Katedra Informatiky
Fakulta Matematiky, Fyziky a Informatiky
Univerzita Komenského, Bratislava

Steganografické systémy a digitálna vodotlač pre vektorové digitálne mapy

(diplomová práca)

Martin Filo

Vedúci: RNDr. Richard Ostertág

Bratislava, 2005

Čestne prehlasujem, že som túto diplomovú prácu vypracoval samostatne s použitím citovaných zdrojov.

. . . . . .

Poďakovanie

Chcel by som sa poďakovať vedúcemu mojej diplomovej práce RNDr. Richardovi Ostertágovi, za jeho ochotu, rady a pripomienky pri písaní tejto práce. Mojej snúbenici Lenke za jej neoceniteľné rady z oblasti štatistiky, mojim rodičom a všetkým priateľom, ktorí mi akokoľvek pomohli pri čomkoľvek.

Obsah

Kapitola 1

Úvod

Steganografia *(z gréckeho steganos graphein)* je veda, ktorá sa zaoberá takými metódami komunikácie, pri ktorých sa utajuje samotný fakt komunikácie. Metódami klasickej steganografie sú rôzne neviditeľné atramenty, známa mikrobodka, kódovanie informácie do detských kresieb atď. [10],....

S príchodom výpočtovej techniky sa aj pre steganografiu otvorili nové možnosti. Cieľom steganografie nie je nahradiť kryptografiu, ale utajiť jej použitie v situáciách, keď sa nemôže použiť. Takáto situácia nastane v prípade, ak správa ide cez cenzora, ktorý zašifrované správy nepustí ďalej, alebo je použitie kryptografie zakázané.

S rozmachom digitálneho spracovania informácií a internetu je stále viac autorských dokumentov v elektronickej podobe. Výhodou je rýchle vyhľadávanie, ľahké kopírovanie s prakticky nulovými nákladmi a bez straty kvality, čo pri klasických médiách, ako je napríklad papier, nie je možné. Nevýhodou ale je, že nie je možné rozoznať originál od kópie. Riešením tohto problému je ochrana autorstva pomocou digitálnej vodotlače. Digitálna vodotlač je aplikáciou steganokrafie. Ďalšie dôležité požiadavky, ktoré musia byť splnené na to, aby začal byť väčší záujem o publikáciu diel v elektronickej podobe sú: ochrana diela pred zmenami, kontrola používania, sledovanie začleňovania do iných diel atď.... Na splnenie týchto požiadaviek sa používajú aj rôzne steganografické algoritmy.

Ciele diplomovej práce

Existuje veľa steganografických algoritmov pre obrázky, alebo hudbu, ale na digitálne vektorové mapy ich je málo a neexistuje žiadny formálny model, ktorý by ich popisoval. Táto diplomová práca sa zaoberá problematikou digitálnej vodotlače a steganorafických systémov pre vektorové mapy. Jej cieľom je

- poskytnúť stručný úvod do problematiky steganografie a vodotlače so zreteľom na vektorové mapy
- formulovať teóriu na popis matematických vlastností robustných steganografických systémov pre vektorové mapy
- poskytnúť ucelený pohľad na existujúce, reálne použiteľné algoritmy
- využiť formálny model na ich porovnanie, nájdenie slabín, prípadne vylepšenie

Štruktúra diplomovej práce

V kapitole 2 uvedieme základné všeobecné pojmy zo steganografie a digitálnej vodotlače. Keďže pojmy z oblasti steganografie a digitálnej vodotlače nie sú veľmi známe, táto kapitola slúži na základné oboznámenie čitateľa s problematikou. Ak by čitateľ potreboval podrobnejšie oboznámenie s problematikou, odporúčame publikácie [10], [15] a [6].

Jedným z hlavných výsledkov tejto práce je kapitola 3, ktorá obsahuje formálny model pre steganografické systémy a digitálnu vodotlač na vektorových mapách. Jej výsledkom sú dve optimálne bázy pre robustný informovaný steganorgafický systém.

Kapitola 4 obsahuje prehľad tried algoritmov s analýzou ich vlastností. Druhý hlavný výsledok je využitie nášho formálneho modelu na analýzu existujúceho robustného vodotlačového algoritmu a jeho vylepšenie.

V kapitole 5 je návrh neinformovaného steganografického systému, ktorý je robustný proti útoku vyhladzovaním a zašumením.

V závere (kapitola 6) zhrnieme dosiahnuté výsledky a uvedieme ciele ďalšieho teoretického výskumu.

Kapitola 2

Základné pojmy steganografie a digitálnej vodotlače

Čo je steganografia?

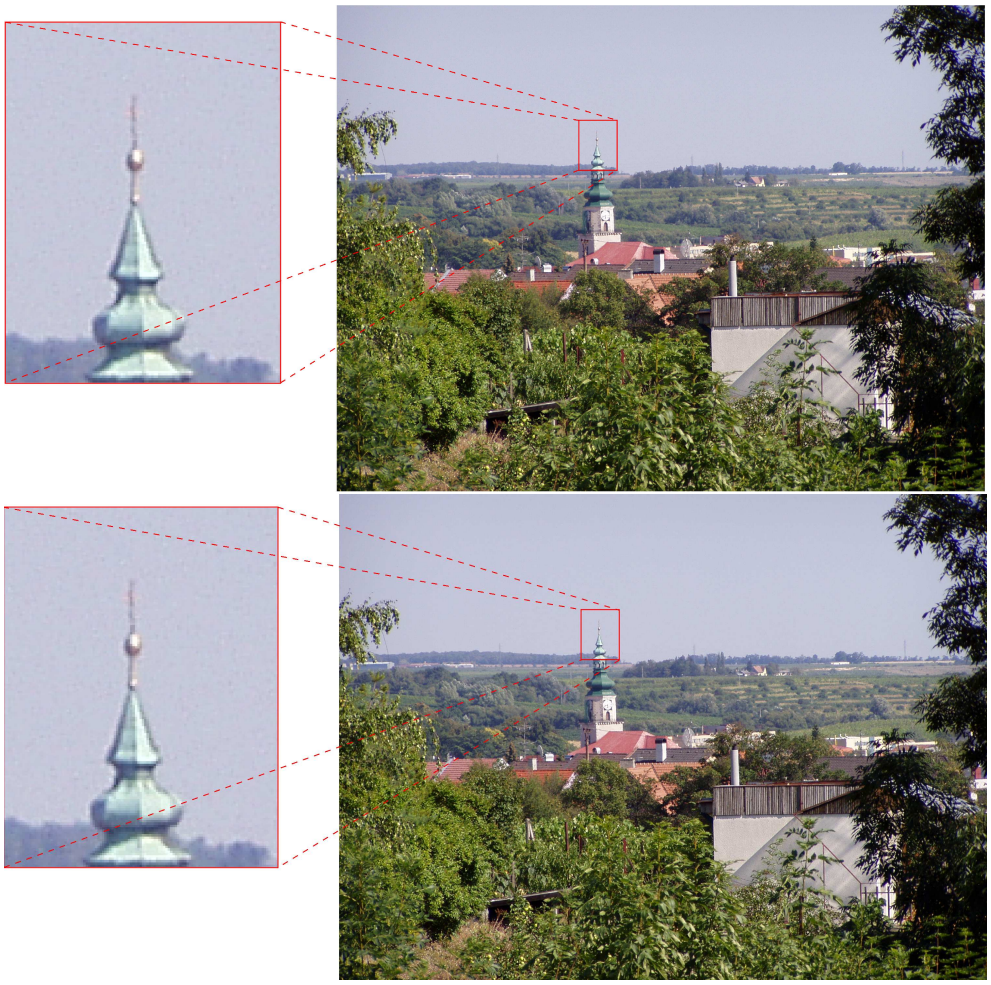
Najjednoduchšie bude ilustrovať to na jednoduchom príklade, ktorý sa síce netýka máp, ale je dobrý na ozrejmenie pojmu steganografia.

Vezmime si neskoprimovaný obrázok 2.1 rozmerov $1\,984 \times 1\,488$ v 24-bitových farbách (RGB), ktorého veľkosť je $(1\,984 \times 1\,488 \times 24)/8 = 8\,856\,576$ bajtov.[1] Každý bod obrázku je reprezentovaný tromi 8-bitovými číslami, ktoré reprezentujú úroveň troch základných farieb (červenej, zelenej a modrej (RGB)). Ak zmeníme najmenej významný bit každej farby, tak sa jej úroveň zmení maximálne o ± 1 a to na výslednom obrázku vôbec nebude vidieť. Tým sme ale do obrázku vložili nejakú ďalšiu informáciu. V tomto prípade je jej maximálna dĺžka $(1\,984 \times 1\,488 \times 3)/8 = 1\,107\,072$ bajtov.

Takto možno prostredníctvom nezaujímavých obrázkov prenášať zaujímavé správy[2]. Takáto správa však neprežije žiadnu modifikáciu obrázku.

[1] Tieto rozmery má fotografia z digitálneho fotoaparátu vo formáte tif.

[2] Táto metóda sa nazýva LSB (The Least Significant Bit)



Obr. 2.1: Hore je pôvodný obrázok. V spodnom obrázku je do horného pomocou programu S-Tools 4.0 vložený román Georga Orwella 1984 vo formáte pdf s veľkosťou 619 079 bajtov.

2.1 Základné pojmy zo steganografie

Nižšie uvedené pojmy boly prevzaté a upravené z [15]

2.1.1 Úvodné definície

Definícia 2.1.1. ***Digitálna vodotlač*** *je aplikácia steganografie, ktorá ukrýva do dát informácie s nimi súvisiace.*

Definícia 2.1.2. ***Originál, predloha, neoznačené dáta*** *sú dáta, do ktorých vkladáme* ***správu, vodotlač*** *vo väčšine algoritmov pomocou* ***kľúča****.*

Definícia 2.1.3. ***Modifikované dáta, označené dáta*** *sú dáta, v ktorých je vložená správa.*

Definícia 2.1.4. ***Extrakcia*** *je procedúra ktorá z modifikovaných dát zistí správu, ktorá bola do nich vložená.*

Definícia 2.1.5. ***Detekcia*** *je procedúra, ktorá z modifikovaných dát zistí či tam bola daná správa vložená, alebo nie, prípadne pravdepodobnosť, toho že informácia tam bola vložená.*

Definícia 2.1.6. ***Referenčné dáta*** *sú tá časť predlohy, ktorá je potrebná na extrakciu, alebo detekciu.*

Definícia 2.1.7. ***Odosielateľ, autor*** *je ten, kto vkladá správu do predlohy.*

Definícia 2.1.8. ***Príjemca*** *je ten, kto oprávnene extrahuje, alebo detekuje správu z označených dát.*

Definícia 2.1.9. ***Útočník*** *je ten, kto neoprávnene extrahuje správu s označených dát, alebo sa neoprávnene pokúša zistiť prítomnosť vloženej správy, alebo sa ju pokúša zmeniť, znečitatelniť, alebo zmazať.*

2.2 Rozdelenie steganografických systémov

Na vlastnosti steganografických systémov sa môžeme pozerať z viacerých hľadísk.

- Hľadisko vnímateľnosti
  - *vnímateľný steganografický systém* (visible, perceptible) Správa je vnímateľná zmyslami. Napríklad rôzne symboly vložené do predlohy.
  - *nevnímateľný steganografický systém* (invisible, inperceptible) Správa v označenej kópii nie je vnímateľná zmyslami. Na jej extrakciu je potrebné ju digitálne spracovať.
- Hľadisko odolnosti
  - *robustný steganografický systém* (robust, tamper-resistant) Správa by mala odolať modifikáciám, ktoré sú spôsobené bežnou manipuláciou, alebo útokom. V ideálnom prípade pre digitálnu vodotlač do tej miery, kým dáta nebudú modifikované až tak, že autor nebude mať záujem ich chrániť.
  - *krehký steganografický systém* (fragile, tamper-detect) Správa podlieha zmenám tak isto ako aj dáta a nepreživje žiaden útok. Možno ho využiť na detekciu integrity dát. Ak sa z označených dát podarí extrahovať správu, tak integrita dát nebola po označení porušená, a ak sa to nepodarí, tak bola porušená ich integrita.
- Hľadisko závislosti
  - *závislý (informovaný) steganografický systém* (private, informed-detection) Na zistenie prítomnosti, alebo extrakciu správy sú potrebné originálne, alebo referenčné dáta.
  - *nezávislý (slepý) steganografický systém* (public, oblivious, blind-detection) Na zistenie prítomnosti, alebo extrakciu vodotlače nie je potrebný originál ani referenčné dáta.

