ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ
КІБЕРБЕЗПЕКИ ТА ЗАХИСТУ ІНФОРМАЦІЇ
КАФЕДРА ТЕХНІЧНИХ СИСТЕМ КІБЕРЗАХИСТУ

КВАЛІФІКАЦІЙНА РОБОТА

на тему:

«Удосконалення системи захисту конфіденційних даних при передачі інформації стеганографічними методами»

на здобуття освітнього ступеня магістра
зі спеціальності __125 - _Кібербезпека та захист інформації»_____
(код, найменування спеціальності)
освітньо-професійної програми Технічні системи інформаційного та кібернетичного захисту

Кваліфікаційна робота містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело
_____ Олександр МЕРКУЛОВ_

Виконав: здобувач вищої освіти групи СЗДМ-61
Олександр МЕРКУЛОВ

Керівник:_____Олександр ТУРОВСЬКИЙ_____
д.т.н., професор Ім'я, ПРІЗВИЩЕ

Рецензент:_____
Ім'я, ПРІЗВИЩЕ

Київ 2025

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ
КІБЕРБЕЗПЕКИ ЗАХИСТУ ІНФОРМАЦІЇ

Кафедра ___Технічних систем кіберзахисту_____
Ступінь вищої освіти ____магістр_____
Спеціальність ___Кібербезпека та захист інформації_____
Освітньо-професійна програма _Технічні системи інформаційного та кібернетичного захисту

ЗАТВЕРДЖУЮ
Завідувач кафедри ТСКБ
_____Олександр ТУРОВСЬКИЙ

«____» _____ 2024 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУРОБОТУ

Меркулову Олександру Сергійовичу
(прізвище, ім'я, по батькові здобувача)

1. Тема кваліфікаційної роботи:
«Удосконалення системи захисту конфіденційних даних при передачі інформації стеганографічними методами»
керівник кваліфікаційної роботи ____ТУРОВСЬКИЙ Олександр д.т.н., професор

затверджені наказом Державного університету інформаційно-комунікаційних технологій
від « 15 » жовтня 2024 р. № 320

2. Строк подання кваліфікаційної роботи 14.12.2024 р.

3. Вихідні дані до кваліфікаційної роботи: Загрози витоку інформації стеганографічним каналом. Система захисту для протидії витоку конфіденційних даних та стегоаналізу. Надійність захисту інформації.

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)
1.__ Огляд технології стеганографічного захисту даних в системі захисту інформації об'єкту інформаційної діяльності___
2.__Дослідження можливостей застосування методів стеганографії та стеганоаналізу при забезпеченні захисту конфіденційних даних на об'єкті інформаційної діяльності._____
3.__Розробка рекомендацій по комбінованому захисту конфіденційних даних з використанням методів стеганографії та криптографії

5. Перелік графічного матеріалу: ___Презентаційний матеріал на_____слайдах_____
_____

6. Дата видачі завдання _____20.10.2024 ___ _____

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1	Підбір науково-технічної літератури		
2	Написання першого розділу роботи		
3	Написання другого розділу роботи		
4	Написання третього розділу роботи		
5	Написання висновків по роботі		
6	Підготовка демонстраційних матеріалів		
7	Підготовка доповіді		

Здобувач вищої освіти _____ Олександр МЕРКУЛОВ
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

Керівник роботи _____ Олександр ТУРОВСЬКИЙ
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

РЕФЕРАТ

Текстова частина магістерської кваліфікаційної роботи: стор., рис., табл., джерел.

Об'єкт дослідження – Стеганографічні методи захисту інформації.

Предмет дослідження – Методи стеганографічного захисту конфіденційних даних при їх передачі.

Мета роботи – Удосконалити системи передачі конфіденційних даних стеганографічними методами.

Методи дослідження – системний аналіз, опрацювання літератури за даною темою.

У роботі проаналізовано методи стеганографічного захисту. Розглянуто можливість використання стеганографії для захисту конфіденційних даних.

Ґрунтуючись на проведеному досліджені було удосконалено стеганографічний метод захисту інформації та підвищено його надійність від витоку конфіденційних даних.

Галузь використання – захист конфіденційних даних на об'єкті інформаційної діяльності.

Апробація:

О.С. Меркулов Удосконалення системи захисту конфіденційних даних при передачі інформації стеганографічними методами*: Актуальні проблеми безпеки інформаційно-телекомунікаційних систем*. м. Київ, 03 листопада 2024 року, Київ: РВЦ ДУІКТ. – 024. С.21 - 22. https://duikt.edu.ua/uploads/p_2661_93669247.pdf

Ключові слова: СТЕГАНОГРАФІЧНИЙ КАНАЛ, ЗАГРОЗИ ІНФОРМАЦІЇ, СТЕГОАНАЛІЗ, ЗАХИСТ КОНФІДЕНЦІЙНИХ ЗАХИСТ, ШИФРУВАННЯ, ІДЕНТИФІКАЦІЯ.

ABSTRACT

The text part of the master's qualification work: pages, figures, tables, sources.

The object of research is steganographic methods of information protection.

The subject of the research is methods of steganographic protection of confidential data during their transmission.

The purpose of the work is to improve systems for transmitting confidential data using steganographic methods.

Research methods – system analysis, numerical methods, literature review on this topic.

The work analyzes the methods of steganographic protection. The possibility of using steganography to protect confidential data is considered.

Based on the conducted research, the steganographic method of information protection was improved and its reliability against leakage of confidential data was increased.

Approbation:

O.S. Merkulov Improvement of the system of protection of confidential data when transmitting information by steganographic methods: Current problems of security of information and telecommunication systems. Kyiv, November 03, 2024, Kyiv: RVC DUIKT. – 024. P.21 - 22. https://duikt.edu.ua/uploads/p_2661_93669247.pdf

Field of use – protection of confidential data at the object of information activity.

STEGANOGRAPHIC CHANNEL, INFORMATION THREATS, STEGOANALYSIS, PRIVACY PROTECTION, ENCRYPTION, IDENTIFICATION.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ 9
ВСТУП 10
РОЗДІЛ1. ТЕОРЕТИЧНІ ОСНОВИ СТЕГАНОГРАФІЇ ТА ЇЇ РОЛЬ У ЗАБЕЗПЕЧЕННІ КІБЕРБЕЗПЕКИ 12
1.1 Загальне про стеганографію 12
1.2 Стегонаграфія через історію 13
1.3 Сучасна стеганографія 16
1.4 Принцип роботи стеганографії 17
1.5 Типи стеганографії 18
1.5.1 Текстова стеганографія 18
1.5.2 Стеганографія в зображеннях 19
1.5.3 Стеганографія в відео 19
1.5.4 Стеганографія в аудіо 19
1.5.5 Стеганографія в мережах 20
1.6 Використання стеганографії 20
1.7 Роль стеганографії в кібербезпеці 21
1.7.1 Зі сторони кіберзахисту: 21
1.7.2 Зі сторони кіберзлочинця: 22
1.8 Використання стеганографії у кібератаках 23
1.9 Приклади використання стеганографії в кібератаках. 24
1.10 Захист від атак с використанням стеганографії 25
1.11 Виявлення та протидія стеганографії 26
1.11.1 Візуальна перевірка 26
1.11.2 Статистичний аналіз 26
1.11.3 Інструменти стеганалізу 26
1.11.4 Перевірка цілісності файлів 27
1.11. 5Аналіз мережевого трафіку 27
1.11.6 Фільтрація контенту 27
1.11.7 Освіта та обізнаність користувачів 27
1.12 Стеганографія та водяні знаки 28
1.13 Стеганографія vs криптографія 29
1.14 Стеганографія та NFT 29
1.15 Висновок до першого розділу 30
РОЗДІЛ2. КОМПЛЕКСНЕ ДОСЛІДЖЕННЯ МЕТОДІВ СТЕГАНОГРАФІЇ ТА СТЕГОАНАЛІЗУ 31
2.1 Формати цифрового зображення 31

2.1.1 Представлення кольору 31
2.1.2 Вибірка кольорів 34
2.2 Стеганографічний канал 35
2.3 Стеганографія за вибором об'єкта 38
2.3 Стеганографія за допомогою синтезу покриття 39
2.4 Стеганографія через модифікацію контейнера 42
2.5 LSB-впровадження 47
2.6 Атака на гістограму 53
2.7 Кількісний напад на Jsteg 55
2.8 Практичні стеганографічні методи 58
2.8.1 Стеганографія, що зберігає модель 59
2.8.2 Статистичне відновлення 59
2.8.3 Стеганографія на основі моделей 62
2.8.4 Стеганографія шляхом імітації природного оброблення 67
2.8.5 Стохастична модуляція 68
2.9 Питання оптимального стего шуму 72
2.10 Стегоаналіз 75
2.11 Типові сценарії 76
2.11.1 Статистичний стегоаналіз 78
2.11.2 Стеганоаналіз як проблема виявлення 78
2.11.3 Моделювання зображень за допомогою ознак 79
2.12 Отримувач операційної характеристики (ROC) 82
2.13 Висновок до другого розділу 85
РОЗДІЛ3. ПРАКТИЧНА РЕАЛІЗАЦІЯ КОМБІНОВАНОГО ЗАХИСТУ КОНФІДЕНЦІЙНИХ ДАНИХ З ВИКОРИСТАННЯМ СТЕГАНОГРАФІЇ ТА КРИПТОГРАФІЇ 86
3.1 Використані інструменти та технології 86
3.1.1 Python 86
3.1.2 Django 86
3.1.3 Комбінація HTML та CSS: 87
3.1.4 SQL 88
3.1.5 AES-256 Encryption 88
3.1.6 Least Significant Bit (LSB) Steganography 89
3.2 Демонстрація розробленого рішення. 93
3.3 Висновок до третього розділу. 97
ВИСНОВКИ 98
ДОДАТКИ 101

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

ПЗ – програмне забезпечення.

SPIE (the international society for optics and photonics) – спільнота оптики та фотоніки

IEEE(ICIP) (international conference on image processing) - міжнародна конференція з обробки зображень.

LSB (Least Significant Bit) – найменш значущий біт.

SVG (Scalable Vector Graphics) – масштабована векторна графіка.

NIDS (network intrusion detection system) – система виявлення вторгнення.

NFT (non-fungible token) - незамінний токен.

RGB (Red, Green, Blue) – модель кольорів.

CMY (Cyan, Magenta, Yellow) – модель кольорів.

TIFF (Tagged Image File Format) – формат зображення.

JPEG (Joint Photographic Experts Group) - формат зображення.

MPEG (Moving Picture Experts Group) – формат рухомого зображення.

DKL (Kullback–Leibler divergence) - дивергенція Кульбака-Лейблера.

ROC (receiver operating characteristic) - отримувач операційної характеристики.

HTML (HyperText Markup Language) – мова гіпертекстової розмітки.

CSS (Cascading Style Sheets) – каскадні таблиці стилів.

SQL (Structured Query Language) – мова структурованих запросів.

AES (Advanced Encryption Standard) – симетричний алгоритм блочного шифрування.

ВСТУП

Актуальність дослідження. У сучасному світі, де інформація є одним із найцінніших ресурсів, захист конфіденційних даних стає ключовим завданням для багатьох сфер діяльності: від державного управління до приватного бізнесу. Традиційні методи шифрування забезпечують високий рівень безпеки, але часто привертають увагу зловмисників через сам факт наявності зашифрованих даних. У таких умовах стеганографія, яка дозволяє приховати сам факт існування передаваних даних, стає важливим елементом систем захисту інформації.

Стеганографія, як наука та практичний інструмент, пропонує широкий спектр методів приховування інформації в цифрових носіях, таких як зображення, аудіо- та відеофайли, забезпечуючи її передачу без явних ознак втручання в структуру файлу. Проте стрімкий розвиток технологій і зростання обсягів цифрового трафіку породжують нові виклики. Зокрема, виникає необхідність підвищення стійкості стеганографічних методів до виявлення за допомогою стегоаналізу, а також удосконалення алгоритмів приховування інформації для роботи з різними форматами даних.

Актуальність дослідження обумовлена потребою в ефективних та надійних системах захисту конфіденційної інформації в умовах сучасного інформаційного простору, де загрози кіберзлочинності, промислового шпигунства та несанкціонованого доступу стають дедалі серйознішими. Використання стеганографії у поєднанні з іншими методами захисту даних відкриває нові можливості для забезпечення інформаційної безпеки, особливо в критично важливих сферах, таких як банківська система, оборона та медицина.

Метою цієї магістерської роботи є вдосконалення системи захисту конфіденційних даних при передачі інформації стеганографічними методами шляхом розробки та аналізу нових підходів до приховування даних і підвищення їх стійкості до виявлення. У рамках дослідження будуть розглянуті сучасні методи стеганографії, проаналізовано їх сильні та слабкі сторони, а також запропоновано удосконалення алгоритмів для підвищення ефективності захисту.

Об'єкт дослідження – Стеганографічні методи захисту інформації.

Предмет дослідження – Методи стеганографічного захисту конфіденційних даних при їх передачі.

Мета роботи – Удосконалити системи передачі конфіденційних даних стеганографічними методами.

Методи дослідження – системний аналіз, опрацювання літератури за даною темою.

Наукові завдання:

дослідити методи стеганографічного захисту на об'єкт інформаційної діяльності;

проаналізувати ймовірні загрози на об'єкти інформаційної діяльності;

удосконалити систему захисту конфіденційних даних з використанням стеганографії.

Практичне значення одержаних результатів полягає у удосконалені системи захисту конфіденційних даних с використанням комбінованого стеганографічно-криптографічного захисту.

РОЗДІЛ1.
ТЕОРЕТИЧНІ ОСНОВИ СТЕГАНОГРАФІЇ ТА ЇЇ РОЛЬ У ЗАБЕЗПЕЧЕННІ КІБЕРБЕЗПЕКИ

1.1 Загальне про стеганографію

Стеганографія це один зі способів для скритої комунікації. Вона працює приховуючи повідомлення в непримітних об’єктах які надсилаються до запланованих отримувачів. Найбільш важливою вимогою до будь-якої стеганографічної системи це те, що особа яка не має допуску до інформації не повинна розрізняти звичайні об’єкти, та об’єкти що містять секретні дані.

Сучасна стеганографія відносно молода. До початку 1990-х років цей незвичний спосіб таємного спілкування використовувався переважно шпигунами. На той час це навряд чи можна було назвати дослідницькою дисципліною, оскільки методи були простою колекцією хитрих прийомів без теоретичної основи, яка дозволила б стеганографії розвиватися так, як ми це бачимо сьогодні. З подальшим спонтанним переходом комунікацій від аналогових до цифрових, ця давня галузь пережила вибухове оновлення. Приховування повідомлень в електронних документах з метою прихованого спілкування здавалося достатньо простим для тих, хто мав базові знання з програмування. Незабаром стеганографічні додатки з'явилися в Інтернеті, надаючи широким масам можливість приховувати файли в цифрових зображеннях, аудіо або текстах. Одночасно стеганографія привернула увагу науковців і швидко розвинулася в сувору дисципліну. Завдяки цьому стеганографія вийшла на передній план обговорень на професійних зустрічах, таких як щорічні збори SPIE з електронної обробки зображень у Сан-Хосе, Міжнародна конференція з обробки зображень IEEE (ICIP) та ACM Multimedia and Security Workshop. У 1996 році перший семінар з приховування інформації відбувся в Кембриджі, і з того часу ця серія семінарів стала провідним щорічним місцем для презентації останніх досягнень у теорії та застосуванні приховування даних.

Стеганографія має багато спільних рис із суміжною, але фундаментально іншою галуззю цифрового водяного знака. Наприкінці 1990-х років цифрові водяні знаки домінували в дослідженнях приховування даних завдяки численним вигідним застосуванням, таким як управління цифровими правами, безпечний розподіл медіафайлів і автентифікація. У міру розвитку водяних знаків інтерес до стеганографії та стеганалітики поступово зростав, особливо після того, як з'явилися побоювання, що стеганографія може бути використана злочинцями.

Тип носія	Кількість
Аудіо	445
Диск	416
Фото	1689
Мережа	39
Інше	81
Текст	255
Відео	86

Рис. 1.1 - Кількість стеганографічних програм, які можуть приховувати дані в електронних носіях станом на червень 2008 р.

1.2 Стегонаграфія через історію

Слово "стеганографія" є складовим з грецьких слів "steganos", що означає "покритий", і "graphia", що означає "писання". Іншими словами, стеганографія – це мистецтво прихованого спілкування, коли сама наявність повідомлення є секретною. Термін "стеганографія" вперше був використаний Йоганном Трітемієм (1462–1516) у його трилогії "Поліграфія" та "Стеганографія". Перші два томи описували давні методи шифрування повідомлень (криптографія), а третій том (1499 рік), здавалося, був присвячений окультним силам, чорній магії та методам спілкування з духами. Том був опублікований у Франкфурті в 1606 році, а в 1609

році Католицька Церква внесла його до списку "libri prohibiti" (заборонених книг). Незабаром вчені почали підозрювати, що книга містить код, і намагалися розгадати її таємницю. Зусилля з розшифровки таємного повідомлення книги увінчалися успіхом у 1996 та 1998 роках, коли двоє дослідників незалежно розкрили приховані повідомлення, зашифровані в числах через кілька таблиць відповідностей, що містилися в книзі. Повідомлення виявилися досить буденними. Перше було латинським еквівалентом речення: "Швидкий бурий лис перестрибує через ледачого собаку," яке містить усі літери алфавіту. Друге повідомлення було таким: "Носій цього листа є шахраєм і злодієм. Остерігайтеся його. Він хоче щось зробити вам." Нарешті, третє було початком 21-го Псалма.

Перше письмове свідчення про використання стеганографії для передачі повідомлень належить Геродоту, який розповідає про раба, якого його господар Гістіей відправив до іонійського міста Мілет із таємним повідомленням, витатуйованим на його голові. Після нанесення татуювання раб відростив волосся, щоб приховати повідомлення. Він подорожував до Мілета і, прибувши, поголив голову, щоб показати повідомлення регенту міста Арістагору. У повідомленні Арістагору рекомендували почати повстання проти перського царя. Геродот також задокументував історію Демарата, який використовував стеганографію, щоб попередити Спарту про заплановане вторгнення до Греції перського царя Ксеркса. Щоб приховати своє повідомлення, Демарат зішкреб віск із поверхні дерев'яної таблички, вирізав повідомлення на дереві, а потім знову покрив табличку шаром воску, щоб вона виглядала як звичайна чиста табличка, яку можна було безпечно доставити до Спарти без викликання підозр. Еней Тактик вважається винахідником багатьох винахідливих стеганографічних методів, таких як приховування повідомлень у жіночих сережках або використання голубів для доставки таємних повідомлень. Крім того, він описав кілька простих методів приховування повідомлень у тексті, змінюючи висоту штрихів літер або позначаючи літери в тексті маленькими отворами.

У 1966 році винахідливий і спонтанний стеганографічний метод дозволив військовополоненому, командору Джеремі Дентоуну, таємно передати одне слово,

коли його в'єтнамські полонителі змусили його дати інтерв'ю на телебаченні. Знаючи, що він не може сказати нічого критичного про своїх полонителів, він під час розмови моргав очима в азбуці Морзе, викладаючи слово T-O-R-T-U-R-E (тортури). Стеганографія стала предметом суперечки під час матчу між Віктором Корчним і Анатолієм Карповим за звання чемпіона світу з шахів у 1978 році. Під час однієї з партій помічники Карпова подали йому піднос із йогуртом. Це було технічно проти правил, які забороняли контакт між гравцем і його командою під час гри. Глава делегації Корчного, Петра Левверік, негайно висловила протест, стверджуючи, що команда Карпова могла передавати йому таємні повідомлення. Наприклад, фіолетовий йогурт міг означати, що Карпов має запропонувати нічию, тоді як шматочок манго міг повідомити гравця про відмову від пропозиції нічиєї. Час подачі їжі також міг використовуватися для передачі додаткових повідомлень (стеганографія в каналах часу). Цей протест, який був наслідком параної, що панувала на шахових матчах під час Холодної війни, був сприйнятий досить серйозно. Офіційні особи дозволили Карпову вживати лише один вид йогурту (фіолетовий) у певний час під час гри. Використовуючи термінологію цієї книги, ми можемо трактувати цей захід як дію активного наглядача, спрямовану на запобігання використанню стеганографії.

Останній вибух інтересу до стеганографії зумовлений досить раптовим і широким використанням цифрових медіа, а також стрімким розширенням Інтернету (на Рис. 1.1 показана річна кількість дослідницьких статей на тему стеганографії, опублікованих IEEE). Сьогодні стало звичною практикою ділитися з друзями та родиною зображеннями, відео та звуками. Такі об'єкти створюють дуже сприятливе середовище для приховування таємних повідомлень з однієї важливої причини: типові цифрові медіафайли складаються з великої кількості окремих елементів (наприклад, пікселів), які можна непомітно змінити для кодування таємного повідомлення. І немає потреби в технічній експертизі для тих, хто бажає використовувати стеганографію, оскільки сам процес приховування може бути виконаний за допомогою комп'ютерної програми, яку будь-хто може безкоштовно завантажити з Інтернету. Станом на кінець 2008 року, коли писалася

ця книга, можна вибрати з кількох сотень стеганографічних продуктів, доступних в Інтернеті. На Рис. 1.2 показано кількість нових програм або нових версій існуючих програм, здатних приховувати дані в цифрових медіа та текстах. Деякі програмні додатки, які орієнтовані на безпеку, конфіденційність і анонімність, пропонують можливість приховувати зашифровані повідомлення в зображеннях і музиці як додатковий рівень захисту.

1.3 Сучасна стеганографія

Оскільки електронні комунікації дуже вразливі до прослуховування та зловмисних втручань, питання безпеки та конфіденційності сьогодні актуальні як ніколи. Традиційні рішення базуються на криптографії, яка є зрілою, добре розвиненою галуззю з суворими математичними основами.

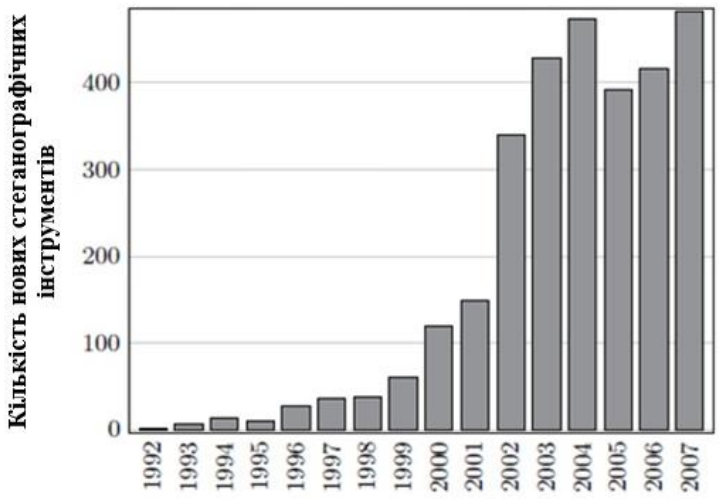


Рис 1.2 - Кількість нещодавно випущених програм стеганографічного програмного забезпечення або нових версій на рік.

Криптографічний підхід до конфіденційності полягає в тому, щоб зробити обмінювану інформацію нерозбірливою для тих, хто не має правильного ключа для дешифрування. Коли зашифроване повідомлення перехоплюється, навіть якщо зміст повідомлення захищений, очевидним залишається той факт, що суб'єкти

ведуть таємне спілкування. У деяких ситуаціях може бути важливо уникнути привернення уваги і натомість вбудувати конфіденційні дані в інші об'єкти, щоб сам факт передачі таємної інформації не був помітним. Саме такий підхід використовує стеганографія.

Стеганографія пропонує реальну альтернативу шифруванню в репресивних режимах, де використання криптографії може привернути небажану увагу, або в країнах, де шифрування юридично заборонено. Цікавий задокументований випадок використання стеганографії був представлений на 4-й Міжнародній конференції з приховування інформації. Два суб'єкти розробили власну стеганографічну схему для приховування повідомлень у нестиснених цифрових зображеннях і успішно використовували її протягом кількох років, коли один із них перебував у ворожій країні, де шифрування було прямо заборонено. Причиною їхньої параної була історія, розказана їхнім другом, який уже проживав у цьому регіоні, і який спробував надіслати зашифрований електронний лист, але його було повернуто місцевим інтернет-провайдером із повідомленням: "Будь ласка, не надсилайте зашифровані листи – ми не можемо їх прочитати."

На початку 1980-х років Сіммонс описав цікаві політичні наслідки можливості надсилати дані через прихований канал зв'язку. Відповідно до договору про роззброєння ОСО, США та Радянський Союз взаємно домовилися оснастити свої ядерні об'єкти датчиками, які повідомляли б іншій стороні кількість ракет, але не таку інформацію, як їхнє місце розташування. Усі комунікації повинні були бути захищені за допомогою стандартних цифрових підписів, щоб запобігти несанкціонованій зміні показників датчиків. Однак обидві сторони швидко занепокоїлися можливістю приховування додаткової інформації через так звані сублімінальні канали, які існували у більшості схем цифрового підпису на той час. Це призвело до досліджень у напрямку розробки цифрових підписів, вільних від сублімінальних каналів.

1.4 Принцип роботи стеганографії

Принцип роботи стеганографії базується на приховувані інформації таким чином, щоб вона не викликала підозри. Однією з найпопулярніших технік є стеганографія найменш значущого біта (LSB). Цей метод полягає в тому, що секретні дані вбудовуються в найменш значущі біти цифрового файлу. Наприклад:

Кожен піксель зображення включає в собі три байти даних, що відповідають кольорам червоного, зеленого і синього. Але в деяких форматах присутній четвертий байт для прозорості, який називається "альфа". LSB-стеганографія змінює найменш значущий біт кожного з байтів для приховування біта конфіденційної інформації. Тому, щоб приховати один мегабайт даних, потрібно вісім мегабайтів зображення. При зміні останнього біта пікселя не викликає видимих змін в зображені, тому при порівнянні оригіналу і зміненого стеганографічно зображення різниця буде майже непомітною. Цей підхід можна використовувати майже в усіх цифрових медіа, таких як аудіо- та відеофайли, де дані приховуються в тих частинах, які викликають найменші зміни в звукових або візуальних ефектах.

