VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA INFORMAČNÍCH TECHNOLOGIÍ
FACULTY OF INFORMATION TECHNOLOGY

ÚSTAV INTELIGENTNÍCH SYSTÉMŮ
DEPARTMENT OF INTELLIGENT SYSTEMS

WATERMARKING JAKO OCHRANA DOKUMENTŮ

WATERMARKING AS DOCUMENT PROTECTION

BAKALÁŘSKÁ PRÁCE
BACHELOR'S THESIS

AUTOR PRÁCE **PATRIK SEGEDY**
AUTHOR

VEDOUCÍ PRÁCE **Doc. Dr. Ing. PETR HANÁČEK**
SUPERVISOR

BRNO 2017

Zadání bakalářské práce/19843/2016/xseged00

Vysoké učení technické v Brně - Fakulta informačních technologií

Ústav inteligentních systémů Akademický rok 2016/2017

Zadání bakalářské práce

Řešitel: **Segedy Patrik**
Obor: Informační technologie
Téma: **Watermarking jako ochrana dokumentů**
Watermarking as Document Protection
Kategorie: Bezpečnost

Pokyny:

1. Prostudujte dostupné materiály o problematice watermarkingu.
2. Analyzuje možnosti praktického využití této techniky při ochraně obrazového záznamu.
3. Navrhněte způsob ochrany obrazového záznamu pomocí watermarkingu.
4. Implementuje základní moduly programového systému, který by takovou ochranu zabezpečoval, v jazyce C/C++.
5. Zhodnoťte navržené řešení.

Literatura:

- Schneier, B.: Applied Cryptography Second Edition: Protocols, Algorithms and Source Codes in C.John Wiley and Sons, Inc. 1996.
- Menezes, A. J., van Oorschot, P. C., Vanstone, S. A.: Handbook of applied cryptography. CRC-press, Boca Raton 1996.
- Dekker, M.: Watermarking Systems: Engineering Enabling Digital Assets Security and Other Applications
- Information Hiding Techniques for Steganography and Digital Watermarking, Artech House
- Dle pokynů vedoucího.

Pro udělení zápočtu za první semestr je požadováno:

- Body 1 až 3 zadání.

Podrobné závazné pokyny pro vypracování bakalářské práce naleznete na adrese http://www.fit.vutbr.cz/info/szz/

Technická zpráva bakalářské práce musí obsahovat formulaci cíle, charakteristiku současného stavu, teoretická a odborná východiska řešených problémů a specifikaci etap (20 až 30% celkového rozsahu technické zprávy).

Student odevzdá v jednom výtisku technickou zprávu a v elektronické podobě zdrojový text technické zprávy, úplnou programovou dokumentaci a zdrojové texty programů. Informace v elektronické podobě budou uloženy na standardním nepřepisovatelném paměťovém médiu (CD-R, DVD-R, apod.), které bude vloženo do písemné zprávy tak, aby nemohlo dojít k jeho ztrátě při běžné manipulaci.

Vedoucí: **Hanáček Petr, doc. Dr. Ing.**, UITS FIT VUT
Datum zadání: 1. listopadu 2016
Datum odevzdání: 17. května 2017

L.S.

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
Fakulta informačních technologií
Ústav inteligentních systémů
612 66 Brno, Božetěchova 2

doc. Dr. Ing. Petr Hanáček
vedoucí ústavu

Abstrakt

Táto práca sa zaoberá ochranou dokumentov pomocou digitálneho watermarkingu. Najprv sú prezentované vlastnosti vodoznakov. Potom nasledujú rôzne možnosti využitia tejto techniky. Ďalšia časť je venovaná rozboru súčasného vývoja v oblasti vodoznačenia, využitiu rôznych princípov vkladania vodoznaku pre rozličné typy multimediálnych dát. Následne je navrhnutý spôsob vkladania vodoznaku do statického obrazu, ktorý je neskôr implementovaný. Nakoniec je implementovaný algoritmus podrobený útokom za účelom poškodenia vodoznaku. Tento vodoznak je potom extrahovaný a je zhodnotená jeho podobnosť s vloženým vodoznakom.

Abstract

This thesis is dealing with document protection using a digital watermarking. First, a watermark characteristics are presented. Then, different usages of the watermarking are discussed. Next part of the thesis is dedicated to current development in watermarking field. It is aimed at various principles of watermark embedding into different multimedia types. Subsequently, a watermarking scheme for still images is proposed and implemented. Finally, the watermarking scheme undergoes attacks, which should damage embedded watermark. Attacked watermark is then extracted and compared to the embedded watermark.

Kľúčové slová

vodoznačenie, vodoznak, QR rozklad, vkladanie vodoznaku, extrakcia vodoznaku, PSNR, NC

Keywords

watermarking, watermark, QR decomposition, watermark embedding, watermark extraction, PSNR, NC

Citácia

SEGEDY, Patrik. *Watermarking jako ochrana dokumentů.* Brno, 2017. Bakalářská práce. Vysoké učení technické v Brně, Fakulta informačních technologií. Vedoucí práce Doc. Dr. Ing. Petr Hanáček

Watermarking jako ochrana dokumentů

Prehlásenie

Prehlasujem, že som túto bakalársku prácu vypracoval samostatne pod vedením pána Doc. Dr. Ing. Petra Hanáčka. Uviedol som všetky literárne pramene a publikácie, z ktorých som čerpal.

.....
Patrik Segedy
16. mája 2017

Poďakovanie

Rád by som sa poďakoval Doc. Dr. Ing. Petrovi Hanáčkovi za odborné vedenie bakalárskej práce a poskytnuté rady, ktoré mi pomohli s vypracovaním tohto zadania. Tiež sa chcem týmto poďakovať mojej rodine za neustálu podporu pri štúdiu.

Obsah

Kapitola 1

Úvod

Prvé papierové vodoznaky sa objavili okolo roku 1282 v Taliansku. Znaky boli vytvorené tak, že do foriem na papier sa pridali tenké drôtené vzory, ktoré zapríčinili to, že papier bol v týchto miestach tenší, a teda viac priesvitný. [7]

Najprv boli papierové vodoznaky využívané ako ochranná známka spoločnosti, ktorá papier vyrobila. Neskôr sa začali využívať ako ochranný prvok proti falšovaniu bankoviek, čo poznáme dodnes. Práve odtiaľ môžeme vidieť analógiu medzi papierovým vodoznakom a digitálnym vodoznakom. Ako papierový vodoznak na bankovkách, tak aj digitálny vodoznak môže slúžiť k ochrane diela proti falšovaniu. Podľa knihy *Information hiding techniques for steganography and digital watermarking* [14] bola prvá publikácia venujúca sa digitálnemu watermarkingu publikovaná Tanakom v roku 1990.

Dnes pri náraste digitálnych technológii je umožnený jednoduchý prístup k digitálnym informáciám. Vďaka takémuto vývoju je dnes bezproblémové digitálne dáta bezstratovo kopírovať a potom ďalej rozširovať. To umožňuje ďalej šíriť aj diela, ktoré sú chránené autorským právom. Aj keď sú CD, DVD a Blu-ray nosiče vybavené ochranou proti kopírovaniu, často je takáto ochrana nedostatočná. Po prelomení ochrany sú multimediálne dáta kopírované a distribuované na Internete a následne nelegálne užívané. Samozrejme, že pôvod filmov a hudby je ľahko zistiteľný, no nájsť autora fotografie alebo obrázku je zložitejšie. Práve to bolo motiváciou k zavedeniu digitálneho watermarkingu.

Vývoj v oblasti watermarkingu sa sústreďuje na hľadanie nových metód, ktoré ponúknu najlepší pomer medzi robustnosťou, nevnímateľnosťou a kapacitou vodoznaku, čo sú tri základné vlastnosti vodoznaku.

Cieľom tejto práce je preskúmať techniky watermarkingu pre ochranu obrazových dát a implementovať moduly programového systému, ktorý bude zabezpečovať ochranu pomocou watermarkingu. Na začiatok v kapitole 2 uvedieme čo je to watermarking, vysvetlíme jeho vlastnosti a ukážeme rôzne účely, ku ktorým môžeme watermarking použiť. V rovnakej kapitole si ukážeme typy útokov, ktorých cieľom je vložený vodoznak poškodiť alebo odstrániť. Súčasnému stavu a aktuálnym výskumom sa budeme venovať v kapitole 3. Kapitola 4 sa zameria na návrh vodoznačiacej metódy pre ochranu statického obrazu. Tento návrh bude následne implementovaný a v kapitole 5 popíšeme implementáciu navrhovaného systému. Implementovaný algoritmus pre vkladanie a extrakciu vodoznaku je potrebné otestovať. Testovanie prebieha spôsobom vykonania útokov na vodoznačený obraz. Jednotlivým útokom, ktoré testujú robustnosť vodoznačiacej metódy a ich vyhodnoteniu bude venovaná kapitola 6.

Kapitola 2

Watermarking

Watermarking je proces skrývania digitálnej informácie do nosného signálu.

Na jednej strane je watermarking úzko spätý so steganografiou, ale na druhej strane je založený na iných základných filozofiách, potrebách a aplikáciách. To má za následok, že použité techniky svojimi vlastnosťami jasne oddeľujú watermarking od steganografie.

Steganografia aj watermarking popisujú techniky, ktoré sa používajú k nepostrehnuteľnému sprostredkovaniu informácie pomocou vloženia tejto informácie do nosných dát. Steganografia je typicky spájaná s ukrytím informácií pri point-to-point komunikácii medzi dvoma stranami. Metódy steganografie nie sú zvyčajne robustné voči modifikáciám dát alebo majú limitovanú robustnosť a ochranu vloženej informácie proti technickým modifikáciám, ktoré môžu nastať pri prenose dát alebo pri ich ukladaní. Ako príklad takejto modifikácie môže byť napríklad konverzia formátu, kompresia alebo konverzia digitálneho signálu na analógový.

Watermarking má dodatočnú odolnosť proti pokusom vymazať skryté dáta. Populárnou aplikáciou watermarkingu je dokázanie vlastníctva digitálnych dát prostredníctvom vloženia vyhlásenia o autorských právach. Je nepochybné, že pre tento účel by vložené informácie mali byť robustné proti manipuláciám, ktoré sa ich pokúšajú odstrániť. Inou aplikáciou môže byť monitorovanie a sledovanie, kde sa užívateľ zaujíma o monitorovanie prenosu dát, napríklad za účelom kontroly platieb. [14]

2.1 Klasifikácia vodoznakov

Vlastnosti, ktoré musí spĺňať vodoznak sa líšia na základe konkrétneho použitia tohto vodoznaku. Preto môžeme vodoznaky klasifikovať na základe ich vlastností. Medzi vlastnosti, ktoré rozlišujeme pri vodoznakoch patria tieto:

- Nevnímateľnosť
- Kapacita vodoznaku
- Viacnásobné vloženie
- Robustnosť
- Blindness
- Detekovateľnosť

- Reverzibilita

Medzi najdôležitejšie z vyššie vymenovaných vlastností môžeme považovať *nevnímateľnosť*, *kapacitu* a *robustnosť* vodoznaku. Kvalitná metóda vodoznačenia musí nájsť kompromis medzi týmito troma vlastnosťami. Každá z týchto vlastností vodoznaku bude bližšie vysvetlená v nasledujúcich podkapitolách.

2.1.1 Nevnímateľnosť

Modifikácie spôsobené vložením vodoznaku by mali byť pod hranicou vnímateľnosti, nezávisle na účele za ktorým bol watermarking použitý. Artefakty zavedené procesom watermarkingu sú nie len otravné a nežiadúce, ale môžu tiež znížiť komerčnú hodnotu takto označených dát. Dôsledkom toho, že požadujeme aby bol vodoznak nevnímateľný, individuálne vzorky (pixely, voxely, atď.) sú modifikované len v malej miere. Pre posúdenie nevnímateľnosti musia byť stanovené určité kritéria, aby sme boli schopní kvantifikovať skreslenie. [14]

2.1.2 Kapacita

Napriek tomu, že vo všeobecnosti kapacita vodoznaku nezávisí na konkrétnom použitom algoritme, ale je častejšie spájaná s charakteristikou signálu skresleného vkladaním vodoznaku a silou útoku, dáva zmysel hovoriť o kapacite danej techniky, ako o veľkosti informácie v bitoch, ktorú je možné viac či menej spoľahlivo do signálu zaviesť. Kapacita je základnou vlastnosťou akéhokoľvek vodoznačiaceho algoritmu, ktorá veľmi často určuje či sa použitím danej techniky niečo v danom kontexte získa alebo nie.

Požiadavky musia byť nastavené vzhľadom na aplikáciu konkrétnej techniky. Možné požiadavky na kapacitu môžu byť v rozsahu od niekoľko stoviek bitov, v aplikáciách zameraných na bezpečnosť, po tisícky bitov v aplikáciách zameraných na titulkovanie alebo označovanie (captioning or labeling), ktorých primárnou potrebou je možnosť vloženia veľkého počtu bitov.

