

# Psaní na mokrý papír

Andrew Kozlik

KA MFF UK

# Motivace

- ▶ **Problém:** Vkládání do některých prvků nosiče má vysoký dopad na detekovatelnost.
- ▶ PNG/GIF: Oblasti s nízkou texturou.
- ▶ JPEG: Nulové AC koeficienty.
- ▶ **Řešení:** Při vkládání i extrakci budeme tyto citlivé prvky přeskakovat.
- ▶ **Nový problém:** Proces vkládání může mít za následek, že
  - ▶ textura oblasti klesne pod prahovou hodnotu, nebo
  - ▶ nenulový AC koeficient se vynuluje.Příjemce prvky přeskočí a vložená informace je tak ztracena.
- ▶ **Řešení:** Dojde-li ke ztrátě, vložíme informaci znovu.
- ▶ U JPEGu vede ke smrštění kapacity o cca 25 %.

# Přirovnání k psaní na mokrý papír

- ▶ Máme obrázek na papíře.
- ▶ Některé pixely jsou suché, jiné mokré.
- ▶ Suché smíme upravovat, mokré nikoliv.
- ▶ Upravený obrázek odešleme, ale ten cestou uschne.
- ▶ Příjemce nepozná, kam jsme vložili zprávu, protože neví, které pixely byly suché a které nikoliv.

## Věta (o mokrém nosiči)

*Pro každé  $\varepsilon > 0$ ,  $\delta > 0$  a  $\sigma \in [0, 1]$  existuje  $n \in \mathbb{N}$  a stegosystém takový, že do nosiče velikosti  $n$  symbolů, z nichž  $\sigma n$  je suchých, lze s pravděpodobností alespoň  $1 - \delta$  vložit informaci velikosti  $(\sigma - \varepsilon)n$  symbolů.*

## Důkaz.

- ▶ Nechť  $\Sigma$  je množina symbolů a  $q := |\Sigma|$ .  
(Typicky  $\Sigma = \mathbb{F}_2$  nebo  $\Sigma = \mathbb{F}_3$ .)
- ▶ Nechť  $Z$  je množina zpráv velikosti  $|Z| = q^{(\sigma - \varepsilon)n}$ .
- ▶ Konstrukce stegosystému:
  - ▶ Vytvoříme kódovou knihu  $\mathcal{B} = \{\mathcal{P}_z : z \in Z\}$ .
  - ▶ Stránky knihy  $\mathcal{P}_z$  jsou indexovány množinou zpráv  $Z$ .
  - ▶ Slova z množiny  $\Sigma^n$  rozmístíme do knihy náhodně tak, aby na každé stránce bylo  $q^{(1 - \sigma + \varepsilon)n}$  slov.
  - ▶ Čili  $\Sigma^n = \bigcup_{z \in Z} \mathcal{P}_z$ .

## Důkaz (pokračování).

- ▶ Příjemce a odesílatel kódovou knihu sdílejí.
- ▶ **Vkládání:**
  - ▶ Vstup: Nosič  $x \in \Sigma^n$  s  $n - \sigma n$  mokřými prvky a zpráva  $z \in Z$ .
  - ▶ Pokusíme se na stránce  $\mathcal{P}_z$  najít  $n$ -tici, která se na mokřích pozicích shoduje s nosičem.
  - ▶ Podaří-li se, je nalezená  $n$ -tice stegoobjektem a mokré pozice zůstávají nezměněny.
- ▶ **Extrakce:**
  - ▶ Vstup: Stegoobjekt  $y \in \Sigma^n$ .
  - ▶ Vyhledáme  $y$  v knize. Podíváme se na index stránky, na které jsme  $y$  našli a zpráva = index.

