

## 1.2. Системы встраивания информации

Материалы курса лекций "Цифровые водяные знаки и стеганография"

Федосеев В.А.

Самарский университет  
Кафедра ГИиИБ

2 сентября 2024 г.

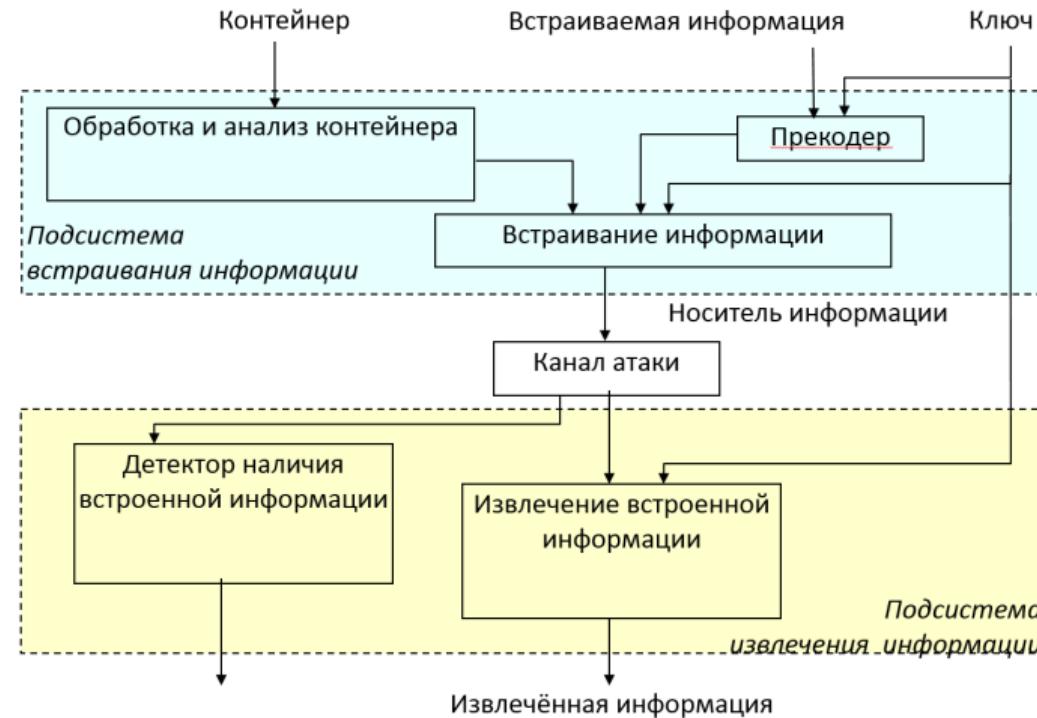
## 1.2.1. Понятие систем встраивания информации

### Определения

- Совокупность методов и средств, образующих единое решение для встраивания информации в цифровой сигнал, будем называть **системой встраивания информации (СВИ)**
- К СВИ относятся стегосистемы и ЦВЗ-системы
- Любая СВИ состоит из двух основных блоков (подсистем): встраивания информации и извлечения информации

## 1.2.1. Понятие систем встраивания информации

### Упрощённая схема СВИ



## 1.2.1. Понятие систем встраивания информации

### Специфика стегосистем

- Ключевое требование – недопустимость обнаружения наличия скрытой информации несанкционированным получателем
- Основной целью атак является обнаружение факта наличия встроенной информации (извлечение её содержания не является необходимым)
- Разработка таких атак является задачей **стегоанализа**
- Если стегосистема является устойчивой к ним, то говорят, что она обладает **стеганографической стойкостью**
- Методы должны позволять встраивать большой объём данных

## 1.2.1. Понятие систем встраивания информации

### Специфика ЦВЗ-систем

- Ключевой характеристикой ЦВЗ-систем также является стойкость, но она имеет несколько иной смысл
- Под **стойкостью ЦВЗ-систем** понимается возможность извлечения встроенной информации из искажённого (преднамеренно или случайно) контейнера
- Стойкость как правило определяется применительно к конкретному типу искажений
- В ряде задач требуется, чтобы ЦВЗ был гарантированно нестойким к определённым преобразованиям
- Различают защищённые, стойкие, полухрупкие и хрупкие СВИ