Vo všeobecnosti potreba na kapacitu vždy bojuje proti dvom iným dôležitým požiadavkám, ktorými sú nevnímateľnosť a robustnosť vodoznaku. [3]

2.1.3 Viacnásobné vloženie

V niektorých prípadoch je požadované vložiť viac ako jeden vodoznak. Predpokladajme napríklad, že máme systém na ochranu autorských práv, kde každá chránená časť dát pozostáva z 2 vodoznakov: jedného s identitou autora a druhého indikujúceho meno autorizovaného zákazníka. Algoritmy umožňujúce vkladanie viacerých vodoznakov musia zvládnuť to, aby každý vodoznak bol korektne prečítaný dekodérom. Vloženie niekoľkých vodoznakov nesmie zhoršiť kvalitu hostiteľských dát. [3]

2.1.4 Robustnosť

Robustnosť udáva schopnosť detegovať watermark po aplikovaní bežných operácií pri spracovaní signálov. Medzi bežné operácie nad obrazom patrí priestorové filtrovanie, stratová kompresia, vytlačenie a následné skenovanie a geometrické deformácie (rotácia, premiestnenie, škálovanie a pod.). Vodoznaky vo videu musia byť robustné voči tým istým transformáciám, ale aj napríklad voči nahratiu na videokazetu, zmenu počtu snímkov za sekundu

a iným vplyvom. Audio vodoznaky by mali byť robustné proti takým procesom, ako je časová filtrácia, nahratie na audiokazetu a variácie s rýchlosťou prehrávania, ktorých výsledkom je kolísanie zvuku.

V niektorých prípadoch môže byť robustnosť úplne irelevantná, či dokonca nechcená. V skutočnosti sa veľká časť zameraná na výskum vodoznakov sústreďuje na krehké vodoznaky. Krehký vodoznak je navrhnutý tak, aby nebol robustný. Napríklad vodoznak navrhnutý za účelom autentifikácie by mal byť krehký. Akákoľvek metóda spracovávania signálu aplikovaná na obraz, by mala spôsobiť, že vodoznak bude stratený. [7]

2.1.5 Blindness

Algoritmus vodoznaku sa nazýva *blind*, ak sa nie je potrebné uchýliť k porovnaniu medzi originálnym neoznačeným a označeným aktívom pre obnovenie vodoznaku. Naopak vodoznačiaci algoritmus sa nazýva *non-blind*, ak sú potrebné pôvodné dáta pre extrahovanie informácie obsiahnutej vo vodoznaku. Niekedy sú *blind* techniky označované ako *oblivious* alebo *private*. [3]

2.1.6 Detekovateľnosť

Dôležitým rozdielom medzi metódami ukrývania dát je, či je možné vložený kód čítať alebo je ho možné iba detegovať. V prvom prípade (*readable watermarking*) je možné bity obsiahnuté vo vodoznaku prečítať bez ich znalosti vopred. Naopak v druhom prípade (*detectable watermarking*) je možné len verifikovať, či sa daný kód nachádza v dokumente. Inými slovami, je možné povedať, že ak je vodoznak detekovateľný, prítomnosť vodoznaku môže byť odhalená iba vtedy, ak je vopred známy obsah vodoznaku. [3]

2.1.7 Reverzibilita

Ak bol raz vodoznak dekódovaný/detegovaný je možné ho odstrániť zo zdrojového nosiča a tým pádom je možné obnoviť originálny nosič. O takomto vodoznaku hovoríme, že je *strict-sense reversible* (SSR). Vodoznak je *wide-sense reversible* (WSR), ak je možné ho urobiť nedekódovateľný/nedetekovateľný bez viditeľných zmien zdrojového nosiča, potom čo už raz bol dekódovaný/detegovaný. [3]

2.2 Použitie vodoznakov

Watermarking je možné použiť pre rôzne účely. Vo všeobecnosti sa dá povedať, že ak je pre nás užitočné pripojiť k dokumentu nejaké ďalšie informácie, tak tieto metadáta môžeme vložiť do dokumentu vo forme vodoznaku. Existuje mnoho rôznych spôsobov ako priložiť metadáta k dokumentu. Napríklad vloženie dát do hlavičky digitálneho súboru alebo zakódovanie do obrázku vo forme čiarového kódu.

Podľa [7] je watermarking od ostatných techník rozdielny v troch dôležitých bodoch a vďaka týmto trom vlastnostiam sa stáva nenahraditeľným pre niektoré potreby.

1. Watermarking je neviditeľný. Vodoznaky narozdiel od čiarových kódov nenarúšajú estetiku obrazu.

2. Vodoznaky sú neoddeliteľné od dokumentu do ktorého sú vložené. Nie sú odstránené ako hlavička súboru, keď je dokument zobrazovaný alebo pri konverzii na iný typ formátu súboru.

3. Vodoznaky sú vystavované rovnakým transformáciám ako dokumenty do ktorých sú vkladané. To znamená, že niekedy je možné zistiť niečo o týchto transformáciách pozretím sa na výsledný vodoznak.

Ako je uvedené v [7], skúmame osem možností použitia vodoznakov: monitoring vysielania, identifikácia vlastníka, dôkaz o vlastníctve, sledovanie transakcií, autentifikácia obsahu, ochrana proti kopírovaniu, ovládanie zariadení a spätne kompatibilné vylepšenie systému.

2.2.1 Monitoring vysielania

V roku 1997 prepukol v Japonsku škandál kvôli televíznym reklamám. Najmenej dve televízne stanice pravidelne plánovali viacero reklám v rovnaký vysielací čas. Inzerenti platili za tisíce reklám, ktoré neboli nikdy odvysielané [7]. Takéto praktiky boli vo veľkej miere nedetekovateľné po dobu viac ako 20 rokov, hlavne kvôli tomu, že neexistovali žiadne systémy pre monitoring aktuálne vysielaných reklám.

Tradičnou, jednoduchou metódou pre sledovanie vysielania je využitie ľudských pozorovateľov, ktorí budú sledovať vysielanie a zaznamenávať čo videli a počuli. Táto metóda je drahá a náchylná k chybám. Preto je veľmi vhodné nahradiť to automatizovaným monitorovaním. Techniky pre dosiahnutie tohto cieľa môžeme rozdeliť do dvoch skupín. Pasívny monitoring sa snaží o simulovanie ľudských pozorovateľov (spoľahlivejšie a lacnejšie), teda sa snaží o rozoznanie vysielaného obsahu. Aktívny monitoring sa spolieha na informácie ktoré sú pridružené k vysielanému obsahu.

Pasívny systém pozostáva z počítača, ktorý monitoruje vysielanie a porovnáva získaný signál s databázou známych diel. Keď sa porovnaním nájde zhoda, pieseň, film, TV program alebo vysielaná reklama môže byť identifikovaná. Takýto systém sa využíva napríklad na odhadnutie, koľko míňa konkurenčná spoločnosť na reklamu. Tento systém sa nevyužíva na účel verifikácie (napríklad, či reklama bola odvysielaná). Jedným z dôvodov môže byť, že systém rozpoznávania nie je dostatočne presný.

Pre zaistenie dostatočnej presnosti pre verifikačné účely je pravdepodobne potrebné využiť aktívny monitorovací systém, kde strojovo rozpoznateľná identifikačná informácia je prenášaná spoločne s obsahom. Aktívny monitoring je technicky jednoduchší na implementáciu ako pasívny monitoring. Identifikačná informácia je postačujúca na spoľahlivé dekódovanie a nie je potrebná databáza pre interpretovanie tejto informácie. [7]

2.2.2 Identifikácia vlastníka

Textové upozornenia o autorských právach, ako technológia pre identifikáciu vlastníka diela, majú niekoľko obmedzení. Je ich jednoduché odstrániť z kopírovaného dokumentu, dokonca aj bez priameho zámeru. Napríklad, pri kopírovaní strán knihy sa zabudne na fotokópiu upozornenia o autorských právach na titulnej strane. Následkom čoho, človek ktorý chce ďalej využiť toto dielo nevie, či dielo je chránené autorským právom. Dokonca aj keď je predpokladané, že dielo je chránené, môže byť zložité vyhľadať identitu tvorcu alebo osoby, od ktorej musí byť žiadané povolenie.

Pretože vodoznaky môžu byť zároveň neviditeľné a neoddeliteľné od diela v ktorom sú vložené, mali by byť vhodnejšie ako text pre identifikáciu autora. Ak užívatelia diela budú mať k dispozícii detektory vodoznakov, budú schopní zistiť vlastníka označeného diela. Možné by to bolo dokonca aj v prípade, že dielo bolo modifikované spôsobom, ktorý by odstránil textové upozornenie o autorských právach.

Presne na tento účel bol navrhnutý vodoznak pre obrázky od firmy *Digimarc*. Podarilo sa im dosiahnuť veľké rozšírenie ich detektoru vodoznakov zabudovaním detektoru do programu *Photoshop* od spoločnosti *Adobe*. Keď tento detektor rozozná vodoznak, kontaktuje centrálnu databázu a použije správu vo vodoznaku ako kľúč pre nájdenie informácii o vlastníkovi. [7]

2.2.3 Dôkaz o vlastníctve

Je lákavé použiť vodoznak nie len na identifikáciu vlastníka, ale aj na dokázanie vlastníctva. To je niečo, čo textové upozornenie nedokáže zabezpečiť, pretože je ho jednoduché sfalšovať.

Autor vloží do svojho diela vodoznak, ktorý má zabezpečiť ochranu autorských práv. Niekto ďalší však dielo ukradne a pretože ho chce vydávať za svoje, vloží doň svoj vodoznak. Následne pri extrakcii vodoznaku vieme zistiť, že dielo autora obsahuje jeho vodoznak a neobsahuje žiadne časti iného vodoznaku. V prípade druhého diela, sme schopní extrahovať vodoznak vložený zlodejom, avšak tiež vieme extrahovať aspoň časť pôvodného vodoznaku. Týmto spôsobom vieme dokázať kto je autorom diela.

Problémom je, že ak je dostupný detektor, a teda je možné vodoznak zobraziť, potom je ho možné aj odstrániť a nahradiť vlastným. Preto bude pre tento účel nevyhnutné zabrániť dostupnosti detektoru. [7]

2.2.4 Sledovanie transakcií

V tomto prípade watermarkingu, vodoznak zaznamenáva jednu alebo viac transakcií, ktoré sa uskutočnili v histórii kópie diela. Povedzme, že vo vodoznaku môže byť zaznamenaný príjemca predaja alebo distribúcie diela. Majiteľ alebo autor diela môže umiestniť rôzne vodoznaky pre každú kópiu. Ak dielo bolo následne zneužité (únik do médií alebo ilegálna redistribúcia), majiteľ je schopný zistiť, kto je za to zodpovedný.

V literatúre na tému sledovania transakcií sa osoba, ktorá je zodpovedná za zneužitie diela niekedy označuje ako **zradca** (*traitor*) a osoba, ktorá získa dielo od zradcu ako **pirát** (*pirate*).

Sledovanie transakcií je často označované ako *fingerprinting*, pretože každá kópia diela je jedinečne identifikovateľná vodoznakom, čo je analógia k ľudským odtlačkom prstov, ktoré jedinečne identifikujú osobu.

Existuje niekoľko technológií pre tento účel, ktoré nespadajú medzi našu definíciu vodoznakov. Jednou častou alternatívou ku vodoznaku je použitie viditeľných značiek. Citlivé obchodné dokumenty ako napríklad obchodný plán, sú často na pozadí potlačené veľkými sivými číslami, kde pre každú kópiu je toto číslo iné. Následne sú uchované záznamy o tom, kto má ktorú kópiu. Tieto značky sú často označované ako vodoznaky kvôli fyzickej podobe s papierovými vodoznakmi. Napriek tomu to nie sú vodoznaky v našom chápaní tohto termínu, pretože neviditeľnosť uvažujeme ako základnú definujúcu charakteristiku.

Vodoznak pre sledovanie transakcií bol implementovaný dnes už zaniknutou spoločnosťou *DiVX Corporation*. *DiVX* predával vylepšený DVD prehrávač, ktorý implementoval biznis model založený na platbe za prehratie. Vytvorili množstvo bezpečnostných metód aby zabránili pirátstvu ich diskov. Jednou z týchto metód bolo využitie vodoznaku navrhnutého pre sledovanie transakcií. Každý prehrávač podporujúci *DiVX* umiestnil unikátny vodoznak do každého prehraného videa. Ak niekto toto video potom nahral a začal predávať jeho kópie na čiernom trhu, *DiVX* korporácia dekódovaním vodoznaku dokázala identifikovať škodcu (alebo aspoň jeho *DiVX* prehrávač). [7]

2.2.5 Autentifikácia obsahu

Dnes sa falšovanie diela stáva čoraz jednoduchším v spôsobe, ktorý je ťažké detegovať. Napríklad modifikovať obrázok tak, že sa odstráni z neho osoba. Ak by takýto obrázok bol kritickou časťou evidencie alebo policajného vyšetrovania, tak by takýto spôsob falšovania mohol spôsobiť seriózny problém.

Problém autentifikačných správ bol podrobne študovaný v kryptografii. Častým kryptografickým prístupom k riešeniu tohto problému je vytvorenie digitálneho podpisu. Využíva sa algoritmus šifrovania s využitím asymetrického kľúča, teda kľúč potrebný na zašifrovanie a dešifrovanie správy je rôzny. Vďaka tomu, človek, ktorý sa snaží zmeniť správu, nie je schopný vytvoriť nový podpis. Ak niekto následne porovná modifikovanú správu proti originálnemu podpisu, zistí, že podpisy sa nezhodujú a správa bola modifikovaná.