## Důkaz (pokračování).

- ▶ Podaří se vkládacímu algoritmu najít na stránce  $\mathcal{P}_z$   $n$ -tici, která má na  $n - \sigma n$  určených pozicích určené hodnoty?
- ▶ V celé knize je takových  $n$ -tic dohromady  $q^{\sigma n}$ .
- ▶ Jaká je pravděpodobnost, že žádná z nich není v  $\mathcal{P}_z$ ?
- ▶  $\mathcal{P}_z$  vznikla náhodným výběrem  $q^{n-\sigma n+\varepsilon n}$  prvků z  $\Sigma^n$ .
- ▶ Pravděpodobnost selhání  $p$  je méně než

$$p < \left( \frac{q^n - q^{\sigma n}}{q^n} \right)^{q^{n-\sigma n+\varepsilon n}} = \left( \underbrace{\left( 1 + \frac{-1}{q^{n(1-\sigma)}} \right)^{q^{n(1-\sigma)}}}_{\text{jde k } e^{-1} \approx 0,37 \text{ pro } n \rightarrow \infty} \right)^{q^{\varepsilon n}}.$$

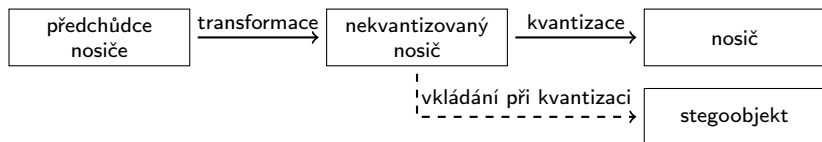
- ▶ Pro dostatečně velká  $n$  je označený výraz menší než  $\frac{1}{2}$ .
- ▶ Od jistého  $n$  tedy platí  $p < \left(\frac{1}{2}\right)^{q^{\varepsilon n}} \rightarrow 0$ .



# Praktické řešení

- ▶ Algoritmy z důkazu označme:
  - ▶  $y = \text{Emb}_{\mathcal{B}}(x, S, z)$ .
  - ▶  $z = \text{Ext}_{\mathcal{B}}(y)$ .
  - ▶  $S \subseteq \{1, \dots, n\}$  je množina indexů suchých složek nosiče.
- ▶ Pomocí samoopravného kódu  $\mathcal{C}$ :
  - ▶  $\Sigma = \mathbb{F}_q$ .
  - ▶  $\mathcal{B} = \mathbb{F}_q^n / \mathcal{C}$ .
  - ▶  $\mathcal{P}_z = \mathcal{C}(z)$ .
  - ▶  $\text{Ext}_{\mathbb{F}_q^n / \mathcal{C}} = \mathbf{H}y$ , kde  $\mathbf{H}$  je paritní matice kódu  $\mathcal{C}$ .
- ▶ Lze tedy využít maticové vkládání. Cílem však není minimalizovat počet změn, ale zajistit, aby k nim docházelo jen na určených pozicích.

# Vkládání při kvantizaci



- ▶ Kvantizace: Zaokrouhlení na nejbližší povolenou hodnotu.
- ▶ Množina povolených hodnot může být např.  $\{0, 1, \dots, 255\}$  nebo  $\{\dots, -3, 0, 3, 6, \dots\}$ .
- ▶ Příklady transformací:
  - ▶ Snížení hloubky barev rastrového obrázku.
  - ▶ Zmenšení rozměrů rastrového obrázku a intrpolace.
  - ▶ Blok  $8 \times 8$  hodnot jasové složky obrázku na blok  $8 \times 8$  DCT koeficientů.



## Příklady kvantizace vs. vkládání při kvantizaci

- ▶ Množina povolených hodnot je  $\mathbb{Z}$ .
- ▶ Nezaokrouhlený prvek:  $\tilde{x}_i = 14,9$ .
- ▶ Kvantizace: Zaokrouhlíme na 15. Distorze je  $0,1^2$ .
- ▶ Vkládání při kvantizaci:
  - ▶ Vložení bitu 0: Zaokrouhlíme na 14. Distorze je  $0,9^2$ .
  - ▶ Vložení bitu 1: Zaokrouhlíme na 15. Distorze je  $0,1^2$ .
  - ▶ Průměrná distorze při vkládání  $(0,9^2 + 0,1^2)/2 = 0,41$ .
- ▶ Vkládáním při kvantizaci se distorze v průměru zvýší o  $\rho_i = 0,41 - 0,01 = 0,4$ .
- ▶ Jiný příklad:  $\tilde{x}_i = 14,5$ .
- ▶ Vkládáním se distorze nezvýší. Říkáme, že  $\tilde{x}_i$  je *nestranný*.

