Portál pre odborné publikovanie ISSN 1338-0087

Obrazová stegoanalýza v DWT oblasti

Palko Tomáš · Informačné technológie, MATLAB/Comsol

20.05.2015

Tento príspevok je venovaný detekcie tajnej správy v statických obrazoch, čo je realizované stegoanalýzou v transformovanej DWT oblasti. Navrhnutá bola metóda stegoanalýzy, ktorá využíva diskrétnu waveletovú transformáciu a extrakciu 46 štatistických parametrov z obrazových súborov. Na trénovanie a klasifikáciu je využitý algoritmus podporných vektorov (SVM) s lineárnou kernel funkciou. Programová realizácia navrhnutej metódy bola realizovaná v prostredí MATLAB a následne tento algoritmus bol verifikovaný z hľadiska úspešnosti detekcie tajnej správy v obrazových dátach.

Úvod

Stegoanalýza spolu so steganografiou sa v súčasnom modernom svete stávajú oveľa dôležitejšou, ako tomu bolo v minulosti, kedy ich hlavné využitie spočívalo hlavne vo vojenskej sfére. Denno denne prichádzame do styku s digitálnymi médiami, ale máloktorí z nás sa zamyslia nad tým, že obyčajná fotografia môže obsahovať aj niečo viac, ako len peknú spomienku na dovolenku. Práve tu prichádza na rad stegoanalýza, ako vedná disciplína, ktorá skúma prítomnosť ďalších informácii ukrytých v médiách. Existuje nespočetné množstvo steganografických algoritmov a k nim prislúchajúcich metód stegoanalýzy. Väčšina z nich však v prípade transformovanej oblasti využíva DCT transformáciu. Práve menšie množstvo metód založených na DWT transformácií dalo námet na vznik tohto príspevku.

1. Steganografia a stegoanalýza

Steganografia a stegoanalýza sa ako vedné disciplíny začali výraznejšie presadzovať až v 90.-tych rokoch. Všeobecná definícia steganografie tvrdí, že všetci účastníci komunikujú tak, aby existenciu správy nebolo možné odhaliť. Na rozdiel od kryptografie, ktorá sa snaží zachovať dôvernosť obsahu správy, steganografia pridáva vrstvu utajenia tým, že utajuje vlastnú existenciu komunikácie. Cieľom je teda zaručenie nedetekovateľnosti. Z definície steganografie ako bezpečnostnej techniky vyplýva, že jej hodnotenie kvality nie je možné vykonať bez vyjadrenia, ako ťažká, zložitá je detekcia prítomnosti tajnej správy. Toho výsledkom je, že pokrok v steganografii je úzko spätý s vyspelosťou stegoanalýzy, vednej disciplíny ktorá sa zaoberá detekciou tajnej správy. Tieto dva aspekty sa nedajú skúmať oddelene.

1.1 Steganalytický systém

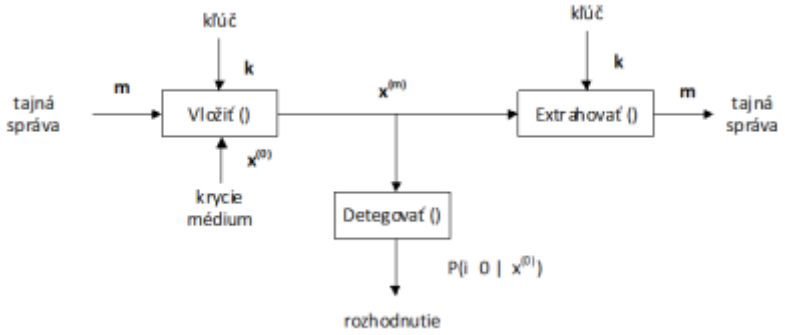
Bezpečnosť steganografického systému je definovaná ako jeho odolnosť voči detekcii. Snaha o detekciu prítomnosti tajnej správy sa nazýva stegoanalýza. Predpokladá sa, že stagaoanalytik má prístup k prenosovému kanálu a hľadá v ňom podozrivú komunikáciu. Metóda steganografie je považovaná za prelomenú, ak pravdepodobnosť detekcie pomocou stegoanalytickej metódy je vyššia ako náhodné hádanie.

1.2 Prístupy v stegoanalýze

Z pohľadu bezpečnosti, môžeme definovať dva typy útočníkov na komunikačný kanál a to pasívny a aktívny útočník. V analógii s tým, pre stegoanalýzu definujeme pasívneho a aktívneho pozorovateľa.

