ČESKÁ ZEMĚDĚLSKÁ UNIVERZITA V PRAZE

PROVOZNĚ EKONOMICKÁ FAKULTA

Katedra informačních technologií

Ochrana veřejně přístupných grafických dat

Disertační práce

Autor: Ing. Simona Pejsarová

Školitel: Doc. Ing. Zdeněk Havlíček, CSc.

Praha 2011

Poděkování

Ráda bych touto cestou poděkovala všem, kteří mi při zpracování této disertační práce ochotně pomáhali.

Zvláště děkuji svému školiteli, Doc. Ing. Zdeňkovi Havlíčkovi, CSc., za odbornou pomoc, ochotu a cenné připomínky k obsahu práce. Dále děkuji Doc. PhDr. Ivaně Švarcové, CSc., Ing. Markovi Čandíkovi, Ph.D. a všem kolegům z katedry informačních technologií PEF ČZU za poskytnuté rady a připomínky.

Mé poděkování patří také mým rodičům a blízkým za neutuchající podporu, jazykové a stylistické korektury.

Ochrana veřejně přístupných grafických dat

Protection of publicly available graphical data

Abstrakt

Disertační práce se zabývá problematikou zabezpečení veřejně přístupných grafických dat. Uvádí možnosti zabezpečení těchto dat metodami utajené komunikace a technikami digitálního vodotisku. V rámci práce je věnována pozornost také dílčím vazbám na legislativu, problematiku barev, jejich vnímání lidským okem a grafickým formátům.

Na těchto uvedených teoretických základech a řadě testování práce navrhuje konkrétní implementaci obecného steganografického algoritmu a metodický postup jeho efektivního využití pro zabezpečení veřejně přístupných obrazových dat a vyšší ochranu autorských práv. Následně je demonstrována aplikace metodiky na konkrétních příkladech, porovnány získané výsledky s obdobnými postupy a uvedeny závěry a doporučení pro užití metodiky v konkrétních oblastech.

Klíčová slova: Steganografie, digitální vodotisk, vodoznak, zabezpečení, veřejně přístupná data, autorský zákon, problematika barev, fyziologie lidského oka, obrazový formát, vkládání a extrakce vodoznaku, bezpečnost, nevnímatelnost, robustnost, statistická nedetekovatelnost, spolehlivá detekce, přidružený klíč.

Abstract

The dissertation thesis aims the security of publicly available graphical data. Shows possibilities of data securing using methods of secret communication and digital watermarking. The thesis focuses also on legislation relative to its field, color theory, color perception of the human eye and graphical formats.

Based on the theoretical basis and a number of tests, the paper proposes a specific implementation of general steganographic algorithm and methodology of its effective usage to ensure security of publicly available graphical data and protection of copyright holder rights. Subsequently, application of methodology is demonstrated on particular examples, comparing the results obtained with similar procedures and provided conclusions and recommendations to use the methodology in specific areas.

Keywords: Steganography, digital watermarking, watermark, security, publicly available data, the Copyright Act, color theory, physiology of the human eye, image formats, insertion and extraction of the watermark, security, imperceptibility, robustness, statistical non-detectability, reliable detection, associated key.

Obsah

1 Úvod

Obrovský rozvoj informačních a komunikačních technologií v posledních letech mění současnou společnost na společnost informační. Pro řídící pracovníky platí, kdo z nich nejrychleji získá správné informace, ten se může včas a správně rozhodnout. Tedy rychlejší a přesnější informace přinesou konkurenční výhodu a v konečném důsledku pravděpodobně i větší zisky.

Informace jsou potřebné nejen pro vrcholový management, ale také pro pracovníky nižších útvarů podniku a všechny ostatní, kteří o ně projeví zájem. Po celém světě se v různých zájmových sférách organizují konference, semináře, sympozia, výstavy, veletrhy, zasedání a přednášky, na kterých lidé získávají množství potřebných informací.

Pro šíření informací hraje však také stále důležitější úlohu internet, jenž představuje v současnosti největší informační dálnici. Jeho prostřednictvím mohou různé instituce, jednotlivci, firmy a společnosti nejrůznějšího zaměření publikovat, informovat a v neposlední řadě i obchodovat.

Relativně snadné získávání informací prostřednictvím nejrůznějších prezentací ať již on-line či off-line s sebou přináší i stinné stránky. Čím dál častěji se v souvislosti s distribucí veřejně přístupných informací, především na internetu, hovoří o problematice zabezpečení grafických dat. Týká se především nelegálního šíření, kopírování a úprav takovýchto dat, které jsou vlastnictvím někoho jiného. Vzniká tak problém porušování autorských práv.

Jak je tedy vůbec možné zabezpečit informace, v tomto případě především grafická data, které jsou záměrně poskytovány široké veřejnosti? Tuto otázku mohou částečně řešit metody utajené komunikace neboli steganografie a metody zabezpečení digitálních dat technikami digitálního vodotisku.

