3.2 Методы модификации компонент сигнала при встраивании информации

1. Аддитивное встраивание

- Обобщённая форма (в пространственной области)

$$C^W(n_1,n_2) = \alpha_1 \cdot C(n_1,n_2) + \alpha_2 \cdot \beta(n_1,n_2) \cdot W(n_1,n_2)$$

  - α_1, α_2 – постоянные множители
  - $\beta(n_1,n_2) \in [0;1]$ – адаптивная маска усиления. Она строится на основе модели человеческого зрения

- Наиболее распространённая форма

$$C^W(n_1,n_2) = C(n_1,n_2) + \alpha \cdot \beta(n_1,n_2) \cdot W(n_1,n_2)$$

- Встраивание в пространстве признаков

$$f^W(\boldsymbol{m}) = f(\boldsymbol{m}) + \alpha \cdot \beta(\boldsymbol{m}) \cdot W(\boldsymbol{m})$$

2. Мультипликативное встраивание

- Обобщённая форма (в пространственной области)

$$C^W(n_1,n_2) = \alpha_1 \cdot C(n_1,n_2) + \alpha_2 \cdot \beta(n_1,n_2) \cdot g\big(C(n_1,n_2)\big) \cdot W(n_1,n_2)$$

  - $g(x) \in \mathbb{R}$ – некоторая функция, применяемая к значениям яркости пикселей контейнера
  - $g(x) = x$ – самый распространённый случай
- Наиболее распространённая форма

$$C^W(n_1,n_2) = C(n_1,n_2)\big(1 + \alpha \cdot \beta(n_1,n_2) \cdot W(n_1,n_2)\big).$$

- Встраивание в пространстве признаков

$$f^W(\boldsymbol{m}) = f(\boldsymbol{m})\big(1 + \alpha \cdot \beta(\boldsymbol{m}) \cdot \Omega(\boldsymbol{m})\big)$$

3. Встраивание информации с расширением спектра

- Концепция встраивания информации в цифровые сигналы с расширением спектра состоит в распределении встраиваемой информации (ЦВЗ или секретного сообщения) внутри контейнера, имеющего гораздо больший размер, на основе функции, зависящей от секретного ключа.
- Простым примером расширения спектра является генерация псевдослучайного шаблона, при этом начальное значение генератора однозначно определяется парой «ЦВЗ – ключ»

E_BLIND/D_LC

- Встраивается один бит информации: $\mathbf{b} = b \in \{0,1\}$
- $W_r(n_1, n_2) \sim N(0,1)$, строится на основе ключа $\mathbf{k}$
- Модуляция исходного бита ЦВЗ $\mathbf{b}$ с расширением спектра (подготовка встраиваемого сигнала)

$$W_{mod}(n_1, n_2) = (-1)^{\boldsymbol{b}+1} = \begin{cases} W_r(n_1, n_2), & \mathbf{b} = 1, \\ -W_r(n_1, n_2), & \mathbf{b} = 0. \end{cases}$$

- Встраивание ЦВЗ (аддитивное)

$$C^W(n_1, n_2) = C(n_1, n_2) + \alpha \cdot W_{mod}(n_1, n_2),$$

E_BLIND/D_LC

- Детектирование ЦВЗ

$$\rho\left(\widetilde{C^W}, W_r\right) = \frac{1}{N_1 N_2} \sum_{n_1=0}^{N_1-1} \sum_{n_2=0}^{N_2-1} \widetilde{C^W}(n_1, n_2) \cdot W_r(n_1, n_2),$$

$$\boldsymbol{b}^{\boldsymbol{R}} = \begin{cases} 1, & \rho\left(\widetilde{C^W}, W_r\right) > \tau_{lc}, \\ 0, & \rho\left(\widetilde{C^W}, W_r\right) < -\tau_{lc}, \\ \text{нет ЦВЗ}, & \text{иначе.} \end{cases}$$