Tieto podpisy sú metadáta, ktoré musia byť prenášané spoločne s dielom. Preto je ľahké normálnym používaním stratiť tieto podpisy. Uvažujme systém pre autentifikáciu obrazu, ktorý uchováva metadáta v hlavičke JPEG súboru. Ak bude tento obraz konvertovaný na iný formát súboru, ktorý nemá dostatok miesta v hlavičke pre podpis, tak tento podpis bude stratený.

Vhodnejším riešením sa javí byť vloženie podpisu priamo do diela použitím watermarkingu. Tento vložený podpis budeme označovať ako autentifikačnú značku. Autentifikačná značka musí byť navrhnutá tak, aby sa stala nevalidnou po čo i len najmenšej modifikácii diela. Takéto značky sú krehkými vodoznakmi.

Keď dielo obsahujúce autentifikačnú značku bude modifikované, značka bude modifikovaná spolu s ním. To nám otvára možnosť skúmania spôsobu, akým bolo dielo sfalšované. Ak je napríklad obraz rozdelený do niekoľkých blokov a každý blok má vlastnú autentifikačnú značku, tak budeme schopní zistiť, ktoré časti obrazu sú autentické a ktoré boli zmenené. [7]

2.2.6 Ochrana proti kopírovaniu

Väčšina použití watermarkingu, ktoré sú spomenuté vyššie nadobúdajú zmysel, ak niekto urobil niečo zlé. Napríklad monitoring vysielania pomáha dolapiť nečestných vysielateľov potom, čo neodvysielali reklamy, za ktoré dostali zaplatené. Sledovanie transakcií identifikuje osoby potom, ako rozširovali nelegálne kópie. Tieto technológie slúžia ako odstrašujúci prostriedok proti takémuto konaniu. Samozrejme je lepšie predvídať a predchádzať takýmto nelegálnym skutkom. Pri využití ochrany proti kopírovaniu sa zameriavame na prevenciu pred tým, aby ľudia vytvárali nelegálne kópie obsahu, ktorý je chránený autorskými právami.

Prvou a najsilnejšou ochranou proti ilegálnemu kopírovaniu je šifrovanie. Šifrovaním diela prostredníctvom unikátneho kľúča dokážeme zabezpečiť, že dielo je nepoužiteľné pre toho, kto nevlastní tento kľúč. Kľúč je poskytnutý oprávneným používateľom takým spôsobom, aby ho nebolo jednoduché kopírovať alebo redistribuovať. Ako príklad môže slúžiť satelitné televízne vysielanie, ktoré je šifrované. Dešifrovacie kľúče sú k dispozícii každému platiacemu zákazníkovi spôsobom *smart card*, táto karta musí byť vložená do zákazníkovho televízneho set-top boxu. Bez tejto karty nie je možné sledovať vysielanie.

Existujú tri základné spôsoby ako môže útočník prekonať šifrovanie. Prvým a najzložitejším spôsobom je dešifrovanie dát bez získania kľúča. Tento prístup väčšinou zahrňuje istú formu hľadania, kde sa útočník vyčerpávajúco snaží dešifrovať signál pomocou miliónov kľúčov. Ak je šifrovací systém dobre navrhnutý, tak útočník musí vyskúšať každý jeden možný kľúč. Toto je nepraktické ak je kľúč dlhší ako 50 bitov.

Jednoduchším prístupom pre útočníka je získať validný kľúč. Pre získanie kľúča je možné využiť reverzné inžinierstvo nad hardvérom alebo softvérom, ktorý obsahuje tento kľúč. V knihe [7] je príklad pre tento spôsob demonštrovaný na DeCSS programe, ktorý bol napísaný Jonom Johansenom a dvomi nemeckými spolupracovníkmi. CSS (Content Scrambling System) je šifrovací systém používaný pre ochranu DVD videa pred nelegálnym kopírovaním. Johanson a jeho spolupracovníci boli schopní využiť reverzné inžinierstvo nad DVD prehrávačom a jeho dešifrovacími kľúčmi. To im umožnilo vytvoriť DeCSS, ktorý dešifruje akékoľvek video zašifrované pomocou CSS.

Najjednoduchším spôsobom ako obísť šifrovanie je legálne získanie kľúča a rozširovanie obsahu potom, čo bol týmto kľúčom dešifrovaný. Útočník, ktorý si praje nahrať a redistribuovať satelitné vysielanie, sa najprv prihlási ako zákazník, získa prístupovú kartu smart card a pripojí výstup set-top boxu na vstup jeho nahrávacieho zariadenia. Toto ukazuje hlavnú slabosť ochrany šifrovaním. Predtým ako môže byť obsah použitý, musí byť dešifrovaný, akonáhle je dešifrovaný, ochrana je stratená.

Watermark je vložený do obsahu, teda je jeho súčasťou a je prítomný v každej reprezentácii obsahu. Preto by mal poskytnúť lepšiu ochranu a jeho využitie by malo byť vhodnejšou metódou implementácie ochrany proti kopírovaniu. Ak by každé nahrávacie zariadenie obsahovalo detektor vodoznakov, potom by mohlo toto zariadenie zabrániť nahrávaniu ak by bol detegovaný vodoznak, ktorý by mal toto dielo chrániť pred kopírovaním.

Napriek tomu je tu jeden podstatný netechnický problém pri zavádzaní systému ochrany proti kopírovaniu založenom na watermarkingu. Neexistuje žiaden prirodzený motív ako zabezpečiť, aby každý výrobca vynaložil zvýšené výdavky kvôli začleneniu detektorov vodoznakov do ich produktov. V skutočnosti to môže byť odradzujúce, pretože detektor vodoznakov môže znižovať hodnotu rekordéru z pohľadu zákazníka, pretože zákazník by radšej vlastnil zariadenie, ktoré je schopné vyrábať nelegálne kópie.

Pre tento účel bol vymyslený VEIL vodoznak (Video Encoded Invisible Light), ktorý je jednoduchou metódou modulujúcou intenzitu jedného riadku videa (*scanline*). Tento vodoznak pre video má za úlohu šifrovať Rights Assertion Mark (RAM), čo sa používa ako podpora pre CGMS-A signalizáciu. CGMS-A (Copy Generation Management System Analog) pozostáva z dvoch bitov informácii reprezentujúcich štyri stavy:

- Copy freely
- Copy no more
- Copy once
- Copy never

CGMS-A je video štandard, ktorý prenáša dva bity v čase medzi koncom posledného riadku obrazu a začiatkom prvého riadku nasledujúceho obrazu, ktorý sa nazýva *vertical blanking interval*. Takéto dáta je možné jednoducho stratiť alebo odstrániť. Značka RAM je vložená do obsahu videa, ktoré obsahuje CGMS-A signalizáciu. Ak je CGMS-A signál stratený, ale značka RAM je prítomná, nahrávacie zariadenie je navrhnuté tak, aby neumožnilo kopírovanie video signálu. [7]

2.2.7 Ovládanie zariadení

Ochrana proti kopírovaniu spadá do širšej kategórie možných použití, ktoré môžeme označovať ako ovládanie zariadení. Existuje niekoľko iných aplikácií, kde zariadenie reaguje na

vodoznak, ktorý deteguje v obsahu. Z pohľadu užívateľa sú tieto aplikácie často odlišné od ochrany proti kopírovaniu, pretože detegovaný vodoznak prináša nejakú pridanú hodnotu a neslúži k zamedzeniu používania.

V knihe [7] sa dozvedáme, že v roku 1953 Tomberlin et al. popísali systém, ktorý mal za úlohu redukovať cenu distribúcie reprodukovanej hudby do kancelárií, obchodov a iných priestorov. Táto hudba bola tradične distribuovaná prostredníctvom pevnej linky, čo bolo finančne náročné. MusicScan, držiteľ patentu, sa rozhodol pre zníženie tejto ceny tým, že nahradí vyhradenú rozvodnú sieť systémom bezdrôtového rozhlasu. Predsa len využitie vlastného rádiového vysielania by bolo taktiež príliš drahé. Preto priestory boli ozvučené hudbou z komerčnej rádio stanice, ktorá okrem hudby vysiela reklamy, rozhovory a iné relácie. Tomberlin et al. práve kvôli tomuto vymysleli, že do rádiového vysielania vložia vodoznak, ktorý bude indikovať, kedy rádio vysiela hudbu a kedy má byť vysielanie ignorované. Dosiahnuté to bolo dvomi kontrolnými signálmi (vložené ako ultrazvukové alebo infrazvukové audio frekvencie), ktoré určovali začiatok a koniec segmentu, ktorého vysielanie malo byť blokované.

Ďalšia raná aplikácia watermarkingu pre ovládanie zariadenia je popísaná patentom z roku 1981, ktorého vynálezcom je Ray Dolby. V tom čase množstvo FM rádio staníc vysielalo hudbu s použitím techniky na redukciu hluku zvanou Dolby FM. Pre plné využitie Dolby FM je vyžadované, aby rádio prijímač obsahoval korešpondujúci dekodér. Poslucháči sa preto museli spoľahnúť na zoznam staníc, aby mohli rozhodnúť, ktorá stanica vysiela Dolby FM signál a pre tieto stanice museli manuálne zapnúť dekodér. Dolby navrhol, aby rádiá boli schopné automaticky zapnúť dekodér na základe nepočuteľného tónu vysielaného v rámci frekvenčného audio spektra. Takýto tón vytvára jednoduchý vodoznak.

V rovnakej knihe je uvedené, že v roku 1989 Broughton a Laumeister získali patent za techniku, ktorá umožňovala vzájomné pôsobenie akčných figúrok a televízneho vysielania. V tejto technike sa využíval jednoduchý vodoznak, ktorý moduloval intenzity horizontálnych riadkov (scanlines) v každom obraze videa. Tento modulačný signál je detegovaný svetlo citlivým zariadením, ktoré je umiestnené blízko televízneho prijímača. Týmto spôsobom je možné synchronizovať akčné figúrky s videom, ktoré je pozerané v televízii. Broughton a Laumeister taktiež spomenuli, že modulácia intenzít scanlines vyvoláva detekovateľný rádio frekvenčný (RF) signál a to môže byť využité ako základ pre alternatívny detektor.

Novším spôsobom využitia watermarkingu pre ovládanie zariadení je systém od spoločnosti Digimarc, ktorý vloží jedinečný identifikátor do tlačených a distribuovaných obrázkov, ako sú napríklad reklamy v časopisoch, vstupenky a podobne. Po tom čo je obrázok zachytený pomocou fotoaparátu mobilného telefónu, vodoznak je prečítaný softvérom na telefóne a identifikátor je určený k presmerovaniu na webovú stránku. [7]

2.2.8 Spätne kompatibilné vylepšenie systému

Niekedy nastáva situácia, že máme veľmi rozsiahly, nasadený systém, ale rozhodneme sa ho vylepšiť za účelom zlepšenia funkcionality. Toto vylepšenie však môže byť nekompatibilné so súčasným systémom. Ako príklad môžeme použiť prechod z analógového vysielania televízie na digitálny, čo je finančne aj časovo náročný proces. Počas prechodu musí byť použité úplne nové zariadenie pre digitálne vysielanie a zákazníci si musia kúpiť digitálne televízne prijímače. Starší analógový systém však medzitým musí stále fungovať, kým väčšina zákazníkov neprejde na digitálnu technológiu.

Ideálne by sme chceli vylepšiť systém takým spôsobom, aby bol spätne kompatibilný. Digitálny watermarking je jedným zo spôsobov ako je to možné dosiahnuť. V skratke si

ukážeme príklady, ktoré to ilustrujú. Systém pre medzinárodné riadenie letovej prevádzky používa analógový komunikačný systém na komunikáciu medzi lietadlom a pozemnými miestami riadenia letovej prevádzky. Podľa protokolu je vyžadované, aby všetci piloti začali komunikáciu povedaním volacej značky. Vznikol však záujem vylepšiť tento systém tak, aby obsahoval strojovo čitateľný identifikátor pre autentifikáciu prenosu. Samozrejme by bolo extrémne drahé nahradiť analógové komunikačné systémy vo všetkých lietadlách, od najväčšieho až po najmenšie jednomiestne lietadlá.

Eurocontrol, Európska organizácia pre bezpečnosť letovej prevádzky zvažovala, či je možné automaticky vložiť digitálny vodoznak do komunikácie s pilotom. Watermarkingom všetkej komunikácie je možné zabezpečiť digitálny identifikátor podobne ako číslo na chvoste, ktoré jednoznačne určuje lietadlo. Tento systém je kompatibilný so súčasným komunikačným vybavením v lietadlách aj v centrách riadenia letovej prevádzky.

Ďalším príkladom môže byť využitie digitálneho vodoznaku pre synchronizáciu audio a video signálu od firmy Tektronix. Problém nastáva ak sú video a audio kanály televízneho vysielania spracovávané samostatne. Spracovanie digitálneho signálu pre audio a video kanály môže mať rôznu odozvu, čo môže viesť ku známemu problému, keď pohyb pier nesedí s rečou. Riešením je vložiť vysoko komprimovaný audio signál do video signálu. Po spracovaní všetkých signálov je audio signál porovnaný s vloženým audio signálom pre zistenie, či bolo zavedené nejaké časové oneskorenie. [7]

2.3 Ukazovatele kvality

Pri posudzovaní kvality vodoznačiacej metódy môžeme pristupovať buď objektívne alebo subjektívne. Subjektívny prístup je taký, pri ktorom pohľadom určíme, či bol obraz po vložení vodoznaku poškodený a či sme schopní v extrahovanom vodoznaku rozpoznať vodoznak, ktorý bol do obrazu vkladaný. Pre získanie objektívneho pohľadu na kvalitu algoritmu pre watermarking si musíme stanoviť určité ukazovatele.

