4.4 СВИ для видео, их особенности, примеры использования

Назначение СВИ для видео

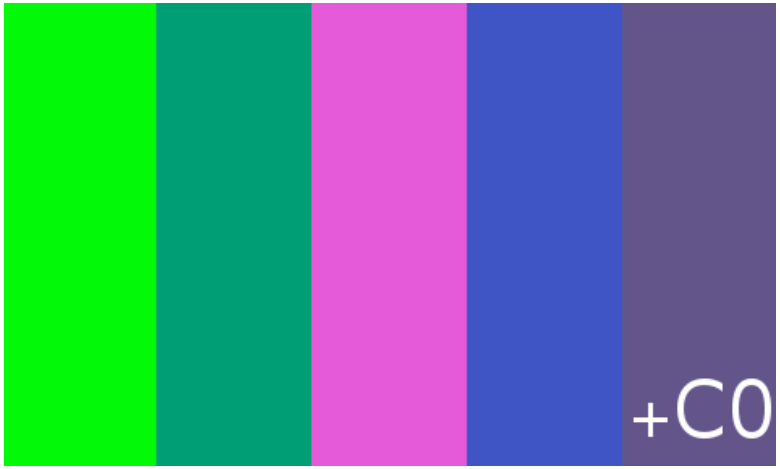
- Скрытая передача информации
- Защита авторских прав
- Защита от копирования
- Защита от изменений
- Встраивание метаданных
- Контроль копирования
- Мониторинг вещания

Требования по стойкости для СВИ в изображения и видео

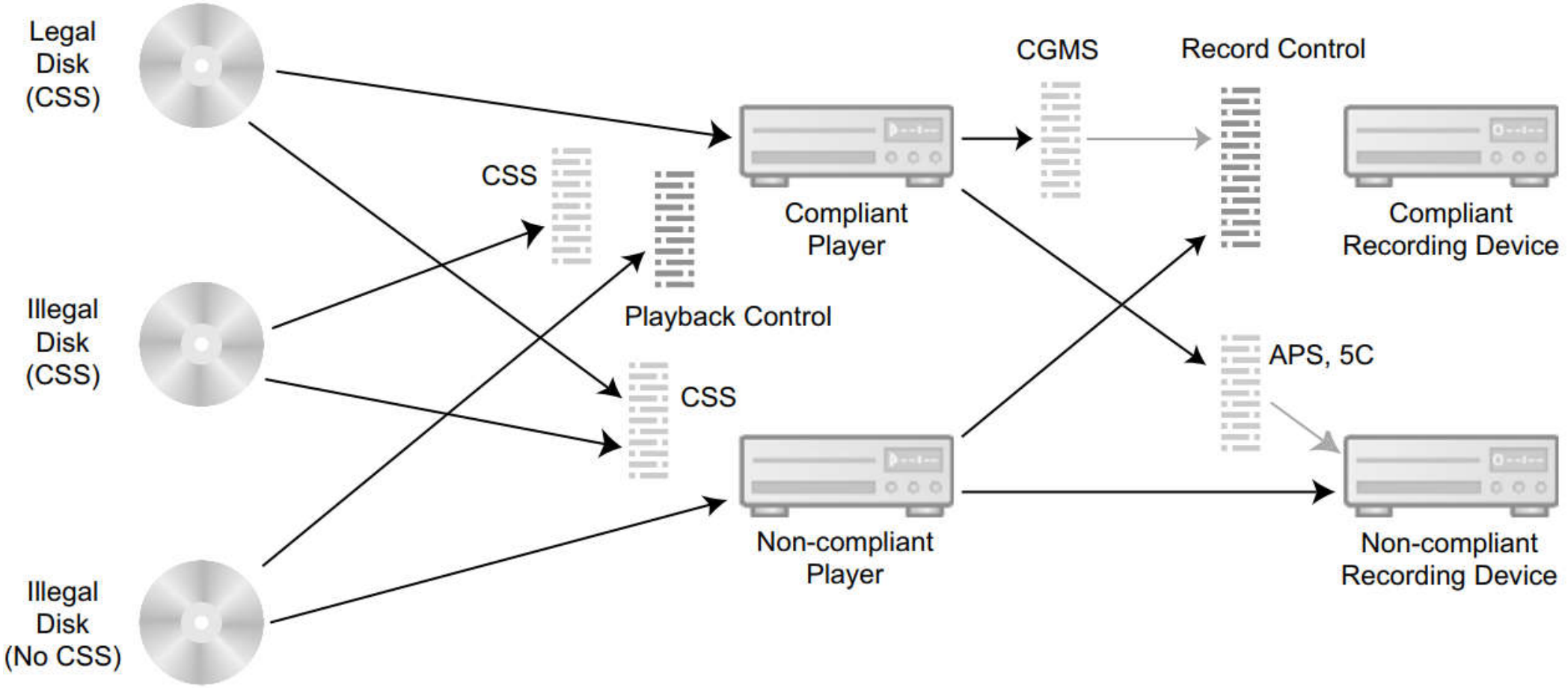
Искажения	Важность для СВИ в изображения	Важность для СВИ в видео
1. Линейные искажения	+	+
2. Зашумление	+	+
3. Фильтрация	+	+
4. Геометрические преобразования	+	-
5. Потеря части пространственных данных	+	+-
6. Пропуск кадров и сцен	-	+
7. Сжатие с потерями	+	++
8. ЦАП – АЦП	+-	+
9. Встраивание повторного ЦВЗ	+-	+-