E_BLIND_MULTI/D_LC

- $\mathbf{b} = \left(b_0, b_1, \dots, b_{N_b-1}\right)$
- $\mathrm{M}(n_1, n_2) \in [0; N_b - 1]$ - «карта встраивания»
- Модуляция битов ЦВЗ

$$W_{mod}(n_1, n_2) = (-1)^{b_{M(n_1,n_2)}+1} = \begin{cases} W_r(n_1, n_2), & b_{M(n_1,n_2)} = 1, \\ -W_r(n_1, n_2), & b_{M(n_1,n_2)} = 1. \end{cases}$$

- Вспомогательные массивы $W_{r,k}$ $k = 0..N_b - 1$ для детектирования

$$W_{r,k}(n_1, n_2) = \begin{cases} W_r(n_1, n_2), & M(n_1, n_2) = k, \\ 0, & M(n_1, n_2) \neq k. \end{cases}$$

СВИ (Patchwork)

- Случайным образом выбирается подмножество S всех пикселей изображения
- S делится на два равных подмножества S_1 и S_2 согласно ключу $\mathbf{k}$
- Встраивание информации

$$\begin{cases} C^W(n_1, n_2) = C(n_1, n_2) + d, & C(n_1, n_2) \in S_1 \\ C^W(n_1, n_2) = C(n_1, n_2) \cdot d, & C(n_1, n_2) \in S_2 \end{cases}$$

- Детектирование

$$\rho = \frac{2}{\|S\|}\left(\sum_{C(n_1,n_2)\in S_1} C^W(n_1, n_2) - \sum_{C(n_1,n_2)\in S_2} C^W(n_1, n_2) \right)$$

СВИ (Patchwork)

- Детектирование

$$\rho = \frac{2}{\|S\|}\left(\sum_{C(n_1,n_2)\in S_1} C^W(n_1,n_2) - \sum_{C(n_1,n_2)\in S_2} C^W(n_1,n_2)\right)$$

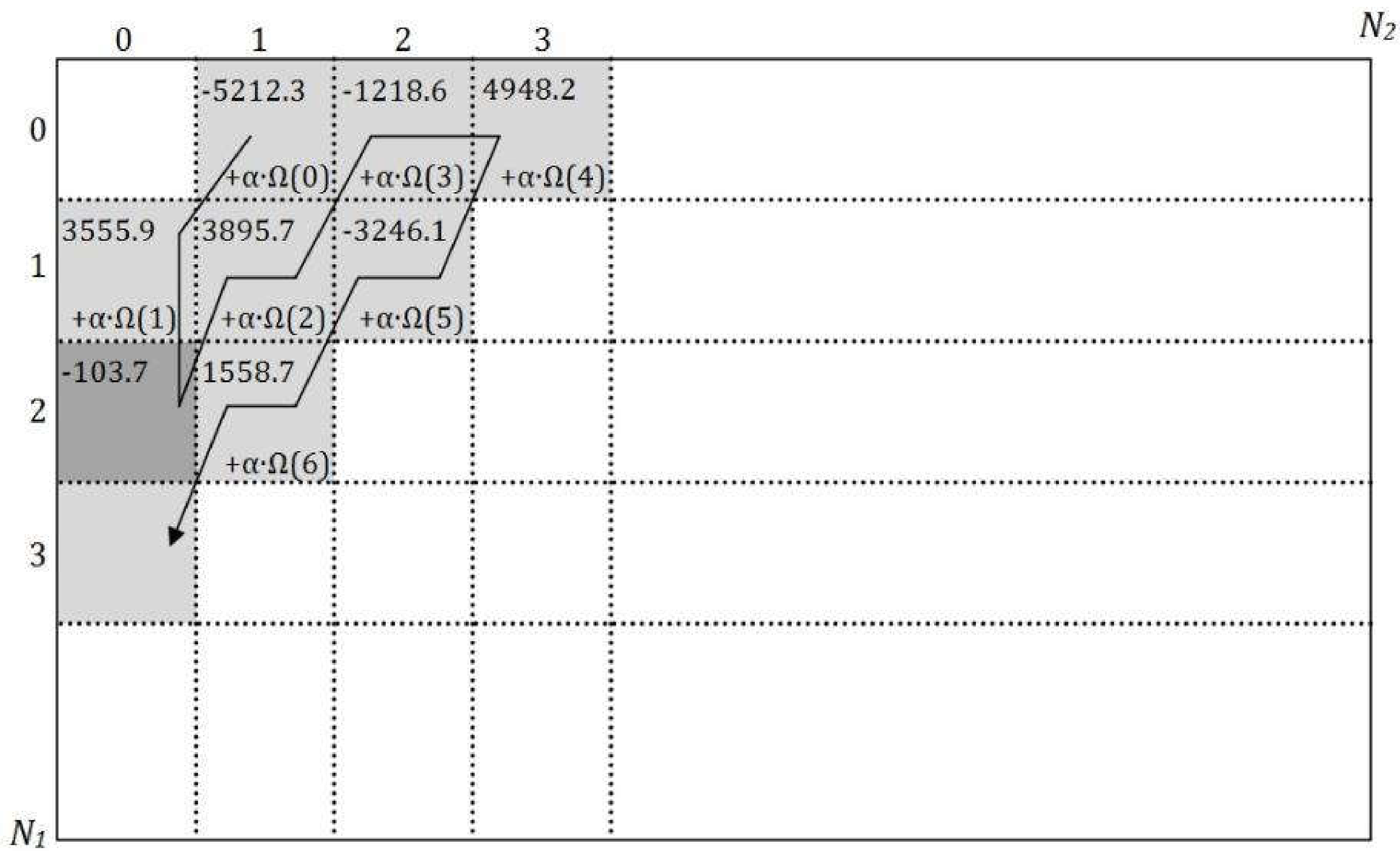
$$= \frac{2}{\|S\|}\left(\|S_1\|\cdot d + \|S_2\|\cdot d + \left[\sum_{C(n_1,n_2)\in S_1} C(n_1,n_2) - \sum_{C(n_1,n_2)\in S_2} C(n_1,n_2)\right]\right)$$

