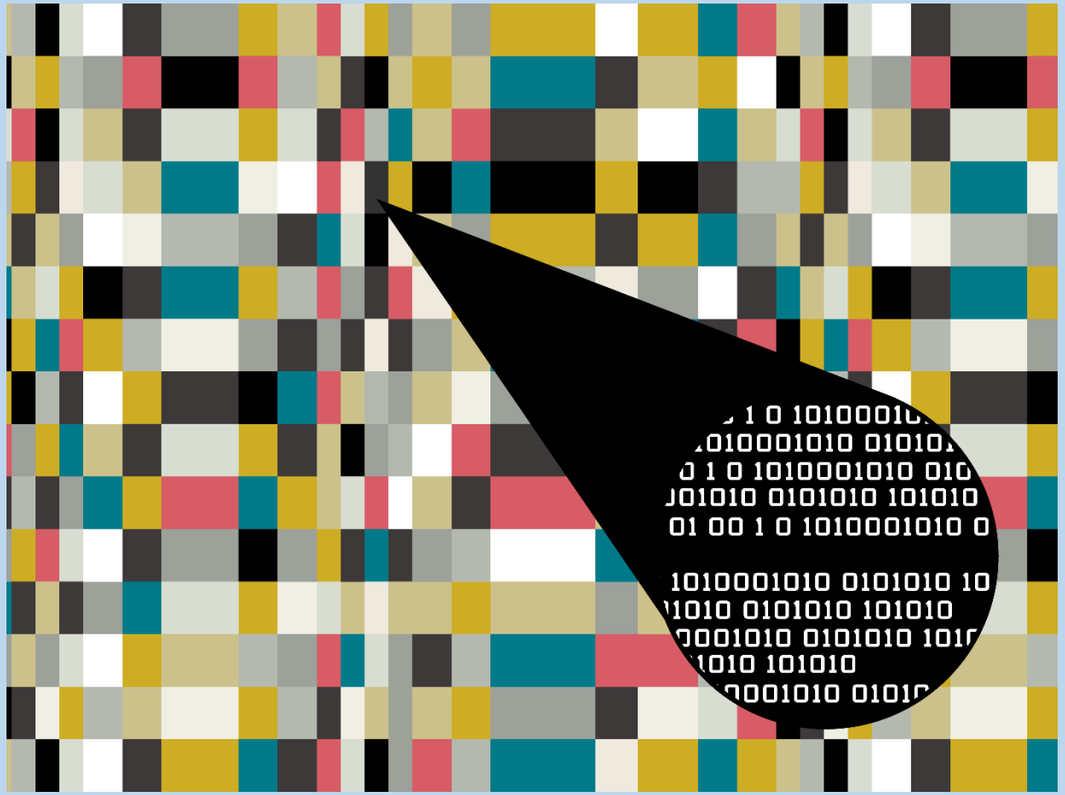
ЛЕКЦІЯ 14

ЖИТОМИРСЬКА ПОЛІТЕХНІКА
ДЕРЖАВНИЙ УНІВЕРСИТЕТ

Цифрова стеганографія



План

1. Поняття цифрової стеганографії
2. Модель стеганосистеми
3. Класифікація стеганосистем
4. Поняття ЦВЗ, класифікація
5. Стеганографічні методи приховування інформації

1. Поняття цифрової стеганографії

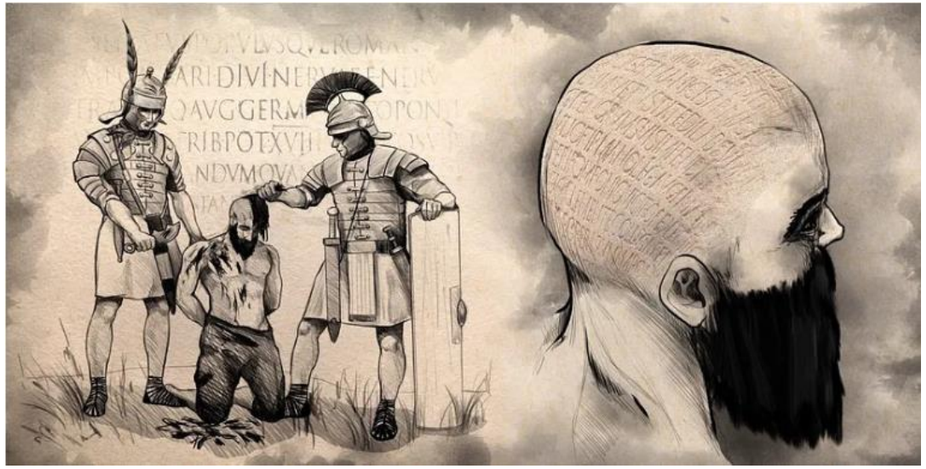
Стеганографія - це наука, яка вивчає способи й методи приховування конфіденційної інформації, основною задачею якої є приховування самого факту існування секретних даних при їхній передачі, зберіганні або обробці.

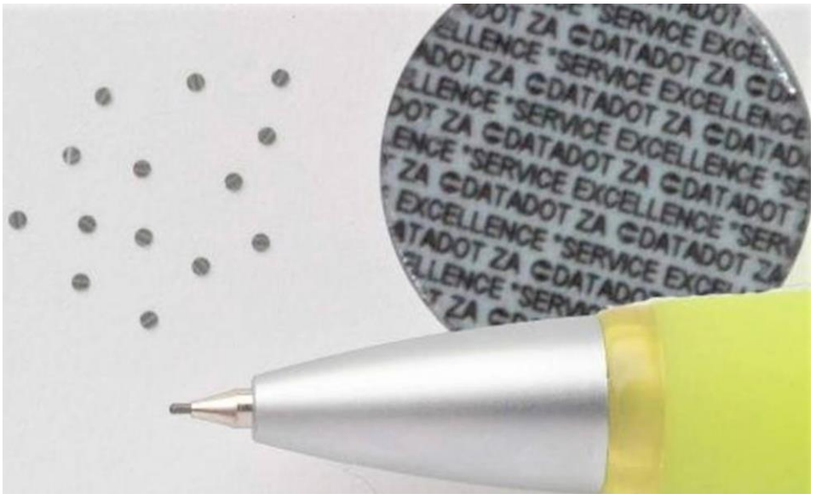
Розвиток засобів обчислювальної техніки в останні десятиліття дав новий поштовх для розвитку *комп'ютерної стеганографії.*

