1. **Стеганографія. Основні поняття - стеганографічна система, повідомлення, контейнер, ключ.**  
   Стеганографія - це наука про приховану передачу інформації шляхом збереження в таємниці самого факту передачі. На відміну від криптографії, яка приховує вміст секретного повідомлення, стеганографія приховує саме його існування.  
   Стеганографічна система (стегосистема) - об'єднання методів і засобів, що використовуються, для створення прихованого каналу для передачі інформації. При побудові такої системи домовилися про те, що:
   1. ворог уявляє роботу стеганографічної системи. Невідомим для противника є ключ за допомогою якого можна дізнатися про факт існування і змісту таємного повідомлення.
   2. При виявленні супротивником наявності прихованого повідомлення, він не повинен мати змогу отримати повідомлення до тих пір поки він не буде володіти ключем.
   3. Противник не має технічних та інших переваг.

Повідомлення - це термін, що використовуються, для загальної назви переданої прихованої інформації, буде це текст написаний молоком на білому папері або цифровий файл, в якому захована інформація.  
Контейнер - так називається будь-яка інформація, яка використовується для приховування таємного повідомлення. Порожній контейнер - контейнер, що не містить таємного послання. Заповнений контейнер (стегоконтейнер) - контейнер, що містить таємне послання.  
Ключ (стегоключ) - таємний ключ, потрібний для приховання стегоконтейнера. Ключі в стегосистемі бувають двох типів: приватні та публічні. Якщо стегосистеми використовує приватний ключ, то він повинен бути створений або до початку обміну повідомленнями, або переданий по захищеному каналу. Стегосистема, що використовує публічний ключ, повинна бути влаштована таким чином, щоб було неможливо отримати з нього приватний ключ. В цьому випадку публічний ключ ми можемо передавати по незахищеному каналу.

1. **Комп'ютерна стеганографія. Приклади.**  
   Комп'ютерна стеганографія - напрям класичної стеганографії, заснований на особливостях комп'ютерних платформ. Приклади - стеганографічна файлова система StegFS для Linux, приховування даних в невикористовуваних областях форматів файлів, підміна символів в назвах файлів, текстова стеганографія і т.д.  
   Приклади:
   1. Використання зарезервованих полів комп'ютерних форматів файлів - суть методу полягає в тому, що частина поля розширень, що не заповнена інформацією про розширення, за замовчуванням заповнюється нулями. Відповідно ми можемо використовувати цю «нульову» частину для запису своїх даних. Недоліком цього методу є низький ступінь прихованості(скритності) і малий обсяг інформації, що передається.
   2. Метод приховування інформації в місцях гнучких дисків, що не використовуються - при використанні цього методу інформація записується в частини диска, що не використовуються, наприклад, на нульову доріжку. Недоліки: низька продуктивність, передача невеликих за обсягом повідомлень.
   3. Метод використання особливих властивостей полів форматів, які не відображаються на екрані - цей метод заснований на спеціальних «невидимих» полях для отримання зносок, покажчиків. Наприклад, написання чорним шрифтом на чорному тлі. Недоліки: низька продуктивність, невеликий обсяг інформації, що передається.
   4. Використання особливостей файлових систем - при зберіганні на жорсткому диску файл завжди займає ціле число кластерів (мінімальних обсягів інформації, що адресуються). Наприклад, в файловій системі FAT32 стандартний розмір кластера- 4 КБ. Відповідно для зберігання 1 КБ інформації на диску виділяється 4 КБ, з яких 1КБ потрібен для зберігання файлу, а решта 3 ні на що не використовуються - відповідно їх можна використовувати для зберігання інформації. Недолік даного методу: легкість виявлення.
2. **Цифрова стеганографія. Алгоритми.**  
   Цифрова стеганографія - напрям класичної стеганографії, заснований на приховуванні або впровадженні додаткової інформації в цифрові об'єкти, викликаючи при цьому деякі спотворення цих об'єктів. Але, як правило, дані об'єкти є мультимедіа-об'єктами (зображення, відео, аудіо, текстури 3D-об'єктів) та внесення спотворень, які знаходяться нижче порога чутливості середньостатистичної людини, не приводить до помітних змін цих об'єктів. Крім того, у відцифрованих об'єктах, що спочатку мали аналогову природу, завжди присутній шум квантування; далі, при відтворенні цих об'єктів з'являється додатковий аналоговий шум і нелінійні спотворення апаратури, все це сприяє кращому прихованню інформації.  
   Всі алгоритми вбудовування прихованої інформації можна розділити на кілька підгруп:
   1. Працюючі з самим цифровим сигналом. Наприклад, метод LSB.
   2. «Накладення» інформації, що приховується. В даному випадку відбувається накладення зображення (звуку, іноді тексту), що приховується за оригіналом. Часто використовується для вбудовування цифрових водяних знаків (ЦВЗ).
   3. Використання особливостей форматів файлів. Сюди можна віднести запис інформації в метадані або в різні інші зарезервовані поля файлу, що не використовуються.
3. **Метод LSB.**  
   LSB (Least Significant Bit, найменший значущий біт) - суть цього методу полягає в заміні останніх значущих бітів в контейнері (зображення, аудіо або відеозапису) на біти повідомлення, що приховується. Різниця між порожнім і заповненим контейнерами повинна бути не відчутна для органів сприйняття людини.  
   Приклад

