

Moderné metódy obrazovej steganografie

Tomáš Jozef · Informačné technológie

30.06.2014



Tento príspevok je zameraný na podrobný opis a porovnanie moderných steganografických algoritmov, ktoré sú využívané na utajený prenos správ v pozadí bežne prebiehajúcej komunikácie. V prvej časti práce je opísaný steganografický systém, analýza jeho vlastností a základné rozdelenie. Druhá časť práce je venovaná všeobecnému prehľadu moderných metód steganografických algoritmov, ktoré vkladajú tajnú správu do statických obrazov v JPEG formáte. V záverečnej časti práce je opis vytvorenej databázy a porovnanie experimentálnych výsledkov pre vybrané steganografické metódy.

Úvod

Keďže pre každého človeka je istá forma súkromia veľmi dôležitá, ustrážiť si ju v dnešnej dobe informačných technológií je čoraz náročnejšie. V súčasnom uponáhľanom svete ľudí prebieha veľké množstvo našej komunikácie, vyjadrení a jeho zdieľaní so širokým okolím v digitálnej podobe. Na jednej strane je takáto forma digitalizácie vítaná, pretože nám uľahčuje prácu a poskytuje služby v pohodlí domova. Na druhej strane je však zneužívaná pre nelegálnu činnosť, alebo činnosti ktoré ohrozujú spoločnosť ako napríklad teroristické či hackerské útoky s úmyslom poškodenia. Práve ochrana informácií a bezpečnosť pri ich prenose informačnými kanálmi v digitálnej podobe je momentálne celosvetovým problémom.

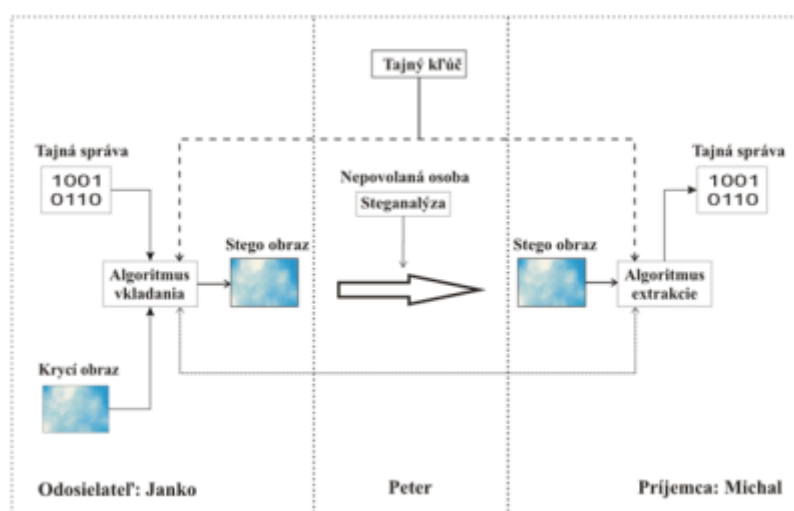
Tu sa však otvára priestor pre vývoj vedných disciplín ako je steganografia. Aj keď je steganografia známa už tisíce rokov, pre mnoho ľudí sú pojmy steganografia a steganografické metódy úplne neznámymi pojmami. Slovo steganografia pochádza z gréčtiny a pozostáva z dvoch slov a to zo slova „steganos“ (skrytý) a „graphein“ (písať). Je to veda o utajovaní komunikácie prostredníctvom ukrytia tajnej informácie v správe [1]. Úspešný steganografický systém nedáva nepovolánym osobám vôbec vedieť, že je nejaká dodatočná (tajná) informácia prítomná.

1. Steganografia

Steganografia je vednou disciplínou, ktorej úlohou je preniesť tajnú správu v pozadí neutajenej komunikácie. Takáto kamufláž dokáže ochrániť tajnú správu medzi odosielateľom a prijímateľom pred útokmi nepovoláných osôb. Tento prístup sa líši od kryptografie tým, že kladie dôraz na zneprístupnenie komunikácie a nie na utajenie správy. Pre zvýšenie bezpečnosti sa niektoré systémy kryptografie využívajú aj v

steganografii.