Є два основні напрямки в комп'ютерній стеганографії:

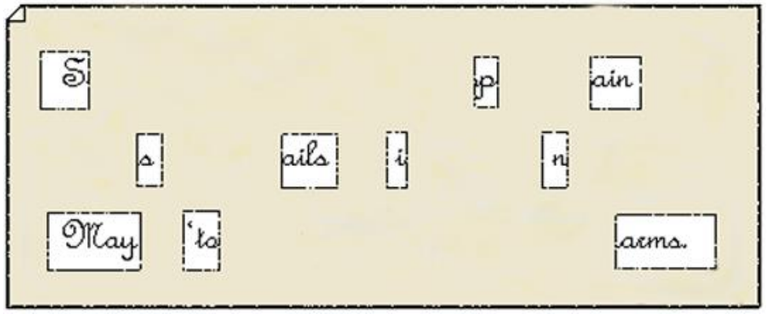
- Пов'язаний з цифровою обробкою сигналів (повідомлення вбудовують у цифрові дані, які мають аналогову природу: аудіо, зображення, відео, текстові файли і файли програм)
- Не пов'язаний з цифровою обробкою сигналів (повідомлення може бути вбудоване в заголовки файлів, заголовки пакетів даних)

1. Поняття цифрової стеганографії

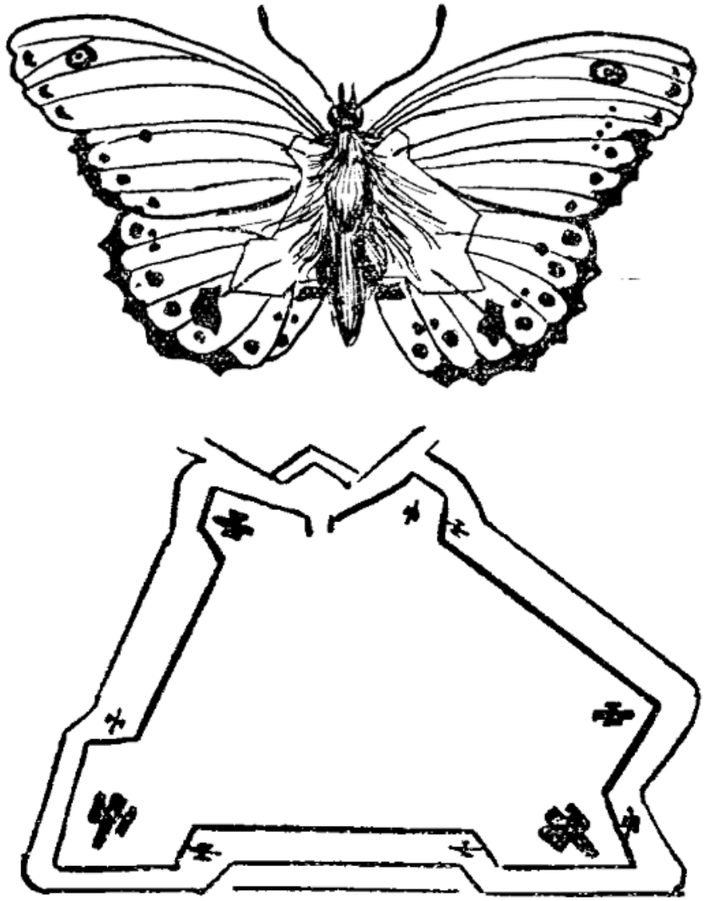


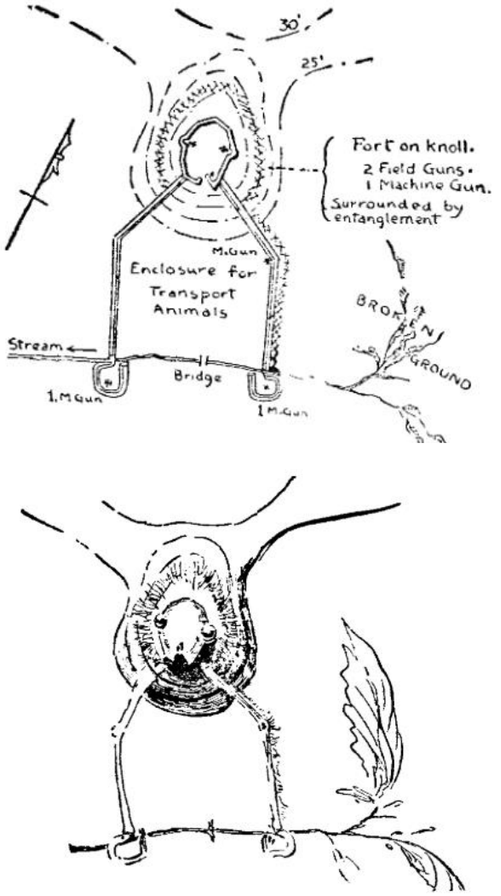


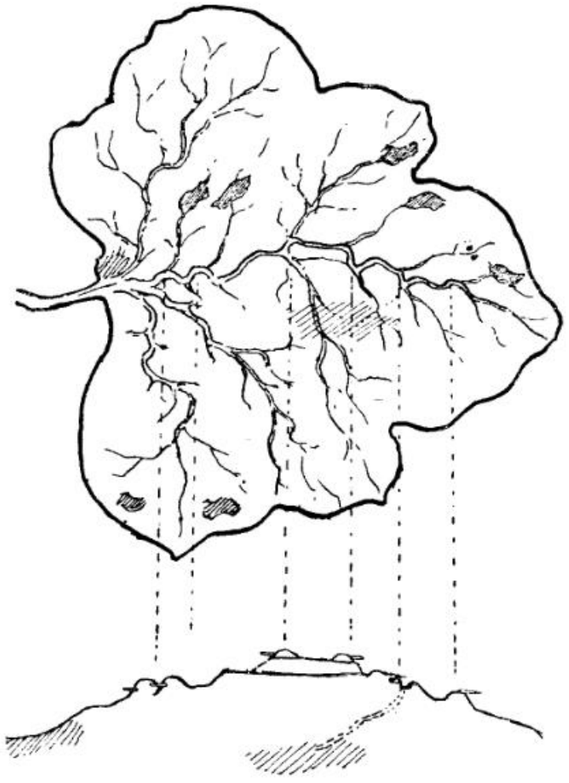
Sir John regards you well and spekes again that
all as rightly 'vails him is yours now and ever.
May he 'tone for past a'lays with many charms.



