

МІНІСТЕРСТВО ОСВІТИ ТА НАУКИ УКРАЇНИ
ОДЕСЬКИЙ НАЦІОНАЛЬНИЙ МОРСЬКИЙ УНІВЕРСИТЕТ

**Навчально-науковий інститут інформаційних технологій та
інноваційного підприємництва**

Кафедра кібербезпеки та захисту інформації

Конспект лекцій

з дисципліни

СТЕГАНОГРАФІЯ ТА СТЕГАНОАНАЛІЗ

(частина I)

для здобувачів

другого (магістерського) рівня вищої освіти
спеціальності F5 Кібербезпека та захист інформації
галузі знань F Інформаційні технології

Одеса-2025

Розробник: Кобозєва Алла Анатоліївна, доктор технічних наук, професор, завідувачка кафедри «Кібербезпека та захист інформації»

Конспект лекцій схвалено на засіданні кафедри «Кібербезпека та захист інформації»

(Протокол від «06» жовтня 2025 р. № 2)

Конспект лекцій схвалено на засіданні НМК ННІ ІТІП

(Протокол від «14» жовтня 2025 р. № 2)

ЗМІСТ

ВСТУП	4
Тема 1. ЦИФРОВА СТЕГАНОГРАФІЯ. ВИМОГИ ДО СТЕГАНОГРАФІЧНОЇ СИСТЕМИ	6
Тема 2. ЗАГАЛЬНИЙ ПІДХІД ДО ОЦІНКИ І ПОРІВНЯННЯ ВЛАСТИВОСТЕЙ СТЕГАНОГРАФІЧНИХ АЛГОРИТМІВ	23
Тема 3. МЕТОД ПІДВИЩЕННЯ СТІЙКОСТІ СТЕГАНОАЛГОРИТМУ ДО АТАК ПРОТИ ВБУДОВАНОГО ПОВІДОМЛЕННЯ	34
Література	44

ВСТУП

У сучасному цифровому просторі інформаційна безпека підприємств, критичної інфраструктури та державних систем тривалий час розглядалася переважно крізь призму криптографічного захисту. Проте суперечливість традиційних криптографічних підходів полягає в тому, що сам факт наявності зашифрованого контенту неминуче привертає увагу потенційного зломисника, збільшує ефективність його атак. У цих умовах принципового значення набуває комп'ютерна стеганографія - наука про прихований зв'язок, яка забезпечує непомітність самого факту передачі конфіденційних даних шляхом їх маскуванню всередині легітимних цифрових контейнерів (зображень, аудіо- та відео потоків тощо).

Зворотним і не менш критичним боком цієї медалі є стеганоаналіз - галузь, що досліджує методи виявлення присутності прихованих повідомлень, оцінки їх обсягу та локалізації. Для фахівців з кібербезпеки володіння цими знаннями є життєво необхідним, оскільки приховані канали зв'язку сьогодні активно використовуються внутрішніми порушниками для організації несанкціонованого витоку даних, управління шкідливим програмним забезпеченням тощо.

Метою дисципліни «Стеганографія та стеганоаналіз» є забезпечення розвитку фахових компетентностей майбутніх магістрів шляхом оволодіння сучасними підходами до вирішення проблем стеганографії та стеганоаналізу, зокрема шляхом застосування та розвитку загального підходу до аналізу стану й технології функціонування захищених інформаційних систем, розробленому та безперервно удосконалюваному фахівцями кафедри «Кібербезпека та захист інформації» ОНМУ, набуття практичних навичок застосування стеганографічних та стеганоаналітичних методів в практичній діяльності.

Завданнями, що мають бути вирішеними у процесі викладання дисципліни, є формування у здобувачів теоретичного базису для розв'язку задач організації та виявлення прихованого каналу зв'язку, набуття практичних навичок застосування, розробки, удосконалення сучасних стеганографічних та стеганоаналітичних методів та алгоритмів з використанням інформаційних технологій, математичних методів.

Загальні компетентності:

КЗ-1. Здатність застосовувати знання у практичних ситуаціях.

КЗ-2. Здатність проводити дослідження на відповідному рівні.

Фахові компетентності:

КФ1. Здатність обґрунтовано застосовувати, інтегрувати, розробляти та удосконалювати сучасні інформаційні технології, фізичні та математичні моделі, а також технології створення та використання прикладного і спеціалізованого програмного забезпечення для вирішення професійних задач у сфері інформаційної безпеки та/або кібербезпеки..

Вивчення освітнього компонента (навчальної дисципліни) передбачає здобуття таких **результатів навчання**:

РН4. Застосовувати, інтегрувати, розробляти, впроваджувати та удосконалювати сучасні інформаційні технології, фізичні та математичні методи і моделі в сфері інформаційної безпеки та/або кібербезпеки.

РН21. Використовувати методи натурного, фізичного і комп'ютерного моделювання для дослідження процесів, які стосуються інформаційної безпеки та/або кібербезпеки.

РН22. Планувати та виконувати експериментальні і теоретичні дослідження, висувати і перевіряти гіпотези, обирати для цього придатні методи та інструменти, здійснювати статистичну обробку даних, оцінювати достовірність результатів досліджень, аргументувати висновки.

Тема 1. ЦИФРОВА СТЕГАНОГРАФІЯ. ВИМОГИ ДО СТЕГАНОГРАФІЧНОЇ СИСТЕМИ

План

1. Цифрова стеганографія. Предмет, термінологія, області застосування.
2. Структурна схема стеганосистеми. Класифікація стеганосистем.
3. Атаки на стеганосистеми
4. Пропускна спроможність каналів передачі приховуваної інформації
5. Поняття стійкості стеганосистеми
6. Загальні вимоги до стеганографічної системи.
7. Метод модифікації найменшого значущого біта як найпоширеніший стеганографічний метод.
8. Особливості й переваги використання частотної області контейнера для стеганоперетворення. Метод Коха і Жао.
9. Поняття та актуальність селективної стеганографії.

1. Цифрова стеганографія. Предмет, термінологія, області застосування

Завдання захисту інформації від несанкціонованого доступу вирішувалося за всіх часів протягом історії людства. Уже в прадавньому світі виділилося два основні напрямки розв'язку цього завдання, що існують і по сьогоднішній день: криптографія й стеганографія. Метою криптографії є приховання вмісту повідомлень за рахунок їх шифрування. На відміну від цього, при стеганографії приховується сам факт існування таємного повідомлення.

Слово «стеганографія» має грецьке коріння й буквально означає «тайнопис». Історично цей напрямок з'явився першим, але потім був витиснутий криптографією. Тайнопис здійснюється всілякими способами. Загальною рисою цих способів є те, що приховуване повідомлення або додаткова інформація (ДІ) вбудовується в деякий об'єкт, що не привертає увагу, який далі називається контейнером, або основним повідомленням (ОП). Результат такого вбудовування будемо називати стеганоповідомленням (СП), а сам процес вбудовування - стеганоперетворенням (СПр) контейнера. Потім стеганоповідомлення відкрито транспортується адресатові або зберігається в отриманому виді.

При використанні криптографії наявність шифрованого повідомлення сама по собі привертає увагу супротивників, при використанні стеганографії ж наявність прихованого зв'язку залишається непомітною.

Згідно із принципом Кергоффа, система захисту інформації повинна забезпечувати свої функції навіть при повній поінформованості супротивника про її структуру й алгоритмах функціонування; Уся таємність системи захисту переданих відомостей повинна полягати в ключі, тобто в попередньо (як правило) розділеному між адресатами фрагменті інформації.

Стеганографія - це наука, яка вивчає способи й методи приховування конфіденційної інформації, основною задачею якої є приховування самого факту існування секретних даних при їхній передачі, зберіганні або обробці. Під прихованням існування інформації мається на увазі не тільки неможливість виявлення в перехопленому повідомленні наявності іншого (прихованого) повідомлення, але й взагалі неможливість виникнення будь-яких підозр на цей рахунок.

Розвиток засобів обчислювальної техніки в останнє десятиліття дав новий поштовх для розвитку *комп'ютерної стеганографії*. З'явилося багато нових областей застосування. Повідомлення вбудовують тепер у цифрові дані, які, як правило, мають аналогову природу. Це - аудіо, зображення, відео. Відомі також пропозиції по вбудовуванню інформації в текстові файли й в файли програм.

Існують два основні напрямки в комп'ютерній стеганографії: пов'язаний із цифровою обробкою сигналів і не пов'язаний. В останньому випадку повідомлення можуть бути вбудовані в заголовки файлів, заголовки пакетів даних. Цей напрямок має обмежене застосування у зв'язку з відносною легкістю розкриття й/або знищення прихованої інформації. Більшість поточних досліджень в області стеганографії так чи інакше пов'язані із цифровою обробкою сигналів. Це дозволяє говорити про цифрову стеганографію, яка й розглядається далі.

Розвиток стеганографії сьогодні відбувається стрімко й багатогранно. Можна виділити дві причини популярності досліджень в області стеганографії в цей час: обмеження на використання криптозасобів у ряді країн світу (у тому числі, в Україні) і поява проблеми захисту прав власності на інформацію, представлену в цифровому виді. Перша причина спричинила велику кількість досліджень у дусі класичної стеганографії (тобто приховування факту передачі інформації), друга - ще більш численні роботи в області так званих водяних знаків. *Цифровий водяний знак* (ЦВЗ) – спеціальна мітка, впроваджувана в зображення або інший цифровий сигнал з метою тим або іншим способом контролювати його використання.

Для конкретності далі будемо розглядати цифрові зображення (ЦЗ).

Цифрова стеганографія як наука народилася буквально в останні роки; Як відносно молода наука вона ще не має загально визнаної класифікації й навіть термінології, Однак можна запропонувати наступну класифікацію напрямків, які містить у собі стеганографія:

- вбудовування інформації з метою її прихованої передачі (класична стеганографія);
- вбудовування цифрових водяних знаків (watermarking);
- вбудовування ідентифікаційних номерів (fingerprinting) - «відбитків пальців»;
- вбудовування заголовків (captioning).

Класична стеганографія зазвичай спрямована на організацію прихованого каналу зв'язку в каналі загального користування й до недавнього часу залучала до себе основну увагу фахівців. Однак на сьогоднішній день у зв'язку з бурхливим розвитком інформаційних технологій, комп'ютерної техніки, використовуваної повсюдно, переводу левинної частки інформації в цифрову форму акценти трохи змістилися, принаймні, як можна судити по публікаціях у відкритій пресі: основна увага приділяється другому з перерахованих напрямків стеганографії.

ЦВЗ можуть застосовуватися, в основному, для захисту від копіювання й несанкціонованого використання. У зв'язку з розвитком технологій мультимедіа гостро встало питання захисту авторських прав і інтелектуальної власності, представленої в цифровому виді. Прикладами можуть бути фото, аудіо й відеозаписи й т.д. Переваги, які дають представлення й передача повідомлень у цифровому виді, можуть виявитися перекресленими легкістю, з якої можливо їх злодійство або модифікація. Тому розробляються різні заходи захисту інформації, організаційного й технічного характеру. Один з найбільш ефективних технічних засобів захисту мультимедійної інформації й полягає у вбудовуванні в об'єкт, що захищається, невидимих (видимих) міток - ЦВЗ. Розробки в цій області ведуть в усьому світі. Оскільки методи ЦВЗ почали розроблятися зовсім недавно (першою статтею на цю тему була, очевидно, робота 1989 р.), то тут є багато неясних проблем, що вимагають свого рішення. Назву ці методи отримали від усім відомого способу захисту цінних паперів, у тому числі й грошей, від підробки. Невидимі ЦВЗ аналізуються спеціальним декодером, який виносить рішення про їхню коректність. ЦВЗ можуть містити деякий автентичний код, інформацію про власника, або яку-небудь керуючу інформацію. Найбільш підходящими об'єктами захисту за допомогою ЦВЗ є нерухомі зображення, файли аудіо й відеоданих.

Технологія вбудовування ідентифікаційних номерів виробників має багато спільного з технологією ЦВЗ. Відмінність полягає в тому, що в першому випадку кожна захищена копія має свій унікальний номер, що вбудовується (звідси й назва - дослівно «відбитки пальців»). Цей ідентифікаційний номер дозволяє виробникові відслідковувати подальшу долю свого дітища: чи не зайнявся хто-небудь із покупців незаконним тиражуванням. Якщо так, то «відбитки пальців» швидко вкажуть на винного.

Вбудовування заголовків (невидиме) може застосовуватися, наприклад, для підпису медичних знімків, нанесення легенди на карту й т.д. Метою є зберігання різноманітної представленої інформації в єдиному цілому. Це, мабуть, єдине застосування стеганографії, де в явному виді відсутній потенційний порушник.

Двома основними вимогами до стеганоперетворення є:

- непомітність - надійність сприйняття стеганоповідомлення;
- стійкість до різного роду спотворень.

Слово «непомітність» має на увазі обов'язкове включення людини в систему стеганографічної передачі даних. Людина тут може розглядатися як додатковий приймач даних, що пред'являє до системи передачі вимоги, що досить важко формалізувати.

Якими б не були різними напрямки стеганографії, пропоновані ними вимоги багато в чому співпадають. Найбільш істотна відмінність постановки завдання прихованої передачі даних від постановки завдання вбудовування ЦВЗ полягає в тому, що в першому випадку порушник повинен виявити приховане повідомлення, тоді як у другому випадку про його існування, частіше за все, знають.

2. Структурна схема стеганосистеми

Завдання вбудовування й виділення повідомлень із іншої інформації виконує стеганосистема, яка, як правило, складається з наступних основних елементів, представлених на рис.1.1:

- попередній кодер - пристрій, призначене для перетворення приховуваного повідомлення (конфіденційної інформації (КІ), ЦВЗ) до виду, зручного для вбудовування в контейнер;
- кодер - пристрій, призначене для здійснення вкладення додаткової інформації в контейнер з урахуванням його моделі (його особливостей);
- пристрій виділення вбудованого повідомлення;
- детектор – пристрій, призначений для визначення наявності вкладки ДІ;
- декодер – пристрій, що відновлює конфіденційну інформацію. Цей вузол може бути відсутнім.

Дані, що містять приховане повідомлення, можуть піддаватися навмисним атакам або випадковим перешкодам, зокрема, у каналі атаки.

Перш, ніж здійснити вкладення КІ, ЦВЗ у контейнер, КІ (ЦВЗ) повинна бути перетворена до деякого підходящого виду, наприклад, якщо в якості контейнера виступає зображення, то й перетворена в попередньому кодері КІ (ЦВЗ) найчастіше представляється як двовимірний масив біт. Обробка в попередньому кодері виконується з використанням ключа K для забезпечення таємності вбудовування. Результатом попереднього кодування є додаткова інформація, що представляє із себе, як правило (але не обов'язково), бітову послідовність. Далі ДІ «вбудовується» у контейнер, наприклад, шляхом модифікації молодших значущих біт значень яскравості пікселів (у випадку цифрового зображення-контейнера). Цей процес можливий завдяки

особливостям системи сприйняття людини: добре відомо, що зображення мають велику психовізуальну надлишковість; око людини подібне низькочастотному фільтру, що пропускає дрібні деталі. Особливо непомітні спотворення у високочастотній області зображень. Ці особливості людського зору використовуються, наприклад, при розробці алгоритмів стиску зображень і відео.

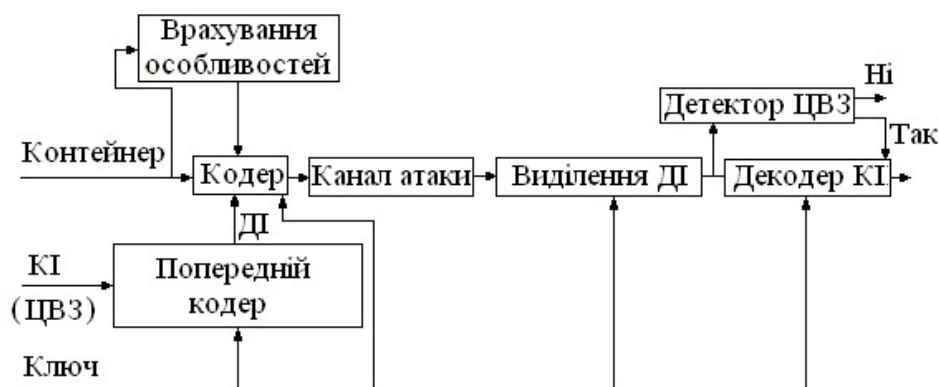


Рис.1.1 – Схема типової стеганосистеми

Процес вбудови ДІ також повинен урахувати властивості системи сприйняття людини. Стеганографія використовує наявну в сигналах психовізуальну надлишковість, але іншим, чим при стиску даних, образом. Наведемо простий приклад. Розглянемо півтонове зображення з 256 градаціями сірого. Добре відомо, що око людини не здатне помітити зміну молодшого значущого біта. Ще в 1989 році був отриманий патент на спосіб прихованого вкладення інформації в зображення шляхом модифікації молодшого значущого біта – LSB-метод. У цьому випадку детектор стего аналізує тільки значення цього біта для кожного пікселя, а око людини, навпаки, сприймає тільки старші 7 біт. Хоча даний метод простий у реалізації й ефективний, він не задовольняє деяким важливим вимогам, зокрема не забезпечує стійкість до атак проти вбудованого повідомлення.