Zovšeobecnený model steganografického systému, ktorý vytvára podprahovú komunikáciu, je možné vidieť na Obr. 1. Hlavným princípom tohto modelu je ukrytie tajnej informácie v digitálnych dátach tak, aby ju tretia strana (nepovolaná osoba) nedokázala odhaliť. Prvým krokom pri vytváraní steganografického modelu je výber krycieho média (cover medium), ktoré je nosičom tajnej správy. Krycie médium môže tvoriť akékoľvek multimédium, napr. text, statické obrázky, audio, video a iné. Platí však zásada, že médium musí obsahovať dostatočne veľké množstvo redundancie, do ktorých sa vkladá tajná informácia. V druhom kroku sa musí vybrať vhodný algoritmus pre ukrytie dát do krycieho média. Tento algoritmus musí byť rovnaký aj na strane príjemcu. Prostredníctvom algoritmu sa vloží tajná informácia do krycieho média, čím vzniká stego objekt (stego médium). Pre vyššiu bezpečnosť používajú niektoré algoritmy v procese vkladania tajný kľúč.



Obr. 1 Bloková schéma steganografického systému

Na strane príjemcu, ktorý pozná použitý steganografický algoritmus, sa pomocou tajného kľúča, ktorý bol použitý v procese vkladania tajnej informácie, vyextrahuje zo stego objektu tajná správa. Tak ako proti každej zbrani existuje protizbraň a proti každému vírusu existuje vakcína tak ani moderná steganografia nie je výnimkou. Zostáva dodať len toľko, že rovnako ako existuje špecializovaný systém pre ukrývanie tajných správ, existuje aj podobný systém, ktorý je určený k ich vyhľadávaniu. Tento systém sa nazýva steganalyza.

1.1 Charakteristika systémov steganografie

Steganografický systém charakterizujú nasledujúce vlastnosti [1]:

- Nedetekovateľnosť (Undetectability)
- Kapacita (Capacity)
- Perceptívna transparentnosť (Perceptual transparency)
- Bezpečnosť a robustnosť (Security and robustness)

Nedetekovateľnosť je základná vlastnosť, ktorá vyjadruje počet vykonaných štatistických zmien, ktoré sú spôsobené vložením tajnej správy. *Kapacita* je vyjadrením maximálneho množstva tajnej informácie, ktoré je možné vložiť do krycieho média

prostredníctvom danej metódy. Kapacita sa udáva v bitoch. *Bezpečnosť* systému je vlastnosť, ktorou sa ochraňuje tajná správa, resp. vyjadruje obtiažnosť pri extrakcii tajnej správy z označeného média.

Robustnosť systému je odolnosť systému vzhľadom na útoky, znehodnotenie alebo pokusy o odstránenie tajnej správy z označených médií tak, aby nedošlo k zničeniu alebo poškodeniu tajnej správy. *Perceptívna transparentnosť* je schopnosť zachovania si požadovanej kvality daného krycieho média aj po vložení tajnej informácie. Pozorovateľ tak nie je schopný postrehnúť nižšiu kvalitu, resp. rozoznať krycie médium od stego média. Táto metóda sa vyžaduje najmä pri audiovizuálnych dátach.