K vyhodnoteniu podobnosti medzi originálnym vodoznakom ω a extrahovaným vodoznakom ω' sa využíva normalizovaná korelácia (NC) [17]

$$NC = \frac{\sum_i \omega_i \omega'_i}{\sum_i \omega_i^2}, \quad \omega, \omega' \in \{-1, 1\}. \tag{2.1}$$

Kvalitu vodoznačeného obrazu zistíme na základe pomeru medzi špičkovou hodnotou signálu a hodnotou šumu (PSNR), ktorý je definovaný ako

$$PSNR = 20 \log_{10} \frac{255}{\sqrt{MSE}}, \tag{2.2}$$

kde MSE značí strednú kvadratickú chybu (mean square error), ktorá je daná nasledujúcim vzorcom

$$MSE = \frac{1}{N \times N} \sum_i \sum_j [I_O(i,j) - I_W(i,j)]^2, \tag{2.3}$$

kde $N \times N$ je veľkosť obrázku, I_O je originálny obrázok a I_W je vodoznačený obrázok. [17]

Tieto ukazovatele budú v tejto práci neskôr použité pre zhodnotenie kvality implementovanej metódy vkladania a extrakcie vodoznaku.

2.4 Útoky

Útoky na vodoznačené dielo môžu byť prevádzané za rôznymi účelmi. Zatiaľ čo niektoré útoky sú použité pre poškodenie vodoznaku, aby ho nebolo možné detegovať, iné majú za úlohu z chráneného diela vodoznak úplne odstrániť.

Útoky na obraz môžeme rozdeliť do dvoch kategórií:

- Spracovanie obrazu (image processing)
- Geometrické skreslenie (geometric distortion)

Do prvej kategórie zaraďujeme útoky ako kompresia, zaostrenie, šum a zmena špecifických pixelov. Druhú kategóriu tvoria útoky ako rotácia, zmena veľkosti a vystrihnutie. K týmto bežným útokom môžeme pridať aj print-scan útok, ktorý je novou výzvou, pretože nie len že mení hodnoty pixelov (spracovanie obrazu), ale mení aj ich pozíciu (geometrické skreslenie). Väčšina watermarking systémov zlyháva pri takomto hybridnom útoku. [4]

Na základe aplikácie a požiadaviek watermarkingu môžeme uvažovať napríklad nasledujúci zoznam skreslení a útokov: [14]

- Zlepšenie signálu (ostrenie, zlepšenie kontrastu, korekcia farby, gamma korekcia)
- Aditívny a multiplikatívny šum (Gaussovský, uniformný, mosquito)
- Lineárna filtrácia (dolnopriepustná, hornopriepustná, pásmová)
- Nelineárna filtrácia (mediánový filter, morfologický filter)
- Stratová kompresia (obraz: JPEG, video: H.261, H.263, MPEG-2, MPEG-4, audio: MPEG-2, MP3, MPEG-4, G.723)
- Lokálne a globálne afinné transformácie (posun, rotácia, zmena veľkosti, skosenie)
- Redukcia dát (orezanie, vystrihnutie, modifikácia histogramu)
- Prekódovanie (H.263 -> MPEG-2, GIF -> JPEG)
- D/A a A/D prevod (print-scan, analógové TV vysielanie)
- Viacnásobné vodoznačenie
- Štatistické priemerovanie
- Mozaikový útok

Niektoré útoky z tohto zoznamu použijeme na testovanie robustnosti vodoznačiacej metódy v kapitole 6. Konkrétne budeme používať útoky, ktoré majú za účel zlepšenie obrazu, budeme tiež vkladať šum, využijeme nelineárnu filtráciu, afinné transformácie, ale aj modifikáciu histogramu alebo kompresiu.

2.5 Statický obraz vs. audio vs. video

Pre čo najväčšiu všeobecnosť je potrebné diskutovať ako skryť informáciu v rôznych typoch médií. Preto sa budeme venovať ako obrazu, tak aj audiu. Nebudeme sa venovať ukrývaniu informácii v texte alebo grafických súboroch, pretože tam vznikajú iné problémy. Taktiež sa nebudeme venovať ukrývaniu dát v 3D objektoch.

Hoci vloženie vodoznaku do obrazu je rozdielne od vloženia rovnakej informácie do video sekvencie alebo do audio signálu, väčšina konceptov zostáva rovnaká. Medzi problémy, ktoré sú nezávislé na médiu patrí napríklad:

- Zakódovanie informácie, ktorá má byť ukrytá
- Definícia pravidla pre vkladanie vodoznaku
- Spôsob detekcie/dekódovania

Z tohto dôvodu nerozprávame o watermarkingu každého média samostatne, ale práve naopak sa snažíme byť čo najviac všeobecní. Samozrejme musíme rozlišovať medzi obrazom, video sekvenciami alebo audiom, ak sa chceme zamerať na ich konkrétne špecifiká. Sem môžu patriť rôzne stratégie pri vkladaní vodoznaku, popis možných útokov alebo popis konkrétnych praktických algoritmov.

Vo všeobecnosti môžeme povedať, že väčšina výskumu sa zameriava práve na vkladanie digitálnych dát pomocou watermarkingu obrazu. Následne je mnoho týchto algoritmov podobných tým, ktoré sú použité pri watermarkingu videa alebo audia. [3]

Kapitola 3

Súčasný stav

Pri skúmaní súčasného stavu je potrebné sústrediť sa na rôzne spôsoby použitia watermarkingu v rozličných typoch médií. Sledujeme viacero prístupov ku vkladaniu vodoznaku, ktoré vedú k rôznym účelom využitia watermarkingu v danom médiu. V roku 2004 bolo v [3] uvedené, že vo všeobecnosti je možné povedať, že väčšina výskumu týkajúceho sa skrývania digitálnych dát je zameraná na watermarking obrazu. S týmto tvrdením môžeme súhlasiť aj dnes. Pri hľadaní vedeckých článkov na tému watermarking stále narazíme na väčšinu diel venujúcich sa hľadaniu nových prístupov pre watermarking obrazu.

3.1 Watermarking obrazu

Watermarking obrazu je stále populárnou témou vedeckého výskumu. Skúmajú sa možnosti vkladania vodoznakov do obrazov v odtieňoch šedej, ale aj do farebných obrazov. Hľadajú sa nové metódy vkladania vodoznakov. Vytvárajú sa nové algoritmy, ktoré môžu byť reverzibilné, či využívajúce genetické algoritmy.

3.1.1 Obrazy v odtieňoch šedej

Naderahmadian a Hosseini-Khayat [17] prezentujú rýchlu, robustnú a blind watermarking techniku, ktorá je založená na QR dekompozícii. Táto metóda je prezentovaná v priestorovej aj frekvenčnej doméne. V článku ukazujú, že QR dekompozícia poskytuje porovnateľnú alebo lepšiu kapacitu a robustnosť ako watermarking založený na DCT (diskrétna kosínusová transformácia) a SVD (singulárna dekompozícia) transformáciách.

Thabit a Khoo sa v [19] zamerali na metódu bezstratového robustného watermarkingu. Dosiahnutie bezstratovosti bolo dosahované za cenu zníženia kapacity a kvality vodoznačeného obrazu. Autori prezentujú využitie Slantlet transformácie (SLT). V porovnaní s predchádzajúcimi metódami sľubujú vyššiu kapacitu, vyššiu robustnosť a zlepšenú vizuálnu kvalitu.

Pre watermarking je možné použiť aj geometrické modelovanie, čo je ukázané v [12]. Hamghalam, Mirzukuchaki a Ali Akhaee pomocou štyroch vzoriek vlnkovej aproximačnej transformácie pre každý blok obrazu spolu so strednou hodnotou ostatných koeficientov na tomto bloku boli schopní tieto koeficienty namodelovať ako tri body v 2D priestore. Vrcholový uhol je použitý ako premenná pre watermarking. Za účelom vloženia vodoznaku je vrcholový uhol zmenený premiestnením bodov. Táto metóda je robustná proti útokom šumom a kompresiou.

Jednou z horúcich tém pri watermarkingu obrazu je využitie momentov obrazu, čo ponúka vysokú robustnosť. Tejto téme sa venovali Tsougenis, Papakostas, a Koulouriotis [20], ktorí využívajú oddeliteľné momenty (SMs – separable moments). Tieto momenty reprezentujú obraz ako kombináciu rôznych ortogonálnych polynómov, ktoré generujú sériu nových rodín momentov. V práci porovnávajú výkonnosť navrhovaných rodín momentov oproti originálnym momentom a klasickým metódam. Článok odôvodňuje, že diskrétne ortogonálne SMs vytvárajú novú atraktívnu transformáciu pre použitie watermarkingu založenom na momentoch obrazu.

Konvenčné techniky digitálneho watermarkingu obrazu trpia na zraniteľnosť voči deformáciam ako je rotácia, zmena veľkosti a posun (RST – Rotation, Scaling, Translation). Tieto deformácie desynchronizujú informáciu vloženú vodoznakom, a teda zabraňujú detekcii vodoznaku. Na vyriešenie tohto problému Abbasi, Woo, Ibrahim, Islam a Coles [1] prichádzajú s technikou watermarkingu založenou na frakčnom kalkule (fractional calculus). Frakčný kalkul a jeho aplikácie sú významné v rozmanitých oblastiach matematiky, fyziky, počítačových vied a inžinierstva. Frakčné deriváty sú výborným nástrojom pre popis všeobecných vlastností rôznych materiálov a procesov ako je spracovanie signálu a obrazu. V rovnakom diele sa tvrdí, že nedávne výskumy úspešne aplikovali operátory frakčného kalkulu pre zlepšenie kvality obrazu, detekciu hrán a opravu obrazu. Pre vytvorenie domény používajú Heviside function of order alpha (HFOA). HFOA pre vloženie vodoznaku modeluje signál ako polynóm. Pre detekciu vodoznaku je využitá krížová korelácia založená na frakčnom Gaussovom poli (fraction Gaussian field). Autori tak vymysleli techniku, ktorá má veľkú mieru robustnosti a patrí medzi blind vodoznaky, čiže pre detekciu vodoznaku nie je potrebný pôvodný obraz.

3.1.2 Farebné obrazy

V posledných rokoch bol zaznamenaný významný pokrok vo watermarkingu obrazov v odtieňoch šedej použitím frakčných metód. Barni a Bartolini [3] uviedli schému pre watermarking farebných obrazov, ktorá je založená na krížovej korelácii RGB kanálov. V ich metóde je vodoznak vložený do nosného obrazu modifikáciou DCT koeficientov každého farebného kanálu. Lu, Zou, Yang a Wang [16] prezentujú metódu založenú na frakčnom watermarkingu pre farebné obrazy. V navrhovanej metóde je farebný pixel uvažovaný ako 3D vektor v RGB priestore.

Vo všeobecnosti môžeme hovoriť o dvoch prístupoch pre odhalenie porušenia autorských práv. Jedným je watermarking a tým druhým je fingerprinting. Základnou myšlienkou watermarkingu je vložiť informáciu, vodoznak do obrazu. Ak je podobný vodznak získaný z podozrivého obrazu, tak je považovaný za duplikát. Princípom fingerprintingu je extrahovať jedinečné vlastnosti z pôvodného obrazu, z podozrivého obrazu a porovnať ich. Ak sú si podobné, autorské práva môžu byť potvrdené. Fingerprinting je časovo náročnejší na spracovanie, pretože potrebuje extra čas pre porovnanie odtlačkov s tými ktoré sú uložené v databáze. Na druhej strane je fingerprinting robustnejší. [13]

Hsieh, Chen a Shen [13] využívajú komplementárnosť digitálneho watermarkingu a fingerprintigu pre identifikáciu autorských práv vo farebnom obraze. Využívajú overovacie logo a extrahované vlastnosti nosného obrazu pre generovanie odtlačku, ktorý je následne uložený v databáze a taktiež vložený do nosného obrazu ako vodoznak. Ak nastane spor ohľadom autorských práv, tak najprv je podozrivý obraz spracovaný watermarkingom. Ak je možné vodoznak získať, tak boli autorské práva potvrdené. V inom prípade vodoznak slúži ako fingerprint a je spracovaný fingerprintingom. Ak nastane zhoda medzi odtlačkom

získaným z podozrivého obrazu a odtlačkom, ktorý je uložený v databáze, tak je podozrivý obraz považovaný za duplikát. Pretože tento návrh využíva watermarking aj fingerprinting, tak je robustnejší ako len v prípade použitia watermarkingu a tiež sa skôr dopátrame k predbežnému výsledku na rozdiel od použitia samotného fingerprintingu. V prípade, že obraz podliehal ľahším útokom, tak na dokázanie autorských práv je postačujúci samotný watermarking. Pri tvrdších útokoch však môže byť vodoznak nečitateľný. Vtedy je použitý fingerprinting, ktorý dokáže úspešne identifikovať autorské práva. Týmto je demonštrovaná efektivita tejto metódy.