# Využití psaní na mokrý papír

- ▶ Ke každému  $\tilde{x}_i$  přiřadíme  $\rho_i$ :

$$\rho_i = (\text{průměrná distorze při vkládání}) - (\text{distorze při zaokrouhlení})$$

- ▶ Je-li množina povolených hodnot  $\mathbb{Z}$ , pak

$$\begin{aligned}\delta_i &= \text{dist}(\tilde{x}_i, \mathbb{Z}) = |[\tilde{x}_i] - x_i| \\ \rho_i &= \frac{\delta_i^2 + (1 - \delta_i)^2}{2} - \delta_i = \frac{1}{2} - \delta_i.\end{aligned}$$

- ▶ Množinu  $S$  volíme tak, aby součet  $\sum_{i \in S} \rho_i$  byl minimální.
- ▶ Vkládání provádíme usměrněním zaokrouhlení.

## Vkládání při dvojité ztrátové kompresi

- ▶ **Problém:** Chceme nestranné prvky, ale ty jsou vzácné.
- ▶ **Řešení:** Vytvoříme je přirozenou cestou.
- ▶ Předchůdce nosiče: JPEG s faktorem kvality  $f_1$ .
- ▶ Transformace: Rekomprimace obrázku na nižší kvalitu  $f_2$ .
- ▶ Za příznivých okolností vznikne v nekvantizovaném nosiči hodně nestranných DCT koeficientů.
- ▶ Pro  $f_1 = 85$  a  $f_2 = 70$  je jich v našem cvičném obrázku 14 % z celkového počtu všech koeficientů.

## Příklad kvantizačních matic

$$Q^{(85)} = \begin{pmatrix} 5 & 3 & \boxed{3} & 5 & 7 & 12 & 15 & 18 \\ 4 & 4 & 4 & 6 & 8 & 17 & 18 & 17 \\ 4 & 4 & 5 & 7 & 12 & 17 & 21 & 17 \\ 4 & 5 & 7 & 9 & 15 & 26 & 24 & 19 \\ 5 & 7 & 11 & 17 & 20 & 33 & 31 & 23 \\ 7 & 11 & 17 & 19 & 24 & 31 & 34 & 28 \\ 15 & 19 & 23 & 26 & 31 & 36 & 36 & 30 \\ 22 & 28 & 29 & 29 & 34 & 30 & 31 & 30 \end{pmatrix}, \quad Q^{(70)} = \begin{pmatrix} 10 & 7 & \boxed{6} & 10 & 14 & 24 & 31 & 37 \\ 7 & 7 & 8 & 11 & 16 & 35 & 36 & 33 \\ 8 & 8 & 10 & 14 & 24 & 34 & 41 & 34 \\ 8 & 10 & 13 & 17 & 31 & 52 & 48 & 37 \\ 11 & 13 & 22 & 34 & 41 & 65 & 62 & 46 \\ 14 & 21 & 33 & 38 & 49 & 62 & 68 & 55 \\ 29 & 38 & 47 & 52 & 62 & 73 & 72 & 61 \\ 43 & 55 & 57 & 59 & 67 & 60 & 62 & 59 \end{pmatrix}$$

- ▶ DCT koeficienty na pozici (1,3) v předchůdci nosiče jsou zaokrouhlovány na násobek 3.
- ▶ Při snížení kvality se zaokrouhlují na násobek 6.
- ▶ Téměř polovina bloků bude mít na této pozici nestranný DCT koeficient.
- ▶ Na pozicích s větším kvantizačním koeficientem bude nestranných výrazně méně než polovina, např. 5 %.  
(V předchůdci nosiče je totiž většina zaokrouhlena na 0.)

# Dvojitá ztrátová komprese

- ▶ Nejlepších výsledků se dosahuje, když se berou nestranné DCT koeficienty z bloků s vysokou neuniformitou.
- ▶ Neuniformitu můžeme například měřit jako součet čtverců DCT koeficientů v bloku (energie bloku).
- ▶ Shrnutí:
  - ▶ Máme zprávu délky  $m$ , potřebujeme počet suchých  $s > m$ .
  - ▶ Postupně nabíráme nestranné koeficienty do  $S$ , dokud jich nemáme dost.
  - ▶ Přednostně vybíráme koeficienty z nejvíce neuniformních bloků.