Z výše uvedených důvodů se tato práce bude zabývat ochranou autorských práv metodami utajené komunikace a digitálního vodotisku. Bude uvedeno jak právo autorské, tak trestní, dále pak základní vlastnosti optického systému lidského oka a barevného vidění, které na první pohled neposkytují přímou vazbu na danou problematiku, ale přesto jsou pro tuto práci velmi důležité. Práce se bude zabývat dále také grafickým modelem RGB, vlastnostmi barev, grafickými formáty a další problematikou s prací ať již přímo či nepřímo související.

V konečném důsledku a na základě řady zkoumání se práce pokusí navrhnout efektivní metodiku zabezpečení veřejně přístupných grafických dat tak, aby byla v co největší míře zachována statistická nedetekovatelnost, vizuální nepostřehnutelnost a maximální odolnost proti možným útokům.

2 Cíl disertační práce

Předkládaná disertační práce se zaměřuje především na problematiku zabezpečení veřejně přístupných grafických dat.

Veřejně distribuovaná grafická data nemají parametry chráněné komunikace a jejich zabezpečení je tím daleko složitější. Navíc dynamický rozvoj informačních a komunikačních technologií, masové využívání internetu, stále více rostoucí obliba sociálních síti, digitalizace v komerční a nekomerční sféře tento problém ještě více prohlubují.

Společnosti, firmy, různé organizace či jednotlivci využívají grafická data pro nejrůznější veřejné prezentace. Zřídka však tyto subjekty uvažují o možném odcizení takových to veřejně prezentovaných dat a o možných následných negativních důsledcích.

Hlavním cílem práce je nalézt, navrhnout a detailně popsat takový způsob zabezpečení veřejně přístupných grafických dat, který zajistí vyšší ochranu autorských práv a současně bude minimalizovat negativní důsledky při případném odcizení těchto dat. Navržený způsob (metodiku) bude možné implementovat jak v rámci různorodých podnikových systémů, tak samostatně.

Dílčí cíle předkládané disertační práce jsou seskupeny do tří logických celků:

1) Teoretická východiska související s problematikou práce

- Analyzovat teoretické zdroje zabývající se problematikou zabezpečení grafických dat metodami utajené komunikace a digitálního vodotisku,
- prozkoumat možnosti zabezpečení grafických dat metodami utajené komunikace a digitálního vodotisku,
- charakterizovat kritéria na steganografické systémy, vodoznaky a metody vkládání vodoznaků,
- specifikovat dílčí oblasti související s problematikou práce.

2) Návrh metodiky EZOD (Efektivní Zabezpečení Obrazových Dat)

- Navrhnout konkrétní implementaci obecného steganografického algoritmu s cílem zvýšení robustnosti při zachování maximální statistické nedetekovatelnosti a vizuální nepostřehnutelnosti,
- analyzovat vlastnosti imperceptibility (nevnímatelnosti) při vložení vodoznaku do různých bitových rovin,
- zajistit testování odolnosti konkrétní implementace algoritmu proti možným útokům,
- syntetizovat teoretické a praktické poznatky a navrhnout metodická doporučení a optimální postup pro zabezpečení grafických dat.

3) Praktická aplikace metodiky EZOD

- Demonstrovat praktické možnosti ochrany grafických dat na konkrétních příkladech,
- porovnat navržené řešení s obdobnými postupy,
- poukázat na konkrétní oblasti vhodné pro aplikaci navržené metodiky.

3 Metodika

Ke splnění cílů doktorské práce budou analyticko-syntetickými metodami analyzovány literární zdroje, které lze rozdělit do následujících čtyř skupin:

- Kmenová literatura daného oboru a související vědecké články,
- základní dokumenty standardizačních organizací,
- firemní literatura a dokumentace,
- podložené zdroje různých diskusních fór a příspěvků.

Získané poznatky budou následně formulovány do celkového přehledu. Při zpracování rešeršní části práce bude zvolen postup směřující od obecného ke konkrétnímu. Tento postup by měl poskytnou výchozí rámec práce, který bude postupně konkretizován až na základní techniky zabezpečení grafických dat.

V praktické části práce bude navržena konkrétní implementace obecného steganografického algoritmu a prováděna četná zkoumání pro dosažení optimálních vlastností tohoto algoritmu včetně metodiky jeho efektivní využití.

Bude prováděna analýza imperceptiblity vloženého vodoznaku v různých bitových rovinách. K analýze vlastnosti imperceptibility budou použity následující subjektivní a objektivní metody.

Objektivní metody

Pro objektivní analýzu kvality digitálních obrazů budou zvoleny následující uvedená kritéria:

- Střední kvadratická chyba (MSE – *Mean Square Error*),
- Střední absolutní chyba (MAE – *Mean Absolute Error*),
- Odstup signálu od šumu (SNR – *Signal to Noise Ratio*),
- Vrcholový odstup signálu od šumu (PSNR – *Peak Signal to Noise Ratio*).

Subjektivní metody

Subjektivní kritéria je možné popsat dvojím způsobem:

- Kvantitativně,
- Kvalitativně.

V praktické části bude dále prováděny pokusy zvýšení robustnosti vkládané informace při zachování maximální statistické nedetekovatelnosti a vizuální nepostřehnutelnosti. Taktéž budou prováděna testování odolnosti algoritmu proti různým typům útoků.