1. Поняття цифрової стеганографії







1. Поняття цифрової стеганографії

Цифрова стеганографія — напрям класичної стеганографії, що полягає у впровадженні додаткової інформації у цифрові об'єкти (контейнери), викликаючи при цьому деякі спотворення цих об'єктів. Дана технологія призначена для організації таємного зв'язку, що є класичним завданням стеганографії, проте вона використовується також для захисту інтелектуальної власності.

1. Поняття цифрової стеганографії

Напрямки цифрової стеганографії

1)Вбудовування інформації з метою її прихованої передачі (спрямоване на організацію прихованого каналу зв’язку в каналі загального користування).

2)Вбудовування цифрових водяних знаків (watermarking) (застосовується для захисту від копіювання і НС використання).

3)Вбудовування ідентифікаційних номерів (fingerprinting) – «відбитків пальців» (кожна захищена копія має свій унікальний номер, що вбудовується).

4)Вбудовування заголовків (captioning) (зберігання різнорідно представленої інформації в єдиному цілому).

1. Поняття цифрової стеганографії

Галузі застосування стеганографії

Захист від копіювання

Електронна комерція, контроль за копіюванням (DVD), розповсюдження мультимедійної інформації (відео за запитом)

Прихована анотація документів

Медичні знімки, картографія, мультимедійні бази даних

Автентифікація

Системи відеоспостереження, електронна комерція, голосова пошта, електронне конфіденційне діловиробництво

Прихований зв'язок

Військові та розвідувальні додатки, а також використання у випадках, коли криптографію використовувати не можна

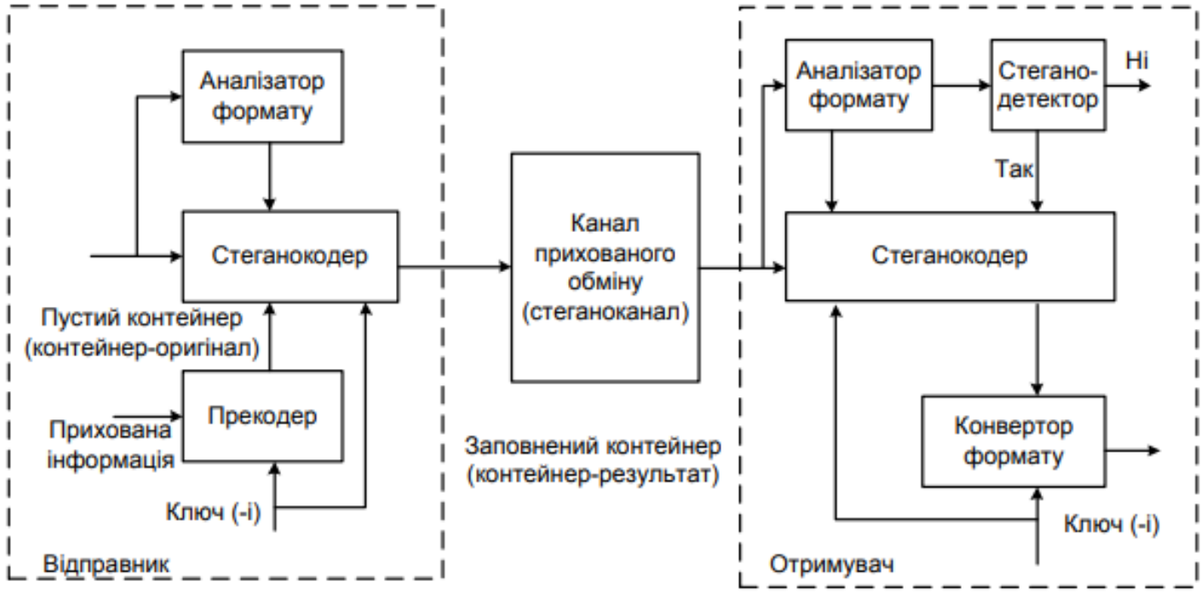
2. Модель стеганосистеми

Завдання вбудовування і виділення повідомлень із іншої інформації виконує **стеганосистема**, яка складається з таких основних елементів:

- ✓ Прекодер - пристрій, призначений для перетворення приховуваного повідомлення до виду, зручного для вбудовування в сигнал-контейнер.
- ✓ Контейнер - інформаційна послідовність, у якій ховається повідомлення.
- ✓ Стеганокодер – пристрій, призначений для здійснення вкладення прихованого повідомлення в інші дані з урахуванням їх моделі.
- ✓ Пристрій виділення вбудованого повідомлення.
- ✓ Стеганодетектор – пристрій, призначений для визначення наявності стегаповідомлення
- ✓ Декодер – пристрій, що відновлює приховане повідомлення. Цей вузол може бути відсутнім, це буде пояснено далі.

2. Модель стеганосистеми

Структурна схема стеганосистеми як системи зв’язку



Основними стеганографічними поняттями є повідомлення і контейнер.

Повідомленням М є секретна інформація, наявність якої необхідно приховати.