- Hľadisko dostupnosti
  - *čistý steganografický systém* (pure) Nepoužíva žiadny kľúč na vkladanie, alebo extrakciu správy.
  - *symetrický steganografický systém* (secret-key, symetric) Na vkladanie aj detekciu správy sa používa ten istý kľúč.
  - *asymetrický steganografický systém* (public-key, asymetric) Používa iný kľúč na vkladanie a iný na extrakciu, respektíve detekciu správy.
- Hľadisko domény [3]
  - steganografické systémy pracujúce *v priestorovej doméne* (spatial-domain) vkladajú správu priamo do predlohy
  - *transformačné steganografické systémy* (transform-domain) predlohu najprv pretransformuje do vhodnejšej bázy v nej sa vkladá správa.
- Hľadisko druhu dát
  - *bitmapové obrázky, videodáta, hudba* obsahujú veľa redundantných informácií, a teda je relatívne jednoduché do nich ukrývať správy. Výskum v tejto oblasti pokročil a existuje veľa dobrých algoritmov.
  - *vektorové obrázky* obsahujú oveľa menej redundantných informácií ako porovnateľné bitmapové obrázky, preto je veľmi ťažké do nich ukrývať správy. Robustné algoritmy pre ne začali vznikať len nedávno. Sem patria aj vektorové mapy.
  - *spustitelné súbory* Keďže predloha aj modifikované dáta musia vykonávať to isté, je veľmi ťažké skonštruovať pre ne steganografický systém.
  - *textové dáta* modifikujú tvary a umiestnenia písmen, medzery medzi slovami, riadkami, zamieňajú slová za ich synonymá...

[3] Pojmy budú presnejšie vysvetlené v 2.3

Na steganografický systém je kladených veľa protichodných požiadaviek.

- robustnosť versus veľkosť vloženej správy
- robustnosť versus modifikácia predlohy

Definícia 2.2.1. [4]***Čistá steganografia*** *(Pure steganography) Je štvorica* $\mathcal{S} = (C, M, D, E)$*, kde* C *je množina možných predlôh,* M *je množina tajných správ s* $|C| \geq |M|$*,* $E : C \times M \rightarrow C$ *je vkladacia funkcia a* $D : C \rightarrow M$ *je extrakčná funkcia, taká, že pre* $\forall m \in M$ *a* $\forall c \in C$ *platí* $D(E(c, m)) = m$

Definícia 2.2.2. [5]***Symetrická steganografia*** *(secret key steganography) Je pätica* $\mathcal{S} = (C, M, K, D', E')$*, kde* C *je množina možných predlôh,* M *je množina tajných správ s* $|C| \geq |M|$*,* K *je množina tajných kľúčov,* $E' : C \times M \times K \rightarrow C$ *je vkladacia funkcia a* $D' : C \times K \rightarrow M$ *je extrakčná funkcia, taká, že pre* $\forall m \in M$*,* $\forall c \in C$ *a* $\forall k \in K$ *platí* $D'(E'(c, m, k), k) = m$

V tejto práci sa budeme venovať symetrickým steganografickým systémom.

2.3 Princípy robustnej steganografie

Na obrázku 2.1 sme videli príklad krehkého algoritmu. Často je však potrebné preniesť správu tak, aby prežila aj rôzne modifikácie predlohy. Na to potrebujeme robustné algoritmy. Robustnosť je požadovaná najmä v oblasti digitálnej vodotlače, kedže tá musí odolať útokom zameraným na jej odstránenie. Ak ale umiestnime správu do najmenej významnej časti predlohy, tak potom útočníkovi stačí zašumieť, prípadne úplne odstrániť málo významnú časť dát a nepotrebuje vôbec vedieť, či sa tam nachádza nejaká správa. Na robustný steganografický systém preto potrebujeme správu uložiť do významnej časti predlohy, v ktorej sa šum prejaví v čo najmenšej miere. Lenže ako zistiť, ktorá časť dát je významná a ktorá nie? Týmto problémom sa zaoberá aj teória stratovej kompresie dát.Na tento účel sa používajú transformačné techniky, ktoré pretransformujú predlohu do podoby, v ktorej sa dajú jednoduchšie oddeliť dôležité dáta od nedôležitých dát.

[4]Prevzaté z [6] definícia 2.1
[5]Prevzaté z [6] definícia 2.3

2.3.1 Transformačné steganografické systémy

V ďalšom texte budeme pre jednoduchosť uvádzať predlohu ako vektor $(a_1, \ldots, a_n)$, ktorého definícia je závislá od druhu dát. Formálnu definíciu zavedieme len pre tie prípady, ktoré budeme používať.

Pojem transformačného steganografického systému si najprv ozrejmíme na jednoduchom príklade. Vezmime si obrázok rozmerov $m \times n$. Tento možno reprezentovať maticou

$$M = \begin{pmatrix} a_{11} & a_{12} & \ldots & a_{1n} \\ a_{21} & a_{22} & \ldots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \ldots & a_{mn} \end{pmatrix}$$

kde a_{ij} sú hodnoty farieb jednotlivých bodov obrázku[6]. Zaveďme si operátor L, ktorý nám zreťazí riadky matice M, a k nemu inverzný operátor L^{-1}.

$$L(M_{m\times n}) = ((m,n), \vec{v})) =$$

$$= \big((m,n), (a_{11}, a_{12}, \ldots, a_{1n}, a_{21}, a_{22}, \ldots, a_{2n}, \ldots, a_{m1}, a_{m2}, \ldots, a_{mn})^T\big)$$

$$M = L^{-1}\Big((m,n), \vec{v})\Big)$$

Nech p, q sú ľubovoľné prirodzené čísla také, že platí $pq = mn$. Potom $\vec{v}$ patrí do mn rozmerného priestoru všetkých obrázkov rozmeru $p \times q$.

Definícia 2.3.1. *Nech predloha je vektor* $(a_1, a_2, \ldots, a_m)^T$, *nech* $(a_{i_1}, a_{i_2}, \ldots, a_{i_n})^T$, *kde* $n < m, \{i_1, \ldots, i_n\} \subseteq \{1, \ldots, m\}, i_k \neq i_l$ *ak* $k \neq l$ $k, l \in \{1, \ldots, n\}$ *sú tie zložky predlohy do ktorých chceme vložiť správu. Potom identická matica* $\boldsymbol{I}$ *s* $dim(\mathbf{I}) = n$ *je matica bázy* ***priestorovej domény*** (spatial domain) *a vektor* $(a_{i_1}, a_{i_2}, \ldots, a_{i_n})^T$ *je reprezentáciou časti predlohy v štandardnej báze.*

Transformačná báza (transform domain)T *je ľubovoľná iná báza a vektor* $(a'_{i_1}, a'_{i_2}, \ldots, a'_{i_n})^T$ *taký, že* $(a_{i_1}, a_{i_2}, \ldots, a_{i_n})^T = T(a'_{i_1}, a'_{i_2}, \ldots, a'_{i_n})^T$ *je reprezentáciou časti predlohy v transformačnej báze.*

[6]Napríklad v RGB

Definícia nevyžaduje od transformačnej bázy žiadne ďalšie vlastnosti, ako by sa dalo očakávať. Je to preto, že už použitím tejto techniky sa steganografický systém stáva transformačný. Na robustnú steganografiu však potrebujeme bázu, v ktorej je možné ľahšie určiť, ktoré zložky predlohy sú významné a ktoré nie.

Definícia 2.3.2. Spektrálna báza *je taká transformačná báza v ktorej vieme odlíšiť podstatné zložky predlohy od šumových zložiek.*

2.4 Stegoanalýza

Stegoanalýza sa venuje útokom na steganografické systémy a digitálnu vodotlač. Na útoky sa môžeme pozerať z viacerých hľadísk.

- Hľadisko cieľa útokov
  - *Extrakčné útoky* cieľom útokov je získať správu bez znalosti kľúča. Ak je správa navyše zašifrovaná, tak nie je ich cieľom správu dešifrovať.
  - *Detekčné útoky* ich cieľom je zistiť či dáta obsahujú ukrytú správu, samotná správa je nezaujímavá.
  - *Mazacie útoky* pri týchto útokoch nie je vôbec dôležité, či dáta pred útokom obsahujú ukrytú správu. Ich cieľom je, aby ju neobsahovali po útoku. Pre robustnú digitálnu vodotlač je potrebné, aby odolala týmto typom útokov.

- Spôsoby útokov
  - *Útoky na robustnosť* (robustness attacks) sa snažia z dát odstrániť správu.
  - *Prezentačné útoky* (presentation attacks, detection-disabling attacks, synchronization attacks) správu neodstraňujú, ale označené dáta upravia tak, aby extrakčný/detekčný algoritmus nenašiel správu. Príklad takého útoku je rozdelenie obrázku na časti a jeho následné zobrazenie na stránke ako veľa obrázkov vedľa seba. Iný príklad uvádzame v časti 4.1.7.

  - *Interpretačné útoky* (interpretation attack, ambiguity attack) sa týkajú len vodotlače. Snažia sa spochybniť hodnovernosť vodotlače.
  - *Právny útok* (legal attacks) sa tiež týkajú len vodotlače. Ich cieľom je právne spochybnenie vodotlače.

- Podľa úmyslu
  - *Neúmyselné útoky* (unintended, simple, unintentional) sú dôsledkom rôznych bežných transformácii, ako napríklad stratovej kompresie zmeny veľkosti, orezania atď...
  - *Úmyselné* útoky (intentional).

- Podľa znalosti algoritmu
  - *Stego-only útok* (stego only attck) k dispozícii sú len modifikované dáta.
  - *Útok s predlohou* (known cover attack) k dispozícii je predloha aj modifikované dáta.
  - *Útok so znalosťou správy* (known message attack) k dispozícii je správa aj modifikované dáta. Cieľom je získať informácie, ktoré by pomohli pri ďalšom útoku.
  - *Útok na známy algoritmus* (chosen stego attack) k dispozícii je algoritmus aj modifikované dáta. Pri posudzovaní odolnosti steganografických systémov sa budeme venovať tomuto typu útoku.
  - *Útok s možnosťou volby správy* (Chosen message attack) pri tomto útoku útočník má k dispozícii algoritmus, nemá kľúč, ale má možnosť vkladať správu do predlohy. Cieľom útoku je pomocou analýzy korešpondujúcich častí v označených dátach zistiť, aký kľúč bol použitý.
  - *Útok so znalosťou časti správy* (known stego attack) K dispozícii sú algoritmus, modifikované dáta a časť správy. Cieľ útoku je zistiť celú správu.

Kapitola 3

Teoretický základ steganografie a digitálnej vodotlače pre vektorové mapy

Potreba digitálnych máp rastie. Používajú sa napr. v navigačných systémoch áut, mobilných telefónoch s GPS lokalizáciou, v mapových službách na internete, v geografických informačných systémoch (GIS), v rozvojových plánoch, atď ...
Ako všetky digitálne dáta, ľahko sa dopĺňajú, rozmnožujú a distribuujú, či už legálne, alebo nelegálne.
Dvojrozmerné mapy môžeme rozdeliť na dve skupiny

- *rastrové mapy* sú to klasické veľké rastrové obrázky, a teda na ne možno použiť algoritmy pre rastrové obrázky. Ich nevýhodou je obmedzená presnosť, veľký objem dát[1], strácanie kvality bežnou manipuláciou geometrickými a topologickými transformáciami. Ich užitková hodnota je veľmi obmedzená. V tejto práci sa im nevenujeme.