## Dvouúrovňové $\pm 1$ vkládání

Jednoduché  $\pm 1$  vkládání zprávy  $\mathbf{z} \in \{0, 1\}^m$  do nosiče  $\mathbf{x} \in \mathbb{Z}^n$ :

- ▶ Jestliže  $\text{LSB}(x_i) = z_i$ , pak  $y_i := x_i$ .
- ▶ Jestliže  $\text{LSB}(x_i) \neq z_i$ , pak  $y_i := x_i + a$ , kde  $a \in_{\mathcal{R}} \{-1, 1\}$ .
- ▶ Obrana proti kvantitativním útokům na LSB embedding.

Rozhodnutí přičíst anebo odečíst 1 nám dává plnou kontrolu nad hodnotou druhého nejnižšího bitu:

Poslední dvě cifry binárního rozvoje				
$x_i$	$(\dots 00)_2$	$(\dots 01)_2$	$(\dots 10)_2$	$(\dots 11)_2$
$x_i + 1$	$(\dots 01)_2$	$(\dots 10)_2$	$(\dots 11)_2$	$(\dots 00)_2$
$x_i - 1$	$(\dots 11)_2$	$(\dots 00)_2$	$(\dots 01)_2$	$(\dots 10)_2$

# Dvouúrovňové $\pm 1$ vkládání

Značení:

- ▶  $\mathbf{H}$  je paritní matice  $[n, n - m_1]_2$  kódu  $\mathcal{C}$  s průměrnou vzdáleností  $r_a$ , relativní kapacitou  $\alpha$  a efektivitou  $e$ .
- ▶  $\mathcal{B}$  je kódová kniha, která umožňuje vkládat  $m_2$  bitů do nosiče délky  $n$  bitů, z nichž  $r_a$  je suchých.
- ▶  $\mathbf{x}'$  a  $\mathbf{y}'$  vektor nejnižších bitů nosiče a stegoobjektu.
- ▶  $\mathbf{x}''$  a  $\mathbf{y}''$  vektor druhých nejnižších bitů nosiče a stegoobjektu.
- ▶ Zpráva má dvě části  $\mathbf{z}' \in \mathbb{F}_2^{m_1}$  a  $\mathbf{z}'' \in \mathbb{F}_2^{m_2}$ .

Extrakce:

$$\mathbf{z}' = \text{Ext}_{\mathbf{H}}(\mathbf{y}') \quad \text{a} \quad \mathbf{z}'' = \text{Ext}_{\mathcal{B}}(\mathbf{y}'').$$

## Dvouúrovňové $\pm 1$ vkládání

Vkládání:

- ▶ První zpráva bude vložena maticovým vkládáním

$$\mathbf{y}' = \text{Emb}_H(\mathbf{x}', \mathbf{z}').$$

- ▶ Na pozicích, kde dochází ke změnám, jsme schopni ovlivnit druhý nejnižší bit. Tyto označíme jako suché

$$\mathcal{S} = \{i \mid x'_i \neq y'_i\}; \quad E[|\mathcal{S}|] = r_a.$$

- ▶ Druhá zpráva bude vložena metodou psaní na mokré papír

$$\mathbf{y}'' = \text{Emb}_B(\mathbf{x}'', \mathcal{S}, \mathbf{z}'').$$

- ▶ Stegoobjekt  $\mathbf{y}$  se vytvoří z nosiče  $\mathbf{x}$  změnami  $+1$  nebo  $-1$  tak, aby  $\mathbf{y}'$  byly nejnižší bity a  $\mathbf{y}''$  druhé nejnižší bity stegoobjektu.