2. Základné rozdelenie steganografických systémov

Základným rozdelením steganografických metód by som označil rozdelenie podľa typu vstupných dát. V podstate je možné použiť všetky digitálne dáta, avšak najčastejšie používanými sú audio súbory a obrázky. Tento príspevok je zameraný najmä na techniky, ktoré sú používané v rámci statických obrazov. Metódy steganografie v statických obrazoch je možné rozdeliť podľa spôsobu vkladania tajnej informácie do krycieho média. Z tohto hľadiska ich môžeme zatriediť do šiestich základných skupín [2]:

- Substitučné metódy
- Metódy v transformovanej oblasti
- Metódy s rozprestretým spektrom
- Štatistické metódy
- Metódy skreslenia
- Metódy založené na generovaní krycieho obrazu

2.1 Substitučné metódy

Ich podstata spočíva v zamieňaní nadbytočných častí krycieho obrazu, alebo častí obrazu ktoré sú čo najmenej potrebné, za tajnú informáciu. Zámena je realizovaná tak, aby voľným okom nebolo možné postrehnúť rozdiel na krycom obraze. Aby prijímateľ mohol tajnú informáciu správne dekodovať, musí byť oboznámený o presnej pozícii, kde sa tajná informácia nachádza. Výhodou substitučných metód je ich jednoduchosť, spôsob ukrývania tajnej informácie a tiež aj poskytovanie vysokej miery perceptívnej transparentnosti. Na druhej strane je ich veľkou nevýhodou bezpečnosť. Tým že sa pri ukrývaní tajnej informácie menia štatistické vlastnosti obrazu je jej odhalenie veľmi jednoduché. V súčasnosti je používanie substitučných metód v digitálnej steganografii na ústupe.

2.2 Metódy v transformovanej oblasti

Postačujúcu bezpečnosť pre ukrývanie tajných správ nám poskytujú metódy v transformovanej oblasti, pretože ukrývanie informácií vo frekvenčnej oblasti je viac odolné voči narušeniu ako v časovej oblasti. Výhodou týchto metód je ukrývanie tajnej správy do oblastí krycieho obrazu, ktoré sú odolnejšie voči orezávaniu a kompresii. Podmienkou je však malá veľkosť tajnej správy, čím sa zabezpečí čo najmenšia zmena štatistických vlastností obrazu a to je z hľadiska kapacity ich veľkou nevýhodou.

2.3 Metódy s rozprestretým spektrom

V komunikačných technológiách sa metódy s rozprestretým spektrom vyvíjali už od roku 1950. Tieto metódy poskytujú veľmi dobrú perceptívnu transparentnosť a taktiež aj veľkú kapacitu pre ukrývanie tajných správ. Ukrytá tajná správa je rozprestretá po celom krycom médiu.

2.4 Štatistické metódy

Štatistické metódy sú známe aj ako metódy, ktoré obnovujú štatistické vlastnosti obrazu. Hlavnou úlohou je teda vykonanie čo najmenších zmien štatistických vlastností obrazu. Používanie štatistických metód závisí vo veľkej miere od výberu vhodného krycieho obrazu. Pri použití obrazu s veľkým množstvom nulových DCT koeficientov klesá kapacita, ale je možné dosiahnuť vyššiu bezpečnosť utajenej správy. Pretože ide o metódy pracujúce v transformovanej oblasti, tak ich perceptívna transparentnosť je veľmi dobrá.

2.5 Metódy skreslenia

Metódy skreslenia sa veľmi podobajú substitučným metódam. Rozdiel medzi nimi spočíva v procese extrakcie, kde metódy skreslenia stále potrebujú originálny obraz, do ktorého bola tajná správa vložená. Ich princíp spočíva v doručení stego obrazu prijímateľovi spolu s originálnym obrazom. Na základe ich porovnania prijímateľ extrahuje tajnú správu.

2.6 Metódy založené na generovaní krycieho obrazu

Metódy založené na generovaní krycieho obrazu si počas procesu vkladania vytvárajú vlastný krycí obraz. Ich použitie môžeme nájsť v lingvistickej steganografii, kde sa tajná správa ukrýva pomocou textu. Tieto metódy sú veľmi nevýhodné z hľadiska časovej náročnosti, ktorá je pri vkladaní a extrakcii tajnej správy veľmi veľká.

