Fakulta elektrotechniky a informatiky
Slovenská Technická Univerzita v Bratislave

Ing. Matúš Jókay

Autoreferát dizertačnej práce

Steganografia v obraze a videu

na získanie vedecko–akademickej hodnosti
philosophiae doctor, PhD.
v doktorandskom študijnom programe
9.2.9 aplikovaná informatika

Bratislava 2011

Dizertačná práca bola vypracovaná v dennej forme doktorandského štúdia na oddelení Bezpečnosti informačných systémov Ústavu informatiky a matematiky FEI STU v Bratislave.

Predkladateľ: Matúš Jókay
ÚIM FEI STU
Ilkovičova 3
812 19 Bratislava

Školiteľ: Prof. RNDr. Otokar Grošek, PhD.
FEI STU Bratislava

Oponenti: prof. Ing. Jaroslav Polec, PhD.
Ústav telekomunikácií
FEI STU v Bratislave
Ilkovičova 3
81219 Bratislava
Slovenská republika

Ing. Thomas Seidmann, PhD.
Synergetics AG
Kantonsstrasse 3
CH-6246 Altishofen
Switzerland

Autoreferát bol rozoslaný dňa .....

Obhajoba dizertačnej práce sa koná ..... o ..... h
na Fakulte elektrotechniky a informatiky STU, Ilkovičova 3, 812 19 Bratislava,
v .....

doc. RNDr. Gabriel Juhás, PhD.
Dekan FEI STU

Obsah

Úvod

Snaha o ukrytie existencie informácie sprevádza človeka počas celej jeho histórie jestvovania. Prvé písomné zmienky o technikách ukrývania jestvovania správ pochádzajú zo starého Egypta spred štyroch tisícročí [47]. Od čias Egypťanov sa vynašlo mnoho steganografických techník a oblastí ich využitia.

S príchodom rozvoja informatiky a digitalizáciou informácií sa oblasť využitia steganografie natoľko rozšírila, že sa dostala do popredia záujmu odbornej verejnosti. Hoci samotné ukrývanie jestvovania správ je možné v reálnom svete realizovať oveľa väčším množstvom spôsobov než v tom digitálnom, hlavným nedostatkom steganografie reálneho sveta ostáva doručenie správy k príjemcovi. Problémom je nielen neprijateľné časové zdržanie, ale aj samotný transport správy. Tieto dva základné nedostatky odstránil digitálny prenos informácie. Pomocou neho je možné správu prenášať v rámci celej planéty v reálnom čase.

Globalizácia umožňuje komunikáciu ľudí celého sveta bez časového a priestorového obmedzenia. Počet osôb, s ktorými môže každý človek komunikovať, sa rádovo zvýšil oproti technickým možnostiam komunikácie predošlých storočí. Zavedenie celosvetovej siete informácií dovoľuje zdieľať textové, zvukové a obrazové dokumenty všetkými účastníkmi siete. Takto sa Internet a jeho všeobecná dostupnosť stali vhodným komunikačným kanálom na šírenie steganografických správ.

Techniky steganografie sa využívajú v zásade dvoma skupinami ľudí. Prvou sú tí, ktorí pomocou ukrývania dodatočných informácií do média chcú zabezpečiť čo najpresnejšie určenie páchateľa pri zneužití aktíva, ktoré je chránené steganografickými informáciami. Špeciálnou oblasťou ochrany v tomto zmysle je je tzv. vodotlač — vkladanie rôznych informácií do digitálnych médií (napríklad do obrázkov, zvuku, videa, dokumentov). Ľudia, ktorí zneužívajú možnosti steganografie, patria do druhej skupiny. Zneužitím chápeme využitie steganografických systémov na dosahovanie cieľov, ktoré sú v rozpore so zákonom. Príkladom môže byť dorozumievanie členov teroristických skupín ohľadom plánovaných útokov.

Pre zníženie možnosti zneužitia systémov na ukrývanie existencie informácií je nutné venovať pozornosť možnostiam detekcie utajených správ. Touto oblasťou sa zaoberá stegoanalýza. Vzhľadom na šírku komunikačného kanála Internetu je dôležité, aby bola detekcia optimálna (jej kritériom je rýchlosť a efektívnosť). Žiaľ, skupina steganografických systémov založených na tom istom médiu zväčša vyžaduje svoj vlastný steoanalytický prístup. To znemožňuje jednoduché zjednotenie steganoanalytických metód. Navyše, mnohé steganoanalytické postupy sú výsledkom skôr umenia než vedy, nakoľko pri voľbe parametrov steganografických algoritmov nie je možné exaktne určiť ich počiatočné hodnoty. Inicializácie (a niekedy i vyhodnocovanie výstupov) algoritmov sú tak dané skúsenosťami toho, kto vykonáva steganoanalýzu.

V našej práci sme zamerali pozornosť na návrh a implementáciu steganografických systémov v oblasti pohyblivého obrazu (t.j. videa), nakoľko sa tejto oblasti venuje oveľa menej pozornosti než steganografii v statickom obraze. Oblasti pohyblivého a statického obrazu sú úzko prepojené. Preto sme (ako bude ukázané ďalej) do práce zahrnuli aj implementáciu a analýzu steganografických systémov statických obrázkov.

Okrem návrhov, implementácií a stegoanalýze viacerých steganografických sys-

témov sme sa zaoberali aj analýzou vhodnosti využitia techník a metód z oblasti evolučných výpočtov a umelej inteligencie v návrhu steganografického systému. Zhodnotili sme efektivitu genetických algoritmov, neurónových sietí a horolezeckého algoritmu vo fáze vkladania steganografickej informácie do média. Za kritérium efektivity sme zvolili mieru odchýlky zvolených štatistík pôvodného média (bez vloženej správy) od steganografického nosiča (obsahujúceho steganografickú informáciu).

Čiastočné výsledky boli zverejnené (alebo poslané na uverejnenie) v publikáciách uvedených v časti 5.1. Výskum bol spolufinancovaný z grantov VEGA 1/3115/06, VEGA 1/0244/09 a NIL-I-004, a taktiež Národným bezpečnostným úradom SR. Na praktickej realizácii na ÚIM FEI STU sa podieľali aj Ing. Ján Baroš, Ing. Tomáš Moravčík, Bc. Peter Šrámek, Ing. Tibor Marko, Ing. Branislav Šulej, Ing. Marek Dubovský a Ing. Radoslav Blaško.

1 Ciele dizertačnej práce

Oblasť steganografie sa stáva čoraz populárnejšou predovšetkým vďaka verejnému zdieľaniu multimediálneho obsahu na Internete. Väčšina steganografických systémov používa techniky modifikácie statických obrázkov. V oblasti videa však chýba realizácia praktického systému; oproti statickému obrazu jestvuje iba niekoľko akademických úvah o algoritmoch aplikovateľných na špecifické vlastnosti videa. Preto boli hlavnými cieľmi našej práce návrh, analýza a implementácia praktických steganografických systémov v oblasti obrazu a videa:

1. analýza možnosti návrhu uvažovaných steganografických systémov,
2. špecifikácia typu (pohyblivého) obrazu, pre ktorý budú systémy navrhnuté,
3. návrh algoritmus na vloženie a vybratie tajnej správy pre každý systém,
4. zváženie možností stegoanalýzy navrhnutých systémov.