1.5 Типи стеганографії

Наразі, існує п’ять основних типів стеганографії це:

1.5.1 Текстова стеганографія

Текстова стеганографія приховує конфіденційні дані або секретні повідомлення в звичайному тексті. Цей метод використовується в комунікаційних каналах, таких як електронні листи, публікації на форумах або повідомлення в соціальних мережах. Для вбудовування прихованих повідомлень можна застосовувати різні техніки.

Прості методи, такі як тонкі зміни в форматуванні тексту, наприклад, використання специфічних знаків пунктуації або шаблонів пробілів, можуть бути використані. Більш складні методи, такі як застосування стеганографічних

алгоритмів для кодування інформації безпосередньо в тексті, також можуть бути використані для підвищення надійності захисту.

1.5.2 Стеганографія в зображеннях

Стеганографія в зображеннях — це техніка, що використовується для приховування секретної інформації в цифрових зображеннях. За допомогою цього методу надлишкові дані, що присутні в файлах зображень, можуть бути тонко змінені без суттєвих змін візуального вигляду зображення для людського ока.

Одним з поширених підходів є маніпулювання найменш значущими бітами (LSB) значень пікселів, що дозволяє кодувати двійкові дані в зображенні без помітних спотворень. Техніки, такі як приховування в просторовій області, також можуть вбудовувати одне зображення в інше шляхом стратегічного модифікування певних областей або кольорових каналів зображення.

1.5.3 Стеганографія в відео

Стеганографія в відео передбачає приховування відео в іншому мультимедійному контенті. Цей метод використовує тимчасову безперервність між послідовними кадрами відео, що дозволяє безшовно вбудовувати приховану інформацію в потік відео.

Однією з технік, що використовуються, є кодування окремих кадрів прихованого відео в відповідні кадри відео-покриття. Інші техніки включають використання векторів руху та маніпулювання певними компонентами відеоданих.

1.5.4 Стеганографія в аудіо

Аудіо стеганографія передбачає приховування секретних повідомлень в аудіофайлах при збереженні сприйнятної якості звуку. Цей метод використовує обмежену чутливість людської слухової системи до тонких змін в звукових хвилях, що дозволяє вносити непомітні зміни в аудіо зразки.

Деякі з поширених технік аудіо стеганографії включають модифікацію найменш значущих бітів (LSB) аудіо зразків для кодування прихованих даних або вбудовування повідомлень у специфічні частотні діапазони, щоб мінімізувати чутні артефакти.

1.5.5 Стеганографія в мережах

Мережна стеганографія приховує інформацію в мережевих комунікаціях, щоб уникнути виявлення механізмами безпеки. Цей метод в основному використовується зловмисниками, оскільки він використовує вроджену надмірність і змінність мережевих протоколів, що дозволяє таємно вбудовувати дані в заголовки пакетів, корисні навантаження або в патерни передачі.

Техніки, що використовуються в мережевій стеганографії, включають вбудовування даних у невикористовувані поля мережевих протоколів та маніпулювання характеристиками часу мережевих пакетів.

1.6 Використання стеганографії

В нинішній час стеганографія в основному використовується на комп'ютерах, цифрових даних, а канали високошвидкісної доставки — мережами.

При використанні стеганографії передбачається:

Уникнення цензури: Може бути використана для передачі нової інформації уникаючи цензури та без страху, що повідомлення буде відстежено до відправника.

Цифрові водяні знаки: Також використовується для створення невидимих водяних знаків, які не спотворюють зображення і які все ще можна відстежувати, щоб перевірити, чи було воно використано без дозволу.

Захист інформації: Використовується системою правоохоронних органів та урядовими установами для передачі надзвичайно чутливої інформації іншим сторонам без подальшого її розповсюдження.

1.7 Роль стеганографії в кібербезпеці

1.7.1 Зі сторони кіберзахисту:

Захист даних та конфіденційність

ІТ-спеціалісти та фахівці з безпеки використовують стеганографію як захисний захід для захисту чутливих даних і підвищення конфіденційності. Вони можуть застосовувати стеганографічні техніки для приховування конфіденційної інформації, такої як ключі шифрування або облікові дані для автентифікації, всередині цифрових активів. Приховуючи критичні дані в безневинних файлах або комунікаціях, організації можуть захиститися від несанкціонованого доступу та витоків даних.

Стеганографію також використовують фахівці з кібербезпеки для цифрового водяного знака та захисту авторських прав. Вбудовуючи унікальні ідентифікатори або інформацію про право власності в мультимедійний контент, такий як зображення або відео, організації можуть запобігти несанкціонованому використанню або розповсюдженню інтелектуальної власності. Прихована інформація, вбудована у файли, може бути використана як доказ у випадку порушення авторських прав.

Контррозвідка та судова експертиза

Стеганографію використовують у контррозвідці та цифрових судових розслідуваннях для виявлення та аналізу прихованої інформації в цифрових активів. ІТ-спеціалісти та фахівці з безпеки можуть застосовувати спеціалізовані техніки стеганоаналізу для виявлення прихованих комунікацій, шкідливих завантажень або зашифрованих даних, прихованих за допомогою стеганографічних методів.

Аналізатори кібербезпеки також можуть використовувати стеганографію для виявлення потенційних загроз безпеці та пом'якшення ризиків, пов'язаних з прихованим шкідливим ПЗ або витоком даних. Це здійснюється шляхом

ретельного аналізу підозрілих файлів або мережевого трафіку на наявність ознак стеганографічної маніпуляції.

1.7.2 Зі сторони кіберзлочинця:

Приховування злочинної діяльності

Зловмисники часто використовують стеганографію для приховування своїх дій, щоб уникнути виявлення системами безпеки. Наприклад, вони можуть вбудовувати шкідливе ПЗ, таке як віруси або трояни, у здавалося б безневинні файли, такі як зображення або документи, використовуючи стеганографічні техніки. Це дозволяє їм обходити традиційні засоби безпеки, такі як антивірусне програмне забезпечення, яке може не виявляти приховане шкідливе ПЗ.

Стеганографію також використовують кіберзлочинці для приховування вкрадених даних, таких як фінансова інформація або інтелектуальна власність, під час ексфільтрації з скомпрометованих систем. Приховуючи чутливі дані в файлах або комунікаціях, які виглядають безневинно, зловмисники можуть уникати виявлення засобами моніторингу безпеки.

Приховане спілкування

Стеганографія дозволяє хакерам встановлювати приховані канали зв’язку для обміну інструкціями, командами або вкраденою інформацією зі скомпрометованими системами. Вбудовуючи повідомлення в здавалося б безневинні файли або мережевий трафік, зловмисники можуть спілкуватися з зараженими точками безпеки, не викликаючи підозр.

Кримінальні групи також можуть використовувати стеганографію для координації незаконної діяльності, такої як розповсюдження піратського контенту, здійснення фінансового шахрайства або організація кібератак. Приховуючи комунікації в цифровому контенті, вони можуть уникати спостереження та зусиль правоохоронних органів з перехоплення незаконної діяльності.

1.8 Використання стеганографії у кібератаках

З точки зору кібербезпеки, зловмисники можуть застосовувати стеганографію для прихованого впровадження шкідливих даних у файли, які на перший погляд здаються безпечними. Оскільки стеганографія потребує ретельної підготовки та значного рівня майстерності для досягнення бажаного ефекту, її використання зазвичай асоціюється з цілеспрямованими атаками, здійснюваними висококваліфікованими загрозами. Нижче описано кілька методів здійснення атак із застосуванням стеганографії:

Приховування шкідливого коду в цифрових медіа: Зображення часто стають об’єктами атак через значну кількість надлишкових даних, які можна змінювати без видимих порушень їхньої структури або вигляду. Крім зображень, для розміщення шкідливого навантаження за допомогою стеганографії також використовуються відеофайли, документи, аудіофайли та навіть підписи в електронній пошті.

Вимагачі та крадіжка даних: Кіберзлочинці, що займаються вимагачами, можуть використовувати стеганографію для приховування даних під час атак. Цей метод дозволяє заховати чутливу інформацію в легітимних комунікаціях, що дає змогу отримати дані без виявлення.

Приховування команд на веб-сторінках: Зловмисники можуть використовувати веб-сторінки для приховування команд, які керують їхніми імплантами, застосовуючи пробіли або журнали налагодження, опубліковані на форумах. Такий підхід дозволяє таємно передавати вкрадені дані та підтримувати активність за допомогою зашифрованого коду.

Шкідлива реклама: Зловмисники можуть застосовувати стеганографію в рекламних кампаніях, вбудовуючи шкідливий код у банерну рекламу. Після завантаження таких банерів код витягується та перенаправляє користувачів на сторінки з експлойтами.

1.9 Приклади використання стеганографії в кібератаках.

Скімінг електронної комерції: У 2020 році платформа безпеки електронної комерції Sansec виявила, що зловмисники використовували стеганографію для вбудовування скімінгового шкідливого програмного забезпечення в масштабовані векторні графіки (SVG) на сторінках електронної комерції. Шкідливе навантаження було приховане всередині SVG-ізображень, а декодер розміщувався в інших частинах веб-сторінок. Користувачі, які вводили свої дані на зламаних сторінках оформлення замовлення, не помічали нічого підозрілого, оскільки зображення виглядали як звичайні логотипи відомих компаній. Оскільки навантаження виглядало як дійсне використання синтаксису елемента SVG, стандартні сканери безпеки не змогли виявити загрозу.

SolarWinds: Також у 2020 році зловмисники приховали шкідливе ПЗ в легітимному програмному оновленні компанії SolarWinds, яка займається управлінням IT-інфраструктурою. Зловмисники успішно зламали Microsoft, Intel, Cisco та різні урядові агенції США. Вони використали стеганографію, щоб замаскувати викрадену інформацію під безневинні XML-файли, що надсилалися у HTTP-відповідях з контрольних серверів. Команди, передані в цих файлах, були замасковані під звичайні текстові рядки.

Промисловість: У 2020 році компанії у Великобританії, Німеччині, Італії та Японії стали жертвами кампанії, що використовувала стеганографічні документи. Зловмисники уникали виявлення, завантажуючи стеганографічне зображення на авторитетні платформи, такі як Imgur, для інфікування Excel-документів. Шкідливе програмне забезпечення Mimikatz, яке викрадає паролі Windows, завантажувалося за допомогою прихованого скрипту, вбудованого в зображення.

1.10 Захист від атак с використанням стеганографії

Атаки, що використовують стеганографію, відносно легко здійснювати, тоді як захист від них є значно складнішим завданням. Щоб зменшити ризики таких атак, можна вжити наступні заходи:

Збільшення обізнаності про кібербезпеку: Навчання працівників щодо ризиків, пов'язаних із завантаженням медіа з ненадійних джерел, може суттєво знизити ймовірність успішних атак. Це навчання має включати також навички розпізнавання фішингових електронних листів, що можуть містити шкідливі файли, а також розуміння стеганографії як потенційної кіберзагрози. На базовому рівні важливо навчити співробітників звертати увагу на зображення з незвично великими розмірами файлів, що може свідчити про наявність прихованих даних.

Впровадження веб-фільтрації та оновлень безпеки: Організації повинні впроваджувати веб-фільтрацію для забезпечення безпечного серфінгу в Інтернеті та регулярно оновлювати програмне забезпечення, встановлюючи останні оновлення безпеки, щоб знизити ризик уразливостей і атак.

Впровадження сучасних технологій захисту кінцевих точок: Компанії повинні використовувати технології, які перевершують статичні перевірки та базові сигнатури. Такі рішення здатні динамічно виявляти прихований код у зображеннях та інших формах маскування. Основні зусилля щодо виявлення шкідливих даних повинні бути зосереджені на кінцевих точках, де шифрування та маскування даних є легшими для виявлення.

Використання розвідки загроз: Компанії повинні активно використовувати розвідку загроз з різних джерел, щоб бути в курсі нових тенденцій, особливо щодо кібер-атак, що використовують стеганографію в їхній галузі.

Використання комплексних антивірусних рішень: Сучасні антивірусні програми допомагають виявляти, ізолювати та видаляти шкідливий код з пристроїв. Вони регулярно оновлюються, забезпечуючи захист від новітніх вірусів і інших видів шкідливого програмного забезпечення.

1.11 Виявлення та протидія стеганографії

1.11.1 Візуальна перевірка

Візуальна перевірка включає ретельний аналіз підозрілих файлів або комунікацій на наявність аномалій, які можуть свідчити про приховані дані. Цей ручний метод може виявити ненормальності в зображеннях, такі як незвичайні візерунки або розбіжності у значеннях пікселів. Хоча цей метод може бути корисним для виявлення очевидних ознак маніпуляцій, він вимагає багато часу через свою ручну природу. Крім того, він не є достатнім для всебічного виявлення стеганографії через тонкість сучасних стеганографічних технік.

1.11.2 Статистичний аналіз

Статистичні методи відіграють важливу роль у виявленні стеганографії, аналізуючи цифрові медіафайли на предмет відхилень від очікуваних патернів. Наприклад, аналіз розподілу значень пікселів в зображеннях або частотного спектра аудіофайлів може виявити приховані дані, закодовані за допомогою стеганографічних методів. Цей підхід вимагає спеціалізованих інструментів та алгоритмів для точного виявлення статистичних аномалій, які вказують на стеганографію.

1.11.3 Інструменти стеганалізу

Програмні засоби стеганалізу автоматизують процес виявлення, використовуючи алгоритми та статистичні моделі для аналізу файлів на предмет ознак стеганографії. Ці інструменти розроблені для ефективного виявлення прихованої інформації в цифрових медіа, що робить їх цінними активами у стратегіях захисту кібербезпеки.

1.11.4 Перевірка цілісності файлів

Перевірка цілісності файлів передбачає порівняння хеш-значень або контрольних сум файлів до і після передачі, щоб виявити зміни, внесені стеганографічними техніками. Будь-які розбіжності в цілісності файлу можуть вказувати на наявність прихованих даних.

1.11. 5Аналіз мережевого трафіку

Атаки, що ґрунтуються на мережевій стеганографії, можуть бути виявлені за допомогою комплексного аналізу мережевого трафіку. Моніторинг заголовків пакетів, розмірів корисного навантаження та часу передачі може виявити незвичайні патерни або аномалії, що вказують на стеганографічну активність. Це може бути здійснено за допомогою систем виявлення вторгнень у мережу (NIDS) та технологій глибокого аналізу пакетів (DPI).

1.11.6 Фільтрація контенту

Впровадження механізмів фільтрації контенту допомагає запобігти передачі прихованих даних, скануючи файли та комунікації на наявність відомих стеганографічних патернів або підписів. Рішення для фільтрації контенту можуть автоматично виявляти та блокувати підозрілий контент, зменшуючи ризик проникнення стеганографічних атак у мережі організації. Регулярні оновлення бази даних фільтрації контенту є важливими для випередження еволюційних стеганографічних технік та векторів загрози.

1.11.7 Освіта та обізнаність користувачів

Освіта користувачів щодо ризиків, пов’язаних зі стеганографією, і популяризація найкращих практик безпечної комунікації є важливими

компонентами стратегій запобігання стеганографії. Програми навчання повинні акцентувати увагу на важливості використання безпечних каналів зв'язку, уникнення використання несанкціонованого програмного забезпечення чи послуг, а також розпізнавання потенційних ознак стеганографічної активності.

1.12 Стеганографія та водяні знаки

Хоча водяні знаки та стеганографія мають деякі фундаментальні подібності в тому, що вони обидва приховано зберігають інформацію, вони вирішують дуже різні завдання. У стеганографії зображення, що використовується як покриття, є просто приманкою і не має жодного зв'язку з таємним повідомленням. Натомість водяний знак зазвичай несе додаткову інформацію про зображення-покриття або інші дані, пов’язані з ним, такі як мітки, що ідентифікують відправника або отримувача. Наприклад, під час покупки пісні у форматі MP3 через Інтернет інформація про продавця і/або покупця може бути вставлена в пісню у вигляді нечутного, але надійного водяного знака. Водяний знак може бути використаний пізніше для відстеження незаконно розповсюджених копій пісні. Водяні знаки також можуть передавати інформацію про саму пісню (наприклад, її надійний хеш або дайджест), щоб пізніше можна було перевірити її цілісність, порівнюючи пісню з водяним знаком.

Другою і, можливо, ще важливішою відмінністю між стеганографією та водяними знаками є питання існування таємного повідомлення в зображенні. Якщо в стеганографії вкрай важливо, щоб зображення не виявляло жодних слідів прихованих даних, то наявність водяного знака часто рекламується, щоб запобігти незаконним діям, таким як несанкціоноване копіювання або розповсюдження. Крім того, стеганографія є засобом комунікації, тому вона повинна дозволяти передачу великих обсягів даних. Навпаки, навіть дуже короткий цифровий водяний знак може бути досить корисним. Наприклад, наявність водяного знака (з корисним навантаженням в один біт) може свідчити про право власності на зображення. Ці

дуже різні вимоги, які пред'являються до цих двох застосувань, роблять їх дизайн і аналіз зовсім різними.

1.13 Стеганографія vs криптографія

Стеганографія та криптографія мають спільну мету — захистити повідомлення або інформацію від несанкціонованого доступу, але вони досягають цього різними методами. Криптографія перетворює інформацію в зашифрований текст, який можна розшифрувати лише за допомогою спеціального ключа. Проте, якщо хтось перехопить таке повідомлення, він одразу зрозуміє, що було використано шифрування, оскільки зашифрований текст є явним індикатором застосування криптографії.

Натомість стеганографія не змінює саму інформацію, а приховує сам факт її існування. Замість того щоб зашифровувати дані, стеганографія маскує їх всередині інших файлів або повідомлень, роблячи їх невидимими для сторонніх. Це забезпечує додатковий рівень секретності, оскільки факт наявності прихованого повідомлення залишається непомітним, що робить стеганографію ефективним інструментом для тих, хто прагне приховати навіть факт комунікації.

1.14 Стеганографія та NFT

Існують деякі схожості між стеганографією та NFT (незамінними токенами).

Коли створюється NFT, часто є можливість додати додатковий контент, доступний лише для власника цього токена. Цей контент може включати різноманітні матеріали, такі як високоякісні зображення, повідомлення, відео, доступ до закритих спільнот, коди або навіть смарт-контракти. Подібно до стеганографії, де інформація приховується всередині інших файлів або повідомлень, NFT дозволяють інтегрувати додаткові, приховані елементи, доступні тільки обраним користувачам.

1.15 Висновок до першого розділу

Стеганографія, як один із найдавніших методів приховування інформації, має багатогранну історію розвитку, яка починається з фізичних методів, таких як приховані написи чи шифри, і доходить до складних цифрових технологій сучасності. Незмінною залишається її основна мета — забезпечення прихованого передавання інформації, яка залишається непомітною для сторонніх спостерігачів. У наш час завдяки розвитку інформаційних технологій стеганографія стала потужним інструментом роботи з цифровими носіями, зокрема зображеннями, аудіо, відео та текстами, дозволяючи надійно приховувати дані в структурах цих файлів.

Сучасна стеганографія знаходить широке застосування у захисті даних в різних сферах, таких як особисті комунікації, корпоративна безпека, державне управління та фінансовий сектор. Зокрема, у банківських структурах вона використовується для забезпечення конфіденційності транзакцій, автентифікації користувачів та захисту від витоку даних. Стеганографія також є важливим компонентом кібербезпеки, оскільки забезпечує додатковий рівень захисту в поєднанні з іншими методами, такими як шифрування.

Однак стеганографія має і зворотний бік: її можливості нерідко використовуються у кіберзлочинності для прихованого обміну інформацією, шкідливого програмного забезпечення та уникнення виявлення. Це створює виклики для експертів із безпеки, які повинні розробляти все більш досконалі методи стегоаналізу для виявлення прихованих даних.

Таким чином, стеганографія залишається не лише потужною технологією для приховування інформації, але й ключовим елементом сучасної кібербезпеки. Її багатогранність дозволяє вирішувати широкий спектр завдань у захисті даних, але водночас вимагає постійного вдосконалення для боротьби із сучасними загрозами в умовах цифрової епохи. Вона вдало поєднує історичні традиції та сучасні досягнення, забезпечуючи нові підходи до безпечного обміну інформацією.

РОЗДІЛ2.
КОМПЛЕКСНЕ ДОСЛІДЖЕННЯ МЕТОДІВ СТЕГАНОГРАФІЇ ТА СТЕГОАНАЛІЗУ.

2.1 Формати цифрового зображення

2.1.1 Представлення кольору

Видиме світло є накладенням електромагнітних хвиль з довжинами в інтервалі від приблизно 380 нм до 750 нм. Кожен колір можна пов'язати зі спектральною функцією щільності P(λ), яка описує кількість енергії, присутньої при довжині хвилі λ. Таким чином, хоча можна сказати, що існує нескінченна (або навіть незліченна) кількість різних кольорів, кожен з яких відповідає певній функції щільності P(λ), людське око здатне розрізняти лише відносно невелику частину всіх можливих кольорів. В сітківці ока є три різні типи рецепторів, що називаються колбочками, з піковою чутливістю до червоного, зеленого і синього світла. Колбочки, які реєструють синє світло, мають найменшу чутливість до інтенсивності світла, тоді як колбочки, що реагують на зелене світло, мають найвищу чутливість. Електричні сигнали, що виробляються колбочками, передаються до мозку, що дозволяє нам сприймати колір. Це теорія трикомпонентного сприйняття кольору.

Ця теорія призводить до так званої адитивної моделі кольору. Згідно з цією моделлю, будь-який колір можна отримати як лінійну комбінацію трьох базових кольорів (або колірних каналів) – червоного, зеленого та синього. Позначаючи кількість кожного кольору як R, G і B, де кожне число знаходиться в інтервалі [0,1] (від нульової до повної інтенсивності), кожен колір може бути представлений як тривимірний вектор у колірному кубі RGB $(R, G, B) \in [0, 1]^3$. Апаратні системи, які випромінюють світло, зазвичай моделюються як адитивні. Наприклад, старі монітори з електронно-променевими трубками (CRT) створюють кольори, комбінуючи три люмінофори RGB на екрані. Рідкокристалічні дисплеї (LCD) поєднують світло від трьох сусідніх пікселів. Повна інтенсивність усіх трьох

кольорів сприймається як білий колір, тоді як низька інтенсивність у всіх каналах – як темний або чорний.

Субтрактивна модель кольору використовується для апаратних пристроїв, які створюють кольори шляхом поглинання певних довжин хвиль, а не випромінювання світла. Хорошим прикладом субтрактивного пристрою є принтер. Стандартні базові кольори для субтрактивних систем, за домовленістю, – це блакитний, пурпуровий та жовтий, що призводить до представлення кольору за допомогою вектора CMY. Ці три кольори отримують шляхом видалення з білого кольорів червоного, зеленого та синього відповідно. Система CMY доповнюється четвертим кольором, чорним (скорочено K), щоб покращити контраст друку та заощадити кольоровий тонер.

Між адитивною RGB і субтрактивною системами CMY існує такий зв’язок:

$$C = 1 - R, \quad (2.1)$$

$$M = 1 - G, \quad (2.2)$$

$$Y = 1 - B. \quad (2.3)$$

Хоча адитивна кольорова модель RGB досить добре описує кольори, які сприймає людина, вона є надлишковою, оскільки три сигнали висококорельовані між собою, що робить її не найекономічнішою для передачі. Дуже популярною кольоровою системою є модель YUV, спочатку розроблена для передачі сигналів кольорового телебачення. Вимога зворотної сумісності зі старими чорно-білими телевізорами призвела до того, що колірний телевізійний сигнал було сформовано як яскравість, доповнена сигналами кольоровості. Читачеві варто зауважити, що відтепер буква Y завжди позначатиме яскравість, а не жовтий, як у колірній системі CMY(K).

Яскравість Y визначається як зважена лінійна комбінація каналів RGB, причому ваги встановлюються відповідно до чутливості людського ока до трьох кольорів RGB.

$$Y = 0.299R + 0.587G + 0.114B. \quad (2.4)$$

Компоненти хромінансів – це різниці між кольоровими каналами та яскравістю.

$$U = R - Y, \quad (2.5)$$

$$V = B - Y \quad (2.6)$$

що передає інформацію про колір. Перетворення між системами RGB та YUV є лінійним,

$$\begin{pmatrix} Y \\ U \\ V \end{pmatrix} = \begin{pmatrix} 0.299 & 0.587 & 0.114 \\ 0.701 & -0.587 & -0.114 \\ -0.299 & -0.587 & 0.886 \end{pmatrix} \begin{pmatrix} R \\ G \\ B \end{pmatrix} \quad (2.7)$$

$$\begin{pmatrix} R \\ G \\ B \end{pmatrix} = \begin{pmatrix} 1 & 1 & 0 \\ 1 & -0.509 & -0.194 \\ 1 & 0 & 1 \end{pmatrix} \begin{pmatrix} Y \\ U \\ V \end{pmatrix} \quad (2.8)$$

Якщо кольори RGB представлені 8-бітними цілими числами в діапазоні {0, . . . , 255}, то яскравість Y поділяє цей же діапазон, тоді як U та V потрапляють у діапазон {-179,...,179}. Щоб привести всі три компоненти до одного діапазону, що може бути представлений 8 бітами, компоненти кольору далі лінійно перетворюють у C_r і C_b, отримуючи таким чином колірну модель Y $C_r C_b$.

$$\begin{pmatrix} Y \\ C_r \\ C_b \end{pmatrix} = \begin{pmatrix} 0 \\ 128 \\ 128 \end{pmatrix} + \begin{pmatrix} 0.299 & 0.587 & 0.114 \\ 0.5 & -0.419 & -0.081 \\ -0.169 & -0.331 & 0.5 \end{pmatrix} \begin{pmatrix} R \\ G \\ B \end{pmatrix} \quad (2.9)$$

Оскільки людські очі значно менш чутливі до змін у хромінансі, ніж до яскравості, сигнали хромінансу часто представляються з меншою кількістю бітів без впровадження видимого спотворення в зображення. Цей факт використовується в форматі стиснення JPEG, а також у телевізійних сигналах, де менша смуга пропускання виділяється для сигналів хромінансу, а ширша смуга пропускання використовується для яскравості. Цифрові формати зображень, що використовують модель Y $C_r C_b$, включають IIF, TIFF, JFIF, JPEG та MPEG (рухомий JPEG).

