

СТЕГАНОГРАФИЯ



Криптография

- это наука о методах обеспечения:

- конфиденциальности (невозможности прочтения информации посторонним),
- целостности данных (невозможности незаметного изменения информации),
- аутентификации (проверки подлинности авторства или иных свойств объекта),
- невозможности отказа от авторства.

Шифрование (на основе шифра и ключа) – процесс применения преобразования открытого текста на основе ключа, в результате которого возникает шифрованный текст

Стеганография

- это наука о скрытой передаче информации, путём сохранения в тайне самого факта передачи



Я сказал не
"прием", а "при
нем". Билет
номер 9, а при
нем - задача.

Классификация стеганографии

- Классическая стеганография до появления компьютеров



- Компьютерная стеганография основана на особенностях компьютерной платформы (каналы связи, ОС, файлы, разработка специальных программ)
- Цифровая стеганография основана на сокрытии или внедрении дополнительной информации в цифровые объекты (изображения, звук)

Классическая стеганография

Симпатические чернила

- Текст, записанный такими чернилами, проявляется только при определённых условиях
- Изобретатель (?) - в I веке н. э. Филон Александрийский

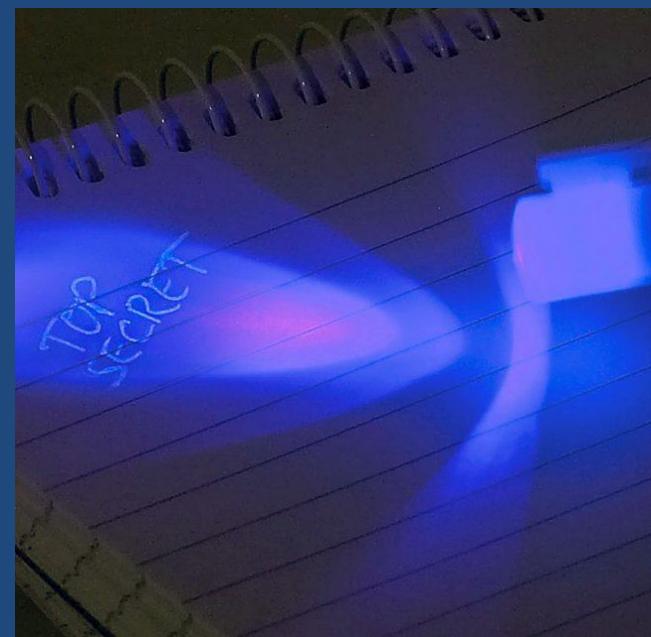


животе свои пухлые ручки, стал оглядывать Незнайку с головы до ног.

— Наверно, в капкан попался? — спросил наконец он.

— С ГРИБАМИ ТУТ ТУРБОЗАТ
— Так точно, господин Клопс. Жрал малину и попался в капкан.

— Так, так, — промычал Клопс. — Ну, я тебе покажу, ты у меня попляшешь! Так зачем ты малину жрал, говори?



Симпатические чернила

Чернила	Проявитель
Пиво и белое вино	пепел сожженной бумаги (текст слегка увлажняется дыханием...)
Сахарная вода и фабричный яблочный сок	пепел бумаги (при увлажнении текста)
Яблочный сок (при "макании" в яблоко) и молоко (разбавленное)	нагрев
Сок лука и брюквы	нагрев
Пищевая лимонная кислота	бензилоранж
Пирамидон (в спиртовом растворе)	нагрев
Аспирин	соли железа
Крахмал	йодная настойка