$$= 2d + \frac{2}{\|S\|}\left[\sum_{C(n_1,n_2)\in S_1} C(n_1,n_2) - \sum_{C(n_1,n_2)\in S_2} C(n_1,n_2)\right]$$

$$\xi = \begin{cases} 1, & \rho \ge d, \\ 0, & \rho < d, \end{cases}$$

СВИ (Cox et al.)

- $\mathbf{b}$ и $\mathbf{k} \to \Omega \in \mathbb{R}^1_{[N_\Omega]}, N_\Omega = 1000, \Omega(m) \sim N(0,1)$
- ДКП всего изображения
- Зигзагообразная развёртка



СВИ (Cox et al.)

- Встраивание информации (мультипликативное)

$$f^W(m) = f(m)\big(1 + \alpha \cdot \Omega(m)\big)$$

- Извлечение информации

$$\tilde{\Omega}(m) = \frac{\widetilde{f^W}(m) - f(m)}{\alpha \cdot f(m)}$$

$$\rho\big(\Omega, \tilde{\Omega}\big) = \frac{\sum_{m=0}^{N_\Omega - 1} \Omega(m)\tilde{\Omega}(m)}{\sqrt{\sum_{m=0}^{N_\Omega - 1} \Omega^2(m)} \cdot \sqrt{\sum_{m=0}^{N_\Omega - 1} \tilde{\Omega}^2(m)}}$$

$$\xi = \begin{cases} 1, & \rho(x, x^R) \geq T_\rho, \\ 0, & \rho(x, x^R) < T_\rho, \end{cases}$$

СВИ (Cox et al.)

- (+) является стойким к сжатию, поэлементным преобразованиям, процедурам обработки скользящим окном, а также многим другим видам обработки изображений
- (-) трудоёмкость операции вычисления двумерного ДКП всего изображения
- (-) необходимость использования контейнера на этапе извлечения информации

СВИ (Piva et al.)