Шифрование контента DVD

- CSS - Content Scrambling System (1995)
  - Шифрует поток MPEG-2
  - 2 ключа по 40 бит: 1 - уникальный для диска, 2 - для MPEG-файла
  - Из-за уязвимости фактическая длина 16 бит
- AACS - Advanced Access Content System (2005 - ...)
  - 2 ключа по 128 бит, шифрование AES
  - При появлении ключей расшифровки в открытом доступе они перестают использоваться при записи новых дисков
  - Универсальный ключ 09 F9 11 02 9D 74 E3 5B D8 41 56 C5 63 56 88 C0 «Флаг свободы слова» (2007)
- CGMS - Copy Generation Management System
  - copy-always, copy-never, copy-once
- 5C - 5 companies
  - Шифрование, ключи известны 5 компаниям-производителям

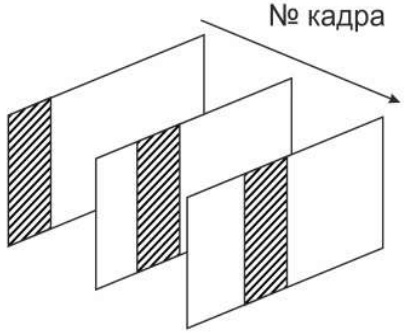


Защита DVD от копирования

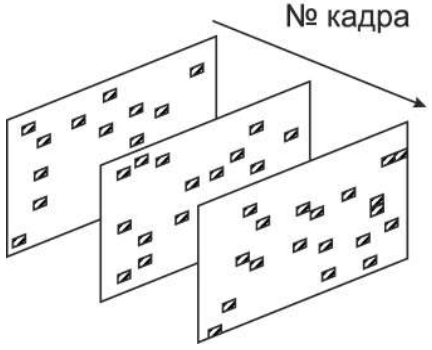


Два подхода

- Видео рассматривается как набор независимых кадров (изображений), и в каждый кадр встраиваются одни и те же данные
  - + Стойкость к потере синхронизации
  - - Объем данных невелик – определяется размером кадра
  - - В базовом варианте подвержен атаке с «приближённым вычислением ЦВЗ» (“watermark estimation attack”)



- Видео рассматривается как набор упорядоченных кадров, и встраиваемая информация распределяется между многими кадрами
  - + Объем данных пропорционален продолжительности видео
  - - Нужно обеспечить стойкость к потере синхронизации