S úlohou hlavných téz úzko súvisí vytvorenie základného uceleného prehľadu o oblasti steganografie s ohľadom na rozšírené možnosti optimalizácie pomocou techník umelej inteligencie (neurónové siete, genetické algoritmy).

Návrh algoritmu na vloženie správy si vyžaduje dôkladné spracovanie oblasti steganografických techník statického obrazu, a to nielen z pohľadu algoritmického návrhu, ale aj steganografickej analýzy.

Doplnkové tézy vytvárajú priestor na definovanie znalostnej bázy, ktorá je východiskom na riešenie problematiky návrhu, analýzy a implementácie steganografických systémov v oblasti videa.

2 Teória a metódy

Steganografia je veda, ktorá sa zaoberá návrhom, analýzou a implementáciou algoritmov, metód a systémov, ktoré umožňujú:

- prenášať informáciu nepodozrivým komunikačným kanálom,
- utajiť samotné jestvovanie správy v komunikačnom kanále.

Steganoanalýza (alebo tiež zaužívaný kratší termín stegoanalýza) je vedná disciplína, ktorá sa zaoberá návrhom, analýzou a implementáciou algoritmov, metód a systémov, ktoré umožňujú potvrdiť alebo vyvrátiť existenciu informácie v sledovanom komunikačnom kanále. Primárnym cieľom nie je informáciu extrahovať.

Ako vidno z definície, steganografia využíva metódy utajenia komunikácie s cieľom realizovať utajený (skrytý) prenos informácie, ktorý prebieha v pozadí neutajenej komunikácie. Medzi steganografiou a kryptografiou je podstatný rozdiel práve v tom, že kryptografia utajuje iba informačný obsah, nie samotnú existenciu správy. Zjednodušene povedané, kryptografia transformuje pôvodne čitateľnú správu na takú, ktorú dokáže spätne transformovať na čitateľnú iba legitímny príjemca. Transformovaná správa sa posiela verejným komunikačným kanálom, kde

k nej môže mať prístup aj nelegitímny príjemca. Ten sa môže pokúsit o transformáciu správy do čitateľnej podoby, ale jeho úspešnosť bude závisieť od odolnosti kryptografického systému, ktorý bol na transformáciu pôvodnej správy použitý.

Steganografia študuje rôzne techniky ukrývania existencie nejakej (druhotnej) správy v inej (prvotnej) správe. Primárna správa sa nazýva nosič alebo obálka, sekundárna sa označuje prívlastkom tajná. Nosič informácie, v ktorom je ukrytá tajná správa, sa nazýva steganografické médium.

Podla [15] steganografia pokrýva tri ciele bezpečnosti: dôvernosť, schopnosť prežitia (robustnosť, odolnosť) a neodhaliteľnosť (nedetegovateľnosť). V návrhu našich steganografických systémov sme požiadavku dôvernosti dosahovali pomocou (predpokladanej) fázy predspracovania údajov, ktoré sa vkladajú do nosiča. V tomto predspracovaní sa správa transformuje pomocou kryptografického systému do (nelegitímnemu príjemcovi) nečitateľnej podoby. Ďalej sme predpokladali, že prenosový kanál, použitý na transport steganografického média nie je zdrojom šumu, a preto správa počas prenosu zachováva svoju integritu. Napokon pre naplnenie požiadavky nedetegovateľnosti sme navrhli použiť viaceré spôsoby kódovania informácie:

- minimalizáciu modifikácie bitov nosiča pomocou Hammingových kódov (kapitola 6 dizertačnej práce) a
- voľba kódovania, ktoré zachováva štatistické vlastnosti nosiča (napríklad pomer núl a jednotiek, kapitola 7 dizertačnej práce).

Steganografia v statickom obraze patrí medzi najpreskúmanejšie. Medzi základné steganografické techniky v tejto oblasti patria: modifikácia najmenej významného bitu, využitie štruktúry nosiča, kódovanie oblasťami.

Pri ukrývaní informácie do obrazu sa využíva nedokonalosť ľudského optického rozlišovania malých zmien farebných tónov. Dve farby sa v bitovej reprezentácií najmenej líšia pri zmene najmenej významného bitu. Tento sa oznacuje LSB z anglického Least Significant Bit. Technika ukrývania informácií do obrazovej mapy zmenou najmenej významného bitu sa označuje ako LSB technika.

Nie všetky typy reprezentácií obrazu používajú v priestorovej doméne mapu obrazových bodov, v ktorej má každý bod priamo definované hodnoty jednotlivých farebných zložiek. Niektoré reprezentácie používajú na mieste popisu farieb odkazy do tabuľky farieb. Výhodou tohto prístupu je menšia veľkost reprezentácie obrazu. Stačí, ak sa uložia použité farby v obraze do jednorozmerného poľa, a v mape obrazových bodov sú hodnoty farieb uložené ako indexy do tabuľky použitých farieb. Počtu bitov, ktoré sú použité na reprezentáciu farby jedného obrazového bodu, sa hovorí farebná hĺbka obrazu. Techniku LSB je možné použiť aj v prípade indexovaných obrazových súborov. Modifikácia spočíva v poprehadzovaní farieb v palete tak, aby boli usporiadané podľa najmenších rozdielov farebných hodnôt príslušných dvojíc indexov, ktoré sa algoritmom LSB na seba vzájomne mapujú (ide vždy o dvojicu farieb v palete na párnom a nasledujúcom nepárnom mieste).

Podobne ako v priestorovej oblasti, je možné využívať techniku LSB aj vo frekvenčnej oblasti. V procese komprimácie po vypočítaní kvantizovaných DCT koeficientov sa dajú tieto použiť na prenos informácie tak, že informačné bity budú kódované najmenej významnými bitmi vybraných DCT koeficientov. Okrem modifikovania alebo dekrementovania DCT koeficientov je možné využiť techniku modulácie. Pri nej sa vopred (alebo na základe tajného kľúča) zvolí minimálne jedna

dvojica DCT koeficientov v bloku (blok je tvorený zvyčajne 64 koeficientami). Informačný bit sa kóduje pomocou vzájomného rozdielu zvolenej dvojice koeficientov.

Základná schéma kodérov videa je približne rovnaká. Najprv sa urobí transformácia obrazových údajov do modelu YC_bC_r. V tomto modeli je oddelená jasová (Y) zložka od obrazových (C_b pre modrú farbu a C_r pre červenú; informácie pre zelenú zložku je možné vypocítat z týchto dvoch). Dôvodom transformácie je skutočnosť, že ľudské oko je viac citlivé na jas než na farbu. Preto je potrebné jasovú zložku spracovávat s väčšou presnosťou než obrazovú. Naopak, obrazovú zložku je možné redukovať bez pozorovateľnej degradácie obrazu.