- *vektorové mapy* sa skladajú z geometrických primitív ako body, čiary, polygóny reprezentujúce objekty na mape ako napr. budovy, cesty, rieky, atď.... Možno ich zväčšovať, zmenšovať, otáčať bez straty kva-

[1] napríklad mapa Iraku v mierke 1:1250000 obsahujúca len veľké rieky mestá, letiská a dôležité cesty, má rozlíšenie 10056×10864 a vo formáte jpeg zaberie 21 MB

lity. Možno z nich vyčítať oveľa presnejšie a použiteľnejšie údaje ako z rastrových máp. Ich veľkosť je, pri porovnateľnej presnosti, oveľa menšia ako pri rastrových mapách. Vďaka tomu sú oveľa zaujímavejšie ako rastrové mapy.

Na porovnanie vlastností jednotlivých algoritmov nepoužijeme experimentálne metódy ako ich autori, ale preskúmame ich matematické vlastnosti. Na tomto základe ich porovnáme a pozrieme sa, čo by sa na nich dalo vylepšiť.

3.1 Základné pojmy a vety zo štatistiky, algebry a spektrálnej teórie matíc

Veta 3.1.1. *Nech $A \in \mathbb{R}^{n\times n}$ je symetrická matica, nech $\vec{v}_i$ a $\vec{v}_j$ sú vlastné vektory A, kde $i, j = 1 \dots n$, $i \neq j$, nech g je štandardný skalárny súčin. Potom $g(v_i, v_j) = 0$, teda vlastné vektory symetrickej matice sú ortogonálne.*

Veta 3.1.2. *Nech $A \in \mathbb{R}^{n\times n}$ je symetrická matica. Potom všetky jej vlastné vektory sú reálne.*

Definícia 3.1.1. *Matica $A \in \mathbb{R}^{n\times n}$ je kladne semidefinitná, ak pre všetky $\vec{x} \in \mathbb{R}^n$ platí $\vec{x}^T A\vec{x} \geq 0$.*

Definícia 3.1.2. *Nech A a B sú štvorcové matice stupňa n a nech P je regulárna matica stupňa n. Potom matica A je podobná matici B vtedy a len vtedy, ak $B = PAP^{-1}$.*

Veta 3.1.3. *Nech A a B sú podobné matice, potom ich vlastné hodnoty sú rovnaké a majú rovnakú násobnosť.*

Dôkaz v [2]

Veta 3.1.4. *Nech A je matica, nech $C^{-1}AC$ je matica podobná matici A. Potom ak $\vec{v}$ je vlastný vektor A s prislúchajúcou vlastnou hodnotou λ, tak $C^{-1}\vec{v}$ je vlastný vektor matice $C^{-1}AC$ prislúchajúci vlastnej hodnote λ. Ak $\vec{w}$ je vlastný vektor matice $C^{-1}AC$ s prislúchajúcou vlastnou hodnotou λ, tak $C\vec{w}$ je vlastný vektor matice A prislúchajúci vlastnej hodnote λ.*

Dôkaz v [2]

Definícia 3.1.3. *Náhodný vektor* $\vec{x} = (x_1, \ldots, x_n)^T$, $\vec{x} : \Omega \to \mathbb{R}^n$ *s distribučnou funkciou* F *sa nazýva* absolútne spojitý, *ak existuje taká nezáporná integrovateľná funkcia* $f : \mathbb{R}^n \to \mathbb{R}$, *že pre každé* $\vec{x} = (x_1, \ldots, x_n)^T \in \mathbb{R}^n$ *platí*

$$F(x_1, \ldots, x_n) = \int_{-\infty}^{x_1} \cdots \int_{-\infty}^{x_n} f(t_1, \ldots, t_n) dt_1, \ldots, dt_n$$

Funkciu f *nazývame* hustotou *náhodného vektoru* $\vec{x}$.

Definícia 3.1.4. *O náhodnom vektore* $\vec{x} = (x_1, \ldots, x_m)^T$ *hovoríme, že má* prvé momenty, *ak existujú stredné hodnoty jeho zložiek* $\mathcal{E}(x_1), \ldots, \mathcal{E}(x_n)$ *a výraz*

$$\mathcal{E}(\vec{x}) = \Big(\mathcal{E}(x_1), \ldots, \mathcal{E}(x_n)\Big)^T$$

nazývame jeho strednou hodnotou.

Definícia 3.1.5. *Nech* $\vec{x} = (x_1, \ldots, x_m)^T$ *má konečné druhé momenty,* $\mathcal{E}(x_i^2) < \infty$, $i = 1, \ldots, n$. *Potom* kovarianciou *premenných* x_i, x_j *pre* $1 \leq i, j \leq n$ *budeme nazývať výraz*

$$\operatorname{cov}(x_i, x_j) = \mathcal{E}\bigg(\Big(x_i - \mathcal{E}(x_i)\Big)\Big(x_j - \mathcal{E}(x_j)\Big)\bigg)$$

So zreteľom na praktické použitie je výhodnejší ekvivalentný tvar

$$\operatorname{cov}(x_i, x_j) = \mathcal{E}(x_i x_j) - \mathcal{E}(x_i)\mathcal{E}(x_j)$$

Rozptyl (disperzia, variancia) *premennej* x_i *pre* $1 \leq i \leq n$ *budeme nazývať výraz*

$$\operatorname{var}(x_i) = \operatorname{cov}(x_i, x_i)$$

Definícia 3.1.6. *Nech* $\vec{x} = (x_1, \ldots, x_m)^T$ *je náhodný vektor. Nech pre rozptyl náhodných premenných* x_k, $k = 1, \ldots, n$ *platí* $D(x_k) < \infty$. Kovariančnou maticou *náhodného vektoru* x *nazývame symetrickú* $n \times n$ *rozmernú maticu*

$$\Sigma(\vec{x}) = \begin{pmatrix} \operatorname{var}(x_1) & \operatorname{cov}(x_1, x_2) & \ldots & \operatorname{cov}(x_1, x_n) \\ \operatorname{cov}(x_2, x_1) & \operatorname{var}(x_2) & \ldots & \operatorname{cov}(x_2, x_n) \\ \vdots & \vdots & \ddots & \vdots \\ \operatorname{cov}(x_n, x_1) & \operatorname{cov}(x_n, x_2) & \ldots & \operatorname{var}(x_n) \end{pmatrix}$$

Definícia 3.1.7. *Nech* $\vec{x} = (x_1, \ldots, x_n)^T$ *je náhodný vektor,* $\vec{\mu} = (\mu_1, \ldots, \mu_n)^T$ *je daný vektor a* Σ *je symetrická kladne semidefinitná matica typu* $n \times n$*. Hovoríme, že* $\vec{x}$ *má* n-rozmerné normálne rozdelenie s parametrami $\vec{\mu}, \Sigma$*, píšeme* $\vec{x} \sim N_n(\vec{\mu}, \Sigma)$*, ak pre ľubovoľný vektor* $\vec{a} \in \mathbb{R}^n$ *platí*

$$\vec{a}^T\vec{x} \sim N(\vec{a}^T\vec{\mu}, \vec{a}^T\Sigma\vec{a})$$

t.j. $\vec{a}^T\vec{x}$ *má jednorozmerné normálne rozdelenie so strednou hodnotou* $\vec{a}^T\vec{\mu}$ *a disperziou* $\vec{a}^T\Sigma\vec{a}$*.*

Ak je matica Σ *regulárna, tak hovoríme o regulárnom* n*-rozmernom normálnom rozdelení, ak je singulárna, tak hovoríme o singulárnom* n*-rozmernom rozdelení.*

Veta 3.1.5. *Nech náhodný vektor* $\vec{x} \sim N_n(\mu, \Sigma)$*. Potom*

- *ak* Σ *je regulárna tak* $\vec{x}$ *má hustotu*

$$f(\vec{x}) = f(x_1, \ldots, x_n) = \frac{1}{(2\pi)^{p/2}\|\Sigma\|^{1/2}}\, e^{-\frac{1}{2}(\vec{x}-\vec{\mu})^T\Sigma^{-1}(\vec{x}-\vec{\mu})}$$

- *ak* Σ *je singulárna tak* $\vec{x}$ *má hustotu*

$$f(\vec{x}) = f(x_1, \ldots, x_n) = \frac{(2\pi)^{-k/2}}{\sqrt{\lambda_1, \ldots, \lambda_k}}\, e^{-\frac{1}{2}(\vec{x}-\vec{\mu})^T\Sigma^{-}(\vec{x}-\vec{\mu})}$$

  kde Σ^- *je zovšeobecnená inverzia* Σ *a* $\lambda_1, \ldots, \lambda_k$ *sú nenulové vlastné hodnoty* Σ*.*

Veta 3.1.6. *Nech náhodný vektor* $\vec{x}$ *má* n*-rozmerné normálne rozdelenie* $\vec{x} \sim N_n(\vec{\mu}, \Sigma)$ *a nech* $\vec{y} = A\vec{x} + \vec{c}$*, kde* A *je matica typu* $m \times n$ *a* $\vec{c}$ *je* m*-rozmerný vektor. Potom* $\vec{y}$ *má* m*-rozmerné normálne rozdelenie,* $\vec{y} \sim N_m(A\vec{\mu} + \vec{c}, A\Sigma A^T)$*.*

Dôkaz v [7]

Definícia 3.1.8. *Nech* ε *je postupnosť náhodných premenných z* $\mathbb{R}$ *taká, že* $\varepsilon_i \sim N(0, \sigma^2)$*, kde* σ^2 *je konštanta a pre* $\forall i, j$ $i \neq j$ *platí* $\operatorname{cov}(\varepsilon_i, \varepsilon_j) = 0$*. Potom postupnosti* ε *hovoríme biely šum.*

3.2 Formálna definícia vektorovej mapy a spektrálna doména pre vektorové mapy

Definícia 3.2.1. *Nech $G_M = (V_M, E_M)$ je graf s n vrcholmi a A je matica susednosti grafu G_M, nech S je reálna matica typu $n \times k$ taká, že jej i-ty riadok je vektor súradníc veľkosti k i-teho vrcholu grafu G_M. Potom dvojici $M = (A, S)$ hovoríme* k-rozmerná sieť.

Definícia 3.2.2. *Ak je pre všetky vrcholy počet susedov rovnaký, hovoríme, že sieť je pravidelná, inak je nepravidelná.*

Definícia 3.2.3. *Mapa je 2-rozmerná sieť.*

Poznámka: Nevyžadujeme planárnosť grafu G_M

Poznámka: Keďže v práci sa venujeme mapám, budeme ďalej uvažovať len 2-rozmerné siete a pojmy mapa a sieť budeme používať ako synonymá.

Bez ujmy na všeobecnosti budeme ďalej kvôli zjednodušeniu a lepšej čitateľnosti uvažovať len x-ové súradnice mapy, čiže $\vec{s}$ bude stĺpcový vektor. Neskôr si ozrejmíme, prečo si to môžme dovoliť.

Podľa našich vedomostí optimalita bázy pre steganografiu a digitálnu vodotlač pre vektorové mapy nebola skúmaná a doposiaľ neexistuje na jej popis žiadny formálny model. Pri budovaní formálneho modelu na popis vlastností spektrálnej bázy využijeme prácu [14], ktorá sa síce vôbec nevenuje steganografii, ale je možné ju prispôsobiť pre teoretický popis spektrálnej bázy, ktorá je odolná proti útoku zašumením a proti útoku vyhladzovaním. S týmto modelom budeme schopní porovnať vlastnosti existujúcich transformačných algoritmov a nájsť možnosti na ich zlepšenie.

Keď zašumíme sieť, tak tým rovnakou mierou modifikujeme všetky prvky S. Ako sme si povedali v časti 2.3.1, hľadáme bázu, v ktorej sa tieto zmeny prejavia čo najmenej. Čiže potrebujeme bázu, kde vieme povedať, v ktorej časti vektoru je väčšina informácie siete. Súčasne od bázy vyžadujeme, aby zápis správy čo najmenej vizuálne poškodil mapu.