Dle výsledků analýz imperceptibility, odolnosti algoritmu a dalších zkoumání bude navržena efektivní metodika zabezpečení veřejně přístupných grafických dat.

Praktická aplikace metodiky bude demonstrována na konkrétních příkladech a porovnána s obdobnými postupy. Následně bude poukázáno na konkrétní oblasti jejího vhodného využití a formulovány syntetické závěry a praktická doporučení.

4 Oblast zkoumání

„Co chceme, tomu také ochotně věříme, a doufáme,
že si i ostatní myslí, co si myslíme sami.“
Gaius Julius Ceasar

Účelem této kapitoly je analýza současného stavu problematiky zabezpečení veřejně přístupných dat z různých hledisek. Nejdříve bude uvedena problematika zabezpečení a ochrany dat v níž bude specifikována oblast steganografie a digitálního vodotisku.

Pro získání uceleného pohledu na problematiku budou zde dále uvedeny dílčí oblasti, které se zkoumanou problematikou nepřímo souvisí. Bude uveden současný stav z hlediska legislativy, strategie EU, z hlediska problematiky barev a barevného vidění, barevných formátů z nichž bude specifikován pouze nejužívanější.

V závěrečné části této kapitoly bude uveden praktický příklad, který jasně demonstruje porušování autorských práv a nedostatečné zabezpečení obrazových dat s kterým se v současné době setkáváme v podstatě na každém kroku.

4.1 Bezpečnost a ochrana dat

Bezpečnost (anglicky security) představuje vlastnost prvku (např. informačního systému), který je na určité úrovni chráněný proti ztrátám, resp. představuje stav ochrany (na určité úrovni) proti ztrátám. Bezpečnost informačních technologií zahrnuje ochranu činností zpracování, úschovy, distribuce a prezentace informací. Tato kapitola čerpá především z literatury [24].

Současnou dobu lze charakterizovat jako dobu informací v různých podobách, ať již jde o počítačová data, audio statické obrazy nebo video. Tyto informace v našem případě prezentace se šíří prostřednictvím telekomunikačních sítí, přičemž se používají různá přenosová média. Velký stimul v tomto rozvoji poskytl internet. Rozsáhlá distribuce internetových dat podnítila rozvoj nových přenosových technologií a služeb. Stále se zdokonalují hardwarové a softwarové prostředky ulehčující člověku práci. Na druhé straně však umožňují též nelegální šíření a zacházení s informacemi, které jsou vlastnictvím někoho jiného.

V této souvislosti se dostává do popředí problematika bezpečnosti a ochrany dat. V případě digitálních prezentacích je tato problematika ztížena zejména díky základní funkci prezentací tj. prezentovat výrobky, jednotlivce, firmy, společnosti a další subjekty. Tyto prezentace probíhají veřejně a jsou k dispozici ať již ve formě nějakého média (CD, DVD) či přímo na internetu.

Zde tedy vzniká problém, jak tyto veřejně přístupné prezentace ochránit. Ve většině případů nejde o zabezpečení samotného textu, ale především o grafická data, která mohou být zneužita např. znovu použita jiným subjektem bez souhlasu majitele a kde po jejich úpravě nelze jednoznačně prokázat skutečného vlastníka. V těchto případech jde tedy o zabezpečení dat z hlediska jejich autorství.

Cílem této kapitoly je poskytnutí některých pohledů a možností v oblasti zabezpečení digitálních dat. Tato kapitola se bude věnovat zejména metodám utajené

komunikace (tj. steganografie) a metodám zabezpečení dat technikami digitálního vodotisku.

Je nutné si uvědomit, jaké subjekty obecně přicházejí do styku s daty. Lze je rozdělit do tří skupin:

- **Autor** (vlastník autorských práv) – osoba nebo organizace, která vlastní originál dat.
- **Uživatel** – osoba nebo organizace, která vlastní data a má od autora dočasné či trvalé právo tyto data používat.
- **Útočník** – osoba, která nevlastní data, resp. nemá od autora dočasné či trvalé právo tyto data používat a snaží se data získat, upravit, nebo prezentovat tak, aby buď nesloužily svému účelu, nebo aby byly interpretovány jako data s dočasným nebo trvalým právem je používat[23].

4.1.1 Obecný popis digitálních obrazů

Předpokládáme-li, že originální obraz, do kterého chceme vložit vodoznak, bude statický víceúrovňový (šedý) obraz *I*. Statické obrazy se charakterizují prostorovým a jasovým rozlišením, resp. prostorovou a jasovou rozlišovací schopností. Tato podkapitola čerpá z literatury [3].

Prostorová rozlišovací schopnost (prostorové rozlišení) se popisuje počtem obrazových prvků (op) reprezentujících obraz v horizontálním a vertikálním směru připadajících na jednotku délky (např. palec = 25.4 mm). Nutno poznamenat, že pro označení obrazového prvku se užívá akronymu pixel z anglického picture element. [7]

Prostorová rozlišovací schopnost obrazu je charakterizována:

- horizontální rozlišovací schopností,
- vertikální rozlišovací schopností.

Horizontální rozlišovací schopnost se udává počtem obrazových prvků na jednotku délky (palec) a tato jednotka se označuje jako dpi (dots per inch).