Spracovanie jednotlivých video snímok sa môže robiť v jednom z dvoch základných módov: *inter* alebo *intra*. Pri inter móde sa ďalej spracúva rozdiel dvoch snímok (po sebe idúcich alebo rozdiel vzhľadom na referenčnú). Snímky kódované v inter móde sa označujú symbolom P alebo B v závislosti od toho, či sa jedná o doprednú (P) alebo spätnú (B) predikciu. V intra móde je každý obrázok spracovaný nezávisle od ostatných (tieto snímky sa zvyknú označovať symbolom I). Pred konečným kódovaním sa snímka (alebo rozdiel snímok) rozdelí na bloky (zvyčajne veľkosti 8×8 bodov), ktoré sa spracujú diskrétnou kosínusovou transformáciou. Skupina za sebou idúcich snímok sa označuje ako *GOP* (Group of Pictures). Skupina je tvorená začiatočnou I snímkou. Za ňou môžu ísť P alebo B snímky. Počet snímok medzi dvoma I snímkami určuje dĺžku GOP. V štandarde MPEG sa táto veličina označuje symbolom N. Parameter M určuje vzdialenosť snímky P od I.

Na základe počiatočného obrázka typu I v GOP-e môže kodér odhadovať nasledujúci obrázok. Obrázky odhadované dopredu sa označujú ako tzv. P snímky. Tento typ snímok môže byť zdrojom pre nasledujúce P snímky. V štandardoch MPEG má kodér možnosť zvoliť okrem doprednej predikcie aj snímky, ktoré sa určujú spätnou predikciou. B snímky sa tvoria pomocou obojsmernej interpolačnej predikcie. Kodér zvolí, v akom pomere sa spraví priemer oboch predikcií a tento výsledok sa stane základom pre kompresiu podľa pravidiel kompresie P snímok. Počet použitých B snímok v GOP-e nie je nijak štandardom obmedzený. B snímky nie je možné použiť pre predikciu nasledujúcich (alebo predošlých) snímok. Tým je zaručené, že chyby spôsobené týmto kódovaním obrazu nebudú šírené ďalej.

V našej dizertačnej práci sme v kapitolách 3.1 až 3.5 bližšie opísali 5 rôznych techník vkladania informácie do videa. Jedná sa o techniky využívajúce kvantizátory, kódy s variabilnou dĺžkou slova alebo pohybové vektory používané na kódovanie rozdielov vzhľadom na referenčný snímok.

Žiadna z analyzovaných techník nevyužívala samotnú štruktúru multimediálneho kontajnera na prenos tajnej informácie. V našom výskume (kapitola 7 dizertačnej práce) sme sa preto zamerali na možnosť použiť na prenos údajov štruktúru nosiča nezávislú od obrazových dát.

Na stegoanalýzu steganografického systému pre obrázky typu BMP sme využili test dobrej zhody. Vo všeobecnosti sa dá popísať tento test nasledovne. Predpokladajme, že uskutočníme n krát experiment, ktorého výsledok môže nadobudnúť k rôznych hodnôt $\{h_1, \ldots, h_k\}$. Nech symbol Y_i označuje počet výskytov hodnoty h_i medzi realizovanými náhodnými pozorovaniami, pričom výsledok jedného po-

zorovania nemá vplyv na žiadne ďalšie. Ďalej nech p_i označuje očakávanú hodnotu pravdepodobnosti výskytu h_i. Hodnota

$$\chi^2 = \sum_{i=1}^{k} \frac{(Y_i - np_i)^2}{np_i} \tag{1}$$

označuje mieru, v akej sa líši pozorovaná veličina od očakávanej. Otázkou zostáva, ako interpretovať chybu H_0 prvého druhu, t.j. aká je pravdepodobnosť, že pozorovaná veličina s hodnotou χ^2 má rovnaké rozdelenie pravdepodobnosti ako veličina očakávaná. Toto sa zakladá na χ^2 rozdelení náhodnej premennej, keďže veličina χ^2 má v limitnom prípade charakter χ^2 rozdelenia s $k-1$ stupňami voľnosti. Od toho sa odvíja aj spôsob interpretácie konkrétnej hodnoty χ^2 testu.

Naším cieľom bolo určiť vhodnosť vybranej obdĺžnikovej oblasti O pre steganografické účely. Snažili sme sa určiť, do akej miery sa zmení štatistický profil oblasti po vložení správy. Na tento účel sme použíli χ^2 test, pomocou ktorého je možné zisťovať štatistické odchýlky oblastí pred a po vložení údajov.

Okrem testu dobrej zhody sme pri analýze steganografického systému v oblasti nekomprimovaného videa použili aj metódu skúmania histogramu vzhľadom na vzájomne zviazané páry hodnôt. Pri modifikovaní najmenej významných bitov nastáva situácia, keď sa hodnoty môžu meniť iba veľmi obmedzeným spôsobom. Vždy nastáva jav, pri ktorom sa hodnota buď nezmení, alebo sa zmení na druhú a táto druhá hodnota sa pri technike LSB môže zmeniť jedine na prvú. Takto vznikajú navzájom zviazané páry hodnôt. Uvedená situácia sa dá jednoduchým spôsobom využiť pre detegovanie použitia klasickej LSB metódy.

Aby nebolo možné využiť detekciu použitia LSB techniky, v steganografickom systéme využívajúcom na ukrytie informácie JPEG kompresiu sme použili kódovanie správy pomocou samoopravných kódov. Po zvážení teoretického modelu predstaveného v práci [87] sme pre náš steganografický systém použili Hammingov kód. Jeho implementácia je jednoduchá a veľmi efektívna (vzhľadom na potrebný výpočtový výkon). Takto pomocou $2^k - 1$ pôvodných bitov nosiča vieme vložiť k informačných bitov. Na to používame Hammingov kód charakteristiky $(2^k - 1,\, 2^k - k - 1)$, kde $k \geq 1$. Priemerný počet zmien v bloku o veľkosti $2^k - 1$ je potom daný vzťahom

$$h_k = \frac{1}{2^k}. \tag{2}$$

Efektivitou systému chápeme priemerný počet bitov správy, ktoré spôsobia zmenu jedného bitu v bloku originálneho nosiča o veľkosti $2^k - 1$ bitov. Určíme ju na základe vzťahu

$$e_k = \frac{s_k}{h_k} = \frac{k}{1 - 2^{-k}} \tag{3}$$

Pri vkladaní informácie do nosiča je nutné pre dosiahnutie najvyššej miery efektivity maximalizovať hodnotu parametra k. Ten je možné určiť na základe kapacity média a veľkosti vkladanej správy.

Aj keď je nami implementovaný steganografický systém v oblasti statických obrázkov typu JPEG odolný voči vyššie spomínaným útokom, podľa [31] možno

spoľahlivo určiť použitie vkladania (algoritmami triedy LSB) pomocou tzv. kalibračného útoku. Ten využíva koreláciu jednotlivých zložiek frekvenčného spektra v rámci všetkých blokov obrazu. Ak sa za počiatočný bod obrazu zvolí ľubovoľný bod, histogramy frekvenčného spektra cez všetky bloky obrazu by mali byť približne rovnaké. Ak však bola do obrazu vložená tajná informácia, histogramy pre pôvodný počiatočný bod obrazu sa budú líšiť od ostatných.