3.1.3 Print and scan

Veľa vodoznačiacich schém chrániacich autorské práva bolo predstavených a každá z týchto schém musela čeliť útokom, ktoré sa snažili vodoznak poškodiť alebo odstrániť. Medzi rôzne útoky patrí aj print-scan útok, ktorý sa snaží vodoznak poškodiť tým, že sa chránený obraz vytlačí a následne naskenuje. Čeliť tomuto útoku je zložité, pretože sa menia hodnoty pixelov a taktiež je zmenená pozícia pôvodných pixelov. Chen a Lin [4] navrhujú vodoznačiaci systém, ktorý využíva diskrétnu kosínusovú transformáciu pre farebné obrazy. Efektívnym integrovaním troch komponent, červenej, zelenej a modrej, navrhovaný systém vykazuje lepšiu robustnosť proti rôznym útokom vrátane útoku print-scan.

Viacero výskumníkov pracovalo na štúdiách ohľadom extrahovania vodoznaku z vytlačeného obrázku pomocou skenovania. Tieto systémy sú odolné voči print-scan procesu. Avšak tieto systémy vykazujú niektoré obmedzenia a slabé stránky v situáciách, keď obrázky nie sú jednoducho skenovateľné za účelom overenia obrázku. Práve preto Lee, Ting, a Wu [15] definovali nový spôsob spracovania obrazu, ktorý nazvali print-and-photo (PP) proces. Táto technika je vhodná zvlášť v takých prípadoch, keď nie je možné použiť skener, napríklad pri obrázku na pohybujúcom sa autobuse. Takto získané zábery môžu byť otočené, môžu mať zmenenú veľkosť, skreslenú sýtosť, či perspektívne skreslenie po PP procese. V navrhovanom systéme je spôsob vkladania a extrakcie vodoznaku založený na modifikácii a porovnaní rádovej veľkosti stredných hodnôt DCT v RGB farebnom modeli. Vodoznak môže byť extrahovaný z vodoznačeného obrazu bez použitia pôvodného obrazu alebo akýchkoľvek doplňujúcich informácii. Pre zlepšenie robustnosti využívajú QR kód pre korekciu chýb.

3.1.4 Využitie genetických algoritmov a reverzibility

Golshan a Mohammadi [11] prezentujú možnosť ako zlepšiť robustnosť a neviditeľnosť vodoznaku. Využívajú algoritmus singulárnej dekompozície (SVD) pre vytvorenie kompromisu medzi robustnosťou a neviditeľnosťou. V navrhovanom algoritme najprv rozdelia obraz do blokov o veľkosti 8 x 8. Následne sú niektoré špeciálne bloky transformované pomocou diskrétnej kosínusovej trasformácie (DCT). Ďalším krokom metódy je použitie SVD dekompozície nad DCT koeficientami špeciálnych blokov. Nakoniec je do obrazu vložený binárny vodoznak do singulárnych hodnôt pomocou kvantizačnej metódy. Hlavnou vlastnosťou navrhovanej metódy je však využitie genetického algoritmu pre generovanie binárneho vodoznaku. Genetický algoritmus pomáha vyriešiť optimalizačný problém medzi robustnosťou a neviditeľnosťou. Vodoznak teda môže byť premenný a prispôsobený obrazu. Simuláciou dokázali, že navrhovaná metóda vykazuje robustnosť proti rôznym útokom v porovnaní s nedávnou podobnou existujúcou prácou.

Moderné systémy pre zdravotnú starostlivosť sú založené na spravovaní diagnostických informácií pacientov cez E-health. K E-health patria aplikácie zdravotnej starostlivosti ko-

munikujúce cez internet, ktoré zahŕňajú prenos osobných zdravotných záznamov alebo informácii, teda bezpečnostné hrozby spôsobujú veľké obavy. Anusudha, Venkateswaran a Valarmathi [2] preto predstavujú hybridnú vodoznačiacu a šifrovaciu techniku pre ochranu autorských práv a pre overenie lekárskych obrázkov. Lekársky obrázok je vodoznačený vo vlnkovej doméne, kde elektronický zdravotný záznam (Electronic Health Record - EHR) je použitý ako vodoznak a logo nemocnice ako referenčný obrázok. K vylepšeniu bezpečnosti obrazu využívajú výhody šifrovania založeného na DNA a genetických algoritmoch. Genetický algoritmus je využitý pre nájdenie najlepšej DNA masky, deje sa to iteratívne, kým nie sú splnené požadované podmienky.

Pre konvenčné aplikácie nie je potrebné zachovať pôvodný obrázok po extrahovaní vodoznaku. Ak hovoríme o reverzibilnom algoritme pre ukrývanie dát, tak musí byť možné obnoviť a extrahovať pôvodný obsah aj vložené tajné dáta. Chen a Huang [5] navrhli watermarking systém, ktorý využíva genetický algoritmus a je aj reverzibilný. Genetický algoritmus využívajú pre zvolenie vhodného základu z prípustných základov vlnkovej transformácie za účelom zvýšiť robustnosť. Experimentálnymi výsledkami ukazujú, že navrhovaná metóda je odolná voči niektorým formám spracovania obrazu, ako napríklad zaostrenie. Použitie lokálnej predikcie pre reverzibilné vodoznaky poskytuje veľmi dobré výsledky za cenu vysokej výpočtovej náročnosti, pretože je potrebné počítať pre každý pixel vypočítať prediktor metódy najmenších štvorcov. Dragoi a Coltus [8] skúmali možnosť počítať prediktory nie pre každý pixel zvlášť, ale pre skupinu pixelov. Pri predikcii na kosoštvorci, ktorý má štyroch horizontálnych a vertikálnych susedoch zistili, že pri výpočte prediktoru pre dvojicu pixelov je výpočtová zložitosť polovičná bez straty na kvalite.

3.2 Audio watermarking

Súčasný výskum sa okrem watermarkingu obrazu venuje aj hľadaniu rôznym spôsobom ako a za akým účelom vložiť vodoznak do audio súborov. V poslednej dobe bolo prezentovaných niekoľko algoritmov pre audio watermarking. Audio watermarking je bezpečnejší, hlavne kvôli malému počtu rôznych metód pre vkladanie tajnej informácie do audia. Dôvodom menšieho počtu známych metód je to, že väčšina watermarking techník je určená pre obraz. [22]

Na základe domény pre vkladanie vodoznaku môžeme techniky pre watermarking audia rozdeliť do dvoch skupín, techniky využívajúce časovú doménu a metódy, ktoré fungujú vo frekvenčnej doméne. [10]

Zaujímavému riešeniu pre odstrániteľný watermarking systém pre audio sa vo svojej práci venovali Dutta, Gupta a Pathak [9]. V tejto práci navrhli systém, ktorý využíva nevnímateľný aj vnímateľný watermarking. Na začiatku máme audio súbor, ktorého časť chceme urobiť dostupnú pre prehratie ukážky a do zvyšnej časti vložíme vnímateľný vodoznak. Tento vodoznak je vložený do vybraných DCT koeficientov audio signálu tak, aby pomer šumu bol vysoký, čo zabezpečí to, aby tento signál bol otravný pre ľudský sluch. Ak je audio súbor dešifrovaný privátnym kľúčom, tak sa do tohto súboru vloží nový vodoznak, ktorý je nevnímateľný pre ľudský sluch. Vďaka tomuto dvojitému watermarkingu vytvorili nový spôsob pre kontrolu nad právami pre digitálne audio súbory.

Zamani, Mazdak a Manuf [22] vymysleli v roku 2015 nový algoritmus pre krehký watermarking audio súborov, ktorý je založený na genetickom koncepte. Zmyslom tohto algoritmu je redukovať skreslenie spôsobené substitúciou najmenej významných bitov za tajnú informáciu, zlepšiť pomer signálu ku šumu (PSNR) a zvýšiť kapacitu.

Fallahpour a Megias [10] sa zamerali na výskum novej vysoko kapacitnej audio watermarking metódy pracujúcej vo frekvenčnej doméne. Ku vkladaniu vodoznaku využívajú rýchlu Fourierovu transformáciu (Fast Fourier transform - FFT). Kľúčovou myšlienkou je rozdeliť FFT spektrum do krátkych rámcov a zmeniť veľkosť hodnoty FFT vzoriek na základe priemernej hodnoty vzoriek v každom rámci. Autori uvádzajú, že táto metóda má vysokú kapacitu bez významného vnímateľného skreslenia a ponúka robustnosť proti pridávaniu šumu, filtrovaniu a MPEG kompresii.

Jednou z tém výskumu audio watermarkingu je aj reverzibilita. Reverzibilné audio watermarking systémy sú konfrontované s problémami ako nízky pomer signálu ku šumu alebo nízka kapacita. Nový reverzibilný audio watermarking systém predstavujú Wang, Xie a Chen [21]. Táto metóda je založená na vylepšenej expanzii predikcie chyby (prediction error expansion) a na posune histogramu. Pre optimalizáciu koeficientov pre predikciu využívajú evolučný algoritmus.

3.3 Video watermarking

Výskum sa okrem watermarkingu obrazu a audia venuje taktiež videu. Ukážeme si dva rôzne prípady watermarkingu videa. Prvý z nich sa venuje problému akým spôsobom vložiť vodoznak do videa s HEVC (High Efficiency Video Coding) kódovaním. Druhá metóda sa okrem samotného watermarkingu videa zaoberá tiež praktickou aplikáciou na Blu-ray diskoch.

Stále pomerne novým a viac sa rozširujúcim video kodekom je HEVC, ktorý ponúka lepšiu kompresiu v porovnaním s jeho predchodcom H.264. Hlavne kvôli tomu, že HEVC môže mať v budúcnosti široké možnosti využitia, sa Swati, Hayat, Shahid a Pappalardo [18] rozhodli navrhnúť algoritmus určený pre watermarking tohto kodeku. Prezentovaný algoritmus má mať veľkú kapacitu a má potenciál pre použitie napríklad v skrývaní metadát pri vysielaní. Vodoznak je vložený do QT (Quantized Transform) koeficientov počas procesu kódovania. Neskôr pri procese dekódovania je vložená správa detegovaná a kompletne extrahovaná. Navrhovaný algoritmus viditeľne neovplyvňuje kvalitu videa a ani nezvyšuje bitrate.

De Cock, Hofbauer, Stütz, Uhl a Unterweger [6] predstavujú framework pre H.264 Blu-ray watermarking, ktorý operuje na úrovni bitového toku a zachováva dĺžku tohto toku. Okrem popisu prístupu pre vkladanie a detekciu vodoznaku sa venujú možnej kapacite pre rôzne Blu-ray disky na základe charakteristík ich bitového toku. Taktiež sa venujú diskusii o rôznych návrhových možnostiach a praktických problémoch, ktoré nastávajú pri návrhu watermarking frameworku na priemyselnej úrovni.

Kapitola 4

Návrh implementácie

V tejto kapitole sa zameriame na návrh implementácie vloženia a extrakcie vodoznaku pomocou QR rozkladu[1] do statického snímku v odtieňoch šedej ako to bolo prezentované v článku *Fast and robust watermarking in still images based on QR decomposition od Yashar Naderahmadian a Saied Hosseini-Khayat* [17].

Najprv sa budeme venovať tomu čo je to QR rozklad matice. Potom sa v sekciách 4.2 a 4.3 budeme venovať navrhovanému programovaciemu jazyku, použitým knižniciam pre implementáciu a samotnému spôsobu vloženia a extrakcie vodoznaku v priestorovej doméne. Následne navrhneme spôsob testovania a konkrétnych útokov voči ktorým budeme testovať odolnosť navrhnutého princípu vloženia vodoznaku.

Navrhovaným riešením je použiť obrázok vo formáte JPEG, ktorý bude potrebné previesť do odtieňov šedej a následne vytvoriť 2D maticu s hodnotami intenzity čiernej v rozsahu 0-255.

4.1 QR rozklad

Pri definícii QR rozkladu vychádzame z poznatkov uvedených v článku [17]. V lineárnej algebre je QR rozklad matice A definovaný ako rozklad tejto matice na súčin 2 matíc. Z nich jedna je ortogonálna (alebo má aspoň vzájomne ortonormálne stĺpce) a druhá je v hornom trojuholníkovom tvare. Teda v QR rozklade je $m \times n$ matica A reprezentovaná ako:

$$A = QR \tag{4.1}$$

Kde Q je $m \times n$ matica s ortonormálnymi stĺpcami a R je matica v hornom trojuholníkovom tvare. V tejto metóde sú stĺpce matice Q vytvorené zo stĺpcov matice A pomocou Gramovho-Schmidtovho procesu. Ak A a Q, dané ako $A = [a_1, a_2, \ldots, a_n], Q = [q_1, q_2, \ldots, q_n]$ sú vektormi stĺpcov, potom matica R môže byť vypočítaná ako:

$$R = \begin{bmatrix} \langle a_1, q_1 \rangle & \langle a_2, q_1 \rangle & \ldots & \langle a_n, q_1 \rangle \\ 0 & \langle a_2, q_2 \rangle & \ldots & \langle a_n, q_2 \rangle \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \ldots & \langle a_n, q_n \rangle \end{bmatrix} \tag{4.2}$$

[1] QR decomposition https://en.wikipedia.org/wiki/QR_decomposition

Kde $\langle a, q \rangle$ znamená skalárny súčin. Stĺpce matice Q (nového ortonormálneho základu pre n-dimenzionálny vektorový priestor) sú získané zo stĺpcov A pomocou Gramovho-Schmidtovho procesu. Potom projekcia stĺpcov matice A na nový základ vyprodukuje maticu R.