У стегодетекторі відбувається виявлення ДІ в можливо зміненому зображенні. Ця зміна може бути обумовлена впливом помилок у каналі зв'язку, операцій обробки сигналу, навмисних атак порушників.

3. Класифікація стеганосистем

Залежно від того, яка інформація потрібна детектору для виявлення ДІ, стеганосистеми розподіляються на три класи:

- відкриті,
- напівзакриті,
- закриті.

Ця класифікація наведена в табл.1.1.

Табл.1.1. Класифікація стеганосистем

Клас стеганосистеми		Що потрібно детектору		Вихід детектора	
		Вхідний сигнал	Вхідна ДІ	Так/ні	ДІ
Закриті	Тип I	+	+	+	-
	Тип II	+	-	-	+
Напівзакриті		-	+	+	-
Відкриті		-	-	-	+

Найбільше застосування мають відкриті стеганосистеми. Найбільшу стійкість стосовно зовнішніх впливів - закриті стеганосистеми I типу.

Класифікація стеганосистем потребує конкретизації поняття й типів контейнера. До кодера (рис.1.1) – це порожній контейнер, після нього – заповнений контейнер, або стеганоповідомлення (СП). СП повинно візуально не відрізнятися від порожнього контейнера при організації прихованого каналу зв'язку.

Розрізняють два основні типи контейнерів: *потоківий* і *фіксований*.

Потоковий контейнер являє собою послідовність біт, що безперервно подається; повідомлення вкладається в нього в реальному масштабі часу, так що в кодері невідомо заздалегідь, чи вистачить розмірів контейнера для передачі всього повідомлення. В один контейнер великого розміру може бути вбудовано й кілька повідомлень. Потоківий контейнер має велике практичне значення: наприклад, стегоприставка до звичайного телефону: під прикриттям звичайного, незначного телефонного переговорів можна передавати іншу розмову, дані й інше, і, не знаючи секретного ключа, не можна не тільки довідатися про зміст прихованої передачі, але й сам факт її існування. Не випадково, що робіт, присвячених розробці стеганосистем з потоковим контейнером практично не зустрічається у відкритій пресі.

У *фіксованого* контейнера розміри й характеристики заздалегідь відомі, що дозволяє здійснювати вкладення даних оптимальним у деякому сенсі образом.

Контейнер може бути *обраним*, *випадковим* або *нав'язаним*. *Обраний контейнер* залежить від повідомлення, що вбудовується, а в граничному випадку є його функцією. Цей тип контейнера більше характерний для класичної стеганографії. *Нав'язаний контейнер* може з'явитися в сценарії, коли особа, що

надає контейнер, підозрює про можливу приховану переписку й бажає запобігти їй. На практиці ж найчастіше зустрічаються з *випадковим* контейнером.

Вбудовування повідомлення в контейнер проводиться з використанням ключа, одного або декількох. Приховувана інформація, як правило, вбудовується відповідно до ключа в ті відліки, спотворення яких не приводить до істотних спотворень контейнера. Ці відліки утворюють *стеганопуть*. Залежно від області застосування під істотним спотворенням можна розуміти спотворення, що приводить як до неприйнятності для людини-адресата заповненого контейнера, так і до можливості виявлення факту наявності прихованого повідомлення після стеганоаналізу.

Захист цифрового контейнера від його несанкціонованого використання доцільно проводити з використанням ЦВЗ, які можуть бути трьох типів: робастні, хрупкі й напівхрупкі (*semifragile*), і використовуються залежно від переслідуваної мети.

Під робастністю ЦВЗ розуміється його стійкість до різного роду збурних дій на СП. Більшість досліджень у цьому напрямку стеганографії присвячено робастним ЦВЗ.

Хрупкі ЦВЗ руйнуються при незначній модифікації СП; вони застосовуються для автентифікації контейнера. Відмінність від засобів електронного цифрового підпису полягає в тому, що хрупкі ЦВЗ все-таки допускають деяку модифікацію контенту. Це важливо для захисту мультимедійної інформації, тому що законний користувач може, наприклад, побажати стиснути зображення. Інша відмінність від засобів електронного цифрового підпису полягає в тому, що хрупкі ЦВЗ повинні не тільки відобразити факт модифікації контейнера, але також вид і місце розташування цієї зміни, що робить їх кращими в умовах автентифікації контейнера.

Напівхрупкі ЦВЗ стійкі стосовно одних збурних дій і нестійкі стосовно інших. Загалом кажучи, усі ЦВЗ можуть бути віднесені до цього типу. Однак напівхрупкі ЦВЗ спеціально проектує так, щоб бути нестійкими стосовно певного роду операцій. Наприклад, вони можуть дозволяти виконувати стиск зображення, але забороняти вирізку з нього або вставку в нього фрагмента.

4. Атаки на стеганосистеми

Стеганосистема утворює стеганоканал, по якому передається СП. Цей канал вважається підданим впливам з боку порушників. У стеганографії зазвичай розглядається така постановка завдання («проблема ув'язнених»). Двоє ув'язнених, Аліса й Боб, бажають конфіденційно обмінюватися повідомленнями, не зважаючи на те, що канал зв'язку між ними контролює охоронець Віллі. Для того, щоб таємний обмін повідомленнями був можливий, передбачається, що Аліса й Боб мають деякий відомий обом секретний ключ. Дії Віллі можуть полягати не тільки в спробі виявлення прихованого каналу зв'язку, але й у руйнуванні переданих повідомлень, а також їх модифікації й створенні нових, хибних повідомлень. Відповідно, можна виділити три типи порушників, яким повинна протистояти стеганосистема: *пасивний, активний і злочинний порушники*.

1. *Пасивний порушник* може лише виявити факт наявності стегоканалу й (можливо) читати повідомлення. Чи зможе він прочитати повідомлення після його виявлення залежить від стійкості системи шифрування, і це питання, як правило, не розглядається в стеганографії. Якщо в порушника є можливість виявити факт наявності прихованого каналу передачі повідомлень, то стеганосистема зазвичай вважається нестійкою. Хоча існують і інші точки зору на стійкість стеганосистем. Здійснення виявлення стеганоканалу є найбільш трудомістким завданням, а захист від виявлення вважається основним завданням стеганографії за визначенням.
2. Діапазон дій *активного порушника* значно ширше. Приховане повідомлення може бути їм вилучене або зруйноване. У цьому випадку адресат, можливо, довідається про факт втручання. У більшості випадків це суперечить інтересам порушника (наприклад, за юридичними мотивами). Інша справа - видалення або руйнування цифрового водяного знака, які можуть розглядатися як основні погрози в цій області.
3. Дії *злочинного порушника* найнебезпечніші. Він здатний не тільки руйнувати, але й створювати хибні СП. Історія протистояння розвідки й контррозвідки знає чимало прикладів, коли реалізація цієї погрози приводила до катастрофічних наслідків. Ця погроза актуальна й стосовно систем ЦВЗ. Володіючи здатністю створювати водяні знаки, порушник може створювати копії контенту, що захищається, створювати хибні оригінали й т.д.

Для здійснення тієї або іншої погрози порушник застосовує атаки.

Найбільш проста атака - *суб'єктивна*. Порушник уважно розглядає зображення (слухає аудіозапис), намагаючись визначити “на око”, чи є в ньому приховане повідомлення. Ясно, що подібна атака може бути проведена лише проти зовсім незахищених стеганосистем, проте, вона найпоширеніша на практиці, принаймні, на початковому етапі розкриття стеганосистеми.

Для більшості сучасних методів, які використовуються для приховання повідомлень у файлах цифрового формату при організації прихованого каналу зв'язку, має місце залежність надійності сприйняття СП від обсягу даних, що вбудовуються, представлена на рис.1.2, де очевидним є той факт, що збільшення обсягу даних, що вбудовуються, значно знижує надійність сприйняття СП.

Надійність сприйняття - суб'єктивна характеристика: спотворення контейнера за рахунок вбудови ДІ не повинне бути помітно людині. Таким чином, у систему стеганографічної передачі даних включається людина, що вносить додаткові, неподоланні до цього моменту труднощі у процес математичної формалізації забезпечення розглянутої вимоги, хоча робота в цьому напрямку ведеться дуже активно, із залученням великого математичного апарата.



Рис.1.2. Взаємозв'язок між надійністю сприйняття стегоповідомлення й обсягом приховуваного повідомлення при незмінному розмірі контейнера

Нехай у якості контейнера розглядається зображення в градаціях сірого, $n \times n$ -матриця якого позначається F . Вбудову ДІ в контейнер, незалежно від способу й області цієї вбудови, можна представити як збурення ΔF поданої матриці F . Матриця стегоповідомлення $\bar{F}$ очевидно задовольняє співвідношенню:

$$\bar{F} = F + \Delta F, \text{ де } \Delta F = f(F), \quad (1.1)$$

тобто ΔF є деякою функцією F .

Будь-які перетворення, які проводяться над СП при його транспортуванні або зберіганні, включаючи активні атакуючі дії, будемо розглядати як додаткові збурення матриці контейнера F .

Дотепер при аналізі рівня візуальних спотворень, які вносяться в контейнер при стегоперетворенні, широко застосовуються різницеві показники, що ґрунтуються на різних модифікаціях відношення «сигнал-шум»:

Різницеві показники рівня візуальних спотворень ЦЗ:

- відношення «сигнал-шум»: $SNR = \frac{\|F\|_F^2}{\|\Delta F\|_F^2}$;
- максимальне (пікове) відношення «сигнал-шум»: $PSNR = \frac{n^2 \max_{i,j} f_{ij}^2}{\|\Delta F\|_F^2}$;
- якість зображення: $IF = 1 - \frac{\|\Delta F\|_F^2}{\|F\|_F^2}$,

де $\|\bullet\|_F$ - матрична норма Фробеніуса ($\|F\|_F = \sqrt{\sum_{i,j=1}^n f_{ij}^2}$), хоча слабкі місця таких показників давно відомі

(наприклад, відсутність кореляції цих показників із зором людини). Як видно з наведеного на рис.1.3 ілюстративного прикладу, пікове відношення «сигнал-шум» PSNR може бути значним, але при цьому відбувається явне порушення надійності сприйняття (рис.1.3 (б)), а при набагато меншому значенні PSNR видимі зміни на ЦЗ не спостерігаються.

Широке використання різницевих показників спотворення ЦЗ пояснюється тим, що всі існуючі моделі зорового сприйняття є лише частковим і обмеженим відображенням зорової системи людини в силу її складності, а показники спотворення, засновані на таких моделях, інформація про які доступна з відкритих джерел, усе ще залишаються недосконалими й досить складними в реалізації.



Рис.1.3. Ілюстрація недосконалості різницевих показників для оцінки візуальних спотворень ЦЗ: а - вхідне ЦЗ, б - спотворене ЦЗ ($PSNR = 48 \text{ dB}$), в – спотворене за допомогою гауссівського шуму ЦЗ ($PSNR = 28 \text{ dB}$)

Оскільки стегаперетворення контейнера, а також збурні дії, які зазнає стегаповідомлення, повинні забезпечувати надійність його сприйняття, то $\|\Delta F\|$ не може бути нескінченно великою (де ΔF - матриця збурення контейнера або СП), оскільки у цьому випадку достовірною подією виявиться порушення висунутої вимоги. Крім того, при $\|\Delta F\| \rightarrow 0$ імовірність забезпечення надійності сприйняття для СП буде прямувати до одиниці для кожного контейнера. Значення згаданих вище різницевих показників для заданого зображення F визначаються $\|\Delta F\|_F$: чим менше $\|\Delta F\|_F$, тим краще кількісний показник візуального спотворення F для кожного з них. Враховуючи це, далі будемо вважати, що, чим менше $\|\Delta F\|_F$, тим більше ймовірність забезпечення надійності сприйняття для зображення з матрицею $F + \Delta F$ при заданому вхідному ЦЗ F .

Таким чином, для забезпеченні досить високої ймовірності збереження надійності сприйняття стегаповідомлення при заданому контейнері стегаметод повинен забезпечувати малу норму (зокрема, Фробеніуса) матриці збурення при стегаперетворенні.

Суб'єктивна атака, будучи однією з найпоширеніших стегаграфічних атак, не єдина. За аналогією із криптоаналізом у стегаграфії можна виділити наступні атаки:

- *Атака на основі відомого заповненого контейнера.* У цьому випадку в порушника є одне або декілька СП. В останньому випадку передбачається, що вбудова приховуваної інформації здійснювалося одним способом. Завдання порушника може полягати у виявленні факту наявності стегаканалу (основна), а також у його декодуванні або визначенні ключа. Знаючи ключ, порушник одержить можливість аналізу інших стегаповідомлень.
- *Атака на основі відомого вбудованого повідомлення.* Цей тип атаки більшою мірою характерний для систем захисту інтелектуальної власності, коли в якості водяного знака використовується відомий логотип фірми. Завданням аналізу є отримання ключа. Якщо відповідний до прихованого повідомлення заповнений контейнер невідомий, то завдання розв'язується вкрай важко.
- *Атака на основі обраного прихованого повідомлення.* У цьому випадку порушник має можливість пропонувати для передачі свої повідомлення й аналізувати СП, які виходять.
- *Атака на основі обраного заповненого контейнера.* Цей тип атаки більше характерний для систем ЦВЗ. Стегааналітик має детектор СП у вигляді «чорного ящика» і декілька СП. Аналізуючи детектовані приховані повідомлення, порушник намагається розкрити ключ.

У порушника може бути можливість застосувати ще три атаки, що не мають прямих аналогій у криптоаналізі:

- *Атака на основі відомого порожнього контейнера.* Якщо він відомий порушникові, то шляхом порівняння його з передбачуваним СП він завжди може встановити факт наявності стеганоканалу. Незважаючи на тривіальність цього випадку, у ряді робіт приводиться його інформаційно-теоретичне обґрунтування. Набагато цікавіше сценарій, коли контейнер відомий приблизно, з деякою похибкою (як це може мати місце при додаванні до нього шуму).
- *Атака на основі обраного порожнього контейнера.* У цьому випадку порушник здатний змусити користуватися запропонованим їм контейнером. Наприклад, запропонований контейнер може мати великі однорідні області (однотонні зображення), і тоді буде важко забезпечити таємність вбудови.
- *Атака на основі відомої математичної моделі контейнера або його частини.* При цьому атакуючий намагається визначити відмінність підозрілого повідомлення від відомої йому моделі. Наприклад, припустимо, що біти усередині зображення корельовані. Тоді відсутність такої кореляції може служити сигналом про наявне приховане повідомлення. Завдання того, хто вбудовує повідомлення, полягає в тому, щоб не порушити статистики контейнера. Ті, хто вбудовує ДІ, і атакує, можуть мати у своєму розпорядженні різні моделі сигналів, тоді у протистоянні переможе той, хто має кращу модель.

Розглянуті вище атаки мають одну особливість: вони не змінюють стеганоповідомлення. У цьому полягає їхня позитивна сторона: дії порушника навряд чи здатні насторожити відправника й одержувача.

Атаки іншого типу - це *атаки проти вбудованого повідомлення*, які змінюють стеганоповідомлення, а значить можуть змінити й вбудовану в контейнер інформацію. Однією з таких атак є атака, заснована на застосуванні алгоритму стиску Jpeg до СП. Однак набагато більше представлення про переваги того або іншого стеганоалгоритму можна одержати, комплексно використовуючи різні атаки. Загальнодоступна в Інтернеті програма Stirmark дозволяє більш повно аналізувати робастність (стійкість) стегоалгоритмів.

Геометричні атаки - найнебезпечніші на сьогоднішній день, вони змінюють стеганоповідомлення шляхом внесення просторових або часових спотворень, також будучи атаками проти вбудованого повідомлення. Геометричні атаки математично моделюються як афінні перетворення з невідомим декодеру параметром. Афінні перетворення: масштабування, зміна пропорцій, повороти, зсув й усікання. Ці атаки приводять до втрати синхронізації в детекторі ДІ й можуть бути локальними або глобальними (тобто застосованими до всього сигналу). При цьому можливо вирізання окремих пікселів або рядків, перестановка їх місцями, застосування якихось перетворень і т.д. Подібні атаки реалізовані в програмах Unsign (локальні атаки) і Stirmark (локальні й глобальні атаки).