- Для чего требуется исходное изображение в Cox et al.?
  - чтобы отыскать N_Ω наибольших ДКП-коэффициентов и проранжировать их по порядку
  - чтобы вычислить оценку $\tilde{\Omega}$ по формуле

$$\tilde{\Omega}(m) = \frac{\widetilde{f^W}(m) - f(m)}{\alpha \cdot f(m)}$$

- Изменения:
  - всегда отбираются одни и те же коэффициенты (среднечастотные), отсортированные в порядке зигзагообразной развёртки
  - оценку $\tilde{\Omega}$ рассчитываем по формуле

$$\tilde{\Omega}(m) = \widetilde{f^W}(m),$$

СВИ (Piva et al.)

- Меняется и формула встраивания:

$$f^W(m) = f(m) + \alpha \cdot |f(m)| \cdot \Omega(m).$$

- Оценка близости

$$\rho\left(\Omega, \tilde{\Omega}\right) = \sum_{m=0}^{N_\Omega - 1} \Omega(m)\tilde{\Omega}(m).$$

Обоснование:

$$\rho\left(\Omega, \tilde{\Omega}\right) = \sum_{m=0}^{N_\Omega - 1} \Omega(m)\widetilde{f^W}(m) \approx \sum_{m=0}^{N_\Omega - 1} \Omega(m) f(m) + \alpha \sum_{m=0}^{N_\Omega - 1} \Omega^2(m) \cdot |f(m)|.$$

- Для повышения точности детектирования ЦВЗ длина N_Ω увеличивается
  - для изображений размером 512×512 рекомендуется использовать коэффициенты ДКП со строки 180 до строки 250 – ~15000 значений

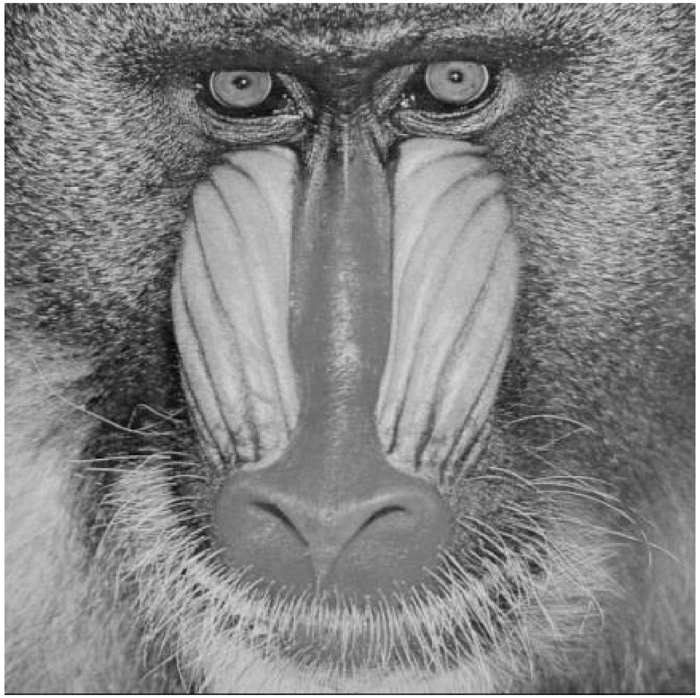
СВИ (Piva et al.)

- Дополнительное снижение визуальной различимости

$$C^W(n_1,n_2) = \mathcal{F}^{-1}\left(C^W_{DOT}(m_1,m_2)\right)\cdot\beta(n_1,n_2) + C(n_1,n_2)\cdot\left(1-\beta(n_1,n_2)\right)$$

$$\beta(n_1,n_2) = \frac{C_{MSE,9\times9}(n_1,n_2)}{\max\limits_{i.j} C_{MSE,9\times9}(i,j)}$$

$C_{MSE,9\times9}(n_1,n_2)$ – результат отыскания локального СКО в окне 9×9



4. Quantization Index Modulation

- Brian Chen, 2001
- Удобный инструмент для проектирования систем хрупких и полухрупких ЦВЗ
- Это не один алгоритм, а целое семейство методов
- Функция встраивания информации $\mathcal{E}$ представляется в виде семейства функций-квантователей, причём каждая из них незначительным образом изменяет яркости пикселей контейнера
- Основные параметры:
  - шаг переквантования $\Delta \in \mathbb{N}$
  - функция переквантования $Q(x, \Delta)$, где x – квантуемое значение:

