{i1})$, (a_{i1}, a_{i2}), …, $(a_{i,k-1}, +\infty)$ таким чином, щоб мали місце наступні рівності, графічно представлені на рисунку 2.1:

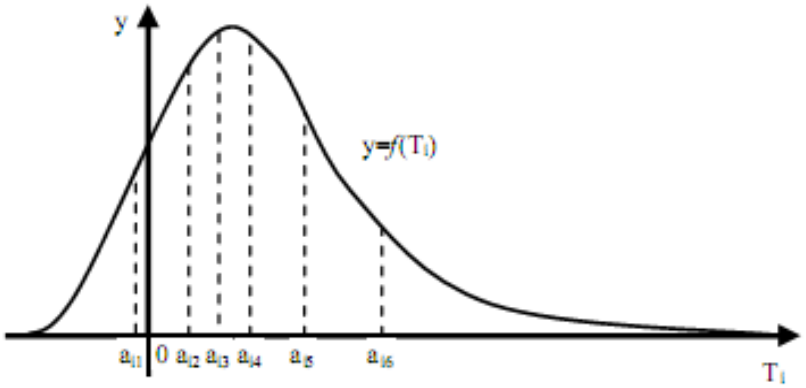

Рисунок 2.1 – Рівноймовірні категорії (k=7)

У цьому випадку маємо справу з рівноймовірними категоріями і можна використовувати спрощену формулу (2.2) для визначення стійкості по параметру T_i.

Для того, щоб одержати оцінку, яка буде враховувати всі параметри T_i, будемо слідувати очевидній логіці – просумуємо зважені значення стійкості по всіх параметрах, тобто:

$$V = \sum_{i=1}^{m} \lambda_i \left(\frac{k_i}{n} \sum_{s=1}^{k_i} \nu_{i,s}^2 - n_i \right). \qquad (2.4)$$

З огляду на залежності між коефіцієнтами λ_i ($\lambda_i \geq 0$ та $\sum_{i=1}^{m} \lambda_i = m$), і підставляючи їх в (2.4), отримаємо остаточний вигляд формули

$$V = \sum_{i=1}^{m} \lambda_i \frac{k_i}{n} \sum_{s=1}^{k_i} \left(r_{i,s} \right)^2 - \sum_{i=1}^{m} \lambda_i n_i \ . \qquad (2.5)$$

яка показує оцінку стійкості для складних систем тайнопису.

Продемонструємо застосування методу при оцінці стійкості реальних систем тайнопису. Як приклад візьмемо метод LSB (Least Significant Bit – метод найменшого значущого біту) для приховування даних у графічних контейнерах типу BMP. У якості параметра для аналізу контейнерів виберемо один з найбільш відомих параметрів, що визначає відхилення кількості сусідніх номерів кольору в пикселях зображення. Контейнерами будемо вважати BMP–файли з 24–бітною глибиною кольору та роздільною здатністю 800×600 пікселів. Простір приховування методом LSB для даного виду файлів дорівнює 468,75 кілобайт. Розглянемо, як змінюється значення стійкості такої системи тайнопису при зміні кількості приховуваних даних.

Визначимо параметр T_1 як різницю кількості пікселів з встановленим молодшим бітом червоної компоненти кольору від кількості пікселів з скинутим молодшим бітом. Параметри T_2 і T_3 будуть аналогічні T_1, але для зеленої та синьої компоненти кольорів відповідно. Аналіз приблизно 10000 порожніх контейнерів вищеозначеного виду дав зображений на рисунку 2.2 приблизний вигляд функції щільності розподілу різниці кількості сусідніх колірних компонентів для трьох обраних кольорів.

Після одержання очікуваного розподілу імовірностей по всіх категоріях та трьох колірних компонентам, можна перейти до оцінки різних модифікацій методу LSB. Розходження в основному представлялося у вигляді використаного простору приховування (ВПП). Також були застосовані різні техніки розподілу приховуваної інформації по всьому контейнеру. У таблиці 2.1 наведені оцінки

стійкості такої системи залежно від ВПП. Простір приховування становив 468,75 кБ.

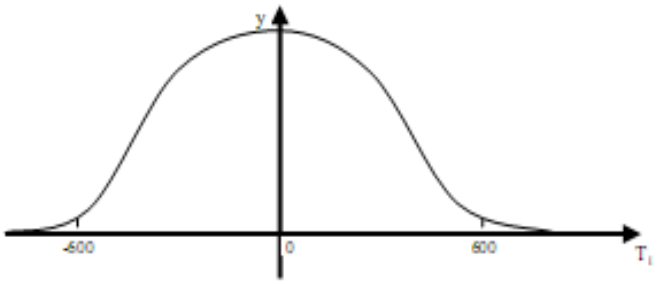

Рисунок 2.2 – Сподіваний розподіл розглянутого параметра при аналізі LSB методу

Таблиця 2.1 – Залежність стійкості від ВПП

ВПП	Стійкість (V)
0%	33
100%	1164
50%. Приховування відбувалося у верхній частині зображення	731
50%. Приховування відбувалося у нижній частині зображення	961
50%. Приховування відбувалося послідовно у кожний другий піксель зображення	1099
50%. Приховування відбувалося послідовно у кожний четвертий піксель зображення	696

В якості контейнера було використане те саме зображення. Як і очікувалося, чим менше даних приховується у контейнері, тим вище значення стійкості.

2.4 Про правило вибору елементів стеганографічного контейнера в приховуючому перетворенні

На стійкість стеганографічної системи критичним є вплив правила вибору елементів стеганографічного контейнера, що модифікуються в процесі

вбудовування інформації. Під елементом контейнера будемо розуміти атомарну частину цифрового об'єкта, що модифікується в процесі вбудовування інформації (яскравість колірних компонентів пікселів, коефіцієнти JPEG– та вейвлет−перетворення тощо).

Завдання полягає у побудові методу оптимального вибору елементів контейнера для вбудовування інформації − методу, що дозволяє максимізувати або стійкість стеганографічної системи при заданому розмірі приховуваного повідомлення, або пропускну здатність стегосистеми при заданій стійкості.

Різні елементи контейнера можуть бути об'єднані в групи, які не перетинаються, таким чином, що елементи однієї групи будуть мати подібні властивості та однаковий розподіл.

Розглядаємо контейнер як набір з m груп елементів. Кожна група характеризується кількістю k_i елементів, що містяться в ній, і їх розподілом. Позначимо через C_i область допустимих значень елементів контейнера, що входять в i−ту групу. Передбачається, що модифікація одного елемента i−ої групи дозволяє вмонтувати q_i біт, $q=log_2|C_i|$. Таким чином, розглядаємо цифровий об'єкт (контейнер, стего) у вигляді набору векторів елементів контейнера $c_1^i c_2^i ... c_{k_i}^i$, $c_i^j \in C_i$, $i = 1,...,m$.

Позначимо через x_i кількість елементів i−ої групи, що модифікуються, $0 \le x_i \le k_i$, $\Sigma x_i q_i = n$.

Нехай $f_i(c)$ − функція щільності розподілу елементів i−ої групи незміненого стеганографічного контейнера. Приховувана інформація має високу ентропію, тому що часто буває зашифрованою й/або стиснутою. Ця властивість прихованого повідомлення дозволяє знайти функцію щільності розподілу елементів i−ої групи контейнера з вбудованою інформацією − $\bar{f}_i(c, x_i)$, де x_i − кількість змінених елементів:

$$\bar{f}_i(c, x_i) = \frac{k_i - x_i}{k_i} f_i(c) + \frac{x_i}{k_i} \cdot \frac{1}{|C_i|}. \qquad (2.6)$$

Позначимо через $P(S)$ імовірність того, що як контейнер буде обраний цифровий об'єкт S:

$$P(S) = \prod_{i=1}^{m} \prod_{j=1}^{k_i} f_i(c_i^j). \qquad (2.7)$$

Ймовірність $\bar{P}(S)$ того, що в результаті вбудовування інформації буде отримане стего S, обчислюється аналогічно:

$$\bar{P}(S) = \prod_{i=1}^{m} \prod_{j=1}^{k_i} \bar{f}_i(c_i^j, x_i). \qquad (2.8)$$

Викладене вище дозволяє оцінити стійкість стеганографічної системи за допомогою теоретико−інформаційного підходу та відносної ентропії (відстані Кулльбака – Ляйблера) [24]:

$$D(P \| \bar{P}) = \sum_{S} P(S) \log_2 \frac{P(S)}{\bar{P}(S)}. \qquad (2.9)$$

Чим менша величина $D(P \| \bar{P})$, тим вища стійкість стегосистеми. Задача оптимального розподілу приховуваного повідомлення в стеганографічному контейнері зводиться до знаходження такого вектора $\{x_i\}_i$, $0 \le x_i \le k_i$, $\Sigma x_i q_i = n$, при якому величина $D(P \| \bar{P})$ була б мінімальною. Ця задача може бути вирішена, якщо функції $f_i(c)$ відомі.

Отримані в роботі результати дозволяють значно підвищити пропускну здатність стеганографічно системи при фіксованій стійкості або підвищити стійкість стегосистеми при заданій пропускній здатності. Ціль наступних досліджень полягає в адаптації запропонованої моделі до поширених форматів зображень, аудіо− та відеофайлів, що дозволить створювати більш досконалі стеганографічні системи.

2.5 Стегосистеми ідентифікаційних номерів, стійкі до атаки змовою

У теперішній час для захисту від копіювання та несанкціонованого використання медіаконтенту широко застосовується такий клас цифрових водяних знаків (ЦВЗ), як ідентифікаційні номери (ІН).

У випадку застосування ІН у контейнер, призначений кожному користувачеві, присвоюється персональний номер, що дозволяє контролювати подальший шлях цього контейнера. Якщо користувач виявиться медіапіратом і почне поширення своєї копії, то ідентифікаційний номер дозволить швидко визначити його.

Відповідно до термінології, використаної в роботі [11], множини ІН називаються стегосистемами ідентифікаційних номерів. При цьому, крім типових атак для ЦВЗ, таких, як перекодування, афінні та інші перетворення, для стегосистем ІН існує дуже небезпечна атака змовою.

Вона полягає у тому, що зловмисник побітно порівнює наявні у нього копії деяких медіаданих, що містять різні ІН, і робить висновок, що біти, у яких порівнювані дані розрізняються, виступають бітами ІН. Потім він установлює ці біти в деякі значення так, щоб отриманий ІН, який називається помилковим, не збігався з жодним з використаних при порівнянні. При цьому зловмисник переслідує одну з наступних цілей: знищити ІН або змінити його таким чином, щоб він ідентифікував когось іншого.

Для успішного протистояння атаці змовою необхідно використовувати допустимі множини. Це множина $W_n \subset \{0,1\}^n$ (або W, якщо довжина неістотна), у якій кожній підмножині $P \subseteq W_n$ однозначно зіставляється найменший інтервал $I(P)$, який його покриває. Надалі інтервал $I(P)$ будемо називати відповідним множині P.