1.2.1 Pasívny pozorovateľ

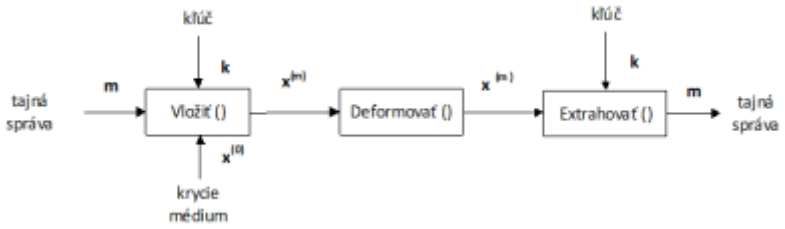
Pasívny pozorovateľ je steganalytik, ktorý nezasahuje do obsahu komunikačného kanála. Cieľom steganalytika je správne identifikovať existenciu tajnej správy pomocou funkcie Detegovať, ktorej výstupom je metrika na rozhodovanie či médium x(i) je možné považovať za stego médium alebo nie (Obr. 1).



Obr. 1 Bloková schéma – Pasívny pozorovateľ

1.2.2 Aktívny pozorovateľ

V prípade aktívneho pozorovateľa, steganalytik má prístup na čítanie ale aj na zápis do komunikačného kanálu. Cieľom útočníka je zabrániť tajnej komunikácii prípadne ju obmedziť znížením kapacity kanála. Môžeme to modelovať funkciou Deformovať v komunikačnom kanáli na Obr. 2. Systematická deformácia s cieľom znehodnotiť stego objekt môže tiež nepriaznivo ovplyvniť schopnosť komunikačného kanála prenášať informácie.



Obr. 2 Bloková schéma – aktívny pozorovateľ

2.3 Delenie metód stegoanalýzy

Steganalytické metódy môžeme vo všeobecnosti rozdeliť do dvoch hlavných tried. Stegoanalýza na základe modelov a štatistickú stegoanalýzu. Navrhované delenie je

založené na skutočnosti, či sa klasifikáciu prítomnosť tajnej informácie vloženej steganografickou metódou použijú príznaky steganografickej metódy alebo štatistické vlastnosti obrazov. Podtriedy sú následne delené podľa toho, či konkrétna steganalytická metóda je zameraná na detekciu jednej (špecifická stegoanalýza), prípadne viac steganografických metód (univerzálna stegoanalýza) [2].

3. Diskrétna waveletová transformácia (DWT)

Diskrétna waveletová transformácia sa stala veľmi obľúbeným nástrojom, ktorý sa používa pri spracovaní signálu a obrazu. V oblasti steganografie ponúka širokú škálu možností pre ukrývanie a prenos tajnej správy. Pri spracovaní obrazu zvyčajne využívame tzv. 2D DWT. Jedno-úrovňovú 2D DWT dekompozíciu obrazu získame tak, že najskôr na vstupný obraz, ktorý predstavuje maticu čísel, aplikujeme 1D DWT po riadkoch čím získame subpásma L, ktoré obsahuje nízke frekvencie a H, ktoré obsahuje vysoké frekvencie pre každý riadok. Následne zopakujeme postup pre každý stĺpec. Uvedeným postupom získame štyri subpásma : aproximačné LL, horizontálne LH, vertikálne HL, diagonálne HH tak ako je to znázornené na Obr. 3. Ak si označíme riadky ako x a stĺpce ako y tak môžeme povedať, že subpásmo LL zodpovedá aplikácii horno-priepustného filtra v x aj y smere, subpásmo HL zodpovedá aplikácii horno-priepustného filtra v x smere a dolno-priepustného filtra v y smere, subpásmo LH zodpovedá aplikácii horno-priepustného filtra v y smere a dolno-priepustného filtra v x smere a subpásmo LL zodpovedá aplikácii dolno-priepustného filtra v x aj y smere [3].

Obr. 3 Jedno – úrovňová 2D DWT dekompozícia obrazu

Aplikácia dvoj-úrovňovej 2D DWT na vstupný obraz je znázornená na Obr. 4. Aplikovaním 1D DWT na subpásmo LL získame ďalšie štyri subpásma (LL2, HL2, LH2, HH2). Pre získanie n-úrovňovej 2D DWT musíme rozkladať subpásmo LLn.

