STEGANOGRAFIE A DIGITÁLNÍ MÉDIA

ZKOUŠKOVÉ OTÁZKY 2013/14

U všech otázek se předpokládá schopnost definovat související pojmy, popřípadě dokázat pomocná tvrzení nebo formulovat pomocné algoritmy.

1. Popište histogramový útok na LSB embedding.
2. Popište kvantitativní útok na Jsteg.
3. Popište jeden z útoků založených na sample pairs analysis.
4. Popište kvantitativní útok na EzStego založený na párové analýze.
5. Popište vkládání s optimálním přiřazením parity a dokažte správnost algoritmu optimálního přiřazení parity.
6. Popište stegosystém OutGuess a odvoďte vzorec pro relativní kapacitu nosiče.
7. Popište algoritmus vkládání využívaný ve stegosystému F5 a odvoďte vzorec pro relativní kapacitu nosiče (bez maticového kódování).
8. Formulujte a dokažte algoritmus maticového vkládání pomocí minimum-distance dekodéru.
9. Formulujte a dokažte větu o maticovém vkládání a její důsledek týkající se efektivity maticového vkládání.
10. Odvoďte horní mez na spodní efektivitu maticového vkládání v závislosti na relativní kapacitě.
11. Odvoďte horní mez na efektivitu maticového vkládání pro kód s parametry $[n, k]_q$ a její souvislost s perfektními kódy.
12. Vysvětlete co to jsou SDCS a jakým způsobem se používají ve steganografii. Odvoďte horní mez na spodní efektivitu SDCS vkládání.
13. Formulujte a dokažte větu o mokrém nosiči.
14. Vysvětlete vkládání při kvantizaci a vkládání při dvojité ztrátové kompresi.
15. Popište modifikované maticové vkládání. Vysvětlete jaká je časová složitost MME2 a MME3.
16. Vysvětlete dvouúrovňové ± 1 vkládání a jak zlepšuje kapacitu a efektivitu, zejména ve vztahu k horní mezi na spodní efektivitu maticového vkládání.
17. Popište stegosystém ZZW a odvoďte vzorec pro relativní kapacitu a efektivitu.
18. Vysvětlete vlastnosti MDS kódů ve vztahu k maticovému vkládání do mokrého nosiče.
19. Popište algoritmus maticového vkládání do mokrého nosiče založený na robustním solitonovém rozdělení a odvoďte jeho časovou složitost. (Vzorce si pamatovat nemusíte, viz nápověda na další straně.)

Nápověda

Definice. Nechť m je přirozené číslo, $\delta > 0$ a $c > 0$. Označme $R = c \cdot \ln(m/\delta)\sqrt{m}$,

$$\rho(i) = \begin{cases} \frac{1}{m} & \text{pro } i = 1, \\ \frac{1}{i(i-1)} & \text{pro } i = 2, \ldots, m, \\ 0 & \text{pro } i > m, \end{cases} \quad \text{a} \quad \tau(i) = \begin{cases} \frac{R}{m}\frac{1}{i} & \text{pro } i = 1, \ldots, m/R - 1, \\ \frac{R}{m}\ln(R/\delta) & \text{pro } i = m/R, \\ 0 & \text{pro } i > m/R. \end{cases}$$

Řekneme, že diskrétní náhodná veličina X má *robustní solitonové rozdělení* s parametry (m, δ, c), jestliže

$$\Pr[X = i] = \frac{\rho(i) + \tau(i)}{\sum_{j=1}^{m} \rho(j) + \tau(j)}.$$