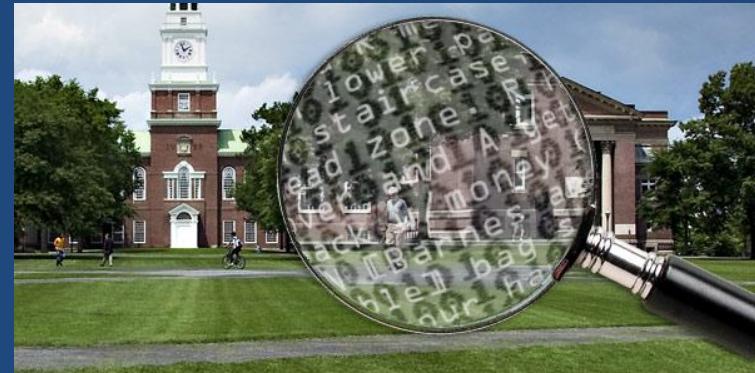
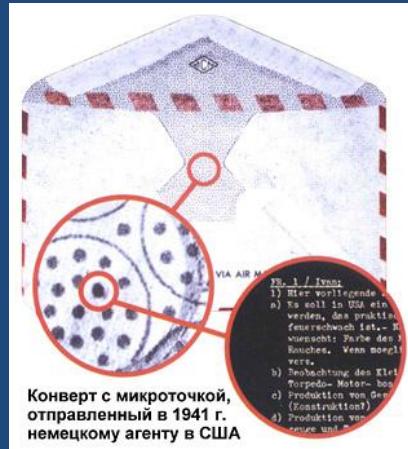
Симпатические чернила

Чернила	Проявитель
Фенолфталеин	всякая разбавленная щелочь
Квасцы	нагрев
Серная (аккумуляторная) кислота (при 10-15%)	нагрев
Воск (хоть как-то заостренный фрагмент свечи...)	кальция карбонат, или зубной порошок (посыпать и стряхнуть)
Стиральный порошок (с оптическим отбеливателем)	свет лампы ультрафиолета
Слюна	очень разбавленные водой чернила
Кровь (при сильном разбавлении)	слабый (0,1%) раствор люминола (1 ч) с двуукглекислой содой (5 ч)
Вяжущие средства для дезинфекции рта и глотки	нагрев

Классическая стеганография

Другие методы

- микроточки



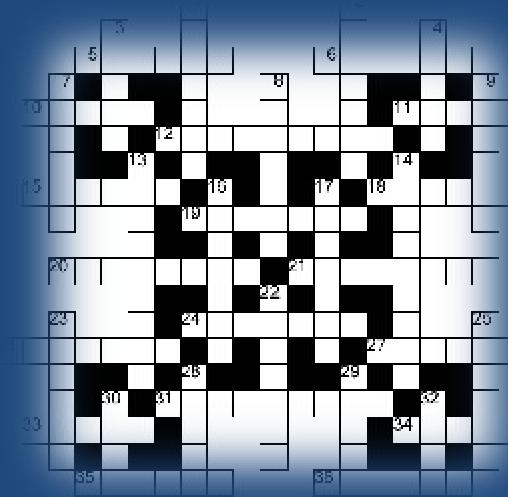
- запись на боковой поверхности колоды карт)
- текст под наклеенной почтовой маркой
- "Аве Мария", в кодовом варианте которого каждому слову, а порой и фразе, ставятся в соответствие несколько слов



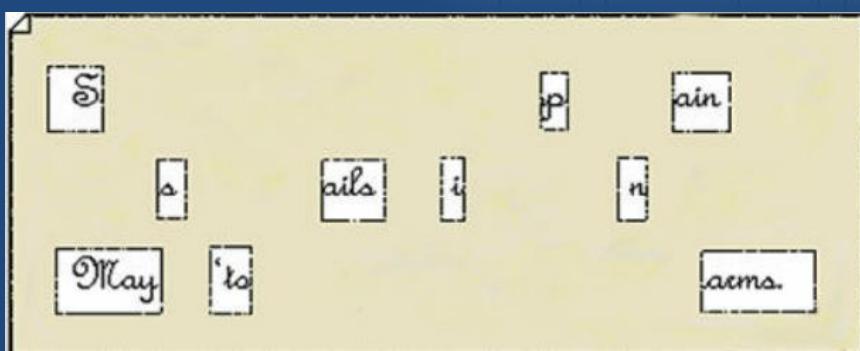
Классическая стеганография

Другие методы

- записи лишь в вертикальных столбцах полностью заполненного кроссворда (горизонтальные строки при этом заполняются произвольно)
- записи по трафарету, все остальное пространство здесь тщательно заполняется "пустым" содержанием



Sir John regards you well and speaks again that
all as rightly 'wails him is yours now and ever.
May he 'lone for past & lays with many charms.



