

# Minimalizace vlivu vložené informace ve steganografii pomocí řídkých kódů

Tomáš Filler

26. června 2007

# Minimalizace vlivu vložené informace ve steganografii

$\mathbf{x} \in \{0, 1\}^n$  - nosič informace

$\mathbf{m} \in \{0, 1\}^m$  - zpráva

$$P(\mathbf{x}_i = 0) = P(\mathbf{x}_i = 1) = \frac{1}{2}$$

$\mathbf{y} \in \{0, 1\}^n$  - cílové slovo

$f : \{0, 1\}^n \times \{0, 1\}^m \rightarrow \{0, 1\}^n$

$g : \{0, 1\}^n \rightarrow \{0, 1\}^m$

ukrývání zpráv  $\mathbf{y} = f(\mathbf{x}, \mathbf{m})$

extrakce zpráv  $\mathbf{m} = g(\mathbf{y})$

$$\mathbf{y} = \arg \min_{g(\mathbf{y})=\mathbf{m}} \|\mathbf{x} - \mathbf{y}\|_H$$

## Syndromová metoda

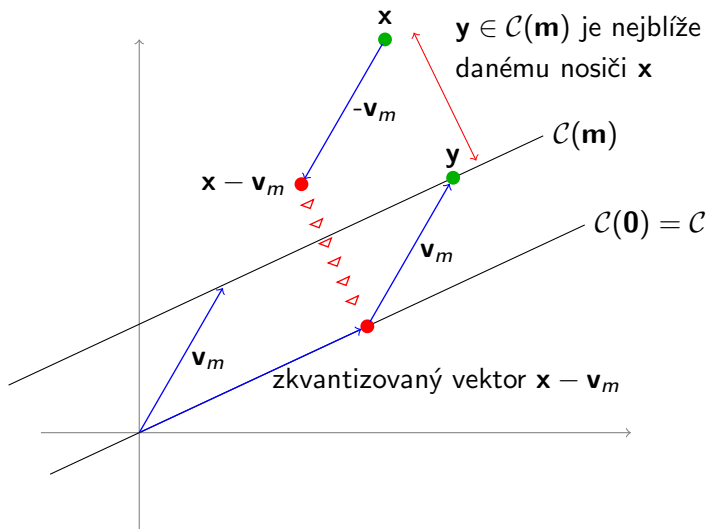
$\mathcal{C}$  - binární lineární  $(n, k)$  kód, kde  $k = n - m$

$\mathbf{G}$  - generující matice kódu  $\mathcal{C}$

$\mathbf{H}$  - kontrolní matice kódu  $\mathcal{C}$

$$\mathbf{m} = g(\mathbf{y}) = \mathbf{H}\mathbf{y}$$

# Geometrická interpretace syndromové metody

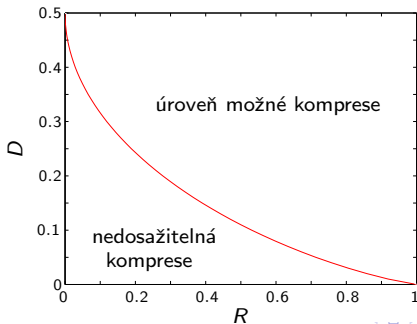


# Binární kvantizace, ztrátová komprese

$$\mathbf{y} = \arg \min_{\mathbf{c} \in \mathcal{C}} \|\mathbf{x} - \mathbf{c}\|_H$$

- NP-úplný problém
- Relativní zkreslení (distortion)  $D = \frac{1}{n} \mathbb{E} [\|\mathbf{x} - \mathbf{y}\|_H]$
- Pro  $R = \frac{k}{n}$  platí následující mez (rate-distortion bound)