Перераховані стеганографічні атаки не вичерпують усього їх різноманіття, будучи найбільше широко й часто використовуваними.

5. Пропускна спроможність каналів передачі прихованої інформації

Для стеганографічних систем важливо визначити, наскільки великою може бути пропускна спроможність каналів передачі приховуваних повідомлень, і як вона залежить від інших характеристик стеганосистем і умов їх використання. Неформально визначимо, що під *пропускною спроможністю* каналів передачі приховуваних повідомлень або просто пропускною спроможністю прихованого каналу зв'язку (ПСПК) будемо розуміти максимальну кількість інформації, яка може бути вкладена в один елемент контейнера. При цьому приховувані повідомлення повинні бути безпомилково передані одержувачеві й захищені від атак порушника, таких як спроби виявлення факту наявності каналу прихованому зв'язку, читання приховуваних повідомлень, навмисного введення хибних повідомлень або руйнування вбудованої в контейнер інформації. Канал прихованого зв'язку утворюється усередині каналу відкритого зв'язку (каналу загального користування). Пропускна спроможність каналу відкритому зв'язку визначається як кількість інформації, яку потенційно можна передати без помилок за одне використання каналу. При цьому не пред'являється ніяких вимог до захищеності від атак організованого порушника. Тому логічно припустити, що ПСПК повинна бути менше пропускної спроможності каналу відкритого зв'язку, у якому за одне використання каналу передається один елемент контейнера, у який вкладена приховувана інформація.

6. Поняття стійкості стеганосистеми

У порівнянні з достатньо добре дослідженими криптографічними системами, поняття й оцінки безпеки стеганографічних систем більш складні й допускають більше число їх тлумачень. Зокрема, це пояснюється як недостатнім теоретичним і практичним проробленням питання безпеки стеганосистем, так і великою різноманітністю завдань стеганографічного захисту інформації. Стеганосистеми водяних знаків, зокрема, повинні виконувати завдання захисту авторських і майнових прав на електронні повідомлення при різних спробах активного порушника спотворення або стирання вбудованої в них автентифікуючої інформації. Формально говорячи, системи ЦВЗ повинні забезпечити автентифікацію відправників електронних повідомлень. Подібне завдання може бути покладеном на криптографічні системи електронного цифрового підпису (ЕЦП) даних, але на відміну від стеганосистем водяних знаків, відомі системи ЕЦП не забезпечують захист авторства не тільки цифрових, але й аналогових повідомлень, і в умовах, коли активний порушник вносить спотворення в повідомлення, що захищається, й автентифікуючу інформацію. Інші вимоги по безпеці пред'являються до стеганосистем, призначених для приховання факту передачі конфіденційних повідомлень від пасивного порушника.

Як і для криптографічних систем захисту інформації, безпека стеганосистем описується й оцінюється їхньою стійкістю (стеганографічною стійкістю або для стислості стеганостійкістю). Під *стійкістю* різних стеганосистем розуміється їхня здатність приховувати від кваліфікованого порушника факт прихованої

передачі повідомлень, здатність протистояти спробам порушника зруйнувати, спотворити, вилучити потай передані повідомлення, а також здатність підтвердити або спростувати автентичність потай переданої інформації.

Дослідимо стегосистеми, завданням яких є прихована передача інформації. У криптографічних системах ховається зміст конфіденційного повідомлення від порушника, у той час як у стеганографії додатково ховається факт існування такого повідомлення. Тому визначення стійкості й злому цих систем різні. У криптографії система захисту інформації є стійкою, якщо, маючи перехоплену криптограму, порушник не здатний читати повідомлення, що міститься в ній. Неформально визначимо, що *стеганосистема є стійкою, якщо порушник, спостерігаючи інформаційний обмін між відправником і одержувачем, не здатний виявити, що під прикриттям контейнерів передаються приховувані повідомлення, і тим більше читати ці повідомлення.*

Назвемо в загальному випадку стеганосистему нестійкою, якщо протидіюча сторона здатна виявляти факт її використання.

Стійкість різних стеганосистем може бути розділена на:

- стійкість до виявлення факту передачі (існування) приховуваної інформації,
- стійкість до витягу приховуваної інформації,
- стійкість до нав'язування хибних повідомлень по каналу прихованого зв'язку (імітостійкість),
- стійкість до відновлення секретного ключа стегосистеми,
- стійкість до атак проти вбудованого повідомлення.

Очевидно, що якщо стеганосистема є стійкою до виявлення факту передачі (існування) приховуваної інформації, то логічно припустити, що вона при цьому є стійкою й до читання приховуваної інформації. Зворотне в загальному випадку невірно. Стеганосистема може бути стійкою до читання приховуваної інформації, але факт передачі інформації під прикриттям контейнера може виявлятися порушником.

Стійкість стеганосистеми до нав'язування хибних повідомлень по каналу прихованого зв'язку характеризує її здатність виявляти й відкидати сформовані порушником повідомлення, що вводяться їм у канал передачі приховуваних повідомлень із метою видачі їх за оригінальні, такі, що виходять від законного відправника. Якщо в системі ДІ зловмисник здатний увести в контейнер, завірений законним відправником, свій водяний знак, і детектор буде виявляти водяний знак зловмисника й не виявляти ЦВЗ дійсного відправника, то це означає дискредитацію (злом) системи ЦВЗ.

Стійкість до відновлення секретного ключа стеганосистеми характеризує її здатність протистояти спробам порушника обчислити секретну ключову інформацію даної стеганосистеми. Якщо порушник здатний визначити ключ стеганосистеми, то він може однозначно виявляти факти передачі приховуваних повідомлень і читати їх або нав'язувати хибні повідомлення без усяких обмежень. Таку подію можна назвати повною компрометацією стеганосистеми. Очевидно, що атаки порушника на ключ стеганосистеми можуть бути побудовані аналогічно атакам на ключ систем шифрування інформації й систем автентифікації повідомлень.

Якщо порушник здатний обчислити ключ вбудовування водяного знака якого-небудь автора (власника) інформаційних ресурсів, то він може поставити цей водяний знак на будь-який контейнер. Тим самим порушник дискредитує або водяний знак даного автора (власника), або цілком усю систему ЦВЗ. В обох випадках ставиться під сумнів законність прав одного або всіх власників інформаційних ресурсів на те, що дійсно їм належить.

Стійкість стеганосистеми до атак проти вбудованого повідомлення вже обговорювалася вище.

7. Загальні вимоги до стеганографічної системи

- Використовуване стеганоперетворення повинне гарантовано забезпечувати надійність сприйнятті стеганоповідомлення, що формується. Тут необхідно враховувати, що ймовірність виконання цієї вимоги буде тим вищою, чим менше збурення матриці цифрового зображення-контейнера в результаті вбудови додаткової інформації, тобто стеганометоди повинні проводити вбудову елементів додаткової інформації шляхом малих (якнайменших) збурень елементів контейнера;
- Стеганосистема має бути стійкою, в першу чергу, до виявлення, а також забезпечувати стійкість до витягу приховуваної інформації, імітостійкість, стійкість до відновлення секретного ключа стегосистеми;
- Стеганосистема має бути стійкою до атак проти вбудованого повідомлення. Тут необхідно враховувати, що для забезпечення нечутливості стеганоповідомлення до збурних дій збурення елементів контейнера при вбудові додаткової інформації має бути не менше збурень внаслідок атаки. Виходячи з цього, стеганографічні методи повинні проводити вбудову

елементів ДІ шляхом немалих (що перевершують очікувані в результаті атак) збурень елементів контейнера;

- При організації стеганографічного каналу зв'язку необхідно враховувати особливості машинної арифметики, а саме можливість (значного) накопичення обчислювальної похибки при роботі з дійсними числами, що спричинить зниження ефективності декодування додаткової інформації.;
- забезпечити можливість ефективної роботи при декодуванні додаткової інформації та перевірки її цілісності та автентичності як з наявністю, так і без контейнера. Це дасть можливість вибору того чи іншого способу реалізації стеганосистеми залежно від умов, у яких створюється прихований канал зв'язку, конкретних вимог щодо нього. Так, якщо критичним є забезпечення максимальної стійкості стеганосистеми до стеганоаналізу, то має сенс використовувати контейнер в якості додаткової складової частини секретного ключа. Якщо ж стеганосистема, що формується, знаходиться в умовах, коли стеганоаналітичні атаки на неї малоімовірні, то більш переважним буде використання «сліпого» стеганометода та його алгоритмічних реалізацій;
- З урахуванням значних розмірів сучасних цифрових контейнерів, зокрема зображень, а також для забезпечення перспективи використання стеганографічних методів у разі, коли в якості контейнера виступає відеопослідовність, у тому числі, для організації стеганоперетворення тут в режимі реального часу, необхідним є забезпечення малої обчислювальної складності;
- Існування потенційної можливості розпаралелювання використовуваних стеганометодів.

Одночасне забезпечення всіх вимог на практиці є малоімовірним, тому їх пріоритет обирається у відповідності з умовами використання стеганосистеми, що формується.

8. Метод модифікації найменшого значущого біта як найпоширеніший стеганографічний метод

Метод модифікації найменшого значущого біта (LSB — Least Significant Bit) є широко використовуваним методом сучасної стеганографії в просторовій області. Його суть полягає в заміні молодших бітів відліків цифрового сигналу-контейнера (зображення, аудіо чи відео) бітами секретного повідомлення. Оскільки молодший біт несе найменше інформаційне навантаження про інтенсивність кольору пікселя або амплітуду звукового сигналу, його зміна призводить до мінімальних спотворень, які практично не сприймаються органами чуття людини (зоровою або слуховою системою).

У цифрових зображеннях, де кожен колірний канал (R, G, B) зазвичай кодується 8 бітами (значення від 0 до 255), зміна молодшого біта змінює яскравість пікселя лише на 1 одиницю, що робить втручання візуально непомітним.

Однією з головних переваг методу LSB є його висока ємність (Capacity) — потенційна можливість забезпечення високої пропускнуєї спроможності прихованого каналу. Якщо ми використовуємо по одному молодшому біту в кожному з трьох каналів (RGB) зображення розміром 800*600, ми можемо

приховано передати 180000 байт інформації. Проте в професійній стеганографії рідко використовують повну ємність, оскільки заповнення всіх молодших бітів створює характерні статистичні аномалії, які легко виявляються методами стеганоаналізу.

Критичним недоліком класичного LSB є його вразливість до будь-якої атаки проти вбудованого повідомлення, зокрема спроба стиснення з втратами стеганоповідомлення (наприклад, збереження в JPEG), фільтрація або зміна розміру зображення призводить до знищення секретного повідомлення. Це робить метод LSB придатним лише для «стерильних» каналів зв'язку, де потенційно відсутні атаки проти вбудованого повідомлення.

З погляду стеганоаналізу, метод LSB вразливий до статистичних атак, що розглядається в наступних темах.

Для підвищення стійкості алгоритму до стеганоаналізу часто застосовують псевдовипадковий вибір пікселів для вбудовування. Замість послідовного запису від першого пікселя до останнього, використовується генератор псевдовипадкових чисел, ініціалізований секретним ключем. Це дозволяє «розсіяти» повідомлення по всьому контейнеру, знижуючи щільність локальних спотворень і ускладнюючи роботу стеганоаналітика, оскільки тепер він не знає точного порядку вкладення даних.

9. Особливості й переваги використання частотної області контейнера для стеганоперетворення. Метод Коха і Жао.

Забезпечення стійкості стеганографічного методу до різних атак - задача актуальна й нетривіальна. Складність забезпечення цієї стійкості залежить від того, яка область контейнера (просторова, частотна, іншого перетворення) використовується для вбудови ДІ. Забезпечити стійкість до атак проти вбудованого повідомлення в просторовій області ЦЗ-контейнера складніше, чим у частотній, хоча це жодним чином не означає, що неможливо забезпечити нечутливість стеганоповідомлення в просторовій області.

Існує кілька способів представлення ЦЗ у частотній області. При цьому використовується та чи інша декомпозиція ЦЗ-контейнера. Наприклад, існують методи на основі використання дискретного косинусного перетворення, дискретного перетворення Фур'є, вейвлет-перетворення та ін. Такі перетворення можуть застосовуватися чи до окремих частин ЦЗ, чи до зображення в цілому. Найбільше поширення серед таких перетворень в стеганографії отримали вейвлет-перетворення і ДКП, що певною мірою пояснюється їх застосуванням в алгоритмах стиску ЦЗ. Крім того, застосування при приховуванні даних саме того перетворення зображення, якому це зображення буде піддаватися під час можливої атаки, є доцільним, оскільки в такому випадку можливо врахувати всі особливості перетворення для підвищення ймовірності збереження ДІ. Наприклад, враховуючи, що алгоритм ДКП є базою в стандарті Jpeg, а вейвлет-перетворення – в Jpeg2000, доцільно при вбудові ДІ, якщо передбачається стиск ЦЗ-стеганоповідомлення алгоритмом Jpeg, використовувати область ДКП, а якщо стеганоповідомлення може піддатися атаці стиском з використанням Jpeg2000, то вбудову ДІ проводити саме в області дискретного вейвлет-перетворення. Зауважимо, що таке врахування специфіки можливих атак на стеганоповідомлення є

доцільним, є найбільш простим, але це не означає, що обов'язковим, тобто, наприклад, забезпечення стійкості стеганоалгоритму до стиску Jpeg може бути проведеним не тільки тоді, коли вбудова ДІ відбувається в області ДКП. Існує первна кількість стеганоалгоритмів, які проводять вбудову ДІ в просторовій області контейнера, в області сингулярного (спектрального) розкладання, але є стійкими до атак проти вбудованого повідомлення, зокрема до атаки стиском.

Відомо, що реальні ЦЗ не представляють собою випадкові процеси, більша частина енергії ЦЗ сконцентрована в низькочастотній складовій. Високочастотні складові ЦЗ найбільшим чином піддаються впливу з боку різноманітних алгоритмів обробки зображення, таких як стиск, низько-частотна фільтрація тощо. Таким чином, можна зробити висновок, що для вбудови ДІ найбільш прийнятною є середньо-частотна складова його спектру.

Розглянемо один зі стеганографічних методів, який позиціонується, як стійкий до незначних атак проти вбудованого повідомлення: метод відносної заміни величин коефіцієнтів дискретного косинусного перетворення (метод Коха й Жао) - це один з найпоширеніших на сьогодні методів приховання конфіденційної інформації в частотній області зображення, який полягає у відносній заміні величин коефіцієнтів дискретного косинусного перетворення (ДКП).

На початковому етапі первинне зображення стандартним чином розбивається на 8×8 -блоки. До кожного блоку, який будемо позначати В, застосовується ДКП, тим самим здійснюючи переведення кожного блоку із просторової в частотну область. У результаті виходить 8×8 -блок коефіцієнтів ДКП. Кожний блок призначено для приховання одного біта ДІ.

Існує дві реалізації алгоритму:

1. Для вбудови біта ДІ використовуються 2 коефіцієнта ДКП;
2. Для вбудови біта ДІ використовуються 3 коефіцієнта ДКП.

Розглянемо докладно перший варіант.

Під час організації прихованого каналу зв'язку абоненти повинні попередньо домовитися (зв'язатися по захищеному каналу зв'язку) про два конкретних коефіцієнта ДКП із кожного блоку, які будуть використовуватися для приховання даних. Задамо дані коефіцієнти їх індексами (u_1, v_1) і (u_2, v_2) в масивах коефіцієнтів ДКП:

$$\begin{bmatrix} (1,1) & \dots & (1,8) \\ \vdots & \dots & (u_1, v_1) & \dots & \vdots \\ \vdots & \dots & (u_2, v_2) & \dots & \vdots \\ (8,1) & \dots & & & (8,8) \end{bmatrix}.$$

Відмітимо, що зазначені індекси повинні відповідати середньочастотним коефіцієнтам ДКП, що забезпечить:

- Прихованість інформації;
- Вбудована інформація не буде спотворюватися при Jpeg-стиску зі значними коефіцієнтами якості (або, що те ж саме, з малими коефіцієнтами стиску).

На практиці найчастіше використовуються $(u_1, v_1) = (4, 5)$ і $(u_2, v_2) = (5, 4)$.