Контейнер С - несекретна інформація, яку можна використати для приховання повідомлення (пустий контейнер(контейнер-оригінал) не містить прихованої інформації, заповнений контейнер(контейнер-результат) містить приховане повідомлення)

У більшості стеганосистем для пакування і видобування повідомлення використовується ключ, який зумовлює секретний алгоритм, що визначає порядок занесення повідомлення до контейнера.

2. Модель стеганосистеми

Основні типи контейнерів

Потоковий

- Динамічний потік даних, який передається в реальному часі або створюється під час обробки.
- Прихована інформація впроваджується під час створення або передачі потоку (мережевий трафік, потоки аудіо або відео, сигнал у телефонній мережі)
- Немає жорсткого обмеження на обсяг прихованої інформації, якщо потік триває.
- Впровадження та вилучення даних потребують спеціалізованих алгоритмів у реальному часі.

Фіксований

- Розміри і характеристики є заздалегідь відомими (зображення, аудіофайл, відеофайл, текстовий документ)
- Прихована інформація інтегрується в наявний контейнер без створення нового потоку.
- Обмежений розмір для прихованих даних: кількість інформації залежить від ємності контейнера.
- Можна легко вбудовувати і вилучати дані, аналізувати на наявність змін.

2. Модель стеганосистеми

Вимоги для забезпечення надійності стеганосистеми

1)Безпека системи повинна повністю визначатися секретністю ключа

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

3) Заповнений контейнер повинен візуально не відрізнятися від незаповненого

4)Стегосистема повинна мати низьку ймовірність помилкового виявлення прихованого повідомлення в сигналі, що його не містить.

5) Повинна забезпечуватися необхідна пропускна здатність.

6)Стегосистема повинна мати прийнятну обчислювальну складність реалізації.

3. Класифікація стеганосистем

Методи цифрової стеганографії

3. Класифікація стеганосистем

Типи стеганосистем

Безключові

- Не використовують ключі для впровадження або вилучення прихованої інформації.
- Простота реалізації.
- Низький рівень захищеності.
- Метод LSB без шифрування даних.

З відкритим ключем

- Використовують публічний ключ для вбудовування інформації, а приватний — для її вилучення.
- Висока безпека передачі інформації між сторонами.
- Складність реалізації через криптографічні операції.
- Системи, що базуються на криптографії RSA

З закритим ключем

- Один і той самий секретний ключ використовується як для вбудовування, так і для вилучення даних.
- Простота обчислень.
- Необхідність безпечної передачі ключа між сторонами.
- Класичні методи із симетричним шифруванням.

Змішані

- Поєднують механізми відкритого та закритого ключа для підвищення безпеки.
- Оптимальний баланс між безпекою і швидкістю.
- Вища складність у порівнянні з іншими типами.
- Використання симетричного ключа для стеганографії та асиметричного для його передачі.

3. Класифікація стеганосистем

Класифікація стеганосистем

Відкрита

- система, в якій кожен може перевірити наявність прихованої інформації. В такій системі можуть бути застосовані різноманітні алгоритми і методи, що дозволяють вбудовувати інформацію в об'єкт з відомими параметрами, наприклад, зображення з відомою кількістю пікселів.

Напівзакрита

- система, в якій можна перевірити наявність прихованої інформації з деякими обмеженнями. Іншими словами, система має обмеження на доступність інформації, необхідної для перевірки наявності прихованої інформації. Наприклад, може бути доступна тільки частина зображення, або тільки заголовок текстового документу.

Закрита

- система, в якій неможливо перевірити наявність прихованої інформації без відповідної ключової інформації. Такі системи використовуються для захисту конфіденційної інформації, оскільки навіть якщо хтось дізнається про приховану інформацію, він не зможе її прочитати без ключа. В таких системах, ключ є важливою частиною процесу вкладення інформації і декодування її в майбутньому.

4. Поняття ЦВЗ, класифікація

Цифровий водяний знак (ЦВЗ) - спеціальна мітка, яка приховано впроваджується в зображення або інший сигнал з метою тим чи іншим способом контролювати його використання.

Предметом вивчення ЦВЗ є можливості маркування мультимедійної інформації з метою її ідентифікації, автентифікації, а також моніторингу її поширення і копіювання.

У системах з ЦВЗ застосовуються методи, за допомогою яких одні дані приховуються в інших. Але, на відміну від стеганографії, ЦВЗ захищають сам носій, тобто контейнер.

ЦВЗ містять спеціальну інформацію про час і місце його створення, про авторські права та ін., і можуть бути розпізнані лише спеціальними засобами.

4. Поняття ЦВЗ, класифікація

Види цифрових водяних знаків

Видимі

- Знаходяться у видимій частині зображення або відео і можуть бути розпізнані неозброєним оком.
- Часто виглядають як логотипи, текст або інші графічні елементи, накладені на контейнер.
- «+» Простота реалізації, захист авторських прав через очевидну ідентифікацію.
- «-» Легко видаляються або маскуються.
- Пр.: Логотип телеканалу на відео.

Напіввидимі

- Менш помітні, ніж видимі, але все ще можуть бути помічені при детальному огляді або під певними умовами.
- Розташовуються у певних ділянках контейнера з мінімальним впливом на його візуальну якість.
- «+» Баланс між прихованістю та видимістю, ускладнює видалення, оскільки менш очевидний.
- «-» Потребує точного налаштування алгоритму впровадження
- Пр.: Зображення або текст з низькою прозорістю на фото.

Невидимі

- Приховані від візуального сприйняття і можуть бути виявлені лише за допомогою спеціальних алгоритмів або інструментів.
- Використовуються для захисту авторських прав, перевірки автентичності, прихованого маркування.
- «+» Непомітні для зловмисників, що ускладнює їх видалення. Не впливають на сприйняття контейнера.
- «-» Складні алгоритми реалізації. Можуть бути пошкоджені при обробці контейнера.
- Пр.: Вбудовування даних у частотну область зображення.