Классическая стеганография

Другие методы

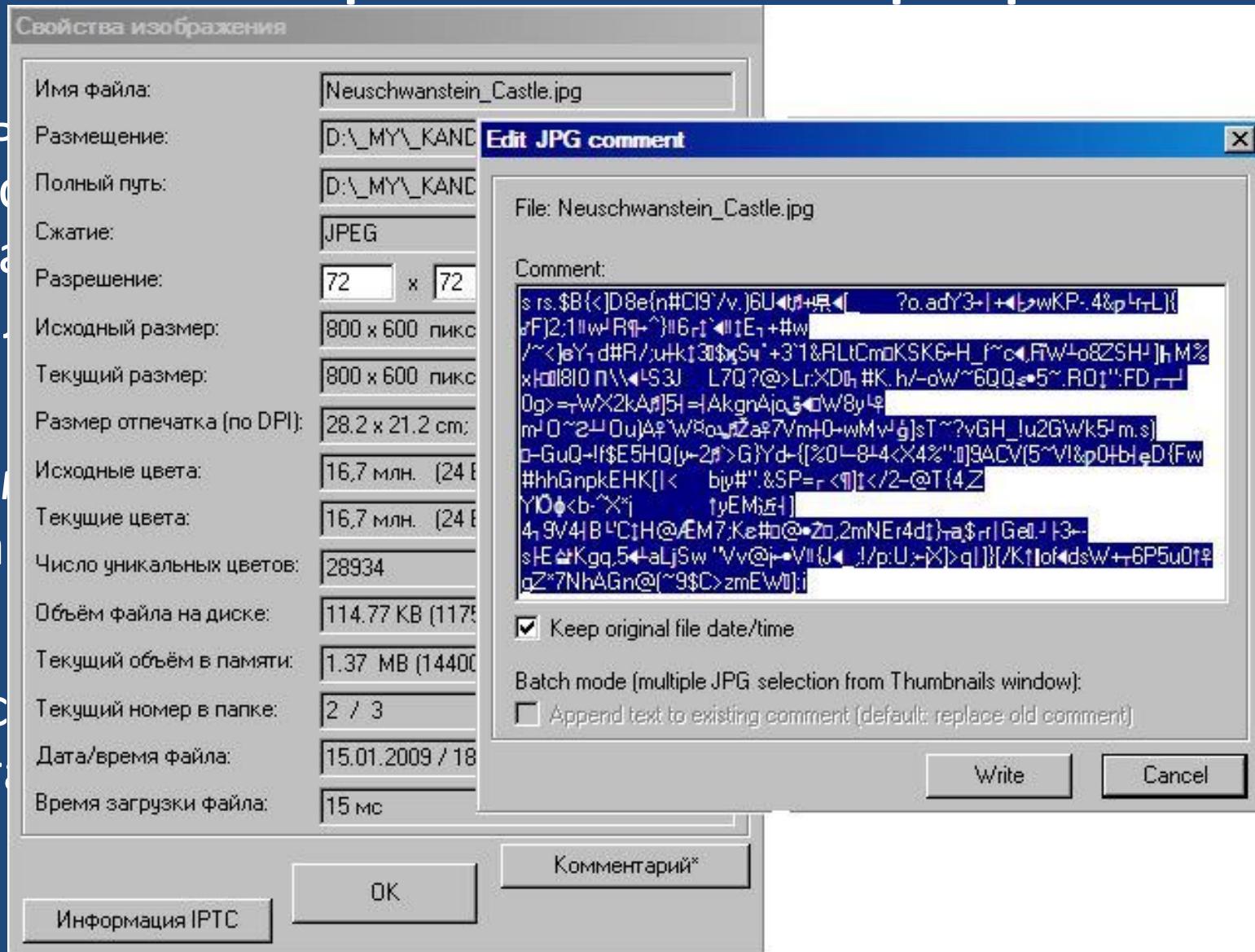
- запись внутри объектов (на внутренней поверхности спичечного коробка, внутри вареного яйца, ...)
- наколы в тексте (иголкой)
- чтение определенных букв или слов в тексте
- акrostих:
- пазлы
- семаграмма
(код в виде рисунка)

Желаю тебе успеха,
День свадьбы не забудь назвать,
И кольцо выбрать поможем.