Розглянемо деякі властивості допустимих множин:

1) якщо W_n допустима, то $|W_n| \le n$. Дана властивість накладає обмеження на кількість користувачів системи. Приміром, для того, щоб забезпечити ІН мережу з восьми мільйонів користувачів, то довжина кожного із цих номерів повинна бути

не менш мегабайта. Такий об'єм додаткового матеріалу є істотним і його подальше збільшення може створювати проблеми на етапі впровадження;

2) всі допустимі множини максимальної потужності ($|W_n|=n$) мають вигляд $O1(a)$, де $O1(a)=\{x\in\{0,1\}^n, d_H(a, x)=1\}$, $d_H(a, x)$ − відстань Хемінга між векторами a та x. Іншими словами, будь−яка допустима множина максимальної потужності − це сфера одиничного радіуса з деяким вектором a в якості центра.

2.5.1 Матричне подання стегосистем ІН

Розглянемо допустиму множину W_n потужності k. Представимо її у вигляді булевої матриці $||W||_{k\times n}$, рядками якої будуть вектори із множини W_n. Матриці, що відповідають допустимим множинам, будемо називати допустимими:

$$W_n=\begin{pmatrix} w_1[1] & w_1[2] & \dots & w_1[n] \\ w_2[1] & w_2[2] & \dots & w_2[n] \\ \dots & & & \\ w_k[1] & w_k[2] & \dots & w_k[n] \end{pmatrix}_{k\times n}$$

Виходячи із властивостей допустимих множин, доцільно розглядати матриці, для яких $k<n$. Визначимо наступні операції над допустимими матрицями:

1) перестановка стовпців і рядків;

2) інверсія стовпця;

3) видалення повторюваних стовпців.

Причому застосування операцій 1−3 ніяк не впливає на властивість допустимості. Матриці A та A' будуть еквівалентними, якщо вони можуть бути отримані одна з одної шляхом застосування визначених вище операцій. Допустимі множини W та W' будуть еквівалентними, якщо відповідні їм допустимі матриці еквівалентні. У кожному класі еквівалентності існує матриця $W_n=(E_kA_{n-k})$ де $E_k=\begin{pmatrix} 1 & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 \\ & & & \\ 0 & 0 & \dots & 1 \end{pmatrix}_{k\times k}$, $A=||A||k\times(n-k)$. Множина W буде називатися

сильно допустимою, якщо видалення будь–якого стовпця у відповідній йому матриці спричинює втрату властивості допустимості. Причому матриця, яка відповідає будь–якій сильно дпустимій множині, еквівалентна E_k. Якщо W_n – допустима множина, то існує матриця W_n'=($E_k A$), еквівалентна матриці W_n, у якої підматриця A не є допустимою. Із наведених тверджень випливає, що властивість допустимості ґрунтується на наявності підматриці, еквівалентної одиничній. Решта матриці не впливає на допустимість і може бути обрана довільно.

2.5.2 Ідентифікація зловмисників по помилковому ІН

Розглянемо сильно допустиму множину, задана матрицею E_k. У кожному стовпці цієї матриці всі елементи, за винятком одного, дорівнюють нулю. Отже, одиниця у будь–якій компоненті помилкового ІН може з'явитися в тому і тільки в тому випадку, якщо відповідний користувач брав участь в атаці змовою. Відповідно до цього, ідентифікувати учасників змови по побудованому ними помилковому ІН можливо у всіх випадках, крім одного − коли ІН складається із всіх нулів. Спостерігаючи одиницю в i–ій компоненті помилкового ІН, робимо висновок, що i–ий користувач брав участь у змові. При інвертуванні i–го стовпця в матриці E_k на зловмисника вкаже єдиний нуль в i–му стовпці. Проглядаючи покомпонентно помилковий ІН, можна зробити висновок про ступінь провини кожного учасника. Зловмисниками виявляться користувачі з номерами i, такими, що $w' = \bar{f}_{maj}(w_1, w_2, ..., w_k)$, де w'– помилковий ІН, а f_{maj} – мажоритарна функція. Описаний спосіб ідентифікації зловмисників може бути використаний у будь–якій допустимій множині.

При використанні запропонованого методу ідентифікації завжди існує помилковий ІН, що не ідентифікує нікого: $w = f_{maj}(w_1, w_2, ..., w_k)$, i=1, 2, ... , k. Надалі будемо позначати його w_{maj}. Виникає закономірне питання: чи завжди зловмисник може побудувати w_{maj} і чи існує стратегія, яка дозволяє будувати саме його його, а не будь–який випадковий вектор з інтервалу, що відповідає наявним у нього ІН?

Відповідь полягає у тому, що коли потужність множини P більша або дорівнює 2, то w_{maj} належить $I(P)$. Крім того, $w_{maj}[i] = f_{maj}(w_1[i], w_2[i], w_3[i])$, i=1, 2, …, k, де w_1, w_2, w_3 – будь–які попарно різні вектори з W. Звідси випливає, що коли потужність множини більша або дорівнює 3, то зловмисник завжди може побудувати ІН, який не ідентифікує нікого.

Описаний спосіб побудови помилкового ІН будемо називати мажоруючою атакою. Це окремий випадок атаки змовою, що характеризується строго визначеним вибором вектора з $I(P)\backslash P$. Відповідно до запропонованого методу ідентифікації, побудова вектора w_{maj} являється єдиним способом для групи зловмисників уникнути відповідальності в повному об'ємі, тобто жоден з них не буде виявлений. В зв'язку із цим подальше завдання полягає в розробці вузьконапрямленого методу ідентифікації, що протистоїть мажоруючій атаці.

2.5 Алгоритм побічної стеганографії для активного і пасивного супротивників

Суть розробленого алгоритму побічної стеганографії [19] полягає в наступному. У відправника й одержувача містяться однакові масиви даних, які є секретними ключами. Байти інформації, що підлягають захисту, замінюються (за певним алгоритмом) байтами секретного масиву даних. Отриманий новий масив даних розміром вихідного повідомлення передається адресатові. Отриманий по каналу масив даних піддається зворотньому перетворенню: байти цього масиву даних замінюються байтами секретного масиву даних (дзеркальний алгоритм).

Загальна схема непрямої стеганографії показана на рисунку 2.3.

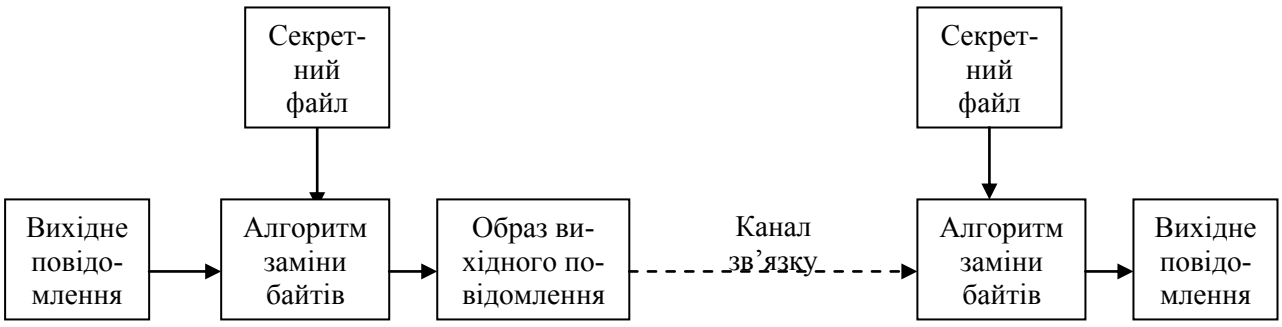

Рисунок 2.3 – Загальна схема побічної стеганографії

Для побічної стегосистеми, згідно пункту 1.3, можна дати наступне визначення: сукупність $Y=(C, @C, M, D, E)$, де C – множина контейнерів–ключів, $@C$ – множина параметрів елементів множини C (множина непрямих контейнерів), M – множина секретних повідомлень, $E_{@}$: $C\times M\rightarrow @C$, $D_{@}$: $C\times @C\rightarrow M$ – стеганографічне перетворення з властивістю $D_{@}(E_{@}(c, m), @c)=m$ для будь – яких $m\in M$, $c\in C$ і $@c\in @C$, являє собою побічну стегосистему.

Згідно цього визначення, множина C являє собою секретний (або особистий) ключ, що використовується для шифрування та дешифрування вихідних повідомлень (секретних даних). Крім того, вимога $|C| \geq |M|$ не являється строгою.

На відміну від класичних формальних стегосистем, де криптоаналітику доступна множина контейнерів, побічна стегосистема передбачає можливість доступу лише до параметрів елементів контейнера. Крім того, якщо в класичних системах приховані (від криптоаналітика) або алгоритми перетворення (наприклад, E: $C\times M\rightarrow C$, D: $C\rightarrow M$), або ключі шифрування, або й те і інше, то в пропонованій системі секретною інформацією є вміст самого контейнера, що дозволяє розробляти досить високостійкі системи захисту інформаційних ресурсів у комп'ютерних системах і мережах.

В якості параметрів елементів контейнера можуть бути використані адреси розміщення елементів, їх колірні гами, формати, кореляційні показники і т.п. Для спрощення подальшого викладу будемо розглядати адресні параметри елементів контейнера–ключа C. Варто мати на увазі, що незалежно від того, як задані значення параметрів – прямо або побічно, вони повинні адекватно відбивати значення елементів множини M.

Нехай задано алфавіт з скінченною множиною букв. Будемо вважати, що контейнер–ключ C формується з букв алфавіту. Розташування букв алфавіту у контейнері повинно бути довільним (наприклад, псевдовипадковим) з можливістю їх багаторазового входження. Кожній букві алфавіту ставиться у відповідність значення адресного простору. Сукупність значень адресного

простору становить множину @C (побічний контейнер). Кількість букв алфавіту повинна бути такою, щоб з них можна було скласти будь−яке повідомлення *M*. Таким чином, повідомлення подібні до контейнера−ключа *C* в тому розумінні, що вони складаються з однакових букв із різною кількістю їх повторень і різним місцем розташування.

Нехай необхідно передати секретне повідомлення *M* по каналу зв'язку. Для цього довільним чином вибирається початкова адреса розміщення якого−небудь елемента (букви) у контейнері−ключі. Починаючи із цієї адреси (у будь−якому напрямку) здійснюється пошук першого елемента (букви) повідомлення в масиві елементів (букв) контейнера−ключа. Оскільки контейнер обов'язково містить всі букви алфавіту і кожна буква повторюється в довільному порядку в масиві елементів контейнера багаторазово, то пошук завершиться успішно. Перша буква повідомлення замінюється адресою знайденого елемента (букви) контейнера. Далі в масиві−контейнері здійснюється пошук другого елемента (букви) повідомлення, що заміщується адресою знайденого елемента (букви). Процес повторюється до повного формування множини адрес. Сформована в такий спосіб множина адресних даних являє собою побічний контейнер @C, що відправляється адресатові по відкритому каналу. Адресат має такий же секретний масив *C* (контейнер−ключ), як і у відправника. У відправленому побічному контейнері також утримуються стеганографічні образи початкового (стартового) значення адреси пошуку, параметри масиву повідомлень, тимчасового штампа й т.п., тобто алгоритм розшифровки повідомлень являється «дзеркальним» відображенням алгоритму шифровки: за значенням першого елемента побічного контейнера *@C* у контейнері−ключі здійснюється пошук букви (елемента), адреса якого записана в першому елементі *@C*. Вміст знайденої адреси заміщує перший елемент побічного контейнера *@C*. Далі здійснюється пошук другої букви і т. д. В кінцевому результаті букви множини *@C* будуть збігатися з буквами множини *M*.