2.1.2 Вибірка кольорів

Навіть якщо деякі формати зображень дозволяють довільно точне представлення значень інтенсивності кольору (IIF, PostScript), більшість форматів представляють інтенсивності у квантизованій формі, використовуючи фіксовану кількість n_c біт, що дозволяє захоплювати 2^{n_c} різних відтінків. Найбільш відповідне кольорове семплювання сильно залежить від застосування. З одного боку, більшість факс-машин працюють лише з двома кольорами (чорний та білий), тоді як супутникові знімки високої роздільної здатності або фотореалістичні синтетичні зображення можуть використовувати до 16 біт на колірний канал (48 біт для кольору). Приклади типових значень кольорового семплювання для вибраних застосувань наведені в таблиці 2.1.

Таблиця 2.2 показує, яку глибину кольору дозволяє кожен формат. Для палетних форматів глибина кольору представляє діапазон індексів палітри.

Таблиця 2.1

Типова бітова глибина кольору для різних застосувань. Для $n_c \geq 8$ вибірка кольорових зображень здійснюється в бітах на колірний канал.

n_c	Кольори	Застосування
1	2	Факс, чорно-білі малюнки
2	4	
4	16	Малювання ліній, графіки, мультиплікація
8	256	Сірі зображення, повноцінні кольорові фото
12	4096	Сірі медичні зображення, сканування, цифровий вивід з датчиків
14	16384	Сканування, цифровий вивід з датчиків, зображення з якістю як з фільму
16	65536	Фото реалістичні синтетичні зображення, сканування, зображення зі спутників

Таблиця 2.2

Вибірка для популярних форматів зображень.

	Колір	Відтінки сірого	Палітра
BMP	24	8	1, 4, 8
TIFF	24, 30, 36, 42, 48	4-8	1-8
PNG	24, 48	1, 2, 4, 8, 16	1, 2, 4, 8
GIF	-	-	1-8
JPEG	24	8, 12	-

2.2 Стеганографічний канал

Основною метою стеганографії є передача секретних повідомлень без явного свідчення про те, що відбувається комунікація секрету. Це може бути досягнуто шляхом приховування повідомлень у звичайних об'єктах, які потім передаються відверто через певний канал зв'язку. У цьому розділі ми розглянемо окремі елементи, які визначають стеганографічну комунікацію.

Ми розрізняємо п'ять основних елементів кожного стеганографічного каналу (див. рисунок 2.1):

- Джерело покриттів,
- Алгоритми вбудовування та витягування даних,
- Джерело стегоключів, що керують алгоритмами вбудовування/витягування,
- Джерело повідомлень,
- Канал, який використовується для обміну даними між відправником та отримувачем.

Сучасна стеганографія зазвичай робить деякі основні припущення щодо джерела покриттів, що дозволяє формальний аналіз. Наприклад, розглядаючи джерело покриттів як випадкову змінну, можна провести аналіз стеганографії за допомогою теорії інформації. Альтернативно, джерело покриттів може бути

інтерпретовано як оріакл, до якого можна звертатися. Це призводить до вивчення стеганографії з точки зору складності.

Рис 2.1 - Елементи стеганографічного каналу

Алгоритм вбудовування — це процедура, за допомогою якої відправник визначає зображення, що передає необхідне секретне повідомлення. Процедура може залежати від секрету, спільного між відправником та отримувачем, який називається стегоключем. Цей ключ потрібен для правильного витягування секретного повідомлення з стегозображення. Наприклад, відправник може вбудувати свій секретний бітовий потік у найменш значущі біти пікселів, обраних по непересічному псевдовипадково згенерованому шляху через зображення (визначеному за допомогою стегоключа).

Протокол, який відправник та отримувач використовують для вибору стегоключів, зазвичай моделюється за допомогою випадкової змінної на просторі всіх ключів. Наприклад, розумною стратегією є випадковий вибір стегоключа (з рівномірним розподілом) із набору всіх можливих стегоключів.

Джерело повідомлення має значний вплив на безпеку стеганографічного каналу. Уявіть собі дві крайні ситуації. З одного боку, відправник та отримувач завжди спілкуються лише коротким повідомленням, скажімо, 16 бітів, у кожному стегозображенні. З іншого боку, вони мають потребу в спілкуванні великими повідомленнями та часто вбудовують стільки бітів у зображення, скільки дозволяє

алгоритм вбудовування. Інтуїтивно, учасники перебувають під значно більшим ризиком у другому випадку. Розподіл повідомлень можна змоделювати за допомогою випадкової змінної на просторі всіх можливих повідомлень.

Фактичний канал зв'язку, що використовується для надсилання зображень, вважається моніторинговим. Захищаюча сторона може виконувати три різні ролі. Зайнявши позицію пасивного моніторингу, сторона захисту перевіряє лише трафік і не втручається у саму комунікацію між учасниками стеганографічного обміну. Це називається сценарієм пасивного вартового. Альтернативно, захист може підозрювати, що відправник і отримувач можуть використовувати стеганографію, і спробувати заздалегідь зруйнувати стеганографічний канал, навмисно спотворюючи зображення, які підлягають обміну. Наприклад, можна стиснути зображення за допомогою JPEG, змінити розмір або обрізати зображення, застосувати невелику кількість фільтрації тощо. Якщо не використовувати стеганографію, яка є стійкою (робуста) до таких обробок, стеганографічний канал буде зламаний діями захисту. Це називається сценарієм активного вартового. Нарешті, захист може спробувати вгадати стеганографічний метод, який використовують відправник і отримувач, і спробувати видати себе за одного з них чи іншим чином втрутитися, щоб заплутати комунікуючі сторони. Існує різниця між так званим зловмисним вартовим і активним вартовим. Дії активного вартового спрямовані на те, щоб зробити стеганографію неможливою для комунікації, тоді як зловмисний вартовий не обов'язково має намір повністю зруйнувати стеганоканал, а скоріше використовувати його на свою користь, щоб визначити, чи має місце стеганографія. Пасивний випадок це випадок комунікації через стандартні Інтернет-протоколи, де засоби виправлення помилок та автентифікації гарантують безпомилкову передачу даних.

Вище написане підкреслює необхідність розглядати стеганографічну комунікацію в більш широкому контексті. Під час розробки стеганографічної схеми у учасників комунікації є вибір у відборі основних елементів для формування їхньої комунікаційної схеми.

Алгоритми вбудовування та витягування очевидно є найважливішими частинами будь-якої стегосистеми. Стеганографічні алгоритми можуть використовувати три різні фундаментальні архітектури, які визначають внутрішній механізм алгоритмів вбудовування та витягування. Відправник може "виконати вбудовування", вибравши зображення, яке вже має бажане повідомлення, заховане всередині. Це називається стеганографією за вибором об'єкта. Або ж він може створити об'єкт, який передає повідомлення. Ця стратегія називається стеганографією за синтезом об'єкта. Третя опція, яка є найпрактичнішою для передачі великих обсягів даних, — це стеганографія за модифікацією об'єкта. Це вважається основним методом підходу до стеганографії.

2.3 Стеганографія за вибором об'єкта

У стеганографії за вибором об'єкта відправник має фіксовану базу даних зображень, з якої вона обирає одне, яке передає бажане повідомлення. Наприклад, один біт інформації можна надіслати, вибравши картину в ландшафтній або портретній орієнтації. Альтернативно, присутність тварини на зображенні може мати приховане значення, наприклад, «атака завтра» тощо. Алгоритм вбудовування може працювати, просто випадковим чином вибираючи зображення з бази даних, поки не знайдеться зображення, яке передає бажане повідомлення. Стего-ключ тут, по суті, є набором правил, які вказують учасникам комунікації, як інтерпретувати зображення.

Важливим випадком стеганографії за вибором об'єкта є функції хешування. Відправник вибирає зображення з бази даних і застосовує до нього функцію хешування (ця функція може залежати від ключа і повинна бути спільною з отримувачем). Якщо хеш відповідає бажаній бітовій послідовності повідомлення, зображення пересилається, інакше відправник вибирає інше зображення, поки не отримає відповідність. Очікувана кількість спроб, необхідних для отримання відповідності, експоненційно залежить від довжини хешу, і тому швидко стає непрактично великою. Отримавши зображення, отримувач просто витягує хеш,

щоб прочитати повідомлення. Перевагою цього підходу є те, що об'єкт завжди є «100% природним», оскільки це реальне зображення, яке не було змінено жодним чином. Очевидним недоліком є непрактично низька пропускна спроможність.

При уважному розгляді можна виявити одну потенційну проблему зі стеганографією за вибором об'єкта, яка заважає нам стверджувати, що вона є «справді непомітною». Щоб зробити проблему більш очевидною, ми використовуємо дуже просту функцію хешування, яка складається з найменш значущих бітів перших трьох пікселів зображення.

$$h(x) = \{x[1]\ mod\ 2, x[2]\ mod\ 2, x[3] mod 2\} \qquad (2.10)$$

Зверніть увагу, що дайджест складається з трьох бітів. Проблема може виникнути, коли відправник вирішує використовувати цю техніку для комунікації не лише один раз, а й повторно. Якщо з однаковою ймовірністю надсилати кожну трійку біт з усіх восьми можливих трійок (що є розумним припущенням, наприклад, надсилаються частини зашифрованого документа), стего-зображення, надіслані відправником, з однаковою ймовірністю створюватимуть будь-які з 8-бітних трійок як дайджест. Проте, як ми можемо дізнатися, що в природних зображеннях розподіл найменш значущих бітів (LSB) перших трьох пікселів у верхньому лівому куті відповідає цьому розподілу? Найімовірніше, що це не так, оскільки ці пікселі, ймовірно, належать до частини неба, і тому їх значення далеко не є незалежними. Зверніть увагу, що ця проблема виникає лише тому, що ми розглядаємо багаторазове використання стеганографічного каналу і дозволяємо захисту перевіряти всі передачі від відправника, а не розглядаємо одне зображення за раз.

2.3 Стеганографія за допомогою синтезу покриття

В стеганографії за допомогою синтезу покриття відправник створює покриття таким чином, щоб воно передавало бажане повідомлення. У пресі з’являлися деякі спекуляції про те, що відео може містити приховані повідомлення,

передані через будь-який елемент цього відео, одягу, речей і просто аудіо складової. Це було б прикладом стеганографії за допомогою синтезу покриття.

Ще один досить цікавий приклад, який включає текст як покриття, а не цифрові зображення, - це кодування повідомлень таким чином, щоб вони нагадували спам. Тут стеганограф використовує той факт, що спам часто містить незв'язні або незвичайні формулювання, які можна використати для кодування повідомлення. Програма SpamMimic (www.spammimic.com) використовує функції імітації, щоб приховувати повідомлення в штучно створеному тексті, схожому на спам.

Стеганографію шляхом синтезу покриття можна поєднати зі стеганографією шляхом вибору покриття, щоб зменшити експоненційну складність вбудовування за допомогою хешування. Припустимо, що ми можемо зробити велику кількість зображень точно тієї ж сцени з тією ж цифровою камерою. Наприклад, ми могли б зафіксувати камеру на штативі та зробити кілька зображень за постійних умов освітлення. Припустимо, що зображення мають 8-бітну градацію сірого, де $x_j[i]$ позначає інтенсивність i-го пікселя в j-му зображенні, де i = 1,…, n, j = 1, …, K. Тепер ми робимо ключове спостереження: значення інтенсивності світла в певному пікселі i, коли їх розглядати через усі зображення j, дещо змінюються через випадкові джерела шуму, які присутні на зображеннях, такі як шум від вибуху, шум зчитування та шум від електроніки на чіпі.

Стеганограф використовує криптографічну хеш-функцію, модифіковану для повернення 4 бітів, коли вона застосовується до 16 пікселів. Наприклад, може використовуватися останні 4 біти з хешу MD5. Значення 4 і 16 вибрані довільно, і, звичайно, можуть бути використані інші значення. Щоб вбудувати своє повідомлення, відправник ділить кожне зображення на несумісні блоки по 4 × 4 пікселі та складає нове зображення блок за блоком, так що кожен блок 4 × 4 передає 4 біти повідомлення.

Щоб вбудувати перші 4 біти в перший блок пікселів 4 × 4, стеганограф шукає хеші $h\big(x_j[1], \dots, x_j[16]\big)$, де $j \in \{1,2, \dots, K\}$, поки не знайде збіг між хешем перших 16 пікселів і повідомленням, що відбудеться для зображення номер j_1. Потім

переходить до наступного блоку і знаходить $j_2 \in \{1, \ldots, K\}$, так що $h\big(x_j[17], \ldots, x_j[32]\big)$ відповідає наступним 4 бітам повідомлення тощо. Остаточне стего-зображення y буде мозаїкою, зібраною з блоків з різних зображень y = ($x_{j_1}[1]$, …, $x_{j_1}[16]$, $x_{j_2}[17]$, … $x_{j_2}[32]$, $x_{j_3}[33]$, …). Ймовірність знайти збіг в одному конкретному блоці серед усіх K зображень становить$1 - (1 - 1 / 16)^K$.

Ймовірність можливості вбудувати все повідомлення, яке складається з n/16 груп по 4 біти, таким чином $(1 - (1 - 1 / 16)^k)^{n/16}$. При збільшенні кількості зображень K цю ймовірність можна наблизити до 1. Наприклад, для квадратного зображення розміром n = 512 × 512 і лише K = 400 зображень ця ймовірність становить 0.9999998993… .

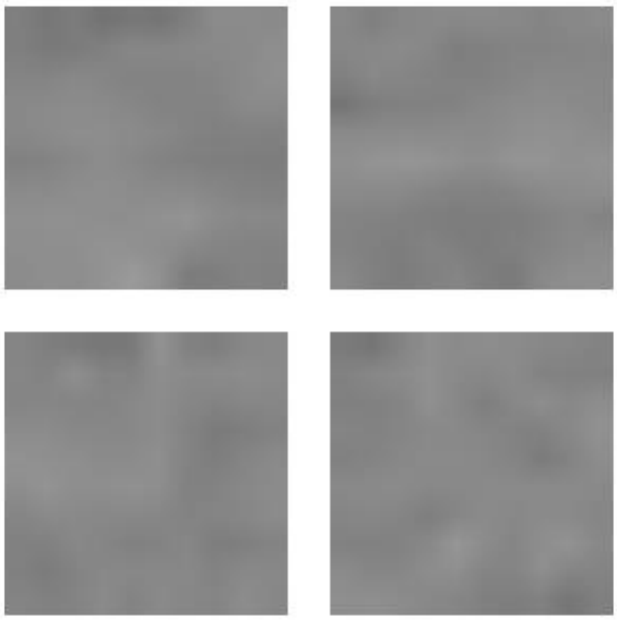


Рис 2.2 - 16 на 16 пікселів блок з чотирьох не стиснутих TIFF зображень синього неба знятого з однієї камери з коротким інтервалом. На перший погляд блоки не однорідні навіть не дивлячись на те, що сцена чудово однорідна. Друге, блоки відрізняються в кожному зображені через випадкові джерела шуму.

Цей метод є скоріше теоретичною конструкцією, ніж практичною стеганографічною технікою. Це пов'язано з тим, що насправді важко отримати

багаторазові вибірки одного сигналу (ідентичні фотографії однієї сцени з точністю до частки ширини пікселя). Невеликі варіації в часі експозиції через механіку затвора та інші механічні вібрації обмежуватимуть вирівнювання між різними знімками.

Схема робить неявне припущення, що пікселі на межах блоків є незалежними, або, точніше, що випадкові компоненти зображень є незалежними. Як ми вже знаємо з розділу 3, різні види обробки всередині камери, такі як інтерполяція кольорів або фільтрація, створюють залежності між сусідніми пікселями, а отже, і між їхніми шумовими компонентами. В результаті захист може розпочати атаку, аналізуючи залежності між пікселями, що перетинають межі блоків, і порівнювати їх із залежностями між сусідніми пікселями всередині блоків.

Існує якісно інше втілення стеганографії шляхом синтезу покриття, яке називається маскуванням даних. Ідея полягає в тому, що всі інструменти стеганоаналізу в кінцевому підсумку є автоматизованими і працюють, виділяючи набір числових ознак із зображення, які потім аналізуються на сумісність з ознаками, що зазвичай отримуються з покриттєвих зображен. Таким чином, усе, чого відправнику потрібно досягти, щоб уникнути виявлення, — це зробити так, щоб стего-зображення виглядало як покриття у просторі ознак. Саме "зображення" не обов'язково має виглядати як природне, оскільки, якщо його ознаки сумісні з ознаками природних зображень, воно повинне пройти через детектор. Практичний метод маскування даних був створений шляхом застосування інверсного фільтра Вінера, що змінюється з часом, для формування кожних 1024 біт повідомлення у відповідність з еталонним аудіокадром.

2.4 Стеганографія через модифікацію контейнера

Відправник починає з контейнерного зображення і вносить у нього зміни, щоб вбудувати секретні дані. Учасники комунікації працюють з набором усіх можливих контейнерів, а також із наборами ключів і повідомлень, які, в найзагальнішому випадку, можуть залежати від кожного контейнера:

C . . . set of cover objects x ∈ C, (2.11)

K(x) . . . set of all stego keys for x, (2.12)

M(x) . . . set of all messages that can be communicated in x. (2.13)

Відповідно до діаграми, наведеної на Рисунку 2.3, стеганографічна схема являє собою пару функцій вбудовування та вилучення Emb і Ext.

Emb : C ×K×M→C, (2.14)

Ext : C ×K→M, (2.15)

таких, що для всіх x ∈ C, усіх k ∈ K(x), m∈M(x),

Ext (Emb(x, k,m), k) = m. (2.16)

Інакше кажучи, відправник може взяти будь-яке покриття x ∈ C і вбудувати в нього будь-яке повідомлення m ∈ M(x), використовуючи будь-який ключ k ∈ K(x), отримуючи зображення стеганографії y = Emb(x, k, m). Кількість повідомлень, які можна передати в конкретному покритті \(x \), залежить від стеганографічної схеми, а також може залежати від самого покриття. Наприклад, якщо C — це набір усіх 512 × 512 градацій сірого, і стеганограф вбудовує один біт повідомлення на піксель, то $M = \{0,1\}^{512x512}$ і $|M(x)| = 2^{512x512}$ для всіх x ∈ C.

З іншого боку, якщо C — це набір усіх 512 × 512 градацій сірого JPEG з якістю $=q_f$ 75, і вбудовується один біт у кожен ненульовий квантизований DCT коефіцієнт, то кількість повідомлень, які можна вбудувати в конкретне покриття, залежить від самого покриття, оскільки кількість ненульових DCT коефіцієнтів у JPEG файлі залежить від змісту зображення.

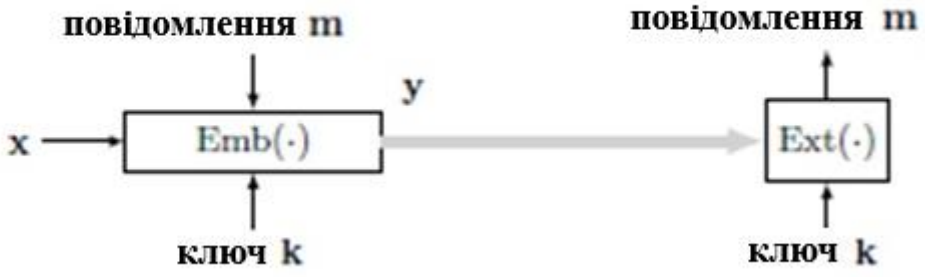


Рис 2.3 - Стеганографія модифікацією обгортки.

Таким чином, ми визначаємо ємність вбудовування (вантажопідйомність) покриття x у бітах як

$$log_2|M(x)|, \qquad (2.17)$$

а відносна ємність вбудовування становить

$$\frac{log_2|M(x)|}{n}, \qquad (2.18)$$

де n — це кількість елементів у x, таких як кількість пікселів або ненульових коефіцієнтів DCT. Для растрових зображень відносну ємність часто виражають у bpp(біт на піксель). Для JPEG-зображень використовують одиницю bpnc (біт на ненульовий DCT коефіцієнт). Беручи математичне сподівання в (4.8) та (4.9) стосовно деякого розподілу покриттів x, ми можемо говорити про середню ємність вбудовування та відносну ємність вбудовування.

Мабуть, найбільш фундаментальним поняттям у стеганографії є стеганографічна ємність, визначена як максимальна кількість біт, яку можна вбудувати, не створюючи статистично виявлених артефактів. Зазвичай стеганографічна ємність набагато менша за ємність вбудовування.

Алгоритми вбудовування багатьох стеганографічних схем потребують представлення покривних і стего зображень за допомогою бітів або, загальніше, символів з деякого алфавіту A за допомогою функції призначення символів π,

$\pi : X \rightarrow A$, (2.19)

де X є діапазоном окремих елементів покриття, таких як пікселі або коефіцієнти DCT. Однією з часто використовуваних функцій призначення бітів (парності) є найменш значущий біт.

LSB(x) = x mod 2. (2.20)

Якщо алгоритм вбудовування розроблений так, щоб уникати внесення змін у певні області зображення-покриття, це називається адаптивною стеганографією. Наприклад, можна пропустити рівні області зображення та зосередити зміни в текстурованих регіонах. Підмножина зображення, де дозволені зміни для вбудовування, називається каналом вибору. Іншим прикладом каналу вибору є вбудовування бітів повідомлення вздовж псевдовипадкового шляху через

зображення, згенерованого зі стего-ключа. Загалом, в інтересах учасників комунікації не розкривати або розкривати якомога менше інформації про канал вибору, оскільки це знання може допомогти зловмиснику. Якщо канал вибору доступний тільки одному з учасників, він називається ненаділеним каналом вибору.

Стеганографія шляхом модифікації покриття вводить спотворення в покриття. Спотворення зазвичай вимірюється за допомогою відображення d(x, y), d : C × C → [0,∞). Одна з часто використовуваних сімей мір спотворення параметризується значенням γ ≥ 1,

$$d_\gamma(x,y) = \sum_{i=1}^{n} |x[i] - y[i]|^\gamma. \qquad (2.21)$$

Для γ = 1,

$$d_1(x,y) = \sum_{i=1}^{n} |x[i] - y[i]|. \qquad (2.22)$$

Для L_1норма між векторами x та y, поки

$$d_2(x,y) = \sum_{i=1}^{n} |x[i] - y[i]|^2. \qquad (2.23)$$

є енергією для внутрішніх змін.

Міра

$$v(x,y) = \sum_{i=1}^{n} 1 - \delta(x[i] - y[i]). \qquad (2.24)$$

це кількість змін під час вбудовування, де δ — дельта Кронекера (2.23). Зверніть увагу, що якщо амплітуда змін під час вбудовування становить $|x[i] - y[i]| = 1$, d_γ збігаються для всіх γ.

Наведену вище міру спотворення можна вважати абсолютною, оскільки вона вимірює загальне спотворення. Часто доцільно виражати спотворення на один елемент контейнера (наприклад, на піксель), і в такому випадку ми говоримо про відносне спотворення.

$$\frac{d(x,y)}{n} \qquad (2.25)$$

Кількість

$$\beta = \frac{v(x,y)}{n} \qquad (2.26)$$

називається частотою змін і зазвичай позначається як β.

Два популярних відносних показники — це середньоквадратична помилка (MSE)

$$MSE = \frac{d_2(x,y)}{n} = \frac{1}{n}\sum_{i=1}^{n} |x[i] - y[i]|^2, \qquad (2.27)$$

та відношення пікової сигналу до шуму (PSNR).

$$PSNR = 10\log_{10}\frac{x_{max}^2}{MSE}, \qquad (2.28)$$

де x_{max}— це максимальне значення, яке може набрати x[i]. Наприклад, для 8-бітних градацій сірого x_{max} = 255.

Середнє значення вбудованого спотворення — це очікуване значення E [d(x, y)], взяте по всіх x ∈ C, k ∈ K, m ∈ M, обраних відповідно до певних ймовірнісних розподілів з їх відповідних множин.

Дуже важливою характеристикою стегосистеми, яка суттєво впливає на її безпеку, є ефективність вбудовування. Ми визначаємо її тут, скоріше, неформально як середню кількість бітів, вбудованих на одиницю середнього спотворення.

$$e = \frac{E_x[\log_2 |M(x)|]}{E_{x,m}[d(x,y)]}, \qquad (2.29)$$

Складність обчислення ефективності вбудовування залежить від стеганографічної схеми, її внутрішнього механізму та джерела покриття. Для найпростіших схем вбудовування, таких як вбудовування найменш значущих бітів (LSB) або вбудовування ±1 у просторовій області, ефективність вбудовування можна легко оцінити аналітично. З іншого боку, для деяких стеганографічних методів максимальний обсяг даних, що можуть бути вбудовані, а також спотворення можуть бути досить складною функцією вмісту покриття або навіть

стего-ключа, що ускладнює аналітичне обчислення ефективності вбудовування через нашу неточну інформацію про джерело покриття. У таких випадках ефективність вбудовування визначається експериментально. Нарешті, зауважимо, що ефективність вбудовування залежить від міри спотворення d.

2.5 LSB-впровадження

// **Ініціалізація PRNG використовуючи стего ключ**
//**Ввести: повідомлення** $\mathbf{m} \in \{0,1\}^m$, **зображення** $\mathbf{x} \in \mathcal{X}^n$
$\mathbf{Path} = \mathrm{Perm}(n)$;
// $\mathrm{Perm}(n)$ **Псевдо-рандомна перестановка** $\{1, 2, \ldots, n\}$
$\mathbf{y} = \mathbf{x}$;
$m = \min(m, n)$;
// **Якщо повідомлення більше за доступний об'єм, вкоротити його**
for $i = 1$ to m {
  $\mathbf{y}[\mathbf{Path}[i]] = \mathbf{x}[\mathbf{Path}[i]] + \mathbf{m}[i] - \mathbf{x}[\mathbf{Path}[i]] \bmod 2$;
}
// **y це стего зображення з m вписані біти повідомлення**

Алгоритм 2.1 - вбудоване повідомлення $m \in \{0,1\}^m$ прихована в зображені $x \in x^n$.