Припустимо, є 8-бітове зображення в градаціях сірого. 00h (00000000b) позначає чорний колір, FFh (11111111b) - білий. Усього є 256 градацій (28). Також припустимо, що повідомлення складається з 1 байта - наприклад, 01101011b. При використанні 2 молодших біт в описах пікселів, нам буде потрібно 4 пікселя. Припустимо, вони чорного кольору. Тоді пікселі, що містять приховане повідомлення, будуть виглядати наступним чином: 00000001 00000010 00000010 00000011. Отже колір пікселів зміниться: першого-на 1/255, другого і третього-на 2/255 і четвертого- на 3/255. Такі градації, мало того що непомітні для людини, можуть взагалі не відображатися при використанні низькоякісних пристроїв виведення зображення.

Методи LSB є нестійкими до всіх видів атак і можуть бути використані тільки при відсутності шуму в каналі передачі даних. Виявлення LSB-закодованого стего здійснюється за допомогою аномальних характеристик розподілу значень діапазону молодших бітів відліку цифрового сигналу.

Інші методи приховування інформації в графічних файлах орієнтовані на формати файлів з втратою, наприклад, JPEG. На відміну від LSB вони більш стійкі до геометричних перетворень. Це можливо за рахунок змін у широкому діапазоні якості зображення, що призводить до неможливості визначення джерела зображення.

1. **Стегоаналіз.**   
   Стегоаналіз - це протидія стеганографії, як криптоаналіз - це протидія криптографії. Основна мета стеганографії - приховати факт передачі даних. Отже, основна мета стегоаналіза - виявити факт приховування передачі даних.  
   Розглянемо метод виявлення послідовного вбудовування в LSB одного біта на прикладі зображення у форматі BMP.

Існує думка, що в зображеннях LSB є випадковими. Насправді це не так! Хоча людське око і не помітить змін зображення при зміні останнього біту, статистичні параметри зображення будуть змінені. Перед приховуванням дані зазвичай архівуються (для зменшення об’єму) або шифруються (для забезпечення додаткової стійкості повідомлення при потраплянні у чужі руки). Це робить біти даних дуже близькими до випадкових. Послідовне вбудовування такої інформації замінить LSB зображення випадковими бітами. І це можна виявити!

Для прикладу візьмемо одну кольорову компоненту повнокольорового зображення BMP і на ній покажемо процес знаходження вбудовування. Яскравість кольорової компоненти може приймати значення від 0 до 255. У бінарній системі - від 0000 0000 до 1111 1111.

Розглянемо пари:

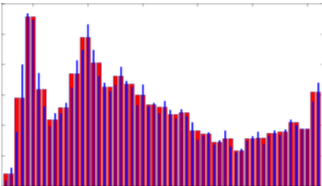
0000 00**00** <-> 0000 00**01**;

0000 00**10** <-> 0000 00**11**;

...

1111 11**00** <-> 1111 11**01**;

1111 11**10** <-> 1111 11**11**.

Дані числа відрізняються між собою тільки в LSB (виділені жирним). Таких пар для кольорової компоненти BMP зображення: 256/2 = 128. У разі стеганографічного вбудовування тобто заміни LSB на випадкову послідовність, кількість пікселів в парах вирівняється. Гістограма приймає «сходинковий» ​​вид (два сусідніх значення яскравості зустрічаються з однаковою частотою).  
  
На малюнку синім кольором позначена гістограма зображення без вбудовування, а червоним - гістограма того ж зображення після вбудовування даних замість. Порівняння двох гістограм дає можливість стегоаналізу послідовно приховуваних біт.