Як приклад розглянемо простий варіант реалізації алгоритму непрямої стеганографії. Нехай повідомлення M являє собою комп'ютерний файл F, довжина якого дорівнює *l* байтів. Вибираємо алгоритм псевдовипадкових чисел $\wp(\lambda)$, що відповідає вимогам стійкості генерованих даних (у теперішній час ученими

розроблено безліч таких алгоритмів. Наприклад, повторюваність алгоритму, описаного в [20], становить приблизно 6000 десяткових знаків). Нехай стартове число $\lambda=\lambda_0$ для $\wp(\lambda)$. Вибір можна здійснювати або навмання, або за допомогою простого генератора випадкових чисел разового користування. У першій версії реалізованого алгоритму непрямої стеганографії генерація псевдовипадкових чисел виконується таким чином. Генератор $\wp(\lambda)$, починаючи з стартової точки $\lambda=\lambda_0$, генерує 2^{20} рядків. Кожний рядок складається з 256 байтів. У кожному рядку містяться всі двійкові числа від 0 до 255, розташовані випадковим чином за законом генератора $\wp(\lambda)$, що гарантує генерацію неоднакових чисел у кожному рядку. Крім того, гарантується відсутність однакових рядків у вибраній довжині генерованого масиву чисел. Таким чином, формується двовимірний масив випадкових чисел $C(i, j)$, де $i = 256$, $j = 4096$.

Процес шифрування файлу F полягає в наступному. За допомогою простого випадкового генератора вибирається рядок $j=\varpi$ у масиві $C(i, j)$ (номер рядка ϖ також підлягає шифруванню для відправлення одержувачеві). Вміст першого байта [1] файла F представляється як адреса байта @[1] у рядку $j=\varpi$. Вміст байта [@[1]] записується в перший байт файла F, тобто [1]:= [@[1]]. Потім вміст другого байта [2] файла F представляється як адреса байта @[2] у рядку $j=\varpi\pm1$. Вміст байта [@[2]] у рядку $j=\varpi\pm1$ записується в другий байт файла F, тобто [2]:=[@[2]]. Процес повторюється до заміщення останнього байта значенням масиву випадкових чисел за обраною адресою. Таким же чином заміщуються значення ряду службових даних, у тому числі значення ϖ. У випадку, коли $l > 2^{20}$, процес повторюється по колу.

У реалізованій для завдань реального часу версії алгоритму непрямої стеганографії, так званому «алгоритмі на льоту», немає необхідності повторювати процес по колу, тому що кількість генерованих неповторюваних чисел набагато більша, ніж обсяг будь–яких файлів, що відправляються по мережі. Цей же алгоритм може бути використаний не тільки для завдань реального часу, але і для звичайних блокових даних, що підлягають шифруванню.

Безумовно, наукове обґрунтування криптостійкості алгоритму непрямої стеганографії вимагає глибокого аналізу з боку криптоаналітиків. Однак

проведені дослідження та отримані експериментальні результати дозволяють судити про його високу криптостійкість.

Слід зазначити, що алгоритми непрямої стеганографії мають схожі властивості із класом криптоалгоритмів, що не розкриваються, описаних К. Шенноном [25] і досить докладно проаналізованих пізніше [14].

Практичні особливості реалізації непрямої стеганографії такі:

1) проблема поширення ключа (передача контейнера *C*). Оскільки ця проблема актуальна для всіх методів і технологій криптографії із ключами, то можна використовувати самі передові алгоритми та способи поширення ключів. Істотним є той факт, що, на відміну від інших методів, у цьому випадку потрібна разова гарантія доставки ключа, тому що після гарантованого одержання ключа адресатом можна при першому ж сеансі замінити вміст контейнера *C*. Тому, наприклад, вміст контейнера можна передати за допомогою відкритих ключів, довжина яких свідомо гарантує неможливість дешифрування вмісту контейнера (2048, 4096). Безумовно, при цьому буде потрібно набагато більше часу для шифрування та дешифрування вмісту контейнера, але з огляду на те, що відповідні обчислення виконуються один раз, такий спосіб є виправданим.

2) імовірність відновлення вмісту контейнера *C* по відомому криптоаналітику шифру @C. Насамперед, варто звернути увагу на те, що довжина ключа–контейнера *C*, у порівнянні з відомими методами шифрування з використанням ключів, незрівнянно більша ($|C| \geq |M|$). Тому відновлення контейнера за значеннями стає неможливим. Наприклад, у програмно реалізованому варіанті шифрування комп'ютерних файлів кількість варіантів перебору дорівнює 256! (біля 2^{1700} варіантів).

Використання запропонованого методу захисту інформації в різних прикладних системах, залежно від області застосування, має деякі особливості. Автори досліджували застосування непрямої стеганографії в комп’ютерних розподілених мережах у завданнях захисту переданого трафіка, проведення процедур аутентифікації та авторизації користувачів, а також у мобільних мережах для рішення завдань захисту голосового трафіка під час розмови між користувачами.

У сучасних розподілених комп'ютерних системах для проведення процедур аутентифікації та авторизації користувачів, як правило, використовуються наступні варіанти: використання пари логін\пароль; застосування електронних пристроїв.

Найбільш простим і розповсюдженим методом є використання пари «логін\пароль». З огляду на те, що сучасні обчислювальні засоби дозволяють вирішувати завдання розкриття простих паролів невеликої довжини за лінійний час, то використовують довгі паролі (довжина більше 8–10 символів), які складно запам'ятовувати. Використання непрямої стеганографії в таких алгоритмах дозволяє уникнути вищеописаної проблеми, тому що передана інформація для системи аутентифікації та авторизації користувачів не має корельованої інформації з використаним паролем, зокрема його довжини та складності. Таким чином, при пересиланні необхідної інформації неможливо відновити пароль за перехопленими повідомленнями, тому що вони будуть кожен раз різними. Для узгодження ключа контейнера можливим є використання системи «Діффі–Хеллмана–Меркле» [22]. У такому випадку лінії зв’язку повинні бути надійно захищені від модифікації повідомлень при узгодженні контейнера–ключа або заданих параметрів його генерації.

Використання електронного пристрою при реалізації алгоритму непрямої стеганографії дозволяє реалізувати механізм одноразових паролів досить простим способом. Оскільки використання цього алгоритму передбачає наявність контейнера–ключа, що у цьому випадку буде зберігатися у пам'яті електронного пристрою, то він може бути використаний як набір одноразових ключів для проходження процедур верифікації користувача. Використання такої реалізації процедури авторизації та аутентифікації користувачів не припускає початкового обміну заданими параметрами (контейнера–ключа, початкові параметри генерації й т.п.).

Використання пропонованого алгоритму захисту переданих даних в існуючих мобільних мережах поєднано з вирішенням ряду складних завдань. Такі мережі в основній своїй масі є гетерогенними мультисервісними з різними можливостями. Тому при впровадженні алгоритму захисту передаваної

інформації від несанкціонованого доступу необхідно забезпечити деякі можливості.

1) інтероперабельність алгоритму шифрування та його реалізацій. Забезпечується за рахунок застосування алгоритму на прикладному рівні моделі OSI, а також апаратно незалежною побудовою схеми шифрування. Таким чином забезпечується прозорість використання алгоритму на різних мобільних мережах;

2) потоковий режим функціонування алгоритму шифрування;

3) малі вимоги до ресурсів, які необхідні для ефективного функціонування використовуваних алгоритмів шифрування;

4) висока криптостійкість та швидкість виконання операцій. Це є найбільш суперечлива вимога, тому що в різних криптосистемах криптостойкість самої системи визначається тільки складністю вирішення відповідної математичної задачі, покладеної в основу алгоритму або швидкості виконання криптографічних операцій.

Використання запропонованого алгоритму організації захищеного інформаційного обміну дозволяє реалізувати швидкі, криптостійкі рішения, які можуть значно підвищити захищеність інформації від несанкціонованого доступу. Особливо варто виділити використання даного алгоритму для побудови систем ідентифікації та аутентифікації, які дозволяють використовувати короткі й прості для запам'ятовування паролі.

У запропонованому новому методі шифрування вихідний файл не шифрується, а замість нього передаються по мережі тільки відповідні ознаки зашифрованого файлу. Обчислювальна складність алгоритму мінімальна, тому що шифрування файлів припускає тільки заміщення байтів вихідного файлу байтами спеціально організованого файлу−ключа. При даному способі шифрування ніякими методами та засобами не можна розшифрувати перехоплений шифр, якщо навіть криптоаналітику буде мати попередній шифр та попередній вихідний текст.

Висновки до розділу 2

1. Досліджено метод теоретико-статистичної оцінки стійкості стеганографічних систем та показано її вплив на практичну оцінку стійкості.

2. Удосконалено алгоритм побічної стеганографії для активного і пасивного супротивників, який має більшу стійкість до стеганоаналізу.

3. Обгрунтовано правило вибору елементів стеганографічного контейнера в приховуючому перетворенні в розрахунку на активного і пасивного супротивників.

3 МОДЕЛІ СТЕГАНОГРАФІЧНИХ ПЕРЕТВОРЕНЬ З ВРАХУВАННЯМ ПАСИВНИХ ТА АКТИВНИХ АТАК

3.1 Аналіз стійкості стеганографічних систем в моделі пасивного супротивника

Аналізуючи ринок відповідних програмних продуктів, легко побачити, що переважна більшість з них для приховування повідомлень використовують різні модифікації методу найменшого значущого біта (НЗБ) [11]. Користувач обирає довільний контейнер, розміри якого дозволяють розмістити в ньому повідомлення, і в результаті отримує стегозображення, яке візуально нічим не відрізняється від оригіналу. Наскільки ж безпечним є використання таких програм?

Раніше вважалося, що НЗБ пікселів зображення, а також НЗБ аудіосигналу, незалежні між собою та незалежні від усіх інших бітів елемента контейнера. Але насправді між молодшими бітами сусідніх елементів природних контейнерів та між молодшим бітом і іншими бітами елемента стегоконтейнера існують суттєві кореляційні зв’язки, які можуть бути порушені вбудовуванням повідомлення. Для розпізнавання стегоповідомлення, сформованого з таких контейнерів, достатньо найпростішого аналізу – візуальної атаки, спрямованої на найменші значущі біти.

Як видно з рисунків 3.1–3.4, програми Steganos Security Suite 6.0 та S–Tools 4.0 не здійснюють аналіз зображення на наявність у ньому зон однорідного кольору, що повністю дискредитує їх при виборі користувачем контейнера з наявними такими зонами або при можливості противника нав’язувати контейнер.

Один із можливих підходів при визначенні зон однорідності полягає у використанні дискретних ортогональних перетворень. Всі отримані спектральні коефіцієнти блоку зображення, що належить до зони однорідності, крім постійної складової, будуть близькі до нуля. При цьому кращу ефективність дають ті ж перетворення, які дають кращу ефективність при стисненні.