Можна стверджувати, що LSB-впровадження є найпростішим стеганографічним алгоритмом. Його можна застосувати до будь-якої колекції числових даних, представлених у цифровій формі. Припустимо, що x[i] ∈ X = $\{0, \cdots, 2^{n_c} - 1\}$ — це послідовність цілих чисел. Наприклад, x[i] може бути світловою інтенсивністю в і-му пікселі в 8-бітному градаційному зображенні ($n_c = 8$), індексом палітри в файлі GIF ($n_c = 8$) або квантизованим DCT-коефіцієнтом у файлі JPEG ($n_c = 11$). В залежності від формату зображення та обраної глибини бітів для представлення окремих значень, кожне x[i] може бути представлене з використанням n_c бітів b[i, 1], … , b[i, n_c],

$$x[i] < \sum_{k=1}^{n_c} b[i,k] 2^{n_c - k}, \qquad (2.30)$$

Отже, можна розглядати послідовність (b[i, 1], … , b[i, n_c]), як двійкове представлення x[i] у формі big-endian (найзначніший біт b[i, 1] йде першим). LSB — це останній біт b[i, n_c].

LSB-вставка, як випливає з назви, працює шляхом заміни LSB значень x[i] на біти повідомлення m[i], в результаті чого отримується стего-зображення y[i]. Алгоритм 5.1 показує псевдокод для вставки потоку бітів у зображення вздовж псевдовипадкового шляху, згенерованого з секретного ключа, який спільний для учасників стеганографічної комунікації.

Зверніть увагу, що в кольоровому зображенні кількість елементів у покритті n в три рази більша, ніж для сірого зображення. Таким чином, псевдовипадковий шлях вибирається через усі пікселі та кольорові канали. Повідомлення, вставлене за допомогою Алгоритму 2.1, можна витягти за допомогою псевдокоду в Алгоритмі 2.2.

Амплітуда змін у вставці LSB дорівнює 1, $max_i|x[i] - y[i]| = 1$, що є найменшою можливою зміною для будь-якої операції вставки. За звичайних умов перегляду зміни вставки в 8-бітному сірому або справжньому кольоровому зображенні не є візуально помітними. Більше того, оскільки природні зображення містять невелику кількість шуму через різні джерела шуму, які присутні під час захоплення зображень, площина LSB сирих, ніколи не стиснених природних зображень вже виглядає випадковою. Рисунок 2.4 показує оригінальне покривне зображення та його площину LSB b[i, n_c] для червоного каналу.

```
// ініціалізація PRNG за допомогою стего ключа

Path = Perm(n);

for i = 1 to m {
  m[i] = y[Path[i]] mod 2;
}
// m це витягнуте секретне повідомлення
```

Алгоритм 2.2 вбудоване повідомлення m з стего зображення y.

Таблиця 2.3

Відносна кількість бітів, сусідніх пар і трійок бітів від площини LSB зображення.

Частота подій	
Біти	0.49942, 0.50058
Пари	0.24958, 0.24984, 0.24984, 0.25073
Тріо	0.1246, 0.1250, 0.1247, 0.1251, 0.1250, 0.1249, 0.1251, 0.1256

Таблиця 2.3 містить частоти появи окремих бітів у b[i, n_c], 1, …, n, пар сусідніх бітів (b[i, n_c], b[i + 1, n_c]) та трійок сусідніх бітів (b[i, n_c], b[i + 1, n_c], b[i + 2, n_c]). Дані узгоджуються з твердженням, що площина LSB є випадковою. Хоча це не є доказом випадковості, аргумент достатньо переконливий, щоб інтуїтивно вважати, що будь-які спроби виявити акт випадкового перевертання підмножини бітів з площини LSB приречені на провал. Це, здавалося б, інтуїтивне твердження далеке від істини, оскільки вставку LSB у зображення можна дуже надійно виявити.

Навіть якщо площина LSB покриттів була б насправді випадковою, все ще може бути можливим виявити зміни вставки через перевертання LSB, якщо, наприклад, друга площина LSB b[i, n_c - 1] і площина LSB якимось чином були б залежними! У най екстремальнішому випадку залежності, якщо b[i, n_c - 1] = b[i, n_c] для кожного і, виявлення змін LSB було б тривіальним. Все, що нам потрібно було б зробити, це порівняти площину LSB з другою площиною LSB.

Вставка LSB належить до класу стеганографічних алгоритмів, які вставляють кожен біт повідомлення в один елемент покриття. Іншими словами, кожен біт розташовується в певному елементі. Процес вставки здійснюється шляхом відвідування окремих елементів покриття та застосування операції вставки (перевернення LSB) за необхідності, щоб узгодити LSB з бітами повідомлення. Не всі стеганографічні схеми повинні слідувати цій простій парадигмі вставки. Методи, що використовують синдромне кодування, залучають кілька елементів покриття для вставки кожного біта в тому сенсі, що алгоритм витягування повинен бачити більше ніж один елемент, щоб витягнути один біт.

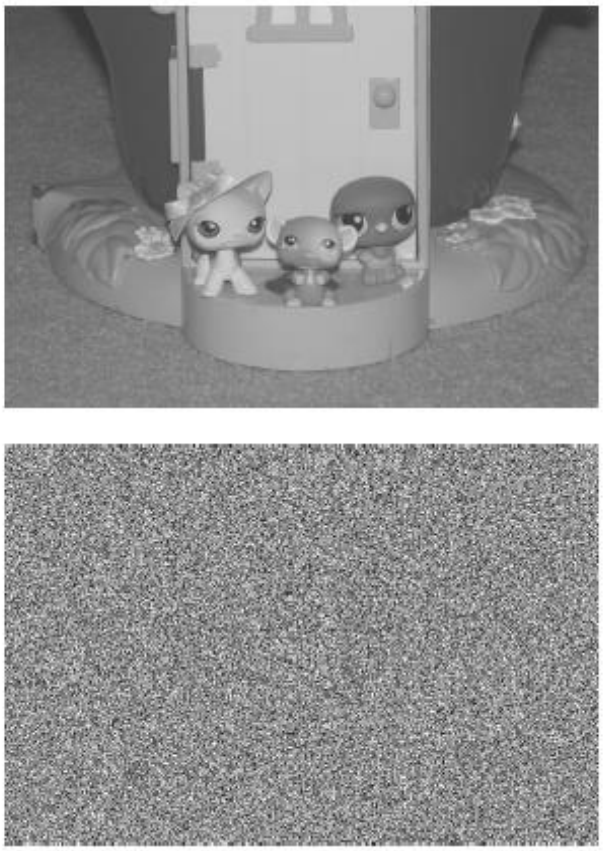


Рис. 2.4 - Справжній колір 800 x 548 фотографії та LSB площині його червоного каналу.

Операцію вставки, що полягає в перевертанні LSB, можна записати математично багатьма різними способами:

$$LSBflip(x) = \begin{cases} x + 1 \text{ коли x парний} \\ x - 1 \text{ коли x не парний} \end{cases} \quad (2.31)$$

LSBflip є ідемпотентною операцією, яка задовольняє рівнянню LSBflip(LSBflip(x)) = x. Це означає, що повторна вставка LSB частково скасовує сама себе, і таким чином існує межа на максимальне очікуване спотворення, яке може бути введено внаслідок повторної вставки LSB. Багато інших операцій вставки не мають цієї властивості. Часткове скасування змін вставки можна використовувати для атаки на схеми, які використовують вставку LSB [87].

Вставка LSB також індукує 2^{n_c-1} несуміжних пар LSB у множині всіх можливих значень елементів $\{0, 1, \ldots, 2^{n_c-1}\}$,

$$\{0,1\},\{2,3\},\dots,\{2^{n_c}-2,2^{n_c}-1\} \qquad (2.32)$$

Зверніть увагу, що якщо x[i] знаходиться в парі LSB {2k, 2k + 1}, вона повинна залишатися там після вставки, оскільки елементи пари відрізняються лише своїми LSB (2k ↔ 2k + 1). Це просте спостереження є початком багатьох потужних атак на вставку LSB.

Для будь-якого методу стеганографії часто корисно математично виразити вплив вбудовування на гістограму зображення. Багато стеганографічних технік вводять характерні артефакти в гістограму, і ці артефакти можуть бути використані для виявлення наявності секретних повідомлень (атак конструкцій). Нехай h[j], j = 0, . . . , $2^{n_c}-1$, буде гістограмою елементів з покривного зображення.

$$h[j]=\sum_{i=1}^{n}\delta(x[i]-j), \qquad (2.33)$$

де δ — це дельта Кронекера (2.33). Ми будемо припускати, що відправник вбудовує потік m випадкових бітів. Припущення про випадковість є обґрунтованим, оскільки відправник, природно, хоче мінімізувати вплив вбудовування, тому стискає повідомлення і, напевно, також шифрує його, щоб ще більше покращити безпеку комунікації. Позначимо α = m/n як відносний обсяг, який передається. Припускаючи, що будуть вбудовані біти уздовж псевдовипадкового шляху через зображення, ймовірність того, що піксель не змінюється, дорівнює ймовірності того, що він не вибирається для вбудовування, 1 − α, плюс ймовірність того, що він вибирається, α, помножена на ймовірність того, що зміна не буде необхідною, що відбувається з ймовірністю 1/2, оскільки ми вбудовуємо випадковий бітовий потік. Таким чином, для будь-якого j,

$$\Pr\{y[i]=j|x[i]=j\}=1-a+\frac{a}{2}=1-\frac{a}{2}, \qquad (2.34)$$

$$\Pr\{y[i]\neq j|x[i]\}=\frac{a}{2} \qquad (2.35)$$

Оскільки під час вбудовування LSB значення пікселів у парі LSB {2k, 2k + 1}, k = 0, . . . , $2^{n_c-1}-1$, змінюються одне на одне, але ніколи не на будь-яке інше значення, сума h_α[2k] + h_α[2k + 1] залишається незмінною для будь-якого α і, отже,

є інваріантом під час вбудовування LSB. Тут позначена гістограма стегозображення як hα. Таким чином, очікуване значення h_α [2k] дорівнює кількості пікселів зі значеннями 2k, які залишилися незмінними, плюс кількість пікселів зі значеннями 2k + 1.

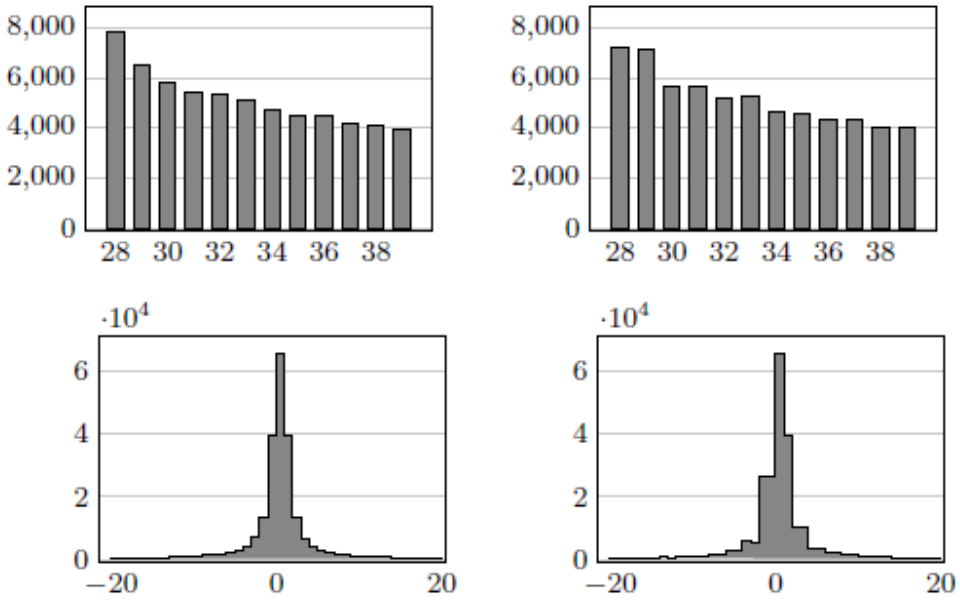


Рис. 2.5 - вплив вбудовування LSB на гістограму. Вгорі: збільшена частина гістограми зображення, показаного на рисунку 2.5, після перетворення його на 8-бітну градацію сірого до та після вбудовування LSB. Внизу: гістограма квантованих коефіцієнтів DCT того самого зображення до та після вбудовування за допомогою Jsteg. Ліві зображення відповідають зображенням обкладинки, праві цифри – стего.

які були змінені на 2k:

$$E\left[h_a[2k]\right] = \left(1 - \frac{a}{2}\right) h[2k] + \frac{a}{2} h[2k+1] \qquad (2.36)$$

$$E\left[h_a[2k+1]\right] = \frac{a}{2} h[2k] + \left(1 - \frac{a}{2}\right) h[2k+1] \qquad (2.37)$$

Зверніть увагу, що якщо повністю заповнити своє покривне зображення n бітами (α = 1), ми маємо:

$$E\left[h_1[2k]\right] = E\left[h_1[2k+1]\right] = \frac{h[2k] + h[2k+1]}{2}, k = 0, \dots, 2^{n_c-1} - 1 \quad (2.38)$$

Тому стверджуємо, що вбудовування LSB має тенденцію вирівнювати гістограму в межах кожного біну. Це призводить до характерного артефакту у вигляді сходів у гістограмі стеганографічного зображення (Рисунок 2.5), який може бути використаний як ідентифікуюча ознака для зображень, повністю вбудованих за допомогою LSB. Це спостереження кількісно оцінюється у так званій атакі на гістограму, яку ми тепер опишемо.

2.6 Атака на гістограму

У повністю вбудованому стеганографічному зображенні (α = 1) ми очікуємо

$$h_a[2k] = \frac{h_a[2k] + h_a[2k+1]}{2}, k = 0, \dots, 2^{n_c-1} - 1 \quad (2.39)$$

Офіційно, атака на гістограму зводиться до наступної комбінованої задачі тестування гіпотез:

$$H_0: h_\alpha \sim \bar{h} \quad 2.40$$

$$H_1: h_\alpha \sim \bar{h} \quad 2.41$$

яку ми розглядаємо, використовуючи χ^2 тест Пірсона. Цей тест визначає, чи рівні значення сірого кольору в стего зображенні відповідають відомому розподілу h[2k], k = 0, . . . , 2^{n_c-1}− 1. Тест χ^2 спочатку обчислює статистику тесту S,

$$s = \sum_{k=0}^{d-1} \frac{(h_a[2k] - \bar{h}[2k])^2}{\bar{h}[2k]}, \quad (2.42)$$

де d = 2^{n_c-1}. Згідно з нульовою гіпотезою, парні значення сірого кольору відповідають функції маси ймовірності $\bar{h}$[2k], а статистика тесту (2.42) приблизно слідує розподілу χ^2, S ∼ x^2_{d-1}, з d − 1 ступенями свободи. Це справедливо, якщо всі d кошики, h[2k], k = 0, . . . , 2^{n_c-1} − 1, достатньо заповнені. Будь-які непоповнені

кошики повинні бути об'єднані, щоб $\bar{h}[2k] > 4$ для всіх k, щоб S приблизно розподілявся за законом χ^2.

Можна інтуїтивно зрозуміти, що якщо парні градації сірого кольору відповідають очікуваному розподілу, значення S буде малим, що вказує на те, що стего зображення повністю вбудоване за допомогою вбудовування LSB. Великі значення S означають, що відповідність погана і сповіщають нас про те, що зображення, яке перевіряється, не є повністю вбудованим. Таким чином, ми можемо створити детектор зображень, повністю вбудованих за допомогою вбудовування LSB, встановивши поріг γ на S і вирішуючи, що це "кришка", коли S > γ, і "стего" в іншому випадку. Ймовірність ненавмисного виявлення повністю вбудованого стего зображення (ймовірність пропущення) є умовною ймовірністю того, що S > γ для стего зображення,

$$P_{MD}(\gamma) = \Pr\{S > \gamma | x \; is \; stego\}. \qquad (2.43)$$

Ми встановлюємо поріг γ так, щоб ймовірність пропуску була не більше P_{MD}. Позначаючи функцію щільності ймовірності x_{d-1}^2 як $f_{x_{d-1}^2}(x)$, поріг визначається з (2.43),

$$P_{MD}(\gamma) = \int_{\gamma}^{\infty} f_{x_{d-1}^2}(x)dx = \int_{\gamma}^{\infty} \frac{e^{-\frac{x}{2}} x^{\frac{d-1}{2}-1}}{2^{\frac{d-1}{2}}(\frac{d-1}{2})} dx \qquad (2.44)$$

Значення $P_{MD}(\gamma)$ називається p-значенням і вимірює статистичну значущість γ. Це ймовірність того, що випадкова змінна, розподілена за законом хі-квадрат з d − 1 ступенями свободи, досягне значення, більшого або рівного γ.

Атака на гістограму може виявляти зображення, повністю вбудовані з випадковими повідомленнями (α = 1), а також може бути використана для виявлення повідомлень з α < 1, якщо відомий порядок вбудовування (наприклад, послідовний). У цьому випадку m = αn біти повідомлення вбудовуються вздовж відомого шляху в зображенні, представленому за допомогою вектора індексів Path[i], i = 1, . . . , n. Оцінюючи i-не p-значення p_v[i] з гістограми {x[Path[1]], . . . , x[Path[i]]} з стего зображення, після короткої транзитної фази p_v[i] досягне значення, близького до 1. Воно раптово впаде до нуля, коли ми досягнемо кінця

повідомлення (приблизно при i ≈ αn) і залишиться на нулі, поки ми не вичерпаємо всі пікселі. Це пов'язано з тим, що статистика тесту S перестане слідувати розподілу хі-квадрат. Рисунок 2.6 показує pv[i] для послідовно вбудованого повідомлення з α = 0.4 (зображення покриття показано на рисунку 2.4). Таким чином, для послідовного вбудовування цей тест не тільки визначає з дуже високою ймовірністю, що випадкове повідомлення було вбудовано, але й оцінює довжину повідомлення.

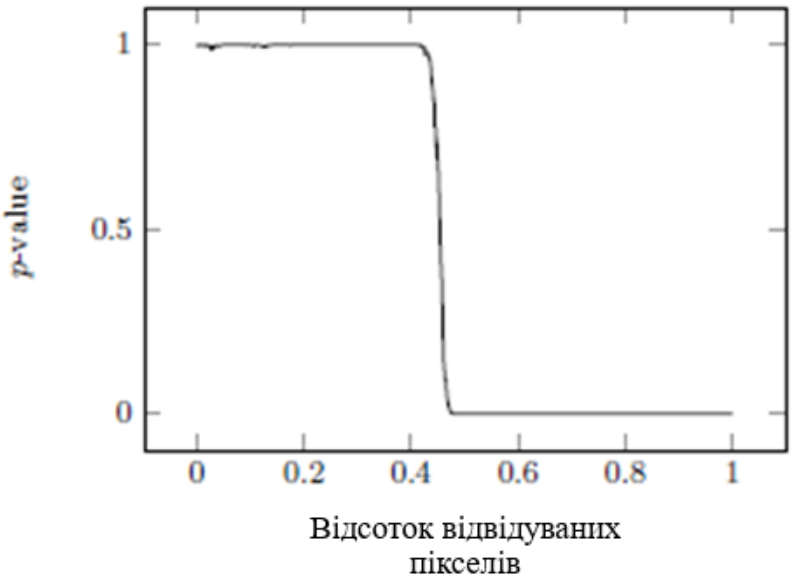


Рис. 2.6 - значення P для гістограмної атаки на послідовно вбудованою 8-бітної сірої фотографії з повідомленням довжиною a = 0.4

2.7 Кількісний напад на Jsteg

Вбудовування LSB можна застосувати до будь-якої колекції числових даних. Якщо елементи покриття слідують розподілу, про який ми маємо певні апріорні знання, ми можемо використати їх для побудови атаки наступним чином [255]. Нехай ми опишемо наші апріорні знання про покривне зображення, використовуючи деяку функцію гістограми покриття h,

$$F(h) = 0 \qquad (2.45)$$

З рівнянь (2.46) і (2.47) h можна виразити, використовуючи E[h_α], розв'язавши систему з двох лінійних рівнянь для h[2k] і h[2k + 1],

$$h[2k] = aE\left[h_a[2k]\right] - bE\left[h_a[2k+1]\right] \qquad (2.46)$$

$$h[2k+1] = -bE\left[h_a[2k]\right] + aE\left[h_a[2k+1]\right] \qquad (2.47)$$

з a = (1 − α/2)/(1 − α) та b = (α/2)/(1 − α). Використовуючи наближення $h_\alpha \approx$ E[h_α], ми можемо підставити (2.45) та (2.46) в (2.44) і, таким чином, отримати рівняння для невідомої відносної довжини повідомлення α. Це рівняння міститиме лише гістограму стего зображення h_α, яка відома.

Зверніть увагу, що ця атака забезпечує оцінку невідомої довжини повідомлення незалежно від того, чи відомий шлях його розміщення. Методи стеганографічного аналізу, які оцінюють довжину повідомлення або, точніше, кількість змін вбудовування, називаються кількісними. Ми ілюструємо цей загальний метод, атакуючи стеганографічний алгоритм Jsteg, який вбудовує дані в зображення JPEG.

Jsteg використовує принцип вбудовування LSB, застосований до квантизованих коефіцієнтів DCT, за винятком того, що пара LSB {0, 1} пропускається, оскільки дозволення вбудовування у 0 призвело б до досить неприємних артефактів. Гістограма квантизованих коефіцієнтів DCT у файлі JPEG приблизно симетрична. Ці апріорні знання можна виразити як

$$h[j] - h[-j] = 0, j = 1,2, \ldots. \qquad (2.48)$$

Більш того, гістограма монотонно зростає для j < 0 і зменшується для j > 0. Оскільки пари LSB є . . . , {−4,−3}, {−2,−1}, {0, 1}, {2, 3}, . . . і оскільки вбудовування LSB вирівнює різниці в підрахунках для кожної пари LSB, h[2k] зменшується, а h[2k + 1] збільшується з вбудовуванням для k > 0, а ефект є протилежним для k < 0 (h[2k] збільшується, а h[2k + 1] зменшується). Таким чином, використовуємо наступну функцію гістограми для атаки на Jsteg:

$$F(h) = \sum_{k>0} h[2k] + \sum_{k<0} h[2k+1] - \sum_{k<0} h[2k] \qquad (2.49)$$

Звернемо увагу, що для покривного зображення F(h) = 0, як і вимагалося. Крім того, при вбудовуванні F зростає через вплив вбудовування LSB на парні та

непарні позитивні та негативні значення DCT. Підставивши (2.46) та (2.47) у (2.48) та використовуючи наближення $h_\alpha \approx \mathrm{E}[h_\alpha]$, ми отримуємо

$$\sum_{k>0}(ah_a[2k]-bh_a[2k+1])+\sum_{k<0}(-bh_a[2k]+ah_a[2k+1]) \qquad (2.50)$$

$$-\sum_{k>0}(-bh_a[2k]-ah_a[2k+1])-\sum_{k<0}(ah_a[2k]-bh_a[2k+1]) \qquad (2.51)$$

Переставляючи члени, отримуємо рівняння для невідомої відносної довжини повідомлення α,

$$(a+b)\sum_{k>0}(h_a[2k]-h_a[2k+1])+(a+b)\sum_{k<0}(h_a[2k+1])-h_a[2k]=h_a[1] \qquad (2.52)$$

де a + b = 1/(1 − α) (h_α відомий, оскільки це гістограма стего зображення). Розв'язуючи для α, ми в кінцевому підсумку отримуємо його оцінку

$$a=1-\frac{\sum_{k\neq 0}\Delta h_a[k]}{h_a[1]} \qquad (2.53)$$

Де

$$\Delta h_a[k]=h_a[2k]-h_a[2k+1] \text{ для } k>0 \qquad (2.54)$$

$$\Delta h_a[k]=h_a[2k+1]-h_a[2k] \text{ для } k<0 \qquad (2.55)$$

Цю оцінку можна використати для формулювання наступної задачі тестування гіпотез:

$$H_0: h_\alpha \sim \bar{h} \qquad 2.56$$

$$H_1: h_\alpha \sim \bar{h} \qquad 2.57$$

де H0 та H1 відповідають гіпотезам, що h_α є гістограмою покривного та стего зображення відповідно.

Рисунок 2.7 показує гістограми відповіді детектора ˆα для α = 0, 0.1, 0.2, 0.3 і 0.5 на базі даних з 954 зображень, з яких 315, 320 та 319 походять з цифрових камер Canon G2, Canon S40 та Kodak DC 290 з розмірами 2272 × 1704 для обох камер Canon і 1792 × 1200 для зображень, зроблених Kodak DC 290. Усі зображення були отримані в сирому форматі, потім офлайн конвертовані в градації сірого і збережені як JPEG з якістю 75% перед експериментом. Оцінена довжина повідомлення ˆα

виявляється неупередженою і в цілому є хорошим детектором, здатним розрізняти покривні зображення та зображення, вбудовані за допомогою Jsteg. Звернемо увагу, що розподіл помилки оцінювача значно відрізняється від гаусівського і має досить товсті хвости.

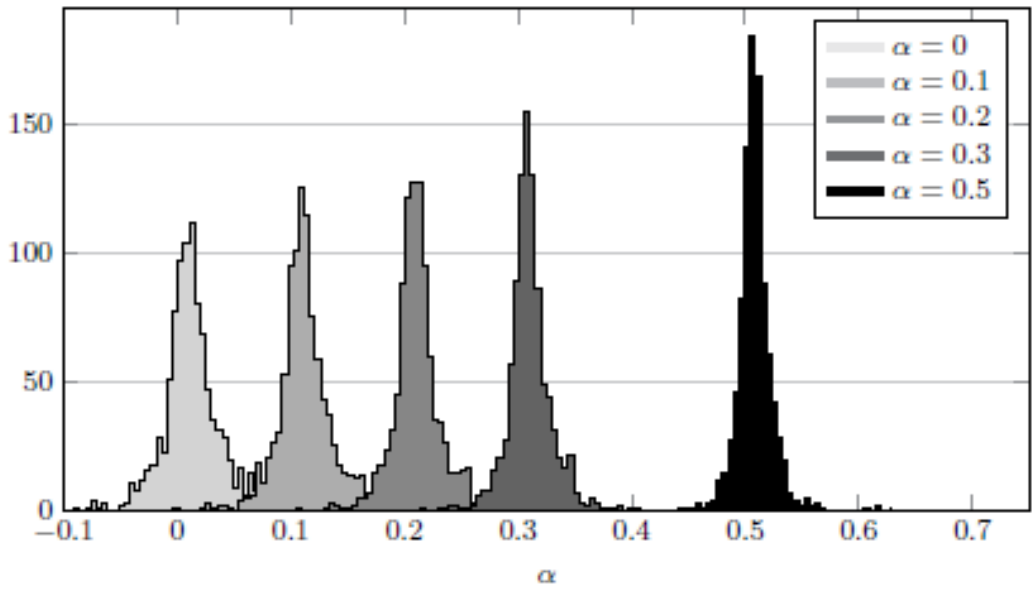


Рис. 2.7 - Гістограма очікуваної довжини повідомлення a для зображень обкладинки та стегозображень, вбудованих за допомогою Jsteg, і відносного корисного навантаження 0,1, 0,2, 0,3, 0,5.