Súradnice vrcholov mapy nie sú nezávislé, ale väčšinou korelujú so súradnicami svojich susedov. Práve táto korelácia sa využíva na výpočet spektrálnej bázy. Tu je namieste pripomenúť, že zmeny v matici susednosti výrazne ovplyvňujú tieto korelácie, keď pridaním, alebo odobratím hrany medzi vrcholmi i a j pridávame, alebo rušíme závislosť medzi súradnicami vrcholov i a j.

Zašumenie siete formálne definujeme takto:

Definícia 3.2.4. *Nech $M = (A, \vec{s})$ je sieť, nech $\vec{\varsigma} = \vec{s} + \vec{\varepsilon}$, kde $(\varepsilon_1, \ldots, \varepsilon_n)$ je biely šum. Dvojici $\mathcal{M} = (A, \vec{\varsigma})$ budeme hovoriť náhodná sieť.*

$\mathcal{M} = (a, \vec{\varsigma})$ je teda náhodná sieť, u ktorej stredná hodnota súradníc predstavuje súradnice pôvodnej siete.

Definícia 3.2.5. *Nech $M = (A, \vec{s})$ je sieť s n vrcholmi, nech B je n-rozmerná ortonormálna báza nad $\mathbb{R}^n$ a $B_{j.}$ je j-ty riadok matice B. Prevod $\vec{s}$ do bázy B je*

$$\vec{\hat{s}} = B^{-1}\vec{s}$$

Prevod $\vec{\hat{s}}$ späť do bázy I je

$$\vec{s} = B\vec{\hat{s}}$$

čiže

$$\vec{s} = \sum_{j=1}^{n} B_{j.}\hat{s}_j$$

Tomuto prevodu budeme hovoriť dekompozícia $\vec{s}$ vzhľadom na B. Projekcia $\vec{s}$ na m-rozmerný podpriestor daný prvými m $(m < n)$ vektormi B je

$$\vec{s}_{(B,m)} = \sum_{j=1}^{m} B_{j.}\hat{s}_j$$

Teraz je už zrejmé, prečo si môžme dovoliť uvažovať vektor súradníc namiesto matice súradníc.

Keďže B je ortonormálna, platí $\|\vec{s}\| = \|\vec{\hat{s}}\|$. Dekompozícia je užitočná, ak sa väčšina informácie reprezentovanej pôvodným vektorom $\vec{s}$ nachádza v čo najmenšej časti vektoru $\vec{\hat{s}}$. Je zrejmé, že optimálna báza pre konkrétny

vektor $\vec{s}$ je vždy $\begin{pmatrix} s_1 & 0 & \dots & 0 \\ s_2 & 0 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ s_n & 0 & \dots & 0 \end{pmatrix}$. Aká je ale optimálna báza pre zašumený vektor?

Definícia 3.2.6. *Nech $\mathcal{M} = (A, \vec{s})$ je náhodná sieť so strednou hodnotou μ a kovariančnou maticou Σ. Hovoríme, že báza Θ je optimálna pre dané rozdelenie náhodného signálu, ak je ortonormálna a minimalizuje bázovú reštrikčnú chybu t.j.*

$$\forall P \ \forall m < n : \ \mathcal{E}(\|\vec{s} - \vec{s}_{(\Theta,m)}\|) \leq \mathcal{E}(\|\vec{s} - \vec{s}_{(P,m)}\|)$$

Ortonormalitu bázy Θ vyžadujeme kvôli minimalizácii vizuálneho poškodenia mapy vplyvom vloženia správy.

Veta 3.2.1. *Nech $\mathcal{M} = (A, \vec{s})$ je náhodná sieť. Potom $\vec{s}$ má singulárne viacrozmerné normálne rozdelenie.*

Dôkaz v [14]

Definícia 3.2.7. *Nech $M = (A, \vec{s})$ je sieť s n vrcholmi, nech P je matica, $P \in \mathbb{R}^{n \times n}$, nech $\lambda_1 \leq \lambda_2 \leq \cdots \leq \lambda_n$ sú vlastné čísla matice P s prislúchajúcimi normalizovanými vlastnými stĺpcovými vektormi $\vec{b_1}, \dots, \vec{b_n}$ tvoriacimi bázu. Položme $B = \left(\vec{b_1}, \dots, \vec{b_n}\right)$. Spektrálna dekompozícia (eigenvalue decomposition) $\vec{s}$ vzhľadom na P je*

$$\vec{s} = B\vec{\hat{s}} = \sum_{j=1}^{n} \vec{b_j}\hat{s}_j$$

kde $\vec{\hat{s}} \in \mathbb{R}$ sa nazýva ED-transformácia *$\vec{s}$ vzhľadom na P.*
Inverzná ED-transformácia *je*

$$\vec{\hat{s}} = B^{-1}\vec{s}$$

Projekcia $\vec{s}$ na m-rozmerný podpriestor daný prvými m $(m < n)$ vlastnými vektormi P je

$$\vec{s}_{(P,m)} = \sum_{j=1}^{m} \vec{b}_j\hat{s}_j$$

Veta 3.2.2. *Nech $\mathcal{M} = (A, \vec{s})$ je náhodná sieť so strednou hodnotou μ a kovariančnou maticou Σ. Pre dané rozdelenie náhodného signálu je optimálna báza daná spektrálnou dekompozíciou autokorelačnej matice $\Phi = \Sigma + \mu\mu^T$. ED-transformácia vzhľadom na Φ sa nazýva KL-transformácia.*

Toto je známy výsledok, ale problém je, že výpočet Φ je príliš drahý, ale keďže pri ED-transformácii využijeme len vlastné vektory Φ, stačí nájsť inú maticu s rovnakými vlastnými vektormi ako má Φ.

Definícia 3.2.8. *Nech $M = (A, \vec{s})$ je sieť s n vrcholmi, nech $G = (V_M, E_M)$ je jej graf. Nech d_i je stupeň i-teho vrcholu grafu. Kirchhoffov operátor $K \in \mathbb{R}^{n\times n}$ pre M je*

$$K_{ij} = \begin{cases} d_i & ak\ i = j \\ -1 & ak\ (i,j) \in E(M) \\ 0 & inak \end{cases}$$

Niektoré zaujímavé vlastnosti Kirchhoffovho operátora K (viď [13]):

- Je symetrický a teda z vety 3.1.1 vyplýva, že má ortogonálne vlastné vektory.
- $\forall i \left(\sum_j K_{ij}\right) = \left(\sum_j K_{ji}\right) = 0$
- Počet nulových vlastných hodnôt je rovnaký ako počet komponentov sieťového grafu.
- Vlastné hodnoty sú v intervale $\langle 0, 2\Delta(G)\rangle$, kde $\Delta(G)$ je maximálny stupeň grafu G.

Veta 3.2.3. *Nech $\mathcal{M} = (A, \vec{s})$ je náhodná sieť so strednou hodnotou μ a kovariančnou maticou Σ. Nech Φ je autokorelačná matica $\vec{s}$, K je Kirchhoffov operátor pre M. Potom vlastné vektory K sú až na poradie rovnaké ako vlastné vektory Φ.*

Dôkaz v [14]

Dôsledok 3.2.1. *ED-transformácia $\vec{s}$ vzhľadom na K je optimálna.*

Poznámka: Starší dôkaz platnosti toho tvrdenia pre jednorozmerný prípad a pre dvojrozmerný prípad s nekrižujúcimi sa hranami je v [1]. Tento dôkaz nerozoberal prípad, ak $I - K$ je singulárna matica.

Definícia 3.2.9. *Nech $M = (A, \vec{s})$ je sieť s n vrcholmi, nech $G = (V_M, E_M)$ je jej graf. Nech d_i je stupeň i-teho vrcholu grafu. Tutte-Laplacov operátor $T \in \mathbb{R}^{n \times n}$ pre M je*

$$T_{ij} = \begin{cases} 1 & ak\ i = j \\ -1/d_i & ak\ (i,j) \in E(M) \\ 0 & inak \end{cases}$$

Niektoré zaujímavé vlastnosti Tutte-Laplacovho operátora T (viď [13]):

- Nie je symetrický a jeho vlastné vektory nie sú ortogonálne.
- Má reálne vlastné čísla z intervalu $\langle 0, 2 \rangle$
- $\forall i : \sum_j T_{ij} = 0$
- Práve jedna vlastná hodnota je 0.

Z týchto vlastností vyplýva nasledujúca veta

Veta 3.2.4. *Nech $\mathcal{M} = (A, \vec{s})$ je náhodná sieť so strednou hodnotou μ a kovariančnou maticou Σ, nech T je Tutte Laplacov operátor pre M. Potom vlastné čísla matice T sú reálne a ED-transformácia $\vec{s}$ vzhľadom na T nie je optimálna.*

ED-transformáciu vzhľadom na T použili Karni a Gotsman ako bázu pre spektrálnu kompresiu 3D siete[4]. Neskôr ju použili Ohbuchi, Ueda a Endoh ako spektrálnu bázu pre digitálnu vodotlač vektorových máp[11], popis ich algoritmu uvádzame v časti 4.2.2. Hlavnou nevýhodou tejto bázy je to, že operátor T nie je symetrický, a teda výpočet vlastných vektorov je oveľa náročnejší, a výsledná spektrálna báza nie je ortonormálna a teda ani optimálna.

Definícia 3.2.10. *Nech $M = (A, \vec{s})$ je sieť s n vrcholmi, nech $G = (V_M, E_M)$ je jej graf. Nech d_i je stupeň i-teho vrcholu grafu. Normalizovaný grafový laplacov operátor $\mathcal{G} \in \mathbb{R}^{n \times n}$ pre M je*

$$\mathcal{G}_{ij} = \begin{cases} 1 & ak\ i = j \\ -1/\sqrt{d_i d_j} & ak\ (i,j) \in E(M) \\ 0 & inak \end{cases}$$

Niektoré zaujímavé vlastnosti normalizovaného grafového Laplacovho operátora $\mathcal{G}$ (viď [13]):

- $\mathcal{G}$ je pozitívne semidefinitná.
- Práve jedna vlastná hodnota je 0 a k nej prislúchajúci vlastný vektor nie je vo všeobecnosti konštantný.
- $\exists i \sum_j \mathcal{G}_{ij} \neq 0$

Veta 3.2.5. *Nech $\mathcal{M} = (A, \vec{s})$ je náhodná sieť so strednou hodnotou μ a kovariančnou maticou Σ, nech $\mathcal{G}$ je normalizovaný grafový laplacov operátor pre M. Potom ED-transformácia $\vec{s}$ vzhľadom na $\mathcal{G}$ nie je optimálna.*

Dôkaz v [13]

Definícia 3.2.11. *Nech $M = (A, \vec{s})$ je sieť s n vrcholmi, nech T je jej Tutte Laplacov operátor. Symetrický druhorádový Tutte Laplacov operátor $U \in \mathbf{R}^{n \times n}$ pre M je*

$$U = T^T T$$

Niektoré zaujímavé vlastnosti symetrického druhorádového Tutte Laplacov operátora U (viď [13]):

- U je pozitívne semidefinitný.
- Je symetrický a teda z vety 3.1.1 vyplýva, že má ortogonálne vlastné vektory.
- $\forall i \sum_j U_{ij} = 0$

- Práve jedna vlastná hodnota je 0, a ak je sieť spojitá, tak prislúchajúci vlastný vektor je konštantný

Veta 3.2.6. *Nech $\mathcal{M} = (A, \vec{s})$ je náhodná sieť so strednou hodnotou μ a kovariančnou maticou Σ, nech Φ je autokorelačná matica $\vec{s}$, U je symetrický druhorádový Tutte Laplacov operátor pre M. Potom vlastné vektory U sú až na poradie rovnaké ako vlastné vektory Φ.*

Dôkaz v [14]

Dôsledok 3.2.2. *ED-transformácia $\vec{s}$ vzhľadom na U je optimálna.*

Je dôležité si uvedomiť, že uvedené vety o optimalite ED-transformácie vzhľadom na Φ, K a U platia pre náhodnú sieť, čiže pre danú sieť sú len rôznymi aproximáciami optimálnej bázy. Pri použití operátorov $\mathcal{G}$ a T tiež dostaneme dobré výsledky, tieto však nie sú optimálne a nevieme o nich povedať, do akej miery sú dobré.