Obr. 4 Dvoj – úrovňová 2D DWT dekompozícia obrazu

4. Navrhnutá metóda stegoanalýzy

Ako námet pre navrhnutú metódu stegoanalýzy poslúžili metódy priblížené v [4][5]. Autori v [4] využili parametre extrahované z obrazov tak z priestorovej oblasti a rovnako aj z DWT domény. Z každej zložky n-úrovňovej waveletevej dekompozície obrazu boli extrahované štyri charakteristické štatistické parametre vyššieho rádu, a to stredná hodnota, odchýlka, špicatosť a šikmosť. Ako ďalšie parametre pri návrhu poslúžili chybové koeficienty lineárneho prediktora dekompozície obrazu, entropia a energia obrazu. Následne tieto parametre boli využité na trénovanie SVM

klasifikátora, ktorý je detailne popísaný v [6].

Algoritmus podporných vektorov (Support Vector Machines – SVM) je metóda strojového učenia určená na binárnu klasifikáciu. Základnou myšlienkou je nájsť hyperrovinu, ktorá oddeľuje n-rozmerné dáta práve do dvoch tried (v našom prípade obrazy s tajnou správou a bez tajnej správy). Avšak, niekedy nie sú vstupné dáta lineárne separovateľné. Pre ten prípad SVM zavádza pojem kernelom indukovaného priestoru parametrov, ktorá rozdelí vstupné dáta do viacrozmerného priestoru, kde sú opäť separovateľné. Na extrakciu parametrov sme využili dvojrozmernú Haarovú DWT dekompozíciu obrazu tretej úrovne. Vi(x,y), Hi(x,y) a Di(x,y) predstavujú dekompozičné koeficienty obrazu vo vertikálnom, horizontálnom a diagonálnom smere, Ai(x,y) predstavuje detailový koeficient konkrétnej úrovne.

4.1 Štatistický vektor

Pre naše potreby sme navrhli vektor štatistických parametrov o dĺžke 46 prvkov. Vektor pozostáva z koeficientov extrahovaných z testovaných obrazov. Prvým prvkom vektora je entropia obrazu pred DWT dekompozíciou. Nasledujúcich 36 koeficientov tvoria štatistické parametre pre každý smerový koeficient dekompozície. Posledných 9 koeficientov tvoria hodnoty chybových signálov. Rozloženie prvkov je znázornené na obrázku:

Entropia	E(H1)	Var(H1)	S(H1)	K(H1)	E(V1)	Var(V1)	...	K(H3)	MSE(A1-H1)	MSE(A1-V1)	...	MSE(A3-D3)

Obr. 5 Rozloženie koeficientov v štatistickom vektore

4.1.1 Entropia obrazu

Majme náhodnú množinu $\{X_i, i=1,2, \dots , N\}$, jej pravdepodobnosť pi, ktorá spĺňa podmienku

$$\sum_{i=1}^{N} p_i = 1, \quad 0 \leq p_i \geq 1, i = 1, \dots, N \tag{1}$$

Shannonova definícia entropie je :

$$H(p_1, p_2, \dots, p_N) = \sum_{i=1}^{N} p_i log_2 p_1 \tag{2}$$

Informačná entropia je miera úrovne chaosu informácie. Digitálne obrazy pozostávajú z obrazových bodov rôznej úrovne jasu ktoré sú rozložené v rôznych oblastiach obrazu. Rôzne obrazové prvky formujú rôzne tvary a rôzne tvary obsahujú rôzne množstvo informácie. Entropia obrazu reflektuje informačný obsah dvojrozmerného digitálneho 256 úrovňového obrazu, a tiež jej rozloženie úrovní. Rozdiely v obrazovej entropii zodpovedajú vizuálnym rozdielom medzi obrazmi. Steganografia pri vkladaní informácie mení rozdelenie pravdepodobnosti obrazových prvkov a tiež informáciu o farbe. Čím viac informácie je ukryté v obraze, tým väčší bude vplyv aj na entropiu. Entropia je prvý parameter vektora štatistických parametrov, ktoré sme počítali z krycích aj cover obrazov [4].