3. Programová realizácia a databáza obrazov

Navrhovaný program je určený pre vybrané moderné metódy obrazovej steganografie ako sú nsF5 [3], MB1 [4], MB2 [4], PQ [5], MHF-DZ [6], ktoré pracujú s obrazmi vo formáte JPEG. Pre tento účel bola vytvorená aj databáza obrazov, ktorá bola získaná pomocou rôznych typov fotoaparátov. V navrhnutom programe sa prostredníctvom steganografických metód a databázy krycích obrazov vytvárajú stego obrazy (obrazy s tajnou správou).

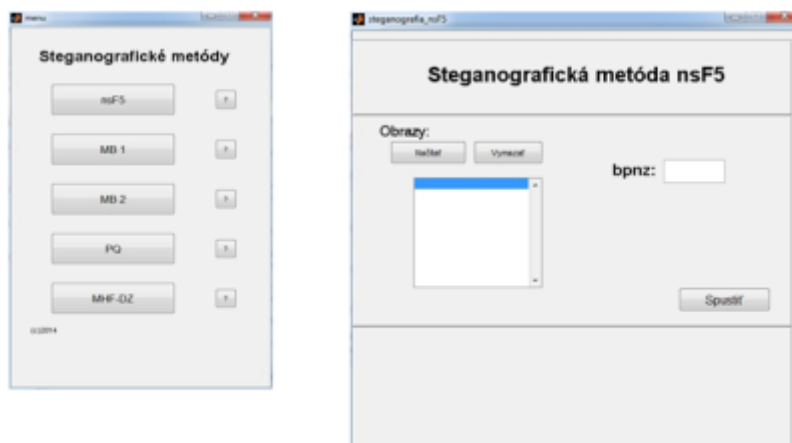
3.1 Databáza obrazov

Na vytvorenie databázy obrazov bolo použitých približne 18000 pôvodných obrazov, ktoré boli nafotené rôznymi typmi fotoaparátov, ako napríklad Nikon D3000, Samsung S730, Sony Ericsson C702, Lumix, Nikon D60, Nikon D3100, Nikon D3200, Olympus FE-115, Olympus X-715. Zo získaných obrazov bola vytvorená množina 2000 obrazov, ktorá bola následne rozdelená do ôsmich skupín, v ktorých boli obrazy tiež zo všetkých fotoaparátov. V každej skupine pozostávajúcej z 250 obrazov som upravil grafické rozlíšenie obrazov na veľkosti 320 x 240 (QVGA), 480 x 320 (HVGA), 640 x 480 (VGA),

800 x 600 (SVGA), 1024 x 768 (XGA), 1600 x 1200 (UXGA) a 1920 x 1080 (HD 1080), aby vzorka pre vkladanie správy bola čo najpestrejšia.

3.2 Programová realizácia

Ovládanie navrhnutého používateľského prostredia celého programu určeného pre moderné metódy obrazovej steganografie je pre používateľa veľmi jednoduché. Realizované je v programovom prostredí GUIDE v simulačnom programe MATLAB 7.9 R2009b. Po spustení programu súborom „menu.m“ sa zobrazí úvodné okno programu, ktoré ponúka na výber moderné metódy obrazovej steganografie, ktoré sú spomenuté v úvode tejto kapitoly (Obr. 2).



Obr. 2 Úvodné okno programu pre výber moderných steganografických metód a okno vybranej steganografickej metódy

Po vybratí metódy sa zobrazí okno zvolenej metódy (Obr. 2), v ktorom pomocou tlačidla „Načítať“ sa zobrazí okno pre výber krycích obrazov vytvorenej databázy. Ďalej je potrebné zadať hodnotu (bit per non-zero AC DCT coefficient), čo je počet bitov tajnej správy na jeden nenulový AC DCT koeficient. Táto hodnota by mala byť zadávaná v tvare desatinného čísla z intervalu od 0 do 1. Vkladanie náhodne vygenerovanej správy do vybraných krycích obrazov sa uskutoční po stlačení tlačidla „Spustiť“. Rovnaký postup pre vkladanie správy do krycích obrazov vytvorenej databázy je pre všetky vybrané steganografické metódy.