Vertikální rozlišovací schopnost se udává počtem řádků na jednotku délky (např. na 1 mm), nebo se udává v dpi.

Prostorová rozlišovací schopnost víceúrovňových statických obrazů je nejčastěji dána jako rozměr matice $m \times n$, kde m je počet řádků resp. obrazových prvků ve vertikálním směru a n je počet obrazových prvků v horizontálním směru. Standardně používaná prostorová rozlišovací schopnost bývá 256×256 resp. 512×512, ale používají se také obrazy s jinou rozlišovací schopností.

Jasová rozlišovací schopnost (jasové rozlišení) víceúrovňových statických obrazů vyjadřuje počet bitů potřebných k popsání obrazové informace v jasových složkách každého obrazového prvku. Obecně je jasová rozlišovací schopnost p bitů/op, kde

$p > 1$, přičemž počet jasových úrovní je 2^p. Standardní víceúrovňové obrazy mají jasovou rozlišovací schopnost 8 bit/op, t.j. počet jasových úrovní je $2^8 = 256$. Je-li počet bitů $p = 1$, jedná se o tzv. binární obrazy s počtem jasových úrovní $2^1 = 2$ (černá, bílá). Speciálním případem binárních obrazů jsou tzv. pseudovíceúrovňové obrazy imitující víceúrovňové (šedé) obrazy technikou označovanou jako halftoning (šedá barva je

vhodně konvertována černými a bílými obrazovými prvky, odstín šedé barvy je dán „koncentraci“ bílých a „koncentraci“ černých obrazových prvků v dané oblasti obrazu).

4.1.2 Techniky ukrývání digitálních dat a steganografie

Pojem digitální označuje informace, vytvořené pomocí číselného zpracování (obvykle v binární formě jedniček a nul), nebo technologie založené na obdobném principu.

Ukrývání digitálních dat je umění a věda týkající se návrhu takových metod komunikace, které kromě zabezpečení důvěrnosti přenášených dat ukryjí také fakt, že jsme se důvěrnost něčeho snažili zabezpečit, případně ukryjí samotnou komunikaci[6].

Problematikou ukrývání informací se zabývají následující oblasti:

- **Kryptografie** (cryptography) – zabývá se studiem matematických postupů, jež se týkají těch aspektů informační bezpečnosti, k nimž patří utajení, integrita dat, autentizace subjektu a autentizace původu dat. Na ochranu obsahu digitálních dat používá **šifrování**, tj. transformaci informace do podoby, která je nesrozumitelná (čitelná jen se speciální znalostí), ale z které je možné získat původní formu použitím inverzní transformace – dešifrováním. Přičemž příslušnou dešifrovací transformaci (dešifrovací klíč) musí poznat pouze osoby, které mají mít možnost zprávě rozumět.

- **Steganografie** (steganography) – je to starší sestra kryptografie (šifrování). zabývá se metodami utajení komunikace, tj. realizuje skrytý přenos informace vložením dat do jiných dat tak, aby modifikace původních dat byla smyslově nepostřehnutelná. Na rozdíl od kryptografie, steganografie tímto smyslově nevnímatelným vložením dat utají informaci o jejich přenosu. Kryptografie umožňuje utajení obsahu správy, ale neutajuje komunikaci. Rozlišují se technické a jazykovědné steganografické techniky. Mezi nejfrekventovanější technické steganografické techniky patří vytváření mikrobodů pod nebo nad krycí text. V současné době je tento steganografický přístup zesílený používáním neviditelných inkoustů. Jazykovědné steganografické techniky využívají jazyk (řeč). Jako příklad je možné uvést používání akrostichu, tj. používání takové formulace textových zpráv, kde první nebo poslední znaky slov vytvářejí slova nebo věty. Jiným příkladem je používání chyb nebo stylistických znaků na definování pozic zprávy v textu.

- **Technika označování autorských práv** (copyright marking) – představuje techniky digitálního vodotisku. Digitální vodotisk vkládá přídavnou informaci (digitální vodoznak) do dat tak, aby modifikace těchto dat byla smyslově nepostřehnutelná. Rozlišuje se *křehký vodotisk* (fragile watermarking) a *robustní vodotisk* (robust watermarking).[14] Techniky křehkého vodotisku modifikují vodoznak při jakékoli operaci s daty, v kterých je vodoznak vložený. Jejich hlavní úlohou je detekce manipulace s daty. Techniky robustního vodotisku se používají na detekci autorských práv, vložený vodoznak musí odolávat manipulaci s daty. Speciálním případem robustních vodotiskových technik je technika identifikačních vodoznaků (fingerprinting), jejíž účelem je umožnění sledování distribuce nelegálních kopií dat. Protože vodotiskové techniky splňují požadavek smyslové nevnímatelnosti vložených vodoznaků, bývají studovány také jako techniky možného utajení komunikačního přenosu a bývají přiřazovány ke steganografickým technikám.

- **Technika krycích kanálů** (covert channels) – využívá při přenosu informací komunikační cesty, které nebyly při přenosu informací navrhované, ani nebyly pro přenos informací plánované. Tato technika je používaná některými softwarovými produkty, jež navenek vykonávají jinou funkci, ale zároveň poskytují přenos skrytých informací. Technika krycích kanálů bývá přiřazována ke steganografickým technikám.