4.1.2 Charakteristické parametre

V každej úrovni DWT dekompozície sa vypočítali štyri parametre, a to strednú hodnotu, rozptyl, šikmosť, špicatosť pre horizontály, vertikálny aj diagonálny koeficient konkrétnej úrovne DWT. Tieto parametre sú definované nasledovne:

Stredná hodnota:

$$E(x) = \frac{1}{n}\sum_{k=1}^{n} x_k \tag{3}$$

Rozptyl:

$$Var(x) = \frac{1}{n-1}\sum_{i=1}^{n}(x_i - E(x))^2 \tag{4}$$

Šikmosť:

$$S(x) = E\left[\left(\frac{x-E(x)}{\sqrt{Var(x)}}\right)^3\right] \tag{5}$$

Špicatosť:

$$S(x) = K(x)\left[\left(\frac{x-E(x)}{\sqrt{Var(x)}}\right)^4\right] \tag{6}$$

Takto sme získali 4x 3 x 3, teda 36 ďalších prvkov nášho štatistického vektora [4].

4.1.3 Stredná kvadratická odchýlka

Stredná kvadratická odchýlka (MSE) vo všeobecnosti je mierou vernosti reprodukcie signálu. Cieľom tejto miery je porovnať dva signály a poskytnúť kvantitatívne ohodnotenie, ktoré opisuje mieru podobnosti/vernosti alebo naopak chyby/skreslenia medzi dvoma signálmi. Predpokladajme, že x={X_i, i=1,2, … , N}, a y={y_i, i=1,2, … , N} sú dva diskrétne signály s konečnou dĺžkou (t.j. vizuálne obrazy), kde N je počet vzoriek signálu (obrazových prvkov, ak obraz je zvolený signál) a xi a yi sú hodnoty i-tej vzorky v signáloch x a y. stredná kvadratická odchýlka je definovaná nasledovne:

$$MSE(x, y) = \frac{1}{N}\sum_{k=1}^{N}(x_i - y_i)^2 \tag{7}$$

V mnohých prípadoch, sa stredná kvadratická odchýlka používa na určenie chybového signálu e_i, ktorý je potom rozdielom e_i=x_i-y_i, čo predstavuje rozdiel medzi originálnym a pozmeneným signálom. Pre náš prípad, sme strednú kvadratickú odchýlku využili ako definíciu chybového signálu, a to medzi detailovými koeficientami A(n) a smerovými koeficientami rovnakej úrovne DWT dekompozície obrazu, keďže vieme povedať, že jednotlivé dekompozičné koeficienty rovnakej úrovne sú navzájom korelované.

$$MSE(A(n), S(n)) = \frac{1}{N}\sum_{k=1}^{N}(A(n)_i - S(n)_i)^2 \tag{8}$$

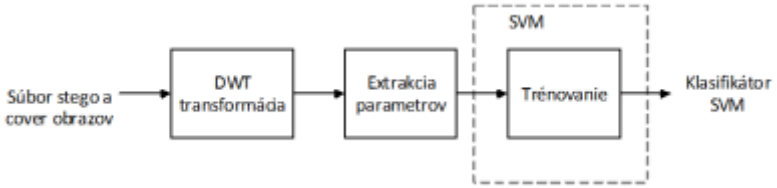
kde

$$S(n) = \{H(n), D(n), V(n)\}, n = 1, 2, 3 \quad (9)$$

Takto sme získali posledných 9 koeficientov pre náš vektor štatistických parametrov.

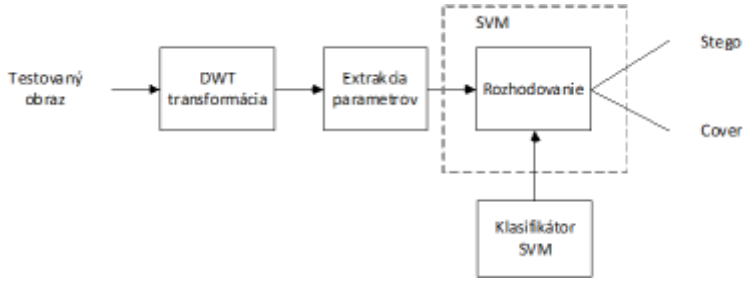
4.2 Navrhnutý algoritmus

Algoritmus navrhnutej steganalytickej metódy môžeme vidieť na nasledujúcich blokových schémach. Vstupom pre proces vytvorenia databázy je množina krycích (obrazy bez tajnej správy) a k nim prislúchajúcich stego obrazov, ktoré sú transformované do DWT oblasti. Potom nasleduje extrakcia vektora štatistických parametrov opísaného v predchádzajúcej podkapitole. Súbor vektorov štatistických parametrov prislúchajúci krycím a stego obrazom následne putuje do bloku SVM, kde prebieha trénovanie. Výsledkom bloku SVM je natrénovaný klasifikátor pre SVM (Obr. 6).