Крихкі

- Порушуються навіть при найменшій зміні контейнера.
- Використовуються для виявлення змін або підробок контейнера (захист автентичності).
- «+» Чутливі до будь-яких модифікацій, що робить їх ідеальними для перевірки цілісності.
- «-» Низька стійкість до стиснення, редагування або обробки контейнера.
- Пр.: Застосування в цифрових підписах для документів чи зображень.

4. Поняття ЦВЗ, класифікація

Види цифрових водяних знаків

Invisible Watermark

Visible Watermark

4. Поняття ЦВЗ, класифікація

Використання цифрових водяних знаків

1)Проблема захисту авторських прав на інформацію, яка подана в цифровому вигляді (ЦВД містять інформацію про законного власника).

2)Системи захисту від несанкціонованого копіювання (для них застосовуються ЦВЗ, які вказують на статус цифрової копії).

3)Автентифікація цифрових даних (застосовуються ЦВЗ, які мають низьку завадостійкість до деяких видів перетворень; за фактом руйнування приймається рішення про автентичність)

4)Моніторинг інформаційних потоків (у кожну легальну копію цифрових даних вносяться різні водяні знаки).

4. Поняття ЦВЗ, класифікація

ЦВЗ повинен відповідати двом суперечливим критеріям: робастності (стійкості до різних зовнішніх впливів) і скритності (забезпечення найменших спотворень зображення в порівнянні з оригіналом).

Залежно від того, яка інформація потрібна детектору для виявлення ЦВЗ, стегосистеми ЦВЗ діляться на три класи:

Клас стегосистеми ЦВЗ		**Вхідні дані, необхідні для детектування**		**Вихідні дані детектора**	
		Вхідний сигнал	Вхідний ЦВЗ	Так/Ні	ЦВЗ
Закриті	Тип I	+	+	+	-
	Тип II	+	-	-	+
Напівзакриті		-	+	+	-
Відкриті		-	-	-	+

Найбільше застосування мають відкриті стеганосистеми.

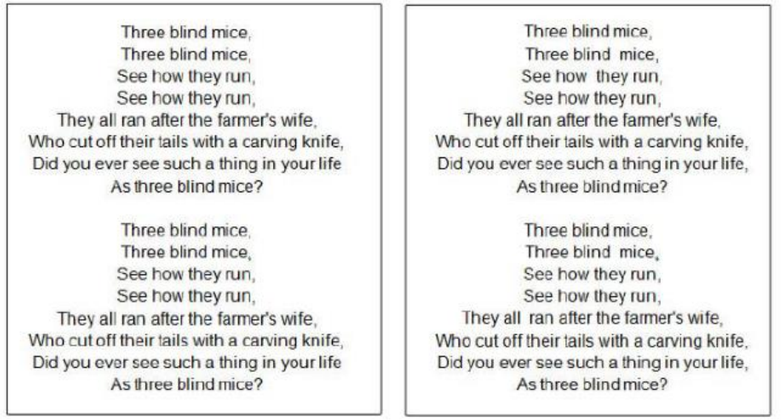
Найбільшу стійкість стосовно зовнішніх впливів – закриті стеганосистеми I типу.

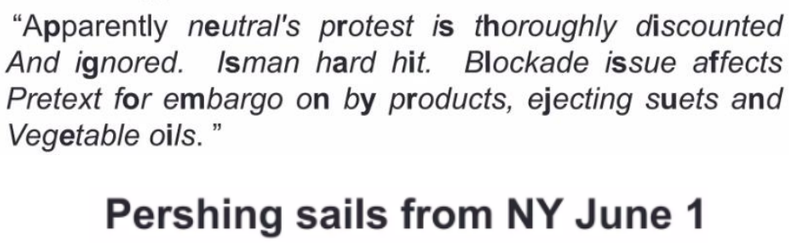
5. Стеганографічні методи приховування інформації

Текстові стеганографи

Методи перекручування формату текстового документу:

- **Додавання пробілів** між словами або наприкінці рядків(наприклад: один пробіл = 0, два пробіли = 1).
- **Зміна відступів і табуляцій** (використання різної кількості відступів або табуляцій для кодування інформації).
- **Розмір шрифту та інтервал між літерами**
- **Колір тексту та фону** (використання різних кольорів (помітно тільки при копіюванні тексту))
- **Використання прихованих символів** (вставка символів Unicode (наприклад, Zero-Width Space, Non-Breaking Space))





5. Стеганографічні методи приховування інформації

Текстові стеганографи

Синтаксичні методи
(зміна граматичної структури тексту без порушення його змісту):

- **Заміна розділових знаків**
- **Розбивка речень на абзаци** (поділ одного речення на кілька абзаців або об’єднання кількох речень).
- **Зміна порядку слів у реченні (**"Книга цікава" → "Цікава книга"**)**
- **Використання активного/пасивного стану** ("Хтось написав книгу" → "Книга була написана кимось").

Методи генерації стеганограм
(створення нових текстів, які приховують інформацію):

- **Статистичний підхід** (використання статистично правдоподібних моделей для створення тексту).
- **Шаблонний підхід** (заздалегідь створюються шаблони текстів, у які вбудовуються приховані дані).
- **Автоматична генерація тексту** (дикористання мовних моделей (GPT, BERT) для створення правдоподібних текстів, у яких приховано інформацію).