$$R = 1 - H(D)$$



# Kódy s řídkou generující maticí (LDGM)

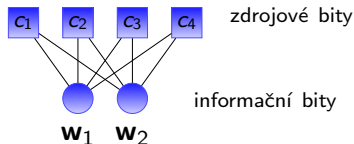
Low Density Generator Matrix codes

## Grafická reprezentace kódu

$\mathbf{G} \in \{0, 1\}^{n \times k} \Rightarrow$  faktorgraf  $\mathcal{G}$

$c_i$  a  $w_j$  jsou ve hraně  $\Leftrightarrow \mathbf{G}_{i,j} = 1$

(2,4) LDGM kód

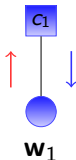


## Způsob zadávání kódů

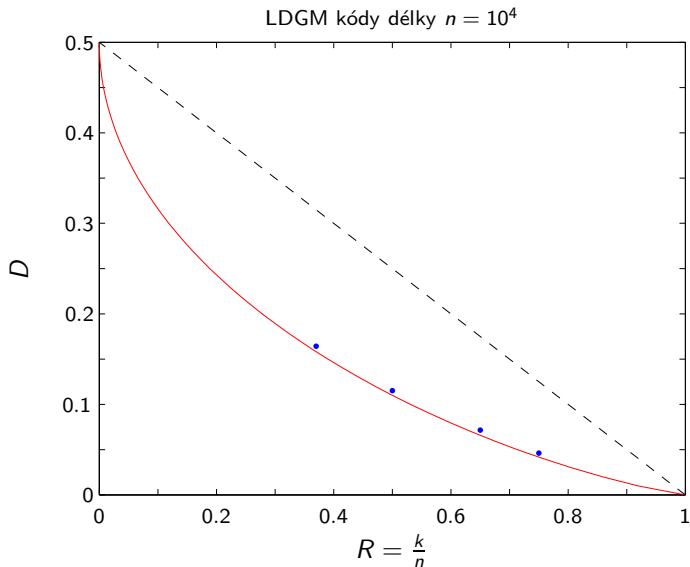
Faktorgraf LDGM kódu délky  $n$  a dimenze  $k$  je náhodný graf na  $n$  zdrojových a  $k$  informačních bitech zachovávající předepsané rozdělení na stupně vrcholů.

# Algoritmus “Bias Propagation” (BiP)

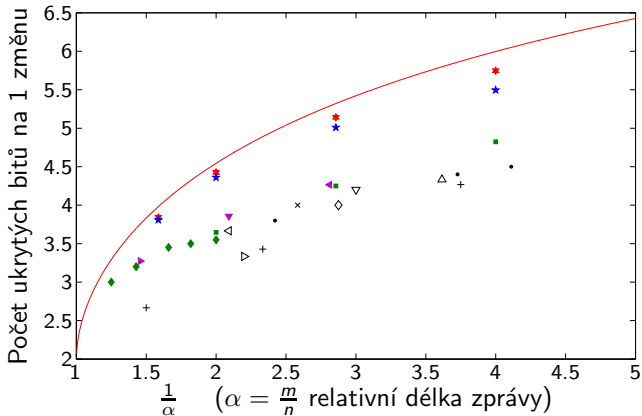
- Iterační algoritmus využívající hran v grafu (message-passing)
- Pro dané  $\mathbf{x} \in \{0, 1\}^n$  BiP hledá odhad nejbližšího  $\mathbf{c} \in \mathcal{C}$
- Složitost algoritmu  $n \ln n$ , kde  $n$  je délka kódu



# Výsledky použití LDGM kódů pro binární kvantizaci



# Výsledky použití LDGM kódů ve steganografii



LDGM kódy

★ délka  $n = 10^5$

★ délka  $n = 10^4$

- |                  |          |                            |                   |
|------------------|----------|----------------------------|-------------------|
| — teoretická mez | × BDS(5) | • Sum(9)(10)               | ▶ Neprim. BCH kód |
| + Hammingův kód  | △ BDS(6) | ■ Náhodné kódy (kodim. 20) | ◀ Neprim. BCH kód |
| ◁ Golayův kód    | ▽ BDS(7) | ◆ Náhodné kódy (dim. 14)   |                   |
| ◇ BDS(3)         | ▷ BDS(8) | ▼ Neprimitivní Golayův kód |                   |

Zdá se vám na tomto obrázku něco podivného?



Hledali byste v minulém obrázku tuto ukrytou zprávu?