V dizertačnej práci sme v kapitole 7 navrhli využitie štruktúry mp4 súborov na prenos steganografickej informácie. Súborový formát mp4 je navrhnutý na uchovávanie rôznych údajových prúdov. Medzi najpoužívanejšie patria audio a video prúdy. Samotný kontajner (formát súboru) je podrobne špecifikovaný medzinárodným štandardom ISO14496-14. Všetky údaje v kontajneri sú organizované v tzv. atómoch. Na začiatku každého atómu sa nachádza jeho identifikátor a dĺžka [28]. Atómy sa môžu vnárať, takže jeden atóm môže obsahovať viacero iných. Atóm `mdat` obsahuje samotné bitové údajové prúdy, ktoré sa vzájomne striedajú. Kontainer mp4 bol navrhnutý s ohľadom na prenos v reálnom čase aj pomocou nízkokapacitných komunikačných kanálov. Preto pri ukladaní údajov využíva techniku časového multiplexu. Každému údajovému prúdu je vyhradený isté časové kvantum, a v rámci tohto má daný údajový prúd k dispozícii celú kapacitu pásma. Preto sa jednotlivé prúdy striedajú. Údaje, ktoré sa počas prideleného časového kvanta stihnú spracovať, tvoria tzv. *zhluky*. Zhluky môžu mať rozličné veľkosti a rôzny počet snímok.

Steganografický systém založený na zhlukoch kóduje informačné bity správy pomocou počtov snímok v jednotlivých zhlukoch. Zmena fyzického usporiadania údajov v kontajneri mp4 so sebou nesie nutnosť zmeny riadiacich a informačných štruktúr kontajnera. Tie sa nachádzajú v príslušných atómoch: `stts`, `stss`, `stsc`, `stsz` a `stco`. Túto techniku vkladania je možné použiť nielen pre video prúd, ale aj pre akýkoľvek iný obsiahnutý v multimediálnom kontajneri mp4.

S návrhom steganografických systémov súvisí veľká snaha o ich kompromitáciu. Hlavným nástrojom na určenie, či médium použité v obrazovom steganografickom systéme obsahuje skrytú správu, je sledovanie odchýlok od štatistických charakteristík podobných médií, ktoré správu neobsahujú. Inšpiratívnymi prácami pre experimenty v tejto oblasti boli [32] a predovšetkým [23].

Realizácia najjednoduchšieho porovnávania zhody dvoch nosičov je založená na výpočte sumy bitových rozdielov príslušných elementov. Toto porovnávanie je možné robiť nielen po bitoch, ale po ľubovoľných n-ticiach bitov. Výslednú sumu normalizujeme, a jej doplnok k jednotke považujeme za mieru zhody:

$$e = 1 - \frac{1}{2^n N} \sum_{i=1}^{N} |a_i - b_i|, \tag{4}$$

kde e je miera zhody, N počet porovnávaných prvkov, n veľkosť bitovej reprezentácie jedného prvku, a a b sú porovnávané nosiče.

Cieľom nášho výskumu nebolo navrhovať štatistické testy zhody médií. Tie sa účinne môžu robiť pre nosiče, kde je známa fyzická štruktúra a jej väzba na informačný tok. Napriek tomu sme navrhli rozšírenie triviálneho testu zhody, aby sme mohli experimentálne overiť nezávislosť testovaných algoritmov od použitého štatistického modelu.

Základnou myšlienkou návrhu je použitie lineárnej regresie na hľadanie miery zhody. Lineárna regresia spočíva vo vyjadrení závislosti prvej premennej od druhej na bodovom grafe [68]. Pre i–ty bit sa vynesie na graf bod so súradnicami (a_i, b_i), kde a a b sú porovnávávané médiá. Pri podobných poliach sú výsledkom body ležiace na diagonále. Všeobecne platí, že body budú ležat v blízkosti myslenej priamky, ktorá je určená rovnicou $a = \alpha + \beta * b$, kde α, β sú konštanty.

Problém nájdenia priamky je problémom nájdenia konštánt α a β. Na ich vyjadrenie sa používa metóda najmenších štvorcov:

$$\sum_{i=1}^{N} a_i = N * \alpha + \beta * \sum_{i=1}^{N} b_i \tag{5}$$

$$\sum_{i=1}^{N} a_i * b_i = \alpha * \sum_{i=1}^{N} b_i + \beta * \sum_{i=1}^{N} b_i^2, \tag{6}$$

kde α, β sú hľadané konštanty a a, b porovnávané médiá.

Po získaní lineárnej charakteristiky priamky je možné vyjadriť samotnú rozdielnosť. Na to sa používa výpočet odchýlky prvkov jednotlivých polí od získanej regresnej priamky:

$$e_i = \alpha + \beta * b_i - a_i \tag{7}$$

Priemerná odchýlka je daná vzťahom:

$$\overline{e} = \frac{\sum_{i=1}^{N} |e_i|}{N} \tag{8}$$

Nakoľko priemerná ochýlka môže nadobúdať hodnoty z rozsahu porovnávaných prvkov, normalizovaním sa získa hodnota, ktorej doplnok k jednotke je považovaný za odhad miery zhody:

$$e = 1 - \frac{1}{2^n N} \sum_{i=1}^{N} |e_i| \tag{9}$$

Na vyrovnanie sledovanej štatistiky steganografického média boli navrhnuté dva genetické algoritmy. Obidva vychádzajú z rovnakého modelu a líšia sa iba v použitom výbere (selekcii). Implementovaný model navyše využíva prekrývajúce sa populácie. V každej populácii umožňuje určiť množstvo jedincov, ktoré budú nahradené novými. Genetický algoritmus č. 1 používa na vytvorenie novej populácie turnajový výber, algoritmus č. 2 ruletový výber. Oba algoritmy majú rovnakú ukončovaciu podmienku, a to mieru konvergencie. Ak sa ohodnotenie nezlepšuje (v algoritme daný) istý počet populácií, výpočet končí.

Modul neurónových sietí je postavený na implementácii doprednej neurónovej sieti s jednou skrytou vrstvou. Implementovali sme dva typy sietí:

1. s 9 neurónmi na vstupe, 3 v skrytej vrstve a 1 na výstupe, a
2. s 5 neurónmi na vstupe, 4 v skrytej vrstve a 2 na výstupe.

Podobne, ako pri genetických algoritmoch, aj v prípade neurónových sietí je ukončovacou podmienkou nie počet opakovaní, ale miera zlepšovania výsledku. Vzhľadom na pamäťové nároky reprezentácie neurónovej siete sa sleduje posledných 30 modifikácií nastavenia váh.

Na ukážku a porovnanie s ostatnými modulmi boli implementované dva najjednoduchšie typy horolezeckého algoritmu: základná verzia a zjednodušená (v prípade zjednodušenej sa neprehľadávajú všetci susedia aktuálne najlepšieho riešenia, ale hľadanie končí po nájdení prvého lepšieho). Pri experimentoch nás zaujímal časový rozdiel behu jednotlivých verzií algoritmu, a taktiež efektivita meraná pomerom čas versus ohodnotenie nájdeného riešenia.

3 Dosiahnuté výsledky dizertačnej práce

Dizertačná práca dosiahla stanovené ciele. Podarilo sa nám analyzovať a implementovať štyri steganografické systémy. Počas nášho výskumu sme sa zaoberali steganografickými systémami založenými na:

- súborovom formáte BMP (kapitola 4 dizertačnej práce),
- nekomprimovanom video prúde (kapitola 5 dizertačnej práce),
- súborovom formáte JPEG (kapitola 6 dizertačnej práce),
- komprimovanom video prúde uchovávanom v multimediálnom kontajneri MP4 (kapitola 7 dizertačnej práce).