Tiež je dôležité si uvedomiť, že tento formálny model, tak ako je budovaný, hovorí o odolnosti proti útoku zašumením a algoritmy, ktoré sú na ňom založené, majú veľkú odolnosť proti zašumeniu. Keďže tento model je postavený na závislostiach definovaných maticou susednosti, zmeny v tejto matici spôsobia vypočítanie inej bázy. Keďže v optimálnej báze je väčšina informácie na začiatku vektora, vzniká otázka, či je výpočet optimálnej bázy nezávislý na poradí vrcholov.

Lema 3.2.1. *Nech $M_1 = (A_1, \vec{s}_1)$ je sieť s n vrcholmi, nech $M_2 = (A_2, \vec{s}_2)$ je sieť, ktorá vznikla zo siete M_1 poprehadzovaním vrcholov, nech $C \in \mathbb{R}^{n \times n}$ je permutačná matica, čiže platí $A_1 = C^T A_2 C$. Nech K_1 respektíve K_2 je Kirchhoffov operátor pre M_1 respektíve M_2, Nech T_1 respektíve T_2 je Tutte-Laplacov operátor pre M_1 respektíve M_2, Nech U_1 respektíve U_2 je symetrický druhorádový Tutte-Laplacov operátor pre M_1 respektíve M_2, Potom platí*

- $$K_1 = C^T K_2 C$$
- $$T_1 = C^T T_2 C$$

- $$U_1 = C^T U_2 C$$

Dôkaz. Nech D_1 je diagonálna matica taká, že v i-tom riadku a i-tom stĺpci je stupeň i-teho vrcholu siete M_1.
Nech D_2 je diagonálna matica taká, že v i-tom riadku a i-tom stĺpci je stupeň i-teho vrcholu siete M_2.
Je zrejmé že premutačná matica C je ortogonálna a platí $CC^T = I = C^T C$.

$$K_1 = D_1 - A_1 = C^T D_2 C - C^T A_2 C = C^T (D_2 - A_2) C = C^T K_2 C$$

$$T_1 = I - D_1^{-1} A_1 = C^T I C - C^T D_2^{-1} C C^T A C = C^T (I - D_2^{-1} A_2) C = C^T T_2 C$$

$$U_1 = T_1^T T_1 = (C^T T_2 C)^T C^T T_2 C = ((C^T T_2) C)^T C^T T_2 C =$$
$$= C^T (C^T T_2)^T C^T T_2 C = C^T T_2^T C C^T T_2 C = C^T T_2^T T_2 C = C^T U_2 C$$

□

Tvrdenie 3.2.1. *Nech $M_1 = (A_1, \vec{s}_1)$ a $M_2 = (A_2, \vec{s}_2)$ sú siete s n vrcholmi, nech P_1, P_2 sú matice, $P_1, P_2 \in \mathbb{R}^{n \times n}$, nech $\vec{\hat{s}}_1$ je ED-transformácia $\vec{s}_1$ vzhľadom na P_1 a nech $\vec{\hat{s}}_2$ je ED-transformácia $\vec{s}_2$ vzhľadom na P_2. Nech existuje ortogonálna matica $C \in \mathbb{R}^n$ taká, že*

$$\vec{s}_1 = C^{-1} \vec{s}_2$$

a

$$P_1 = C^T P_2 C$$

Potom

$$\vec{\hat{s}}_1 \neq \vec{\hat{s}}_2$$

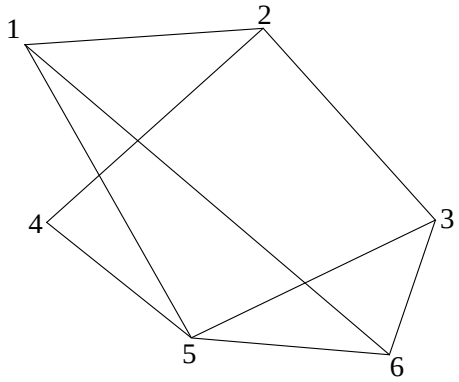
Dôkaz. Nech $\lambda_1 \leq \ldots \leq \lambda_n$ sú vlastné čísla matice P_1 s prislúchajúcimi vlastnými vektormi $\vec{v}_1, \ldots, \vec{v}_n$.
Z vety 3.1.3 vyplýva, že $\lambda_1, \ldots, \lambda_n$ sú vlastné čísla matice P_2.
Z vety 3.1.4 vyplýva, že $C^T \vec{v}_1, \ldots, C^T \vec{v}_n$ sú vlastné vektory matice P_2 prislúchajúce vlastným číslam $\lambda_1, \ldots, \lambda_n$.
Z toho plynie

$$\vec{\hat{s}}_2 = C^T V \vec{s}_2 = C^T V C \vec{s}_1 \neq V \vec{s}_1 = \vec{\hat{s}}_1$$

□

Keďže permutačné matice sú ortonormálne, ED-transformácia vzhľadom na K ani vzhľadom na U nie je odolná proti otrogonálnym podobnostným transformáciám, a teda ani proti poprehadzovaniu vrcholov.

$$K = \begin{pmatrix} 3 & -1 & 0 & 0 & -1 & -1 \\ -1 & 3 & -1 & -1 & 0 & 0 \\ 0 & -1 & 3 & 0 & -1 & -1 \\ 0 & -1 & 0 & 2 & -1 & 0 \\ -1 & 0 & -1 & -1 & 4 & -1 \\ -1 & 0 & -1 & 0 & -1 & 3 \end{pmatrix}$$



$$T = \begin{pmatrix} 1.000000 & -0.333333 & 0.000000 & 0.000000 & -0.333333 & -0.333333 \\ -0.333333 & 1.000000 & -0.333333 & -0.333333 & 0.000000 & 0.000000 \\ 0.000000 & -0.333333 & 1.000000 & 0.000000 & -0.333333 & -0.333333 \\ 0.000000 & -0.500000 & 0.000000 & 1.000000 & -0.500000 & 0.000000 \\ -0.250000 & 0.000000 & -0.250000 & -0.250000 & 1.000000 & -0.250000 \\ -0.333333 & 0.000000 & -0.333333 & 0.000000 & -0.333333 & 1.000000 \end{pmatrix}$$

$$\mathcal{G} = \begin{pmatrix} 1.000000 & -0.333333 & 0.000000 & 0.000000 & -0.288675 & -0.333333 \\ -0.333333 & 1.000000 & -0.333333 & -0.408248 & 0.000000 & 0.000000 \\ 0.000000 & -0.333333 & 1.000000 & 0.000000 & -0.288675 & -0.333333 \\ 0.000000 & -0.408248 & 0.000000 & 1.000000 & -0.353553 & 0.000000 \\ -0.288675 & 0.000000 & -0.288675 & -0.353553 & 1.000000 & -0.288675 \\ -0.333333 & 0.000000 & -0.333333 & 0.000000 & -0.288675 & 1.000000 \end{pmatrix}$$

$$U = \begin{pmatrix} 1.284722 & -0.666666 & 0.284722 & 0.173611 & -0.472222 & -0.604166 \\ -0.666666 & 1.472222 & -0.666666 & -0.833333 & 0.472222 & 0.222222 \\ 0.284722 & -0.666666 & 1.284722 & 0.173611 & -0.472222 & -0.604166 \\ 0.173611 & -0.833333 & 0.173611 & 1.173611 & -0.750000 & 0.062500 \\ -0.472222 & 0.472222 & -0.472222 & -0.750000 & 1.583333 & -0.361111 \\ -0.604166 & 0.222222 & -0.604166 & 0.062500 & -0.361111 & 1.284722 \end{pmatrix}$$

Obr. 3.1: Príklad nepravidelnej siete a jej operátorov K, T, $\mathcal{G}$ a U.

Kapitola 4

Podrobnejšie štúdium vybraných steganografických algoritmov

4.1 Steganografické systémy pracujúce v priestorovej doméne, pre vektorové mapy

V tejto časti popíšeme algoritmy pracujúce v priestorovej doméne. Väčšina z nich je krehká, a teda nevhodná pre digitálnu vodotlač. Dajú sa rozdeliť do skupín podľa toho, ako ukladajú správu.

4.1.1 Algoritmy ukladajúce správu zmenením súradníc vrcholov

Sú to najjednoduchšie algoritmy. Vkladajú správu do najmenej významných bitov v súradniciach vrcholov, preto sa im niekedy hovorí sa aj *roztrasené* (jittering). Ich vlastnosti a využiteľnosť sú veľmi podobné vlastnostiam algoritmu LSB [1]. Jedinými prednosťami sú možnosť vložiť pomerne veľkú správu, a to že pri dobrom algoritme, ktorý nemení štatistické vlastnosti šumu, do

[1] Popis algoritmu LSB je v časti 2

ktorého sa vkladá správa nie je možný extrakčný ani detekčný útok. Na prevedenie mazacieho útoku stačí ľubovoľná zmena v modifikovaných dátach. Ak na uloženie správy algoritmus používa pomery súradníc, tak je odolný aj proti zmene veľkosti. Alternatívne možno krehký algoritmus využiť na detekciu zmeny predlohy. Ak sa z označených dát podarí extrahovať správu, tak dáta neboli po označení nijako menené, ak sa to nepodarí, tak nastala nejaká zmena v označených dátach.

4.1.2 Algoritmy ukladajúce správu zmenením dĺžok hrán

Embedding modifikuje vzdialenosti medzi vrcholmi. Hlavná myšlienka je, že pri orezávaní, alebo geometrických transformáciách sa menia súradnice vrcholov, ale pomery vzájomných vzdialeností sa nemenia. Princíp je podobný ako pri roztrasených algoritmoch, len sa nepoužívajú vrcholy, ale hrany. Ich vlastnosti sú rovnaké ako vlastnosti roztrasených algoritmov. Majú navyše výhodu odolnosti voči rotáciám, ale táto výhoda nemá pri mapách veľký význam, keďže mapy majú sever vždy hore. Ak na uloženie správy algoritmus používa pomery dĺžok strán, tak je odolný aj proti zmene veľkosti.

4.1.3 Algoritmy ukladajúce správu pridávaním nových vrcholov

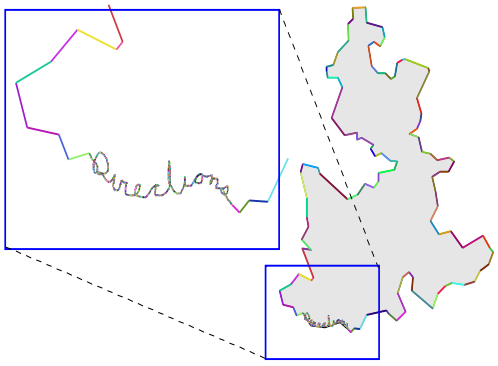
Ďalšia trieda algoritmov vkladá správu ako postupnosť bodov na čiaru. Systémy odolávajú bežným geometrickým transformáciám. Sú teda odolnejšie proti neúmyselným útokom. Ich veľkým problémom je to, že veľmi zväčšujú veľkosť predlohy (na každý bit (prípadne bajt) správy spotrebujú dve desatinné čísla). Ďalší problém je, že takto vložená správa nepreživje žiadnu procedúru na odstraňovanie zbytočných vrcholov. Tento problém sa dá vyriešiť miernym posunutím pridaných vrcholov v smere kolmom na čiaru, na ktorú boli vložené. Trochu agresívne odstraňovanie zbytočných vrcholov aj tak odstráni vloženú správu. Úmyselný extrakčný útok na ne je triviálny.

4.1.4 Algoritmy ukladajúce správu zmenením atribútov hrán

Správa sa ukladá do atribútov hrán, ako sú napríklad farba, alebo hrúbka. Výhodou je jednoduchosť, možnosť uložiť veľkú správu, odolnosť voči bežným transformáciám. Nevýhody sú jednoduché odhalenie aj odstránenie, a problémy pri strojovom použití máp, kde atribút má často ešte nejaký špeciálny význam. Preto nie sú vhodné pre steganografiu, a ani pre digitálnu vodotlač.