2.8 Практичні стеганографічні методи

Визначення стеганографічної безпеки, наведене в попередньому розділі, має бути орієнтиром при розробці стеганографічних схем. Мета чітка — зберегти статистичний розподіл покривних зображень. На жаль, цифрові зображення є досить складними об'єктами, які не дозволяють точно описати себе за допомогою простих статистичних моделей. Найбільшою проблемою є їхня нестабільність і неоднорідність. Хоча можливо отримати прості моделі окремих маленьких плоских сегментів в зображенні, більш складні текстури часто становлять нездоланну проблему для моделювання через брак даних для точного локального моделювання. Цифрові зображення, отримані за допомогою сенсорів,

демонструють безліч складних локальних залежностей, які можуть бути порушені змінами, внесеними під час вбудовування, залишаючи статистично виявлені артефакти. Отже, відсутність хороших моделей зображень відкриває простір для евристичних методів.

2.8.1 Стеганографія, що зберігає модель

Цей принцип безпосередньо випливає з визначення стеганографічної безпеки. Дизайнер спочатку обирає модель покривних зображень, а потім розробляє стеганографічну схему так, щоб вона зберігала цю модель. Це гарантує, що стего-схема буде невидимою, якщо обрана модель повністю описує покриття. Найпростіша модель, ймовірно, складається з послідовності незалежних та ідентично розподілених (iid) випадкових змінних. У цій моделі покриття повністю описується функцією розподілу ймовірності. Це означає, що для даного покривного зображення потрібно зберегти його першу статистику або гістограму. Варто зазначити, що це призведе до невидимих стегосистем як для однорідних, так і для неоднорідних джерел покриття.

Існує багато підходів, які можна застосувати для розробки стеганографічної схеми, що зберігає гістограму. Підхід ґрунтується на загальній ідеї статистичного відновлення, в якій частина зображення резервується і не використовується під час вбудовування, щоб згодом її можна було використовувати для гарантії збереження першої статистики.

2.8.2 Статистичне відновлення

Ілюстрування принципу статистичного відновлення на прикладі стеганографічного алгоритму OutGuess, вперше представленого Провосом. OutGuess вбудовує повідомлення в JPEG-зображення, незначно змінюючи квантовані коефіцієнти DCT. Він також зберігає гістограму всіх коефіцієнтів DCT. Модель iid можна евристично обґрунтувати тим, що коефіцієнти DCT в окремому

блоці 8 × 8 в основному є декорельованими, а також тим, що міжблочні залежності між коефіцієнтами DCT значно слабші, ніж залежності між сусідніми пікселями в просторовій області.

Стеганографічні методи, основані на статистичному відновленні, такі як OutGuess, є процедурами з двома проходами. У першому (вбудовувальному) проході використовується стего-ключ для вибору псевдовипадкової підмножини D_e з усіх коефіцієнтів DCT (як яскісних, так і хроматичних), які будуть використані для вбудовування. Подібно до першого JPEG стеганографічного алгоритму Jsteg, OutGuess вбудовує біт повідомлення, використовуючи просте вбудовування LSB, в коефіцієнти з D_e, пропускаючи всі коефіцієнти, рівні 0 або 1, щоб уникнути внесення деструктивних артефактів. У другому проході вносяться корективи до коефіцієнтів DCT за межами набору D_e, щоб узгодити гістограму стего-зображення з гістограмою покривного зображення.

Перед початком вбудовування OutGuess обчислює максимальну довжину випадково розподіленого повідомлення (максимальний виправний коректований обсяг), який можна вбудувати в покривне зображення під час першого проходу, при цьому забезпечуючи наявність достатньої кількості коефіцієнтів для фази корекції, щоб налаштувати гістограму на її початкові значення. Читача заохочують перевірити, що максимальний виправний коректований обсяг визначається найбільш незбалансованою парою LSB, яка є парою {2k, 2k + 1} з найбільшим співвідношенням.

$$\frac{\max\{h[2k], h[2k+1]\}}{\min\{h[2k], h[2k+1]\}} \qquad (2.58)$$

Оскільки гістограма коефіцієнтів DCT в одноразово стиснутому JPEG-зображенні має пік на нулі (див. обговорення в розділі 2), і оскільки пара LSB {0, 1} пропускається під час вбудовування, найбільш незбалансованою парою LSB є {−2,−1}. Оскільки h[−2] < h[−1] у типовому покривному зображенні, після вбудовування максимального виправного обсягу всі залишкові коефіцієнти зі значенням −2 доведеться змінити на −1 під час фази корекції.

Позначаючи n_{01} як кількість усіх коефіцієнтів DCT, які не дорівнюють 0 або 1, максимальний виправний коректований обсяг становитиме $a_{max}n_{01}$, де $0 \leq a_{max} \leq 1$. Оскільки всі $a_{max}n_{01}$ коефіцієнти вибираються псевдовипадковим чином у фазі вбудовування, кількість невикористаних коефіцієнтів DCT зі значенням −2 після вбудовування дорівнює $(1 - a_{max})$h[−2]. Щоб відновити кількість −1 у стего-зображенні, це значення має бути більшим або рівним очікуваному зменшенню кількості коефіцієнтів зі значенням −1, яке становить $(a_{max}/2)$h[−1] − $(a_{max}/2)$h[−2]. Це пояснюється тим, що, припускаючи, що вбудовується випадкове повідомлення, ймовірність того, що біт повідомлення відповідатиме LSB значення −1, становить 1/2, і, отже, в середньому $(a_{max}/2)$h[−1] коефіцієнтів зі значенням −1 залишаться незмінними під час вбудовування, а така ж кількість буде змінена на −2. Другий термін, $(a_{max}/2)$h[−2], є очікуваною кількістю коефіцієнтів зі значенням −2, які будуть змінені на −1 під час вбудовування. Оскільки h[−2] < h[−1], очікуване падіння кількості коефіцієнтів зі значенням −1 становитиме різницю $(a_{max}/2)$h[−1] − $(a_{max}/2)$h[−2]. Таким чином, ми отримуємо таку нерівність і, зрештою, верхню межу для максимального виправного обсягу a_{max}:

$$(1 - a_{max})h[-2] \geq \frac{a_{max}}{2}h[-1] - \frac{a_{max}}{2}h2[-2] \qquad (2.59)$$

$$a_{max} \leq \frac{2h[-2]}{h[-1] + h[-2]} \qquad (2.60)$$

Ця умова гарантує, що в кінці фази вбудовування в середньому буде достатньо невикористаних коефіцієнтів зі значенням −2, які можна повернути назад до −1, щоб забезпечити збереження пар LSB {−2,−1} після вбудовування. Оскільки це найбільш незбалансована пара LSB, збереження пар LSB практично всіх інших також можна забезпечити за допомогою тієї ж фази корекції. Слід зазначити, що деякі дуже слабо населені гістограми на краях гістограми DCT можуть бути не відновлені коректно під час другої фази, але, оскільки їх кількість статистично незначна, вплив на статистичну виявленість є незначним. Середня ємність a_{max} алгоритму OutGuess для типових природних зображень становить приблизно 0.2 bpnc (біти на ненульовий коефіцієнт DCT).

Стеганографічні схеми, які вбудовують повідомлення в просторовій області, потребують складніших моделей, оскільки сусідні пікселі більш корельовані, ніж коефіцієнти DCT у файлі JPEG. Ці кореляції не можна зафіксувати за допомогою першої статистики. Натомість можна використовувати спільну статистику пар сусідніх пікселів, статистику різниць між сусідніми пікселями або ланцюги Маркова.

2.8.3 Стеганографія на основі моделей

Стеганографія, основана на статистичному відновленні, обирає вибіркову статистику (наприклад, гістограму) як модель для збереження. На відміну від цього, стеганографія на основі моделей підганяє параметричну модель через вибіркові дані та зберігає цю модель, що ґрунтується на даних, без необхідності корекційного етапу. Покривне зображення моделюється як випадкова змінна, яку можна розділити на дві компоненти: x = (x_{inv}, x_{emb}), де x_{inv} є інваріантним щодо вбудовування, а x_{emb} може бути змінено під час вбудовування. Ми позначаємо область кожної випадкової змінної як x_{inv} та x_{emb}. Наприклад, ми можемо розглядати вбудовування LSB у 8-бітних градаціях сірого, де $x_{inv} \in \{0, 1\}^7 = x_{inv}$ — це 7 найбільш значущих бітів (або індекс пари LSB), а $x_{emb} \in \{0, 1\} = x_{emb}$ — це LSB x.

Модель покриття формується умовними ймовірностями $\Pr\{x_{emb}|x_{inv}\}$. Ці ймовірності будуть потрібні для витягування повідомлення і, отже, мають бути відомі отримувачу. Це можна організувати, зробивши $\Pr\{x_{emb}|x_{inv}\}$ залежними лише від інваріантної компоненти x_{inv}.

По-перше, набір усіх покривних елементів (пікселів або коефіцієнтів DCT) записується як об'єднання неперетинних підмножин

$$\bigcup_{x_{inv} \in x_{inv}} C(x_{inv}) \qquad (2.61)$$

де C(x_{inv}) — це набір покривних елементів, інваріантна частина яких дорівнює xinv. Алгоритм вбудовування вбудовує частину повідомлення в кожен C(x_{inv}) таким чином. Спочатку біти повідомлення кодуються з використанням символів з x_{emb}, а потім символи підганяються так, щоб вони з'являлися з ймовірностями Pr$\{x_{emb}|x_{inv} = x_{inv}\}$. Це досягається шляхом пропускання символів повідомлення через декомпресор ентропії, призначений для стиснення символів з x_{emb}, розподілених відповідно до тих самих умовних ймовірностей. Коли декомпресор отримує x_{emb}, розподілений рівномірно в x_{emb}, він видасть символи з ймовірностями Pr$\{x_{emb}|x_{inv}= x_{inv}\}$. Таким чином, коли x_{emb} усіх покривних елементів з C(x_{inv}) замінюється на перетворені символи, елементи стего-зображення відповідатимуть моделі покривного зображення, як і потрібно.

Частка бітів, які можна вбудувати в кожен елемент C(x_{inv}), дорівнює ентропії Pr$\{x_{emb}|x_{inv}= x_{inv}\}$ або де |C(x_{inv})| — це кардинальність C(x_{inv}).

$$H(\Pr\{x_{emb}|x_{inv} = x_{inv}\}) = -\sum_{x_{emb}} P_{x_{emb}|x_{inv}}(x_{emb}|x_{inv}) \log_2 P_{x_{emb}|x_{inv}}(x_{emb}|x_{inv}) \quad (2.62)$$

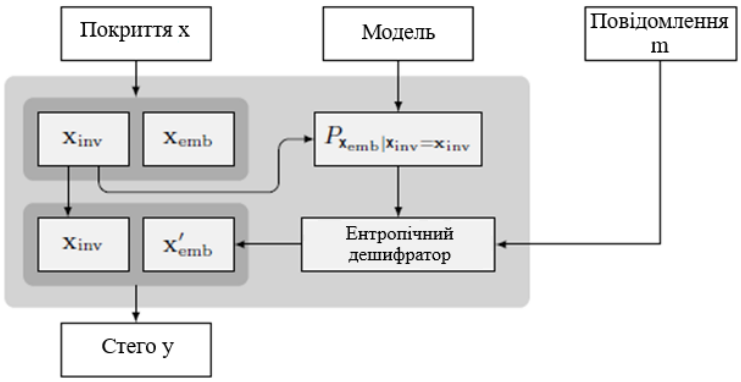


Рис. 2.8. - Модельна стеганографія (вбудовування)

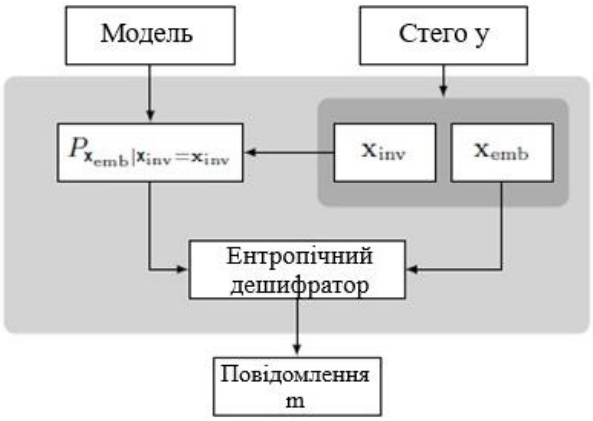


Рис. 2.9 - Модельна стеганографія (витягання)

Де ми жертвуємо для стислості

$$P_{x_{emb}|x_{inv}}(x_{emb}|x_{inv}) = \Pr\{x_{emb} = x_{emb}|x_{inv} = x_{inv}\} \qquad (2.63)$$

це загальна ємність вбудовування

$$\sum_{x_{inv}} |C(x_{inv})|H\ (\Pr\{x_{emb}|x_{inv} = x_{inv}\}) \qquad (2.64)$$

де $|C(x_{inv})|$ це потужність $C(x_{inv})$.

Щоб проілюструвати підхід на основі моделей, ми опишемо конкретну реалізацію стеганографії в JPEG-зображеннях. Подібно до OutGuess або Jsteg, коефіцієнти DCT, рівні 0 або 1, не використовуються для вбудовування, а механізм вбудовування полягає у перевертанні LSB. Також x_{inv} = $\{0, 1\}^7$, а x_{emb} = {0, 1}. Парадигма стеганографії на основі моделей застосовується до кожного режиму DCT окремо. Отже, на початку покривний JPEG-файл розбивається на 64 підмножини, які відповідають 64 режимам DCT (просторовим частотам). Нехай h[i] буде гістограмою коефіцієнтів DCT для одного фіксованого режиму. Оскільки суми h[2i] + h[2i + 1] є інваріантними щодо вбудовування LSB для всіх i, ми можемо використати цю інваріантність і підганяти параметричну модель h(x) через точки ((2i + 2i + 1)/2, (h[2i] + h[2i + 1])/2). Наприклад, ми можемо моделювати коефіцієнти DCT за допомогою узагальненої моделі Коші з pdf.

$$h(x) = \frac{p-1}{2s}\left(a + \frac{|x|}{s}\right)^{-p} \qquad (2.65)$$

і визначити параметри, використовуючи оцінку максимального правдоподібності. Позначаючи 7 найбільш значущих бітів цілого числа a як $MSB_7(a)$, ми визначаємо модель, використовуючи умовні ймовірності

$$\Pr\{x_{emb} = 0 | x_{inv} = MSB_7(2i)\} = \frac{h(2i)}{h(2i) + h(2i+1)} \qquad (2.66)$$

$$\Pr\{x_{emb} = 1 | x_{inv} = MSB_7(2i)\} = \frac{h(2i+1)}{h(2i) + h(2i+1)} \qquad (2.67)$$

Відправник продовжує процес вбудовування, вибираючи всі коефіцієнти DCT h[2i] + h[2i + 1] на вибраному режимі DCT, які дорівнюють 2i або 2i + 1. Їх LSB замінюються на сегмент повідомлення, який був декомпресований за допомогою арифметичного декомпресора до довжини h[2i] + h[2i + 1]. Декомпресор розроблений для перетворення послідовності рівномірно розподілених біт повідомлення в упереджену послідовність, де 0 і 1 з'являються з ймовірностями (2.66)–(2.67). Оскільки ми замінюємо одну бітову послідовність на іншу з тією ж розподілом, модель (2.66)–(2.67) буде збережена.

Одержувач спочатку конструює модель і обчислює ймовірності, наведені в (2.66)–(2.67). Це можна досягти, оскільки h[2i] + h[2i + 1] є інваріантним щодо змін, внесених під час вбудовування. Індивідуальні сегменти повідомлення витягуються шляхом подання LSB для кожного режиму DCT та кожної пари LSB {2i, 2i + 1} в арифметичний компресор і їх конкатенації.

Цей конкретний приклад стеганографії на основі моделей призначений для збереження моделі гістограм усіх окремих режимів DCT. Це контрастує з OutGuess, який зберігає вибіркову гістограму всіх коефіцієнтів DCT, а не обов'язково гістограми режимів DCT. Для JPEG-зображень якості 80% середня ємність вбудовування цього алгоритму становить приблизно 0.8 bpnc, що є вражаюче великим значенням, враховуючи обсяг моделі, і в чотири рази більшим, ніж для OutGuess.

Тепер ми розрахуємо ефективність вбудовування цього алгоритму, визначену як середня кількість бітів, вбудованих на одиницю спотворення. Щоб спростити нотацію, ми встановлюємо

$$p_0 = \Pr\{x_{emb} = 0 | x_{emb} = MSB_7(2i)\} \qquad (2.68)$$

Середня кількість бітів, вбудованих в один коефіцієнт DCT, рівний 2i або 2i + 1 для одного фіксованого режиму DCT, становить

$$H(p_0) = -p_0 \log_2 p_0 - (1 - p_0) \log_2 (1 - p_0) \qquad (2.69)$$

Зміна вбудовування виконується, коли LSB коефіцієнта не відповідає упередженому бітові повідомлення. Оскільки ймовірність того, що упереджений біт повідомлення дорівнює 0, така ж, як ймовірність того, що LSB коефіцієнта дорівнює 0, що дорівнює p_0 зміна LSB вимагає ймовірності $p_0(1 - p_0) + (1 - p_0)p_0 = 2p_0(1 - p_0)$. Отже, ефективність вбудовування становить

$$e(p_0) = \frac{-p_0 \log_2 p_0 - (1 - p_0) \log_2 (1 - p_0)}{2p_0(1 - p_0)} \qquad (2.70)$$

Звернемо увагу, що $e(p_0)$ завжди більша або дорівнює 2 (Рисунок 2.10). Дивно, але це вище, ніж ефективність вбудовування простого LSB-вбудовування, яка становить 2, оскільки в LSB-вбудовуванні в середньому змінюється кожен другий LSB.

Підсумовуючи, цей конкретний приклад стеганографії на основі моделей зберігає моделі гістограм усіх 64 режимів DCT і робить це, забезпечуючи ефективність вбудовування, що перевищує 2. Це є значним поліпшенням у порівнянні з наївним Jsteg.

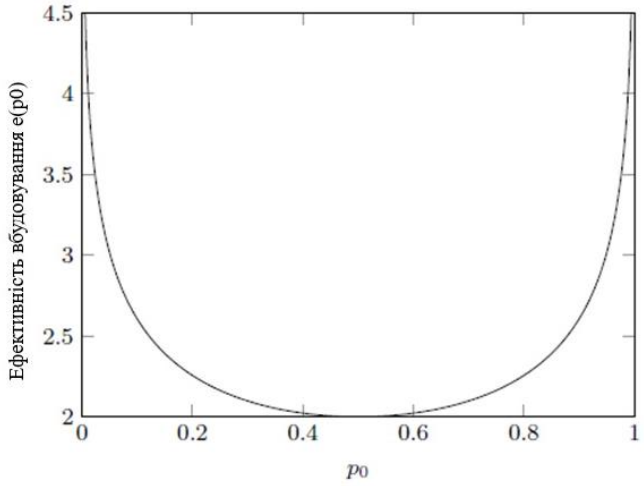


Рис. 2.10 - Ефективність вбудовування стеганографії на основі моделі для jpeg зображень

Існує більш розвинена версія цього алгоритму, яка намагається зберегти одну вищу статистику, звану «блоковістю», що визначається як сума розривів уздовж меж 8 × 8 піксельних блоків у просторовій області. Це досягається за допомогою ідеї статистичного відновлення, шляхом внесення додаткових змін до невикористаних коефіцієнтів DCT в ітераційний спосіб, щоб відрегулювати блоковість до її первісного значення в покривному зображенні. Оригінальну версію стеганографії на основі моделей позначають як MBS1, а більш розвинену версію з де-блокуванням — як MBS2.

2.8.4 Стеганографія шляхом імітації природного оброблення

Схеми стеганографії, що зберігають модель, є недетектованими в межах обраної моделі. Однак, якщо модель не охоплює джерело покриття в повному обсязі, все, що потрібно для побудови алгоритму стеганалізу, — це виявити статистичну величину, яка порушується внаслідок вбудовування. Виявляється, що знайти таку статистику зазвичай не надто складно. Часто, в стеганографії через статистичне відновлення, додаткові зміни на етапі корекції лише ускладнюють ситуацію і фактично полегшують стеганалізу. Збереження більш складного джерела покриття не є практичним вирішенням цієї проблеми, оскільки схеми, засновані на статистичному відновленні, не добре масштабуються з ускладненням моделі. Наприклад, не зовсім зрозуміло, як одночасно зберегти гістограму коефіцієнтів DCT і статистику пар коефіцієнтів DCT з сусідніх 8 × 8 блоків, не жертвуючи ємністю вбудовування. Хоча було описано практичний метод вбудовування, здатний приблизно зберігати кілька статистик (Метод корекції ознак), цей підхід поки не призвів до створення безпечних стеганографічних алгоритмів.

Відсутність точних моделей виправдовує евристичні підходи до стеганографії, такі як ті, що намагаються замаскувати вбудовування як природний процес. Якщо ефект вбудовування буде не відрізнятися від якогось природного оброблення, стего-зображення повинні залишатися сумісними з розподілом

покривних зображень. Маскуючи вбудовування як суперпозицію шуму з заданими статистичними властивостями. Цей підхід може суттєво підвищити шанси на те, що стеганографія залишиться непоміченою, оскільки зміни в зображенні виглядатимуть більш природними.

2.8.5 Стохастична модуляція

Процес цифрового захоплення зображень підлягає впливу численних джерел шуму. Навіть коли знімуть два зображення однієї і тієї ж сцени в однакових умовах і з ідентичними налаштуваннями камери, зображення відрізнятимуться за рахунок шумового компоненту через присутність випадкових явищ, викликаних квантовими властивостями світла (шум від спалахів) і шумом, що виникає в електронних компонентах сенсора. Це натякає на ідею створення стеганографічного методу, так що вплив вбудовування нагадує суперпозицію шуму сенсора під час захоплення зображення. Стеганалісту доведеться розрізняти, чи є компонент шуму зображення лише наслідком захоплення зображення або містить компонент, що виникає внаслідок вбудовування повідомлення. Це, по суті, евристичний план для створення стего-зображень, сумісних з розподілом покривного джерела.

Мета — створити схему вбудовування, так що вплив вбудовування буде еквівалентний додаванню до покривного зображення сигналу, отриманого незалежними реалізаціями випадкової змінної η з заданою функцією ймовірності щільності fη. Оскільки цифрові зображення представлені з обмеженою глибиною бітів, шум також необхідно адекватно квантувати. Припускаючи для спрощення і без втрати загальності, що працюємо з градаціями сірого, позначаємо r[i] = round(η[i]) як реалізації η після округлення до цілих чисел з набору {0, . . . , 255}. Округлена послідовність шуму r[i] називається стего-шумом. Функція маси ймовірності стего-шуму є

$$p[k] = \Pr\{r[i] = k\} = \int_{k-\frac{1}{2}}^{k+\frac{1}{2}} f_n(x)dx \text{ для будь} - \text{яких } i, k \quad (2.71)$$

Теоретично, додаючи реалізації стего-шуму до покривного зображення, ми могли б вбудувати H(p) біт (ентропію round(η)) на кожному пікселі. Замість того, щоб намагатися розробити практичний метод, який досягає цієї ємності, що є непростим завданням, ми пропонуємо простий субоптимальний метод.

Працюючи з бітами, представленими парою {−1, 1}, замість {0, 1}. Таким чином, відтепер до кінця цього розділу −1 і 1 представлятимуть двійкові 0 і 1 відповідно. Далі визначимо функцію парності π з такою антисиметричною властивістю:

$$\pi(u + v, v) = -\pi(u, u) \quad (2.72)$$

для всіх цілих чисел u і v. Наступна функція, наприклад, задовольняє цю вимогу:

$$\pi(u, v) = \begin{cases} (-1)^u \text{ для } 2k[v] \le u \le 2k[v] + [v] - 1 \\ -(-1)^u \text{ для } (2k-1)|v| \le u \le 2k|v| - 1 \\ 0 \text{ для } v = 0 \end{cases} \quad (2.73)$$

де k — це ціле число.

Алгоритм вбудовування починається з генерації псевдовипадкового шляху через зображення за допомогою стего-ключа та двох незалежних послідовностей стего-шуму r[i] і s[i] з функцією маси ймовірності (2.71). Відправник слідує вбудовувальному шляху і вбудовує один біт повідомлення, m, в піксель x[i], якщо і тільки якщо r[i] ≠ s[i]. У цьому випадку відправник завжди може вбудувати один біт, додаючи або r[i], або s[i] до x[i], оскільки завдяки антисиметричній властивості функції парності π (2.72)

$$\pi(x[i] + s[i], r[i] - s[i]) = -\pi(x[i] + s[i] + r[i] - s[i], r[i] - s[i]) \quad (2.74)$$

$$\pi(x[i] + r[i], r[i] - s[i]) \quad (2.75)$$

У випадку, коли r[i] = s[i], відправник не вбудовує жодного біта, замість цього замінює x[i] на y[i] = x[i] + r[i] і продовжує вбудовування в наступному пікселі за псевдовипадковим шляхом.

Однак, щоб завершити алгоритм вбудовування, потрібно вирішити ще одну технічну деталь процесу вбудовування. Якщо під час вбудовування y[i] = x[i] + r[i] виходить за межі динамічного діапазону, відправнику залишається мало варіантів, окрім як трохи відступити від моделі стего-шуму та додати r'[i], щоб забезпечити $\pi(x[i] + r'[i], r[i] - s[i]) = m$, при цьому $|r'[i] - r[i]|$ має бути якомога меншим.

Отримувач спочатку використовує стего-ключ, щоб згенерувати ті ж самі послідовності стего-шуму, r[i] та s[i], а також псевдовипадковий шлях через пікселі. Біт повідомлення зчитується з пікселів стего-зображення y[i] як паритет $m = \pi(y[i], r[i] - s[i])$. Жоден біт не витягується з пікселя y[i], якщо r[i] = s[i].