4. Experimentálne výsledky

Prostredníctvom vytvoreného programu bola do krycích obrazov ukrývaná náhodne vygenerovaná tajná správa. Veľkosť vkladanej správy s je vypočítaná ako

$$s = rand(nzAC, bpnz) \quad (1)$$

kde $nzAC$ je počet nenulových AC DCT koeficientov krycieho obrazu a $bpnz$ je počet bitov na jeden nenulový AC DCT koeficient. Na základe objektívnych a subjektívnych parametrov kvality boli následne porovnávané krycie obrazy s obrazmi, ktoré obsahujú vloženú tajnú správu.

Z objektívnych parametrov kvality bola vybraná stredná kvadratická chyba (MSE), pomocou ktorej bol vypočítaný špičkový pomer signál/šum (PSNR), stredná absolútna chyba (MAE) a maximálnu kapacita vlozenej správy (C). Keďže správa nie je vkladaná

do jedného krycieho obrazu ale do vybranej množiny krycích obrazov s rôznou veľkosťou a rozlíšením, hodnoty zobrazené v tabuľkách sú výsledné priemerné hodnoty. V nasledujúcej tabuľke (Tab. 1) sú vypísané priemerné hodnoty vložených bitov tajnej správy do množiny 250 krycích obrazov.

Tab.1 Priemerná veľkosť vlozenej správy (250 obrazov)

bpnz	nsF5, MB1, MB2, MHF-DZ	PQ
	C (kb)	C (kb)
0.05	5,207	4,209
0.25	26,035	21,045
0.5	52,069	42,089
0.75	78,104	63,135
1	104,138	84,179

Ako si môžeme všimnúť, hodnoty pre steganografické metódy nsF5, MB1, MB2 a MHF-DZ sú rovnaké. Vyplýva to z vyššie uvedeného vzťahu (1) pre výpočet veľkosti vkladanej správy do krycích obrazov, ktorý je použitý pre všetky steganografické metódy. Hodnoty pri steganografickej metóde PQ sú menšie, pretože veľkosť vkladanej správy sa počíta z obrazov v odtieňoch šedej. Po vypočítaní a následnom vložení tajnej správy boli vypočítané priemerné hodnoty MSE, MAE a PSNR, ktoré sú zobrazené v Tab. 2.

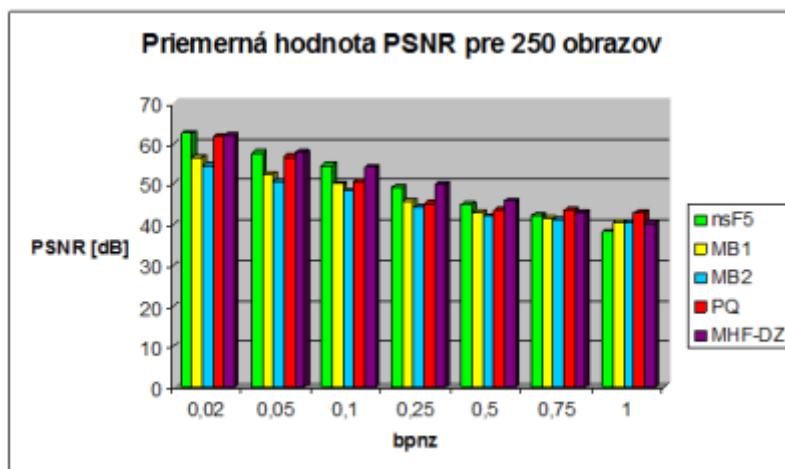
Tab.2 Maximálne priemerné hodnoty PSNR , MSE a MAE pre vzorku 250 obrazov