Погоди только с выбором места,
Отправимся в самое лучшее заведение,
День твоей свадьбы не будет в какой то там захудалой забегаловке
Может даже дворец снимем.
Оторвемся на всю катушку, все пикабу туда поместится.
Гармонии вам в отношениях,
И конечно же, взаимопонимания с ее родителями

Компьютерная стеганография

- скрытие неисходных областей файла
- подделка в наименовании
- текстовая стеганография



Цифровая стеганография



+ «How are you?» =



Метод замены наименее значащего бита

Пиксель

1	1	0	0	0	0	1	1
0	0	1	0	0	0	0	0
0	1	1	0	0	1	1	0

R — 195
G — 32
B — 102



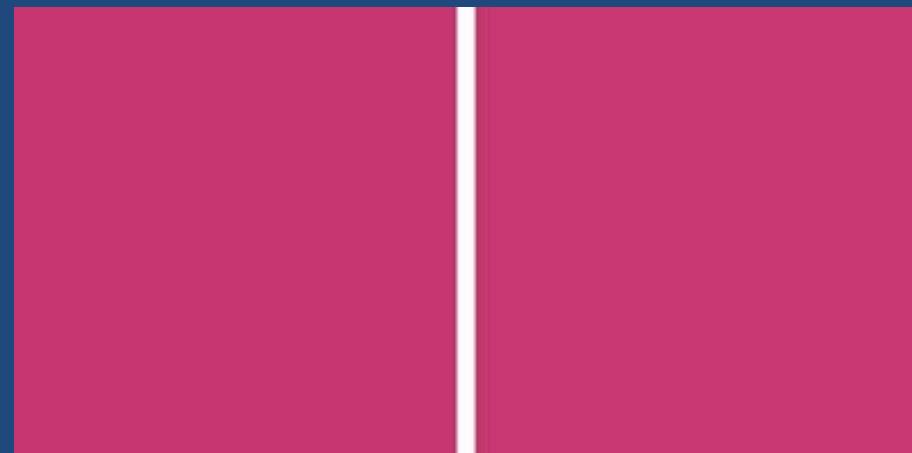
Сокрытие 6 бит – 101100

1	1	0	0	0	0	1	0
0	0	1	0	0	0	1	1
0	1	1	0	0	1	0	0

R — 194
G — 35
B — 100



Новый цвет, очень похожий на первоначальный:



Метод замены наименее значащего бита

ORIGINAL IMAGE

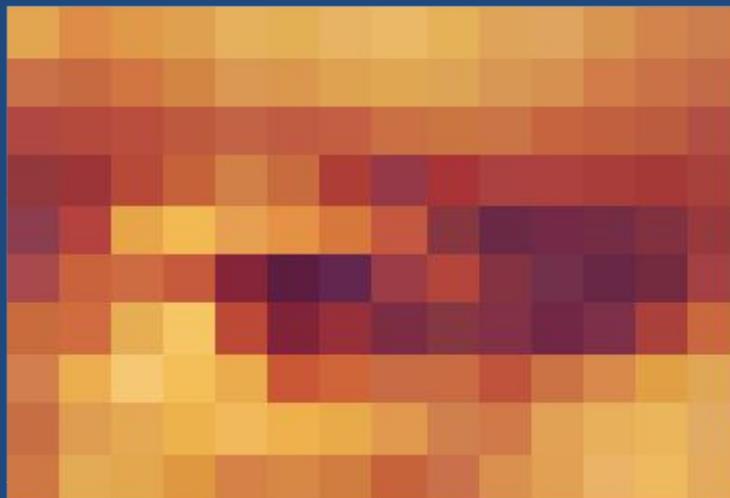


IMAGE WITH HIDDEN DATA



R202 G212 B75
R198 G99 B59
R209 G124 B65
R215 G135 B70
R214 G129 B72
R223 G152 B64
R227 G168 B78
R227 G171 B86
R207 G120 B70

R203 G113 B75
R198 G98 B58
R208 G126 B67
R215 G134 B70
R215 G129 B75
R223 G153 B67
R226 G168 B81
R226 G170 B88
R206 G120 B71