Рисунок 3.1 – Пустий контейнер: графічне зображення розміром 128×128 пікселів

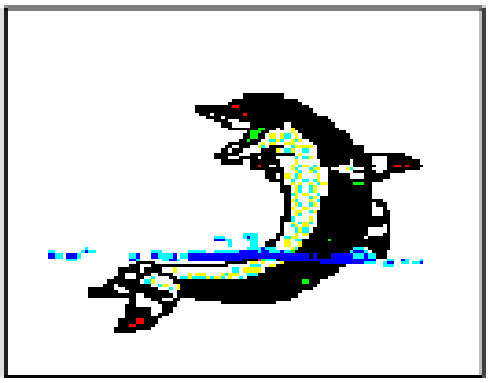

Рисунок 3.2 – Зображення, сформоване з НЗБ пустого контейнера

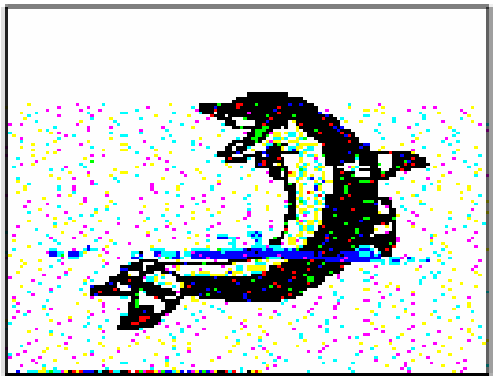

Рисунок 3.3 – Зображення, сформоване з НЗБ стего, отриманого за допомогою програми Steganos Security Suite 6.0, розмір вбудованого повідомлення – 255 байт

Рисунок 3.4 – Зображення, сформоване з НЗБ стего, отриманого за допомогою програми S–Tools 4.0, розмір вкрапленого повідомлення – 255 байт

Разом з тим виключення з області вкраплення зон однорідного кольору не робить систему стійкою до візуальної атаки на найменші значущі біти (рисунки 3.5–3.8).

Ці ж програми дають стійкі до візуальної атаки на НЗБ стего, якщо використовувати в якості пустого контейнера зашумлене зображення. Найпростіший спосіб отримання такого контейнера – це сканування зображення з паперового оригіналу або використання зображення з вебкамери. Проводячи вбудовування» в НЗБ зашумленого контейнера, слід по стегоключу розподілити біти повідомлення рівномірно по всьому об’єму молодших бітів контейнера.

Інакше вбудоване повідомлення також досить легко виявити візуальною атакою на НЗБ (рисунки 3.9–3.12).

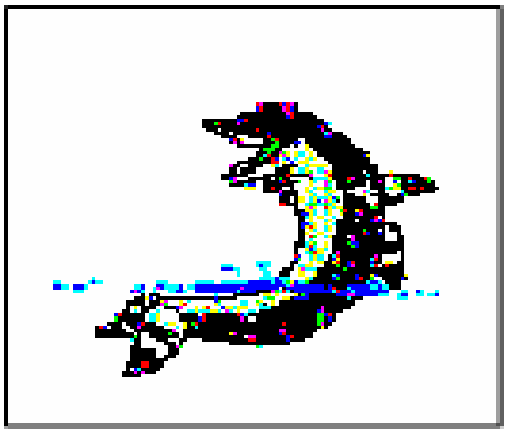

Рисунок 3.5 – Зображення, сформоване з НЗБ стего, отриманого за допомогою програми BMP Secrets, розмір вкрапленого повідомлення – 261 байт

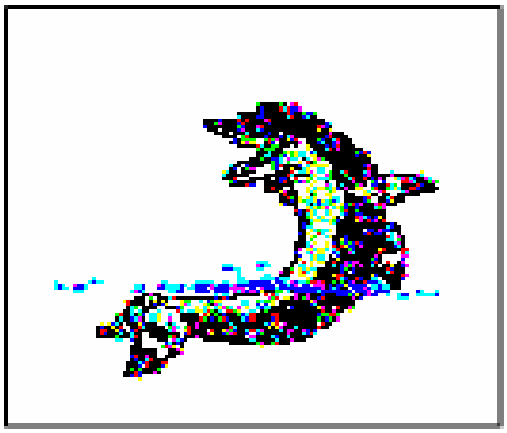

Рисунок 3.6 – Зображення, сформоване з НЗБ стего, отриманого за допомогою програми BMP Secrets, розмір вкрапленого повідомлення – 772 байт

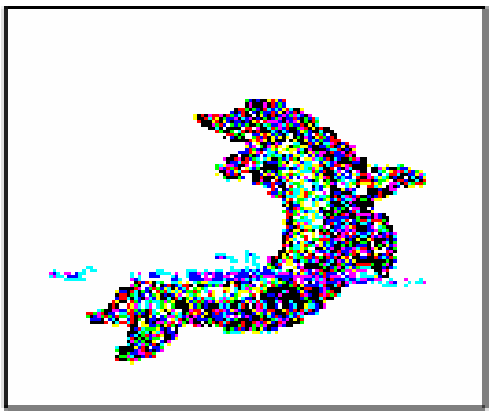

Рисунок 3.7 – Зображення, сформоване з НЗБ стего, отриманого за допомогою програми BMP Secrets, розмір вкрапленого повідомлення – 2,1 кБ

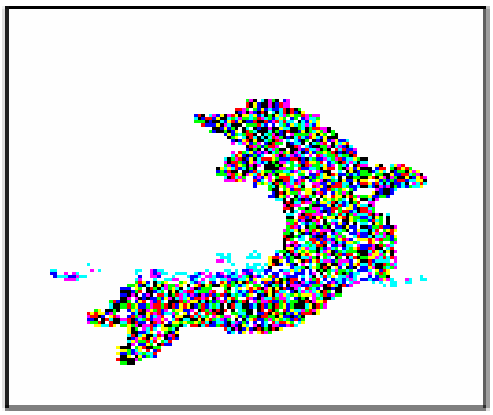

Рисунок 3.8 – Зображення, сформоване з НЗБ стего, отриманого за допомогою програми BMP Secrets, розмір вкрапленого повідомлення – 3кБ

І все ж таки багато програм цього не виконують. Відповідні приклади наведені у таблиці 3.1.

Рисунок 3.9 – Пустий контейнер: відскановане зображення розміром 128×128 пікселів

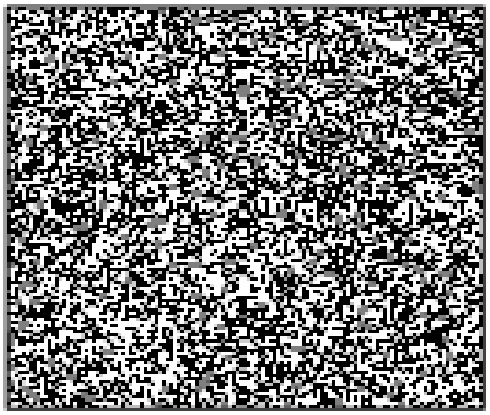

Рисунок 3.10 – Зображення, сформоване з НЗБ пустого контейнера з рисунка 3.11

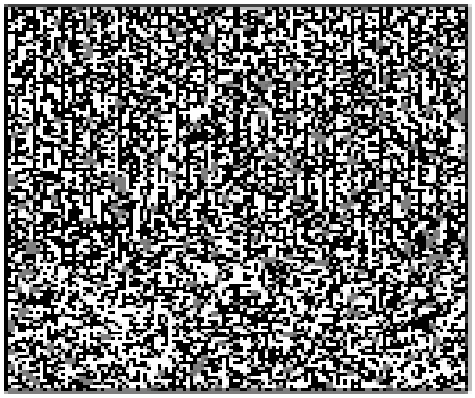

Рисунок 3.11 – Зображення, сформоване з НЗБ стего, отриманого за допомогою програми Stegograph, розмір повідомлення – 3,92 кБ

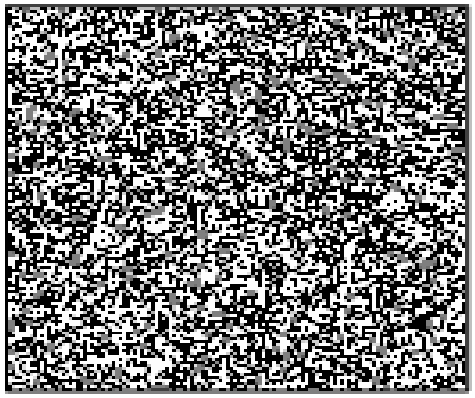

Рисунок 3.12 – Зображення, сформоване з НЗБ стего, отриманого за допомогою програми S–Tools, розмір повідомлення – 3,92 кБ

Таблиця 3.1 – Аналіз стегопрограм по розподілу даних по контейнеру

Стегопрограми, що розподіляють дані по контейнеру	Стегопрограми, що не розподіляють дані по контейнеру
OutGuess	Steganos Security Suite
HideSeek	JSTEG
S–Tools	JPHS
Steaghan	Steghide
BMP Secrets	DC–Stegano

Для зашумленого контейнера більш дієвими є атаки, що базуються на аналізі розбіжностей між статистичними характеристиками природних контейнерів та сформованих із них стего. Статистичні методи аналізу включають в себе оцінку ентропії, коефіцієнтів кореляції, вірогідності появи та залежності між елементами послідовностей, умовні розподіли, розрізнення розподілів за критерієм Хі−квадрат та інше.

Отже, для побудови абсолютно стійкої в рамках моделі пасивного противника стеганографічної системи приховане повідомлення не повинно змінювати статистику контейнера. Для цього можна використовувати методи селектуючої або конструюючої стеганографії.

Підхід селектуючої стеганографії полягає в тому, що потрібно згенерувати досить велику кількість пустих контейнерів і потім вибрати з них найбільш відповідний. У граничному випадку можна знайти контейнер, який вже містить приховане повідомлення при заданому ключі. Тоді контейнер взагалі не буде змінено і виявити факт передачі повідомлення неможливо. Можна провести паралель між описаним методом та шифром одноразового блокноту в криптографії. Разом з тим реалізація такої абсолютно стійкої стегосистеми в більшості випадків потребує великої кількості обчислень та створює стегоканал з низькою пропускною здатністю.

Інший шлях побудови стійкої стеганосистеми – використання конструюючої стеганографії. В конструюючій стеганографії контейнер не обирається, а генерується самою стеганосистемою як функція від повідомлення, при цьому моделюються необхідні статистичні характеристики контейнера. Як приклад таких наробок можна навести використання для генерації стего імітаційних функцій Пітера Уейнера [24]. Отримані за допомогою функцій імітації стего будуть стійкими відносно автоматизованих статистичних атак, але разом з тим у більшості випадків буде втрачатися внутрішній зміст контейнера, що дозволяє виявити наявність стего при аналізі каналу.

Відомо, що стеганосистема, у якій вбудовування повідомлення відбувається у спектральній області контейнера, є більш стійкою у порівнянні з системою, що вбудовує повідомлення безпосередньо в елементи вихідного контейнера.