СВИ (Hartung & Girod)

- $\mathbf{b} \in \mathbb{B}^1_{[N_b]}$, $C \in \mathbb{Z}^3_{[N_1 \times N_2 \times T]}$ ($N_1 \times N_2$ – размеры кадра, а T – число кадров видео)
- Переход к одномерному сигналу: $\varphi(n): n \mapsto (n_1, n_2, t)$
- $f(n) = C\big(\varphi(n)\big)$ - итоговая матрица признаков
- Перед встраиванием осуществляется кодирование информации:

$$\Omega(n) = (-1)^{b_i} \text{ для } i \cdot L \leq n < (i+1) \cdot L,$$

$L \in \mathbb{N}$ – параметр, характеризующий избыточность встраивания

$i = 0..N_b - 1$, а $n = 0..\min(N_b \cdot L, N) - 1$

- Если $N_b \cdot L < N$, то в оставшуюся часть сигнала встраивание не производится.

СВИ (Hartung & Girod)

- Встраивание информации:

$$f^W(n) = f(n) + \alpha \cdot \beta(n) \cdot \Omega(n) \cdot (-1)^{k_n},$$

  - k_n – n-й бит ключа $\mathbf{k} \in \mathbb{B}^1_{[N_b]}$,
  - $\alpha > 0$ – постоянный множитель при встраиваемом сигнале,
  - $\beta(n) > 0$ – адаптивный множитель при встраиваемом сигнале, причём $\forall i \in [0, N_b - 1]\ \forall n \in [i \cdot L, (i+1) \cdot L - 1]\ \ \beta(n) \approx \bar{\beta}_i$,

$$\bar{\beta}_i = \frac{1}{L} \sum_{n=i \cdot L}^{(i+1) \cdot L - 1} \beta(n)\,.$$

СВИ (Hartung & Girod): извлечение

- Слепой метод извлечения
- Оценка матрицы признаков извлечённой информации

$$\tilde{\Omega}(n) = (-1)^{k_n} \cdot h^W(n),$$

где h^W – подбирается таким образом, чтобы

$$h^W(n) \approx f^W(n) - f(n).$$

- Вместо $f(n)$ при извлечении используется оценка $f^W_{mean,S}(n)$ – усреднённый в скользящем окне шириной $S \geq 3$ вектор $f^W(n)$:

$$h^W(n) = f^W(n) - f^W_{mean,S}(n).$$

СВИ (Hartung & Girod): извлечение

- Значение очередного бита b_i^R определяется на основе анализа величины

$$\gamma_i = \mathcal{P}_f^{-1}(\tilde{\Omega}) = \sum_{n=i\cdot L}^{(i+1)\cdot L-1} \tilde{\Omega}(n)\,.$$

- Тогда

$$\gamma_i \approx \sum_{n=i\cdot L}^{(i+1)\cdot L-1} \alpha\cdot\beta(n)\cdot\Omega(n)\cdot(-1)^{2k_n} = \alpha\cdot L\bar{\beta}_i\cdot(-1)^{b_i}.$$

- Поскольку $\alpha L\bar{\beta}_i \geq 0$, имеем:

$$b_i^R = \begin{cases} 0, & \gamma_i > 0, \\ 1, & \gamma_i < 0. \end{cases}$$

JAWS - Just Another Watermarking System

- Шаблон P размерами $M \times M$, $P(m_1, m_2) \sim N(0, 1)$, формируется при помощи ключа $\mathbf{k}$.
- Для каждого кадра t генерируется шаблон ЦВЗ

$$W_t(m_1, m_2) = P(m_1, m_2) - shift(P, \boldsymbol{b_t}),$$

  - $\mathbf{b_t}$ – фрагмент встраиваемой последовательности $\mathbf{b}$, содержащий биты, встраиваемые в кадр t,
  - $\mathrm{shift}(\mathrm{P}, \mathbf{b_t})$ обозначает операцию циклического сдвига строк и столбцов P в соответствии с битами $\mathbf{b_t}$.
- Встраивание информации:

$$C^W(n_1, n_2, t) = C(n_1, n_2, t) + \alpha \cdot \beta(n_1, n_2, t)\mathrm{W_t}\left(\mathrm{n_1}(\mathrm{mod\ M}), \mathrm{n_2}(\mathrm{mod\ M})\right)$$