Нехай у процесі стеганоперетворення треба вбудувати черговий біт $b_k \in \{0, 1\}$ ДІ. Відповідно до секретного ключа для цього вибирається блок B ЦЗ-контейнера. Відповідний йому блок коефіцієнтів ДКП позначимо $B^{ДКП}$:

$$B^{ДКП} = \begin{bmatrix} b_{11}^{ДКП} & b_{12}^{ДКП} & \dots & b_{18}^{ДКП} \\ b_{21}^{ДКП} & b_{22}^{ДКП} & \dots & b_{28}^{ДКП} \\ \dots & \dots & \dots & \dots \\ b_{81}^{ДКП} & b_{82}^{ДКП} & \dots & b_{88}^{ДКП} \end{bmatrix}.$$

Для вбудови b_k використовуються коефіцієнти $b_{u_1, v_1}^{ДКП}$, $b_{u_2, v_2}^{ДКП}$. Вбудова біта b_k відбувається таким чином: якщо $b_k = 0$, то різниця абсолютних значень використовуваних для вбудовування коефіцієнтів ДКП роблять більше деякої заданої додатної величини P , а якщо $b_k = 1$, то ця різниця робиться менше $-P$:

$$\begin{cases} |b_{u_1, v_1}^{ДКП}| - |b_{u_2, v_2}^{ДКП}| > P, & \text{при } b_k = 0, \\ |b_{u_1, v_1}^{ДКП}| - |b_{u_2, v_2}^{ДКП}| < -P, & \text{при } b_k = 1. \end{cases}$$

Таким чином, первинне зображення спотворюється за рахунок внесення змін у коефіцієнти ДКП, якщо їх відносні величини не відповідають приховуваному біту. Чим більше P , тим стеганосистема, створена на основі даного методу, є більш стійкою до стиску, однак якість зображення при цьому може значно погіршитися (рис.1.4).



а



б



в

Рис. 1.4. Приклад використання алгоритму Коха й Жао: а - оригінальне ЦЗ-контейнер; б - стеганоповідомлення, отримане з використанням $P=25$; в - стеганоповідомлення, отримане з використанням $P=75$

Після відповідного внесення корекції в значення коефіцієнтів ДКП, проводиться зворотне ДКП блоку.

У результаті пересилання стеганоповідомлення, як уже говорилося вище, зазнає спотворення, спотворення зазнає й ДІ.

Для витягу ДІ виконується аналогічна процедура вибору коефіцієнтів ДКП у кожному блоці, що були задіяні в стеганоперетворенні, а розв'язок про переданий біт ухвалюється у відповідності з наступним правилом:

$$\begin{cases} b_k = 0, & \text{при } \left| \overline{b}_{u_1, v_1}^{ДКП} \right| > \left| \overline{b}_{u_2, v_2}^{ДКП} \right|, \\ b_k = 1, & \text{при } \left| \overline{b}_{u_1, v_1}^{ДКП} \right| < \left| \overline{b}_{u_2, v_2}^{ДКП} \right| \end{cases},$$

де $\overline{b}_{u_1, v_1}^{ДКП}$, $\overline{b}_{u_2, v_2}^{ДКП}$ - коефіцієнти ДКП блоку можливо зміненого при передачі стеганоповідомлення.

10. Поняття та актуальність селективної стеганографії

Якість забезпечення вимог до стеганосистеми більшою чи меншою мірою залежить від властивостей використовуваного контейнера, при цьому деякі з наявних стеганометодів, маючи обмеження на область застосування, ефективно працюють лише з контейнерами з певними характеристиками.

Всі контейнери можна розподілити на три великі класи: нав'язані, випадкові та обрані, при цьому саме обраний забезпечує найкращі властивості відповідного стеганоповідомлення, роблячи вибір контейнера актуальною задачею сучасної стеганографії. Організація вибору контейнера з певною метою за певним критерієм може відбуватися з використанням двох принципів: спрямованого - під конкретний стеганометод та загального, тобто такого, що не залежить від специфіки використовуваного стеганоалгоритму.

Вибір контейнера може відбуватися у відповідності з різними цілями. Одною з таких цілей є відшукування такого ЦЗ, в якому вже міститься вбудована ДІ відповідно до використовуваного стеганоалгоритма і секретного ключа, що не вимагає жодних змін контейнера при стеганоперетворенні. Такий варіант є оптимальним рішенням для забезпечення прихованості створюваного стеганографічного каналу зв'язку, тобто основної задачі класичної стеганографії, оскільки наявність тут ДІ не зможе бути виявлена жодним стеганоаналітичним засобом, відсутність збурень при стеганоперетворенні гарантує надійність сприйняття стеганоповідомлення. Але на практиці такий варіант вибору контейнера майже не використовується, оскільки, по-перше, є обчислювально складним, по-друге, не гарантує отримання шуканого рішення в завжди скінченній множині ЦЗ-претендентів. На практиці мета селекції часто пом'якшується: віднайти такий з сукупності наявних контентів-претендентів, вбудова в який заданої ДІ у відповідності з секретним ключем призведе до найменших сукупних збурень. Така задача завжди має рішення, яке в загальному випадку може бути далеким від оптимального, але в порівняльному сенсі буде, з великою ймовірністю, найкращим.

Метою вибору контейнера може бути забезпечення максимально можливої надійності сприйняття стеганоповідомлення, яка буде оцінюватися за допомогою тих чи інших кількісних показників (рис.1.5); чи забезпечення максимально можливої стійкості до атак проти вбудованого повідомлення чи до стеганоаналітичних атак. Актуальність вибору контейнера також визначається поняттям пропускнуєї спроможності або ємності контейнера: обрати такий контейнер, що «витримає» великий/найбільш можливий серед

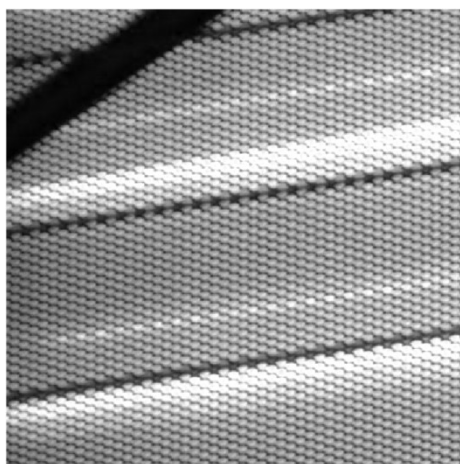
усіх претендентів обсяг додаткової інформації, який можна вбудувати без ризику візуального або статистичного виявлення. І тут важливо пам'ятати існуючий компроміс: чим більший обсяг даних ми намагаємося приховати, тим сильніше ми змінюємо структуру контейнера, і тим простіше пасивному порушнику виявити стеганоканал.



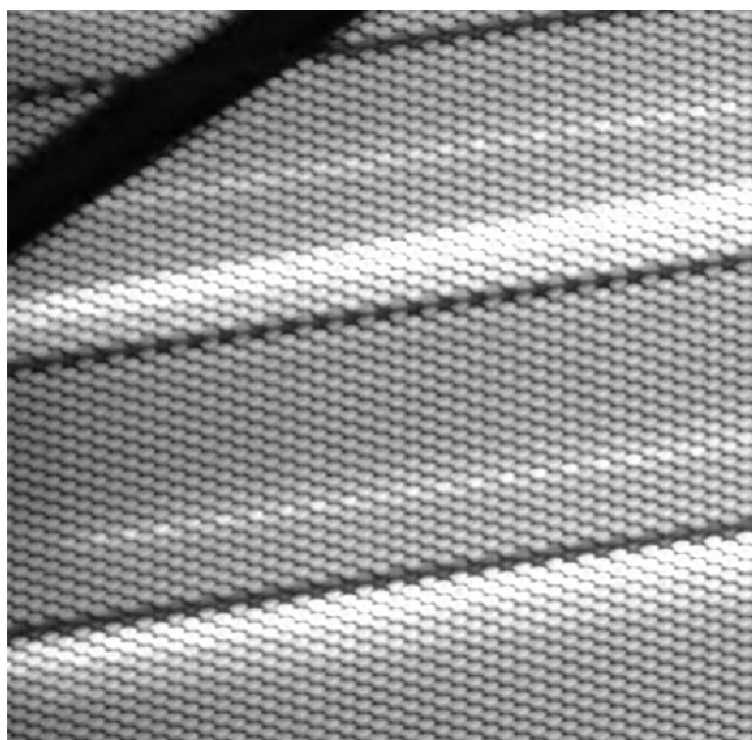
а



б



в



г

Рис.1.5. Ілюстрація різних результатів при вбудові однакової ДІ одним стеганометодом в різні контейнери: а, в – ЦЗ-контейнери; б,г – відповідні стеганоповідомлення

Селективна стеганографія включає в себе не тільки вибір контейнера, а й вибір в контейнері його підобластей, що є найбільш придатними для вбудови

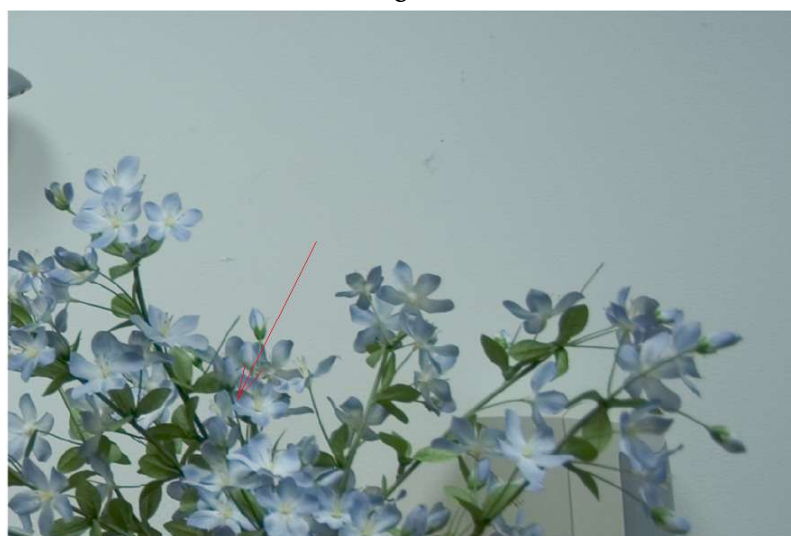
ДІ, адже загалом не всі частини контейнера однаково реагують на порівняно однакові збурні дії – вбудову ДІ (див.рис.1.6).



а



б



в

Рис.1.6. Відмінність «реакції» різних підобластей ЦЗ на стеганоперетворення: а – оригінальний контейнер; б, в – стеганоповідомлення з різною локалізацією області вбудови ДІ

Селективна стеганографія дає змогу застосовувати стеганографічні методи, які з різних причин мають обмеження на область застосування, а також ефективно використовувати випадкові контейнери, обираючи для стеганоперетворення найбільш придатні підобласті.

Питання

1. Що називається контейнером, стеганоповідомленням? Що має сенс використовувати в якості контейнера при організації стеганографічного каналу зв'язку? Чому?
2. Принцип Керхгоффа.
3. Що таке стеганографія, комп'ютерна стеганографія, цифрова стеганографія?
4. Класифікація напрямків, які містить у собі стеганографія.
5. Що таке цифровий водяний знак? Для чого він використовується?
6. Структурна схема стеганосистеми.
7. Класифікація стеганосистем.
8. Що таке потоковий, фіксований контейнер?
9. Що представляє із себе обраний, випадковий, нав'язаний контейнер?
10. Поняття стійкості стеганосистеми.
11. Загальні вимоги до стеганосистеми. В чому полягають труднощі одночасного забезпечення всіх вимог?
12. В чому полягають особливості й переваги використання частотної області контейнера для стеганоперетворення?
13. Основні недоліки та переваги метода модифікації найменшого значущого біта.
14. В чому полягає актуальність селективної стеганографії?
15. Пояснити, чому вибір контейнера і його підобластей, найбільш придатних для стеганоперетворення, робиться не завжди.

Тема 2. ЗАГАЛЬНИЙ ПІДХІД ДО ОЦІНКИ І ПОРІВНЯННЯ ВЛАСТИВОСТЕЙ СТЕГАНОГРАФІЧНИХ АЛГОРИТМІВ

План

1. Основні властивості стеганометоду.
2. Оцінка властивостей і порівняння стеганографічних методів.
3. Приклади використання метода (порівняльної) оцінки властивостей стеганоалгоритмів.
4. Реалізація підвищення стійкості стеганоповідомлення до атак проти вбудованого повідомлення.

1. Основні властивості стеганометоду

Як контейнер розглядається зображення в градаціях сірого, прямокутна (чи квадратна) матриця якого позначається F .

Вбудову ДІ в контейнер, незалежно від способу та області цієї вбудови можна представити як збурення ΔF матриці F відповідно до (1.1) (Тема 1), тобто матриця стеганоповідомлення (СП) F_{st} задовольняє співвідношенню: $F_{st} = F + \Delta F$. Виходячи з цього, *кожне стегоперетворення можна представити у вигляді адитивної вбудови деякої інформації у просторовій області ЦЗ-контейнера*. Будь-які перетворення, які після вбудови виникають із СП, будемо розглядати як додаткові збурення матриці F . Таким чином, стегоперетворення даного зображення, результати атак, які відбуваються під час пересилання СП по каналу зв'язку і т.д. еквівалентним чином представляються у вигляді елементарних матричних операцій.

У якості набору параметрів, що однозначно визначають й всебічно характеризують будь-яке СП/контейнер, можна використовувати будь-який з наборів, який однозначно визначає довільну двовимірну матрицю. Назвемо такі набори параметрів *повними*.

У якості повних наборів можна розглядати:

1. Набір сингулярних чисел (СНЧ) і сингулярних векторів (СНВ) матриці, які визначаються за допомогою її єдиного нормального сингулярного розкладання;
2. Набір власних значень (ВЗ) і власних векторів (ВВ) матриці, які визначаються за допомогою її єдиного нормального спектрального розкладання (в випадку симетричної матриці).

Розглянемо перший повний набір параметрів.

Будь-яке перетворення цифрового зображення (ЦЗ), у тому числі й стегоперетворення, збурить його матрицю F , а значить певним чином збурить її СНЧ і СНВ. У силу цього має місце наступне твердження.

Твердження 1. Будь-яке перетворення ЦЗ, у тому числі й стегоперетворення, представляється у вигляді сукупності збурень СНЧ і (або) СНВ його матриці, що дозволяє природно звести задачу аналізу властивостей ЦЗ (у тому числі, стеганоаналізу) до аналізу збурень СНЧ і СНВ відповідної матриці, а задачу побудови стеганоповідомлення із заданими властивостями - до задачі забезпечення певних характеристик збурень СНЧ і СНВ його матриці.

Позначимо $\sigma = (\sigma_1, \sigma_2, \dots, \sigma_m)^T$ - вектор СНЧ матриці F , де $\sigma_1(B) \geq \sigma_2(B) \geq \dots \geq \sigma_m(B) \geq 0$. Нормуємо цей вектор. В результаті отримаємо вектор:

$$\sigma_n = \frac{\sigma}{\|\sigma\|} = (\sigma_1^{(n)}, \sigma_2^{(n)}, \dots, \sigma_m^{(n)})^T,$$

кожна компонента якого дорівнює: $\sigma_i^{(n)} = \frac{\sigma_i}{\|\sigma\|}, i = 1, \dots, m$.

Для $m = 3$ геометричне представлення стегоперетворення ЦЗ дано на рис.1, де u_1, u_2, u_3 — СНВ матриці контейнера, $\bar{u}_1, \bar{u}_2, \bar{u}_3$ — СНВ матриці СП, σ_n - нормований вектор СНЧ контейнера, $\bar{\sigma}_n$ - нормований вектор СНЧ СП.

Таким чином, про результат перетворення (стегоперетворення) ЦЗ, його властивостях можна судити по характерних рисах сукупності збурень параметрів, що його однозначно визначають - СНЧ і СНВ.

Розглянемо другий з можливих повних наборів параметрів. Для ЦЗ з симетричною матрицею має місце наступне твердження.

Твердження 2. Будь-яке перетворення, у тому числі стегоперетворення, ЦЗ у випадку симетричності його матриці представляється у вигляді збурень спектра й (або) ВВ матриці, що однозначно визначаються нормальним спектральним розкладанням, що дозволяє звести задачу аналізу процесу стегоперетворення й

властивостей СП до аналізу збурень ВЗ і ВВ, а задачу побудови СП із заданими властивостями - до забезпечення певних характеристик збурень ВЗ і ВВ його матриці.