- **Anonymita** (anonymity) – jde o techniku ukrývání identity odesílatelů a adresátů zpráv, přičemž sama informace není mezi uživateli utajovaná. Mezi přístupy této techniky patří posílání zprávy přes několik anonymních osob s jejím následným několikanásobným přesměrováním. Základní myšlenkou bylo ukrýt cestu přenosu zprávy použitím většího počtu anonymních osob a ty přijatou zprávu poslaly další osobě a tak se postupně dostala až k adresátovi. Předpokladem použití byla zejména důvěra a spolehlivost jednotlivých anonymních osob.[19]

Steganografie a technika vodoznaků spolu vzájemně velmi úzce souvisí. Obě techniky popisují způsoby subjektivně nevnímatelného přenosu informací pomocí jejich vložení do krycích dat. Zatímco steganografie se používá především pro komunikaci mezi dvěma skupinami (osobami), technika vodoznaků předpokládá využití způsobem „jeden odesílatel – neomezené množství příjemců“.

Rozdíl mezi steganografií a technikou vodoznaků spočívá v požadavcích na jejich odolnost vůči útokům. Cílem steganografie je ukrytí skutečnosti, že tajná komunikace existuje, proto se na ni nekladou vysoké nároky na odolnost. Technika vodoznaků předpokládá velké množství příjemců, a mezi nimi i takových, kteří se budou snažit vloženou informaci odstranit a nebo poškodit. Proto robustní techniky vodoznaků kladou vyšší požadavky na odolnost vůči útokům nepovolaných osob.

Je třeba poznamenat, že robustní vodoznakové techniky je možné využívat i jako steganografické techniky.

4.1.2.1 Rozdělení steganografických technik

Podle používaných metod v digitální steganografii je možné rozdělit steganografické techniky do třech odlišných skupin[41]:

- **Injekční steganografie** (injection steganography) – využívají vložení dat do jiných dat, tzn. krycích dat jimiž jsou krycí text, krycí obraz, krycí zvuk a nebo krycí programový soubor. Vložení dat do krycích dat způsobí zvětšení velikosti souboru krycích dat, proto musí být data vložené tak, aby na straně příjmu byly klientskými programy nebo prezentačními algoritmy (prohledávače obrázků, audioprohledávače, textové editory) ignorované. Mnohé aplikace injekční steganografii umožňují. Data vložené do krycích dat bývají v steganografii označované jako stegotext data, stegobraz data, stegoaudio data nebo všeobecně stegoobjekt data.

- **Substituční steganografie** (substitution steganography) – využívá nahrazení nevýznamných částí krycích dat, nahrazení ale nesmí způsobit u klientských programů kolizi (např. při kontrole součtu atd.). Pro substituci se používají také části krycích dat, které bývají málokdy použité nebo se vůbec nepoužívají, ale jsou součástí krycích dat. Substituční steganografické přístupy způsobují mírné

zkreslení (degradaci) krycích obrazových dat (statických obrazů nebo videosekvencí), šum u krycích audiosigálů, procesní chyby nebo nestandardní, netypické stavy u krycích programových souborů.

- **Propagační steganografie** (propagation steganography) – nejčastěji využívá prostředky generující jiná data, které slouží jako krycí data. Vložená data jsou potom součástí těchto dat.

Přirozené techniky ukrývání dat jsou variabilní v závislosti na použití krycího média, do kterého jsou vkládané. V zásadě rozlišujeme[25]:

- **Ukrývání dat v textu –** textová data se v porovnání se zvukovými či obrazovými daty vyznačují nižší redundantní informací. Proto se tyto techniky soustřeďují na využití takových přístupů, které jsou pro čtenáře zpráv nepostřehnutelné. Můžeme rozlišovat tři skupiny metod:
  - *Metody využívající prázdná místa v textu, v dokumentu* (open space metods), jež vkládají zprávu do textového dokumentu manipulací „bílých" míst v textu (např. mezery mezi znaky, mezi slovy, pozice počátečního nebo koncového znaku v řádku) a nepoužitého prostoru na stránce. Nejjednodušší je používání mezery mezi jednotlivými slovy v textu – vložení binární zprávy v textu bude realizované jednou mezerou mezi slovy pro hodnotu „0", nebo dvěma mezerami mezi slovy pro hodnotu „1".

    Mezi metody využívající prázdná místa v textu, v dokumentu můžeme zařadit následující:
    - posouvání řádků textu,
    - posouvání slov,
    - úprava písmen.
  - *Syntaktické metody* (syntactic methods) – tyto metody využívají interpunkci.
  - *Sémantické metody* (semantic methods) – využívají pro vložení zprávy vzájemnou manipulaci jednotlivých slov tj. změnu textu bez změny významu nebo používání definovaných synonym v textu atp.