Obr. 6 Bloková schéma procesu trénovania

V prípade klasifikácie testovaného obrazu je proces analogický ako v prípade trénovania. Vstupom do bloku SVM je štatistický vektor extrahovaný z testovaného obrazu a tiež klasifikátor, ktorý je výsledkom predchádzajúceho trénovania. Nastáva rozhodovanie, kde sa určí, do ktorej hyperroviny patrí vektor z testovaného obrazu (Obr. 7).



Obr. 7 Bloková schéma klasifikácie neznámeho obrazu

5. Programová realizácia

Modul stegoanalýzy bol realizovaný vo vývojovom prostredí MATLAB 2014b 64bit.

5.1 Grafická realizácia

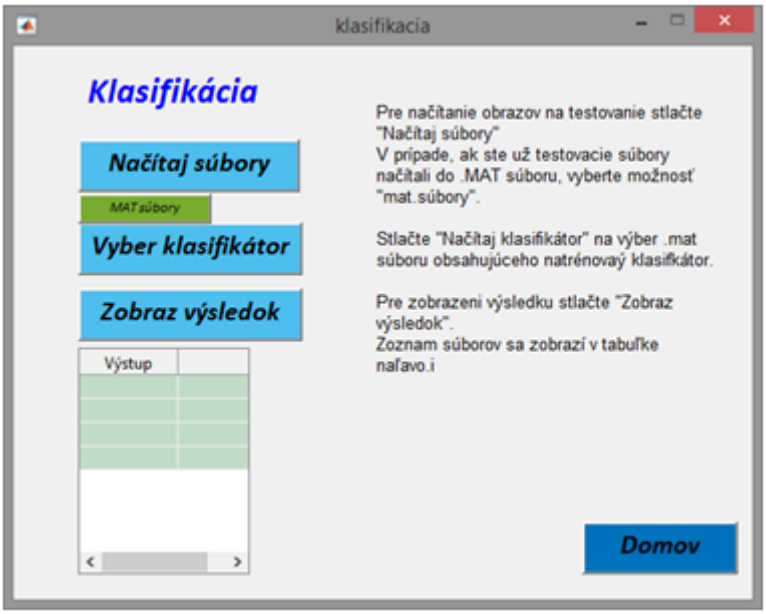
Pre spustenie grafického prostredia navrhnutého modulu je potrebné spustiť súbor domov.m. Po úspešnom spustení súboru sa na obrazovke zobrazí domáca obrazovka modulu.

Obr. 8 Modul – domáca obrazovka

Steganalýzny modul ponúka na výber používateľovi dve možnosti. Umožňuje klasifikáciu testovacích obrazov na základe vopred natrénovaného klasifikátora alebo trénovanie klasifikátora na základe zvolenej množiny testovacích krycích a stego obrazov. Každá obrazovka modulu ponúka stručný návod na popis možností konkrétnej funkcie.

5.1.1 Klasifikácia

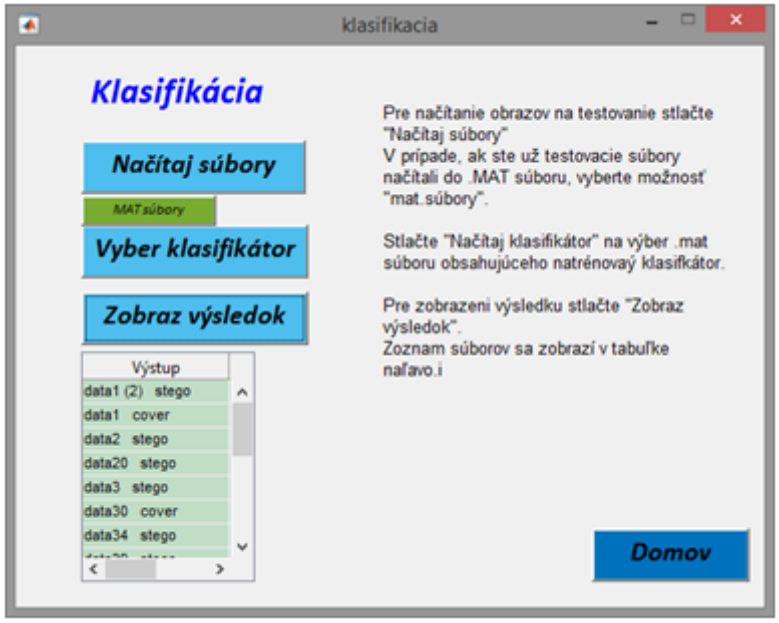
Po výbere možnosti klasifikácie z hlavnej obrazovky modulu, sa používateľovi zobrazí obrazovka funkcie klasifikácia.