Аналіз ринку програмних продуктів показує, що більшість програм, працюючих зі спектром контейнера, використовують для вбудовування коефіцієнти дискретного косинусного перетворення (ДКП), і перш за все тому, що воно лежить в основі розповсюдженого стандарту JPEG. Разом з тим поза увагою залишаються інші перспективні перетворення, такі, як, наприклад, швидке перетворення високої кореляції (ШПВК), вейвлет, швидке перетворення Фур'є (ШПФ).

ШПВК дає можливість розробляти стеганографічні алгоритми з меншою обчислювальною складністю порівняно з алгоритмами на базі косинусного перетворення. Стеганосистеми на основі ШПФ мають більшу пропускну здатність порівняно з системами на базі ДКП.

Таким чином, при розробці програмного забезпечення, орієнтованого на метод НЗБ, потрібно:

1) обмежити множину допустимих контейнерів, використовуючи для прихованої передачі інформації тільки зашумлені;

2) рівномірно розподіляти біти прихованого повідомлення по всьому об'єму молодших бітів контейнера;

3) враховувати при вбудовуванні інформації властивості людського зору, такі, як чуттєвість до контрасту, розмірів, форми, кольору, розташування та інше;

4) використовувати для вбудовування молодші значущі біти не самого зображення, а його спектральних коефіцієнтів, зокрема приховувати інформацію паралельно зі стисненням зображення.

3.2 Узагальнені моделі стеганографічних перетворень інформації з урахуванням пасивних атак

Забезпечення стеганографічного захисту, стійкого до пасивних атак, вимагає врахування особливостей стеганографічного аналізу при вбудовуванні даних. Теоретико−множинна та структурна моделі дозволяють описати стеганографічні перетворення у компактному вигляді.

Пропонується така теоретико−множинна модель стегонаграфічних перетворень з урахуванням пасивних стегоаналітичних атак:

$$SSM = \{I', D, K, \tilde{I}, \tilde{I}', M, F, \tilde{F}, T, E, Emb, m, f, \tilde{f}, t, e, v, Ext\}, \qquad (3.1)$$

де $I, I', D, K, \tilde{I}, \tilde{I}'$ – множини зображень, зображень для оцінки, повідомлень, ключів, стегозображень, стегозображень для оцінки, відповідно;

M – множина параметрів поліноміальної моделі, яка прогнозує значення характеристики бінарної класифікації при стеганографічному аналізі за допомогою множини $I \cup \tilde{I}$;

F – множина характеристик оригінальних зображень, що використовуються для стеганографічного аналізу;

$\tilde{F}$ – множина характеристик стегозображень, що використовуються для стеганографічного аналізу;

T – множина параметрів стегоаналітичного критерію для проведення класифікації в множині $F \cup \tilde{F}$;

E – множина оцінок якості класифікації, що виконується за допомогою стегоаналітичного критерію;

$Emb: I \times D \times K \times M \to \tilde{I}$ – функція вбудовування даних у зображення;

$m: I \times \tilde{I} \times T \to M$ – функція визначення параметрів поліноміальної моделі;

$f: I \times D \times K \times M \to \tilde{I}$ – функція визначення характеристик зображень;

$\tilde{f}: \tilde{I} \times E \to \tilde{F}$ – функція визначення характеристик стегозображень;

$t: F \times \tilde{F} \to T$ – функція визначення параметрів стегоаналітичного критерію;

$e: T \times I' \times \tilde{I}' \to E$ – функція визначення оцінок якості стегоаналітичної класифікації;

$v: E \times \tilde{I} \to \{\varnothing, \tilde{I}\}$ – функція визначення стегозображення, що є стійким до пасивних атак;

$Ext: \tilde{I} \times K \to D$ – функція відновлення даних із стегозображення.

Запропонованій теоретико–множинній моделі стеганографічних перетворень з урахуванням пасивних стегоаналітичних атак відповідає структурна модель, наведена на рисунку 3.13.

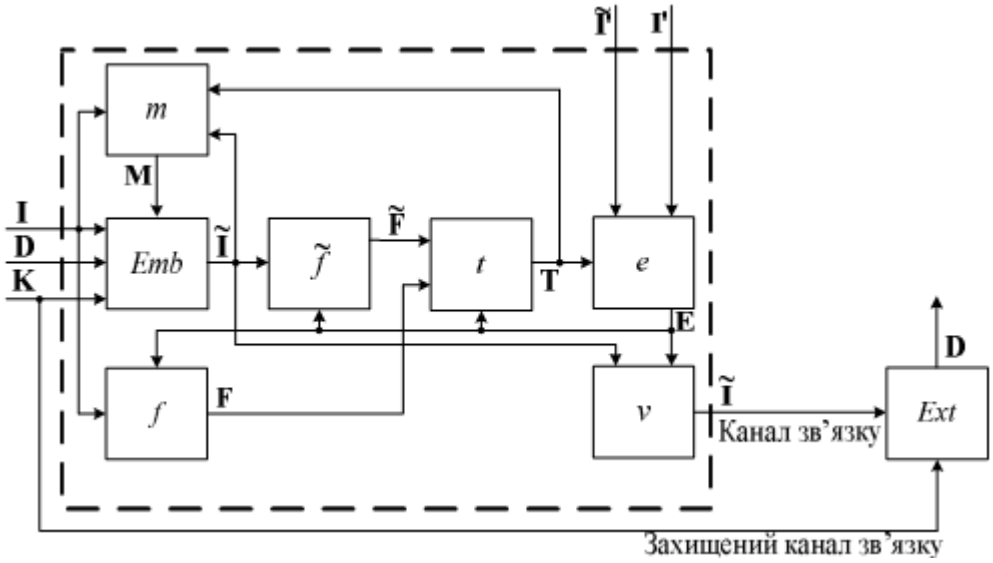

Рисунок 3.13 – Структурна модель стеганографічних перетвореньз врахуванням пасивних стегоаналітичних атак

З аналізу запропонованої моделі стеганографічних перетворень, що враховує особливості стеганографічного аналізу, зрозуміло, що підвищення стійкості до пасивних атак досягається за рахунок створення поліноміальної моделі прогнозування характеристики бінарної класифікації при стеганографічному аналізі зображень, яка використовується для вбудовування даних. Отже, стійкість стеганографічних перетворень залежить від точності даної поліноміальної моделі.

Більшість сучасних методів стеганографічного аналізу використовують бінарні класифікатори на основі методу опорних векторів (МОВ), де точка–характеристика *v* у просторі ознак, які використовуються при стегоаналізі і яка представляє аналізоване зображення *I*, належить одному з півпросторів (“стего” та “не стего”), що утворюються гіперплощиною класифікації *L* (рисунок 3.14).

Таким чином, задачею непомітного вбудовування є забезпечення максимального обсягу таємних даних за умови збереження положення точки

характеристики стегозображення $\tilde{I}$ у півпросторі «не стего». Пропонується один з можливих підходів вирішення даної задачі, що полягає у збереженні показника положення точки характеристики стегозображення $h^*(\tilde{I})$ відносно гіперплощини класифікації L, тобто $h^*(\tilde{I}) = h^*(I)$, де $h^*(I)$ – положення точки характеристики оригінального зображення відносно гіперплощини класифікації L. Для цього пропонується розробити поліноміальну модель прогнозування характеристики бінарної класифікації зображень при стеганографічному аналізі, що описує параметр $h^*(\tilde{I})$ і використовує у якості аргументів значення пікселів зображення.

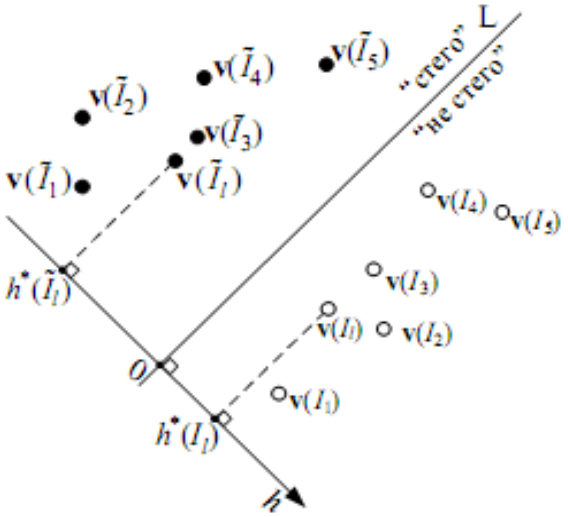

Рисунок 3.14 – Схема класифікації точок характеристик зображень у двовимірному просторі ознак при проведенні стеганографічного аналізу

Для створення поліноміальної моделі, що прогнозує значення $h^*(\tilde{I})$ на основі значень пікселів зображення, пропонується використати метод групового врахування аргументів (МГВА), оскільки ефективність даного методу підтверджена на прикладі чисельних моделей із значною кількістю вхідних аргументів.

Однак, навіть для невеликих зображень, наприклад, розміром 256×256 пікселів, загальна кількість вхідних аргументів складає 65536. Створення поліноміальної моделі за допомогою МГВА з врахуванням зазначеної кількості аргументів вимагає надзвичайних обчислювальних витрат.

З іншого боку при стеганографічному аналізі зображення розміром 256×256 пікселів описуються кількістю характеристик, що не перевищує 300. Тому пропонується вбудовувати дані у сегменти P зображення, які є невеликими за розміром, що дозволяє оцінити значення $h^*(\tilde{})$ (значення оцінки надалі позначається $h(\tilde{})$) за допомогою пікселів сегменту $p_1, p_2, \ldots, p_n$, де n – кількість пікселів, та набору характеристик $v_1, v_2, \ldots, v_m$ для решти зображення K, які використовуються при стегоаналізі, де m – кількість характеристик (рисунок 3.15).

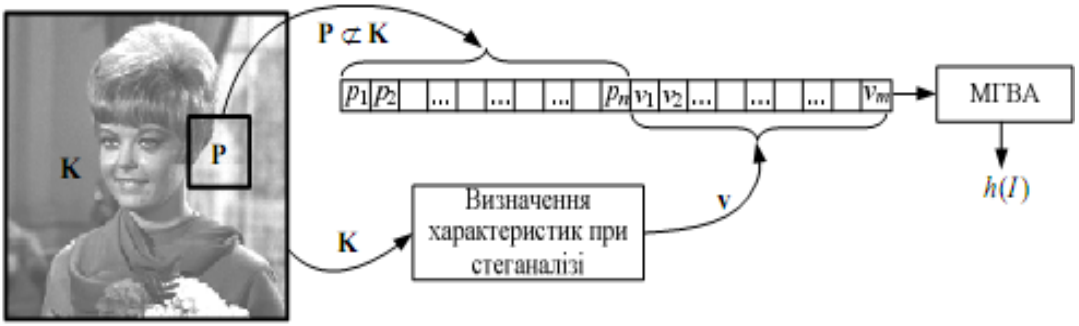

Рисунок 3.15 – Схема визначення поліноміальної моделі прогнозування положення точки характеристики зображення відносно гіперплощини класифікації L

Для вбудовування даних у зображення з врахуванням пасивних стегоаналітичних атак необхідно виконати таку послідовність дій:

1) створити навчальну вибірку зображень ($I_1, I_2, \ldots, I_n$), яка складається з оригінальних зображень та стегозображень з різним обсягом даних, вбудовуваних за допомогою різних методів стеганографічного захисту інформації в КСМ;

2) визначити вектори–характеристики $v(I_1), v(I_2), \ldots, v(I_n)$;

3) провести навчання класифікатора з метою розділення векторів–характеристик у просторі ознак на два класи, що визначають стеганографічно змінені та оригінальні зображення;

4) визначити параметри $h^*(I_1), h^*(I_2), \ldots, h^*(I_n)$, що відповідають положенню точок–характеристик $v(I_1), v(I_2), \ldots, v(I_n)$ відносно гіперплощини класифікації L;

5) використати МГВА з метою отримання поліноміальної моделі прогнозування характеристики $h(I)$ положення $h^*(I)$ точки–характеристики $v(I)$ зображення I відносно гіперплощини класифікації L при стеганографічному аналізі;

6) використати параметри поліноміальної моделі $h(I)$ у якості обмежень при вбудовуванні даних у зображення.