4.1.5 Rukopis

Rukopis(Handwriting) nahradí časť čiar textom viď obrázok 4.1. Ukrytie správy zabezpečuje použitie malého písma. Prežije geometrické transformácie, vkladanie vrcholov, orezávanie. V článku[3] autor tvrdí, že technika je odolná aj proti zašumeniu, s tým však nemôžem súhlasiť, lebo ukrytá správa je oveľa menej odolná voči zašumeniu ako predloha. Nevýhodou je obrovský nárast počtu vrcholov, vzniknuté priesečníky môžu robiť problémy pri používaní, neprežije stratovú kompresiu, správa je ukrytá len pred ľudským okom a ukáže sa pri zväčšení, detekčný, extrakčný aj mazací útok sú triviálne.



Obr. 4.1: Rukopis

Žiaden s týchto algoritmov nie je odolný voči vyhladzovaniu, a ani voči stratovej kompresii mapy. Pri ich implementácii treba zvážiť odolnosť implementácie proti útoku poprehadzovaním vrcholov.

4.1.6 Veľké lokálne deformácie

V civilných mapách, ktoré zverejňuje Vojenský kartografický ústav Harmanec sú v okolí vojenských objektov výrazné odlišnosti medzi tým, čo je zakreslené v mape a skutočnosťou. Robia to asi preto, aby sa ich mapy nedali využiť pri útoku na tieto objekty.Táto technika sa však dá využiť aj pri vodotlači. Na málo frekventovaných miestach sa výrazne pomenia smery elektrických vedení, ciest, potokov, vrstevníc,. . . , ale tak, aby sa to ešte podobalo na pôvodnú krajinu. Jediný možný útok, ale aj jediný možný spôsob dokázania autorstva, vyžaduje porovnanie označených dát s inými dátami, alebo meraniami v teréne. Veľká nevýhoda tohto spôsobu je obtiažna orientácia v teréne, prípadne problémy s plánovaním na tom mieste, kde je mapa takto upravená.

4.1.7 Robustná vodotlač pre vektorové mapy

Doteraz sme si ukázali algoritmy, ktoré kvôli svojej krehkosti neboli vhodné pre vodotlač. Ohbuchi, Ueda a Endoh [8] spravili robustný, závislý algoritmus pre digitálnu vodotlač. Jeho robustnosť je založená na veľkej redundancii vloženej správy. Každý bit správy je zapísaný c-krát, v pozícii aspoň d vrcholov. Tento algoritmus je zaujímavý a preto sa mu budeme venovať podrobnejšie.

Vkladanie správy

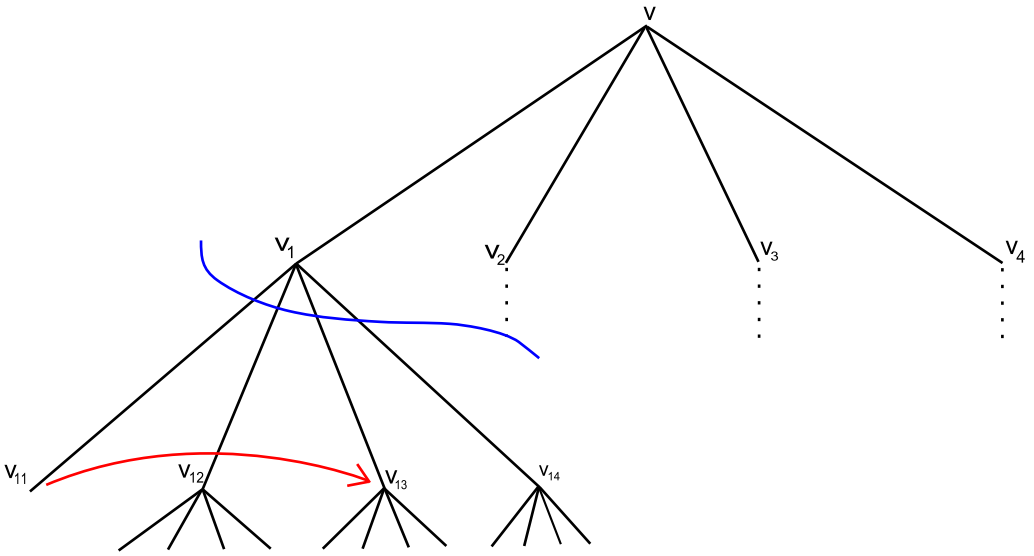
Algoritmus sa najprv pokúsi rozdeliť mapu M na obdĺžnikové podsiete tak, aby

- každý obdĺžnik obsahoval aspoň d vrcholov
- mali všetky obdĺžniky približne rovnako veľa vrcholov

Hodnota d je výsledkom kompromisu. Zvyšovaním d sa zvyšuje odolonosť bitu vloženého do obdĺžnika vďaka spriemerneniu šumu, ale znižuje celkový počet obdĺžnikov. To znamená menší chip rate c, menšiu odolnosť proti orezávaniu, zašumeniu a iným útokom. Na rozdelenie mapy na obdĺžniky sa použije jedna z týchto metód:

- *rovnaké rozdelenie* rozdelí mapu na rovnaké časti s rozmerom $k \times l$

- na rozdelenie mapy sa použije *kvadrantový strom* tak, aby každý obdĺžnik obsahoval aspoň d vrcholov
- *modifikovaný kvadrantový strom* pracuje podobne ako kvadrantový strom, ale ak niektorý obdĺžnik obsahuje menej ako d vrcholov je spojený so svojim bratom s najmenším počtom vrcholov, tak aby vznikol obdĺžnik.



Obr. 4.2: Rozdiel medzi kvadrantovým stromom a modifikovaným kvadrantovým stromom.

Obrázok 4.2 znázorňuje rozdiel medzi kvadrantovým stromom a modifikovaným kvadrantovým stromom v prípade, že obdĺžniky mapy reprezentované uzlami $v_1, \ldots, v_4, v_{12}, v_{13}, v_{14}$ obsahujú viac ako d vrcholov mapy a uzol v_{11} má menej ako d vrcholov. Pričom uzol v_{13} má menej vrcholov ako uzol v_{12}. V kvadrantovom strome je uzol v_1 listom, lebo v_{11} má menej ako d vrcholov. V modifikovanom kvadrantovom strome sa uzly $, v_{11}, v_{13}$ spoja a budovanie stromu pokračuje, až kým všetky listy majú od d do $2d - 1$ vrcholov.

Nech L je počet obdĺžnikov, ktoré majú aspoň d vrcholov, kde $L < n$, potom $c = \lfloor L/n \rfloor$. Ďalej uvažujeme len obdĺžniky ktoré majú aspoň d vrcholov. Označme si ich $M_1, \ldots, M_L$.

Nech $|M_i|$ označuje počet vrcholov v obdĺžniku M_i

Na vloženie správy sa použije nasledovné kódovanie. Nech $a = (a_1, \ldots, a_n)$ je vstupný vektor (správa ktorú chceme uložiť). Opakovacia konštanta c chip rate označuje počet opakovaní každého bitu správy. $\alpha > 0$ je modulačná amplitúda. Na opakovanie správy použije

- opakovanie bitov

$$b = (\overbrace{a_1, \ldots, a_1}^{c\text{-krát}}, \overbrace{a_2, \ldots, a_2}^{c\text{-krát}}, \ldots, \overbrace{a_n, \ldots, a_n}^{c\text{-krát}})$$

- opakovanie správy

$$b = (\overbrace{a_1, \ldots, a_n, a_1, \ldots, a_n, \ldots, a_1, \ldots, a_n}^{c\text{-krát}}$$

Bez ujmy na všeobecnosti budeme ďalej kvôli zjednodušeniu a lepšej čitateľnosti uvažovať len x-ové súradnice mapy. Označme $s_{i,h}$ súradnicu h-tého vrcholu ($1 \leq h \leq |M_i|$) vo štvorci M_i pred vkladaním správy a $\tilde{s}_{i,h}$ je jeho súradnica po vložení správy, $\vec{p}$ je pseudonáhodný vektor $p_i \in \{-1, 1\}$ vygenerovaný z kľúča k a $\alpha > 0$ je modulačná amplitúda. Potom

$$\tilde{s}_{i,h} = s_{i,h} + b'_i p_i \alpha \text{ kde } b'_i = \begin{cases} -1 & \text{ak } b_i = 0 \\ 1 & \text{ak } b_i = 1 \end{cases}$$

Kľúč k je potrebný na extrakciu. Modulačná amplitúda α sa zvolí tak, aby sa vložením správy nezhoršil výzor mapy a zároveň tak, aby sa dosiahla požadovaná odolnosť proti útoku zašumením súradníc vrcholov.

Extrakcia správy

- Normalizácia slúži na odstránenie afinných transformácií, ktoré boli použité na označenú mapu $\tilde{M}$. Algoritmus nájde navzájom si prislúchajúce dvojice významných bodov v predlohe mape M a v označenej mape $\tilde{M}$. Potom na mape $\tilde{M}$ spraví malé rotácie, posunutia, škálovacie transformácie, tak aby minimalizoval euklidovskú vzdialenosť medzi pármi významných bodov v oboch mapách. Autori žiaľ nenapísali, čo považujú za významné body a ako ich spárujú

- Spárovanie vrcholov a nájdenie vrcholov, ktoré boli vložené pri útoku, alebo odstránené[2]

- Demodulácia správy. Rekonštrukcia i-teho bitu správy sa robí hlasovaním všetkých bitov vo všetkých obdĺžnikoch, do ktorých bola správa zapísaná.
  Nech H_i je množina indexov obdĺžnikov do ktorých bol zapísaný i-ty bit správy.

$$H_i = \begin{cases} \{(i-1)c+1, (i-1)c+2, \ldots, ic\} & \text{pri opakovaní bitov} \\ \{i, i+n, \ldots, i+cn\} & \text{pri opakovaní správy} \end{cases}$$

  Potom i-ty bit správy a_i vypočíta takto

$$a_i = \frac{\operatorname{sgn}\left(\sum_{j \in H_i} \sum_{h=1}^{|M_j|} \overbrace{(\tilde{s}_{j,h} - s_{j,h})p_j}^{b'_i \alpha}\right) + 1}{2}$$

Označené dáta sú pri parametroch $d = 10$ a $\alpha = 1$ (10cm v skutočnom svete) pre laika nerozoznateľné od originálu. Pri rozdelení predlohy pomocou modifikovaného kvadrantového stromu sa dosahujú najlepšie výsledky. Správu je lepšie opakovať celú, ako opakovať ju po bitoch, pretože potom je každý bit správy uložený na rôznych miestach mapy, čo zvyšuje odolnosť proti útoku orezávaním.
Algoritmus je robustný vďaka vysokej redundancii. Každý bit vloženej správy je v označenej mape vložený aspoň cd-krát. Jeho veľkou slabinou môže byť výber významných bodov. Autori ho nepopisujú, ale ak sú významné body ľavé dolné súradnice nápisov, tak ako v ich neskoršom algoritme[3], tak útočníkovi na prezentačný útok stačí popresúvať tieto body, to v prípade nápisov mape moc neublíži a algoritmus afinné transformácie neodstráni, ale pridá ďalšie. Následne zle spáruje body z oboch máp. Tento útok na detekčný algoritmus vodotlač neodstráni. Algoritmus je odolný proti pridávaniu a odoberaniu hrán, lebo pri extrakcii správy ignoruje maticu susednosti označenej

[2] Autori nepopi sujú ako prebieha táto časť. Predpokladám, že rovnako ako v ich novšom algoritme4.2.2.

[3] Jeho popis je v 4.2.2

mapy.
Ťažší, avšak oveľa nebezpečnejší interpretačný útok by bol možný, ak by sa dal k postupnosti p vypočítať kľúč k na jej generovanie. Potom by si útočník k označenej mape $\tilde{s}$ zvolil vhodnú správu a' a vypočítal vhodný kľúč k' tak, aby mu vyšlo vhodné b''_i, aby platilo $\tilde{s}_{i,h} = s'_{i,h} + b''_i p'_i \alpha$. Potom by mohol tvrdiť, že autor mu ukradol jeho mapu[4]. Autori na toto nebezpečenstvo neupozornili.