Vlastnosť matice R, ktorá bola dokázaná v [17] a ktorá je použitá v tejto schéme je, že ak sú stĺpce matice A korelované (ako v prípade obrazu), tak s veľkou pravdepodobnosťou je absolútna hodnota prvkov prvého riadku matice R väčšia ako absolútna hodnota ostatných riadkov. Výsledkom toho je, že malé zmeny v prvom riadku by nemali ovplyvniť vizuálnu kvalitu nosného obrazu. Ak teda zvolíme ostatné riadky pre vloženie vodoznaku, tak bude zreteľná vizuálna zmena vo vodoznačenom obraze, čo nie je vhodné. Detaily sú dostupné v prílohe článku *Fast and robust watermarking in still images based on QR decomposition* [17]. Preto sme použili prvý riadok matice R, ako kompromis medzi robustnosťou a neviditeľnosťou vloženého vodoznaku.

4.2 Programovací jazyk a knižnice

Pre implementáciu sa ponúka viacero možností aký programovací jazyk využiť. Teoreticky je pre riešenie problému watermarkingu možné využiť ľubovoľný programovací jazyk. Avšak pre jednoduchšie riešenie je vhodné, ak pre tento jazyk existuje knižnica alebo modul, ktorý ponúka zjednodušenú manipuláciu s obrazom a maticami.

Často využívaným jazykom pre riešenie tohto typu problému je jazyk MATLAB, čo je zreteľné aj vo viacerých vedeckých článkoch zameraných na watermarking. Výhoda tohto jazyka spočíva v jednoduchej manipulácii s maticami. Obsahuje množstvo vstavaných funkcií pre prácu s obrázkami a spomínanými manipuláciami matíc.

Ďalším jazykom, ktorý by pripadal v úvahu, by mohol byť jazyk Python. Momentálne patrí medzi jeden z najviac rozšírených jazykov. Je to multi-paradigmový jazyk, čiže je možné využiť rôzne programátorské prístupy ako objektovo orientované, štruktúrované ale aj funkcionálne programovanie. Jeho veľkou výhodou je jednoduché rozširovanie o množstvo modulov. Pre watermarking sa núka možnosť použiť moduly ako PIL (Python Imaging Library) alebo OpenCV.

Jazykom ktorý budeme využívať pri tejto implementácii bude jazyk C++. Keďže tento jazyk neumožňuje prácu s obrazom, sme nútení siahnuť po knižniciach, ktoré nám to zjednodušia. Prvým problémom ktorý potrebujeme vyriešiť je načítanie obrázku vo formáte JPEG, jeho dekompresia a následné uloženie do matice, nad ktorou budeme vykonávať QR rozklad. Existuje viacero knižníc pre C++, pomocou ktorých sme schopní túto úlohu riešiť. Medzi najviac používané knižnice pre manipuláciu obrazu patria knižnice libjpeg, OpenCV a ImageMagick. Knižnica libjpeg je distribuovaná ako voľný softvér so zdrojovým kódom pod Custom BSD-like licenciou, je napísaná v jazyku C a umožňuje prácu s obrazom vo formáte JPEG. Implementuje JPEG kodek a ďalšie rôzne utility pre narábanie s dátami vo formáte JPEG. Originálny variant je udržovaný a vydávaný Independent JPEG Group (IJC), čiže sa jedná o štandard pre spracovávanie JPEG formátu. Dôležitou vlastnosťou, ktorú budeme potrebovať hlavne pre testovanie odolnosti vodoznaku, je možnosť prispôsobiť kvalitu kompresie.

OpenCV (Open Source Computer Vision) je vydávaná pod BSD licenciou a poskytuje rozhranie pre jazyky C, C++, Python a Java. Hlavným zameraním tejto knižnice je počítačové videnie v reálnom čase. Pre potreby načítania obrazu do matice je táto knižnica zbytočne robustná.

ImageMagick je knižnica pre manipuláciu obrazu v rôznych formátoch (viac ako 200). Umožňuje rôzne operácie nad obrazom, ako napríklad zmenu veľkosti, zrkadlenie, rotáciu, prispôsobenie farieb, kreslenie alebo aplikovanie špeciálnych efektov. Funkcionalita ImageMagick je typicky využívaná prostredníctvom príkazového riadku alebo je možné využiť API pre jeden z množstva programovacích jazykov medzi ktoré patria napríklad jazyky C, C++, PHP alebo Python. Pre jazyk C++ je vytvorené objektovo orientované API s názvom Magick++. Túto knižnicu je vhodné použiť na načítanie a uloženie obrázku, ako aj pri testovaní kvality vodoznačiacej metódy pri transformáciách a kompresii do formátu JPEG.

4.3 Vloženie a extrakcia vodoznaku

Prvou požiadavkou pre aplikovanie vodoznaku je potreba vytvorenia matice z nosného obrázku, kde každý prvok matice bude o veľkosti 8b, teda bude nadobúdať hodnoty v rozsahu 0-255. Ako vodoznak môžu byť použité akékoľvek digitálne dáta.

Následne môžeme pristúpiť k samotnej procedúre vloženia, ktorá je nasledujúca:

1. Nosný obraz rozdelíme do neprekrývajúcich sa blokov o veľkosti 8×8.
2. QR rozklad sa aplikuje na každý 8×8 blok.
3. Vodoznak sa vloží do prvého riadku matice R použitím vzorca 4.3, kde C je vybraný koeficient matice kam sa vloží bit vodoznaku, C' je zmenený koeficient, S je zvolená sila vodoznaku, $T1$ a $T2$ sú prahové hodnoty a ω je bit vodoznaku.

$$\begin{cases} C' = C - (C \mod S) + T_1 & if \quad \omega = 0 \\ C' = C - (C \mod S) + T_2 & if \quad \omega = 1 \end{cases} \tag{4.3}$$

4. Aplikujeme inverzný QR rozklad pre každý blok.

Po prevedení tejto procedúry je potrebné zo vzniknutej matice, ktorá už obsahuje aj vodoznak, vytvoriť opäť obrázok napríklad vo formáte JPEG, čo dosiahneme pomocou knižnice Magick++.

Procedúra pre extrakciu vodoznaku je takáto:

1. Vodoznačený obraz je rozdelený do neprekrývajúcich sa blokov o veľkosti 8×8.
2. QR rozklad sa aplikuje na každý blok.
3. Vodoznak bude extrahovaný z prvého riadku matice R za použitia vzorca 4.4, kde ω' je extrahovaný vodoznak a C'' je vodoznačený koeficient po možných útokoch. Je zrejmé, že táto procedúra nepotrebuje originálny nosný obraz, a preto je tento navrhovaný princíp označovaný ako *blind*.

$$\begin{cases} \omega' = 1, & if (C'' \mod S) > \frac{T_1+T_2}{2} \\ \omega' = 0, & if (C'' \mod S) < \frac{T_1+T_2}{2} \end{cases} \tag{4.4}$$

Na obrázku 4.1 je znázornený postup procesu vkladania a extrakcie vodoznaku.

Obr. 4.1: Diagram vloženia a extrakcie vodoznaku

4.4 Kapacita

V priestorovej doméne je nosný obraz rozdelený do blokov o rozmeroch 8×8 a potom sa do každého z blokov vloží 8 bitov vodoznaku. Ak budeme uvažovať veľkosť nosného snímku ako $N \times N$, potom maximálna kapacita vkladaného vodoznaku je:

$$\frac{\frac{N \times N}{8 \times 8} \times 8}{N \times N} = 0,125(bit/pixel) \tag{4.5}$$

Ako je uvedené v [17], kapacita tejto metódy je vyššia ako vo všetkých spomínaných blind metódach, ktoré sú spomenuté v rovnakom článku. V rovnakom článku sa tvrdí, že kapacita tejto metódy je porovnateľná s non-blind metódami.

4.5 Návrh testovania

Testovanie kvality navrhovanej metódy watermarkingu bude prevádzané prostredníctvom zmeny sily watermarkingu S a útokov na vodoznačený obraz. Následnou extrakciou vodoznaku môžeme merať odolnosť tejto metódy voči konkrétnym útokom.

K vyhodnoteniu kvality po prevedení útokov budeme využívať normalizovanú koreláciu (NC) medzi originálnym vodoznakom ω a extrahovaným vodoznakom ω'.

Kvalita vodoznačeného obrazu bude meraná prostredníctvom pomeru medzi maximálnou možnou energiou signálu a energiou šumu (PSNR). Ako minimálna akceptovateľná hodnota PSNR je považovaná hodnota 37-40dB. Hodnota PSNR sa znižuje so zvyšujúcou sa silou vodoznaku S. Preto musíme nájsť maximálnu hodnotu S takú, aby nebolo možné pozorovať viditeľné vizuálne zmeny na vodoznačenom obraze. Na druhej strane musí byť hodnota S dostatočne vysoká na to aby bolo schopné vodoznak extrahovať bez chyby pri nepoužití žiadneho útoku. Vodoznak je extrahovaný bez chyby ak je NC = 1.

Testovať budeme odolnosť vodoznaku voči rotácii obrazu, zmene veľkosti a orezaniu. Použijeme taktiež útoky vo forme vloženia šumu do obrazu, napríklad Gaussovský šum. Ako ďalšia forma útoku bude použité filtrovanie. Vykonávať budeme mediánové filtrovanie a filtrovanie priemerovaním. Keďže podľa [17] má mať tento systém zvýšenú odolnosť proti JPEG kompresii, tak overíme odolnosť tejto metódy proti rôznym úrovniam JPEG kompresie.

Kapitola 5

Implementácia

Nasledujúca kapitola sa venuje implementácii navrhovaného algoritmu pre digitálne vodoznačenie obrazu. V tejto kapitole budú vysvetlené jednotlivé funkcie použité v programe a taktiež odlišnosti medzi návrhom a implementovaným algoritmom.

Ako už bolo spomenuté v návrhu v kapitole 4.2, algoritmus je implementovaný v jazyku C++ s využitím knižnice ImageMagick. Konkrétne s využitím objektovo orientovaného API tejto knižnice pre jazyk C++, Magick++. Táto knižnica je postačujúca pre načítanie a uloženie obrazu, ako aj pre transformácie výsledného obrazu, pridanie šumu alebo nastavenie úrovne kompresie. Preto nie je potrebné použiť žiadne ďalšie knižnice.

Časť 5.1 sa venuje načítaniu jednotlivých pixelov vstupného obrázku do požadovanej dátovej štruktúry tak, aby bola ďalšia práca s týmito hodnotami čo najjednoduchšia. Nasleduje časť 5.2, ktorá sa zaoberá problémom rozdelenia načítaného obrazu do blokov o veľkosti 8×8 a následného spojenia týchto blokov po prevedení QR rozkladu a vloženia alebo extrakcie vodoznaku. Implementáciu algoritmu pre QR rozklad nájdeme v 5.3. Proces vkladania a extrakcie vodoznaku a nutné zmeny v týchto algoritmoch oproti návrhu nájdeme v 5.4. Nakoniec v časti 5.5 sa nachádza návod na použitie výsledného programu.

5.1 Načítanie dát

Prvým riešeným problémom bolo načítanie intenzít odtieňovej šedej z obrázku do vhodnej dátovej štruktúry s ktorou by sa následne pracovalo. Ako dátovú štruktúru je vhodné použiť 2-rozmerné dynamické pole, čo dosiahneme využitím `std::vector`, výsledný nami definovaný dátový typ je `matrix_t` definovaný ako:

```
template< typename T > using matrix_t = vector< vector<T> >;
```

Obrázok zo súboru načítame pomocou Magick++ metódy `read()`. Táto metóda načíta obrázok do aktuálneho `Magick::Image` objektu. My však potrebujeme iba hodnoty intenzít konkrétnych pixelov. Na tento účel slúži funkcia

```
matrix_t<double> image2matrix(Image &image),
```

ktorá uloží hodnoty jednotlivých pixelov do dátového typu `matrix_t`.

Týmto spôsobom je možné načítať obrázok v akomkoľvek formáte, ktorý je podporovaný knižnicou ImageMagick. My sme si ako vstupný obrázok vo formáte JPEG zvolili známy obrázok Lena 5.1, ktorý je často používaný pre rôzne úlohy spracovávania obrazu. Tento obrázok má rozlíšenie 512×512 pixelov a je v odtieňoch šedej s 8bitovou hĺbkou. Ako vodoznak používame 5.2 vo formáte PBM s 1bitovou farebnou hĺbkou v rozlíšení 256×128

Obr. 5.1: Vstupný obrázok - lena.jpg

Obr. 5.2: Vkladaný vodoznak - fit.pbm

pixelov. Rozlíšenie vodoznaku je maximálne možné vzhľadom na kapacitu vodoznačiacej metódy pri vstupnom obrázku v danom rozlíšení.

Pri načítavaní vstupného obrázku metódou `read()` sme objavili, že načítaný obrázok v odtieňoch šedej nemá iba jeden kanál, ale dva kanály. Jeden kanál obsahuje hodnoty intenzít v rozsahu $0-255$ a druhý v rozsahu $0-65535$ čo odpovedá rozsahu `QuantumRange` z Magick++. Ďalšou nečakanou vecou je, že knižnica pracuje s hodnotou 0 pre čiernu farbu a s hodnotou 255 pre bielu, čiže opačne ako bolo zamýšľané pri návrhu algoritmov pre vkladanie a extrakciu vodoznaku.