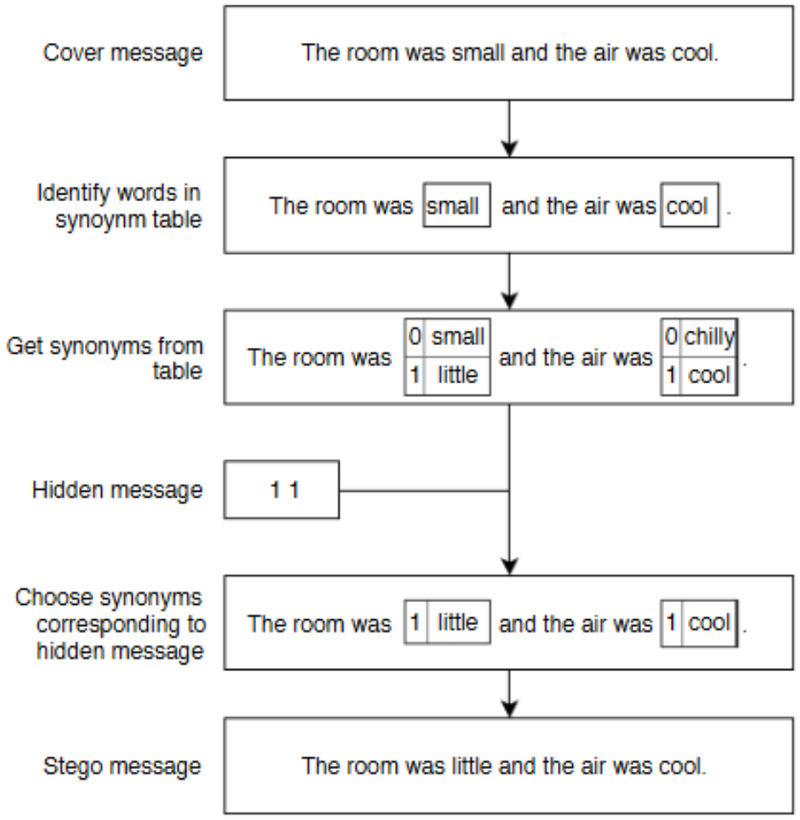
5. Стеганографічні методи приховування інформації

Текстові стеганографи

Семантичні методи

(змінюють слова або фрази на основі їх синонімічності або контексту):

- **Заміна слів синонімами**("великий" → "значний", "купити" → "придбати").
- **Перефразування речень** ("Я пішов додому" → "Додому я повернувся").
- **Використання гіпонімів та гіперонімів (** "собака" → "тварина"**)**
- **Контекстуальне введення додаткових слів** (додавання слів, які не змінюють сенсу, але кодують інформацію).



5. Стеганографічні методи приховування інформації

Приховування даних у растрових зображеннях і відео

Методи заміни в часовій (просторовій) області
(вбудовування інформації у пікселі зображення або кадри відео, зберігаючи їхню візуальну цілісність)

- **Метод модифікації найменш значущого біта (LSB)** (заміна найменш значущого біта пікселя або набору пікселів).
- **Приховування в часових кадрах відео** (дані можуть приховуватися в LSB окремих кадрів або через маніпуляцію пікселями).

	R	G	B
black	0	0	0
red	255	0	0
green	0	255	0
blue	0	0	255
white	255	255	255

(0, 0, 255) (0, 0, 254)

5. Стеганографічні методи приховування інформації

Приховування даних у растрових зображеннях і відео

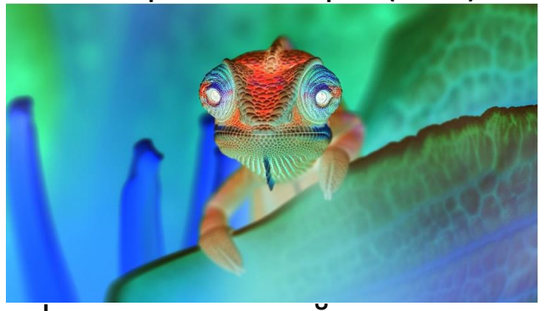
Оригінальне зображення

Канал зеленого кольору (G)

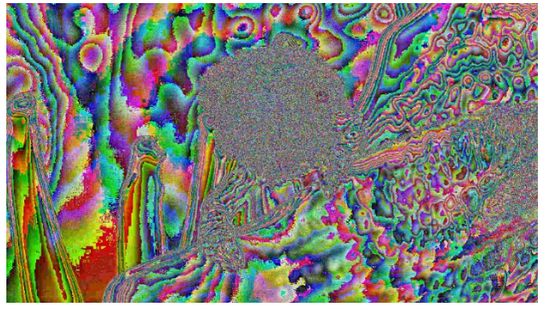
Канал синього кольору (B)

Канал червоного кольору (R)

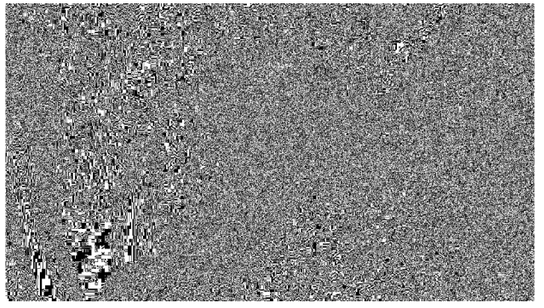
Інверсія кольорів (RGB)



Зображення, сформоване з найменш значущих бітів (LSB)