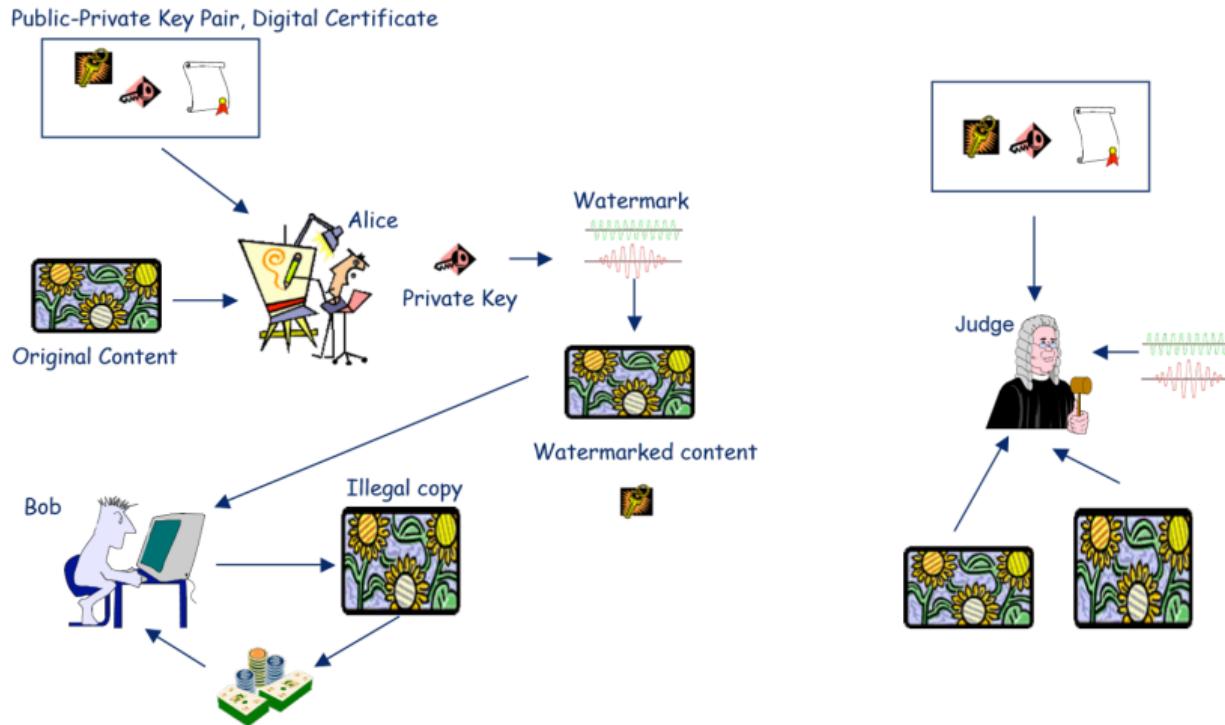
## 1.2.2. Назначение систем встраивания информации

Задачи, решаемые при помощи СВИ

- Скрытая передача информации  
(steganography, стеганография)
- Защита авторских прав  
(robust watermarking, стойкие водяные знаки)
- Защита от несанкционированного распространения  
(fingerprinting, цифровые отпечатки пальцев)
- Защита данных от изменений или подделки  
(fragile watermarking, хрупкие водяные знаки - чаще всего)
- Мониторинг телевещания
- Контроль копирования носителей видео
- Встраивание метаданных