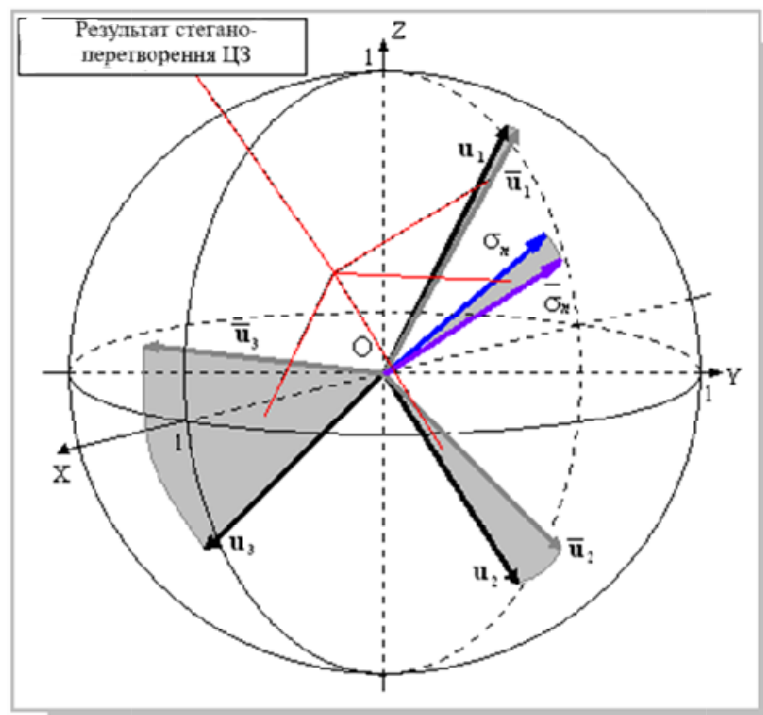


Рис.2.1. Геометричне представлення стеганоперетворення ЦЗ

Якщо матриця F контейнера симетрична, то в якості визначального її повного набору параметрів можна використовувати як множину СНЧ і СНВ, так і ВЗ матриці й множину ВВ. Перевагу в цьому випадку слід віддати другому набору параметрів у силу наступних зауважень:

- побудова спектрального розкладання симетричної матриці має ряд переваг в обчислювальному сенсі в порівнянні з побудовою сингулярного розкладання для матриці довільної структури тих же розмірів й того ж рівня заповненості;
- ВЗ симетричної матриці, як і її сингулярні числа, є добре обумовленими.

Однак, як правило, матриця ЦЗ-контейнера не задовольняє властивості: $F = F^T$. Для отримання її симетричного виду можливо піти по наступному шляху. Поставимо у відповідність довільній квадратній матриці F дві симетричні матриці A , B того ж розміру за наступним правилом:

$$F = \begin{pmatrix} a_{11} & a_{12} & a_{13} & \dots & a_{1n} \\ a_{21} & a_{22} & a_{23} & \dots & a_{2n} \\ a_{31} & a_{32} & a_{33} & \dots & a_{3n} \\ \dots & \dots & \dots & \dots & \dots \\ a_{n1} & a_{n2} & a_{n3} & \dots & a_{nn} \end{pmatrix} \rightarrow A = \begin{pmatrix} a_{11} & a_{12} & a_{13} & \dots & a_{1n} \\ a_{12} & a_{22} & a_{23} & \dots & a_{2n} \\ a_{13} & a_{23} & a_{33} & \dots & a_{3n} \\ \dots & \dots & \dots & \dots & \dots \\ a_{1n} & a_{2n} & a_{3n} & \dots & a_{nn} \end{pmatrix}, B = \begin{pmatrix} a_{11} & a_{21} & a_{31} & \dots & a_{n1} \\ a_{21} & a_{22} & a_{32} & \dots & a_{n2} \\ a_{31} & a_{32} & a_{33} & \dots & a_{n3} \\ \dots & \dots & \dots & \dots & \dots \\ a_{n1} & a_{n2} & a_{n3} & \dots & a_{nn} \end{pmatrix}, \quad (2.1)$$

які будемо розглядати нижче як матриці контейнера.

При вбудові ДІ у вхідний контейнер це стеганоперетворення представляється у вигляді вбудови у верхній (нижній) трикутник матриці $A(B)$ з наступним симетричним відображенням результату відносно головної діагоналі $A(B)$. Нехай підсумком такої вбудови є симетричні матриці $\bar{A}$ і $\bar{B}$. При остаточному реальному формуванні матриці СП використовується верхній трикутник $\bar{A}$ і нижній трикутник матриці $\bar{B}$.

Нехай E — матриця довільного збурення, якого зазнає контейнер (або СП). В загальному випадку $E \neq E^T$. Матриці E поставимо у відповідність дві симетричні матриці того ж розміру, використовуючи правило (1), розглядаючи матрицю, що відповідає верхньому (нижньому) трикутнику E як збурну для контейнера (СП), отриманого на основі $A(B)$, що дає принципову можливість матрицю довільного збурення й, як наслідок, матрицю СП також розглядати нижче як симетричні.

Розгляд матриці контейнера й СП у симетричному виді дозволить також добитися значного збільшення пропускну здатності прихованих каналів, що формуються деякими стеганометадами, у порівнянні з використанням ними вхідного несиметричного варіанту.

Для симетричної матриці контейнера процес стеганоперетворення геометрично можна представити аналогічно рис.1, тільки замість СНВ будуть розглядатися ВВ, а замість СНЧ – ВЗ відповідної матриці.

Одною з основних задач будь-якого стеганоалгоритма є забезпечення збереження в секреті наявності прихованого каналу передачі інформації, інакше кажучи, згенероване СП повинно зберігати надійність сприйняття: спотворення контейнера за рахунок вбудови ДІ не повинно бути помітним. Дотепер при аналізі рівня візуальних спотворень, які вносяться в контейнер F при стеганоперетворенні, широко застосовуються різницеві показники, розглянуті раніше (Тема 1). В Темі 1 було зазначено, що оскільки стеганоперетворення контейнера, а також збурні дії, яких зазнає СП, повинні забезпечувати надійність його сприйняття, то $\|\Delta F\|$ не може бути нескінченно великою, де ΔF — матриця збурення контейнера чи СП, оскільки у цьому випадку достовірною подією виявиться порушення висунутої вимоги. Крім того, при $\|\Delta F\| \rightarrow 0$ імовірність забезпечення надійності сприйняття буде прямувати до одиниці для кожного контейнера. Значення різницевого показників для зображення з матрицею F визначаються величиною $\|\Delta F\|_F$: чим менше $\|\Delta F\|_F$, тим краще кількісний показник візуального спотворення F , тим більше ймовірність забезпечення надійності сприйняття для зображення з матрицею $F + \Delta F$ при заданому зображенні F .

З врахуванням вищевказаного розглянемо матрицю контейнера як симетричну, позначаючи її далі A , щоб відрізнити від довільної матриці F .

Теорема 1. Нехай вбудова ДІ викликає збурення $\delta_{k_1}, \dots, \delta_{k_p}$ ВЗ $\lambda_{k_1}, \dots, \lambda_{k_p}$ матриці A контейнера. Тоді величина норми матриці збурення ΔA не залежить від того, які ВЗ були збурені, а залежить лише від абсолютних величин цих збурень.

Без доказу.

Теорема 2. Нехай стеганоперетворення викликало збурення ВВ матриці A контейнера. Достатньою умовою для забезпечення малого значення норми матриці збурення є відповідність збурених ВВ малим по модулю ВЗ A .

Без доказу.

Теорема 3. Нехай стеганоперетворення збурило ВВ матриці A контейнера. Достатньою умовою для забезпечення малого значення норми матриці збурення є відповідність збурених ВВ власним значенням матриці контейнера з малою абсолютною відокремленістю.

Без доказу.

Оскільки довільне стеганоперетворення еквівалентним чином представляється у вигляді збурення спектра й (або) ВВ матриці контейнера, то з вищевказаного випливає істинність наступного твердження.

Твердження 3. З метою забезпечення великої ймовірності надійності сприйняття СП вбудову ДІ в контейнер доцільно робити таким чином, щоб збурені стеганоперетворенням ВВ відповідали малим по модулю ВЗ або ВЗ, що мають малі абсолютні відокремленості, збурення ВЗ були малі. Чим менше збурення ВЗ, абсолютні відокремленості й модулі ВЗ, що відповідають збуреним ВВ, тим більше ймовірність дотримання надійності сприйняття СП.

Одна з основних вимог, що висуваються до будь-якого СП із метою забезпечення ефективного декодування додаткової інформації, - нечутливість до збурних дій сформованого СП.

Визначення 1. СП будемо називати *чутливим* до збурних дій, якщо навіть незначні збурні дії, яких воно зазнає, здатні зруйнувати значну частину вбудованої ДІ й привести до великого зростання кількості помилок при декодуванні ДІ. Інакше СП будемо називати *нечутливим*.

Скрізь нижче розглядаються такі збурні дії на контейнер і СП, які забезпечують високу ймовірність надійності сприйняття, тобто малі збурні дії.

Для СНЧ $\sigma_j(F)$, $\sigma_j(F + \Delta F)$, $j = \overline{1, n}$, матриць F і $F + \Delta F$ відповідно має місце співвідношення, розглянуте вище: $\max_{1 \leq j \leq n} |\sigma_j(F) - \sigma_j(F + \Delta F)| \leq \|\Delta F\|_2$. Аналогічне співвідношення має місце для ВЗ симетричної матриці. У силу цього збурення СНЧ (ВЗ) порівнянні зі збуренням даних — $\|\Delta F\|_2$, тобто СНЧ (ВЗ симетричної матриці) матриці є нечутливими до збурних дій незалежно від того, чутливим або нечутливим виявиться СП з матрицею $F + \Delta F$.

Зауваження. Для оцінки чутливості СП, отриманого на основі ЦЗ-контейнера з матрицею F має сенс аналізувати лише збурення СНВ (ВВ симетричної матриці) F , що відбулися в процесі стеганоперетворення. Результат стеганоперетворення ЦЗ для встановлення міри чутливості до збурних дій отриманого СП будемо розглядати у вигляді сукупності збурень СНВ (ВВ у випадку симетричної матриці) його матриці.

Нехай розглядається симетрична матриця контейнера A .

Теорема 4. Достатньою умовою забезпечення малої чутливості СП до збурних дій є відповідність збурених при стегаперетворенні контейнера власних векторів його матриці A власним значенням матриці СП $\bar{A}$, що мають великі абсолютні відокремленості.

Наслідок 1. Якщо збурені в результаті стегаперетворення контейнера ВВ відповідають ВЗ матриці СП із малими абсолютними відокремленостями, то отримане СП виявляється чутливим до збурних дій, що, як правило, приводить до недостатньої ефективності декодування ДІ.

Враховуючи, що всі збурення, що впливають на контейнер і СП, є малими, абсолютні відокремленості ВЗ матриць $\bar{A}$ і A незначно відрізняються між собою. Звідки випливає

Наслідок 2. Достатньою умовою забезпечення малої чутливості СП до збурень є відповідність збурених при стегаперетворенні контейнера ВВ власним значенням матриці контейнера, що мають великі абсолютні відокремленості.

Із усього вищесказаного випливає істинність наступного твердження.

Твердження 4. Чутливість СП до збурних дій визначається чутливістю збурених ВВ матриці контейнера при стегаперетворенні. Виходячи зі значень збурень ВВ і абсолютних відокремленостей відповідних ВЗ можливо зробити якісні апріорні оцінки чутливості СП до збурних дій.

Нехай матриця контейнера має довільну структуру.

Твердження 5. Нехай стегаперетворення збурило СНВ матриці контейнера. Достатньою умовою забезпечення малої чутливості одержуваного СП до збурень є відповідність збурених СНВ сингулярним числам з великою відокремленістю. Відокремленість СНЧ, що відповідають збуреним СНВ матриці ЦЗ-контейнера, є мірою чутливості отриманого СП до збурних дій.

Наслідок. Нехай $\bar{F}$ — матриця СП, результатом стегаперетворення є збурення матриці СНВ U , яка отримана нормальним сингулярним розкладанням матриці контейнера F . Якщо збурення U відповідає СНВ, які відповідають СНЧ з малою відокремленістю, то одержуване СП виявиться чутливим до збурних дій незалежно від виду самого стегаметоду й використовуваної області вбудови ДІ.

2. Оцінка властивостей і порівняння стегаграфічних методів

Метод оцінки властивостей довільного стегаметоду полягає в дослідженні збурень спектра та власних векторів матриці контейнера внаслідок стегаперетворення. Основні кроки такого дослідження:

1. Для симетричних матриць A контейнера і A_{st} стегаповідомлення побудувати нормальні спектральні розкладання (НСР):

$$A = U \Lambda U^T, A_{st} = U_{st} \Lambda_{st} U_{st}^T;$$

2. Знайти збурення матриць власних значень

$$\Delta \Lambda = \Lambda - \Lambda_{st}$$

та власних векторів

$$\Delta U = U - U_{st};$$

3. Оцінити значення:

$$\delta \lambda = \max_i |\Delta \Lambda_{ii}|,$$

де $\Delta \Lambda_{ii}$ - діагональні елементи матриці $\Delta \Lambda$;

4. Серед власних векторів визначити ті, які отримали збурення;
5. Серед збурених власних векторів визначити ті, збурення яких найбільші (для цього можна використовувати, наприклад, яку-небудь векторну норму для стовпців ΔU);
6. За отриманими в 1-5 результатами зробити висновки:

- якщо значення $\delta\lambda$ мале в порівнянні з власними значеннями, а збурення власних векторів, які відповідають власним значенням з максимальною абсолютною відокремленістю, малі в порівнянні зі збуреннями решти власних векторів, то використовуваний стеганометод з великою ймовірністю забезпечує надійність сприйняття стеганоповідомлення;
- якщо збурення в процесі стеганоперетворення зазнали власні вектори, які відповідають власним значенням з малою абсолютною відокремленістю, то отримане стеганоповідомлення буде чутливим до будь-яких збурних дій;
- якщо в процесі стеганоперетворення збурення зазнали власні вектори, які відповідають власним значенням з відносно великою абсолютною відокремленістю, то це забезпечить малу чутливість стеганоповідомлення до будь-яких збурень і, як наслідок, порівняно велику ефективність декодування, але при цьому може не забезпечуватися надійність сприйняття стеганоповідомлення;
- забезпечення як надійності сприйняття стеганоповідомлення, так і його малої чутливості до збурних дій буде з великою ймовірністю мати місце в тому випадку, коли основні збурення зазнають ті власні вектори, що відповідають власним значенням, абсолютні відокремленості яких мають середні значення в множині відокремленостей, сформованій для всього спектра.

Для порівняння основних розглянутих властивостей кількох стеганометодів пункти 1-3 виконуються не для однієї матриці A_{st} , а для всіх матриць стеганоповідомлень, отриманих на основі A контейнера порівнювальними стеганометадами (СМ).

Нехай порівнюються між собою p СМ, $\Delta U_1, \dots, \Delta U_p$ - матриці збурень власних векторів, отримані на кроці 2, $\delta\lambda_1, \dots, \delta\lambda_p$ - відповідні їм числові значення, отримані в пункті 3. Аналіз результатів приводить до таких **висновків**:

- найкращу (найгіршу) надійність сприйняття СП з великою ймовірністю забезпечує той алгоритм, при використанні якого отримуємо $\min_{1 \leq i \leq p} \delta\lambda_i$ ($\max_{1 \leq i \leq p} \delta\lambda_i$). Якщо всі $\delta\lambda_1, \dots, \delta\lambda_p$ порівнянні величини, то перевагу треба надати тому СМ, в якому збурення не торкнулися ВВ, що відповідають ВЗ із порівняно великими абсолютними відокремленостями;
- для зрівнюваних СМ найменше чутливими до збурних дій буде СП, отримання якого привело до збурення ВВ, які відповідають ВЗ, абсолютна відокремленість яких є найбільшою порівняно до відокремленостей ВЗ, які відповідають збуреним ВВ в інших СП.

Висновок. Запропонований підхід до оцінки властивостей СМ є універсальним, не залежить від особливостей конкретного методу, може бути використаний також для якісного порівняння довільних СМ. Обчислювальні витрати порівняні до кількості арифметичних операцій для побудови НСР матриці, складають $O(n^3)$, де n - розмір матриці контейнера. Ця кількість

операцій може бути зменшеною до $O(n^2)$, якщо спочатку для матриць контейнера і СП зробити стандартне розбиття на блоки фіксованого малого розміру.