Бітова площина зображення



5. Стеганографічні методи приховування інформації

Приховування даних у растрових зображеннях і відео

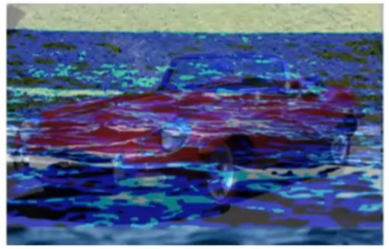
Cover

Hide

LSB

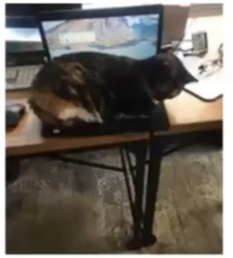
Bit 4

MSB



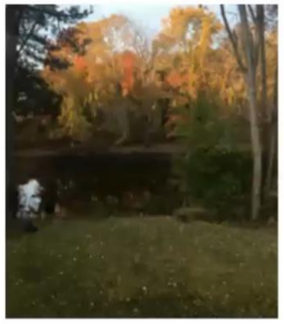
Cover

Hide



LSB

Bit 4



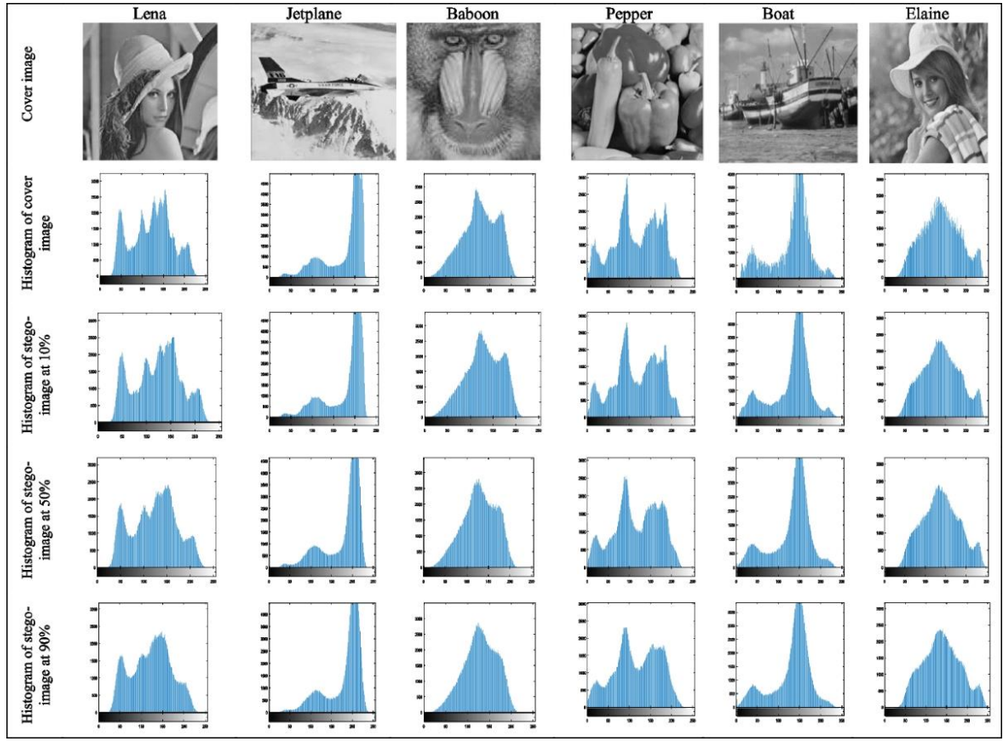
MSB

5. Стеганографічні методи приховування інформації

Приховування даних у растрових зображеннях і відео

Методи приховування в частотній області зображення
(вбудовування даних у частотні компоненти зображення після застосування математичних перетворень)

- **Метод дискретного косинусного перетворення (DCT)** (вбудовування даних у коефіцієнти DCT, які відповідають частотним компонентам зображення).
- **Метод дискретного хвильового перетворення (DWT)** (зміна коефіцієнтів DWT у певних піддіапазонах частот).
- **Метод Фур'є-перетворення (FFT)** (вбудовування інформації у фазову чи амплітудну частину спектра Фур'є).



5. Стеганографічні методи приховування інформації

Приховування даних у растрових зображеннях і відео

Широкосмугові методи

(рівномірне розподілення прихованих даних по всьому зображенню або відео з додаванням шуму)

- **Метод додавання білого шуму** (інформація маскується як низькорівневий шум у зображенні).
- **Пряме розширення спектра** (інформація маскується через розширення сигналу у широкому діапазоні частот).

Статистичні методи

(використання статистичних властивостей зображення для приховування даних)

- **Модифікація гістограм** (вбудовування даних через зміну частоти яскравості пікселів).
- **Перестановка пікселів** (зміна позиції пікселів за певною схемою).

Методи перекручування

(зміна структури або властивостей зображення для приховування інформації)

- **Перекручування геометрії** (накладання легких геометричних трансформацій (масштабування, поворот, зсув) для приховування даних).
- **Маніпуляція пікселями** (зміна груп пікселів у межах заданого блоку).

Структурні методи

(приховування даних через модифікацію логічної структури або метаданих зображення/відео)

- **Використання метаданих** (дані приховуються у полях метаінформації).
- **Зміна порядку блоків** (без порушення цілісності).
- **Модифікація кольорової моделі** (впровадження інформації у додаткові канали кольору).

5. Стеганографічні методи приховування інформації

Приховування даних у векторних зображеннях

Прямі методи

(базуються на безпосередній зміні параметрів графічних об'єктів у векторному зображенні для впровадження прихованих даних)

- **Зміна координат вузлів** (дані кодуються через зсув координат контрольних точок кривих або вузлів об'єктів).
- **Зміна товщини та стилю ліній** (використання різних значень товщини ліній (тонка або товста) для кодування інформації).
- **Маніпуляція кольорами (**зміна кольорів об'єктів або градієнтів).
- **Додавання непомітних елементів**

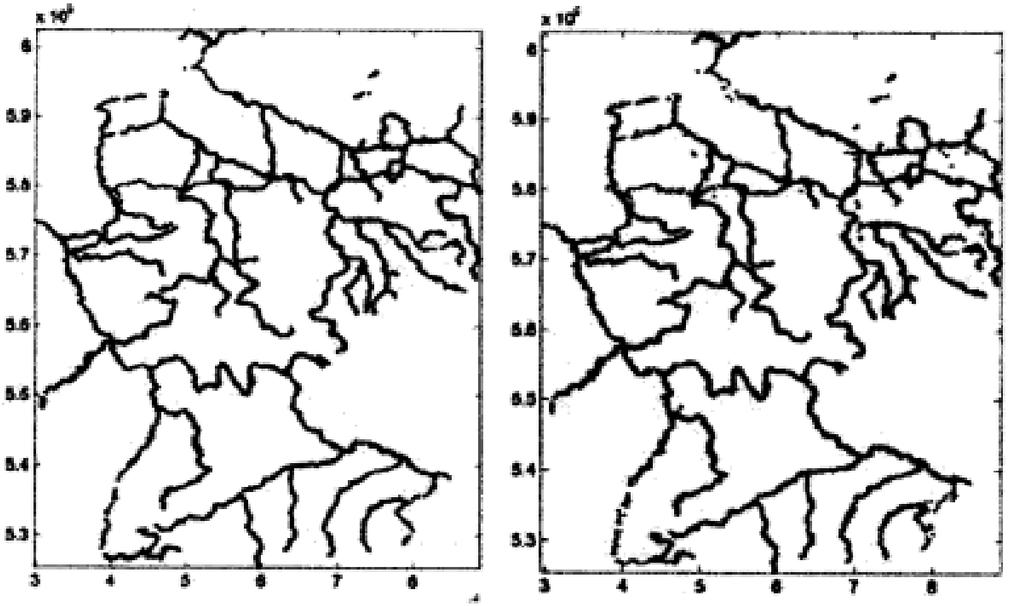
Методи на основі математичних перетворень