5.2 Rozdelenie do blokov

Kvôli zvýšeniu robustnosti navrhovanej metódy je potrebné načítaný obraz rozdeliť do blokov o veľkosti 8 pixelov. Myšlienkou je rozdeliť načítanú maticu intenzít pixelov na skupinu matíc. Na ich uloženie potrebujeme trojdimenzionálne dynamické pole. Ako dátový typ pre uloženie všetkých blokov sme si definovali typ `matrix3d_t`, ktorý je definovaný nasledovne:

```
template< typename T >
using matrix3d_t = vector< matrix_t<T> >;
```

Samotné rozdelenie sa deje pomocou funkcie `get_blocks()`, ktorej prvým argumentom je matica intenzít pixelov a druhým argumentom je veľkosť bloku. Návratovou hodnotou tejto funkcie je pole všetkých blokov. Táto funkcia je deklarovaná ako:

```
template< typename T >
matrix3d_t<T> get_blocks(const matrix_t<T> &matrix, int n=8)
```

Po prevedení QR rozkladu a vložení vodoznaku do nosného obrazu je potrebné bloky naspäť poskladať do výsledného obrazu. Pre zloženie blokov je implementovaná funkcia `concat_blocks()`, ktorá prechádza všetkými blokmi a spojí ich do výslednej matice typu `matrix_t`. Deklarácia funkcie je nasledovná:

```
template< typename T >
void concat_blocks(matrix_t<T> &result, matrix3d_t<T> &blocks)
```

5.3 QR rozklad

Táto časť sa venuje algoritmu QR rozkladu, ktorý je základom pre navrhovaný systém vodoznačenia. QR rozklad môžeme dosiahnuť viacerými spôsobmi. Najjednoduchším algoritmom pre vytvorenie QR rozkladu z matice je *Gramov-Schmidtov proces*[1]. Medzi ďalšie spôsoby patrí *Householderova transformácia*[2] a *Givensova rotácia*[3].

Pre našu implementáciu algoritmu QR rozkladu sme využili *Gramov-Schmidtov* proces, konkrétne jeho modifikovanú variantu. Výhodou modifikovaného Gramovho-Schmidtovho procesu je, že je oproti klasickej verzii numericky stabilný[4]

Tento algoritmus je implementovaný funkciou `gram_schmidt()`, ktorá zo zadanej matice vytvorí matice Q a R a uloží ich do zoznamov týchto matíc. Deklarácia tejto funkcie je takáto:

```
template< typename T >
void gram_schmidt(matrix_t<T> &matrix, matrix3d_t<T> &q_list,
                  matrix3d_t<T> &r_list)
```

Keďže QR rozklad je potrebné vytvoriť nad stĺpcami matice A, čiže nad transponovanou maticou A, bolo potrebné implementovať funkciu `mat_transpose()` pre transpozíciu matice dátového typu `matrix_t`. V algoritme QR rozkladu je potrebné taktiež vypočítať skalárny súčin vektorov a normalizovaný vektor. Pre skalárny súčin slúži funkcia `dot_product()` a pre normalizáciu funkcia `normalize()`.

[1] Gram-Schmidt process https://en.wikipedia.org/wiki/Gram\T1\textendashSchmidt_process
[2] Householder transformation https://en.wikipedia.org/wiki/Householder_transformation
[3] Givens rotation https://en.wikipedia.org/wiki/Givens_rotation
[4] Numerical stability https://en.wikipedia.org/wiki/Numerical_stability

5.4 Algoritmus vkladania a extrakcie

Po prevedení QR rozkladu nad každým blokom môžeme pristúpiť ku vkladaniu vodoznaku do nosného obrazu. Vodoznak vkladáme do matice R, konkrétne do jej prvého riadku.

Za účelom vkladania vodoznaku do obrazu sme implementovali funkciu `embed()`, ktorej deklarácia je takáto:

```
template< typename T >
void embed(matrix_t<T> &matrix, vector<T> &watermark,
           int strength, int iteration, int size=8)
```

Keďže hodnoty pre čierny a biely pixel pri použití knižnice ImageMagick sú opačné ako sme očakávali, museli sme upraviť aj vzorec 4.3 pre vloženie vodoznaku do obrazu. Upraviť bolo potrebné tiež hodnotu vodoznaku, pretože skúmame hodnotu konkrétneho pixelu, ktorá nadobúda hodnoty buď 0 alebo 255. Výsledný vzorec použitý pri implementácii je nasledovný:

$$\begin{cases} C' = C - (C \mod S) + T_1 & if \quad \omega = 255 \\ C' = C - (C \mod S) + T_2 & if \quad \omega = 0 \end{cases} \tag{5.1}$$

Pre extrakciu vodoznaku je implementovaná funkcia `extract()` deklarovaná ako:

```
template< typename T >
void extract(matrix_t<T> &matrix, vector<T> &watermark,
             int strength, int size=8)
```

Vzorec pre extrakciu vodoznaku 4.4 bolo potrebné upraviť podobne ako vzorec pre vkladanie vodoznaku. Dôvodom je taktiež to, že pracujeme s hodnotami 0 a 255. Upravený vzorec je:

$$\begin{cases} \omega' = 255, & if (C'' \mod S) > \frac{T_1+T_2}{2} \\ \omega' = 0, & if (C'' \mod S) < \frac{T_1+T_2}{2} \end{cases} \tag{5.2}$$

5.5 Použitie programu

Výsledný program s názvom `watermarking` dokáže vložiť zadaný vodoznak do obrázku v jednom z vyše 200 podporovaných obrazových formátov, ktoré sú podporované knižnicou ImageMagick. Program dokáže extrahovať vodoznak z obrázku a porovnať ho s referenčným vodoznakom. Umožnené je tiež spustenie programu s útokmi na vodoznačený obraz, ktoré budú využité v kapitole 6.

Prepínače programu sú nasledovné:

- `--help` - zobrazí nápovedu k programu
- `--input FILE` - určenie vstupného obrázku
- `--output FILE` - určenie kam sa uloží vodoznačený obraz
- `--wm-input FILE` - názov súboru obsahujúci vodoznak
- `--wm-output FILE` - názov súboru, kam sa má uložiť extrahovaný vodoznak
- `--strength NUMBER` - nastavenie úrovne sily vodoznačiacej metódy

- `--quality NUMBER<0-100>` - nastavenie úrovne kompresie výstupného vodoznačeného obrazu
- `--embed` - vkladanie vodoznaku
- `--extract` - extrakcia vodoznaku
- `--attack` - prevedenie série útokov na vodoznačený obraz
- `--statistics` - zobrazenie NC extrahovaného a pôvodného vodoznaku a PSNR medzi originálnym a vodoznačeným obrazom

Jedinými povinnými argumentmi sú prepínače `--input` a `--wm-input`, ktorými špecifikujeme vstupné dáta. Pri neuvedení prepínačov `--embed` a `--extract` sa prevedie vloženie a aj následná extrakcia vodoznaku. Použitie prepínača `--statistics` je podmienené extrakciou vodoznaku, čiže je potrebné použiť prepínač `--extract` alebo nepoužiť žiaden z prepínačov `--embed, --extract`.

Kapitola 6

Testy a výsledky

Jednou z hlavných vlastností vodoznaku okrem jeho kapacity a nevnímateľnosti je jeho robustnosť. V prípade použitia vodoznaku pre ochranu autorských práv je táto vlastnosť nesmierne dôležitá. Môžeme mať vodoznačiacu metódu, ktorá má vysokú kapacitu a ktorá dokáže do obrazu vložiť vodoznak, ktorý je ľudským okom nepostrehnuteľný, ale ak je tento vodoznak možné poškodiť bežným spracovaním obrazu natoľko, že nie je čitateľný, tak takáto metóda nebude vhodná napríklad pre ochranu autorských práv.

Práve preto sa táto kapitola venuje testovaniu implementovanej metódy watermarkingu. Pre účely testovania implementovaný program umožňuje použiť prepínač `--attack`, ktorý vykoná všetky útoky zobrazené v nasledujúcich podkapitolách. Testované budú rôzne metódy vylepšenia obrázku v časti 6.3 a vkladania šumu v časti 6.2. V rámci overovania odolnosti taktiež otestujeme tento algoritmus voči zaostreniu obrazu a ekvalizácii histogramu. Následne vyskúšame robustnosť algoritmu proti transformáciám ako sú rotácia alebo zmena veľkosti v časti 6.4. Na záver v podkapitole 6.5 podrobíme testovaný obrázok JPEG kompresii.

6.1 Zvolenie sily vodoznaku

Skôr ako sa pustíme do testovania robustnosti tejto metódy, musíme nájsť vhodnú hodnotu pre silu vodoznačenia. Pre nájdenie vhodnej hodnoty sily vodoznaku S je nutné splniť dve podmienky.

Prvou podmienkou je, že po vložení vodoznaku musí byť možné bez chyby vodoznak z obrázku extrahovať. K porovnaniu vloženého a extrahovaného vodoznaku nám slúži normalizovaná korelácia NC, ak je vodoznak extrahovaný bez chyby, tak $NC = 1$.

Druhou podmienkou je neviditeľnosť vodoznaku. So zvyšujúcou sa silou vodoznaku S rastie počet viditeľných zmien v obraze, preto musíme zvoliť silu vodoznaku tak, aby bola sila vodoznaku čo najvyššia a aby bol vodoznak neviditeľný. K tomuto účelu slúži pomer medzi energiou signálu a energiou šumu $PSNR$. Vo väčšine článkov sa dozvedáme, že minimálna akceptovateľná hodnota $PSNR$ je 37-40dB.

Na základe nižšie uvedených testov rôznych úrovní sily vodoznaku v tabuľke 6.1 sme zvolil hodnotu $S = 24$, pretože pri hodnote $S = 26$ s $PSNR = 37,39dB$ už boli jasne zreteľné zmeny v obraze.

Sila vodoznaku	NC	PSNR
1	1	62,95
5	1	51,64
10	1	45,91
15	1	41,99
20	1	39,43
22	1	38,94
24	1	37,86
26	1	37,39

Tabuľka 6.1: Zvolenie sily vodoznaku

6.2 Vloženie šumu

V nasledujúcej tabuľke 6.2 sú zobrazené útoky vložením šumu do vodoznačeného obrazu. Môžeme si všimnúť, že náš algoritmus vodoznačenia sa dokáže vysporiadať jedine s rovnomerným šumom. Pri ostatných druhoch šumu považujeme vodoznak za nerozoznateľný.

Typ útoku	NC	Vodoznačený obraz	Extrahovaný vodoznak
Gaussovský šum	0.002		
Rovnomerný šum	1		
Laplaceov šum	0.002		
Poissonov šum	0.002		

Tabuľka 6.2: Útoky vložením šumu

6.3 Vylepšenie obrazu

Tabuľka 6.3 zobrazuje vykonané vylepšenia obrazu a ich dopad na vložený vodoznak. Ako môžeme vidieť, algoritmus pre vkladanie vodoznaku je robustnejší proti rôznym metódam vyhladzovania obrazu ako proti útokom, ktoré do obrazu vložia šum.

Z dát z tabuľky vidíme, že najväčšiu robustnosť má algoritmus proti mediánovému filtru, kde sme schopní extrahovať nezmenený vodoznak. Pri odstránení šumu, vyhladení a zaostrení je to už horšie, no stále sme schopní rozoznať vodoznak. Z týchto útokov sa ukázal

ako najtvrdší útok ekvalizovaním histogramu, pri ktorom môžeme považovať vodoznak za zničený.

Typ útoku	NC	Vodoznačený obraz	Extrahovaný vodoznak
Rozmazanie	0.287		
Gaussovské rozostrenie	0.281		
Mediánový filter	1		
Filtrovanie priemerovaním	0.195		
Odstránenie šumu	0.590		
Vyhladenie	0.449		
Zaostrenie	0.408		
Ekvalizácia histogramu	0.031		

Tabuľka 6.3: Útoky vylepšením obrazu

6.4 Transformácie obrazu

Transformácie obrazu sú častým prípadom spracovávania obrazu. V tejto časti overíme odolnosť vodoznaku proti zmene veľkosti obrázku a rotácii.

Typ útoku	NC	Vodoznačený obraz	Extrahovaný vodoznak
Zmenšenie o 25%	0.298		
Zväčšenie o 25%	0.390		
Rotácia o 5 stupňov	0.014		
Rotácia o 10 stupňov	0.160		

Tabuľka 6.4: Útoky transformáciou obrazu

Pri týchto útokoch bolo určenie normalizovanej korelácie zložitejšie ako pri iných útokoch. Dôvodom je, že zmenou veľkosti nosného obrázku sa zmenia aj rozmery extrahovaného vodoznaku. Pre vyriešenie tohto problému sme po extrahovaní vodoznaku tento vodoznak zväčšili alebo zmenšili na základe pomeru v akom sa zmenil nosný obraz. Po zmene veľkosti vodoznaku sme však narazili na ďalší problém, zmenou veľkosti vodoznak nadobudol aj iné hodnoty ako 0 alebo 255. Riešením je následné prahovanie extrahovaného vodoznaku.

Ako vidíme v tabuľke, pri každom z týchto útokov bol vodoznak značne poškodený. Najúspešnejšie dopadol test na zväčšenie vodoznačeného obrazu o 25% s $NC = 0,390$. Naopak najhoršie dopadli obidva útoky rotáciou obrazu. Pri rotáciách je výsledný vodoznak neidentifikovateľný.