# Dvouúrovňové $\pm 1$ vkládání

Relativní kapacita a efektivita:

- ▶ Efektivita kódu  $\mathcal{C}$  je  $e = m_1/r_a$ , čili  $r_a = m_1/e$ .
- ▶ Podle věty o mokrému nosiči je  $m_2 \approx |\mathcal{S}|$  a víme, že  $|\mathcal{S}| \approx r_a$ .
- ▶ Relativní kapacita a efektivita dvouúrovňového  $\pm 1$  vkládání je tedy

$$\alpha_{\pm 1} = \frac{m_1 + m_2}{n} \approx \frac{m_1 + m_1/e}{n} = \alpha + \frac{\alpha}{e},$$
$$e_{\pm 1} = \frac{m_1 + m_2}{r_a} \approx \frac{m_1 + m_1/e}{m_1/e} = e + 1.$$

- ▶ Zároveň si můžeme všimnout, že

$$\frac{\alpha}{e} = \frac{\frac{m_1}{n}}{\frac{m_1}{r_a}} = \frac{r_a}{n} = \frac{\frac{m_1+m_2}{n}}{\frac{m_1+m_2}{r_a}} = \frac{\alpha_{\pm 1}}{e_{\pm 1}}.$$

# Dvouúrovňové $\pm 1$ vkládání

## Tvrzení

*Nechť  $C$  je binární kód, jehož efektivita dosahuje horní meze na spodní efektivitu binárních kódů. Potom dvouúrovňovým  $\pm 1$  vkládáním s kódem  $C$  lze dosáhnout efektivity libovolně blízké horní mezi na spodní efektivitu ternárních kódů, za předpokladu, že kód  $C$  je dostatečně dlouhý.*

# Dvouúrovňové $\pm 1$ vkládání

## Důkaz.

- ▶ Připomeňme, že

$$H_q(x) := -x \log_q x - (1-x) \log_q(1-x) + x \log_q(q-1).$$

- ▶ Dle předpokladu je  $e = \alpha / H_2^{-1}(\alpha)$ , čili  $\alpha = H_2(\alpha/e)$ .
- ▶ Dosadíme a upravíme

$$\begin{aligned} \alpha_{\pm 1} &\approx \alpha + \frac{\alpha}{e} = H_2\left(\frac{\alpha}{e}\right) + \frac{\alpha}{e} \\ &= (\log_2 3) H_3\left(\frac{\alpha}{e}\right) = (\log_2 3) H_3\left(\frac{\alpha_{\pm 1}}{e_{\pm 1}}\right). \end{aligned}$$

- ▶ Vyjádříme

$$e_{\pm 1} \approx \frac{\alpha_{\pm 1}}{H_3^{-1}(\alpha_{\pm 1} / \log_2 3)}.$$

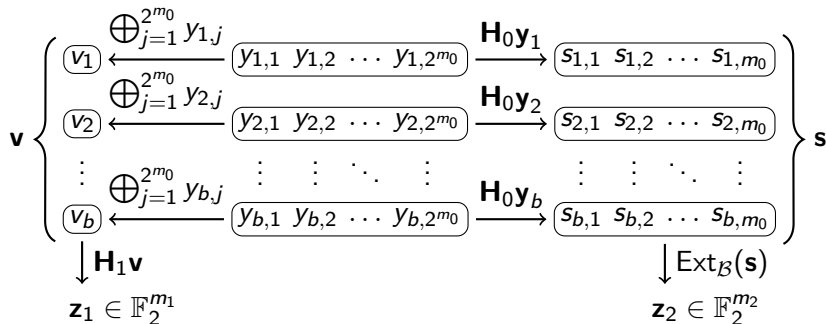


# Stegosystém ZZW

Značení:

- ▶  $\mathbf{H}_0$  vzniká přidáním nulového sloupce k paritní matici Hammingova kódu délky  $2^{m_0} - 1$ .
- ▶  $\mathbf{H}_1$  je paritní matice nějakého  $[b, b - m_1]_2$  kódu  $\mathcal{C}$  s průměrnou vzdáleností od kódu  $r_a$ .
- ▶  $\mathcal{B}$  je kódová kniha, která umožňuje vkládat  $m_2$  bitů do nosiče délky  $bm_0$  bitů, z nichž  $r_a m_0$  je suchých.