4.2 Steganografické systémy pre vektorové mapy pracujúce v transformačnej doméne

Cieľom týchto algoritmov je uložiť správu do významných miest mapy a tým sťažiť jej odstránenie.

4.2.1 Wavelet vodotlač pre vektorové mapy

Wavelet je steganografické metóda určená pre bitmapové obrázky. Kitamura a kol.[5] spravili algoritmus, ktorý transformuje mapu do dvojrozmerného poľa skalárov tak, že rozdelí mapu na štvorcovú sieť. Každý štvorec je reprezentovaný v poli jedným číslom. Teda k ľubovoľnej vygeneruje nejaký rastrový obrázok. Na tento obrázok sa potom použije wavelet steganografický systém[6] pre bitmapový obrázok. Robustnosť takéhoto algoritmu záleží od robustnosti transformácie a od robustnosti wavelet steganografického systému.

[4]Takáto podvodná vodotlač by sa potom nachádzala aj v originále nič netušiaceho autora.

[5]I. Kitamura, S. Kanai, T. Kishinami, Watermarking Vector Digital Map usig Wavelet Transformation, Proc. Annual Conference of Geographical Information Systems Association (GISA) 2000, Vol.9, pp.417-4421, 2000 len po japonsky.

[6]Opis wavelet steganografického systému je mimo témy tejto diplomovej práce, čitateľ ho môže nájsť v [6].

4.2.2 Vodotlač v sieťovo-spektrálnej doméne pre vektorové mapy

Táto transformačná robustná závislá vodotlač je zdokonalením predchádzajúceho algoritmu. Na zvýšenie robustnosti používa spektrálnu bázu, ktorú využili Karni a Gotsman[4] pre stratovú kompresiu 3d siete.

Vkladanie správy

- *Delaunayova triangulácia*, autori nepopisujú aká je jej úloha v algoritme. Ďalej ukážeme, že je veľmi dôležitá.

- *k-d stromové rozdelenie* je dvojrozmerné zovšeobecnenie binárneho vyhľadávacieho stromu. Rozdelí množinu bodov pozdĺž osy x na stĺpce s približne rovnakým počtom vrcholov, a potom pre každý stĺpec zvlášť rozdelí množinu bodov podľa osy y na obdĺžniky s približne rovnakým počtom vrcholov. Zvyšuje odolnosť proti orezávaniu a znižuje výpočtovú náročnosť spektrálnej analýzy. Toto rozdelenie je lepšie ako v predchádzajúcom algoritme 4.1.7. Bez ujmy na všeobecnosti budeme ďalej kvôli zjednodušeniu a lepšej čitateľnosti uvažovať len x-ové súradnice mapy.

- *spektrálna analýza* pre každý štvorec vypočíta spektrálnu bázu. Nech $\vec{s_i}$ je vektor súradníc siete M_i, nech T_i je jej Tutte Laplacov operátor vypočítaný s triangulácie, nech $\vec{\hat{s}_i}$ je ED-transformácia $\vec{s_i}$ vzhľadom na T_i. Potom $\vec{\hat{s}_i}$ je reprezentácia $\vec{s_i}$ v spektrálnej bázy.

- *modulácia* prebieha rovnako ako predchádzajúcom algoritme 4.1.7, s tým rozdielom, že sa používa transformovaný vektor súradníc $\vec{\hat{s}_i}$ a používa sa opakovanie bitov správy.

Extrakcia správy

- *Pose normalizácia* jej účelom je odstrániť afinné transformácie. Použije sa rovnaký algoritmus ako v predchádzajúcom algoritme 4.1.7. Ako významné body použije ľavé dolné súradnice nápisov. Toto je slabina

algoritmu, útočníkovi stačí poposúvať nápisy a extrakcia sama vykoná útok afinnymi transformáciami.

- *Unifikácia (spárovanie) vrcholov* z oboch máp a nájdenie vrcholov, ktoré boli vložené, alebo odobrané pri útoku. Používateľ si zadefinuje parameter t. Algoritmus spraví okolo každého vrcholu s_r v mape M kruh s polomerom t. Ak sa v mape $\tilde{M}$ nachádza v kruhu okolo vrcholu s_r len jeden vrchol s_w, tak je spárovaný s s_r. Ak tam je viac vrcholov, použije sa ten najbližší a ostatné sa vyhodia [7]. Ak sa tam nenachádza žiaden vrchol, tak algoritmus vloží na náhodné miesto v kruhu nový vrchol s_w, a ten spáruje s s_r. Jeho súradnice samozrejme nesedia so súradnicami s_r, sú považované za zašumené.

- *Delaunayova triangulácia* sa skopíruje z referenčnej mapy M.

- *Spektrálna analýza* pre referenčnú mapu M vyprodukuje rovnaké vlastné vektory ako spektrálna analýza pre označenú mapu $\tilde{M}$, takže túto drahú operáciu netreba opakovať.

- *Demodulácia* prebieha rovnako ako predchádzajúcom algoritme 4.1.7, s tým rozdielom, že namiesto vektoru $\vec{s}_i$ sa používa transformovaný vektor $\hat{s}_i$.

Z vety 3.2.4 vyplýva, že spektrálna báza nebude komplexná, takže algoritmus je použiteľný. Ďalej z nej vyplýva, že takáto spektrálna báza nie je optimálna. Keďže T vo všeobecnosti nie je symetrická, spektrálna báza nie je ortonormálna, a jej výpočet je ťažší. To je vážny problém, lebo potom nevieme z hodnoty s_{ij} určiť jej dôležitosť a ani to, ako veľmi sa zápis správy do nej prejaví v predlohe. Na zmiernenie tejto vlastnosti slúži Delaunayova triangulácia. Vďaka nej je menší rozptyl medzi stupňami vrcholov. Cenou za to ale je veľa umelo pridaných závislostí medzi vrcholmi. Teda máme ED-transformáciu Delaunayovej triangulácie a nie ED-transformáciu siete. Autori tento problém riešia tak, že správu zapisujú do všetkých koeficienov vektoru $\vec{\hat{s}}_i$. Ostatné problémy algoritmu a jeho odolnosť proti zmenám v

[7] Autori asi mlčky predpokladajú že v mape M sa v kruhu okolo vrcholu s_r nenachádza žiaden iný vrchol.

matici susednosti sme popísali pri podobnom algoritme 4.1.7. V popise algoritmu je uvedené, že na ukladanie správy sa požíva opakovanie jej bitov. Z toho vyplýva oveľa nižšia odolnosť proti útoku orezávaním ako je v tabuľke 4.1. Domnievame sa, že ide o omyl a pri ukladaní sa používa opakovanie správy, alebo vektor $\vec{b}$ sa pri vkladaní zopakuje toľko krát, koľko krát sa zmestí do predlohy, alebo nesprávne uviedli, že do každého štvorca sa ukladá jeden bit z $\vec{b}$ a ukladá sa tam celé $\vec{b}$

Kedže pred zavedením nášho formálneho modelu sa na porovnanie algoritmov používali iba experimentálne metódy, tak uvedieme výsledky experimentálneho porovnania. Nevýhodou tohto porovnania oproti nášmu modelu je, že z neho nevieme povedať, čo by sa ešte dalo vylepšiť.
Nasleduje popis experimentov:

1. *Posunutie* všetkých vrcholov v mape o 1000 jednotiek v osi x a 500 jednotiek v osi y.

2. *Zväčšenie* celej mapy $5,5$-krát.

3. *Zmenšenie* celej mapy so zaokrúhlením na najbližšie celé číslo

   (a) na 0.3-násobok

   (b) na 0.6-násobok

   vplyvom chyby pri zaokrúhľovaní sa po pose normalizácii tento útok prejaví ako útok šumom.

4. *Otočenie* celej mapy o $\pi/4$

   (a) okolo ľavého horného rohu (bod $(0,0)$)

   (b) okolo stredu (bod $(3750, 2500)$)

5. *Afinná transformácia* vlastne naraz spraví útoky (4b), (1) a (3a).

6. *Lokálna deformácia* Mapa je rozdelená štvorcovou sieťou s veľkosťou 10×10 a vrcholy v každom štvorci sú otočené okolo stredu štvorca o $\pi/180$ ak $(x+y)mod = 0$ vpravo, inak vľavo.

7. *Poprehadzovanie vrcholov* Pri tomto útoku sa zmenia čísla vrcholov.

8. *Vloženie* 3000 vrcholov na čiary.

9. *Zašumenie* súradníc vrcholov pripočítaním šumu s amplitúdou

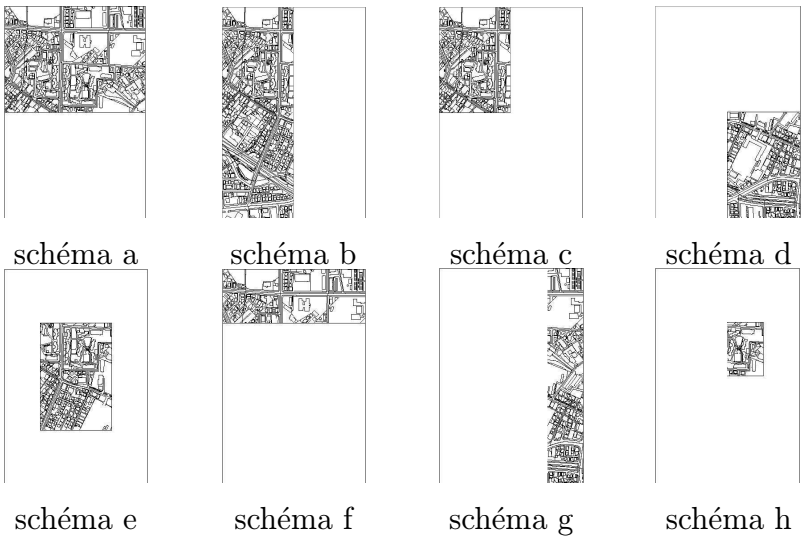
   (a) $\alpha = 10cm$

   (b) $\alpha = 30cm$

   (c) $\alpha = 50cm$

10. *Orezanie* mapy podľa šablón na obrázku 4.3 na 1/2 až 1/16 originálu.

Je zrejmé že útoky (1), (2), (4), (7) a (8) odstráni pose normalizácia. Pose normalizácia zredukuje útok (4) na útok zašumením (9). Útoky (6) a (9) sú v podstate útoky zašumením. Pri tomto type útoku sa ukáže výhodnosť transformačného algoritmu. Z našej teórie vyplýva, že zvolením ED-transformácie vzhľadom na K, alebo U, namiesto ED-transformácie vzhľadom na T ako spektrálnej bázy by sa odolonosť proti tomuto typu útoku ešte zvýšila a znížilo vizuálne poškodenie mapy.



Obr. 4.3: Osem šablón orezávaní použtých pri experimentoch

		Vodotlač v spektrálnej doméne		Vodotlač v priestorovej doméne
Minimálny počet vrhchlov d v štvorci		480	480	10
Modulačná amplitúda α		1,0	1,0	1,0
Opakovacia konštanta c		2	3	NA
(1) Posunutie		$0,0\%$	$0,0\%$	$0,0\%$
(2) Zväčšenie ($5,5$-krát)		$0,0\%$	0.0%	0.0%
(3) Zmenšenie	(3a) $\times 0,6$	$0,0\%$	$0,0\%$	$0,7\%$
	(3b) $\times 0,3$	$0,1\%$	$0,0\%$	nemerané
(4) Otočenie	(4a) Okolo (0,0) o $\pi/4$	$0,0\%$	$0,0\%$	$0,0\%$
	(4b) Okolo (3750,2500) o $\pi/4$	$0,0\%$	$0,0\%$	$0,0\%$
(5) Afinná transformácia ((4b)+(1)+(3a))		$0,1\%$	0.0%	1.0%
(6) Lokálna deformácia		9.2%	8.1%	45.2%
(7) Poprehadzovanie vrcholov		$0,0\%$	0.0%	0.0%
(8) Vloženie vrcholov (3000 vrcholov)		$0,0\%$	0.0%	0.0%
(9) Zašumenie	(9a) $\alpha = 10cm$	$0,0\%$	$0,0\%$	$0,0\%$
	(9b) $\alpha = 30cm$	$0,1\%$	$0,0\%$	nemerané
	(9c) $\alpha = 50cm$	$5,9\%$	$3,4\%$	$8,5\%$
(10) Orezanie	Schéma a	$0,0\%$	$0,0\%$	$1,4\%$
	Schéma b	$0,1\%$	$0,4\%$	$1,8\%$
	Schéma c	$0,7\%$	$1,3\%$	$7,0\%$
	Schéma d	$0,4\%$	$0,0\%$	$6,8\%$
	Schéma e	$0,8\%$	$0,0\%$	$16,7\%$
	Schéma f	$0,4\%$	$0,4\%$	$15,0\%$
	Schéma g	$1,4\%$	$0,4\%$	$11,3\%$
	Schéma h	$18,8\%$	$15,1\%$	$35,9\%$

Tabuľka 4.1: Percento chybne extrahovanej informácie.