Реалізація стеганографічного захисту інформації вимагає, окрім іншого, визначення сегментів P зображення, що використовуються для створення поліноміальної моделі прогнозування характеристики бінарної класифікації та, відповідно, для вбудовування даних, а також визначення обсягу даних, що вбудовуються.

3.3 Методи адаптивного вбудовування даних у сегменти зображень з використанням поліноміальних моделей

Поліноміальна модель $h(I)$ прогнозування характеристик бінарної класифікації при стегоаналізі, що отримана за допомогою МГВА, представляється в загальному вигляді поліномом Колмогорова–Габора. Дана особливість обумовлює значні обчислювальні витрати при адаптивному вбудовуванні даних у сегменти зображень з урахуванням параметрів такої моделі. Тому пропонуються методи адаптивного вбудовування з використанням поліноміальних моделей, що є окремими випадками поліному Колмогорова–Габора, і також можуть використовуватися для прогнозування характеристик бінарної класифікації при стегоаналізі.

Для розробки методу адаптивного вбудовування даних в область коефіцієнтів базисного перетворення розглянемо модель, що підходить для прогнозування характеристик бінарної класифікації при стегоаналізі певного класу зображень I_1:

$$h(\tilde{1}) = a_1 p_{l,1}^{k_1} + a_2 p_{l,2}^{k_2} + \ldots + a_i p_{l,i}^{k_i} + \ldots + a_n p_{l,n}^{k_n}, \qquad (3.2)$$

де $a=(a_1, a_2, \ldots, a_i, \ldots, a_n)$ – вектор коефіцієнтів;

$p_l=(p_{l,1}, p_{l,2}, \ldots, p_{l,i}, \ldots, p_{l,n})$ – вектор пікселів l – ого сегменту зображення I_1, розміром $\sqrt{n} \times \sqrt{n}$.

Для даної моделі пропонується метод стеганографічного захисту інформації, що забезпечує вбудовування даних в область коефіцієнтів базисного перетворення пікселів сегменту зображення, який представлено схематично на рисунку 3.16.

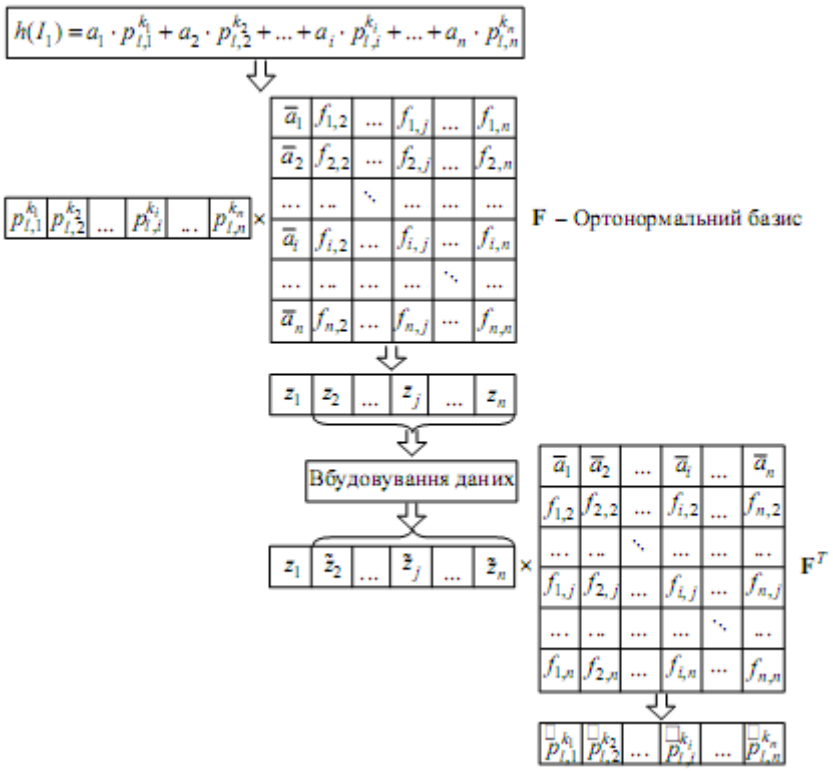

Рисунок 3.16 – Схема вбудовування даних з використанням методу вбудовування даних в область коефіцієнтів базисного перетворення

Метод складається з таких пунктів:

1) визначити ортонормальний базис F, один вектор якого збігається з вектором $\bar{a}$, що отримується шляхом нормалізації a: $\bar{a}_i = a_i / \|a\|$;

2) виконати базисне перетворення послідовності $p_{l,1}^{k_1}, p_{l,2}^{k_2}, \ldots, p_{l,i}^{k_i}, \ldots, p_{l,n}^{k_n}$ з використанням базису F та отримати послідовність коефіцієнтів $z_1, z_2, \ldots, z_j, \ldots, z_n$.

3) виконати вбудовування даних з використанням коефіцієнтів z_2, ..., z_j, ..., z_n та методу бінарної інтерпретації і отримати послідовність змінених коефіцієнтів $\tilde{z}_2,...,\tilde{z}_j,...\tilde{z}_n$;

4) виконати зворотне базисне перетворення послідовності $z_1,\tilde{z}_2,...,\tilde{z}_j,...\tilde{z}_n$ з використанням базису F^T та отримати послідовність $\tilde{p}_{l,1}^{k_1},\tilde{p}_{l,2}^{k_2},...,\tilde{p}_{l,i}^{k_i},...,\tilde{p}_{l,n}^{k_n}$ отримати послідовність $\tilde{p}_{l,1},\tilde{p}_{l,2},...,\tilde{p}_{l,i},...,\tilde{p}_{l,n}$ змінених пікселів l – ого сегменту. Відновлення даних, що приховані за допомогою методу стеганографічного захисту інформації, який використовує модель, представлену формулою (3.2), показано схематично на рисунку 3.17 і описується такою послідовністю дій:

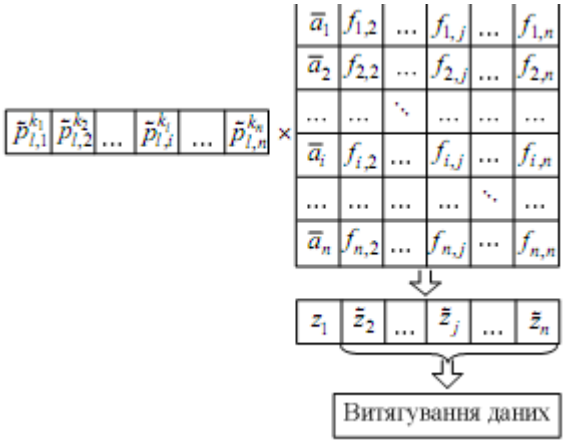

Рисунок 3.17 – Схема відновлення даних

1) виконати базисне перетворення послідовності $\tilde{p}_{l,1}^{k_1},\tilde{p}_{l,2}^{k_2},...,\tilde{p}_{l,i}^{k_i},...,\tilde{p}_{l,n}^{k_n}$ з використанням базису F та отримати послідовність коефіцієнтів $z_1,\tilde{z}_2,...,\tilde{z}_j,...\tilde{z}_n$;

2) за допомогою методу бінарної інтерпретації отримати таємні дані з послідовності коефіцієнтів $\tilde{z}_2,...,\tilde{z}_j,...\tilde{z}_n$.

Для розробки методу адаптивного вбудовування даних у просторову область іншого класу зображень I_2 розглянемо ще один окремий випадок поліноміальної моделі:

$$h(\tilde{z}_2) = A p_{l,1}^{k_1} \cdot p_{l,2}^{k_2} \cdot ... \cdot p_{l,i}^{k_i} \cdot ... \cdot p_{l,n}^{k_n}, \qquad (3.3)$$

де A – константа.

Для даної моделі пропонується метод адаптивного вбудовування даних в область зображень, що забезпечує стеганографічний захист таємної інформації, і який представлено схематично на рисунку 3.18. Метод складається з таких пунктів:

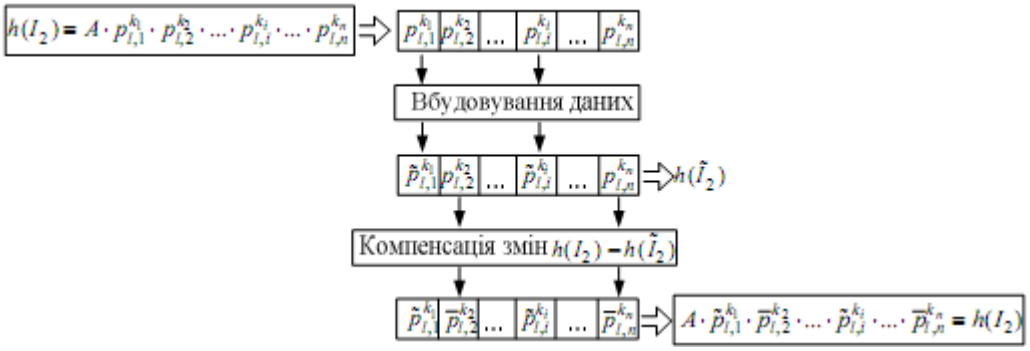

Рисунок 3.18 – Схема вбудовування даних з використанням методу вбудовування даних у область зображень

1) визначити множину пікселів $E_l=\{p_{l,j}\}$ l – ого сегменту зображення I_2 , що використовуються для вбудовування;

2) виконати вбудовування даних з використанням множини E_l та отримати множину змінених пікселів $\tilde{E}_l = \{\tilde{p}_{l,j}\}$;

3) визначити положення $h(\tilde{I}_2)$ точки–характеристики стегозображення $\tilde{I}_2$ з урахуванням змінених пікселів множини $\tilde{E}_l$;

4) визначити множину пікселів $C_l=\{p_{l,i}\}$, $E_l \cap C_l=\varnothing$, які використовуються для компенсації зміни положення $h(I_2) - h(\tilde{I}_2)$ точки–характеристики стегозображення $\tilde{I}_2$ відносно гіперплощини класифікації;

5) змінити пікселі множини C_l таким чином, щоб виконалася умова $h(I_2) - h(\tilde{I}_2) = 0$ та отримати множину змінених пікселів $\overline{C}_l = \{\overline{p}_{l,i}\}$. Об’єднати множини $\tilde{E}_l$ та $\overline{C}_l$, отримати множину змінених пікселів l–ого сегменту стегозображення $\tilde{I}_2$: $\tilde{E}_l \cup \overline{C}_l \to \tilde{p}_l$. Відновлення даних, що приховані за допомогою методу стеганографічного захисту інформації, який використовує

модель, представлену формулою (3.3), показано схематично на рисунку 3.19, та описується такою послідовністю дій:

1) визначити множину пікселів $\tilde{E}_l = \tilde{p}_{l,j}$, що інтерпретують таємні дані;

2) з використанням методу бінарної інтерпретації отримати таємні дані з $\tilde{E}_l$.