Отже, у підсумку відправник починає з генерації двох незалежних послідовностей стего-шуму з потрібною функцією маси ймовірності, а потім на кожному пікселі намагається вбудувати один біт повідомлення, додаючи один з двох зразків стего-шуму. Це працює завдяки антисиметричній властивості функції парності. Якщо два зразки стего-шуму однакові, процес вбудовування не вбудовує жодних бітів. Проте відправник все ж додає шум до зображення, щоб стего-зображення дійсно отримувалося шляхом додавання шуму з даною pmf до покривного зображення, як і вимагалося.

Стовхастична модуляція вбудовує один біт на кожному пікселі, поки $r[i] \neq s[i]$. Отже, відносна ємність вбудовування становить $1 - \Pr\{r = s\} = 1 - \sum_k p[k]^2$ біт на піксель, де ймовірності можна обчислити за формулою (2.71). Випадкові джерела шуму під час захоплення зображення, такі як шум фотонів і шум зчитування, добре моделюються як гауссові випадкові змінні з нульовим середнім значенням і дисперсією σ^2. У цьому випадку відносна ємність вбудовування на піксель, як показано на малюнку 2.11. Оскільки послідовності стего-шуму з більшою ймовірністю будуть однаковими для малого σ, ємність зростає з дисперсією шуму. Також зауважте, що відправник може передавати приблизно 0.7 біт на піксель, використовуючи квантизований стандартний гауссовий шум N(0, 1).

На кожному пікселі вбудовується k p[k]² біт, а не H(p) біт, що є ентропією стего-шуму. Хоча не відомо, як створити стеганографічні системи, які досягають теоретичної ємності вбудовування для загального стего-шуму, існують конструкції, що досягають ємності для спеціальних випадків p, наприклад, коли амплітуда стего-шуму не перевищує 1.

Зверніть увагу, що стохастична модуляція є субоптимальною загалом, оскільки на кожному пікселі вбудовується лише $1 - \sum_k p[k]^2$ біта, а не H(p) біт, що є ентропією стего-шуму. Хоча не відомо, як створити стеганографічні системи, які досягають теоретичної ємності вбудовування для загального стего-шуму, існують конструкції, що досягають ємності для спеціальних випадків p, наприклад, коли амплітуда стего-шуму не перевищує 1.

Незважаючи на те, наскільки правдоподібною звучить евристика стохастичної модуляції, факт залишається таким: її можна надійно виявити за допомогою сучасних методів стеганалітики, заснованих на витяганні ознак і машинному навчанні. Основна причина полягає в тому, що під час захоплення зображення шум вводиться до того, як сигнал буде квантований у перетворювачі A/D та подальше оброблено. Додавання шуму до фінального зображення TIFF або BMP не є тим самим, оскільки це зображення вже містить безліч складних залежностей між сусідніми пікселями через обробку в камері, таку як демозайка, корекція кольору та фільтрація. Отже, стего-шум має бути накладений на вихідні дані з сенсора, а не на фінальне зображення. Проте наразі неясно, як вбудовувати біти в домені пікселів, модифікуючи вихідні дані сенсора. Можливим рішенням є застосування методів кодування для зв’язку з несучими вибірковими каналами.

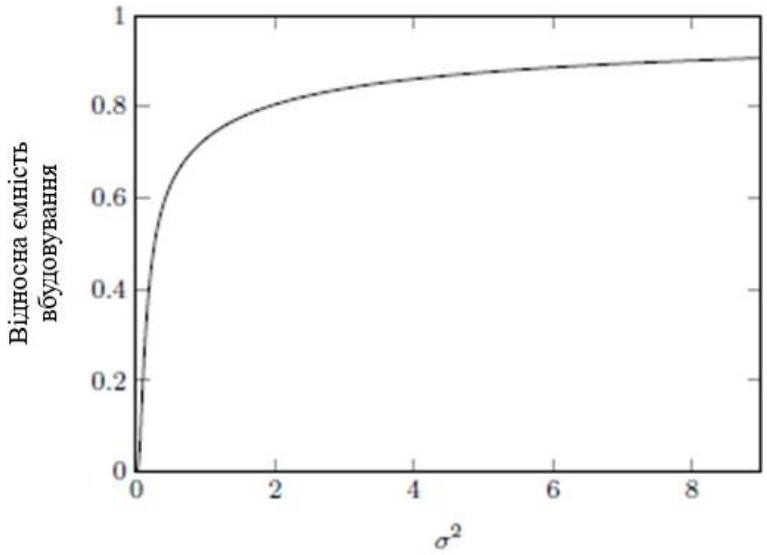


Рис. 2.11 - Відносна вбудована ємність стохастичної модуляції

2.9 Питання оптимального стего шуму

Для ідеального випадку стохастичної модуляції, здатної передавати H(p) біт на піксель, природно виникає питання про найкращий стего-шум, який дозволив би вбудувати найбільше навантаження з найменшими спотвореннями. Стохастична модуляція з таким стего-шумом мінімізувала б спотворення вбудовування, що інтуїтивно могло б зменшити статистичну детектованість.

Властивості оптимального стего-шуму, очевидно, будуть залежати від того, як ми вимірюємо спотворення між покривними та стего-зображеннями, d(x, y). Очікуване значення спотворення вбудовування на піксель, E[d(x, y)], буде деякою функцією ймовірнісної маси стего-шуму p і позначатиметься як d(p) = E[d(x, y)].

Накладаючи обмеження на спотворення вбудовування D, ми прагнемо визначити p_{opt}, яке максимізує відносне навантаження вбудовування.

$$P_{opt} = \arg\max H(p) \quad d(p) \leq D \qquad (2.76)$$

Цей вираз у теорії інформації відомий як межа швидкості-спотворення, яка пов'язує швидкість комунікації та спотворення. Відносне навантаження для оптимального розподілу H(p_{opt}) залежить від межі спотворення D і є також функцією міри спотворення d. Саме тому позначаємо його як H_d(D) = H(p_{opt}). Ми

можемо стверджувати, що, враховуючи обмеження на спотворення вбудовування D, відносне навантаження α, яке може бути вбудоване з використанням будь-якого випадку стохастичної модуляції, повинно задовольняти умову:

$$a \leq H_d(d) \qquad (2.77)$$

Альтернативно, відносне навантаження α може бути вбудоване зі спотворенням, яке не менше ніж $H_d^{-1}(\alpha)$, де H_d^{-1} є оберненою функцією до H_d. Це переводиться в наступну межу на ефективність вбудовування (співвідношення між навантаженням і спотворенням):

$$e \leq \frac{a}{H_d^{-1}(a)} \qquad (2.78)$$

Тепер знайдемо розподіл стего-шуму p_{opt} для конкретного вибору міри спотворення, $d_\gamma(x,y) = |x-y|^\gamma$. Очікуване спотворення на піксель становить:

$$d_\gamma(p) = \sum_k p[k][k]^\gamma \leq D \qquad (2.79)$$

Тепер покажемо, що оптимальний розподіл стего-шуму є дискретним узагальненим гаусівським

$$P_{opt}[k] = \frac{e^{-\lambda[k]^\lambda}}{Z(\lambda)} \qquad (2.80)$$

Де

$$Z(\lambda) = \sum_k e^{-\lambda[k]^\gamma} \qquad (2.81)$$

є нормувальним коефіцієнтом. Щоб це побачити, запишемо для ентропії H(p) довільного розподілу p, який задовольняє межі (2.79):

$$H(p) = \sum_k p[k] \log \frac{1}{p[k]} = \sum_k p[k] \log \frac{1}{P_{opt}[k]} + \sum_k p[k] \log \frac{P_{opt}[k]}{p[k]} \qquad (2.82)$$

$$\leq \log Z(\lambda) + \lambda \sum_k p[k][k]^\gamma \leq \log Z(\lambda) + \lambda D \qquad (2.83)$$

де скористалися невід'ємністю дивергенції Кульбака–Лейблера

$$0 \le D_{KL}(p||p_{opt}) = -\sum_k p[k] \log \frac{p_{opt}}{p[k]} \qquad (2.84)$$

З властивості дивергенції Кульбака–Лейблера рівність досягається, коли $p = p_{opt}$, що доводить оптимальність p_{opt}. Параметр λ визначається з вимоги $\sum_k p[k][k]^\gamma = D$.

Зверніть увагу, що коли спотворення вимірюється як енергія γ = 2, межа (2.83) обмежує дисперсію p. У цьому випадку, шум стего з максимальною ентропією є дискретним гауссовим, відповідно до класичного результату з теорії інформації, що шум з найвищою ентропією серед усіх розподілів з обмеженою дисперсією є гаусовим розподілом.

Для стеганографії, де зміни при вбудовуванні обмежені значеннями ±1, розподіл стего-шуму задовольняє умові p[k] = 0 для k ∈ {-1, 0, 1\}, і $d_\gamma(p)$ стає швидкістю зміни для будь-якого γ > 0. У цьому випадку функцію $H_{d_\gamma}(x)$ можна визначити аналітично [233] як тернарну ентропійні функцію.

$$H_{d_\gamma}(x) = -x \log_2 x - (1-x) \log_2 (1-x) + x \qquad (2.85)$$

2.10 Стегоаналіз

Стегоаналіз — це наукова дисципліна та практичний інструмент, який спрямований на виявлення прихованої інформації в цифрових носіях, такій як зображення, аудіо, відео або текстові файли, що була вбудована за допомогою методів стеганографії. Його основна мета полягає у визначенні самого факту існування прихованих даних, і, за можливості, їх видобутку або знищення. У сучасному світі, де стеганографія активно використовується для захисту інформації або, навпаки, для приховування шкідливих дій, стегоаналіз набув особливого значення в кібербезпеці, цифровій криміналістиці та інших галузях.

Процес стегоаналізу передбачає аналіз цифрових носіїв на предмет змін, які могли бути викликані впровадженням прихованої інформації. Наприклад, вбудовування даних у зображення може викликати ледь помітні зміни у значеннях пікселів або статистичних характеристиках файлу, таких як гістограми яскравості чи розподіл кольорів. У випадку аудіо чи відео це можуть бути відхилення в частотному спектрі чи порушення амплітудних характеристик. Основний інструментарій стегоаналізу варіюється від простого статистичного аналізу до складних методів, таких як машинне навчання, де алгоритми навчаються розпізнавати носії із прихованими даними, базуючись на великих наборах прикладів.

Одним із ключових завдань стегоаналізу є ідентифікація методу приховування даних. Якщо алгоритм відомий, це може значно спростити процес виявлення або вилучення інформації. Проте в більшості випадків стегоаналіз виконується в умовах невизначеності, коли ані алгоритм, ані вихідний (оригінальний) носій невідомі. Такий підхід називається «сліпим» стегоаналізом і є особливо складним, оскільки вимагає створення універсальних моделей, здатних виявляти приховану інформацію без будь-яких підказок

Стегоаналіз знаходить широке застосування в різних сферах. У кібербезпеці він використовується для виявлення прихованих каналів передачі даних, які можуть використовуватися зловмисниками для комунікації або передачі

конфіденційної інформації. У криміналістиці стегоаналіз застосовується для розслідування цифрових злочинів, аналізуючи носії на наявність прихованої інформації, наприклад, у файлах підозрюваних. У військовій сфері його роль полягає в перехопленні та аналізі матеріалів, які можуть містити секретну інформацію, передану прихованими шляхами.

Однак розвиток стеганографічних методів ставить перед стегоаналізом серйозні виклики. З кожним роком алгоритми приховування стають дедалі складнішими, що ускладнює виявлення прихованих даних. Крім того, значний обсяг цифрових даних і обмеження ресурсів змушують дослідників шукати баланс між точністю виявлення та ефективністю алгоритмів.

Таким чином, стегоаналіз є важливою частиною сучасної інформаційної безпеки, спрямованою на боротьбу з приховуванням інформації. Його розвиток вимагає міждисциплінарного підходу, що включає математику, комп’ютерні науки та теорію сигналів, а також адаптації до нових викликів і технічних удосконалень у стеганографії.

2.11 Типові сценарії

Будь-яка інформація про стеганографічний канал, яка доступна відправнику в пріорі, може допомогти у здійсненні атаки. Нагадаємо, що стеганографічний канал складається з п'яти основних елементів:

канал, який використовується для обміну даними між учасниками комунікації,

джерело покриття,

джерело повідомлень,

алгоритми вбудовування та вилучення даних,

джерело стегоключів, що керує алгоритмами вбудовування/вилучення.

Припускаємо, що наглядач є пасивним, що означає, що він пасивно спостерігає за комунікацією і не втручається в неї жодним чином. Отже, фізичний канал, який використовується для обміну інформацією, є безвтратним і не має

жодного впливу на стеганалітичні або стеганографічні аспекти. Проте інші чотири елементи — алгоритм вбудовування та джерела покриттів, повідомлень і стегоключів — є критично важливими. Загалом, чим більше інформації відомо, тим успішніше можна виявити наявність таємно вбудованих повідомлень. Хоча, безумовно, існують різні ситуації з різними рівнями деталей, доступними для спостерігача щодо окремих елементів стеганографічного каналу, два типових і дуже різних сценарії — випадок моніторингу трафіку та аналізу захопленого комп'ютера.

Автоматичний пристрій моніторингу трафіку — це алгоритм, який аналізує кожне зображення, що проходить через певний вузол мережі. Прикладом може бути програма, яка перевіряє кожне зображення, опубліковане в бінарній групі обговорень, або сервер, що моніторить весь трафік через конкретний Інтернет-вузол. У цьому випадку наглядач має обмежену інформацію про джерело покриттів, джерело повідомлень або стегасистему. Це найбільш складна ситуація, в якій принцип Керкхофса не повністю застосовується. Тому наглядачу потрібні стеганалітичні алгоритми, здатні виявляти якомога ширший спектр стеганографічних схем.

Якщо коло сторін, які спілкуються, використовуючи стеганографію, звужується за допомогою деякої супутньої інформації, різноманітність джерела покриття може зменшитися, що дає спостерігачу кращі шанси виявити будь-яку стеганографічну активність. Наприклад, коли наглядач вже підозрює, що хтось може використовувати стеганографію, можна зібрати додаткову інформацію, яка може надати певну інформацію про джерело покриття або стеганографічний алгоритм. Якщо, скажімо, відправник завантажує стеганографічний інструмент, поки за нею спостерігають, наглядач раптово отримує попередню інформацію про алгоритм вбудовування, а також про простір стегоключів. Або якщо знаємо, що надсилається зображення, отримане за допомогою камери, то можна купити камеру тої ж моделі і адаптувати свою атаку до цього джерела покриття.

Стеганалітичний процес може стати значно простішим, коли комп'ютер підозрюваного буде вилучено, і завдання наглядача полягає в стеганалі́зуванні

зображень на жорсткому диску. У цьому випадку стеганографічний інструмент може залишатися на комп'ютері або його сліди можуть бути відновлені навіть після видалення (наприклад, за допомогою Wetstone's Gargoyle http://www.wetstonetech.com). Це надає цінну попередню інформацію про потенційний стегоканал. У деяких ситуаціях спостерігач може виявити кілька версій одного зображення, які є майже ідентичними. Спочатку можна перевірити, чи ці трохи різні версії є результатом стеганографії або якогось іншого природного процесу, наприклад, стиснення одного зображення за допомогою двох різних JPEG-компресорів. Порівнюючи зображення, можна дізнатися про характер змін вбудовування та їхнє місцезнаходження (канал вибору) і, можливо, зробити висновок, що зміни зумовлені вбудовуванням секретного повідомлення. Як тільки спостерігач визначить, що стеганографія відбувається, стеганалі́зування завершено, і можна продовжити судову стеганалітику, спрямовану на витягнення секретного повідомлення, або вирішити перервати канал зв'язку, якщо це в межах компетенції.

2.11.1 Статистичний стегоаналіз

Інформаційно-теоретичне визначення стеганографічної безпеки починається з основного припущення, що джерело покриття можна описати ймовірнісним розподілом P_c на просторі всіх можливих покриттів C. Значення P_c (B) = $\int P_c(x)$ — це ймовірність вибору покриття x ∈ B ⊂ C для приховування повідомлення. Припустимо, що даний стегасистеми використовує на вході покриття x ∈ C, де x ~ P_c, стегоключі та повідомлення (обидва набувають значень у своїх множинах відповідно до деяких розподілів), тоді розподіл стегозображень буде P_s.

2.11.2 Стеганоаналіз як проблема виявлення

Припустимо, що спостерігач може зібрати достатню кількість прикритих зображень і оцінити pdf P_c. Якщо знання про стеганографічний канал дозволяють оцінити pdf P_s або навчитися відрізняти P_c від P_s, використовуючи інструменти

машинного навчання, ми говоримо про стеганалітичний аналіз відомої стегосистеми, що є задачею виявлення, яка веде до простого тестування гіпотез.

$$H_0: x \sim P_c \qquad (2.86)$$

$$H_1: x \sim P_s \qquad (2.87)$$

Оптимальні детектори Неймана-Пірсона та байєсові детектори можуть бути виведені для цієї задачі за допомогою тесту відношення ймовірностей.

Якщо спостерігач не має жодної інформації про стеганографічну систему, проблема стеганалізу стає.

$$H: x \sim P_c \qquad (2.88)$$

що є проблемою тестування складних гіпотез і в загальному випадку є значно більш складною.

Очевидно, існує багато інших варіантів, які знаходяться між цими двома формулюваннями, залежно від інформації про стеганографічний канал, який надано. Наприклад, якщо наглядач знає алгоритм вбудовування, але не джерело повідомлення, тоді P_s буде залежати від невідомого параметра — швидкості зміни β, і спостерігач зіткнеться з композитною односторонньою проблемою тестування гіпотез.

Можна використовувати відповідні інструменти, такі як узагальнений тест правдоподібності, або перетворити цю проблему на просте тестування гіпотез, розглядаючи β як випадкову змінну та припускаючи про її розподіл (байєсівський підхід).

2.11.3 Моделювання зображень за допомогою ознак

Практичний аналіз стеганографії мультимедійних об'єктів, таких як цифрові зображення, не може працювати з повним поданням зображень через їхню велику складність і вимірність. Натомість потрібно прийняти спрощену модель, за допомогою якої проблема виявлення стане більш досяжною. Моделі, що використовуються в стеганалії, зазвичай отримуються шляхом представлення зображень за допомогою набору числових ознак. Кожне зображення, x ∈ C,

відображається на вектор ознак d-вимірного простору f = (f_1(x), . . . , f_d(x)) ∈ R^d, де кожна f_i: C → R. Случайні змінні, що представляють джерело покриття, повинні бути вибрані так, щоб кластери f(x) і f(y) перекривалися якомога менше. Тоді x ∼ P_c, а стегозображення y ∈ P_s трансформуються у відповідні випадкові змінні f(x) ∼ p_c і f(y) ∼ p_s на R^d. Для точного виявлення ознаки потрібно вибрати так, щоб кластери f(x) і f(y) перекривалися якомога менше.

Оптимальні детектори

Будь-який алгоритм стеганалізу є детектором, який можна описати за допомогою відображення F : R^d → {0, 1}, де F(x) = 0 означає, що x вважається покриттям, а F(x) = 1 означає, що x вважається стего. Набір R_1 = {x ∈ R^d | F(x) = 1} називається критичною областю, оскільки детектор вирішує "стего" лише в тому випадку, якщо x ∈ R_1. Критична область повністю описує детектор.

Детектор може робити дві типи помилок — хибні сповіщення та пропущені виявлення. Ймовірність хибного сповіщення, P_{FA}, є ймовірністю того, що випадкова змінна, розподілена відповідно до p_c, буде виявлена як стего, тоді як ймовірність пропущеного виявлення, P_{MD}, є ймовірністю того, що випадкова змінна, розподілена відповідно до p_s, буде неправильно виявлена як покриття:

$$P_{FA} = \Pr\{F(x) = 1 | x \sim p_c\} = \int_{R_1} p_c(x)dx \qquad (2.89)$$

$$P_{MD} = \Pr\{F(x) = 0 | x \sim p_s\} = 1 - \int_{R_1} p_s(x)dx \qquad (2.90)$$

Ймовірності помилок будь-якого детектора повинні задовольняти таку нерівність:

$$(1 - P_{FA}) \log \frac{1 - P_{FA}}{P_{MD}} + P_{FA} \frac{P_{FA}}{1 - P_{MD}} \leq D_{KL}(P_c || P_s) \qquad (2.91)$$

де DKL — це дивергенція Кульбака-Лейблера між двома ймовірнісними розподілами. Для безпечної стеганографії $D_{KL}(P_c||P_s)$ = 0, і єдиний детектор, який може створити спостерігач, — це той, що випадково вгадує між покриттям і стего,

що означає, що наглядач не може побудувати атаку. Для є-безпечних стегосистем $D_{KL}(P_c||P_s) \leq \epsilon$, і надійність виявлення зменшується зі зменшенням є.

У стеганографії корисні детектори повинні мати низьку ймовірність хибного сповіщення. Це важливо, оскільки зображення, які вважаються такими, що потенційно містять секретні повідомлення, ймовірно, підлягатимуть подальшому судово-медичному аналізу, щоб визначити стеганографічну програму, стего-ключ і, зрештою, витягти секретне повідомлення. Це може вимагати жорстоких атак на словники, які можуть бути досить витратними та трудомісткими. Отже, більш цінним є детектор з дуже низькою P_{FA}, навіть якщо його ймовірність пропуску виявлення може бути досить високою (наприклад, $P_{MD} > 0.5$ або вищою). Оскільки стеганографічна комунікація зазвичай є повторюваною, навіть детектор з $P_{MD} = 0.5$ все ще може бути досить корисним, якщо його ймовірність хибного сповіщення мала.

Гіпотетична проблема в стеганалізі майже виключно формулюється за допомогою налаштування Неймана-Пірсона, де метою є створення детектора з найвищою ймовірністю виявлення $P_D = 1-P_{MD}$, при цьому накладаючи обмеження на ймовірність хибних сповіщень, $P_{FA} \leq \epsilon_{FA}$. Хоча можливе асоціювання витрат з обома типами помилок, баєсівські детектори зазвичай не використовуються в стеганалізі, оскільки ймовірності зустрічі зображення покриття або стего зображення рідко можуть бути точно оцінені.

Зважаючи на обмеження на хибні сповіщення, ϵ_{FA}, оптимальний детектор Неймана-Пірсона — це тест відношення правдоподібності.

Навіть якщо теоретично спостерігач може створити оптимальні алгоритми стеганалізу, оцінюючи ймовірнісні розподіли зображень покриття та стегозображень і використовуючи тест відношення правдоподібності, це можна зробити лише для низьковимірних моделей покриттів, які можуть не описувати покриття добре. Оскільки розмірність простору ознак часто є великою, що особливо вірно для сліпого стеганалізу, рідко можна точно оцінити основні ймовірнісні розподіли. Натомість задача виявлення розглядається як задача класифікації (визнання образів) і вирішується шляхом навчання класифікатора на

великій базі даних зображень покриття та стегозображень. Параметри класифікатора зазвичай налаштовуються для отримання низької ймовірності хибних сповіщень.

2.12 Отримувач операційної характеристики (ROC)

Для даного детектора функція $P_D(P_{FA})$ називається кривою характеристик роботи отримувача (ROC), яка описує продуктивність детектора. Кілька прикладів ROC-кривих наведено на рисунку 2.12. ROC-крива поганого методу стеганалізи близька до діагональної лінії (рисунок 2.12(b)), тоді як хороші методи стеганалізи мають ROC-криві, які наближаються до кривої, зображеної на рисунку 2.12(c).

Порівняння детекторів насправді означає порівняння їхніх ROC-кривих. Хоча деякі детектори можуть бути однозначно порівняні, оскільки їхні ROC задовольняють умову $P_D^1(P_{FA}) > P_D^2(P_{FA})$ для всіх $P_{FA} \in [0, 1]$ (наприклад, детектор 1 є надійнішим за детектор 2 для всіх P_{FA}), в загальному випадку ROC можуть перетинатися, і тоді неясно, який детектор є кращим. Приклад двох кривих, які важко порівняти, наведено на рисунку 2.12(d). Цю проблему можна уникнути, якщо ми зможемо витягти скалярну міру продуктивності з кожної ROC, оскільки скаляри можуть бути однозначно впорядковані. Серед різних міри продуктивності, які були запропоновані різними дослідниками, можна виділити наступні три:

Площа ρ між ROC-кривою та діагональною лінією нормалізована так, що ρ = 0 коли ROC збігається з діагональною лінією і ρ ≈ 1 для ROC-кривих, які відповідають майже ідеальним детекторам (рисунок 2.12(c)). Математично,

$$p = 2\int_0^1 P_D(x)dx - 1 \qquad (2.92)$$

Цю величину іноді називають точністю. Інша, але тісно пов'язана міра — це Площа під Кривою (AUC) або Площа під ROC (AUR), що є просто площею під ROC-кривою.

$$AUC = \int_0^1 P_D(x)dx = \frac{1+p}{2} \qquad (2.93)$$

Мінімальна загальна середня помилка рішення за рівних апостеріорних ймовірностей (Pr{x є stego} = Pr{x є cover})

$$P_E = min\frac{1}{2}\left(P_{FA} + P_{MD}(P_{FA})\right) \qquad (2.94)$$

Мінімум досягається в точці, де дотична до ROC-кривої має нахил 1/2.

Рівень помилок при спрацьовуванні з ймовірністю виявлення, рівною P_D = 1/2.

$$P_D^{-1}\left(\frac{1}{2}\right) \qquad (2.95)$$

Жодна з цих величин не є повністю задовільною через відсутність фундаментального обґрунтування. Значення $P_D^{-1}(1/2)$ ймовірно є найбільш корисним для стеганалітики, оскільки, як було зазначено вище, найважливіше — це ймовірність помилки через хибне сповіщення детектора. Робота Кера [136] є спробою порівняти детектори стеганалітики більш фундаментальним чином в межах, коли швидкість змін наближається до нуля.

На практиці підлягаючі розподіли p_c та p_s зазвичай отримуються експериментально у вибірковій формі. Для одновимірних розподілів над множиною дійсних чисел p_s зазвичай є зсувом p_c, і обидва розподіли є унімодальними. У цьому випадку критична область визначається скалярним порогом γ. Таким чином, ROC можна побудувати або шляхом підгонки параметричної моделі до вибіркового розподілу, або безпосередньо, змінюючи поріг γ від -∞ до +∞ і обчислюючи відносну частку ознак cover і stego, що перевищують γ.