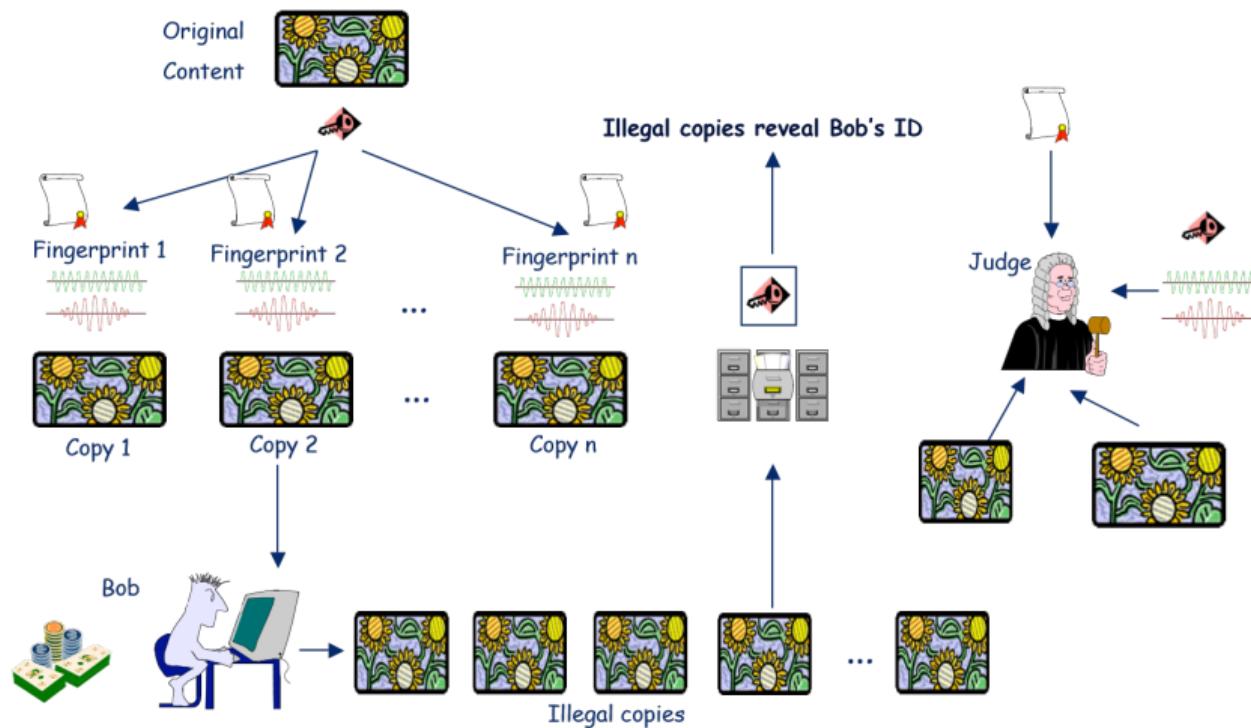
## 1.2.2. Назначение систем встраивания информации

Захист авторських прав: схема розв'язання задачі



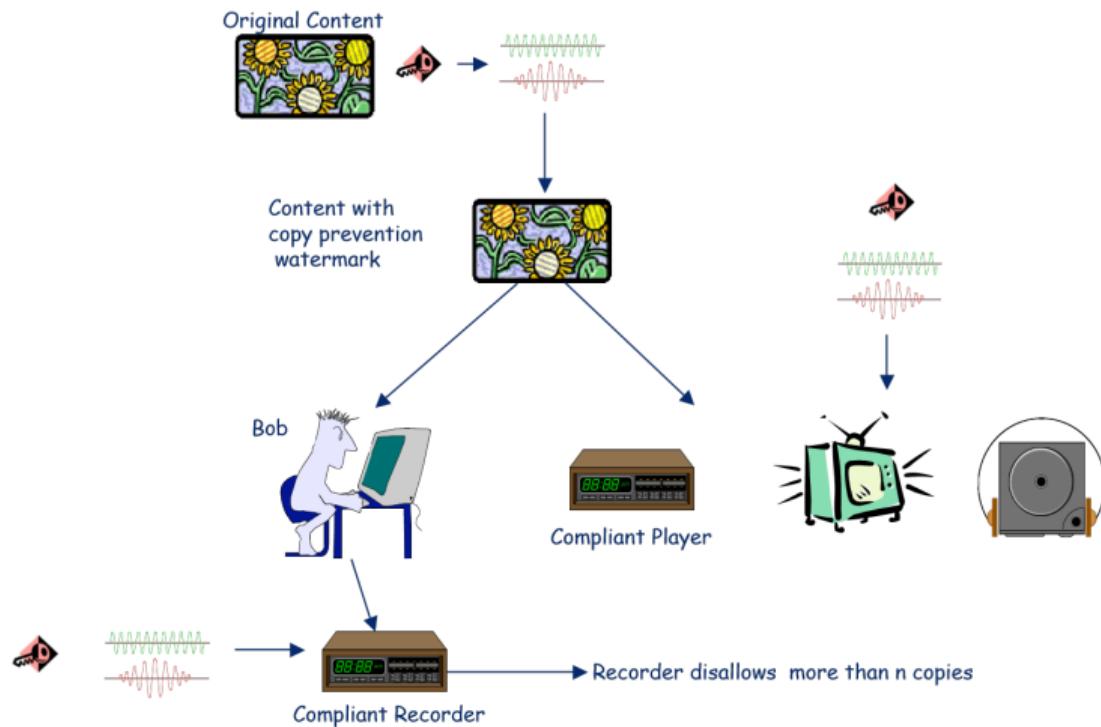
## 1.2.2. Назначение систем встраивания информации