- **Ukrývání dat v obrazových signálech** – steganografické techniky digitálních obrazů umožňují uskutečňování skrytých komunikačních přenosů digitálních obrazů. Tyto metody úzce korespondují s technikou digitálních vodoznaků, a proto bývá obrazová zpráva, steganograficky přenášená nazývána vodoznak. Nejčastějším případem bývá použití binárního vodoznaku, tj. černobílého obrazu se dvěma jasovými úrovněmi – černý obrazový bod „0", bílý obrazový bod „1". Příkladem tohoto typu obrazu mohou být např. skenované textové informace. Nejfrekventovanějším médiem pro ukrytí vodoznaku bývají digitální obrazy – statické šedé, tzv. víceúrovňové obrazy, statické barevné obrazy, příp. obrazové sekvence.

Základní (technické) steganografické techniky digitálních obrazů jsou založené na několika odlišných principech umožňujících vložení vodoznaku do obrazového média. Jsou to:

- *Rozklad obrazu na bitové roviny* – ukrytí dat v obrazové informaci přestavuje v podstatě modifikaci některých binárních hodnot vybrané

bitové roviny originálního obrazu v závislosti na binární hodnotě dat vkládaných do obrazu. Nejčastější je použití nejméně významných bitů pro toto vložení.

- *Metody digitálního halftoningu* – ukrytí dat se realizuje modifikací struktury aproximovaného šedého odstínu v pseudovíceúrovňových obrazech.
- *Subpásmový rozklad obrazů* – jestliže jsou krycí obrazová data frekvenčně rozdělená na určitá pásma a binárními hodnotami vkládaných dat se modifikují některé spektrální části obrazů.
- *Metody digitálního vodotisku obrazů* – realizuje vložení binární informace, nejčastěji ve formě binárního obrazu do krycích dat, jimiž jsou statické obrazy nebo obrazové sekvence.
  Vložení vodoznaku se uskutečňuje:
  - V obrazové oblasti tj. vložení dat (vodoznaku) se přímo modifikují jasové hodnoty krycího obrazu
  - Ve frekvenční oblasti, tj. vložením dat (vodoznaku) se modifikují spektrální koeficienty obrazu
  - V parametrické oblasti, tj. vložení dat (vodoznaku) se realizuje v procesu konverze do jiného obrazového formátu změnou některých jeho parametrů, resp. metadat.

- **Ukrývání dat v audiosignálech** – tyto metody jsou založené na vlastnostech lidského zvukového systému. V digitální reprezentaci zvukových dat hrají významnou úlohu dva parametry, a to vzorkování a kvantování. Vzorkovací frekvence bývá v rozmezí 8 kHz až 44,1 kHz, používaná kvantizace bývá lineární 16ti bitová nebo logaritmická 8 bitová. Mezi základní techniky ukrývání dat v audiosignálech patří:
  - **Modifikace nejméně významných bitů** – využívá se výlučně v digitálním přenosovém prostředí, kdy se modifikují nejméně významné bity digitálně reprezentovaného audiosignálu. Tato modifikace vnáší do signálu akustický šum a je choulostivá na další zpracování signálu. Na druhé straně ale umožňuje vložení velkého množství dat. Vzorková frekvence je 1 kHz.
  - **Fázové kódování** – patří mezi velmi efektivní metody ukrývání dat do audiosignálů. Data jsou kódována substitucí fáze segmentu audio signálu pomocí referenční fáze, která reprezentuje ukrývaná data. Tento postup vnáší do audiosignálu fázovou disperzi a nespojitosti fázového příběhu závislé na každém frekvenčním segmentu. Minimalizace fázové disperze je závislá na použité přenosové rychlosti.
  - **Rozprostřené spektrum** – princip této techniky spočívá v kódování toku informací rozšířením jejich frekvenčního spektra na co možná největší šířku. Tato technika je využívaná při nízkých bitových rychlostech signálu.
  - **Ukrývání datové odezvy** – tato technika realizuje ukrytí dat do audiosignálů zavedením odezvy signálu. Odezva signálu je definovaná třemi parametry – počáteční amplituda, opoždění a rychlost tlumení. Odezvy charakterizované velmi nízkou úrovní zpoždění (méně než 1 m/s), jsou lidským zvukovým vnímáním nepostřehnutelné. Data na ukrytí v jejich binární formě je možné ukrýt do audiosignálů zavedením dvou odlišných odezev, odpovídajících binární „0“, resp. „1“. Hodnota

počáteční amplitudy a rychlosti tlumení musí být dopředu nastavená tak, aby byla pod prahovou úrovní vnímání.

- **Ukrývání dat ve spustitelných souborech** – jde o modifikaci spustitelných souborů na základě vkládaných dat. Ukrývání dat ve spustitelných souborech do jisté míry koresponduje s principem počítačových virů. Z tohoto pohledu je možné algoritmy ukrývání dat ve spustitelných souborech rozdělit na dvě kategorie[39]:
  - **Rozšiřující techniky** – tyto techniky ponechají spustitelný soubor v původním stavu a přidanou informaci vkládají do metadat souboru. Jejich nevýhodou je zvětšení velikosti, rozšíření spustitelného souboru, který ulehčuje jejich detekci (injekční steganografie).
  - **Modifikující techniky** – tyto techniky vkládají informaci přímo do spustitelného souboru (substituční steganografie). Jejich nevýhodou je možné poškození funkčnosti souboru.