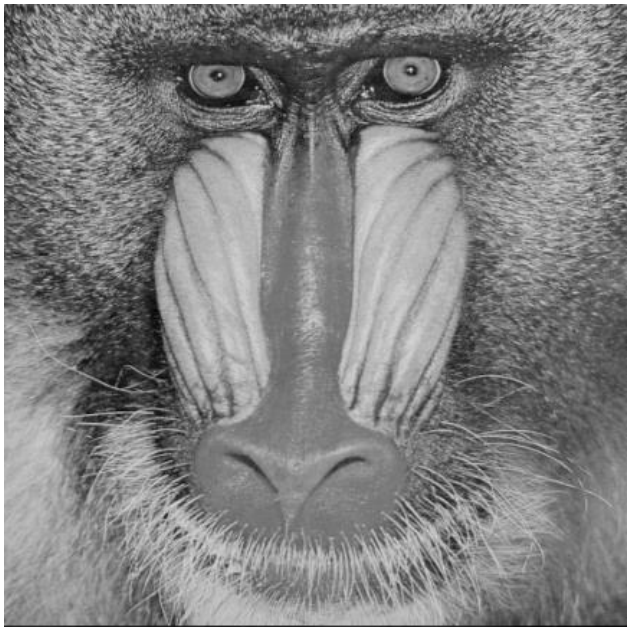
  - α – параметр глобального усиления встраиваемого сигнала,
  - $\beta(n_1, n_2, t)$ – маска адаптивного усиления встраиваемого сигнала,