При проведені стеганографічного аналізу досить важливе значення також мають візуальні характеристики стегозображення. Тому для забезпечення таємності вбудовування даних необхідно мінімізувати спотворення вбудовування.

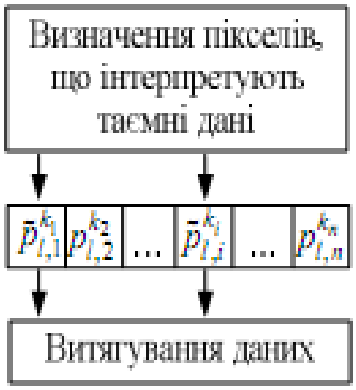

Рисунок 3.19 – Схема відновлення даних

Запропоновані узагальнені моделі стеганографічних перетворень інформації, на відміну від існуючих, враховують відповідні особливості проведення пасивних, а також активних атак, що застосовує зловмисник при стеганографічному аналізі. Використання даних моделей при розробці стеганографічних методів та засобів дозволяє підвищити стійкість до пасивних та активних атак в комп'ютерних системах і мережах. Розроблені методи адаптивного вбудовування даних у сегменти зображень, на відміну від існуючих, використовують поліноміальні моделі прогнозування характеристик бінарної класифікації при стеганографічному аналізі, які є окремими випадками поліному Колмогорова–Габора. Це дозволяє забезпечити стійкість до пасивних та активних атак при вбудовуванні значного обсягу таємних даних.

3.4 Аналіз стійкості метода Коха–Жао стеганографічного вбудовування інформації в статичні зображення

Алгоритм Коха–Жао для приховання даних використовує частотну область контейнера і полягає у відносній заміні величин коефіцієнтів дискретного косинусного перетворення (ДКП). Зображення розбивається на блоки розмірністю 8×8 пікселів і до кожного блоку застосовується ДКП. Кожний блок придатний для запису одного біта інформації. При організації секретного каналу вибираються два коефіцієнти ДКП зі смуги середніх частот, які задаються координатами (υ_1,ν_1) та (υ_2,ν_2). Для передачі біта «0» ці коефіцієнта змінюються так, щоб різниця між ними стала не нижче деякої фіксованої величини P $(\geq P)$. Для передачі біта «1» ця різниця повинна стати не вище, ніж $(\leq -P)$. Після цього відбувається зворотне ДКП. Від вибору параметрів $\upsilon_1,\nu_1,\upsilon_2,\nu_2$ і P залежить величина внесених змін при вбудовуванні інформації в контейнер і стійкість стеганосистеми.

Проведемо дослідження стійкості стеганографічної системи до JPEG–компресії з різними коефіцієнтами стиску α та розробимо рекомендації з вибору параметрів алгоритму Коха–Жао при організації секретного каналу передачі інформації.

Для кількісної оцінки величини спотворення використовувалося пікове відношення сигнал/шум, що обчислюється в децибелах:

$$PSNR = 10log_2 \frac{n \cdot 255^2}{\sum_{i=1}^{n} (x_i - \bar{x}_i)^2}, \qquad (3.4)$$

де n – число пікселей у зображенні, $x_i, \bar{x}_i$ – значення пікселів вихідного зображення й зображення з вбудованим повідомленням, 255 – максимальне значення яскравості напівтонового зображення (тобто 8 біт/піксель). Така модель хоч і не є точною, оскільки погано узгоджується із зоровою системою

людини, але вона дуже популярна у зв'язку із труднощами математичного опису останньої. Якщо в середньому *PSNR*≥28 дб, то величину внесених спотворень можна вважати прийнятною. У деяких випадках можуть бути більше жорсткі вимоги до внесених спотворень.

Для проведення досліджень було відібрано 10 фотографій розміром 200×150 пікселей. У канал синього кольору кожної з них вбудоване повідомлення довжиною 300 біт, що представляє собою бітове зображення розміром 20×15 пікселей. Вбудовування відбувалося в коефіцієнти з координатами (4,5), (5,4) і (3,2), (2,3) при різних значеннях параметра P, що змінювалося від 5 до 55 із кроком 5. Таким чином, було отримано 220 зображень, кожне з яких надалі було піддано компресії з різним коефіцієнтом стиску α, що змінюється від 12 до 2 із кроком 1. Чим менше α, тим більшому стиску піддаються зображення. Із всіх стислих зображень (2420 шт.) відновлювалось повідомлення, що порівнювалося з оригіналом. Для оцінки збігу повідомлень обчислювався коефіцієнт кореляції:

$$\rho = \frac{\sum_{i=1}^{N} w_i \widehat{w}_i}{\sqrt{\sum_{i=1}^{N} w_i^2} \sqrt{\sum_{i=1}^{N} \widehat{w}_i^2}}, \qquad (3.5)$$

де $w_i, \widehat{w}_i$ – елементи оригінального та відновленого повідомлення; N – кількість біт повідомлення.

Різні варіанти відновленого повідомлення і відповідні коефіцієнти кореляції представлені в таблиці 3.2.

Результати досліджень представлені на рисунках 3.20 та 3.21. Аналіз характеру зміни кривих на рисунку 3.20 показує, що при збільшенні параметра P значення коефіцієнта кореляції ρ із зони повного руйнування повідомлення (заштрихована область) переходить у зону часткового руйнування, після чого досягає рівня повної відповідності відновленого та оригінального повідомлень ($\rho = 1$), і надалі не змінюється.

Таблиця 3.2 – Приклади оригінального і спотворених повідомлень після відновлення і відповідні коефіцієнти кореляції

Графічне повідомлення 1					
Коефіцієнт кореляції, ρ	1,00 (оригінал)	0,82	0,79	0,67	0,55
Графічне повідомлення 2					
Коефіцієнт кореляції, ρ	1,00 (оригінал)	0,99	0,94	0,89	0,72

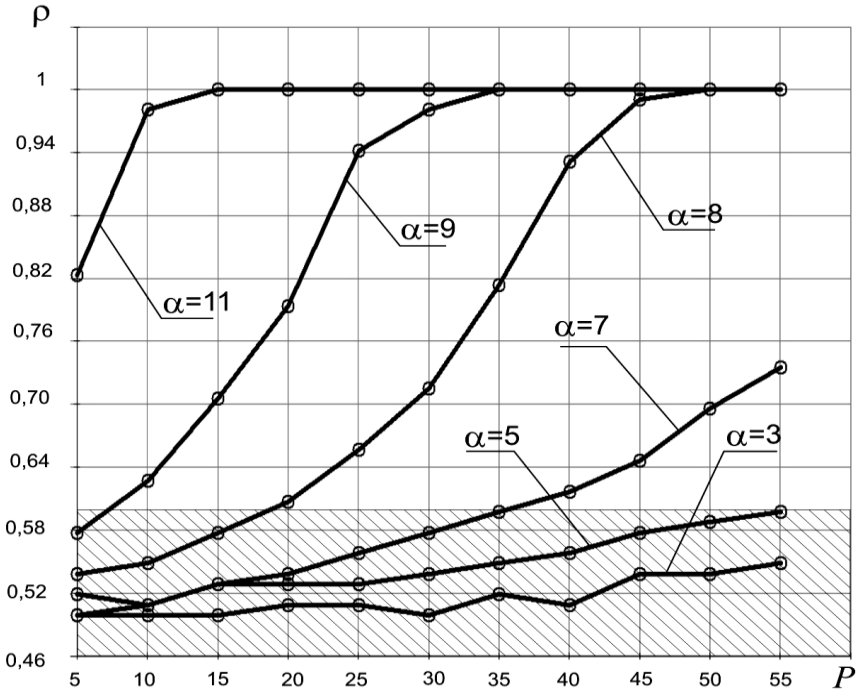

Рисунок 3.20 – Зміна коефіцієнта кореляції для відновленого та

оригінального повідомлень залежно від параметра P при різних коефіцієнтах стиску контейнера α (для вбудовування обрані коефіцієнти (4,5) і (5,4))

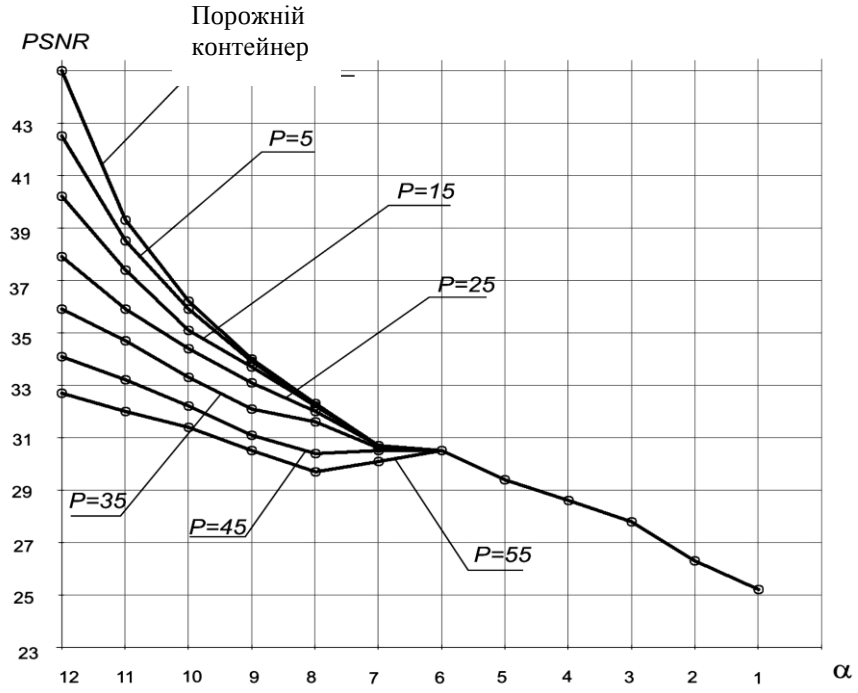

Рисунок 3.21 – Зміна пікового відношення сигнал/шум залежно від параметра *P* при різних коефіцієнтах стиску контейнера α (для вбудовування обрані коефіцієнти (4,5) і (5,4))

Аналіз характеру зміни кривих на рисунку 3.21 показує, що при компресії контейнера з коефіцієнтом стиску $\alpha \le 5$ величина параметра P практично не впливає на пікове відношення сигнал/шум *PSNR* (криві зливаються на цій ділянці), що означає руйнування вбудованого повідомлення. Це підтверджується тим, що криві на рисунку 3.20 при $\alpha \le 5$ перебувають у зоні повного руйнування повідомлення.