(використовують математичні трансформації для приховування інформації у параметрах векторних об'єктів)

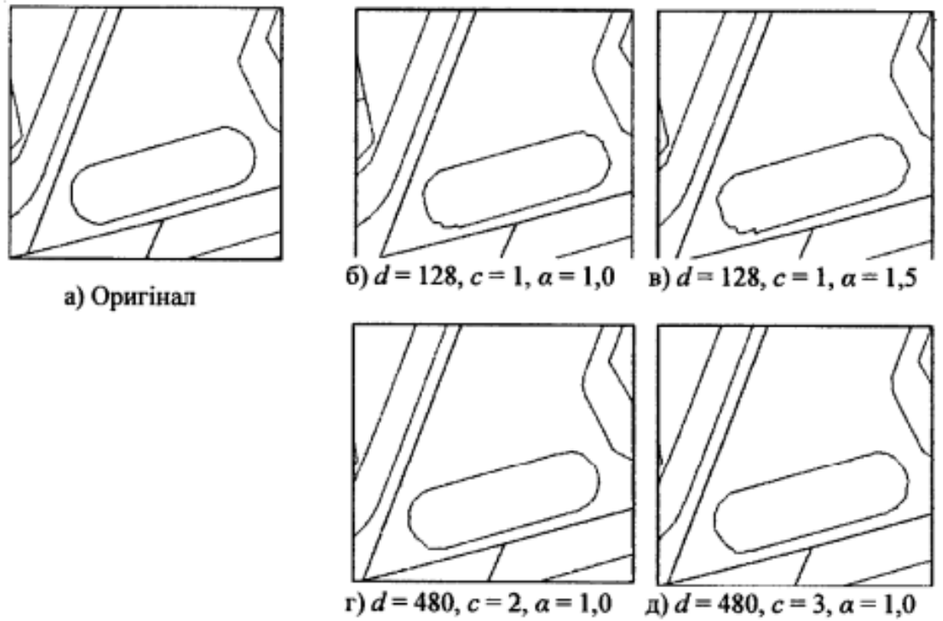
- **Зміна контрольних точок кривих Безьє** (дані кодуються через невеликі зсуви координат контрольних точок кривих Безьє)
- **Маніпуляція матрицями трансформації** (використання матриць масштабування, обертання, зсуву для кодування даних)
- **Приховування у симетрії та геометричних пропорціях**
- **Приховування через оптимізацію геометричних параметрів**

5. Стеганографічні методи приховування інформації

Приховування даних у векторних зображеннях



Оригінал З вбудованим ЦВЗ



а) Оригінал

б) $d = 128, c = 1, \alpha = 1{,}0$ в) $d = 128, c = 1, \alpha = 1{,}5$

г) $d = 480, c = 2, \alpha = 1{,}0$ д) $d = 480, c = 3, \alpha = 1{,}0$

З вбудованими ЦВЗ

5. Стеганографічні методи приховування інформації

Приховування даних у звуковому середовищі

Методи просторової області

(безпосередня зміна амплітуди або цифрових значень звукових семплів)

- **Модифікація найменш значущого біта (LSB)**:
- **Зміна амплітуди**
- **Зміна фази сигналу**
- **Додавання пауз або шуму**

Методи частотної області

(вбудовування інформації у певні частотні діапазони хвильових компонентів звуку)

- **Використання дискретного косинусного перетворення (DCT)**
- **Дискретне хвильове перетворення (DWT)**
- **Зміна гармонік**

Психоакустичні методи

(використовуються особливості людського слуху, такі як маскування звуку)

- **Частотне маскування**
- **Тимчасове маскування**

Широкосмугові методи

- **Розширення спектра** (інформація додається як шум у широкому частотному діапазоні)
- **Впровадження псевдовипадкових сигналів**

5. Стеганографічні методи приховування інформації

Приховування даних у звуковому середовищі

message1 - Notepad

File Edit Format View Help

```
Video provides a powerful way to help you prove your point.
When you click Online Video, you can paste in the embed code for the video you want to add.
You can also type a keyword to search online for the video that best fits your document.
To make your document look professionally produced, Word provides header, footer, cover page,
and text box designs that complement each other.
For example, you can add a matching cover page, header, and sidebar.
Click Insert and then choose the elements you want from the different galleries.
Themes and styles also help keep your document coordinated.
When you click Design and choose a new Theme, the pictures, charts, and SmartArt graphics
change to match your new theme.
When you apply styles, your headings change to match the new theme.
Save time in Word with new buttons that show up where you need them.
To change the way a picture fits in your document, click it and a button for layout
options appears next to it.
When you work on a table, click where you want to add a row or a column, and then
click the plus sign.
Reading is easier.

Video provides a powerful way to help you prove your point.
When you click Online Video, you can paste in the embed code for the video you want to add.
You can also type a keyword to search online for the video that best fits your document.
To make your document look professionally produced, Word provides header, footer, cover page,
and text box designs that complement each other.
For example, you can add a matching cover page, header, and sidebar.
```

Command Window

```
>> encoding
     4

Mesage byte 1
01010110
Audio samples 1-8 initially
1000110111
0010010111
0000011001
0100101110
0101111010
0100101110
0000011001
0100010101
Stego-object bytes 1-8 after embedding
the message at the LSB positions:
1000110110
0010010111
0000011001
0100101110
0101111011
0100101110
0000011001
0100010100
fx >>
```