Конкретна форма відображення ознак f та тип задачі тестування гіпотез залежатимуть від сценарію стеганалірування та стеганографічного каналу.

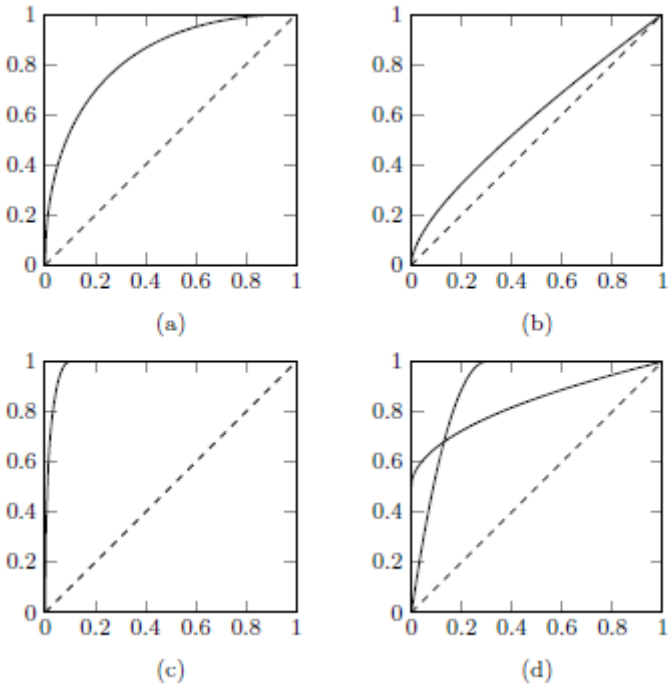


Рис. 2.12 - Приклади ROC кривих. Осі x та y в усіх чотирьох графіках ідентифікатори можливості помилки.

2.13 Висновок до другого розділу

У цьому розділі було детально розглянуто ключові аспекти стеганографії у контексті цифрових зображень, які виступають основним типом носіїв для приховання даних. Аналіз форматів цифрових зображень дозволив визначити їхні особливості та обмеження, що впливають на вибір методів стеганографії. Зокрема, формати JPEG та BMP мають різні характеристики, які визначають можливості вбудовування прихованої інформації, враховуючи компресію, кольорові моделі та розмір файлів.

Стеганографічний канал, як основа прихованого обміну інформацією, був розглянутий із точки зору його структури та функціонування. Цей канал забезпечує передачу даних у прихованому вигляді, не викликаючи підозри з боку сторонніх спостерігачів. У контексті цифрових зображень він передбачає використання як структурних особливостей файлу, так і психологічних аспектів сприйняття зображення людиною.

Методи стеганографії, розглянуті у розділі, включають як прості техніки, такі як модифікація найменш значущих бітів (LSB), так і більш складні алгоритми, засновані на частотному аналізі та зміні коефіцієнтів ДКП (дискретного косинусного перетворення). Кожен метод має свої переваги та недоліки, що залежать від вимог до стійкості, рівня приховання даних і типу носія.

Окрему увагу було приділено стегоаналізу, який виступає протилежним процесом стеганографії. Було розглянуто його основні методи, включаючи статистичний аналіз, сигнатурний аналіз та використання машинного навчання. Важливим є поділ стегоаналізу на сліпий, який не вимагає доступу до оригінального носія чи знань про метод приховання, та не сліпий, що базується на порівнянні із відомим оригіналом.

Таким чином, розглянуті формати зображень, методи стеганографії та принципи стегоаналізу формують комплексне розуміння функціонування прихованих комунікацій.

РОЗДІЛ 3.
ПРАКТИЧНА РЕАЛІЗАЦІЯ КОМБІНОВАНОГО ЗАХИСТУ КОНФІДЕНЦІЙНИХ ДАНИХ З ВИКОРИСТАННЯМ СТЕГАНОГРАФІЇ ТА КРИПТОГРАФІЇ

3.1 Використані інструменти та технології

3.1.1 Python

Python – це високорівнева мова програмування загального призначення, відома своєю чіткістю та легкістю у вивченні. Python підтримує різні парадигми програмування, включаючи об'єктно-орієнтоване, процедурне та функціональне програмування. Основні переваги Python:

- Простота та Лаконічність: Зрозумілий синтаксис, який легко читати та писати.
- Багатий Стандартний Бібліотечний Набір: Велика кількість бібліотек для роботи з даними, веб-розробки, автоматизації, наукових обчислень та багато іншого.
- Кросплатформеність: Може працювати на різних операційних системах, таких як Windows, macOS і Linux.
- Велика Спільнота: Багато ресурсів для навчання, документації та допомоги.

Python широко використовується у веб-розробці, автоматизації, аналізі даних, машинному навчанні та багатьох інших галузях.

3.1.2 Django

Django – це потужний веб-фреймворк для розробки веб-застосунків на мові Python. Він забезпечує швидку розробку та чистий, прагматичний дизайн, пропонуючи набір інструментів та бібліотек для створення веб-сайтів. Основні характеристики Django:

- Швидкість розробки: Django дозволяє створювати веб-застосунки швидко та ефективно завдяки великому набору вбудованих функцій.
- Безпека: Включає захист від найпоширеніших веб-уразливостей, таких як SQL-ін'єкції, XSS, CSRF.
- Масштабованість: Відмінно підходить для великих проектів, де важлива продуктивність і масштабованість.
- Адміністративна Панель: Вбудована адмін-панель для управління контентом без додаткових налаштувань.
- Відкритий Код: Велика спільнота, що підтримує та розвиває фреймворк.

Django часто використовується для створення складних веб-застосунків, таких як соціальні мережі, контент-менеджмент системи (CMS), електронна комерція та багато інших.

HTML (HyperText Markup Language) та CSS (Cascading Style Sheets) – це основні технології для створення та стилізації веб-сторінок.

HTML:

- Структура Веб-сторінки: HTML використовується для створення структури веб-сторінок за допомогою тегів (наприклад, , <p>, <a>, <img>, <table>, тощо).
- Текстовий Контент: Використовується для визначення заголовків, абзаців, списків, посилань та інших текстових елементів.
- Мультимедіа: Інтеграція зображень, відео та аудіо.

3.1.3 Комбінація HTML та CSS:

Разом HTML та CSS є основою веб-розробки, що дозволяє створювати естетично привабливі та функціональні веб-сторінки. HTML визначає структуру та зміст, тоді як CSS відповідає за візуальне оформлення та макет.

Ці технології широко використовуються у створенні як простих веб-сайтів, так і складних веб-додатків.

3.1.4 SQL

SQL – це стандартна мова для управління і маніпуляції реляційними базами даних. Вона використовується для виконання різноманітних операцій з даними в базах даних, таких як збереження, оновлення, видалення та отримання даних. Основні функції SQL включають:

- Запити до бази даних: Використання SELECT для отримання даних з таблиць.
- Модифікація даних: Використання INSERT, UPDATE та DELETE для додавання, зміни та видалення даних.
- Управління структурами даних: Використання CREATE, ALTER та DROP для створення, зміни та видалення таблиць і інших об'єктів бази даних.
- Управління доступом: Використання GRANT та REVOKE для надання або обмеження прав доступу до даних.

SQL використовується в багатьох системах управління базами даних (СУБД), таких як MySQL, PostgreSQL, SQLite, Oracle, Microsoft SQL Server та інших. Його універсальність та потужність робить SQL ключовим інструментом для роботи з даними в різних сферах, включаючи веб-розробку, аналіз даних, бізнес-інтелект та інші.

3.1.5 AES-256 Encryption

AES-256 – це симетричний алгоритм шифрування, який використовується для захисту даних. AES-256 є частиною стандарту AES, що включає також AES-128 та AES-192, і має різницю лише в довжині ключа. Основні аспекти AES-256:

1. Симетричне Шифрування

- Симетричний Ключ: Використовує один і той же ключ для шифрування та дешифрування даних, що означає, що як відправник, так і одержувач повинні знати цей секретний ключ.

- Безпека Ключа: Довжина ключа 256 біт забезпечує високий рівень захисту від криптографічних атак.

2. Структура Алгоритму

- Блокове Шифрування: Працює з блоками даних фіксованого розміру (128 біт).
- Круги Шифрування: AES-256 виконує 14 раундів (кругів) шифрування, кожен з яких включає декілька підпроцесів (SubBytes, ShiftRows, MixColumns, AddRoundKey).

3. Застосування

- Шифрування Даних: Використовується для шифрування конфіденційної інформації, такої як фінансові транзакції, дані користувачів, урядові документи.
- Безпечні З'єднання: Використовується в протоколах безпеки, таких як TLS/SSL, для забезпечення безпеки інтернет-з'єднань.
- Захист Збережених Даних: Широко застосовується в системах збереження даних, таких як дискові шифрувальні системи (наприклад, BitLocker).

4. Переваги AES-256

- Стійкість до Атак: Висока стійкість до різних типів криптографічних атак, включаючи грубі атаки (brute force).
- Продуктивність: Ефективність обробки великих обсягів даних завдяки оптимізованим алгоритмам.

3.1.6 Least Significant Bit (LSB) Steganography

LSB (Least Significant Bit) – це техніка стеганографії, яка використовується для приховування даних у мультимедійних файлах, таких як зображення, аудіо та відео. Основний принцип LSB стеганографії полягає в тому, щоб вбудовувати секретні повідомлення в найменш значущі біти пікселів зображення або семплів аудіо, таким чином, що ці зміни є майже непомітними для людського ока або вуха.

1. Принцип Роботи LSB Стеганографії

- Біти Пікселів: У кольорових зображеннях кожен піксель представлений трьома байтами (RGB – червоний, зелений, синій). Найменш значущий біт (LSB) кожного байта змінюється для збереження секретного біта інформації.
- Зміна Значень: Оскільки зміна найменш значущого біта має незначний вплив на колір пікселя, такі зміни є практично непомітними.
- Вбудовування Даних: Секретне повідомлення кодується побітово у LSB кожного байта пікселів зображення або аудіо семплів.

2. Приклад на Психологічному Рівні

- Оригінальний Байт: 10101010
- Модифікований Байт: 10101011 (заміна останнього біта)

У цьому випадку тільки останній біт змінюється, що майже не впливає на відображення кольору або звук, але зберігає секретну інформацію.

3. Застосування

- Захист Даних: Використовується для приховування конфіденційних повідомлень у зображеннях або аудіо.
- Цифрові Водяні Знаки: Використовується для захисту авторських прав шляхом вбудовування авторських даних у цифровий контент.
- Безпека Комунікацій: Забезпечує прихований обмін інформацією між користувачами.

5. Переваги та Недоліки

Переваги:

- Простота реалізації.
- Приховування даних без значної зміни оригінального файлу.
- Використання для захисту авторських прав та прихованого обміну інформацією.

Недоліки:

- Обмежений обсяг даних, що можна приховати.
- Вразливість до атак з модифікацією файлу.

Комбінування AES-256 шифрування та LSB стеганографії є потужним методом захисту даних, що надає два рівні захисту: шифрування даних та їх приховування. Це забезпечує додатковий захист конфіденційної інформації, особливо під час передачі через незахищені канали.

можеш повторити відповідь, зробити її більш теоретичною, прибрати код, може додай розрахунки які показують перевагу такої комбінації

Теоретичне Комбінування AES-256 та LSB Стеганографії

Комбінування AES-256 шифрування та LSB стеганографії є потужним методом захисту даних, що надає два рівні захисту: шифрування даних та їх приховування. Це забезпечує додатковий захист конфіденційної інформації, особливо під час передачі через незахищені канали.

1. Теоретичні Основи AES-256

- AES-256 (Advanced Encryption Standard) – це симетричний алгоритм шифрування, який використовує ключ довжиною 256 біт. Цей алгоритм є частиною стандарту AES, який також включає AES-128 та AES-192. Основні характеристики AES-256:

- Висока Безпека: Довжина ключа 256 біт забезпечує стійкість до грубих атак (brute force), оскільки кількість можливих комбінацій ключів становить 22562^{256}, що практично неможливо перебрати.

- Блокове Шифрування: AES працює з блоками даних розміром 128 біт, що забезпечує ефективну обробку великих обсягів даних.

- Швидкість та Ефективність: Оптимізовані алгоритми шифрування забезпечують високу продуктивність.

2. Теоретичні Основи LSB Стеганографії

- LSB (Least Significant Bit) Стеганографія – це метод приховування даних у мультимедійних файлах, таких як зображення або аудіо, шляхом зміни найменш значущих бітів кожного пікселя або семплу. Основні аспекти LSB стеганографії:

- Незначна Зміна: Зміна найменш значущого біта незначно впливає на оригінальний файл, роблячи зміни невидимими для людського ока або вуха.

- Приховування Даних: Секретне повідомлення кодується побітово у LSB кожного байта пікселів або аудіо семплів, зберігаючи інформацію непомітно.

3. Переваги Комбінованого Методу

Захист від Грубих Атак

- AES-256 Шифрування забезпечує високу стійкість до грубих атак завдяки великій кількості можливих комбінацій ключів. Кількість комбінацій обчислюється як 22562^{256}, що дорівнює приблизно 1.16×10771.16 \times 10^{77} варіантів. Для порівняння, за поточних обчислювальних можливостей, перебір всіх можливих ключів займе мільйони років.

Непомітність та Прихованість

- LSB Стеганографія дозволяє приховати зашифроване повідомлення у звичайних файлах, таких як зображення, що знижує ймовірність виявлення секретного повідомлення. Зміна лише найменш значущого біта призводить до незначних змін в оригінальному файлі, які важко виявити без спеціалізованих інструментів.

4. Розрахунки Вигоди

Обсяг Даних

- AES-256 шифрує дані блоками по 128 біт. Якщо ми беремо файл розміром 1 МБ (8,388,608 біт), після шифрування розмір файлу залишиться таким самим, але вміст буде повністю зашифрованим.

Ефективність Приховування

- LSB Стеганографія може приховати значну кількість даних у файлах. Наприклад, зображення розміром 800x600 пікселів має 480,000 пікселів, або 1,440,000 байтів (RGB). Використовуючи 1 біт на піксель, ми можемо приховати до 180,000 байтів (приблизно 176 КБ) даних у цьому зображенні, що достатньо для приховування зашифрованого повідомлення.

3.2 Демонстрація розробленого рішення.

Для того щоб удосконалити програму було розроблено невеликий демонстраційний модуль онлайн банкінгу, який зберігає дані клієнта захищаючи їх комбінованим криптографічним та стеганографічним методами. Робота модулю наведена нижче.

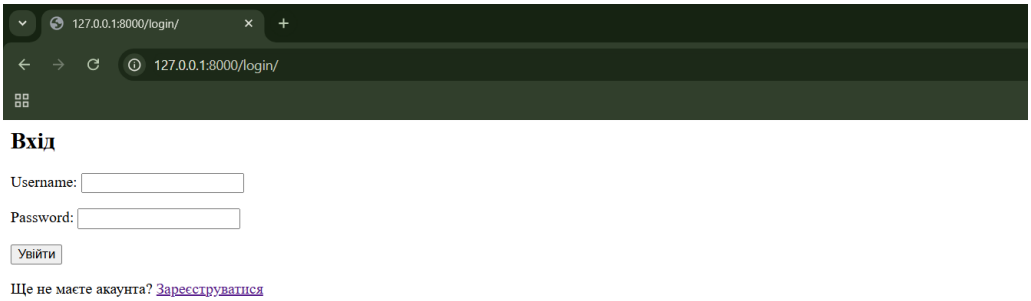


Рис. 3.1 – початкова форма авторизації

На початку роботи з модулем клієнта зустрічає вікно авторизації (Рис. 3.1) на якому він може як здійснити її так і виконати алгоритм реєстрації.

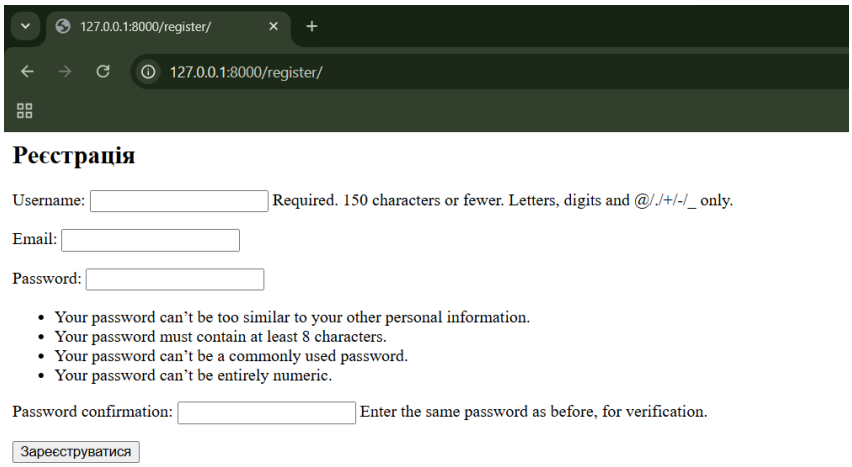


Рис. 3.2 – форма реєстрації

Якщо користувач новий, то далі слідує форма реєстрації (Рис. 3.2) в ньому користувач створює собі юзернейм, пароль та вводить свою пошту. Конкретно ці дані не є специфічними для банкінгу, тому для їх захисту використовується тільки aes-256, плюс алгоритми захисту бази даних.

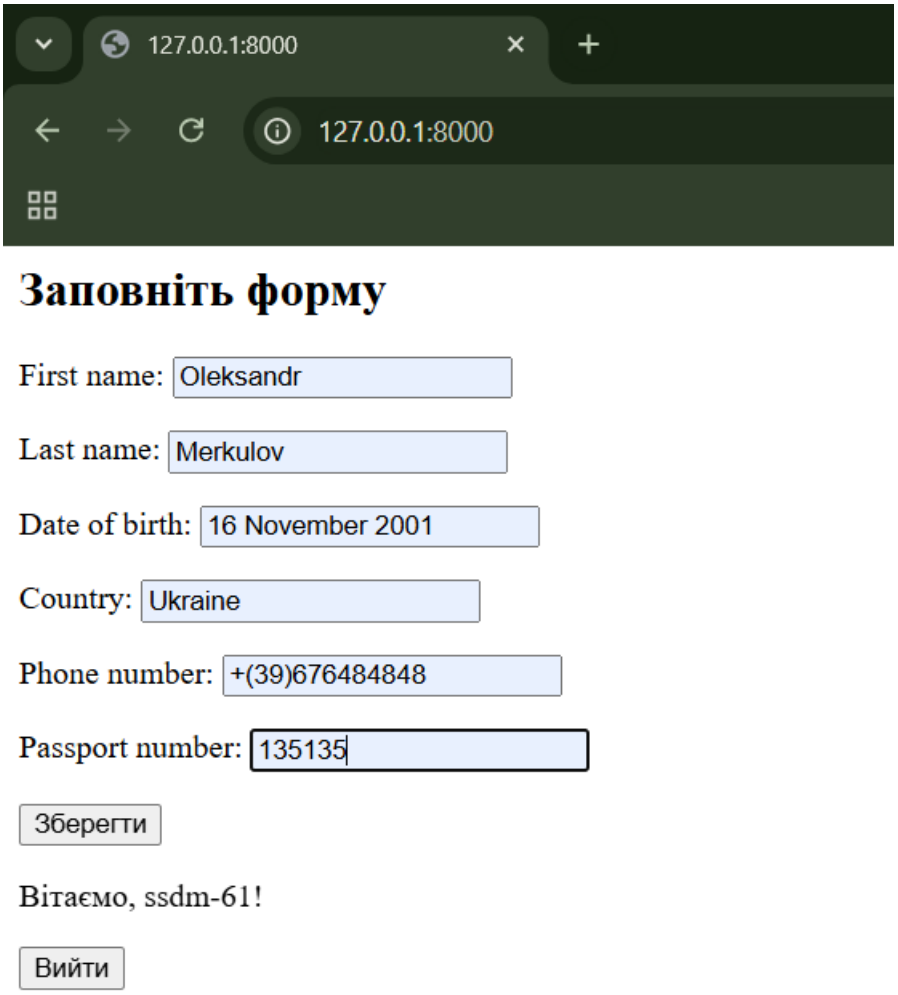


Рис. 3.3 - Форма з банківськими даними

На рисунку 3.3 зображено подальшу форму з даними які заповняються саме для банківської структури, в принципі тут можуть бути будь-які дані у формі, але тут для демонстрації присутні саме базові дані які необхідні для отримання банківської картки.

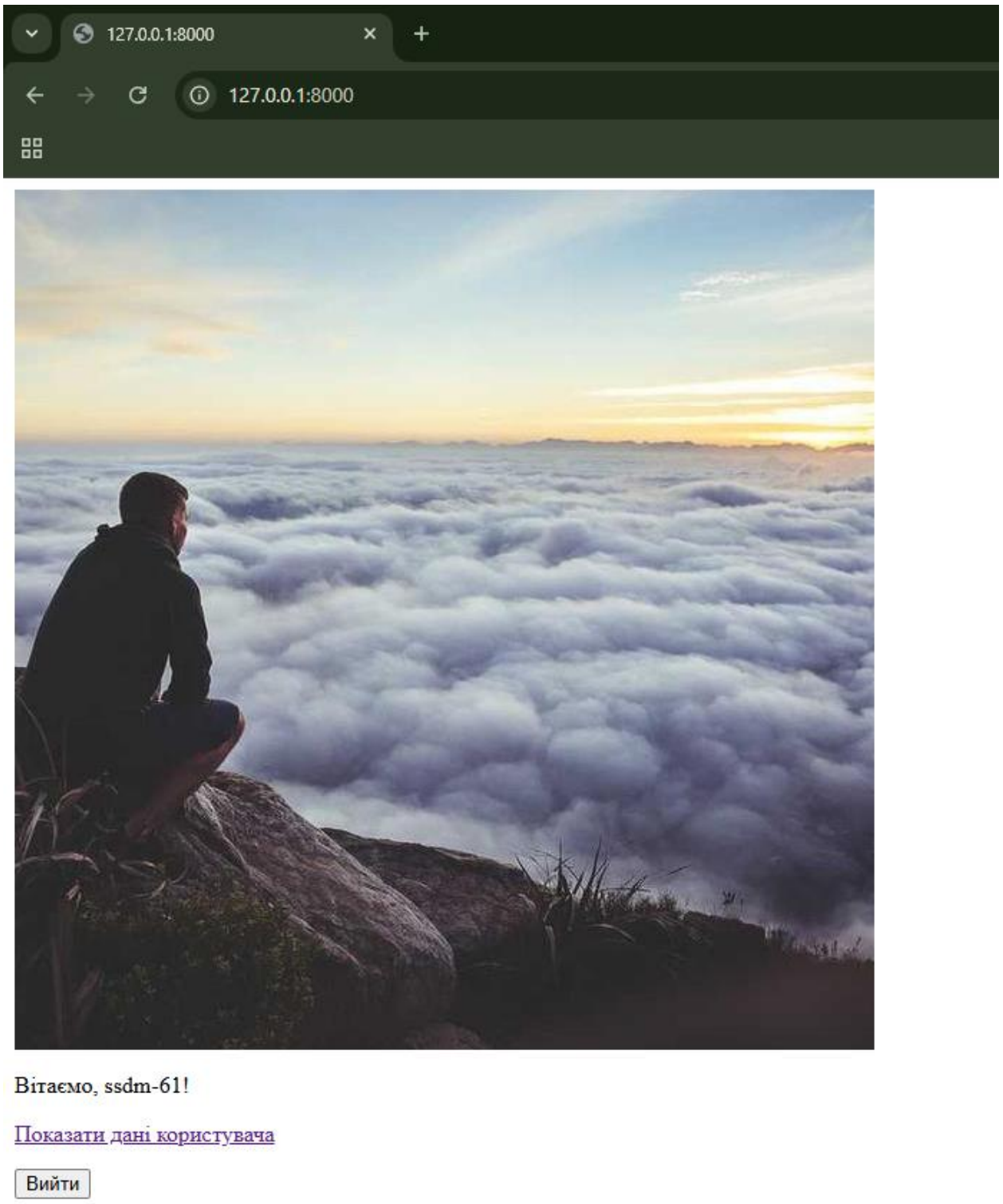


Рис. 3.4 – зображення з конфіденційними даними користувача

Спочатку рисунок 3.4 може здатися якимось дивним, але так і повинно бути. Після того як користувач ввів свої дані та натиснув зберегти, система їх шифрує алгоритмом aes-256, далі після того як дані були зашифровані вони обробляються

за допомоги LSB методу система змінює біти фотографії та приховує повідомлення в випадково згенерованій фотографії яку ми і бачимо на рисунку 3.4.

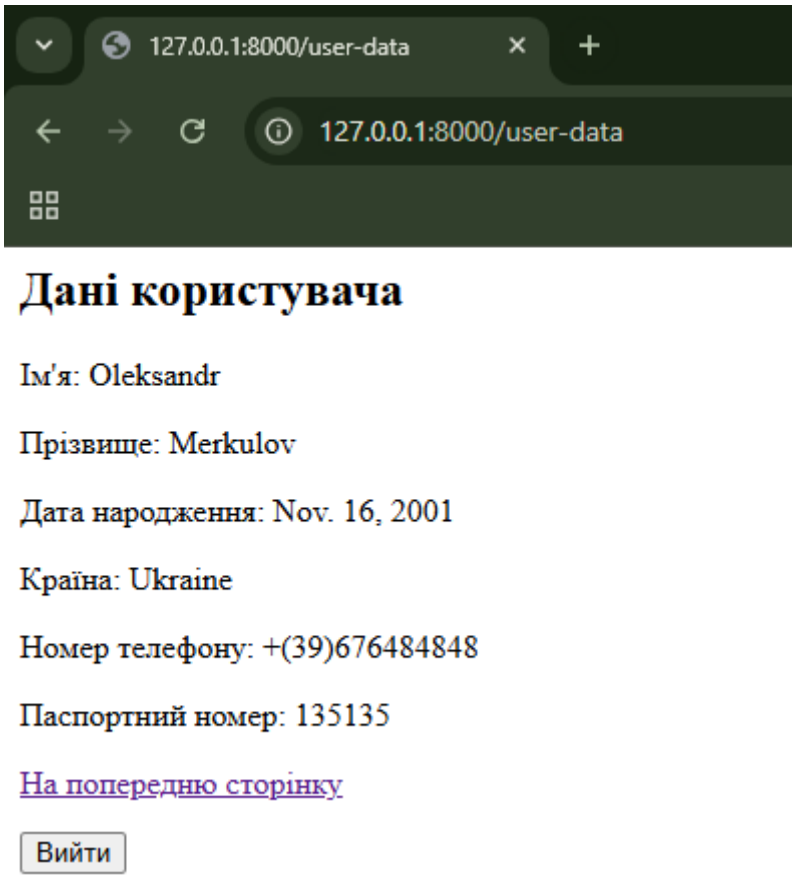


Рис. 3.5 - збережені дані користувача

Рисунок 3.5. демонструє нам саме збережені дані про користувача банку, взагалі такий функціонал не дуже треба, але щоб продемонструвати саме те що вони цілісно зберігаються в системі на платформі можна подивитися їх. Алгоритм їх відображення такий після запиту до системи, вона знаходить збережені фотографії з даними користувачів, видобуває їх, потім розшифровує і демонструє на екрані.