JAWS: адаптивная маска

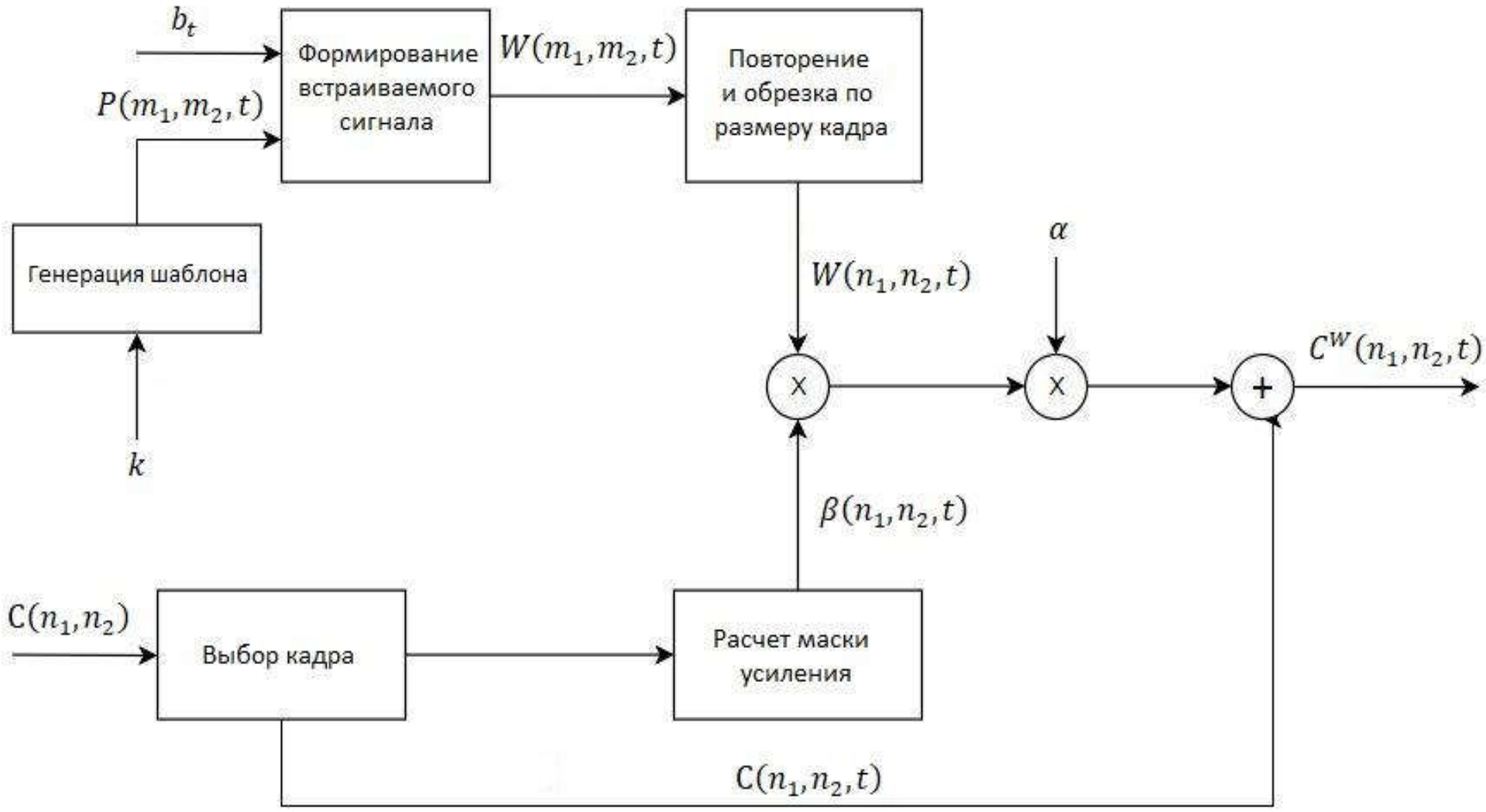
- $\beta(n_1, n_2, t)$ рассчитывается при помощи оператора Лапласа, то есть свёртки кадра $C(n_1, n_2, t)$ с маской вида

$$g(n_1, n_2) = \begin{pmatrix} 0 & 1 & 0 \\ 1 & -4 & 1 \\ 0 & 1 & 0 \end{pmatrix}$$

- с последующим взятием модуля.



JAWS: схема встраивания



JAWS: извлечение

- Оценка встроенного шумоподобного сигнала

$$\widetilde{W}_t(\mathrm{m}_1, \mathrm{m}_2) = \frac{1}{S} \sum_{i=0}^{\lfloor N_1/M \rfloor} \sum_{j=0}^{\lfloor N_2/M \rfloor} \widetilde{C^W}(i \cdot M + m_1, j \cdot M + m_2, t),$$

  - где $S = \lfloor N_1/M \rfloor \cdot \lfloor N_2/M \rfloor$ – количество блоков

- Рассчитывается взаимная корреляционная функция (ВКФ) $\widetilde{W}_t(m_1, m_2)$ и $P(m_1, m_2)$:

$$B = \mathcal{F}^{-1}\left(\mathcal{F}\left(\widetilde{W}_t\right) \cdot \left(\mathcal{F}(P)\right)^*\right)$$

- Другой способ - SPOMF-фильтрация (Symmetrical Phase Only Matched Filtering)

$$B = \mathcal{F}^{-1}\left(\phi\left(\mathcal{F}\left(\widetilde{W}_t\right)\right) \cdot \left(\phi\left(\mathcal{F}(P)\right)\right)^*\right),$$

  - где $\phi(x) = \frac{x}{|x|}$.

JAWS: извлечение

- Отыскиваются два пика:
  - положительный, координаты которого задают сдвиг шаблона P,
  - отрицательный, координаты которого задают сдвиг шаблона $\mathrm{shift}(P, \mathbf{b_t})$
  - вектор между двумя этими пиками кодирует $\mathbf{b_t}$.