**Стеганос-ма** – сов. средств и методов, для формир *скрыт. канала* передачи (хран) инфы.  
Скрытый канал организ. на базе открытого, с исп особенностей восприятия  
*Отличие от крипт*: сам факт наличия канала – тайна

**Стеганос-ма** – нек. мн-во отображений одного пр-ва (мн-во М) в другое (мн-во стеганосообщений S)

**Стеганос-ма ∑** - сов. сообщений М, контейнеров С, ключей К, стеганосооб. S и преобразований (прямого F и обр. F-1), кот. их связывают: ∑ = (M, C, K, S, F, F -1)

**Компоненты:**  
\* контейнер **С** – файл, в кот. тайное сообщ. **М**, он и есть скрытый канал  
\* тайное сообщ **М** – для перед/хран, мб цифр. водяные знаки  
\* ключ. инфа **К** – мб неск: 1 - для осажд/извлеч инфы, 2 - для выбора элем. контейнера для модификации при осажд, 3 – для предвар преобраз тайной инфы  
\* стеганоконтейнер **S** = стеганосообщ. – конт. с осажд. сообщ, перед. по откр каналу  
**Субъекты:**  
\* отправитель  
\* получатель  
**Классы цифр. (комп.) стеганографии:**  
\* аудиостеган.  
\* видеостеган.  
\* граф. стеган.  
\* текст. стеган.  
**Осн. положения стеганос-мы:**  
*«тайное хран/перед одной инфы в другой открытой инфе»*  
\* св-ва контейнера дб измен, но чтобы изменения нельзя выявить при визуальном контроле, не д. привлечь внимание  
\* противник (интруз) знает о стег. с-ме и ее реализации, но не знает ключ, с пом. к-го устан факт наличия скрытого сообщ  
\* если противник узнает о сущ. скрыт. сообщения, он все равно не сможет извлечь его, пока ключ в тайне  
\* у противника не дб преимуществ в раскрытии содержания тайных сообщ

**Изображение:**Чаще контейнер – **изобр**: (текст тоже изобр)  
\* м. внедрить большой V д-х  
\* заранее извествен р-р конт.  
\* есть текстурные области – у них шумовая структ, легко встроить инфу  
\* чел. глаз слабо чувств. к небольш измен. изобр (ярк, контр…)  
\* разраб. хорошие методы их цифр. обработки

**Метод НЗБ:**LSB (Least Significant Bit, наименьший значащий бит) — суть в замене последних значащих битов в контейнере на биты скрываемого сообщения.  
осн. на огранич. способностях зрения и слуха  
пр.: 24 бит растр. изобр, к. точка кодир. 3 байтами (rgb)  
измен. младших битов r,g,b незаметно челу  
~50% бит, кот. мы хотим записать, изменять не нужно (совпад. с контейнером)

изобр 500x500 = 250 000 px = 750 000 цвет. бит  
если хотим измен. т. младшие биты, то VM max < 750 000 бит

**BITMAP:**  
изобр – матрица пикселов, к. точка – x, y, rgb  
контейнеры bitmap: «чистые» и зашумленные  
осаждение сообщ. в контйнер наруш. завис. м/младшими и ост. бит => аналитик заметит  
но если изобр. зашумлено (со сканеры) => опред. осажд. сложнее  
**PNG:**Portable Network Graphics  
размер на 30-40% больше jpeg, gif  
изобр 500x500 = 250 000 px = 750 000 цвет. бит  
если хотим измен. т. младшие биты, то VM max < 750 000 бит

**Методы стеган. анализа:**  
\* визуальный (чаще всего)

**ЗАДАНИЕ:**

\* НЗБ  
- выбор файла-контейнера – по соглас  
- 2 варианта осажд/извлекаемого сообщ: ФИО; текст. часть к-нибудь отчета  
- 2 метода размещ бит. потока осажд. сообщения по содержимому контейнеру  
- сформир цвет. м-цы (12.7), отобр. каждый осажд. уровень младших бит  
- визуальный анализ

**АЛИНА**