3. Приклади використання метода оцінки властивостей стеганоалгоритмів

Розглянемо добре відомий СМ заміни найменшого значущого біта (LSB). Процес стегоперетворення будемо трактувати як аддитивну вбудову ДІ в просторовій області відповідно до: $F_{st} = F + \Delta F$. Зазначимо, що ΔF в загальному випадку не є безпосередньо матрицею ДІ, але вона однозначно будується по заданій ДІ. В даному конкретному прикладі, якщо значення чергового біта, який вбудовується в контейнер, співпадає зі значенням LSB поточного пікселя контейнера, то відповідне значення елемента ΔF буде дорівнювати 0, інакше елемент ΔF природньо приймає значення +1 чи -1. Для наочної ілюстрації використання запропонованого метода розглянемо як контейнер матрицю F розміру 8×8 (рис.2(а)), яка відповідає блоку реального ЦЗ. Матриці F загального виду поставимо в відповідність симетричні матриці A_N , A_V за формулою (1) (рис.2(б, в)). Хай ΔF відповідає ДІ, яка вбудовується в блок F , сформована випадковим чином, має вид, представлений на рис.3(а), $\Delta F \neq \Delta F^T$. Разіб'ємо ΔF на дві частини: нижній трикутник ΔF після симетричного відзеркалення відносно головної діагоналі відповідає тій частині секретного повідомлення ($\Delta F N$ (рис.3(б))), яка буде вбудовуватися в A_N ; верхній трикутник після аналогічної трансформації ($\Delta F V$) - інформація, яка вбудовується в A_V . Далі для простоти викладання будемо розглядати тільки одну матрицю, наприклад, A_N , називаючи її матрицею контейнера.

Для збереження симетричності використовуваних для обробки матриць процес побудови блоку СП F_{st} розкладається на два етапи:

- $FN_{st} = A_N + \Delta FN$,
- $FV_{st} = A_V + \Delta FV$,

блок СП отримується як об'єднання нижнього трикутника FN_{st} і верхнього трикутника FV_{st} .

F=								A _г =								A _в =							
213	214	212	197	137	112	110	109	213	189	159	133	137	189	214	213	213	214	212	197	137	112	110	109
189	210	213	210	167	119	110	108	189	210	204	186	175	164	186	200	214	210	213	210	167	119	110	108
159	204	210	212	189	137	119	107	159	204	210	204	201	175	164	177	212	213	210	212	189	137	119	107
133	186	204	209	194	153	128	107	133	186	204	209	210	199	154	131	197	210	212	209	194	153	128	107
137	175	201	210	195	145	126	107	137	175	201	210	195	175	142	119	137	167	189	194	195	145	126	107
189	164	175	199	175	131	121	108	189	164	175	199	175	131	121	113	112	119	137	153	145	131	121	108
214	186	164	154	142	121	113	107	214	186	164	154	142	121	113	112	110	110	119	128	126	121	113	107
213	200	177	131	119	113	112	106	213	200	177	131	119	113	112	106	109	108	107	107	107	108	107	106
а								б								в							

Рис.2.2. Контейнер та його симетричні представлення: а – матриця блоку контейнера; б, в - симетричні матриці, які відповідають блоку F контейнера.

$\Delta F =$	$\Delta FN =$	$\Delta FV =$
0 1 0 0 -1 0 1 0	0 1 0 1 1 0 0 1	0 1 0 0 -1 0 1 0
1 0 1 1 0 0 1 1	1 0 0 1 0 0 1 1	1 0 1 1 0 0 1 1
0 0 0 1 1 0 -1 0	0 0 0 1 1 0 1 0	0 1 0 1 1 0 -1 0
1 1 1 0 0 1 1 0	1 1 1 0 0 0 -1 0	0 1 1 0 0 1 1 0
1 0 1 0 0 0 0 1	1 0 1 0 0 0 0 1	-1 0 1 0 0 0 0 1
0 0 0 0 0 0 1 0	0 0 0 0 0 0 1 0	0 0 0 1 0 0 1 0
0 1 1 -1 0 1 0 1	0 1 1 -1 0 1 0 1	1 1 -1 1 0 1 0 1
1 1 0 0 1 0 1 0	1 1 0 0 1 0 1 0	0 1 0 0 1 0 1 0
а	б	в

Рис. 2.3. Матриця ДІ: а - яка відповідає блоку F ; б - яка відповідає блоку A_N ; в - яка відповідає блоку A_V .

Побудуємо НСР: $A_N = U_{A_N} \Lambda_{A_N} U_{A_N}^T$ і $FN_{st} = U_{FN_{st}} \Lambda_{FN_{st}} U_{FN_{st}}^T$, результати яких представлені на рис.4. Стегоперетворення досить незначно збурило спектр і ВВ, які відповідають $\lambda_1, \dots, \lambda_5$, а порівняно великі збурення отримали ВВ, відповідні найменшим за модулем ВЗ $\lambda_6, \lambda_7, \lambda_8$ з найменшою абсолютною відокремленістю (на рис.4 жирним шрифтом). Таким чином, розглянуте стегоперетворення *забезпечує надійність сприйняття СП* після вбудови ДІ, але отримане СП *буде чутливим до збурних дій*, що може призвести до великої кількості похибок під час декодування секретного повідомлення в каналі зв'язку, відмінному від ідеального.

Висновки, зроблені на основі теоретичних викладок, повністю відповідають відомим характеристикам метода LSB.

Розглянемо приклад використання запропонованої методики для порівняння параметрів кількох стеганоалгоритмів. Нехай випадково сформоване бінарне повідомлення вбудовується адитивно в контейнер:

- а) в контур;
- б) довільно.

Як контейнер розглянемо той самий блок зображення, матриця якого зображена на рис.2(а). Цей блок містить частину контура. Для визначеності розглянемо матрицю, яка відповідає верхньому трикутнику $F - A_V$. На рис.5(а) представлені результати вбудови ДІ випадковим чином, а на рис.5(б) вбудова відбувалась в контур, $FV_{st} = A_V + \Delta FV$.

1.0e+003*								
1.3703	0.1566	-0.1285	0.0427	-0.0413	-0.0136	0.0025	-0.0017	
a								
1.0e+003*								
1.3738	0.1560	-0.1285	0.0419	-0.0418	-0.0135	0.0029	-0.0021	
б								
0.3694	0.5885	0.5263	0.4334	0.1344	0.0275	0.1755	0.0522	
0.3903	0.1550	0.2293	-0.4885	-0.3651	0.2857	-0.5431	-0.1504	
0.3861	-0.1875	0.1839	-0.4458	-0.1985	-0.4716	0.5422	0.1651	
0.3691	-0.4699	0.1638	0.1631	0.4611	-0.2670	-0.2620	-0.4868	
0.3514	-0.4432	0.0153	0.1163	0.1713	0.5230	0.0211	0.6024	
0.3301	-0.1400	-0.3425	0.4460	-0.5908	0.1627	0.2325	-0.3544	
0.3150	0.2133	-0.4669	0.1723	-0.0283	-0.5049	-0.4258	0.4130	
0.3068	0.3349	-0.5237	-0.3257	0.4663	0.2626	0.2752	-0.2265	
в								
0.3696	0.5870	0.5258	0.4342	0.1393	0.0188	0.0196	0.1838	
0.3903	0.1588	0.2321	-0.4883	-0.3685	0.3002	-0.0282	-0.5508	
0.3859	-0.1936	0.1866	-0.4434	-0.1943	-0.4902	0.0210	0.5510	
0.3692	-0.4682	0.1587	0.1612	0.4737	-0.2341	-0.4189	-0.3724	
0.3513	-0.4419	0.0133	0.1113	0.1588	0.5068	0.5987	0.1678	
0.3295	-0.1405	-0.3374	0.4558	-0.5907	0.1579	-0.3927	0.1481	
0.3155	0.2109	-0.4652	0.1628	-0.0275	-0.5104	0.4856	-0.3406	
0.3070	0.3377	-0.5284	-0.3222	0.4558	0.2685	-0.2728	0.2332	
г								

Рис.2.4. Результати нормального спектрального розкладання: а – спектр матриці A_N ; б – спектр матриці стеганоповідомлення FN_{st} ; в – матриця U_{AN} ; г – матриця власних векторів FN_{st}

Збурення спектра Δ_V при зануренні ДІ								
-0.9370	-0.3020	-0.6883	0.2492	0.6107	-0.0175	0.2514	-0.4516	
Збурення матриці власних векторів Δ_V								
-0.0001	-0.0006	0.0004	-0.0005	-0.0052	0.0086	-0.0459	0.0207	
-0.0001	0.0009	-0.0003	-0.0020	-0.0005	-0.0021	0.0565	-0.0692	
-0.0001	-0.0008	-0.0016	0.0091	0.0075	-0.0217	-0.0181	0.0870	
-0.0001	0.0000	0.0014	-0.0019	-0.0223	0.0163	0.0551	-0.0098	
-0.0001	0.0006	0.0011	-0.0055	0.0137	-0.0032	-0.0743	-0.0471	
0.0003	-0.0005	-0.0006	0.0007	0.0113	0.0092	0.0336	0.0395	
0.0001	-0.0003	-0.0007	-0.0004	-0.0138	-0.0178	-0.0421	-0.0394	
0.0000	0.0006	0.0011	-0.0002	0.0095	0.0114	0.0350	0.0171	
Вектор норм власних векторів								
0.0003	0.0017	0.0029	0.0110	0.0343	0.0369	0.1353	0.1361	
а								
Збурення спектра Δ_V при зануренні ДІ								
-1.1056	-0.3438	-0.4595	-0.6400	-0.0730	-0.6115	0.0271	0.1448	
Збурення матриці власних векторів Δ_V								
0.0000	0.0016	-0.0024	-0.0000	0.0089	0.0250	-0.0318	-0.0245	
-0.0000	0.0014	-0.0008	-0.0051	-0.0137	-0.0503	0.0153	0.0204	
0.0000	0.0019	0.0096	-0.0009	0.0190	0.0531	0.0168	-0.0052	
-0.0000	-0.0040	-0.0085	0.0048	-0.0055	-0.0255	-0.0464	-0.0256	
0.0000	0.0010	0.0049	-0.0026	0.0010	-0.0064	0.0415	0.0215	
0.0000	0.0017	-0.0009	0.0082	-0.0062	0.0114	-0.0037	0.0063	
-0.0000	-0.0051	0.0030	-0.0081	-0.0080	-0.0153	-0.0153	0.0013	
-0.0000	0.0011	-0.0054	0.0039	0.0039	0.0075	0.0247	0.0069	
Вектор норм власних векторів								
0.0000	0.0074	0.0153	0.0143	0.0279	0.0842	0.0791	0.0475	
б								

Рис.2.5. Результати вбудови ДІ в контейнер: а - довільним чином; б - в контур

Порівнюючи збурення матриць ВВ, можна побачити, що збурення при вбудові поза контура зачеплять і ВВ, для якого ВЗ має найбільшу абсолютну відокремленість, у той час, як при вбудові в контур такого не відбувається. Це означає, що надійність сприйняття СП буде кращою при вбудові в контур (це добре відомий факт), чутливість СП до збурних дій в обох методах велика (найбільші збурення отримали ВВ, які відповідають ВЗ з малою абсолютною відокремленістю) і майже однакова, що також відповідає відомим характеристикам зрівнюваних алгоритмів вбудови.

Таким чином, запропонований універсальний метод оцінки основних параметрів будь-якого СМ дозволяє проводити апріорне порівняння властивостей довільних СМ.

Запропонований підхід дає змогу формалізувати процес якісного порівняння СМ, незалежно від їх конкретного виду і використовуваної області вбудови.

4.Реалізація підвищення стійкості стеганоповідомлення до атак проти вбудованого повідомлення

За допомогою загального підходу до аналізу стану інформаційної системи, що заснований на теорії збурень і матричному аналізі, можна довести наступне твердження.

Твердження. Достатньою умовою забезпечення/підвищення стійкості блокового стеганоалгоритму (вбудова ДІ відбувається в блоки контейнера, попередньо отримані за допомогою стандартної розбивки його матриці) до збурних дій (атак проти вбудованого повідомлення) є локалізація збурення СНЧ блоків B контейнера, що відбуваються в результаті вбудови ДІ, в області максимального СНЧ $\sigma_1(B)$.

Звісно, при реалізації стеганоперетворення, де вбудова ДІ не пов'язана з безпосереднім збуренням $\sigma_1(B)$, точно забезпечити отриману достатню умову на практиці вкрай складно: стеганоперетворення може збурити певну кількість/всі СНЧ блоку в результаті вбудови ДІ. Тут отримана достатня умова може бути використана, по-перше, для якісної оцінки відносної чутливості СП; по-друге, для зменшення чутливості СП шляхом перерозподілу збурень, що виникають в процесі вбудови ДІ, між СНЧ блоку, збільшуючи (долю) збурення саме $\sigma_1(B)$ (це є тим математичним результатом, що зафіксує підвищення стійкості до збурної дії методу при його модифікації); по-третє, для вибору параметрів стеганометоду, що забезпечать порівняно значну стійкість до збурних дій.

Розробка/удосконалення стеганометодів, стійких до атак проти вбудованого повідомлення, зокрема до атаки стиском, залишається актуальною задачею сучасної стеганографії. Розглянемо питання підвищення стійкості до збурних дій з використанням наведеної вище достатньої умови одного з найпоширеніших на сьогодні стеганометоду - методу модифікації найменшого значущого біта (*LSB*-метод), використовуючи його основну ідею для вбудови ДІ, але змінивши область стеганоперетворення контейнера з просторової на область сингулярного розкладання його матриці.

Поширення та частота використання *LSB*-методу та його модифікацій (зокрема, коли вбудова біта ДІ відбувається в i -ий з кінця біт двійкового представлення значення яскравості пікселя, де $i > 1$) має декілька причин. Це простота ідеї вбудови та декодування ДІ і порівняно незначна обчислювальна складність його класичної реалізації, потенційно можлива значна пропускна спроможність прихованого каналу (до 3 біт/піксель для кольорового ЦЗ-контейнера) при збереженні надійності сприйняття формованого стеганоповідомлення. Але основним недоліком класичного методу залишається його нестійкість до будь-яких атак проти вбудованого повідомлення при

використанні в просторовій області контейнера, а також нестійкість його до виявлення наявними стеганоаналітичними методами при значній пропускну здатності прихованого каналу. Останнє приводить до того, що сьогодні *LSB*-метод часто використовується з дуже незначною пропускну здатністю.

Розглянемо стеганометод, прототипом якого є *LSB*-метод, що далі для зручності має назву *G*, основні кроки якого наступні. В якості ДІ розглядається бітова послідовність $p_1, p_2, \dots, p_m$.

Вбудова ДІ:

Крок 1. Матриця *F* ЦЗ-контейнера розбивається стандартним чином на $l \times l$ -блоки.

Крок 2. Нехай *B* — блок ЦЗ-контейнера, який у відповідності з секретним ключем є черговим блоком, задіяним у стеганоперетворенні, а p_i — черговий біт ДІ.

2.1 Побудувати сингулярне розкладання *B*: $B = U(B)\Sigma(B)V^T(B)$; визначити $\sigma_1(B)$;

2.2 Вбудова p_i в $\sigma_1(B)$:

2.2.1 Нехай $\sigma = [\sigma_1(B)]$, де $[\cdot]$ — результат округлення аргументу до найближчого цілого;

2.2.2 Нехай $\bar{\sigma} = \text{bitset}(\sigma, k, p_i)$, де операція $\text{bitset}(\sigma, k, p_i)$ встановлює на місце k -го з кінця біта в двійковому представленні σ значення p_i

2.2.3 Формування блоку $\bar{B}$ стеганоповідомлення $\bar{F}$, що відповідає блоку *B* контейнера: $\bar{B} = U(B)\bar{\Sigma}(B)V^T(B)$, де $\bar{\Sigma}(B) = \text{diag}(\bar{\sigma}, \sigma_2(B), \dots, \sigma_l(B))$.

Крок 3. Якщо процес стеганоперетворення не завершено, перехід на крок 2; інакше: результат вбудови ДІ — ЦЗ-стеганоповідомлення з матрицею $\bar{F}$.

Декодування ДІ:

Крок 1. Матриця $\bar{F}$ (можливо збуреного) ЦЗ-стеганоповідомлення розбивається стандартним чином на $l \times l$ -блоки.

Крок 2. Нехай $\bar{B}$ — блок стеганоповідомлення, який у відповідності з секретним ключем є черговим блоком, задіяним у стеганоперетворенні, а $\bar{p}_i$ — черговий біт ДІ, що декодується.

2.1 Побудувати сингулярне розкладання $\bar{B}$, в результаті якого отримати матрицю СНЧ блоку: $\bar{\Sigma}(B) = \text{diag}(\sigma_1(\bar{B}), \sigma_2(\bar{B}), \dots, \sigma_l(\bar{B}))$.

2.2 Декодування $\bar{p}_i$:

2.2.1 Нехай $\sigma = [\sigma_1(\bar{B})]$;

2.2.2 Нехай $\bar{p}_i = \text{bitget}(\sigma, k)$, де операція $\text{bitget}(\sigma, k)$ отримує значення k -го з кінця біта в двійковому представленні σ .