Kapitola 5

Návrh robustného steganografického systému

Z definície spektrálnej bázy je zrejmé, že transformačné algoritmy s dobrou spektrálnou bázou sú odolnejšie proti útoku náhodným šumom ako algoritmy pracujúce v priestorovej doméne, lebo v spektrálnej báze sa šum prejaví minimálne.

5.1 Spektrálna báza

Výskum optimality spektrálnej bázy je pomerne čerstvý. Spektrálnu teóriu grafov, ktorá je pomerne dobre preskúmaná nemožno použiť, pretože spektrum grafu je pre naše účely úplne nevhodné. ED-transformácia vzhľadom na autokorelačnú maticu Φ je optimálna, ale je výpočtovo príliš náročná. Treba teda nájsť inú optimálnu bázu. Prvý pokus dokázať optimalitu bázy bol v [1]. Zhang v [14] ukázal, že ED-transformácia vzhľadom na K, a ED-transformácia vzhľadom na U má vlastnosti, ktoré my požadujeme od spektrálnej bázy na odolnosť proti útoku zašumením alebo vyhladením. Aj keď sa Zhang vôbec nevenuje steganografii, nám sa jeho výsledky hodia.

Model definovaný v kapitole 3 nie je dostatočný na opis zmien v matici susednosti. Chceli sme zaviesť model, ktorý by opisoval zmeny v matici susednosti, ale pri jeho hľadaní sme nenašli žiadne výsledky, o ktoré by sme

sa mohli oprieť. Vybudovanie takejto teórie je dlhodobá práca s otvoreným koncom. Na porovnanie existujúcich algoritmov je však naša teória dostačujúca.
Túto teóriu je navyše možné použiť aj na popis spektrálnych báz pre n-rozmerné siete. Teda aj pre vektorové obrázky.

Z vety 3.2.4 vyplýva, že báza, ktorú navrhli Karni s Gotsmanom a bola použitá v kompresnom algoritme [4] a vo vodotlačovom algoritme [11][1], nie je optimálna. Navyše výpočet ED-transformácie vzhľadom na K, alebo U je oveľa rýchlejší a z viet 3.2.3 a 3.2.6 vyplýva, že to sú dve rozličné optimálne bázy. V tejto súvislosti chceme spomenúť aj úpravu vodotlačového algoritmu 4.1.7 pre vodotlač na 3D sieťach[2]. Autori v článku síce tvrdia, že používajú bázu z [4], čo je v našej teórii ED-transformácia vzhľadom na T, ale v algoritme majú ED-transformáciu vzhľadom na K.

Problémom všetkých doposiaľ publikovaných algoritmov aj báz ktoré sme navrhli ako optimálne odolné proti útoku zašumením je, že ich výpočet je závislý od matice susednosti. Čiže ak pri použití slepého algoritmu útočník zmení maticu susednosti, príjemca nebude schopný vypočítať bázu, ktorú potrebuje na extrakciu správy. Návrh bázy ktorá by bola odolná voči malým zmenám v matici susednosti je veľmi ťažký.

5.2 Kódovanie správy

Pre informovanú vodotlač je výhodné použiť pose normalizáciu. Ako sme ukázali na popise algoritmu 4.1.7, pose normalizácia je dobrá odstránenie útokov ktoré menia maticu susednosti. Výskum pose normalizácie patrí do oblasti grafiky. Kódovanie z algoritmu 4.1.7 je pre informovanú vodotlač dostatočné.

Informovaný steganografický systém má malé možnosti využitia. Vzhľadom na to, že nemáme formálny model, ktorý by popisoval zmeny v matici susednosti a ich dôležitosť pri ED-transformácii, nemôžeme skonštruovať robustný algoritmus pre neinformovanú vodotlač. Avšak pre steganografiu má

[1] Je ho popis je v 4.1.7

[2] Ryutarou Ohbuchi, Akio Mukaiyama, Shigeo Takahashi, Watermarking a 3D shape model as a point set. Publikovaný v novembri 2004

význam aj za týchto podmienok navrhnúť slepý algoritmus. Takýto steganografický systém bude použiteľný všade tam, kde sa počas prenosu predpokladá možnosť zašumenia, alebo vyhladenia mapy, ale neočakávajú sa zmeny v matici susednosti.

Pre neiformovaný steganografický systém navrhujeme pre ne nasledovné kódovanie.

Označme $\vec{a} = (a_1, \ldots, a_n)$ správu, ktorú chceme uložiť, $\vec{p}$ pseudonáhodnú postupnosť vygenorovanú pomocou kľúča k, α modulačnú konštantu a c opakovaciu konštantu.

Nech $\vec{b}$ je vektor, ktorý vznikol z $\vec{a}$ tak, ako v algoritme 4.1.7.

Vloženie správy

$$\tilde{\hat{s}}_i = \hat{s}_i - (\hat{s}_i \mod \alpha) + (b_i \oplus p_i)\alpha/2$$

Extrakcia správy

$$b_i = p_i \oplus \begin{cases} 1 & \text{ak } (\tilde{\hat{s}}_i \mod \alpha) \in \langle \frac{\alpha}{4}, \frac{3}{4}\alpha) \\ 0 & \text{ak } (\tilde{\hat{s}}_i \mod \alpha) \in \langle \alpha, \frac{\alpha}{4}) \cup \langle \frac{3}{4}\alpha, 1) \end{cases}$$

Správu $\vec{a}$ dostaneme z $\vec{b}$ tak ako v algoritme 4.1.7. Na dosiahnutie rovnakej robustnosti ako kódovanie použité v algoritme 4.1.7 je potrebné zvoliť dvojnásobnú modulačnú konštantu α. Hodnota konštanty α je výsledkom kompromisu. Zvyšovaním α zvyšujeme robustnosť, ale znižujeme kvalitu predlohy. Upozorňujeme, že ak je útočník schopný vypočítať bázu, tak je schopný vykonať detekčný útok, lebo po vložení správy sú spektrálne koeficienty násobkom $\alpha/2$.

Kapitola 6

Záver

Diplomová práca prináša ojedinelý ucelený pohľad na problematiku steganografických systémov a systémov digitálnej vodotlače pre vektorové mapy.

Existujúce algoritmy sme si zatriedili do tried podľa spôsobu, akým ukladajú správu. Tieto triedy sme posúdili z hľadiska ich použiteľnosti a robustnosti. Ukázali sme, že transformačné systémy sú lepšie ako systémy pracujúce v priestorovej doméne. Ďalej sme ukázali, že niektoré doposiaľ používané experimentálne metódy, aj keď vyzerali byť rôzne, skutočnosti merali to isté.

Z tohto prehľadu by ma byť čitateľ schopný zorientovať sa v rôznych princípoch práce sterganografických systémov pre vektorové mapy.

Hlavný prínos je vo vytvorení formálneho modelu na popis vlastností rôznych spektrálnych báz. Našli sme dve bázy, ktoré vyhovujú nášmu kritériu optimality.

Náš model však nie je odolný proti zmenám v matici susednosti mapy. Tento problém rieši pri existujúcich informovaných algoritmoch pose normalizácia. Tú však nemožno použiť pri neinformovaných algoritmoch.

Vytvorenie formálneho modelu pre bázu odolnú proti zmenám v matici susednosti je však veľmi problematické a nepodarilo sa nám nájsť ani žiadnu prácu, ktorá by pomohla pri vytváraní tohto modelu. Náš model je dostatočný na rozbor vlastností existujúcich algoritmov. Je možné ho použiť aj na popis spektrálnych báz pre n-rozmerné siete, teda aj pre trojrozmernú vektorovú sieť.

Formálny model, ktorý sme vybudovali, sme aplikovali na rozbor transformačného systému. Ukázali sme, že medzi algoritmami, o ktorých vieme, nebol algoritmus, ktorý by používal optimálnu bázu.

Na záver sme navrhli neinformovaný algoritmus vhodný na nasadenie do prostredia, v ktorom sa predpokladá zašumenie alebo vyhladenie mapy, ale nepredpokladajú sa zmeny v matici susednosti.

Literatúra

[1] Mirela Ben-Chen and Craig Gotsman. On the optimality of spectral compression of meshes, 2003.
`http://w3.impa.br/~pcezar/cursos/mpcg/papers/optimal.pdf`.

[2] David A. Harville, editor. *Matrix Algebra from a Statistician's Perspective*. Springer-Verlag, 1997.

[3] William A. Huber. Vector steganography a practical introduction.
`www.directionsmag.com/article.php?article_id=195`.

[4] Zachi Karni and Craig Gotsman. Spectral compression of mesh geometry. In Kurt Akeley, editor, *Siggraph 2000, Computer Graphics Proceedings*, pages 279–286. ACM Press / ACM SIGGRAPH / Addison Wesley Longman, 2000.
`citeseer.ist.psu.edu/karni00spectral.html`.

[5] Tibor Katriňák, Martin Gavalec, Eva Gedeonová, and Jaroslav Smítal. *Algebra a teoretická aritmetika*. Univerzita Komenského Bratislava, 1985, 1995, 1999.

[6] Stefan Katzenbeisser and Fabien A. P. Petitcolas, editors. *Information hiding techniques for steganography and digital watermarking*. Artech House computer security series. 2000.

[7] František Lamoš and Rastislav Potocký. *Pravdepodobnosť a matematická štatistika Štatistické analýzy*. Univerzita Komenského Bratislava, 1998.

[8] Ryutarou Ohbuchi, Hiroo Ueda, and Shuh Endoh. Robust watermarking of vector digital maps, 2002.
`citeseer.ist.psu.edu/ohbuchi02robust.html`.

[9] Richard Ostertág. Digitálna vodotlač i a ii.

[10] Richard Ostertág. Počítačová steganografia. Master's thesis, Fakulta matematiky, fyziky a informatiky UK, 1996/97.

[11] Ryutarou, Ohbuchi, and Hiroo. Watermarking 2d vector maps in the mesh-spectral domain, 2003.
`citeseer.ist.psu.edu/575092.html`.

[12] Henry Sonnet, Tobias Isenberg, Jana Dittmann, and Thomas Strothotte. Illustration watermarks for vector graphics, 2003.
`www.cs.uni-magdeburg.de/~isenberg/papers/Sonnet_2003_IWF.pdf`.

[13] Hao Zhang. Discrete combinatorial laplacian operators for digital geometry processing, 2004.
`http://www.cs.sfu.ca/~haoz/pubs/04_gdc_operators.pdf`.

[14] Hao Zhang and Hendrik C. Blok. Optimal mesh signal transforms. In *GMP '04: Proceedings of the Geometric Modeling and Processing 2004*, page 373. IEEE Computer Society, 2004.
`http://www.cs.sfu.ca/~haoz/pubs/04_gmp_transform.ps`.

[15] Ľubica Janáčková. Digitálna vodotlač. Master's thesis, Fakulta matematiky, fyziky a informatiky UK, 2000.

Prílohy

modra.bmp pôvodný obrázok k príkladu z obrázku 2.1
modra2.bmp obrázok 2.1 s vloženým románom 1984 od Georga Orwella. Na vloženie bol použitý program S-Tools 4.0, šifrovanie IDEA, kľuč je www.newspeak.org