STEGANOGRAFIE A DIGITÁLNÍ MÉDIA

SEZNAM ZKOUŠKOVÝCH OTÁZEK 2014/15

U všech otázek se předpokládá schopnost definovat související pojmy, popřípadě dokázat pomocná tvrzení nebo formulovat pomocné algoritmy. Dále se předpokládá základní znalost formátu JPEG.

1. Popište histogramový útok na LSB embedding. (Kapitola 5.1.1 [F].)
2. Popište kvantitativní útok na Jsteg. (Kapitola 5.1.2 [F].)
3. Popište útok založený na sample pairs analysis. (Kapitola 11.1.3 [F].)
4. Popište vkládání s optimálním přiřazením parity a dokažte správnost algoritmu optimálního přiřazení parity. (Kapitola 1.3 [K].)
5. Popište kvantitativní útok na vkládání s optimálním přiřazením parity. (Článek [Z].)
6. Popište stegosystém OutGuess a odvoďte vzorec pro relativní kapacitu nosiče. (Kapitola 7.1.1 [F].)
7. Popište algoritmus vkládání využívaný ve stegosystému F5 a odvoďte vzorec pro relativní kapacitu nosiče bez maticového kódování. (Kapitola 7.3.2 [F].)
8. Formulujte a dokažte algoritmus maticového vkládání pomocí minimum-distance dekodéru. (Algoritmus 2.3 [K].)
9. Formulujte a dokažte větu o maticovém vkládání a její důsledek týkající se efektivity maticového vkládání. (Věta 2.4 a důsledek 2.5 [K].)
10. Odvoďte spodní mez na pokrývací poloměr v závislosti na relativní kapacitě. (Lemma 2.6 a věta 2.7 [K].)
11. Odvoďte horní mez na efektivitu maticového vkládání pro kód s parametry $[n, k]_q$ a její souvislost s perfektními kódy. (Věta 2.10 a důsledek 2.11 [K].)
12. Vysvětlete, co to jsou SDCS a jakým způsobem se používají ve steganografii. Odvoďte spodní mez na maximální počet změn vyvolaných SDCS vkládáním. (Věta 3.2 [K].)
13. Formulujte a dokažte větu o mokrém nosiči. (Věta 4.1 [K].)
14. Vysvětlete vkládání při kvantizaci a vkládání při dvojité ztrátové kompresi. (Kapitoly 4.1.1 a 4.1.2 [K].)
15. Vysvětlete dvouúrovňové ± 1 vkládání a jak zlepšuje kapacitu a efektivitu, zejména ve vztahu k horní mezi na spodní efektivitu maticového vkládání. (Kapitola 4.2.1 a tvrzení 4.2 [K].)
16. Vysvětlete, jakým způsobem se ve steganografii využívají konvoluční kódy a Viterbiho algoritmus. (Kapitola 5 a algoritmus 5.3 [K].)

Literatura

[F] Fridrich, J.: *Steganography in digital media: Principles, algorithms, and applications*. Cambridge University Press, 2010.

[K] Kozlík, A.: *Steganografie a digitální média*. 2015.
URL `http://www.karlin.mff.cuni.cz/~kozlik/sdm/sdm.pdf`

[Z] Zhang, X.; Wang, S.: Analysis of Parity Assignment Steganography in Palette Images.
URL `http://dx.doi.org/10.1007/11553939_144`