Защита от несанкционированного распространения: схема метода fingerprinting



## 1.2.2. Назначение систем встраивания информации

Контроль копирования: схема решения задачи



## 1.2.3. Свойства систем встраивания информации

### Список свойств СВИ

- ① Является ли СВИ ЦВЗ-системой
- ② Является ли СВИ стеганографической системой
- ③ Действие, выполняемое подсистемой извлечения информации: *проверка наличия встроенной информации (детектирование) или извлечение встроенной информации (декодирование)*
- ④ Слепое / неслепое извлечение
- ⑤ Тип мультимедиа-контейнера: звук, изображение, видео и пр.
- ⑥ Информированное / слепое встраивание
- ⑦ Способ модификации сигнала при встраивании информации: *аддитивный, мультипликативный, иной*

## 1.2.3. Свойства систем встраивания информации

### Список свойств СВИ

- ⑧ Визуальная различимость встроенной информации
- ⑨ Максимально возможный объем встраиваемой информации: *доля контейнера, фиксированный, ровно 1 бит*
- ⑩ Возможность повторного встраивания другой информации в тот же сигнал тем же методом
- ⑪ Симметричная / асимметричная схема распределения ключей
- ⑫ Удаляемость встроенной информации после извлечения: *у узком смысле / в широком смысле*
- ⑬ Инвертируемость и квазинвентирируемость - возможность детектирования ложного ЦВЗ
- ⑭ Стойкость встроенной информации кискажениям её носителя

## 1.2.3. Свойства систем встраивания информации

### Классификация СВИ по стойкости к искажениям

- **Защищённые СВИ (secure)**: стойкость встроенной информации должна сохраняться как при преднамеренных атаках, так и при непреднамеренных искажениях.
- **Стойкие СВИ (robust)** защищены только от произвольных непреднамеренных искажений.
- **Полухрупкие СВИ (semi-fragile)** устойчивы к одним преобразованиям и неустойчивы к другим
- **Хрупкие СВИ (fragile)**: информация разрушается даже при незначительных модификациях носителя информации.

## 1.2.3. Свойства систем встраивания информации

Требования к свойствам систем встраивания информации в зависимости от их назначения

| Назначение СВИ                                 | Требования по визуальной различимости ВИ | Требования к системам по стойкости | Допустимые способы извлечения |
|--|--|------------------------------------|-------------------------------|
| Защита авторских прав                          | Неразличима или различима                | Секретные и стойкие                | Декодер или детектор          |
| Защита от несанкционированного распространения | Обязательно неразличима                  | Секретные и стойкие                | Декодер                       |
| Защита от изменений                            | Неразличима или различима                | Полухрупкие и хрупкие              | Детектор                      |
| Передача информации                            | Обязательно неразличима                  | Секретные и стойкие                | Декодер                       |
| Защита от подделки                             | Неразличима или различима                | Секретные и стойкие                | Детектор                      |

## 1.2.4. Атаки на системы встраивания информации

Классификация атак по целям, которые преследует нарушитель

- Обнаружение наличия встроенной информации ( $\alpha_0$ )
- Извлечение встроенной информации без отыскания ( $\alpha_d$ )
- Удаление встроенной информации ( $\alpha_r$ )
- Отыскание секретного ключа ( $\alpha_k$ )
- Подмена встроенной информации ( $\alpha_c$ )
- Подделка носителя информации ( $\alpha_f$ )

## 1.2.4. Атаки на системы встраивания информации

Классификация атак по знаниям и возможностям, которыми обладает нарушитель

- только с известным носителем информации
- с известным контейнером
- с известной встроенной информацией
- с выбранным контейнером
- с выбранной встраиваемой информацией

Модели нарушителя:

- пассивная
- активная

## 1.2.4. Атаки на системы встраивания информации

Требования по стойкости СВИ к атакам в зависимости от назначения

| Назначение СВИ        | Стойкость к атакам |            |            |            |            |            |
|-----------------------|--------------------|------------|------------|------------|------------|------------|
|                       | $\alpha_0$         | $\alpha_d$ | $\alpha_r$ | $\alpha_k$ | $\alpha_c$ | $\alpha_f$ |
| Защита авторских прав | –                  | –          | + –        | +          | +          | –          |
| Защита от копирования | –                  | +          | + –        | –          | +          | +          |
| Защита от изменений   | –                  | –          | –          | +          | –          | +          |
| Передача информации   | +                  | +          | + –        | +          | +          | –          |
| Защита от подделки    | –                  | –          | –          | +          | –          | +          |