bpnz	nsF5			MB1			MB2		
	PSNR (dB)	MSE	MAE	PSNR (dB)	MSE	MAE	PSNR (dB)	MSE	MAE
0,02	62,6348	0,05	0,02	56,5777	0,19	0,10	54,7162	0,28	0,15
0,05	57,6474	0,18	0,80	52,5344	0,52	0,26	50,7751	0,72	0,35
0,1	54,7038	0,36	0,15	50,0629	0,89	0,42	48,3463	1,24	0,54
0,25	49,2409	1,32	0,45	45,8122	2,43	0,85	44,3585	3,24	1,03
0,5	45,1549	3,24	0,89	43,0635	4,46	1,26	42,0599	5,59	1,43
0,75	42,4073	6,43	1,36	41,5195	6,65	1,57	41,2878	7,04	1,62
1	38,2689	15,73	2,28	40,5832	7,99	1,76	40,5814	7,99	1,76

bpnz	PQ			MHF-DZ		
	PSNR (dB)	MSE	MAE	PSNR (dB)	MSE	MAE
0,02	61,7301	0,05	0,03	61,8908	0,05	0,05
0,05	56,795	0,19	0,09	57,7513	0,14	0,13
0,1	50,6386	1,19	0,24	54,2440	0,31	0,28
0,25	45,2348	3,72	0,55	49,9873	0,74	0,55
0,5	43,7653	4,42	0,68	45,8973	1,84	0,97
0,75	43,5426	4,67	0,72	42,9717	4,01	1,42

1	43,0123	4,95	0,75	40,4403	8,07	1,93
---	---------	------	------	---------	------	------

Výsledné hodnoty PSNR sú kvôli lepšiemu prehľadu vykreslené na grafe znázornenom na Obr. 3.



Obr. 3 Grafické znázornenie priemerných hodnôt PSNR

Zo zobrazeného grafu a nameraných hodnôt vyplýva, že metódy nsF5 a MHF-DZ dosahujú lepšie výsledky pri menšej veľkosti vlozenej tajnej správy. Z hľadiska perceptívnej nevnímateľnosti vyhovujú všetky metódy, keďže rozdiel medzi krycím a stego obrazom pri maximálnej veľkosti vlozenej tajnej správy je približne 40 dB. Takýto rozdiel medzi obrazmi je ľudským okom nepostrehnuteľný. Následne boli steganografické metódy porovnávané z časového hľadiska. Teda ako dlho trvalo steganografickým metódam vkladanie tajnej správy do množiny 250 krycích obrazov. Pri tomto meraní vplýva na kvalitu výsledkov viacero faktorov, ako sú napríklad používaný operačný systém, výkon procesora, počet spustených aplikácií, procesy bežiacie v pozadí a ďalšie. Aby boli výsledky objektívnejšie, meranie bolo vykonané 3-krát a do Tab. 3 bol uvedený najkratší čas vkladania správy.

Tab.3 Porovnanie metód z hľadiska času pri procese vkladania tajnej správy

bpnz	nsF5	MB1	MB2	PQ	MHF-DZ
0.02	25.19	19:27.37	55:29.84	12:35.39	x
0.05	26.05	16:16.31	53:52.71	10:53.34	x
0.1	27.99	16:45.43	1:01:52.18	13:54.31	x
0.25	28.31	20:29.90	1:03:45.82	12:49.47	x
0.5	27.87	22:13.56	1:54:32.57	13:06.11	x
0.75	37.53	23:53.94	1:55:57.12	12:21.12	x
1	36.64	22:27.45	1:56:47.75	13:10.33	x

Pre lepšie vytvorenie predstavy o veľkosti rozdielu medzi originálnym obrazom a stego obrazmi vybraných steganografických metód bola vložená do krycieho obrazu (Obr.4 a) správa s veľkosťou 0.5, čo predstavuje 22048 bitov pre každú metódu, okrem metódy PQ kde veľkosť vkladanej správy je pri 0.5 17749 bitov. Porovnanie originálneho obrazu so stego obrazmi všetkých vybraných steganografických metód je

zobrazené na Obr.4, spolu s vypočítanými hodnotami PSNR, MSE a MAE. Ako najlepšiu steganografickú metódu pri tomto obraze môžeme určiť metódu MHF-DZ, ktorej PSNR dosahuje najvyššiu hodnotu a stredná kvadratická chyba MSE je najnižšia.