Звичайно, при збільшенні параметра P криві перейдуть у зону часткового руйнування, однак у даній роботі було встановлено, що при значеннях $P > 55$ можуть з'являтися видимі зміни контейнера при вбудовуванні інформації, що є вкрай небажаним при побудові стеганосистеми. Тому був зроблений висновок, що метод Коха–Жао придатний, якщо не потрібна стійкість стеганосистеми до

компресії з коефіцієнтом стиску $\alpha \le 5$.

Отримані результати також показали, що при вбудовуванні повідомлення в коефіцієнти з координатами (3,2), (2,3) стійкість до стиску, а, відповідно, і спотворення контейнера виявилися більші, ніж при вбудовуванні в коефіцієнти з координатами (4,5), (5,4). Крім того, повідомлення не руйнується, коли спотворення, внесені компресією зображень, не перевищують спотворень, внесених вбудовуванням повідомлення.

Цікаво простежити за характером зміни значення пікового відношення сигнал/шум *PSNR* при $P = 55$ (див. рисунок 3.21). На ділянці $8 < \alpha < 12$ значення *PSNR* спадає, а відновлене повідомлення повністю збігається з оригіналом (див. рисунок 3.1). Отже, переважають спотворення, внесені при вбудовуванні інформації. На ділянці $6 < \alpha < 8$ значення *PSNR* зростає, а відновлене повідомлення частково зруйноване. Це значить, що величина внесених спотворень при стиску контейнера наближена до величини спотворень, внесених при вбудовуванні інформації. На ділянці $1 < \alpha < 6$ значення *PSNR* знову спадає, а відновлене повідомлення повністю зруйноване, тому переважають спотворення, внесені при стиску контейнера.

Залежно від вимог, висунутих до стеганосистеми, може бути потрібна різна стійкість до компресії контейнера. Наприклад, це може бути вимога часткової відповідності відновленого та оригінального повідомлень із коефіцієнтом кореляції $\rho = 0{,}8$ при компресії контейнера з коефіцієнтом стиску $\alpha \ge 9$. На підставі результатів досліджень, отриманих у даній роботі, були розроблені рекомендації з вибору параметра P при вбудовуванні повідомлення по алгоритму Коха–Жао залежно від пропонованих вимог до стійкості стеганосистеми (таблиця 3.3).

Таблиця 3.2 – Оптимальне значення параметра алгоритму P в залежності від вимог, висунутих до стійкості стеганосистеми

$\rho \backslash \alpha$	12	11	10	9	8	7	6
0,6	5	5	5	10	20	30	40
0,7	5	5	10	15	30	35	–

0,8	5	5	15	25	35	–	–
0,9	5	10	15	30	40	–	–
1	10	15	25	35	50	–	–

У випадку вимоги часткової відповідності відновленого та оригінального повідомлень із коефіцієнтом кореляції $\rho = 0{,}8$ при компресії контейнера з коефіцієнтом стиску $\alpha \geq 9$ рекомендується значення $P = 25$. Якщо потрібна повна відповідність відновленого та оригінального повідомлень ($\rho = 1$) при компресії контейнера з коефіцієнтом стиску $\alpha \geq 8$ рекомендується значення $P = 50$.

Отримані результати відносяться до вбудовування повідомлення, що представляє собою бітове зображення. Однак, якщо вбудовується текстова інформація, то потрібна повна відповідність відновленого та оригінального повідомлення. У цьому випадку можна піти по наступному шляху. Перед вбудовуванням повідомлення скористатися одним з методів завадостійкого кодування для перетворення текстового повідомлення в завадостійкий код, попередньо стиснувши інформацію. Це дозволить, з одного боку, позбутися надлишковості, що завжди властива текстовій інформації, а з іншого боку – додати специфічну надлишковість, що дозволить відновити повідомлення після часткового руйнування.

Отримані результати дозволяють при організації секретного каналу передачі інформації обґрунтовано вибирати параметри алгоритму Коха–Жао, що забезпечують необхідний рівень стійкості одночасно з максимально можливою «непомітністю» вбудованого повідомлення.

Прийнятне значення параметра P алгоритму Коха–Жао перебуває в діапазоні $5 \leq P \leq 55$. Якщо $P < 5$, то повідомлення руйнується при найменшому стиску контейнера. Якщо $P > 55$, то видимі спотворення, внесені при вбудовуванні інформації в контейнер, надмірно великі. У випадку прийнятних значень параметра P алгоритм Коха–Жао може забезпечити стійкість до компресії контейнера з коефіцієнтом стиску $\alpha \geq 6$ при повній відповідності відновленого повідомлення або частковому його руйнуванні. Якщо потрібна

стійкість до компресії контейнера з коефіцієнтом стиску $\alpha \leq 5$, то алгоритм Коха–Жао непридатний.

Висновки до розділу III

1. Побудовано узагальнені структурні моделі стеганографічних перетворень інформації з урахуванням пасивних і активних стегоаналітичних атак.

2. Розроблено методи адаптивного вбудовування даних у сегменти зображень з використанням поліноміальних моделей та показано їх переваги.

3. Показано, що при організації стеганографічного каналу передачі інформації отримані у роботі результати дозволяють обґрунтовано вибирати параметри алгоритму Коха–Жао, які забезпечують необхідний рівень стійкості системи одночасно з максимально можливою «непомітністю» вбудованого повідомлення.

4. Наведено практичні рекомендації по вибору відповідного параметра алгоритму Коха–Жао із заданою стеганографічною стійкістю до компресії контейнера.

ВИСНОВКИ

1. Проаналізовано структури стеганографічних систем та здійснено системний аналіз методик оцінки їх стійкості, що дає змогу обгрунтувати вибір типу стеганографічного перетворення в моделях пасивного та активного супротивників.

2. Розроблено алгоритм побічної стеганографії для активного і пасивного супротивників, який має більшу стійкість до стеганоаналізу.

3. Показано, що при організації стеганографічного каналу передачі інформації отримані у роботі результати дозволяють обґрунтовано вибирати параметри алгоритму Коха−Жао, які забезпечують необхідний рівень стійкості системи одночасно з максимально можливою «непомітністю» вбудованого повідомлення.

4. Побудовано узагальнені структурні моделі стеганографічних перетворень інформації з урахуванням пасивних і активних стегоаналітичних атак.

5. Розроблено методи адаптивного вбудовування даних у сегменти зображень з використанням поліноміальних моделей та показано їх переваги.

6. Наведено практичні рекомендації по вибору відповідного параметра алгоритму Коха−Жао із заданою стеганографічною стійкістю до компресії контейнера.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ.

1. Задірака В.К., Олексюк О.С., Недашковський Н.О. Методи захисту банківської інформації. – К.: Вища школа, 1999. – 261 с.
2. Хорошко В.А., Чекатков А.А. Методы и средства защиты информации. − К.: Юниор, 2003. − 504 с.
3. Задірака В.К., Олексюк О.С. Комп'ютерна криптологія. – Тернопіль: Збруч, 2002. – 504 с.
4. Хорошко В.А., Шелест М.Е. Введение в компьютерную стеганографию. − К.: НАУ, 2002. − 140 с.
5. Аграновский А.В. , Девянин П.Н. , Хади Р.А. , Черемушкин А.В. Основы компьютерной стеганографии. – М.: Радио и связь, 2003. – 152 с.
6. Stallings W. Cryptography and network security: principles and practice. – New York: Prentice Hall, 2006. – 680 p.
7. Задірака В.К., Мельнікова С.С., Бородавка Н.В. Спектральні алгоритми комп'ютерної стеганографії // Штучний інтелект. – 2002. – № 3. – С. 532-541.
8. Бородавка Н.В., Задирака В.К. Стеганоалгоритмы на базе теоремы о свертке // Кибернетика и системный анализ. – 2004. – № 1. – С. 139-144.
9. Сироватка П.В., Літош М.С., Довгич Н.І., Ануфрієнко К.П. Підвищення рівня стеганографічної стійкості до суб'єктивних атак // АВІА-2011: Матеріали X Міжнародної науково-технічної конференції. – К.: НАУ, 2011. – Т.1. – С. 2.42 - 2.45.
10. Кесслер Г. Стеганография для судебного исследователя // Компьютерно-техническая экспертиза. – 2008. – №2. – С. 13-25.
11. В.К. Задірака, Н.В. Кошкіна, О.С. Олексюк. Аналіз стійкості стеганографічних систем в моделі пасивного противника // Штучний інтелект. – 2004. - №3. – С. 801-805.
12. Андрущенко Д., Козина Г. Анализ стойкости метода Коха-Жао стеганографического встраивания информации в статические изображения // Правове, нормативне та метрологічне забезпечення систем захисту інформації в Україні. – 2008. – В.2. - №17. – С. 70-74.

13. Kaufman C., Perlman R., Speciner M. Network security: private communication in a public world. – Upper Saddle River: Prentice Hall Press, 2002. – 752 p.
14. Зубов А. Совершенные шифры. - М.: Гелиос АРВ, 2003. – 160 с.
15. Галицкий А.В., Рябко С.Д., Шаньгин В.Ф. Защита информации в сети – анализ технологий и синтез решений. – М.: ДМК Пресс, 2004. – 616 с.
16. Грибунин В.Г. Цифровая стеганография. – М.: СОЛОН-Пресс. – 2002. – 261 с.
17. Большаков И.А. Тезаурус в системах подготовки текстов: каким ему быть? // Междунар. форум по информ. и джум. – 1991. – №2. – С. 31.
18. Westfeld A., Pfitzmann A. Attacks on steganographic systems. Breaking the steganographic utilities EzStego, Jsteg, Steganos, and S-Tools and some lessons learned // Proceeding of the Workshop on Information Hiding. - 1999.- P.49-57.
19. Алишов Н.И., Марченко В.А., Оруджева С.Г. Косвенная стеганография как новый способ защиты компьютерных данных // Комп'ютерні засоби, мережі та системи. – 2009.- № 8. - С. 105-112.
20. Matsumoto M., Kurita Y. Twisted GFSR generators // ACM Trans. Model. Comput. Simul. − 1992. − N 2. − P. 179−254.
21. Matsumoto M., Nishimura T. Mersenne twister: a 623-dimensionally equidistributed uniform pseudorandom number generator // ACM Trans. Model. Comput. Simul. −1999. − №8. − P. 3−17.
22. Rescorla E. Diffie-Hellman Key Agreement Method: RFC2631. – East Palo Alto, RTFM Inc., 1999. – 12 p.
23. Крамер Г. Математические методы статистики. – М.:Мир, 1975. – 326 с.
24. Abramowitz M., Stegun I. Handbook of mathematical functions. - Washington, D.C.: U.S. Government Printing Office, 1964. – P. 328.
25. Шеннон К. Теория связи в секретных системах. Работы по теории информации и кибернетике. – М.: Изд. иностр. лит., 1963. – С. 333 – 369.
26. Методичні рекомендації до виконання дипломної роботи з освітньо-кваліфікаційного рівня „магістр". Спеціальність „Комп'ютерні системи та мережі" / М.П.Карпінський, О.М.Березький, Р.Б.Трембач, Н.М.Васильків / Під. ред. М.П.Карпінського – Тернопіль: ТНЕУ, 2008. – 41 с.