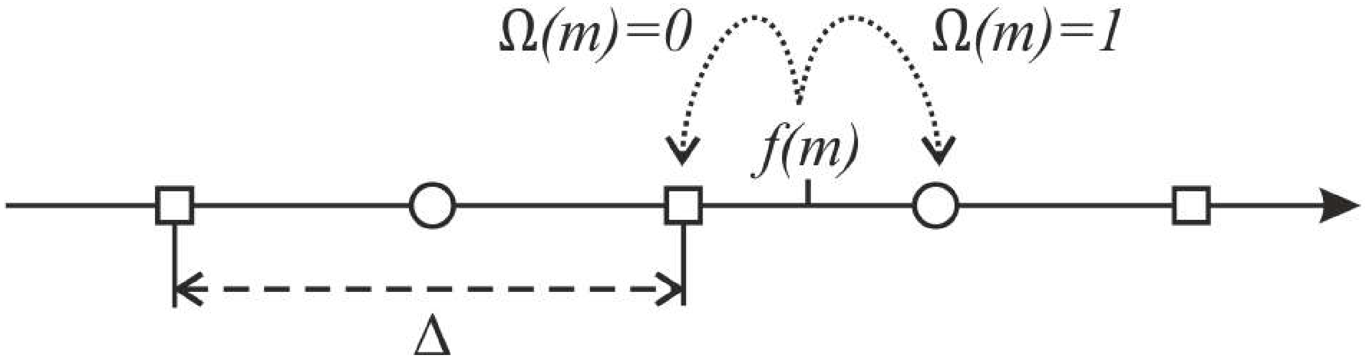
$$Q(x, \Delta) = \Delta \cdot \lfloor x/\Delta \rfloor$$

$$Q(x, \Delta) = \Delta \cdot round\left(\frac{x}{\Delta}\right) = \Delta \cdot \left\lfloor \frac{x + 0.5}{\Delta} \right\rfloor.$$

Simple-QIM

- Встраивание информации

$$C^W(n_1,n_2) = \mathcal{E}_{SQIM}(C,W,\Delta,\vartheta)$$
$$= Q(C(n_1,n_2),\Delta) + \Delta/2 \cdot W(n_1,n_2) + \vartheta(n_1,n_2)$$



- Универсальный способ извлечения информации

$$\widetilde{C_0}(n_1,n_2) = \mathcal{E}_{SQIM}\left(\widetilde{C^W},0,\Delta,\vartheta\right) = Q\left(\widetilde{C^W}(n_1,n_2),\Delta\right) + \vartheta(n_1,n_2),$$
$$\widetilde{C_1}(n_1,n_2) = \mathcal{E}_{SQIM}\left(\widetilde{C^W},1,\Delta,\vartheta\right) = Q\left(\widetilde{C^W}(n_1,n_2),\Delta\right) + \Delta/2 + \vartheta(n_1,n_2)$$
$$\widetilde{W}(n_1,n_2) = arg \min_{p\in\{0,1\}} \left|\widetilde{C^W}(n_1,n_2) - \widetilde{C_p}(n_1,n_2)\right|$$

DM-QIM

- Расшифровка: “Dither Modulation – QIM”
- Два дополнительных параметра - массивы подмешиваемых значений (dither vectors), используемых при встраивании битов “0” и “1” – d_0 и d_1
- $d_0(n_1, n_2), \quad d_1(n_1, n_2) \in [-\Delta/2\,; \Delta/2 - 1].$
- d_0 генерируется на основе ключа (равномерное распределение)
- $d_1(n_1, n_2) = d_0(n_1, n_2) - sign\big(d_0(n_1, n_2)\big) \cdot \Delta/2$

DM-QIM

- Встраивание информации:

$$C^W(n_1,n_2) = \mathcal{E}_{DM-QIM}(C,W,\Delta,d_0)$$
$$= Q\big(C(n_1,n_2) + d_{W(n_1,n_2)}(n_1,n_2),\Delta\big) - d_{W(n_1,n_2)}(n_1,n_2)$$