Táto následnosť návrhu a implementácie jednotlivých systémov nebola náhodná. Jednotlivé systémy na seba nadväzujú. Práca s nekomprimovaným videom predpokladala zvládnutie a pochopenie problematiky nekomprimovaných obrazových údajov. Manipulácia s komprimovaným video prúdom kódovaným v štandarde MPEG vyžaduje porozumenie JPEG kompresie. Napokon návrh steganografického systému založenom na komprimovanom videu v sebe zlučuje špecifické vlastnosti časovo závislého sledu obrázkov a zároveň poznatky z oblasti kódovania a stratovej JPEG kompresie.

V niektorých prípadoch (kapitoly 4.3 až 4.7, 5.3 a 5.4 dizertačnej práce) sme poukázali na limity a obmedzenia použitia steganografických systémov založených na modifikácii najmenej významných bitov nosiča. V iných prípadoch sme dôkladnejšie rozobrali štruktúru návrhu (celá kapitola 7 dizertačnej práce) a možnosti použitia stegoanalytických nástrojov na detegovanie použitia techník vkladania (kapitoly 6.2 až 6.5 dizertačnej práce).

V oblasti implementácie steganografických systémov založených na videu zatiaľ jestvuje iba niekoľko akademických špekulácií ohľadom možnosti využitia aj tohto typu nosiča na prenos správ. Preto sme sa v našej práci pokúsili ukázať možnosti praktickej realizácie takýchto systémov (kapitoly 5 a 7 dizertačnej práce). Zvlášť v oblasti komprimovaného videa (kapitola 7 dizertačnej práce) sme použili netradičný prístup, keď sme zamerali našu pozornosť na vlastnosti kontajnera uchovávajúceho informácie o samotnom videu; pričom na samotné vkladanie informácie nie je potrebné zasahovať do jeho kódovania.

Medzi doplnkové tézy dizertačnej práce patrí optimalizácia steganografických systémov pomocou techník umelej inteligencie a evolučných výpočtov. Tomu sme sa venovali v kapitole 8 dizertačnej práce. V nej sme sa zaoberali možnosťou optimalizácie steganografických systémov v zmysle zvyšovania odolnosti voci detegovaniu vloženia správy pomocou sledovania istých štatistík (kapitola 8.2 diz. práce) jednotlivých nosičov. Na tento účel sme implementovali model steganografického systému (kapitola 8.1 diz. práce), na ktorom sme realizovali experimentálne merania (kapitola 8.7 diz. práce) úspešnosti genetických algoritmov (kapitola 8.3 diz. práce), neurónových sietí (kapitola 8.4 diz. práce) a horolezeckého algoritmu (kapitola 8.5 diz. práce).

Ukázali sme, že v oblasti vyrovnávania sledovaných štatistík je najvýhodnejšie použiť genetické algoritmy. Použité dopredné neurónové siete s jednou skrytou vrstvou sú vhodnejšie na účely klasifikačných problémov, a horolezecký algoritmus v základnej verzii je z časového hľadiska neefektívny.

Literatúra

[1] J. Čapek and P. Fabian. *Komprimace dát, princípy a praxe.* Computer Press, Brno, 2000. ISBN 80-7226-231-9, pp. 186.

[2] M. Arnold, M. Schmucker, and S. Wolthusen. *Techniques and Applications of Digital Watermarking and Content Protection.* Artech House, London, 2003. ISBN 1-58053-111-3, pp. 274.

[3] I. Avcibas, B. Sankur, and K. Sayood. *Statistical evaluation of image quality measures*, volume 11, No. 2. J. Electron. Imaging, April 2002. pp. 206–223.

[4] J. Baroš. *Miera poškodenia videa po vložení na verejné úložisko anonymného zdieľania multimediálneho obsahu.* Slovenská technická univerzita, Bratislava, 2011. Diplomová práca, pp. 61.

[5] Friedrich L. Bauer. *Kryptology — Methods and Maxims*, volume 149/1983. Lecture Notes in Computer Science, Springer–Verlag, Berlin, January 1995. ISBN 978-3-540-11993-7, pp. 31–46.

[6] W. Bender. *Techniques for Data Hiding*, volume 35, No. 3-4. IBM Corp., Riverton, 1996. IBM Systems Journal, pp. 313–336.

[7] R. J. Berger and B. G. Mobasseri. *Watermarking in JPEG Bitstream.* SPIE Proc. on Security and Watermarking of Multimedia Contents III, San Jose, USA, Jan 2005.

[8] R. Blaško, M. Dubovský, B. Šulej, and T. Marko. *Návrh pomocných modulov steganografického systému.* Slovenská technická univerzita, Bratislava, 2010. Tímový projekt.

[9] U. Budhia, D. Kundur, and T. Zourntos. *Digital Video Steganalysis Exploiting Statistical Visibility in the Temporal Domain*, volume (1)4. IEEE Trans. Information Forensics and security, 2006. pp. 502–516.

[10] Christian Cachin. *An Information-Theoretic Model for Steganography*, volume 1525/1998. Springer, New York, January 1998. Parts of this paper appeared in Proc. 2nd Workshop on Information Hiding. ISBN 978-3-540-65386-8, pp. 306–318.

[11] R. Chandramouli, M. Kharrazi, and N. Memon. *Image steganography and steganalysis: Concepts and practice*, volume 2939/2004. Springer-Verlag, Berlin, February 2004. Digital Watermarking, 2nd International Workshop, IWDW 2003, Seoul, Korea. ISBN 978-3-540-21061-0, pp. 204–211.

[12] B. Chen, and G. W Wornell. *Quantization index modulation: a class of provably good methods for digital watermarking and information embedding*, volume 47(4). IEEE Transactions on Information Theory, 2001. pp. 1423—1443.

[13] D. Cinalli, B. G. Mobasseri, and C. O'Connor. *Metadata Embedding in Compressed UAV Video.* Intelligent Ship Symposium, Philadelphia, May 2003.

[14] R. Cinkais. *Detekce steganografie*, volume 6. HAKIN9, 2007. pp. 64–69.

[15] Eric Cole. *Hiding in Plain Sight — Steganography and the Art of Covert Communication*. Wiley John & Sons, New York, 2003. ISBN 0471444499.

[16] I. Cox, J. Fridrich, M. Miller, J. Bloom, and T. Kalker. *Digital watermarking and steganography*. Morgan Kaufmann, Massachusetts, 2008. ISBN 978-0-12-372585-1.

[17] D. L. Currie, and C. E. Irvine. *Surmounting the effects of lossy compression on Steganography*. Conference paper, October 1996.

[18] Y. J. Dai, L. H. Zhang, and Y. X. Yang. *A New Method of MPEG Video Watermarking Technology*, volume 2. International Conference on Communication Technology Proceedings (ICCT 2003), April 2003. pp. 11845–1847.

[19] K. A. DeJong, and W. M. Spears. *An Analysis of the Interacting Roles of Population Size and Crossover in Genetic Algorithms*. Springer-Verlag, Berlin, 1990. Proc. First Workshop Parallel Problem Solving from Nature, pp. 38–47.