Obr. 9 Modul – obrazovka klasifikácie.

Modul klasifikácie ponúka možnosť výberu typu vstupných dát. Vstupom môže byť množina obrazov, ktoré chce používateľ testovať prípadne súbor sample.mat, ktorý už obsahuje načítanú množinu testovacích súborov. Následne používateľ má možnosť výberu klasifikátora, ktorým chce klasifikovať testovaciu množinu. Tento klasifikátor je

výsledkom funkcie trénovania, ktorý priblížime neskôr. V základnom nastavení ponúka modul na výber z viacerých vopred natrénovaných klasifikátorov, ktoré sú uložené v zložke s názvom „Classifiers“.

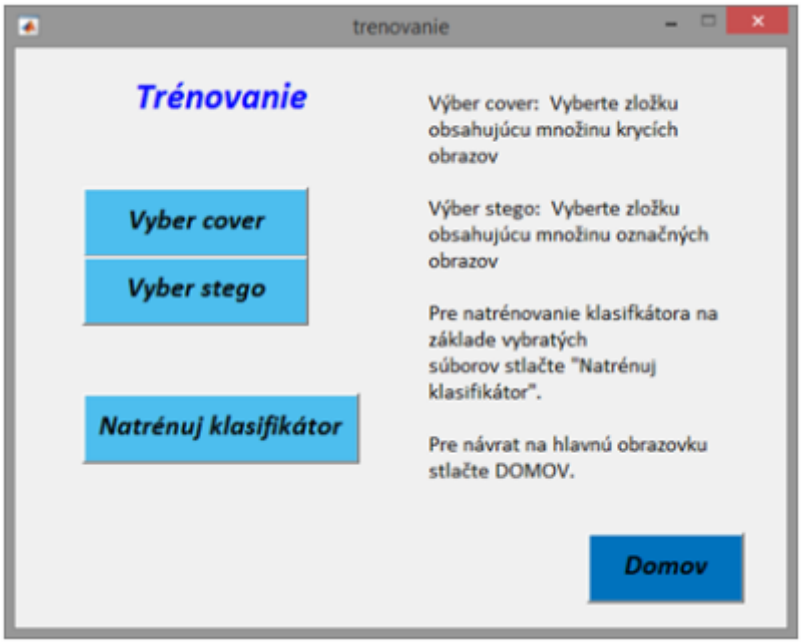


Obr. 10 Modul – obrazovka klasifikácie so zobrazeným výsledkom.

Po výbere klasifikátora modul následne vykoná klasifikáciu testovaných súborov. Pre zobrazenie výsledku klasifikácie je potrebné stlačiť tlačidlo Zobraz výsledok, ktorý v tabuľke umiestnenej v ľavej časti obrazovky vypíše zoznam súborov a k nim prislúchajúcich hodnôt výsledku.

5.1.2 Trénovanie

Druhá funkcia steganalýzneho modulu je funkcia trénovania klasifikátora. Po zvolení funkcie trénovať na hlavnej obrazovke, sa používateľovi zobrazí obrazovka s dostupnými možnosťami.



Obr. 11 Modul – obrazovka trénovania

Tlačidlá Vyber cover a Vyber stego slúžia na výber množiny obrazových súborov, pre ktoré chce používateľ trénovať klasifikátor. Po výbere zložky, v ktorej sa nachádzajú požadované súbory, modul následne vykoná extrakciu štatistického vektora z každého súboru a následne uloží získané vektory do súborov cover.mat resp. stego.mat. tie následne slúžia ako vstup pre funkciu trénovania. Výsledkom trénovania je súbor struct.mat, ktorý môže byť vstupom pre klasifikáciu, opísanú v predchádzajúcej podkapitole.