- Извлечение информации:

$$\widetilde{C_0}(n_1,n_2) = \mathcal{E}_{DM-QIM}\big(\widetilde{C^W},0,\Delta,d_0\big)$$
$$= Q(C(n_1,n_2) + d_0(n_1,n_2),\Delta) - d_0(n_1,n_2)$$

$$\widetilde{C_1}(n_1,n_2) = \mathcal{E}_{DM-QIM}\big(\widetilde{C^W},1,\Delta,d_0\big)$$
$$= Q(C(n_1,n_2) + d_1(n_1,n_2),\Delta) - d_1(n_1,n_2)$$

$$\widetilde{W}(n_1,n_2) = arg \min_{p\in\{0,1\}}\left|\widetilde{C^W}(n_1,n_2) - \widetilde{C_p}(n_1,n_2)\right|$$

DC-QIM

- “Distortion Compensated QIM” – метод QIM-встраивания с компенсацией искажений
- $0 < \alpha \leq 1$ – коэффициент, масштабирующий шаг квантования Δ
- Обозначим C_α^W результат работы какой-либо версии QIM-встраивания (Simple-QIM, DM-QIM и пр.) с изменённым шагом:
$$C_\alpha^W(n_1, n_2) = \mathcal{E}(C, W, \Delta/\alpha, \dots)$$
- Встраивание DC-QIM
$$C^W(n_1, n_2) = \mathcal{E}_{DC-QIM}(C, W, \Delta/\alpha, \dots)$$
$$= C_\alpha^W(n_1, n_2) + (1 - \alpha) \cdot \left(C(n_1, n_2) - C_\alpha^W(n_1, n_2)\right)$$

Понятие информированного встраивания

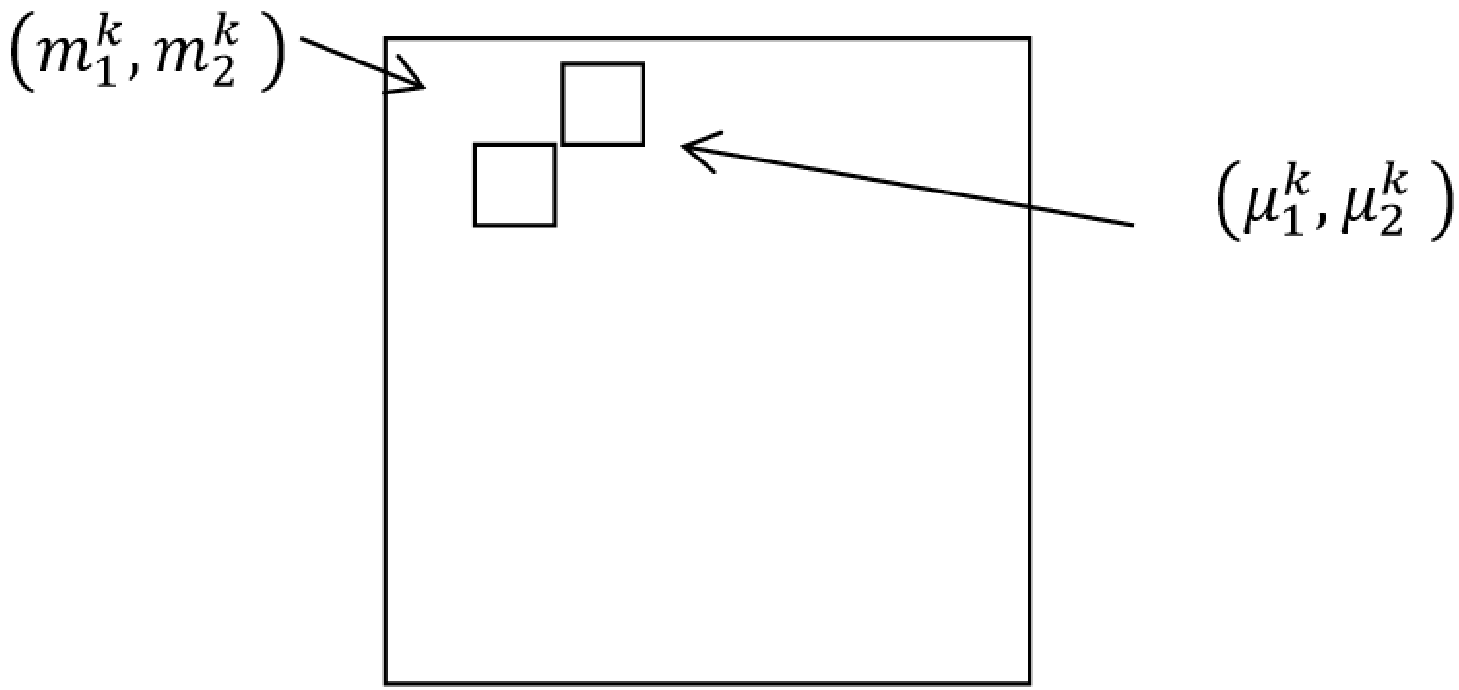
- Информированное встраивание – свойство СВИ, которое характеризует принцип (концепцию, порядок) формирования пары алгоритмов встраивания-извлечения информации
- В информированном встраивании предполагается, что заранее «дан» детектор или декодер информации, представляющий собой простую функцию, например, основанную на:
  - чтении данных в заданных ключом позициях
  - корреляторе с использованием шаблона ЦВЗ
  - …
- Первична функция извлечения, под неё формируется функция встраивания