[20] DevX. Graphics technical options and decisions. Dostupné elektronicky na `http://www.devx.com.projectcool/Article/19997`, January 2000. Sprístupnené 2. 11. 2009.

[21] Michal Dobeš. *Zpracování obrazu a algoritmy v C#*. Ben, Praha, 2008. ISBN 9788073002336.

[22] S. Dumitrescu, X. L. Wu, and Z. Wang. *Detection of LSB Steganography via Sample Pair Analysis*, volume 2578. Springer-Verlag, Berlin Heidelberg New York, 2002. Petitcolas, F.A.P. (ed.): Information Hiding 5th International Workshop, pp. 355–372.

[23] Nameer N. EL-Emam. *Hiding a Large Amount of Data with High Security Using Steganography Algorithm*, volume 3. Spring, 2007. Journal of Computer Science, ISSN 1549-3636, pp. 223–232.

[24] G. El Loco. A few tools to discover hidden data. Dostupné elektronicky na `http://www.guillermito2.net/stegano/tools/index.html`. Sprístupnené 07. 07. 2011.

[25] G. El Loco. Analyzing steganography softwares. Dostupné elektronicky na `http://www.guillermito2.net/stegano`, 2004. Sprístupnené 04. 04. 2010.

[26] G. C. Langelaar et al. *Watermarking Digital Image and Video Data*, volume 17, No. 5. IEEE Signal Processing Magazine, Sept 2000. pp. 20—46.

[27] H. Farid, and L. Siwei. *Detecting Hidden Messages Using Higher-Order Statistics and Support Vector Machines*, volume 2578. Springer-Verlag, Berlin Heidelberg New York, 2002. Petitcolas, F.A.P. (ed.): Information Hiding 5th International Workshop, pp. 340–354.

[28] P. Fernando, and T. Ebrahimi. *The MPEG-4 book*. Upper Saddle River, NJ, Prentice Hall PTR, 2002. ISBN 0-13-061621-4.

[29] J. Fridrich, R. Du, and L. Meng. *Steganalysis of LSB Encoding in Color Images*. Proceedings IEEE International Conference on Multimedia and Expo, New York City, NY, July 30 - August 2 2000. pp. 907–918.

[30] J. Fridrich, and M. Goljan. *Practical Steganalysis of Digital Images —- State of the Art*, volume 4675. In Delp III, Security and Watermarking of Multimedia Contents IV, New York City, NY, 2002. pp. 1–13.

[31] J. Fridrich, M. Goljan, and D. Hogea. *Steganography of JPEG images: Breaking the F5 algorithm*. Springer-Verlag, Berlin Heidelberg, 2003. Information Hiding (5th International Workshop 2002), LNCS 2578, pp. 310—323.

[32] Jessica Fridrich. *Feature-Based Steganalysis for JPEG Images and its Implications for Future Design of Steganographic Schemes*. Springer-Verlag, Berlin Heidelberg, 2004. 6th Information Hiding Workshop, pp. 67–81.

[33] J.J. Grefenstette. *Optimization of Control Parameters for Genetic Algorithms*, volume SMC-16, No. 1. Jan/Feb 1986. IEEE Trans. Systems, Man, and Cybernetics, pp. 122–128.

[34] O. Grošek, M. Vojvoda, and R. Krchnavý. *A New Matrix Test for Randomness*, volume 85. Computing, 2009. ISSN 0010-485X, pp. 21–36.

[35] J. Harmsen, and W. Pearlman. *Steganalysis of additive noise modelable information hiding*, volume 5022. Proc. SPIE Security and Watermarking of Multimedia Contents V, Santa Clara, CA, January 2003.

[36] J. J. Harmsen, and W. A. Pearlman. *Capacity of steganalysis channels*. Proceedings of the 7th Workshop on Multimedia and Security, New York, 2005. ISBN 1-59593-032-9, pp. 11–24.

[37] F. Hartung, and B. Girod. *Watermarking of uncompressed and compressed video*, volume 66(3). Signal Processing, Special Issue on Copyright Protection and Access Control for Multimedia Services, 1998. pp. 283–301.

[38] S. Haykin. *Neural Networks – A Comprehensive Foundation*. Prentice Hall, New Jersey, 2 edition, 1998. ISBN 978-0132733502.

[39] R. Hecht-Nielsen. *Neurocomputing*. Addison-Wesley Publishing Company, Massachusetts, 1990. ISBN 978-0201093551.

[40] Josef Hynek. *Genetické algoritmy a genetické programování*. Grada Publishing, Praha, 2008. ISBN 978-80-247-2695-3, pp. 200.

[41] J. S. Jainsky, D. Kundur, and D. R. Halverson. *Towards Digital Video Steganalysis using Asymptotic Memoryless Detection*, volume (1)4. MM&Sec'07, Dallas, Texas, USA, September 20-21 2007.

[42] M. Jókay. *The design of a steganographic system based on the internal MP4 file structures*. International Journal of Computers and Communications, 2011. Preprint, pp. 8.

[43] M. Jókay, and J. Baroš. *On the suitability of the internet multimedia storage for steganographic information transfer in MP4 files*. Kybernetika, 2011. Preprint, pp. 14.

[44] N. F. Johnson, and S. Jajodia. *Steganalysis of Images Created Using Current Steganography Software*, volume 1525. Springer-Verlag, Oregon, April 1998. Proceedings of the 2nd International Workshop on Information Hiding, ISBN 3-540-65386-4, pp. 273–289.

[45] S. Katzenbeisser, and Fabien Petitcolas. *On defining security in steganographic systems*, volume 4675. Society of Photo-Optical Instrumentation Engineers, Bellingham, January 2002. SPIE proceeding series. ISBN 0-8194-4415-4, pp. 50–56.

[46] M. Kharrazi, H. T. Sencar, and N. Memon. Cover selection for steganographic embedding. Dostupné elektronicky na `http://sharif.edu/ kharrazi/pubs/icip06.pdf`, 2006. Sprístupnené 28. 10. 2009.

[47] Greg Kipper. *Investigator's Guide to Steganography*. Auerbach Publications, Boka Raton, 2004. ISBN 0849324335.

[48] V. Kvasnička. *Úvod do teórie neurónových sietí*. Iris, Bratislava, 1997. ISBN 80-88778-30-1.

[49] V. Kvasnička, J. Pospíchal, and P. Tiňo. *Evolučné algoritmy*. Vydavateľstvo STU, Bratislava, 2000. ISBN 80-227-1377-5.

[50] G. C. Langelaar, and R. L. Lagendijk. *Optimal Differential Energy Watermarking of DCT Encoded Images and Video*, volume 10(1). IEEE Transactions on Image Processing, 2001. pp. 148–158.

[51] B. Liu, F. Liu, Ch. Yang, and Y. Sun. *Secure Steganography in Compressed Video Bitstreams*. The Third International Conference on Availabity, Reliability and Security (ARES 08), March 4-7 2008. DOI 10.1109/ARES.2008.140. ISBN 978-0-7695-3102-1, pp. 1382–1387.

[52] H. H. Liu, and L. W. Chang. *Realtime digital video watermarking for digital rights management via modification of VLCs*. Proceedings of the 11th International Conference on Parallel and Distributed Systems (ICPADS'05), 2005.