6.5 Útoky kompresiou

Stratová JPEG kompresia dokáže poškodiť vložený vodoznak natoľko, že ho nebude možné rozoznať. Práve preto sme sa pri testovaní zamerali aj na tento typ útoku. Nasledujúca tabuľka 6.5 zobrazuje výsledky pri rôznej úrovni kompresie.

Typ útoku	NC	Vodoznačený obraz	Extrahovaný vodoznak
JPEG 70%	0.614		
JPEG 50%	0.429		
JPEG 30%	0.298		
JPEG 20%	0.193		

Tabuľka 6.5: Útoky JPEG kompresiou

Po útokoch stratovou JPEG kompresiou môžeme skonštatovať, že ešte pri 50% kompresii sme schopní rozpoznať extrahovaný vodoznak. Pri zvolení silnejšej kompresie je vodoznak už vážnejšie poškodený.

Kapitola 7

Záver

Cieľom tejto práce bolo analyzovať možnosti využitia watermarkingu pri ochrane obrazového záznamu, navrhnúť a implementovať základné moduly programového systému umožňujúce takúto ochranu a následné zhodnotenie tohto riešenia.

Zo skúmania súčasného stavu môžeme na základe počtu publikovaných vedeckých článkov zhodnotiť, že watermarking je stále aktuálnou témou výskumu. Vo väčšine publikácií stále pretrváva použitie watermarkingu pre statický obraz, no objavujú sa aj diela, ktoré predstavujú návrhy systémov pre ochranu iných typov multimédií. Zaujímavým je napríklad využívanie genetických algoritmov pre vytvorenie optimálneho vodoznaku.

Pri našej implementácii systému pre vkladanie a extrakciu vodoznaku sme využili návrh algoritmu prezentovaný v [17], ktorý využíva QR rozklad pre ukrytie vodoznaku do nosného obrázku. Tento algoritmus bol využitý hlavne kvôli deklarovanej zvýšenej odolnosti tejto metódy proti JPEG kompresii. Na rozdiel od článku v ktorom bol tento prístup prezentovaný, sme využili maximálnu možnú kapacitu metódy. Použili sme iný nosný obrázok do ktorého bol vodoznak vkladaný a tiež sme použili iný vodoznak. Tieto zmeny mohli viesť k rozdielnym výsledkom našej implementácie.

Výsledkom práce je fungujúci systém schopný vkladania a extrakcie vodoznaku. Nosný obrázok v odtieňoch šedej, ako aj vkladaný čiernobiely vodoznak môže byť v jednom z vyše 200 podporovaných formátov. Pri testovaní našej implementácie sme využili nosný obrázok vo formáte JPEG a vodoznak vo formáte PBM. Systém je naprogramovaný v jazyku C++ s využitím knižnice ImageMagick, ktorá slúži pre spracovávanie obrazu.

Pri testovaní prezentovaného riešenia sme zvolili ako najvhodnejšiu hodnotu sily vodoznaku $S = 24$, pri ktorej bol pomer energie signálu k energii šumu $PSNR = 37,86dB$. Následne bolo implementované riešenie podrobené testom. Z testov, ktoré útočili na vodoznačený obraz vložením šumu sme zistili, že algoritmus sa dokáže vysporiadať iba s vložením šumu s rovnomerným rozložením. Pri testoch za účelom vylepšenia obrazu sme zistili, že najlepšie obstál test s využitím mediánového filtrovania, kedy bol extrahovaný vodoznak totožný s vloženým vodoznakom. Naopak po prevedení ekvalizácie histogramu môžeme vložený vodoznak považovať za zničený. Pri skúmaní odolnosti proti zmene veľkosti obrázku a rotácii najlepšie dopadol útok, ktorý vodoznačený obrázok zväčšil o 25%. Z útokov pomocou JPEG kompresie konštatujeme, že ešte pri použití 50% kompresii sme schopní extrahovaný vodoznak vizuálne rozpoznať.

Implementované riešenie bolo preložené a testované na operačnom systéme *Fedora 24* s prekladačom *GCC 6.3.1* a s využitím knižnice *ImageMagick* vo verzii *7.0.5-4*.

Literatúra

[1] Abbasi, A.; Woo, C. S.; Ibrahim, R. W.; aj.: *Invariant Domain Watermarking Using Heaviside Function of Order Alpha and Fractional Gaussian Field. PLoS ONE*, ročník 10, č. 4, 2015: s. 1–14, doi:10.1371/journal.pone.0123427, [Online; navštívené 19.02.2017].
URL
http://journals.plos.org/plosone/article?id=10.1371/journal.pone.0123427

[2] Anusudha, K.; Venkateswaran, N.; Valarmathi, J.: *Secured medical image watermarking with DNA codec. Multimedia Tools and Applications*, ročník 76, č. 2, 2017: str. 2911–2932, ISSN 13807501, doi:10.1007/s11042-015-3213-1, [Online; navštívené 19.02.2017].
URL http://link.springer.com/10.1007/s11042-015-3213-1

[3] Barni, M.; Bartolini, F.: *Watermarking systems engineering: enabling digital assets security and other applications*. Marcel Dekker, 2004, ISBN 0824748069.

[4] Chen, P.-Y.; Lin, C.-L.: *Print and scan resistant watermarking scheme for colour images. The Imaging Science Journal*, ročník 63, č. 5, 2015: s. 273–284, ISSN 1368-2199, doi:10.1179/1743131X15Y.0000000010, [Online; navštívené 19.02.2017].
URL http://www.tandfonline.com/doi/full/10.1179/1743131X15Y.0000000010

[5] Chen, Y. H.; Huang, H. C.: *Reversible Image Watermarking Based on Genetic Algorithm*. In *2014 Tenth International Conference on Intelligent Information Hiding and Multimedia Signal Processing*, IEEE, 2014, ISBN 9781479953905, s. 21–24, doi:10.1109/IIH-MSP.2014.13, [Online; navštívené 19.02.2017].
URL http://ieeexplore.ieee.org/document/6998258/

[6] Cock, J. D.; Hofbauer, H.; Stütz, T.; aj.: *An industry-level blu-ray watermarking framework. Multimedia Tools and Applications*, ročník 74, č. 18, 2015: s. 8079–8101, ISSN 13807501, doi:10.1007/s11042-014-2042-y, [Online; navštívené 19.02.2017].
URL http://link.springer.com/10.1007/s11042-014-2042-y

[7] Cox, I. J.; Miller, M. L.; Bloom, J. A.; aj.: . *Digital watermarking and steganography*. Morgan Kaufmann Publishers, druhé vydání, 2008, ISBN 0-12-372585-2.

[8] Dragoi, I.-C.; Coltuc, D.: *On Local Prediction Based Reversible Watermarking. IEEE Transactions on Image Processing*, ročník 24, č. 4, 2015: s. 1244–1246, ISSN 10577149, doi:10.1109/TIP.2015.2395724, [Online; navštívené 19.02.2017].
URL http://ieeexplore.ieee.org/document/7018019/

[9] Dutta, M. K.; Gupta, P.; Pathak, V. K.: *A perceptible watermarking algorithm for audio signals. Multimedia Tools and Applications*, ročník 73, č. 2, 2014: s. 691–713, ISSN 13807501, doi:10.1007/s11042-011-0945-4, [Online; navštívené 19.02.2017].
URL http://link.springer.com/10.1007/s11042-011-0945-4

[10] Fallahpour, M.; Megias, D.: *High capacity robust audio watermarking scheme based on FFT and linear regression. International Journal of Innovative Computing, Information and Control*, ročník 8, č. 4, 2012: s. 2477–2489, ISSN 1349-4198, [Online; navštívené 19.02.2017].
URL http://www.ijicic.org/ijicic-10-12106.pdf

[11] Golshan, F.; Mohammadi, K.: *SVD-based digital image watermarking using adaptive generated watermark. The Imaging Science Journal*, ročník 62, č. 1, 2014: s. 3–10, ISSN 13682199, doi:10.1179/1743131X12Y.0000000021, [Online; navštívené 19.02.2017].
URL http://www.tandfonline.com/doi/full/10.1179/1743131X12Y.0000000021

[12] Hamghalam, M.; Mirzakuchaki, S.; Akhaee, M. A.: *Vertex angle image watermarking with optimal detector. Multimedia Tools and Applications*, ročník 74, č. 9, 2015: s. 3077–3098, ISSN 13807501, doi:10.1007/s11042-013-1769-1, [Online; navštívené 19.02.2017].
URL http://link.springer.com/10.1007/s11042-013-1769-1

[13] Hsieh, S.-L.; Chen, C.-C.; Shen, W.-S.: *Combining Digital Watermarking and Fingerprinting Techniques to Identify Copyrights for Color Images. The Scientific World Journal*, ročník 2014, č. 454867, 2014: s. 1–14, ISSN 23566140, doi:10.1155/2014/454867, [Online; navštívené 19.02.2017].
URL http://www.hindawi.com/journals/tswj/2014/454867/

[14] Katzenbeisser, S.; Petitcolas, F. A. P.: *Information hiding techniques for steganography and digital watermarking*. Artech House, 2000, ISBN 1-58053-035-4.

[15] Lee, M.-L.; Ting, P.-Y.; Wu, T.-S.: *Photograph watermarking. Multimedia Tools and Applications*, ročník 75, č. 23, 2016: str. 16173–16189, ISSN 13807501, doi:10.1007/s11042-015-2925-6, [Online; navštívené 19.02.2017].
URL http://link.springer.com/10.1007/s11042-015-2925-6

[16] Lu, J.; Zou, Y.; Yang, C.; aj.: *A Robust Fractal Color Image Watermarking Algorithm. Mathematical Problems in Engineering*, ročník 2014, č. 638174, 2014: s. 1–12, ISSN 1024123x, doi:10.1155/2014/638174, [Online; navštívené 19.02.2017].
URL http://www.hindawi.com/journals/mpe/2014/638174/

[17] Naderahmadian, Y.; Hosseini-Khayat, S.: *Fast and robust watermarking in still images based on QR decomposition. Multimedia Tools and Applications*, ročník 72, č. 3, 2014: s. 2597–2618, ISSN 1380-7501, doi:10.1007/s11042-013-1559-9, [Online; navštívené 24.01.2017].
URL http://link.springer.com/10.1007/s11042-013-1559-9

[18] Swati, S.; Hayat, K.; Shahid, Z.; aj.: *A Watermarking Scheme for High Efficiency Video Coding (HEVC). PLoS ONE*, ročník 9, č. 8, 2014: s. 1–8, doi:10.1371/journal.pone.0105613, [Online; navštívené 19.02.2017].
URL https://doi.org/10.1371/journal.pone.0105613

[19] Thabit, R.; Khoo, B. E.: *Capacity improved robust lossless image watermarking. IET Image Processing*, ročník 8, č. 11, 2014: s. 662–670, ISSN 17519659, doi:10.1049/iet-ipr.2013.0862, [Online; navštívené 19.02.2017].
URL http://digital-library.theiet.org/content/journals/10.1049/iet-ipr.2013.0862

[20] Tsougenis, E. D.; Papakostas, G. A.; Koulouriotis, D. E.: *Image watermarking via separable moments. Multimedia Tools and Applications*, ročník 74, č. 11, 2015: s. 3985–4012, ISSN 13807501, doi:10.1007/s11042-013-1808-y, [Online; navštívené 19.02.2017].
URL http://link.springer.com/10.1007/s11042-013-1808-y

[21] Wang, F.; Xie, Z.; Chen, Z.: *High Capacity Reversible Watermarking for Audio by Histogram Shifting and Predicted Error Expansion. The Scientific World Journal*, ročník 2014, č. 656251, 2014: s. 1–7, ISSN 23566140, doi:10.1155/2014/656251.
URL http://www.hindawi.com/journals/tswj/2014/656251/

[22] Zamani, M.; Manaf, A. B. A.: *Genetic algorithm for fragile audio watermarking. Telecommunication Systems*, ročník 59, č. 3, 2015: s. 291–304, ISSN 10184864, doi:10.1007/s11235-014-9936-x, [Online; navštívené 19.02.2017].
URL http://link.springer.com/10.1007/s11235-014-9936-x

Príloha A

Obsah priloženého CD

Adresárová štruktúra CD:

- `src` - Zdrojové súbory
  - `img` - Testovací obrázok `lena.jpg` a testovací vodoznak `fit.pbm`
  - `attacks` - Obrázky po prevedení útokov a extrahované vodoznaky
- `text` - Text práce vo formáte pdf a zdrojové texty pre LaTeX

Príloha B

Návod na inštaláciu

Program pri svojej činnosti využíva knižnicu ImageMagick vo verzii 7.0.5-4. Aktuálnu verziu tejto knižnice si môžete stiahnuť na webovej stránke www.imagemagick.org v sekcii download[1].

Nainštalovanú verziu knižnice ImageMagick zistíte príkazom:

```
identify -version
```

Pred kompiláciou programu bude možno potrebné nastaviť premennú prostredia `PKG_CONFIG_PATH` príkazom

```
export PKG_CONFIG_PATH=/usr/local/lib/pkgconfig
```

Následne je možné skompilovať program pomocou príkazu `make`, ktorý vytvorí spustiteľný program s názvom `watermarking` a priečinok `attacks` do ktorého budú uložené obrázky po prevedení útokov pomocou prepínača `--attack`. Príklad spustenia programu

```
./watermarking --input lena.jpg --wm-input fit.pbm
```

[1] ImageMagick https://www.imagemagick.org/script/download.php