6. Dosiahnuté výsledky

Táto kapitola je venovaná zhodnoteniu výsledkov navrhnutého steganalýzneho modulu. Ako vstup sme využili niekoľko desiatok krycích aj cover obrazov, ktoré sme testovali. Testovali sme účinnosť nášho algoritmu na dvoch steganografických metódach. Databázy krycích a stego obrazov obsahovali obrazy s rozličným rozlíšením, obsahom i formátom. Informácia vkladaná steganografickým algoritmom tiež bola rozdielna. Uvedené výsledky úspešnosti sú uvádzané pre detekciu stego obrazov (obrazy s tajnou správou). Pri detekcii krycích obrazov sme pri testovaní dosiahli porovnateľné hodnoty.

6.1 Testované steganografické metódy

6.1.1 DWT metóda

Steganografická metóda založená na transformovanej DWT oblasti je navrhnutá na ukrývanie textovej informácie do nekomprimovaných .tiff obrazových súborov. Jej princíp činnosti je nasledovný. Na vstupný obraz sa aplikuje dvojrozmerná diskrétna waveletová transformácia po ktorej sa obraz rozdelí na jednotlivé farebné roviny z priestoru RGB. LSB bity týchto rovín následne slúžia na vloženie tajnej správy (dodatočne zašifrovaná štandardom AES). V závislosti od veľkosti tajnej správy sa vyhodnotí kapacita jednotlivých farebných rovín. Ak je veľkosť správy menšia, algoritmus nevyužije na uloženie tajnej správy všetky farebné roviny. Tajná správa sa najprv ukladá do červenej roviny a až v prípade ak je potrebná väčšia kapacita sa využije zelená a modrá rovina.

6.1.2 Steghide

Steghide je steganografický nástroj ktorý umožňuje ukryť dáta v rôznych typoch obrazových a zvukových krycích médií. Vzorkovacia frekvencie nie sú pozmenené, teda nástroj je odolný voči štatistickým testom prvej úrovne. StegHide využíva steganografický prístup na základe teórie grafov. Proces vkladania je nasledovný: ako prvé, sa tajná správa komprimuje a kryptuje. Následne sa vytvorí postupnosť pozícií obrazových prvkov v krycom médiu na základe pseudonáhodnej postupnosti. Do týchto obrazových prvkov sa vloží tajná správa. Zo všetkých vygenerovaných pozícií sa odstránia tie, ktorých hodnota zodpovedá hodnote, ktorú by nadobudli po vložení informácie. Následne párovací algoritmus na báze teórie grafov nájde dvojice obrazových prvkov tak, aby po vzájomnej výmene hodnôt im prislúchala hodnota, ktorá zodpovedá vloženej tajnej správe. Zvyšné pozície, ktoré netvoria pár tiež nadobudnú hodnotu zodpovedajúcu tajnej správe. Nestane sa to výmenou, ale prepísaním hodnoty konkrétneho obrazového prvku. Skutočnosť, že vkladanie informácie je uskutočnené

vzájomnou výmenou hodnôt, teda štatistiky prvého rádu sa nezmenia [7].

6.2 Výsledky testovania

Navrhnutú metódu stegoanalýzy sme podrobili testovaniu. Ako prvú sme testovali steganografickú metódu, ktorá využíva na ukladanie tajnej správy DTW transformovanú oblasť. Zostavili sme trénovaciu databázu, ktorá pozostávala z celkom 229 snímok rôznych rozlíšení a obsahu, v rozložení 100 krycích a k nim prislúchajúcich 129 cover obrazov. Cover obrazy boli označené rôznou veľkosťou tajnej správy. Testovaním sme dospeli k záveru, že pre náš navrhovaný algoritmus je najvhodnejšia kombinácia lineárnej kernel funkcie s využitím metódy SMO (sekvenčná minimalizácia optimalizovaním) na získanie separujúcej hyperroviny. Na poukázanie úspešnosti detekcie sme vykonali aj testovanie na jednej množine krycích obrazov, do ktorej sme metódou DWT vkladali rôznu veľkosť tajnej správy.