[53] X. Liu, F. Liu, B. Lu, and X. Luo. *Real-Time Steganography in Compressed Video*. Proceedings of MRCS 2006, LNCS 4105, Springer-Verlag, Aug 2006. pp. 43–48.

[54] C. S. Lu, J. R. Chen, and K. C. Fan. *Real-time framedependent video watermarking in VLC domain*, volume 20. Signal Processing: Image Communication, 2005. pp. 624–642.

[55] B. G. Mobasseri, and M. P. Marcinak. *Watermarking of MPEG-2 Video in Compressed Domain Using VLC Mapping*. ACM Multimedia and Security Workshop 2005, New York, NY, Aug 2005.

[56] T. Moravčík. *Steganografia v obrazovom súbore JPG*. Slovenská technická univerzita, Bratislava, 2010. Diplomová práca.

[57] J. D. Murray, and W. van Ryper. *Encyklopedie grafických formátøu*, volume 6. Computer Press, druhé vydanie edition, 1997. ISBN 80-7226-033-2.

[58] Nvidia. Developer's zone. Dostupné elektronicky na `http://http://developer.nvidia.com/category/zone/cuda-zone`, 2011. Sprístupnené 11. 07. 2011.

[59] Jan Ondruš. *Bezstrátová komprese JPEG grafiky*. Karlova Univerzita, Praha, 2009. Diplomová práca, pp. 40.

[60] M. Oravec, J. Polec, and S. Marchevský. *Neurónové siete pre číslicové spracovanie signálov*. Faber, Bratislava, 1998. ISBN 80-967503-9-9.

[61] Fernando Perez-Gonzales, and Juan Hernandez. A tutorial on digital watermarking. Dostupné elektronicky na `http://www.gts.tsc.uvigo.es/gpsc/publications/wmark/carnahan99.pdf`. Sprístupnené 11. 05. 2009.

[62] Fabien Petitcolas. Stirmark benchmark 4.0. Dostupné elektronicky na `http://www.cl.cam.ac.uk/~fapp2/watermarking/stirmark`, 20. September 2008. Sprístupnené 20. 05. 2009.

[63] J. Polec, J. Pavlovičová, and T. Karlubíková. *Medzinárodné štandardy pre kompresiu obrazu II*. Slovenská technická univerzita, Bratislava, 2001. ISBN 80-227-1784-3.

[64] B. Rainer. *Advanced statistical steganalysis*. Springer-Verlag, Berlin, 2010. ISBN 978-3-642-14312-0, pp. 285.

[65] Radovan Ridzoň. *Invariantné metódy digitálnej vodotlače v statických obrazoch*. Dizertačná práca, Technická univerzita, Košice, 2007. Odbor Telekomunikácie.

[66] P. Šrámek. *Steganografický systém s použitím hill-climbing algoritmov*. Slovenská technická univerzita, Bratislava, 2011. Záverečná práca.

[67] N. Rougier. Biological neuron schema. Dostupné elektronicky na `https://commons.wikimedia.org/wiki/File:Neuron-figure.svg`, June 2007. Sprístupnené 13. 8. 2011.

[68] Martin Rusnák. Regresná analýza. Dostupné elektronicky na `http://www.healthnet.sk/texts/statistika/regresia/regresia.htm`. Sprístupnené 21. 06. 2011.

[69] P. Sallee. *Model-based steganography*. Springer-Verlag, Berlin Heidelberg, 2004. International Workshop on Digital Watermarking (IWDW 2003), LNCS 2939, pp. 154—167.

[70] A. Sarkar, U. Madhow, S. Chandrasekaran, and B. S. Manjunath. *Adaptive MPEG-2 Video Data Hiding Scheme*, volume 6505. Security, steganography, and watermarking of multimedia contents No9, San Jose CA, 2007. pp. 65051D.1–65051D.9.

[71] Caspar Schott. *Schola steganographia*. Jobus Hertz, Norimberg, 1665.

[72] Ivan Sekaj. Genetické algoritmy — prednášky. Dostupné elektronicky na `http://www.kasr.elf.stuba.sk/index.php?go=studij_mat`, 2010. Sprístupnené 21. 05. 2010.

[73] XRCE TeXnology Showroom. Digital watermarking in printed images. Dostupné elektronicky na `http://www.xrce.xerox.com/showroom/fs/stochas.pdf`. Sprístupnené 11. 05. 2009.

[74] MSSG: Free MPEG software. Chapter on rate control and quantization control. Dostupné elektronicky na `http://www.mpeg.org/MPEG/MSSG/tm5/Ch10/Ch10.html`. Sprístupnené 3. 3. 2011.

[75] K. Solanki, N. Jacobsen, U. Madhow, B. S. Manjunath, and S. Chandrasekaran. *Robust image-adaptive data hiding based on erasure and error correction*, volume 13. IEEE Trans. on Image Processing, December 2004. pp. 1627–1639.

[76] D. Sovič. Kompresný štandard jpeg. Dostupné elektronicky na `http://www.pakuj.host.sk/jpeg/jpeg.html`, 2009. Sprístupnené 04. 04. 2010.

[77] K. Su, D. Kundur, and D. Hatzinakos. *Statistical invisibility for collusionresistant digital video watermarking*, volume (7)1. IEEE Trans. Multimedia, 2005. pp. 43–51.

[78] Ioannes Trithemius. *Polygraphiae libri sex*. Ioannes Birckmannus & Theodorus Baumius, Cologne, 1586.

[79] Gregory K. Wallace. *The JPEG Still Picture Compression Standard*, volume 34. ACM, New York, April 1991. Communications of the ACM, ISSN 0001-0782, pp. 30–44.

[80] A. Westfeld. *F5–A Steganographic Algorithm*, volume 2137. Proceedings of 4th International Conference on Informatio Hiding, Springer-Verlag, 2001. pp. 289–302.

[81] A. Westfeld, and A. Pfitzmann. *Attacks on Steganographic Systems*. Springer-Verlag, Berlin Heidelberg, 1999. Information Hiding, Third International Workshop, IH'99, Dresden, Germany, September/October, 1999, Proceedings, LNCS 1768, pp. 61–76.

[82] C. Xu, X. Ping, and T. Zhang. *Steganography in Compressed Video Stream*. Proceedings of the First International Conference of Innovative Computing, Information and Control, 2006. ISBN 0-7695-2616-0.

[83] D. P. Ye, C. F. Zou, Y. W. Dai, and Z. Q. Wang. *New adaptive watermarking for real-time MPEG videos*, volume 185. Applied Mathematics and Computation, 2007. pp. 907–918.

[84] Zuzana Zeťáková. Genetické algoritmy i. Dostupné elektronicky na `http://neuron-ai.tuke.sk/ãrvayova/bk`. Sprístupnené 23. 05. 2010.

[85] J. Zhang, J. Li, and L. Zhang. *Video Watermark Technique in Motion Vector*. Proceedings of XIV Brazilian Symposium on Computer Graphics and Image Processing, 2001. pp. 179–182.

[86] W. Zhang, X. Zhang, and S. Wang. *Maximizing Steganographic Embedding Efficiency by Combining Hamming Codes and Wet Paper Codes*. Springer-Verlag, 2008. Information Hiding, 10th International Workshop, pp. 60–71.