Při vkládání vodotisku do spustitelných souborů se rozlišuje tzv.:

- Statický vodotisk (static watermark) – program jehož extrakci není třeba spouštět ani simulovat. Statický vodotisk je však lehko atakovatelný transformacemi zachovávajícími sémantiku programu. Při statickém vodotisku mohou být vkládané informace vložené do:
  - Segmentu inicializovaných dat (kde jsou uložené statické řetězce)
  - Kódového segmentu (vykonávatelný kód)
  - Ladících informací
- Dynamický vodotisk (dynamic watermark) – vodotisk je stav během vykonávání programu. Při dynamickém vodotisku aplikace běží na předurčeném vstupu, jež aplikaci přinutí, aby se dostala do pro tento vstup dopředu zvoleného stavu, který reprezentuje vodotisk. Metody se liší podle toho, v které části stavu programu je vodotisk uložen a podle způsobu, jakým je z něho extrahován. Rozlišují se tři techniky dynamického vodotisku – vodotisk se skrytou funkčností, vodotisk v datových strukturách a vodotisk v postupnosti vykonávání.[42]

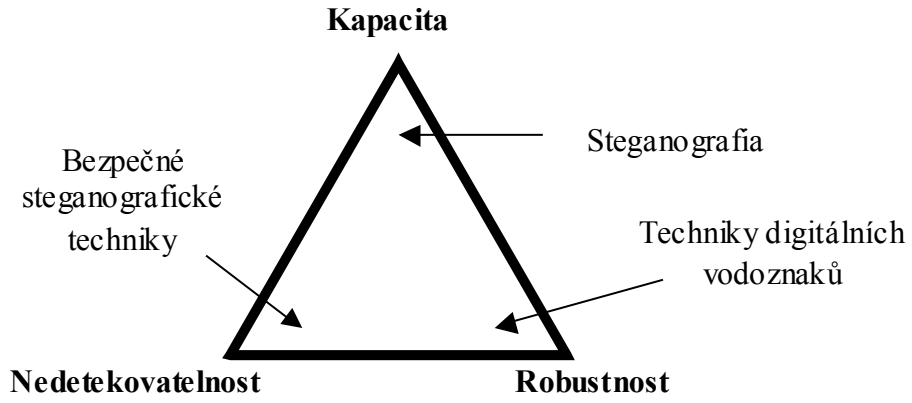
4.1.2.2 Kritéria na steganografické systémy

Pro systémy utajení komunikace, tj. pro steganografické systémy jsou typické následující **hlavní požadavky[7]**:

- **Robustnost** – vložená informace se nazývá robustní, pokud je lehce detekovatelná z krycích dat, do nichž byla vložena a které byly následně poškozené útoky. Robustnost znamená odolnost – imunitu vůči necíleným všeobecným operacím s daty.
- **Statistická nedetekovatelnost** – je typickým požadavkem na bezpečnou tajnou komunikaci. Hovoříme, že vložená informace je nedetekovatelná, pokud její vložení nevyvolá statisticky významnou změnu, kterou by se označená data lišila od originálních dat. Je potřebné poznamenat, že schopnost detekovat vložené informace ještě neznamená schopnost její extrakce.
  Statistickou nedetekovatelnost lze ověřovat prostřednictvím histogramu originálního a označeného obrazu. Histogramy těchto obrazů by neměly vykazovat výrazné změny.[8]

- **Nevnímatelnost** – tento požadavek je založen na vlastnostech lidského vizuálního systému nebo lidského sluchového systému. Vložená informace je nevnímatelná, pokud průměrný člověk není schopný rozlišit originální data od dat obsahujících skrytou informaci. Nevnímatelnost se zkoumá na velkém vzorku dat, v němž buď je nebo není vložená informace, a to tak, že určité množství lidí porovnává tyto vzorky. Jako úspěšná hodnota neviditelnosti se považuje ta, pokud 50% zúčastněných lidí nedokáže odlišit označené vzorky od originálních.
- **Bezpečnost** – o bezpečném algoritmu se hovoří tehdy, pokud vložená informace nemůže být extrahovaná z označených dat bez znalosti algoritmu vkládání a extrakce. Pojem bezpečnost též zahrnuje útoky založené na poznání části procesu vkládání tajné informace.

Výše uvedené požadavky jsou navzájem konfliktní. To znamená, že není možné současně splnit všechny najednou. Pokud chceme dosáhnout vložení velkého množství informací, nemůžeme současně požadovat vysokou odolnost vložených dat nebo jejich nedetekovatelnost. Na druhé straně, pokud chceme dosáhnout vysoké odolnosti, neubráníme se snížení kvality označených dat nebo jejich jednodušší detekovatelnosti. Na následujícím obrázku č. 4.1 je schematicky znázorněná tato situace a taktéž je znázorněno, jaké požadavky jsou upřednostňované v jednotlivých oblastech skryté informace.