Extrakce:



# Stegosystém ZZW

Zakódování první části zprávy:

- ▶ Nosič je rozdělen na  $b$  bloků velikosti  $2^{m_0}$ .
- ▶ Pro každý blok spočteme  $u_i = \bigoplus_{j=1}^{2^{m_0}} x_{i,j}$ .
- ▶ Zakódujeme první část zprávy  $\mathbf{v} = \text{Emb}_{\mathbf{H}_1}(\mathbf{u}, \mathbf{z}_1)$ .
- ▶ Jestliže  $u_i = v_i$ , pak  $\mathbf{y}_i = \mathbf{x}_i$ .
- ▶ Jestliže  $u_i \neq v_i$ , pak  $\mathbf{y}_i$  získáme tak, že v  $\mathbf{x}_i$  provedeme právě jednu změnu. (Volba její pozice v bloku dává prostor k zakódování další zprávy.)
- ▶ Očekávaný počet změn je tedy  $r_a$ .

# Stegosystém ZZW

Zakódování druhé části zprávy:

- ▶ Syndrom  $\mathbf{H}_0\mathbf{x}_i$  lze upravit na libovolnou hodnotu provedením *právě jedné* změny v  $\mathbf{x}_i$ .
- ▶ Pro každý blok spočteme  $\mathbf{r}_i = \mathbf{H}_0\mathbf{x}_i$ .
- ▶ Když  $u_i = v_i$ , označíme složky vektoru  $\mathbf{r}_i$  jako mokré, v opačném případě jako suché.
- ▶ Všechna  $\mathbf{r}_1, \dots, \mathbf{r}_b$  sřetězíme do jediného vektoru  $\mathbf{r}$ .
- ▶ Vektor  $\mathbf{r}$  je mokrá nosič s očekávaným počtem suchých prvků  $r_a m_0$ .
- ▶ Podle věty o mokré nosiči lze do  $\mathbf{r}$  vložit  $m_2 \approx r_a m_0$  bitů informace.

# Stegosystém ZZW

Parametry stegosystému:

- ▶ Délka nosiče =  $b2^{m_0}$ .
- ▶ Celkový počet bitů zprávy =  $m_1 + m_2 \approx m_1 + r_a m_0$ .
- ▶ Očekávaný počet změn =  $r_a$ .
- ▶ Relativní kapacita a efektivita:

$$\alpha \approx \frac{m_1 + r_a m_0}{b2^{m_0}} \quad \text{a} \quad e \approx \frac{m_1 + r_a m_0}{r_a}.$$

# Stegosystém ZZW

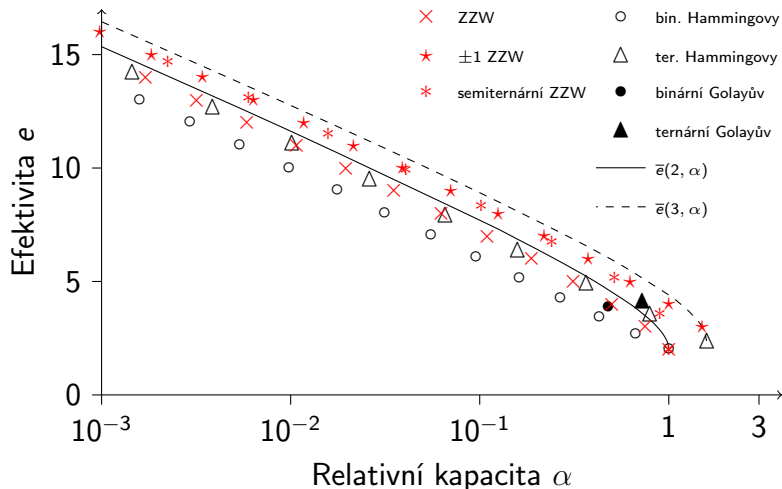
Zobecnění a vylepšení:

- ▶ Bloky nemusejí mít všechny stejnou délku  $2^{m_0}$ .
- ▶ Zpráva  $\mathbf{z}_1$  se nemusí kódovat do  $\mathbf{u}$  najednou. Lze postupovat po blocích.
- ▶ Můžeme použít dvouúrovňové  $\pm 1$  vkládání.
- ▶ Místo binárních Hammingových kódů lze použít ternární. (Kód  $\mathcal{C}$  však zůstává binární.)

Dokonce i pro triviální kód  $\mathcal{C}$  (tj.  $\mathbf{z}_1 = \mathbf{v}$ ) dosahuje stegosystém ZZW výborných výsledků.



# Triviální ZZW vs. perfektní kódy



Odstup od obou mezí je  $< 0,6$ .