Tab. 1 Porovnanie úspešnosti klasifikácie DWT metódy v závislosti od množstva vloženej informácie

Model Cover – DWT(linear, SMO)			
Veľkosť vloženej informácie	98300 bitov	60300 bitov	31300 bitov
Úspešnosť detekcie	100%	95,30%	86%

V tabuľke Tab.1 vidíme, že úspešnosť detekcie algoritmu DWT závisí aj od množstva ukrytej informácie. Keďže táto metóda využíva na ukladanie informácie farebné kanály obrazu podľa veľkosti tajnej správy, jej účinok na štatistické parametre obrazu tým väčšie, čím je veľkosť vkladaného textu väčšia . To však platí pre všetky steganografické metódy. Z charakteru našej navrhovanej metódy vyplýva, že by bola vhodná i na detekciu iných algoritmov, keďže vytvorený štatistický vektor nie je viazaný na parametre opísanej DWT metódy. Algoritmus sme otestovali aj na steganografickom algoritme StegHide, ktorý pre vkladanie tajnej správy využíva priestorovú oblasť. Pre metódu sme tiež natrénovali klasifikátor.

Tab. 2 Úspešnosť detekcie tajnej správy vloženej pomocou metódy StegHide

Detekovaná metóda	**Model Cover-DWT**	**Model Cover-StegHide**
StegHide	62,8%	84,6%

Dosiahnuté výsledky môžeme vidieť v tabuľke Tab. 2. Úspešnosť našej navrhovanej metódy pre túto steganografickú metódu v priestorovej oblasti je nižšia ako v prípade DWT metódy, čo nám hovorí, že navrhnutá stegoanalytická metóda je primárne určená na detekciu steganografických algoritmov pracujúcich v transformovanej DWT doméne.

Záver

Výsledkom tejto práce je novo navrhnutý steganalýzny modul pre statické obrazy spolu s jeho programovou realizáciou v prostredí MATLAB. Ten je založený na vektore štatistických parametrov so 46 prvkami, ktorý bol tiež vytvorený pre účely navrhnutej metódy. Pre trénovanie a klasifikáciu sme si zvolili algoritmus podporných vektorov

(SVM) a to na základe teoretických poznatkov získaných pri skúmaní problematiky. Z týchto základných pilierov sme postavili funkčný algoritmus, ktorým je možné detegovať prítomnosť tajnej správy na základe parametrov získaných z diskrétnej waveletovej transformácie. Úspešnosť navrhnutej metódy sme overili na dvoch dostupných steganografických metódach.

Najlepšie výsledky sme dosiahli pri metóde, ktorá pracuje tiež v DWT oblasti. To je spôsobené tým, že v prípade tejto metódy sú zmeny v DWT oblasti primárne a vznikajú vo väčšej miere. Na rozdiel od toho, ďalšia metóda ktorú sme skúmali bola založená na iných doménach a vplyv vloženej informácie v oblasti DWT bol len sekundárny. Ale i napriek tomu, navrhnutý algoritmus stegoanalýzy bol schopný detegovať i tieto zmeny vďaka dobre zvoleným parametrom, z ktorých pozostáva náš štatistický vektor. Z toho nám vyplýva, že navrhnutá metóda má i univerzálny charakter a je schopná detegovať viacero metód aj keď najvyššia úspešnosť bude dosiahnutá najmä pre steganografické metódy v DWT oblasti.

Zoznam použitej literatúry

1. BÖHME, Rainer : Advanced statistical steganalysis, Springer, 2010, ISBN 978-3-6-2-14312-0 / e-ISBN 978-3-642-14313-7.
2. NISSAR, Arooj; MIR, A.H. : „Classification of steganalysis techniques: A study“, Digital Signal Processing 20 (2010) , str. 1758–1770.
3. Pauly, O.; Padoy, N.; Poppert, H.; Esposito, L; Navab, N.: Wavelet Energy Map: A robust Support for Multi-modal Registration of Medical Images. Technical university Munchen Germany. Dostupné na internete: http://www.cs.jhu.edu/~padoy/media/pubs/pauly-cvpr09.pdf
4. Liu,Changxin; Ouyang, Chunjuan; Guo, Ming; Chen; Huijuan: „Image Steganalysis Based on Spatial Domain and DWT Domain Features“, 2010 Second International Conference on Networks Security, Wireless Communications and Trusted Computing.
5. FARID,Hany, „Detecting hidden messages using higher order statistical models“, Department of computer science, Dartmoth College Hannover.
6. [6] NISSAR, Arooj; MIR, A.H. : „Classification of steganalysis techniques: A study“, Digital Signal Processing 20 (2010) , Str. 1758–1770.
7. StegHide, http://steghide.sourceforge.net/documentation/manpage.php

---

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