Крок 3. Якщо процес декодування ДІ не завершено, перехід на крок 2;

інакше: результат декодування ДІ: $\bar{p}_1, \bar{p}_2, \dots, \bar{p}_m$.

Наведена достатня умова забезпечення/підвищення стійкості стеганометода до збурних дій знайшла своє практичне підтвердження в

результаті розробки G . Максимально зафіксоване підвищення ефективності в порівнянні з LSB склало 57%.

Питання

1. Як формальне представляється стеганоперетворення ЦИ-контейнера з матрицею F ?
2. Чому кожне стеганоперетворення можна представити у вигляді аддитивної вбудови деякої інформації у просторовій області ЦЗ-контейнера?
3. Що таке повний набір параметрів? Навести приклади повних наборів параметрів. Коли який набір має сенс застосовувати?
4. Як через параметри повного набору формально представляється результат стеганоперетворення?
5. Геометричне представлення стеганоперетворення ЦЗ.
6. Як має сенс формально представляти процес стеганоперетворення у випадку симетричної матриці контейнера? Чому?
7. Яким чином можливо представити матрицю довільного ЦЗ-контейнера як симетричну? Що це дає?
8. Геометричне представлення стеганоперетворення ЦЗ у випадку симетричної матриці контейнера.
9. Формальні умови забезпечення надійності сприйняття стеганоповідомлення.
10. Коли СП називається чутливим/нечутливим?
11. Формальні умови забезпечення нечутливості стеганоповідомлення до збурних дій.
12. Яким чином для блоків матриці довільного цифрового зображення будується нормальне спектральне розкладання з дійсними власними значеннями?
13. Чим обумовлена одиничність нормального спектрального розкладання матриці?
14. Як оцінюється збурення власних векторів блоків матриці контейнера при стеганоперетворенні?
15. Які властивості стеганографічного алгоритму розглядаються як основні?
16. Як відбувається формальне порівняння основних властивостей декількох стеганографічних алгоритмів?
17. Формальна оцінка властивостей методу модифікації найменшого значущого біта при різних виборах стеганошляху.

Тема 3. МЕТОД ПІДВИЩЕННЯ СТІЙКОСТІ СТЕГАНОАЛГОРИТМУ ДО АТАК ПРОТИ ВБУДОВАНОГО ПОВІДОМЛЕННЯ

План

1. Спосіб передачі та декодування додаткової інформації.
2. Спосіб забезпечення малого числа обумовленості матриці довільного зображення.
3. Практична реалізація методу підвищення стійкості стеганоалгоритму до атак проти вбудованого повідомлення

1. Спосіб передачі та декодування додаткової інформації

Нехай F — $n \times n$ -матриця контейнера, $\det F \neq 0$. Як додаткова інформація (ДІ) виступає випадково сформована бінарна числова послідовність, що містить n елементів з множини $\{-1, 1\}$, що розглядається далі як вектор x довжини n . Послідовність може містити менш ніж n елементів, тоді вона доповнюється незначущими елементами до потрібної довжини.

Основні кроки *методу двоетапного декодування* ДІ SYSTEMA наступні:

Вбудова ДІ.

Крок 1. Обчислити добуток

$$b = Fx.$$

У припущенні відсутності помилок округлення, вектор x є точним розв'язком системи лінійних алгебраїчних рівнянь (СЛАР)

$$Fx = b. \quad (3.1)$$

Крок 2. Вектор b вбудувати в F замість вектора ДІ x деяким стеганометодом (СМ1).

Декодування.

Крок 1. З отриманого стеганоповідомлення (СП), можливо збуреного (зміненого) при пересиланні, декодувати вбудований вектор b в зміненому (збуреному) вигляді b_B за допомогою СМ1. Після декодування вектора b_B матриця зображення F_B , в загальному випадку, буде відрізнятися від F .

Крок 2. Декодувати x шляхом розв'язку неоднорідної СЛАР

$$F_B x_{np} = b_B, \quad (3.2)$$

де $F_B = F + \delta F$, $b_B = b + \delta b$; δF , δb — збурення матриці системи F і вектора правої частини b відповідно; x_{np} — результат декодування x в умовах збурених вхідних даних.

Використання запропонованого способу SYSTEMA пересилання й декодування ДІ, що включає додатковий етап у вигляді розв'язку СЛАР, при забезпеченні достатньої умови стійкості методу, обґрунтованого нижче, дає можливість збільшити обсяг P правильно відновленої інформації в порівнянні з

безпосереднім пересиланням x замість вектора b при абсолютно аналогічних умовах.

Нехай $x_{np} = x + \delta x$, де $\|\delta x\| = \|x_{np} - x\|$ — абсолютна похибка x_{np} . Тоді СЛАР (2) представляється в вигляді:

$$(F + \delta F)(x + \delta x) = b + \delta b \quad (3.3)$$

Можна показати:

$$\frac{\|\delta x\|}{\|x_{np}\|} \leq \|F^{-1}\| \|F\| \left(\frac{\|\delta b\|}{\|F\| \|x_{np}\|} + \frac{\|\delta F\|}{\|F\|} \right). \quad (3.4)$$

З (4) випливає, що $\text{cond}(F) = \|F^{-1}\| \|F\|$ є числом обумовленості, а тому мірою чутливості задачі про розв'язок СЛАР до похибки у вхідних даних. Якщо число обумовленості матриці ЦЗ-контейнера є малим, задача декодування ДІ на другому етапі SYSTEMA є нечутливою, малі збурення на вході незначно змінять результат, $x_{np} \approx x$.

Припустимо, що значення

$$\|F_B - F\| / \|F\|, \quad \|b_B - b\| / \|b\| \quad (3.5)$$

невеликі. Співвідношення (5) аналізують збурення всієї матриці й усього вектора в цілому. Навіть велика похибка, що виникає в окремих пікселях СП при невеликій їхній кількості не відіб'ється значно на оцінках для виразів (5), а тому при гарній обумовленості матриці F і на значеннях елементів вектора x в силу (4), хоча деякі елементи b можуть бути сильно «зіпсовані». Підтвердженням цього є результати обчислювального експерименту, наведені нижче.

Таким чином, для ефективного використання методу SYSTEMA у якості контейнера потрібно використовувати ЦЗ з добре обумовленою матрицею.

Можна показати, що величина $k(F) = \| |F^{-1}| |F| \|$ — число обумовленості Скіла — краще за $\text{cond}(F)$ дозволяє оцінити відносну похибку результату, де $|F|$ — матриця, що складається з модулів елементів F .

Має місце наступна теорема.

Теорема 1. Нехай матриця зображення, використовуваного в якості контейнера, має мале число обумовленості Скіла, тоді метод SYSTEMA є стійким.

2. Спосіб забезпечення малого числа обумовленості Скіла матриці довільного зображення

Оцінка числа обумовленості Скіла для матриці контейнера є ключовим моментом у питанні вибору підходящого для пересилання ДІ методом

SYSTEMA контейнера. Безпосереднє обчислення числа обумовленості Скіла для матриць великого розміру - процес дорогий. Крім того, якщо контейнер є нав'язаним, його матриця погано обумовлена, це, на перший погляд, взагалі позбавляє можливості використання методу SYSTEMA для забезпечення додаткового захисту інформації, що передається.

Пропонується спосіб, що дозволяє використовувати будь-яке зображення як контейнер у методі SYSTEMA незалежно від його реального числа обумовленості.

Можна показати, що для діагональної матриці F $k(F)=1$ (найменше з можливих значень), а тому метод SYSTEMA буде стійким. Порівнянню картину принципово можна очікувати й у випадку, коли для елементів F виконується умова (значна діагональна перевага):

$$|f_{ii}| \gg \sum_{j=1, j \neq i}^n |f_{ij}|, \quad i = 1, \dots, n. \quad (3.6)$$

Але реальні зображення рідко задовольняють властивості (6). Забезпечимо малість числа обумовленості Скіла матриці зображення, не змінюючи її явно, а лише моделюючи віртуально значну діагональну перевагу.

Нехай D — діагональна матриця розміром $n \times n$ з елементами $d_{ii} = m \sum_{j=1}^n |f_{ij}|$, $i = \overline{1, n}$, де f_{ij} , $i, j = \overline{1, n}$, — елементи матриці F поданого зображення, $m \in N$ — параметр. Вибір m забезпечує для $F+D$ наявність властивостей, близьких до (6), але оскільки b для використовуваної СЛАР обчислюється відповідно до виразу $b = (F + D)x$, то значення m не може бути довільно великим.

Реально матриця F не змінюється, а віртуально побудована для неї матриця $F+D$ очевидно має діагональну перевагу. При отриманні СП, для якого контейнер - це матриця F_B , на другому етапі декодування в SYSTEMA розв'язується СЛАР

$$(F_B + D')x_{np} = b_B, \quad (3.7)$$

де D' — діагональна матриця, яка формується декодером по отриманій збуреній матриці F_B з елементами $f_{B\ ij} : d'_{ii} = m \sum_{j=1}^n |f_{B\ ij}|$, $i = \overline{1, n}$, $\det(F_B + D') \neq 0$.

Оскільки властивості матриці системи (7) близькі до властивостей (6), розв'язок СЛАР (7) $x_{np} \approx x$, δx має мале значення. Таким чином, практичний метод введення віртуальної діагоналі в матрицю реального зображення забезпечує гарну обумовленість Скіла матриці СЛАР для декодування ДІ й стійкість SYSTEMA для будь-якого контейнера.

3. Практична реалізація методу підвищення стійкості стеганоалгоритму до атак проти вбудованого повідомлення

Матриці F поставимо у відповідність нижню трикутну матрицю $\bar{F}$ з елементами

$$\bar{f}_{ij} = \begin{cases} 0, \text{ якщо } f_{ij} \leq 127, \\ 1, \text{ якщо } f_{ij} > 127 \end{cases}, \quad j = \overline{1, n-1}, \quad i = \overline{j+1, n},$$

(3.8)

$$\bar{f}_{11} = m, \quad \bar{f}_{ii} = m \sum_{j=1}^{i-1} \bar{f}_{ij}, \quad i = \overline{2, n}, \quad m \in N$$

Вибір m повинен забезпечити для матриці $\bar{F}$ наявність властивостей, близьких до (6).

Формування вектора правої частини СЛАР для визначення x відбувається в такий спосіб:

Крок 1. Обчислюється вектор $\bar{b} = \bar{F}x$, x є розв'язок СЛАР

$$\bar{F}x = \bar{b} \tag{3.9}$$

За рахунок (8) елементи $\bar{b}$ можуть виявитися досить великими.

Крок 2. По $\bar{b}$ генерується вектор b^* за наступним правилом:

$$b_i^* = \begin{cases} \bar{b}_i, \text{ якщо } -15 \leq \bar{b}_i \leq 15, \\ -15, \text{ якщо } \bar{b}_i < -15 \\ 15, \text{ якщо } \bar{b}_i > 15 \end{cases}, \quad i = \overline{1, n} \tag{3.10}$$

а СЛАР (9) для відновлення x замінюємо на систему $\bar{F}x = b^*$. Оскільки $\bar{F}$ є нижньою трикутною, то кількість арифметичних операцій при розв'язку $\bar{F}x = b^*$ визначається як $O(n^2)$. Ця мета ставилася при кодуванні матриці вхідного зображення матрицею трикутного виду.

Зупинимося більш докладно на доцільності формування b^* відповідно до (10). Кодування F матрицею $\bar{F}$, в основному, зменшує значення елементів матриці, що дає можливість відповідного зменшення й елементів вектора $\bar{b} = \bar{F}x$ в порівнянні з $b = Fx$ (звичайно, якщо m не дуже велике), однак не гарантує їхньої малості. Якщо в якості правої частини системи, використовуваної для відновлення x , розглядати b (СЛАР (1)) або $\bar{b}$ (СЛАР (9)), то перед вбудовою такого вектора для забезпечення надійності сприйняття після вбудови, мабуть, буде потрібний який-небудь спосіб його кодування, наприклад, переведення у бінарну послідовність, що може значно збільшити довжину числової послідовності, що вбудовується. Отже, елементи вектора, що вбудовується, повинні бути настільки малими, щоб уникнути необхідності

якого-небудь кодування для зменшення потужності множини, що містить їхні можливі значення. Однак при виборі конкретних порогових значень в (10), 15 і -15, враховується не тільки ця вимога, до якої ще повернемося нижче.

При практичній реалізації методу встає питання вибору значення параметра m . Очевидно, значення m для забезпечення стійкості декодування повинно бути якнайбільше, хоча реально не може збільшуватися нескінченно; з іншого боку, m безпосередньо бере участь у формуванні елементів вектора $\bar{b}$, по якому генерується b^* . Чим більше буде m , тим більше будуть значення елементів $\bar{b}$, тим більше збурення отримає вектор b^* на етапі формування й, якби мова йшла про класичний розв'язок СЛАР, то такі збурення могли б привести до неприйнятної похибки декодування навіть із урахуванням малого числа обумовленості Скіла матриці системи. Однак, як буде показано нижче, використовуваний підхід до розв'язку системи дозволяє піти від негативних наслідків збурення вектора правої частини на етапі формування. Таким чином, пріоритетним залишається забезпечення стійкості декодування за рахунок вибору m .

Після формування вектора b^* він вбудовується в матрицю F контейнера. При пересиланні СП зазнає збурних дій у каналі зв'язку. Виділення інформаційного вектора x відбувається при розв'язку СЛАР

$$\bar{F}_B x_{np} = b_B^* \quad (3.11)$$

де $b_B^* = b^* + \delta b^*$ — збурений вектор b^* ; матриця $\bar{F}_B$ отримується по збуреній матриці $F_B = F + \delta F$ контейнера аналогічно (8).

Для більшості зображень при малих збуреннях у каналі зв'язку $\bar{F}_B \approx \bar{F}$, а $\|\bar{F}_B - \bar{F}\| \approx 0$. Дійсно, відмінність цих матриць може бути в елементах, що є результатом кодування елементів вхідної матриці, значення яких знаходяться в околі 127. Таким чином, можна вважати, що система (11) відрізняється від системи (9) лише вектором правої частини.

У кожному разі, очевидно, $x_{np} \neq x$. Враховуючи вид множини, якій належать елементи x , для здійснення остаточного декодування по наявному вектору x_{np} доцільно використовувати формулу

$$\bar{x}_i = \text{sign}(x_{np})_i, \quad i = \overline{1, n}. \quad (3.12)$$

Вектор $\bar{x}$ назовемо **sign-розв'язком** системи (11), а безпосередню реалізацію алгоритму, яка запропонована вище й використовує (12), будемо називати СМ-SIGN (реалізація СМ sign-розв'язку системи). Використання формули (12) при декодуванні допускає необмежено великі похибки при розв'язку (11), які ніяк не вплинуть на результат декодування, тобто $\|x_{np} - x\|$ може бути як завгодно велика, якщо при цьому виконуються умови:

$$\text{sign}(x_i) = \text{sign}((x_{np})_i), i = \overline{1, n}.$$

Таким чином, збурення правої частини системи при формуванні b^* , про які говорилося вище, що зберігають знаки елементів вектора розв'язку, не відображаються на результаті декодування, проведеного відповідно до (11), (12). Такий підхід до розв'язку системи є новим, він дає можливість, як показують результати обчислювального експерименту, наведені нижче, отримати великий обсяг P правильно відновленої інформації навіть при великих збуреннях вхідних даних, тобто пропонується реалізація методу SYSTEMA може забезпечувати його стійкість по відношенню навіть до необмежено великих збурних дій, що неможливо забезпечити при безпосередньому пересиланні вектора додаткової інформації.

Недоліком пропонованого методу SYSTEMA залишається обмеженість пропускної спроможності прихованого каналу зв'язку, що організується, оскільки довжина інформаційного вектора x не перевищує n . Збільшення обсягу переданої інформації може бути досягнуте в такий спосіб.

Нехай матриця розміру $n \times n$ відповідає контейнеру. Розіб'ємо її стандартним чином на квадратні блоки фіксованого малого розміру, наприклад, 8×8 . Нехай F — один з таких блоків. До кожного із блоків застосуємо запропонований вище CM-SIGN. Відмітимо, що кількість арифметичних операцій при роботі з F — константа, що не залежить від розміру матриці вхідного зображення. Позначимо її k . Кількість блоків визначається як $kol = \left\lceil \frac{n}{8} \right\rceil^2$, тоді загальна кількість арифметичних операцій при роботі з усім зображенням дорівнює $kol \cdot k = O(n^2)$, а сумарний обсяг інформації, що вбудовується, визначиться як $8kol = O(n^2)$, тобто виявляється на порядок більше, чим при розгляді матриці зображення цілком.