3.3 Висновок до третього розділу.

У цьому розділі представлено практичний мініпроєкт, який демонструє підхід до зберігання конфіденційних даних клієнтів банку за допомогою розробленого Django-модуля.

Розроблений модуль функціонує в кілька етапів. Спочатку конфіденційні дані клієнта шифруються за допомогою алгоритму AES-256, який забезпечує сучасний стандарт захисту інформації через використання стійкого до зламування симетричного шифрування. Далі отримані зашифровані дані приховуються у випадково згенерованому зображенні методом LSB, що дозволяє зробити їх абсолютно непомітними для сторонніх осіб. Цей підхід поєднує переваги криптографії, яка захищає сам зміст даних, та стеганографії, яка приховує сам факт їхньої наявності.

Комплексне використання AES-256 та LSB значно підвищує загальний рівень захисту. Навіть у разі, якщо зображення буде отримане сторонньою особою, без відповідного ключа AES зловмисник не зможе розшифрувати приховану інформацію. Такий підхід додає додатковий рівень безпеки, створюючи багатошарову систему захисту, яка знижує ризики несанкціонованого доступу до конфіденційних даних.

Результати практичної реалізації модуля свідчать про ефективність обраного підходу. Використання Django дозволило забезпечити зручну інтеграцію модуля у веб-додаток, а також підтримку масштабованості та простоти у використанні. Розроблений метод може бути адаптований до інших сфер, де зберігання конфіденційної інформації є критично важливим.

Таким чином, створений у цьому розділі практичний мініпроєкт демонструє, що поєднання шифрування AES-256 із стеганографією на основі LSB є ефективним рішенням для забезпечення високого рівня захисту конфіденційних даних, що відповідає сучасним вимогам інформаційної безпеки.

ВИСНОВКИ

Магістерська робота на тему "Удосконалення системи захисту конфіденційних даних при передачі інформації стеганографічними методами" досліджує актуальну проблему забезпечення конфіденційності даних у сучасному цифровому середовищі. У роботі розглянуто теоретичні аспекти стеганографії, історичний розвиток цієї галузі, сучасні технології приховування інформації, а також виконано практичну реалізацію удосконаленої системи захисту даних.

У першому розділі було детально проаналізовано основи стеганографії, її історію, сучасні підходи та типи, а також її значення для кібербезпеки. Показано, що стеганографія відіграє важливу роль у захисті інформації, забезпечуючи прихованість даних на додаток до традиційного шифрування. Водночас наголошено на необхідності розвитку стегоаналізу як інструменту протидії зловживанням стеганографією у злочинних цілях.

Другий розділ був присвячений аналізу технічних аспектів роботи стеганографічних систем, включаючи формати цифрових зображень, функціонування стеганографічного каналу та сучасні методи приховування даних. Також розглянуто стегоаналіз як процес виявлення прихованої інформації, зокрема його види: сліпий та не сліпий аналіз. Комплексний підхід до вивчення цих процесів дозволив сформувати розуміння ключових технологічних викликів у цій галузі.

У третьому розділі було розроблено практичний Django-модуль для захисту даних клієнтів банку. У ньому реалізовано поєднання двох ключових методів: шифрування AES-256 для захисту змісту даних і стеганографічного приховування за допомогою LSB у випадково згенерованих зображеннях. Це забезпечило багаторівневий підхід до захисту: навіть у разі компрометації стеганографічного носія без ключа AES розшифрувати дані неможливо. Експериментальні результати підтвердили ефективність такого підходу для забезпечення високого рівня конфіденційності.

Отримані результати підкреслюють, що стеганографія у поєднанні з криптографічними методами має великий потенціал для вдосконалення систем захисту інформації. Розроблена система демонструє практичну цінність для застосування у банківському секторі, державних структурах та інших галузях, де безпека даних є критично важливою.

Таким чином, ця магістерська робота зробила внесок у розвиток теорії та практики стеганографії, запропонувавши сучасні підходи до захисту даних, що відповідають викликам сучасного інформаційного простору. Подальше дослідження цієї теми може зосередитися на підвищенні стійкості стеганографічних методів до новітніх технологій стегоаналізу, а також інтеграції їх у масштабовані інформаційні системи.

ПЕРЕЛІК ПОСИЛАНЬ

1. Конахович Г.Ф. Комп'ютерна стеганографія. Теорія і практика / Г.Ф. Конахович, А. Ю. Пузиренко. - Київ: МК-Пресс, 2006. – 288с.

2. Кузнецов О. О. Стеганографія: навчальний посібник / О.О.Кузнецов, С. П. Євсеєв, О. Г. Король. - Х.: Вид. ХНЕУ, 2011. - 232с.

3. Рябко Б. Я., Фионов А. Н. Основы современной криптографии и стеганографии. 2-е изд. / Рябко Б. Я., Фионов А. Н. // М.: Горячая линия - Телеком, 2013. 232 с.

4. Кінзерявий О.М. Стеганографічні методи приховування даних увекторні зображення, стійкі до активних атак на основі афінних перетворень / О.М. Кінзерявий // Київ – 2015, 324 с.

5. Вовк О.О. Методи підвищення стійкості та пропускної здатності систем прихованої передачі інформації / Вовк О.О. – Харків, 2016 – 177с.

6. Грибунин В. Г. Цифровая стеганография / В.Г. Грибунин, И.Н. Оков, И.В. Туринцев. – М.: СОЛОН-Пресс, 2002. – 272 с.

7. Худьо В.Д., Моделювання стійкої стегофонічної системи із заданими характеристиками мережі / В.Д. Худьо // Тернопіль – 2017. – 98с.

8. Юдін О.К., Конахович Г.Ф., Корченко О.Г. Захист інформації в мережах передачі даних: Підручник. К.: Видавництво ТОВ НВП «ІНТЕРСЕРВІС», 2009, 716 с.

9. Fidrich J. Steganography in Digital Media: Principles, Algorithms, and Applications / J. Fidrich. – Cambridge: Cambride University Press, 2009. – 438 p.

10. 34. Kutter M. A fair benchmark for image watermarking systems / M. Kutter, F. Petitcolas // Proc. of SPIE: Security and Watermarking of Multimedia Contents. − San Jose, France, 1999. – vol. 3657 − P. 226 – 239.

11. Кінзерявий О.М. Стеганографічні методи приховування даних у векторні зображення, стійкі до активних атак на основі афінних перетворень / О.М. Кінзерявий // Київ – 2015, 324 с.

12. Лагун А. Використання вейвлет-перетворення для приховування інформації в нерухомих зображеннях / А. Лагун, І. Лагун // Захист інформації і безпека інформаційних систем. – Л., 2013. – С. 98 – 99.

13. Горніцька Д.А. Визначення коефіцієнтів важливості для експертного оцінювання у галузі інформаційної безпеки / Д.А. Горніцька, О.Г. Корченко, В.В. Волянська // Захист інформації. – 2012. – №1. – С. 108 – 121.

14. Ó Ruanaidh J. Rotation, scale and translation invariant digital image watermarking / J. Ó Ruanaidh, T. Pun // Proc. of the ICIP'97. – California, 1997. – vol. 1, P. 536–539.

15. Семенко К.О. Визначення коефіцієнтів важливості для експертного оцінювання стеганографічних методів / К.О. Семенко, наук. кер. О.О. Вовк // 20-й Міжнародний молодіжний форум «Радіоелектроніка і молодь у XXI столітті». – Х.: ХНУРЕ, 2016. – т.4. – С. 167 – 168.

16. Вовк О. О. Визначення коефіцієнтів важливості для експертного оцінювання стеганографічних методів / О. О. Вовк // Науковий журнал «Телекомунікаційні та інформаційні технології». – Київ, 2015. – №3. – С. 70 – 80.

17. Вовк О.О. Розроблення методики оцінювання важливості характеристик стеганографічних алгоритмів / О.О. Вовк, А.А. Астраханцев // Вісник національного університету «Львівська політехніка» «Інформаційні системи та мережі». – Львів, 2014. – № 805. – С. 52 – 60.

18. Вовк О.О. Синтез стеганографічного методу передачі даних, ефективного за критеріями надійності та захищеності / О.О. Вовк, А.А. Астраханцев // Електронне наукове фахове видання ХНУРЕ «Проблеми телекомунікацій». – Харків, 2015. – № 1 (16). – С. 103 – 115.

19. Vovk O. Synthesis of optimal steganographic method meeting given criteria / O. Vovk, A. Astrahantsev // Informatyka Automatyka Pomiary w Gospodarce i Ochronie Środowiska (technical and scientific journal). – Lublin, Poland, 2015. – P. 27-34

20. Сейеди С.А. Сравнение методов стеганографии в изображениях / С.А. Сейеди, Р.Х. Садыхов // Информатика. – БГУИР, 2013. – С. 66 – 75.

21. Вовк О.О. Анализ атак на цифровые водяные знаки в видеофайлах и изображениях / О.О. Вовк наук. кер. А.А. Астраханцев // V Міжнародна науково-практична конференція «Сучасні проблеми і досягнення в галузі радіотехніки, телекомунікацій та інформаційних технологій». – Запоріжжя, ЗНТУ, 2010. – С. 88 – 90.

22. Тігулев М. Стеганография в GIF [Электронный ресурс]. – Режим доступа: http://habrahabr.ru/post/128327.

23. Основи комп'ютерної графіки: навч. посіб. / В.С. Березовський, В.О. Потієнко, І.О. Завадський; за заг. ред. А.М. Гуржія. − К.: BHV, 2009. − 400 с.

24. Грачева Ю.А. Несколько слов о стеганографии – методе защиты графической информации от нарушения авторских прав / Ю.А. Грачева // Московский государственный университет печати. – С. 76 – 81.

25. Adnan M. Watermark re-synchronization using log-polar mapping of image autocorrelation / M. Adnan, J. Meyer // Digimarc Corporation. – P. 1 – 4.

ДОДАТКИ

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ КІБЕРБЕЗПЕКИ ТА ЗАХИСТУ ІНФОРМАЦІЇ

Кваліфікаційна робота здобувача освітнього ступеня «Магістр»

УДОСКОНАЛЕННЯ СИСТЕМИ ЗАХИСТУ КОНФІДЕНЦІЙНИХ ДАНИХ ПРИ ПЕРЕДАЧІ ІНФОРМАЦІЇ СТЕГАНОГРАФІЧНИМИ МЕТОДАМИ

Спеціальність: 125 - Кібербезпека та захист інформації

Виконав: Олександр МЕРКУЛОВ

Керівник: д.т.н., професор Олександр ТУРОВСЬКИЙ

Київ - 2025

АКТУАЛЬНІСТЬ, МЕТА ТА ЗАВДАННЯ ДОСЛІДЖЕННЯ

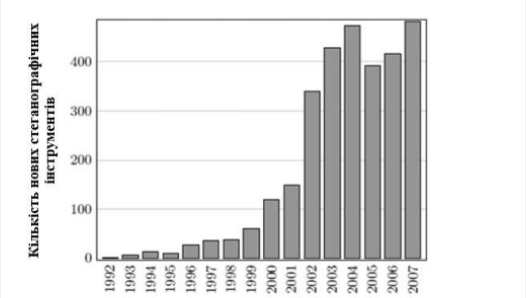
- Актуальність роботи обумовлена потребою приховування самого факту передавання конфіденційних даних у цифровому середовищі.
- Об’єкт дослідження - стеганографічні методи захисту інформації.
- Предмет дослідження - методи стеганографічного захисту конфіденційних даних при їх передачі.
- Мета роботи - удосконалення системи передачі конфіденційних даних стеганографічними методами.
- Завдання: дослідити методи стеганографії, проаналізувати загрози, оцінити стегоаналіз і запропонувати комбінований стеганографічно-криптографічний захист.

РОЛЬ СТЕГАНОГРАФІЇ У ЗАБЕЗПЕЧЕННІ КІБЕРБЕЗПЕКИ

Тип носія	Кількість
Аудіо	445
Диск	416
Фото	1689
Мережа	39
Інше	81
Текст	255
Відео	86

- Стеганографія забезпечує приховану комунікацію шляхом розміщення секретного повідомлення в непримітному цифровому контейнері.
- На відміну від криптографії, приховується не лише зміст, а й сам факт передавання повідомлення.
- У роботі розглянуто текстову, графічну, відео-, аудіо- та мережеву стеганографію.

СУЧАСНИЙ СТАН СТЕГАНОГРАФІЧНИХ ТЕХНОЛОГІЙ

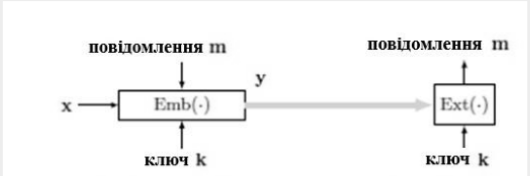


- Розвиток цифрових медіа та мереж спричинив активне поширення стеганографічного програмного забезпечення.
- Цифрові зображення, аудіо, відео та текстові файли є типовими контейнерами для прихованих даних.
- Зростання кількості інструментів одночасно підсилює як захисний, так і атакувальний потенціал стеганографії.

СТЕГАНОГРАФІЧНИЙ КАНАЛ ПЕРЕДАВАННЯ ДАНИХ

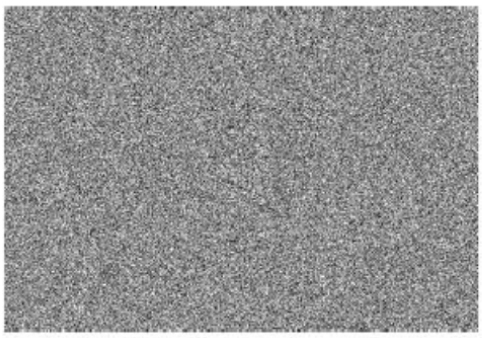
- Стеганографічний канал формується між відправником і отримувачем через контейнер, у який вбудовується секретне повідомлення.
- Для захисту застосовується стего-ключ, що ускладнює виявлення і відновлення прихованого повідомлення сторонньою особою.
- Надійність каналу залежить від непомітності модифікацій контейнера та стійкості до стегоаналізу.

БАЗОВА МОДЕЛЬ ВБУДОВУВАННЯ ТА ВИЛУЧЕННЯ ПОВІДОМЛЕННЯ



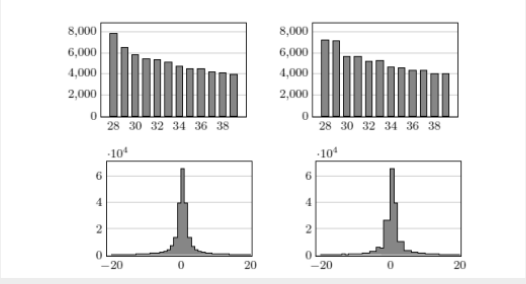
- Модель містить процедури Emb для вбудовування повідомлення та Ext для його вилучення.
- Вхідними елементами є контейнер, повідомлення та ключ, а результатом - стегооб’єкт, придатний для передавання.
- Така структура є узагальненою основою для реалізації різних методів цифрової стеганографії.

ФОРМАТИ ЗОБРАЖЕНЬ І LSB-ВБУДОВУВАННЯ



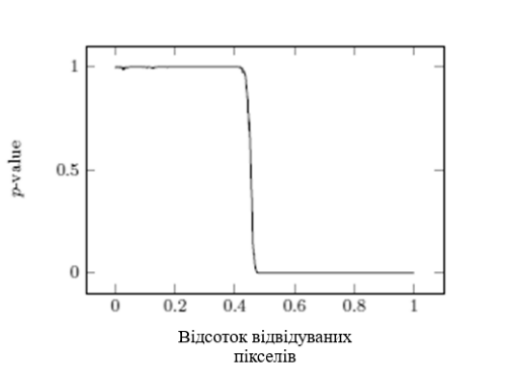
- Метод LSB використовує модифікацію найменш значущих бітів пікселів, що майже не змінює візуальне сприйняття зображення.
- У роботі розглянуто застосування цифрового зображення як контейнера для секретних даних.
- Перевага LSB - простота реалізації, обмеження - потенційна вразливість до статистичного стегоаналізу.

АТАКА НА ГІСТОГРАМУ ЯК МЕТОД СТЕГОАНАЛІЗУ



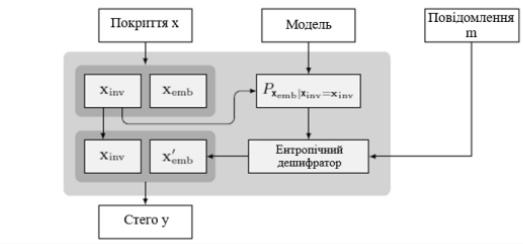
- Гістограмний аналіз дає змогу виявляти статистичні зміни, що виникають після вбудовування прихованих даних.
- Для стегозображення оцінюється розподіл значень пікселів та порівнюється з очікуваним розподілом контейнера.
- Зменшення помітних статистичних відхилень є однією з вимог до удосконаленого методу захисту.

КІЛЬКІСНИЙ НАПАД НА JSTEG ТА ОЦІНКА ПРИХОВАНОГО ПОВІДОМЛЕННЯ



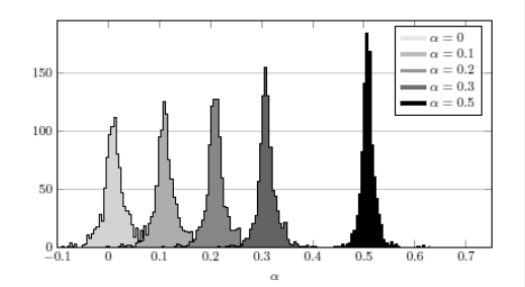
- Кількісний стегоаналіз спрямований на оцінювання частки змінених елементів контейнера та розміру прихованого повідомлення.
- Методи виявлення використовують зміну статистичних закономірностей після модифікації цифрового носія.
- Для підвищення стійкості необхідно мінімізувати регулярні ознаки вбудовування.

ПРАКТИЧНІ СТЕГАНОГРАФІЧНІ МЕТОДИ ТА МОДЕЛЬНА СТЕГАНОГРАФІЯ



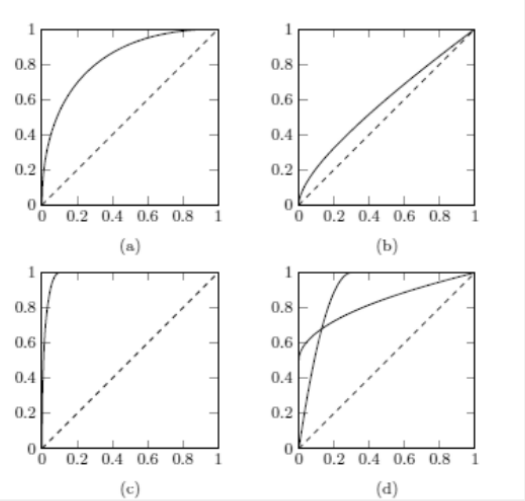
- У роботі розглянуто стеганографію, що зберігає модель, статистичне відновлення та методи на основі моделей.
- Модельна стеганографія формує стегооб’єкт так, щоб його статистичні властивості були близькими до властивостей природного контейнера.
- Такий підхід підвищує непомітність прихованого повідомлення.

ПИТАННЯ ОПТИМАЛЬНОГО СТЕГОШУМУ ТА ЄМНОСТІ ВБУДОВУВАННЯ



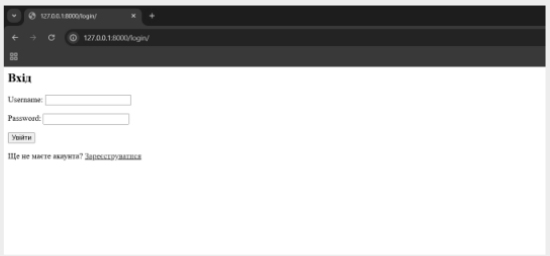
- Стегошум є результатом модифікації контейнера при приховуванні даних і впливає на помітність повідомлення.
- Оптимізація передбачає компроміс між ємністю приховування, якістю контейнера та стійкістю до стегоаналізу.
- Зниження надлишкових змін контейнера підвищує надійність прихованого каналу.

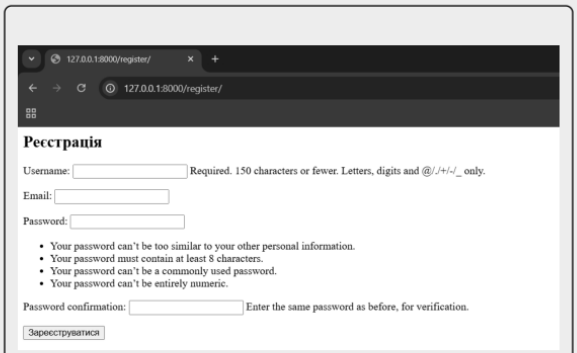
ROC-КРИВІ ДЛЯ ОЦІНЮВАННЯ ЕФЕКТИВНОСТІ СТЕГОАНАЛІЗУ



- ROC-крива застосовується для оцінювання якості виявлення прихованого повідомлення.
- Порівнюються імовірності правильного виявлення та помилкового спрацювання детектора.
- Чим ближче характеристики до випадкового вгадування, тим менш помітним є стеганографічне вбудовування.

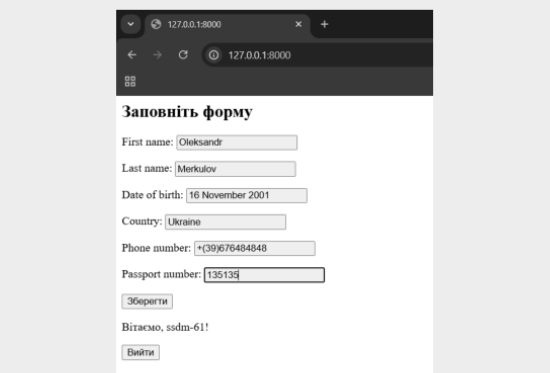
ПРАКТИЧНА РЕАЛІЗАЦІЯ КОМБІНОВАНОГО ЗАХИСТУ

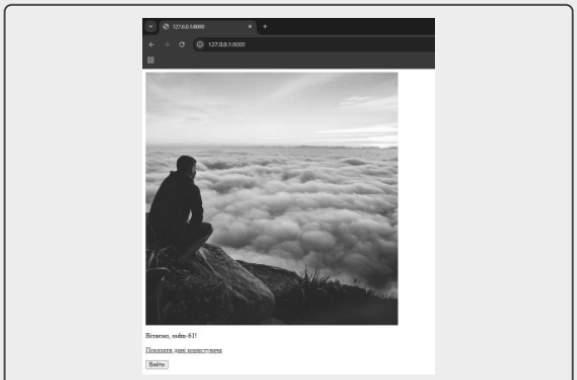




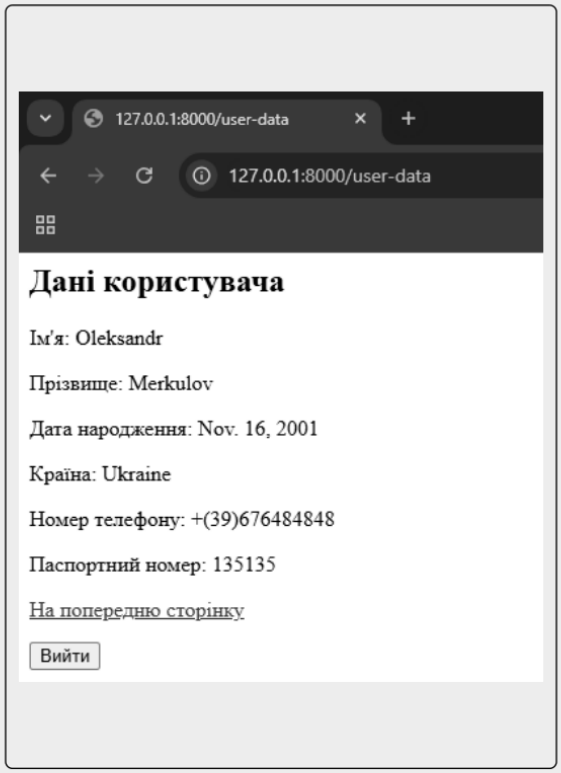
- Практична частина виконана з використанням Python, Django, HTML/CSS, SQL, AES-256 та LSB-стеганографії.
- Розроблене рішення передбачає реєстрацію та автентифікацію користувача, введення конфіденційних даних і їх подальше приховування.
- Комбінування AES-256 і LSB дозволяє одночасно зашифрувати дані та приховати факт їх передавання.

ДЕМОНСТРАЦІЯ РОБОТИ СИСТЕМИ ПРИХОВУВАННЯ ДАНИХ





- Користувач вводить персональні дані у веб-формі, після чого система шифрує повідомлення алгоритмом AES-256.
- Зашифровані дані приховуються в зображенні-контейнері методом LSB.
- Зовнішній вигляд контейнера не повинен вказувати на наявність прихованого повідомлення.



- Проаналізовано теоретичні основи стеганографії, типові загрози, методи виявлення та протидії стеганографічним атакам.
- Досліджено методи LSB-вбудовування, статистичного стегоаналізу, модельної стеганографії та оцінювання ефективності за ROC-кривими.
- Запропоновано комбінований підхід: AES-256 для криптографічного захисту змісту та LSB-стеганографія для приховування факту передавання даних.

ДЯКУЮ ЗА УВАГУ!

Доповідь підготував здобувач вищої освіти Олександр МЕРКУЛОВ

«Удосконалення системи захисту конфіденційних даних стеганографічними метод

Київ - 2025