СВИ (Zhao & Koch)

- Данное описание – упрощённая версия.
- Система очень старая (1995 год) и сейчас (почти?) не используется. Тем не менее, это хорошая классическая иллюстрация концепции информированного встраивания
- Блоки 8x8, ДКП. Результат – $f_{ij}(m_1, m_2)$
- Устанавливается соответствие $k \leftrightarrow (i, j)$, например:
$$k = \lfloor N_2/8 \rfloor \cdot i + j$$
- На основе ключа выбираются два коэффициента $\left(m_1^k, m_2^k\right)$ и $\left(\mu_1^k, \mu_2^k\right)$
- В каждый блок встраиваем 1 бит информации b_k.

СВИ (Zhao & Koch)

- Коэффициенты берутся среди низкочастотных:



- Правило извлечения

$$b_k^R = \begin{cases} 1, & \left|\widetilde{f_{ij}^W}(m_1^k, m_2^k)\right| < \left|\widetilde{f_{ij}^W}(\mu_1^k, \mu_2^k)\right|, \\ 0, & \text{иначе.} \end{cases}$$

СВИ (Zhao & Koch)

- Индуцированный метод встраивания

$$b_k = \begin{cases} 1 \Longrightarrow \left|f_{ij}^W\left(m_1^k, m_2^k\right)\right| + \varepsilon \le \left|f_{ij}^W\left(\mu_1^k, \mu_2^k\right)\right| \\ 0 \Longrightarrow \left|f_{ij}^W\left(m_1^k, m_2^k\right)\right| \ge \left|f_{ij}^W\left(\mu_1^k, \mu_2^k\right)\right| + \varepsilon \end{cases}$$

- $\varepsilon > 0$ – добавка, повышающая стойкость ЦВЗ
- Поясним на примере $b_k = 1$:
  - Если $\left|f_{ij}\left(m_1^k, m_2^k\right)\right| + \varepsilon \le \left|f_{ij}\left(\mu_1^k, \mu_2^k\right)\right|$, то $f_{ij}^W = f_{ij}$ в блоке (i, j)
  - Иначе:

$$\delta = \left|f_{ij}\left(m_1^k, m_2^k\right)\right| - \left|f_{ij}\left(\mu_1^k, \mu_2^k\right)\right|,$$
$$f_{ij}^W\left(m_1^k, m_2^k\right) = f_{ij}\left(m_1^k, m_2^k\right) - \delta/2,$$
$$f_{ij}^W\left(\mu_1^k, \mu_2^k\right) = f_{ij}^W\left(\mu_1^k, \mu_2^k\right) + \delta/2.$$