Таку модифікацію запропонованого методу далі будемо називати блоковою реалізацією CM sign-розв'язку системи (BCM-SIGN).

Основною метою обчислювального експерименту є практичне підтвердження теоретично обґрунтованої більшої стійкості до збурних дій у каналі зв'язку запропонованого CM із двоетапним декодуванням у порівнянні з методом, що використовує безпосереднє пересилання інформаційного вектора. Критерієм для такого порівняння є обсяг правильно відновленої інформації в тому й іншому випадку при однакових умовах проведення експерименту.

Обчислювальний експеримент проводився в середовищі Matlab. Збурення в каналі зв'язку моделювалися за допомогою аддитивного гауссівського шуму, накладання якого здійснювалося стандартною процедурою `imnoise`, з наступними параметрами: математичне очікування покладалося скрізь рівним нулю, а σ приймало значення 0.0001, 0.0005, 0.0008, 0.001, 0.01. Подальше збільшення рівня шуму приводило до втрати інформативності збуреного зображення й тому не розглядалося.

Для демонстрації результатів експерименту обрано два зображення-контейнера: POUT (рис.1(а)) і SATURN (рис.2). Вибір зроблений не випадково. Безпосередньо встановлюється, що матриця першого зображення є добре

обумовленою, а число обумовленості матриці другого зображення нескінченно велике.

Вбудова ДІ в контейнер проводилася в просторову область аддитивно у виділений попередньо контур, причому безпосередня вбудова x і вбудова b^* відбувалася в одні й ті самі пікселі контуру. В CM-SIGN порогові значення -15 і 15 у формулі (10) визначалися експериментально, виходячи з вимоги забезпечення надійності сприйняття СП після вбудови ДІ (рис.1(б)). На отримані СП накладався шум з однаковими параметрами (рис.1(в)), після чого відбувалося одноетапне або двоетапне (CM-SIGN) декодування вектора x (декодування b^* проводилося тим же способом, що і x).

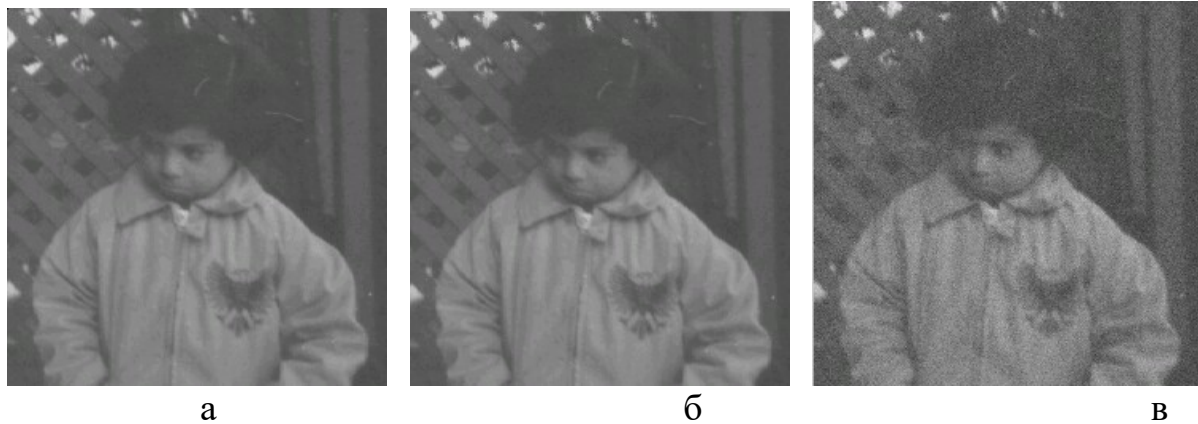


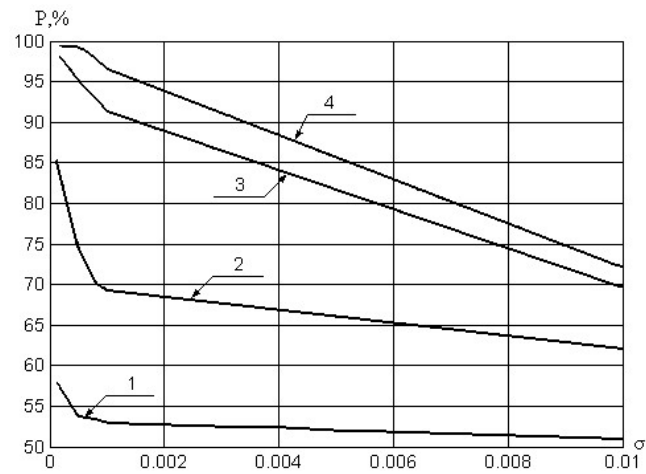
Рис.3.1. Подане зображення POUT (а); СП, сформоване CM-SIGN (б); СП, що зазнало збурення в вигляді аддитивного гауссівського шуму, що використовується для декодування (в)

У результаті обчислювального експерименту була встановлена залежність між рівнем збурних дій у каналі зв'язку й обсягом правильно відновленої інформації P , а також практично підтверджена незалежність результатів роботи СИСТЕМА від реальних властивостей матриці контейнера. Збільшення обсягу P досягалося шляхом варіювання m . Результати проведеного дослідження представлені на графіках залежності P від рівня шуму, характеристикою якого є середньоквадратичне відхилення, при різних значеннях m (рис.3). Для побудови графіків кожний з експериментів складався з 100 незалежних спроб, обумовлених однаковими параметрами. У якості результату експерименту (P при заданому шумі й значенні m) бралось середнє арифметичне значення по всіх 100 спробах.

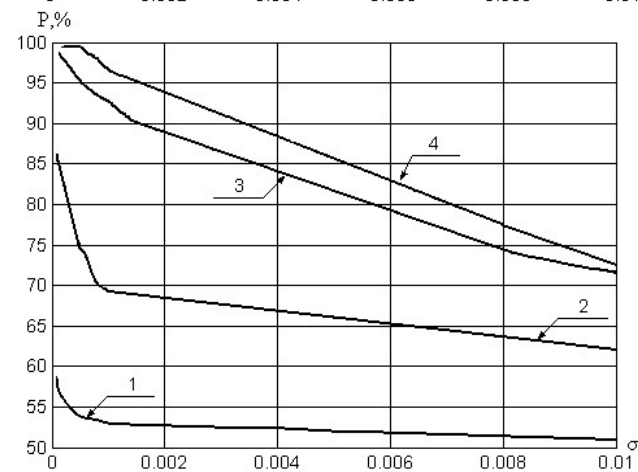


Рис. 2.Зображення SATURN

Результат роботи CM-SIGN, як і очікувалося, у силу віртуального моделювання властивості (б) для матриці системи, не залежить від реальних властивостей матриці зображення-контейнера (рис.3). CM-SIGN може використовуватися для контейнера із довільною матрицею і є більш стійким до збурень у каналі зв'язку в порівнянні з алгоритмом, що здійснює безпосереднє пересилання інформаційного вектора, навіть при досить малих значеннях m .



а



б

Рис. 3.3. Залежність P від σ : а – контейнер SATURN; б – контейнер POUT

1 — безпосереднє пересилання й декодування x ;
 2 — CM-SIGN при $m = 2$; 3 — CM-SIGN при $m = 10$; 4 — CM-SIGN при $m \geq 15$

Реалізація BCM-SIGN, що дає можливість на порядок збільшити пропускну спроможність, не змінила якісної картини роботи порівнюваних методів, описаної вище, як і можна було припустити заздалегідь. Результати знайшли своє відображення на рис.4 для зображення POUT (для зображення SATURN картина ідентична).

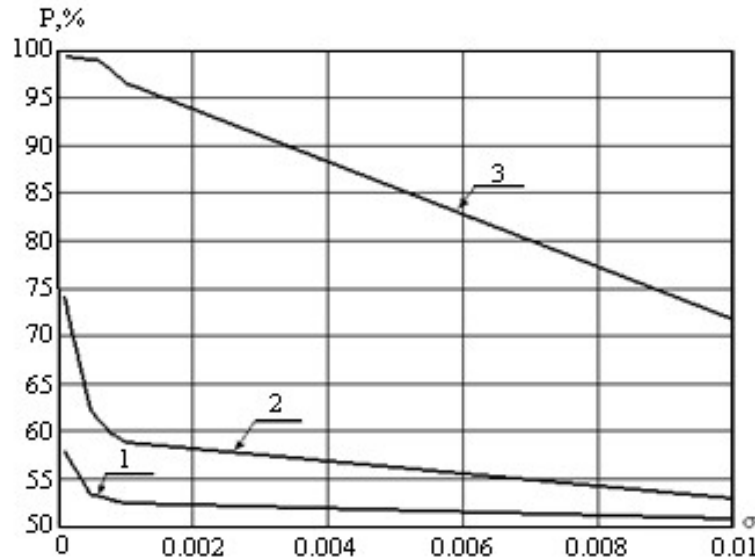


Рис.3.4. Залежність P від рівня шуму: 1 – безпосереднє пересилання і декодування x ; 2 – BCM-SIGN при $m=2$; BCM-SIGN при $m \geq 15$

Таким чином, розробка й практична реалізація CM SYSTEMA дала можливість підтвердити досягнення більшої стійкості методу до збурних дій у каналі зв'язку, у порівнянні з методом, заснованим на безпосередньому пересиланні й декодуванні інформаційного вектора. Цінність CM-SIGN полягає в тому, що він може бути використаний для довільного контейнера, а властивості матриці цього контейнера не впливають на результат декодування.

Запропонована чисельна реалізація методу вимагає $O(n^2)$ арифметичних операцій, де n — розмір матриці СЛАР.

Питання

1. Як визначається обсяг правильно відновленої інформації?
2. Яка задача називається чутливою до збурних дій?
3. Коли стеганоповідомлення називається чутливим до збурних дій?
4. Що таке число обумовленості задачі?
5. Що є мірою чутливості задачі до збурних дій?
6. Основна ідея методу двоетапного декодування. Пояснити.
7. Яким чином досягається зменшення числа обумовленості задачі декодування ДІ в методі двоетапного декодування? Пояснити.
8. Коли метод двоетапного декодування є стійким до атак проти вбудованого повідомлення? Пояснити.
9. Як забезпечується мале числа обумовленості матриці довільного зображення в методі двоетапного декодування? Чи завжди це можна зробити? Пояснити.
10. Яким чином будується матриця системи лінійних рівнянь на другому етапі методу двоетапного декодування при його практичній реалізації? Пояснити доцільність кроків, що використовуються.

- 11.Що таке sign-розв'язок системи лінійних рівнянь в методі двоетапного декодування? Чому його можна тут застосовувати? До чого приводить застосування sign-розв'язку в цьому методі?
- 12.Що є головним недоліком методу двоетапного декодування SYSTEMA? Як цей недолік можна зменшити? Пояснити.
- 13.Чи є обмеження на область застосування методу двоетапного декодування SYSTEMA? Відповідь детально пояснити.

Література

Базова

1. Г.Ф. Конахович, Д.О. Прогонов, О.Ю. Пузиренко, *Комп'ютерна стеганографічна обробка й аналіз мультимедійних даних: підручник*. Київ: Alex Print Centre, 2018. <https://books.google.com.ua/books?id=-clcDwAAQBAJ&printsec=frontcover#v=onepage&q&f=false>
2. Кузнецов О. О. Стеганографія : навчальний посібник / О. О. Кузнецов, С. П. Євсєєв, О. Г. Король. – Х. : Вид. ХНЕУ, 2011. – 232 с
3. Браїловський М.М. Аналіз кіберзахищеності інформаційних систем: монографія/ Браїловський М.М., Кобозєва А.А., Хорошко В.О., Хохлачева Ю.Є. – К.: ФОП Ямчинський О.В., 2021. – 360 с.

Допоміжна

1. Bobok I.I., Kobozeva A.A. Localization of Disturbance Region of Formal Parameters of Steganographic Cover to Ensure Steganosystem Stability. *Radioelectronics and Communications Systems*. 2024, 67(8), pp. 396-409.
2. Kobozeva A.A. et al. Method for Estimating the Bandwidth Capacity of a Steganographic Communication Channel/ PROBLEMELE ENERGETICII REGIONALE. 2(66). 2025 P.90-104 <https://journal.ie.asm.md/ru/contents/electronni-jurnal-266-2025>
3. Kobozeva A.A. et al. Increasing the Resistance of the Steganosystem to Attacks Against an Embedded Message by Selection of Container Blocks / 2024 IEEE 5th International Conference on Advanced Trends in Information Theory (ATIT), Lviv, Ukraine, 2024, pp. 264-269, doi: 10.1109/ATIT64324.2024.11222497
4. Kobozeva A.A. et al. Steganographic method with code control of information embedding based on multi-level code words/Radioelectronics and Communications Systems. 2023 <https://radioelektronika.org/article/view/S0735272723040052>
5. Корольов, В.Ю. Планування досліджень методів стеганографії та стеганоаналізу / В.Ю. Корольов, В.В. Поліновський, В.А. Герасименко, М.Л. Горінштейн // Вісник Хмельницького національного університету. — 2011. — № 4. — С. 187–196.
6. Miller, A. Least Significant Bit Embeddings: Implementation and Detection [Электронный ресурс]: Computer Science Honors Thesis. – 2012. – Режим доступа: <http://aaronmiller.in/thesis>.
7. Козіна М.О. Метод перевірки автентичності інформації, що передається стеганографічним каналом зв'язку / М.О. Козіна. // Вісник Вінницького політехнічного інституту. — 2015. — №1. — С. 99-104.
8. Fridrich J., Goljan M., Du R. Steganalysis based on JPEG compatibility // SPIE Multimedia Syst. and Appl. IV. – 2001. – P. 275–280. https://www.researchgate.net/publication/228575210_Steganalysis_based_on_JPEG_compatibility

9. Fridrich J., Goljan M. Practical steganalysis of digital images-state of the art // Proc. SPIE Photonics West, Electronic Imaging, Security and Watermarking of Multimedia Contents. — 2002. — 4675. — P. 1–13.
<http://www.ws.binghamton.edu/fridrich/Research/steganalysis01.pdf>
10. Friedrich, J. Steganalysis of LSB Encoding in Color Image / J.Friedrich, R. Du, M. Long // IEEE International Conference on Multimedia and Expo. — 2000. — Vol.3. — PP.1279–1282.
11. Geetha, S. Close color pair signature ensemble adaptive threshold based steganalysis for LSB embedding in digital images / S. Geetha, S. Sindhu, and N. Kamaraj // Transactions on Data Privacy. — 2009. — Vol. 1, Iss. 3. — PP. 140–161. <http://www.tdp.cat/issues/tdp.a007a08.pdf>
12. S.Mitra, T.Roy, D.Mazumdar and A.B.Saha. Steganalysis of lsb encoding in uncompressed images by close colour pair analysis
https://pdfs.semanticscholar.org/05b4/7dc5e5a736ffaa3cf33bb7276145f536b701.pdf?_ga=2.129946184.573026617.1584802876-1430525987.1550761339
13. Wen Chen. Study of steganalysis methods. A Thesis Submitted to the Faculty of New Jersey Institute of Technology in Partial Fulfillment of the Requirements for the Degree of Master of Science in Electrical Engineering Department of Electrical and Computer Engineering. January 2005.
<http://archives.njit.edu/vol01/etd/2000s/2005/njit-etd2005-006/njit-etd2005-006.pdf>
14. Узун, І.А. Стеганоаналіз цифрових зображень, збережених в довільних форматах / І.А.Узун // Інформатика та математичні методи в моделюванні. — 2013. — Т.3, №2. — С.179-189.
http://immm.opu.ua/files/archive/n2_v3_2013/n2_v3_2013.pdf
15. Information Hiding in Communication Networks: Fundamentals, Mechanisms, Applications, and Countermeasures / W. Mazurczyk et al. Hoboken: Wiley, 2016. 296 p.
16. Karampidis K., Kavallieratou E., Papadourakis G. A review of image steganalysis techniques for digital forensics. *Journal of Information Security and Applications*. 2018. 40. P. 217–235.
17. Chaeikar S.S., Ahmadi A. Ensemble SW image steganalysis: A low dimension method for LSBR detection. *Signal Processing: Image Communication*. 2019. 70. P. 233–245.
18. PSW statistical LSB image steganalysis / S. Shojae Chaeikar et al. *Multimedia Tools and Applications*. 2018. 77. P. 805–835.
19. Veena S.T., Arivazhagan S. Universal secret payload location identification in spatial LSB stego images. *Annals of Telecommunications*. 2019. 74. P. 273–286.
20. Bobok I.I., Kobozeva A.A. Steganalysis method efficient for the hidden communication channel with low capacity. *Радіотехніка*. 2019. 198. С. 19–31