

Oponentský posudek bakalářské práce
Roman Cinkais: Steganografie a steganoanalýza

Steganografie, stejně jako kryptografie, se snaží zaměřit odhalení tajné zprávy nepřátelské straně. Od kryptografie se liší tím, že úkolem je utajit *existenci* samotné zprávy. Úkolem bakalářské práce Romana Cinkaise bylo zpracovat přehled současných steganografických metod s důrazem na skrývání zpráv v audio a video souborech a diskutovat možnosti detekce digitální steganografie.

Úvodní kapitola obsahuje přehled steganografie, následuje stručný popis některých metod na její odhalení, závěrečná kapitola se zabývá úspěšností těchto metod. Práce obsahuje rozsáhlou přílohu s naměřenými daty a grafy. Přílohou je rovněž DVD s databází obrázků, dat pro jednotlivé testy, detailnější informace o některých obrazových formátech, hlavně však autorem naprogramovanou aplikaci "StegaIs", která umožňuje provádět jednoduché testy zmíněné ve druhé kapitole.

Kromě drobných překlepů, nepřesností a chybné sazby (různé typy odkazu na literaturu – někde [10], jinde (Kahn 2001), 1MB = 10⁶B, vzorce na str. 29, apod.) lze práci vytknout jistou povrchností. Jsou diskutovány pouze nejjednodušší steganoanalytické testy, bylo by dobré alespoň zmínit některé pokročilejší metody, existují-li. Zmíněná nevýhoda je však kompenzována poměrně širokým záběrem, patrným například z rozsáhlé bibliografie, četností a atraktivností textu (barevné ilustrace, historické zmiňky, ...) a rovněž výše zmíněným programem "StegaIs" pro steganoanalýzu.

Bakalářskou práci Romana Cinkaise **doporučuji k obhajobě** a navrhuji ohodnotit stupněm **v ý b o r n ě**.

V Praze dne 30.8.2007

Mgr. Libor Barto, Ph.D.