5 Zoznam publikácii a citácií

5.1 Publikované výsledky dizertačnej práce

Jókay, M., and Moravčík, T. Image-Based JPEG Steganography. In *Tatra Mountains Mathematical Publications.* ISSN 1210-3195. Vol. 45 : NILCRYPT '10 (2010), 65–74.

Jókay, M., and Moravčík, T. Steganografia v obrazovom súbore JPEG. In *EE časopis pre elektrotechniku a energetiku.* ISSN 1335-2547. Roč. 16, mimoriadne číslo (2010), 36–40.

Jókay, M. The Design of a Steganographic system Based on the GOP Structure in the Video Standard MPEG-4. In *Recent Researches in Computers and Computing.* International Conference on Computers and Computing (ICCC'11). Lanzarote, Spain, 27.-29.5.2011. WSEAS Press, 2011. ISBN 978-1-61804-000-8, 95–99.

Jókay, M., and Zajac, P. Analysis of Data Structures in MP4 Files Usable for Steganography. In *ISCAMI 2011.* Malenovice, Czech Republic, 6.-8.5.2011. University of Ostrava, 2011.

Jókay, M. On the suitability of the Internet multimedia storage for steganographic information transfer in MP4 files. Submited to: *Kybernetika*, 2011.

Jókay, M. The design of a steganographic system based on the internal MP4 file structures. Submited to: *International Journal of Computers and Communications*, 2011.

5.2 Ostatné práce

Adamko, L., Vojvoda, M., and Jókay, M. Statistical Analysis of ECRYPT eSTREAM Phase3 Ciphers. In: *EE časopis pre elektrotechniku a energetiku.* ISSN 1335-2547. Roč. 14, mimoriadne číslo (2008), pp. 193–196.

Jókay, M., and Moravčík, T. Image-Based JPEG Steganography. In: *Tatra Mountains Mathematical Publications.* ISSN 1210-3195. Vol. 45 : NILCRYPT '10 (2010), pp. 65–74.

Jókay, M., and Moravčík, T. Steganografia v obrazovom súbore JPEG. In: *EE časopis pre elektrotechniku a energetiku.* ISSN 1335-2547. Roč. 16, mimoriadne číslo (2010), pp. 36–40.

Kostrecová, E., Jókay, M., and Kostrec, M. Počítačová kriminalita. 1. vyd., Bratislava : STU v Bratislave, 2011. 109 s. ISBN 978-80-227-3410-3.

Antal, E., and Jókay, M. Rotorový šifrátor Fialka M-125. Diel 1. Popis šifrátora. In: *Crypto-World.* ISSN 1801-2140. Roč. 13, č. 4 (2011), s. 18–27.

Jókay, M., and Antal, E. Rotorový šifrátor Fialka M-125. Diel 2. Porovnanie s viacerými rotorovými šifrátormi. In: *Crypto-World.* ISSN 1801-2140. Roč. 13, č. 5 (2011), s. 15–23.

Antal, E., and Jókay, M. Rotorový šifrátor Fialka M-125. Diel 3. Vybrané vlastnosti šifry. In: *Crypto-World.* ISSN 1801-2140. Roč. 13, č. 6 (2011), s. 23–32.

Spoluautor 12 technických správ pre NBÚ SR, ktoré podliehajú utajeniu podľa zákona č. 215/2004 Z.z.

5.3 Príspevky na konferenciách

Jókay, M., and Zajac, P. Advances in the Matrix Test Precomputation. In: *Proceedings.* 1st Plenary Conference of the NIL-I-004 Development of Norwegian-Slovak Cooperation in Cryptology : Bergen, Norway, 24.-27.8.2009. Bratislava : STU, 2009. ISBN 978-80-227-3230-7, pp. 1–6.

Jókay, M. The Design of a Steganographic system Based on the GOP Structure in the Video Standard MPEG-4. In: *Recent Researches in Computers and Computing.* International Conference on Computers and Computing (ICCC'11). Lanzarote, Spain, 27.-29.5.2011. WSEAS Press, 2011. ISBN 978-1-61804-000-8, pp. 95–99.

Vojvoda, M., Sýs, M., and Jókay, M. A Note on Algebraic Properties of Quasigroups in Edon80. In: *SASC 2007.* The State of the Art of Stream Ciphers : Workshop. Bochum, Germany, 31.1.-1.2.2007. Bochum : ECRYPT Network of Excelence in Cryptology, 2007, pp. 307–315.

Adamko, L., Jókay, M., and Vojvoda, M. Statistical Analysis of ECRYPT eSTREAM Profile 1 Stream Ciphers. In: *ELITECH ´08 : PhD Students Conference.* Bratislava, Slovak Republic, 20.5.2008. STU v Bratislave, 2008. ISBN 978-80-227-2878-2.

Jókay, M., and Vojvoda, M. Distributed System for Files Decryption. In: *8th International Symposium on Forensic Sciences.* Šamorín-Čilistov, Slovak Republic, 26.-29.9.2007. Bratislava : KEUPZ, 2008. ISBN 978-80-969471-2-6, pp. 31–40.

Jókay, M., and Zajac, P. Parallelization Techniques for the Matrix Test Precomputation. In: *5th International Workshop on Grid Computing for Complex Problems.* GCCP 2009 : Bratislava, Slovak Republic, 26.-28.10.2009, 2009, pp. 103–109.

Jókay, M. Remarks on the GRID Computation of the Characteristics of Boolean Matrices. In: *GCCP 2010 Proceedings : 6th International Workshop on Grid Computing for Complex Problems.* Bratislava, Slovakia, November 8-10, 2010, pp. 57–63.

5.4 Citácie

Hell M., and Johansson T. A Key Recovery Attack on Edon80. In: *Advances in Cryptology.* Asiacrypt, 2007, pp. 568–581.

Daniel J. Bernstein. Which eSTREAM ciphers have been broken? In: *eSTREAM report 2008/010.*

Gligoroski D., Markovski S., and Knapskog S. J. The Stream Cipher Edon80. In: *New Stream Cipher Designs: The eSTREAM Finalists LNCS 2008.* Vol. 4986, 2008, pp. 152–169.

Summary

This thesis deals with the steganography in the area of static images and video. In the first chapter we focused on the steganography in general terms. The second and third chapters deal with the image and video based steganography. We present the basic method of data insertion in this areas.

After explanation of basic notions in steganography, the attention is focused on the design and analysis of the four steganographic systems based on:

- uncompressed BMP image file (chapter 4),
- uncompressed RAW AVI video file (chapter 5),
- compressed JPEG image file (chapter 6), and
- compressed video stored in the MP4 multimedia container (chapter 7).

Systems based on uncompressed data use the least significant bit (LSB) modification method in the spatial domain of the used color model. The system designed for the JPEG compression algorithm uses the modification of the least significant bits of the DCT coefficients in connection with the Huffman encoding. The system based on the MP4 file format uses the internal structure GOP of the video encoded by the MPEG family standards. Moreover, it modifies the structure of the data storage in the MP4 container.

The last part of the thesis (chapter 8) contains experimental results. Our goal was to balance the statistics of the carrier affected by the embedded hidden message. The comparison is provided for the genetic algorithms, neural networks, and the hill-climbing algorithm, respectively.