a) originálny obraz



b) nsF5: PSNR = 41,2075 dB, MSE = 4,92 MAE = 1,15



c) MB1: PSNR = 40,4526 dB, MSE = 5,86 MAE = 1,5



d) MB2: PSNR = 39,2131 dB, MSE = 7,79 MAE = 0,88



e) PQ: PSNR = 39,2131 dB, MSE = 7,05 MAE = 0,88



f) MHF-DZ: PSNR = 45,6487 dB, MSE = 1,77 MAE = 0,92

Obr.4 Porovnanie originálneho obrazu so stego obrazmi vybraných steganografických metód: a) originálny obraz, b) stego obraz nsF5, c) stego obraz MB1, d) stego obraz MB2, e) stego obraz PQ, f) stego obraz MHF-DZ

Záver

Ľudstvo si uvedomuje, že je čoraz náročnejšie ochrániť svoje informácie, ktoré sú v digitálnej podobe. Práve oblasť steganografie nám pomáha riešiť tento problém, vďaka čomu je o ňu v dnešnej dobe zo strany odbornej verejnosti veľký záujem. Za posledných pár rokov bol vyvinutý a zdokonalený veľký počet steganografických metód a preto je pri voľbe vhodnej steganografickej metódy nevyhnutné poznať ich charakteristické vlastnosti. Tento článok je venovaný opisu steganografie v statických obrazoch, moderným steganografickým metódam, ktoré vkladajú tajnú správu do obrazov vo formáte JPEG, vytvoreniu vlastnej databázy krycích obrazov a realizácii softvéru pre vkladanie správ do vybraných steganografických metód. Hlavným cieľom bolo porovnať moderné steganografické metódy z hľadiska kapacity pre vloženie tajnej

správy a z hľadiska perceptívnej nevnímateľnosti. Z nameraných hodnôt bolo zistené, že vybrané steganografické metódy dosahujú z hľadiska preceptívnej nevnímateľnosti veľmi dobré výsledky.

Zoznam použitej literatúry

1. LEVICKÝ, Dušan: Kryptografia v informačnej a sieťovej bezpečnosti. 1. Vyd. Košice: Elfa, s.r.o., 286 s. ISBN 978-80-8086-163-6.
2. NAGHAM, Hamid - ABID, Yahya - BADLISHAH, Ahmad - OSAMAH, M.: Image Steganography Techniques: An Overview. Internal Journal of Computer Science and Security, Volume-6, Issue-3, 2012.
3. FRIDRICH, J. - GOLJAN, M. - SOUKAL, D.: Wet paper codes with improved embedding efficiency, [online], Information Forensics and Security, IEEE Transactions on, vol.1, no.1, pp.102,110, March 2006
4. FRIDRICH, J. - GOLJAN, M. - SOUKAL, D.: Pertrubed quantization steganography. ACM Multimedia System Journal, 11(2): pp.98-107, 2005.
5. SALLEE, P.: "Model-based methods for steganography and steganalysis," International Journal of Image and Graphics, 167-190 (2005).
6. BANOCI, V. - BUGAR, G. - LEVICKY, D. - KLENOVICOVA, Z.: Histogram secure steganography system in JPEG file based on modulus function, [online], Radioelektronika (RADIOELEKTRONIKA), 22nd International Conference , pp.1-4, 17-18 April 2012. ISBN: 978-1-4673-0659-1.

Spoluautorom článku je Ing. Martin Broda, Katedra elektroniky a multimediálnych telekomunikácií, Fakulta elektrotechniky a informatiky, Technická univerzita v Košiciach