Obrázek č. 4.1 – Požadavky na steganografické systémy [7]

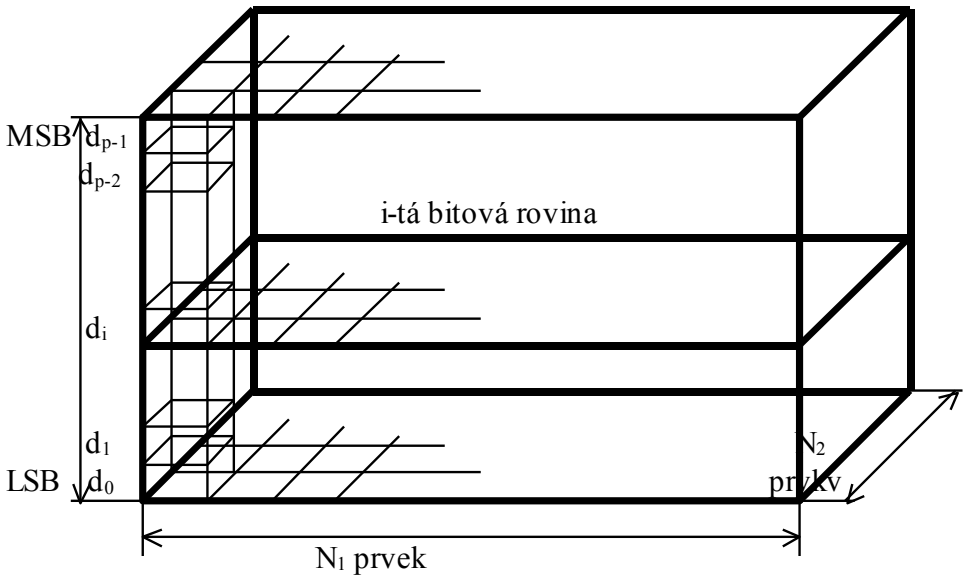
4.1.2.3 Možnosti využití rozkladu krycího obrazu na bitové roviny v steganografii

Víceúrovňový statický obraz se dá interpretovat také jako soubor tzv. bitových rovin. Uvažujme-li statický obraz s jasovou rozlišovací schopností 8 bit/op, tj. 256 jasovými úrovněmi, potom tento obraz můžeme rozložit na 8 bitových rovin. Každý obrazový bod originálního obrazu I je možné popsat p – bitovým slovem $(d_0, d_1, \ldots, d_{p-1})$, což představuje binární reprezentaci úrovně jasu daného obrazového bodu. Popíšeme-li všechny obrazové body jejich binárními reprezentacemi, získáme třírozměrný model originálního obrazu I, kde osy x a y udávají velikost (rastr) obrazu, tedy $n_I \times m_I$, a osa z udává bitovou reprezentaci každého obrazového prvku. Z takového modelu získáme p – bitových rovin obrazu I, přičemž rozměr každé roviny bude $n_I \times m_I$

a každá rovina bude představovat binární (dvouúrovňový) obraz. První bitová rovina je tvořena bity d_0 každého obrazového prvku originálního obrazu I (LSB bity), druhá rovina je tvořena bity d_1 každého obrazového prvku originálního obrazu I, atd., poslední bitová rovina bude tvořena bity d_{p-1} každého obrazového prvku originálního obrazu I. Celkový počet bitových rovin je obecně p pro jasovou rozlišovací schopnost p bitů/pixel, v tomto případě 8. [7]

Bitové roviny se vyznačují těmito vlastnostmi – bitová rovina je binární obraz a informační obsah ve vyšších bitových rovinách narůstá, tzn. Nejvyšší bitová rovina MSB obsahuje nejvíce informací o vizuálním obsahu obrazu.

Trojrozměrný model krycího obrazu je pro ukázku znázorněn na následujícím obrázku č. 4.2.



Obrázek č. 4.2 – Trojrozměrný model krycího obrazu [7]

4.1.2.3.1 Algoritmus vkládání vodoznaku

Data, která se vkládají do původních, originálních, krycích dat se nazývají vodoznaky. Vodoznaky představují digitální signály přidané do krycích dat (digitálního obrazu) způsobující změnu původních dat za účelem jejich utajeného přenosu, respektive za účelem prokázání vlastnictví původních krycích dat (digitální vodotisk).[2]

Vodoznak může mít formu konečné posloupnosti symbolů resp. čísel, obrazové informace (loga), segmentu řečového signálu, ale i bitové informace, která umožňuje indikaci zda původní data byla nebo nebyla vodoznakem označena. Vodoznak může mít charakter textu, souboru čísel, audio signálu, binárního obrazu a dokonce víceúrovňového obrazu.

Vodoznakem bývá nejčastěji obrazová informace binárního obrazu W s prostorovou rozlišovací schopností $m_W \times n_W$. Vložení vodoznaku představuje v podstatě modifikaci některých binárních hodnot vybrané bitové roviny podle příslušných hodnot vodoznaku W.

Při tomto použití vkládání vodoznaku do obrazu se využívá metoda LSB (Least Significant Bit = Nejméně významný bit). V případě použití této metody pro skrytí zprávy či vodoznaku, dojde sice ke změně některých bodů, avšak je to změna natolik nepatrná a nezásadní, že lidské oko nemá šanci jí zaregistrovat a už vůbec nemůže kód odhalit a rozluštit.

Při tomto použití vkládání vodoznaku do obrazu je vhodné vodoznak vkládat nejvíce do poslední bitové roviny (d_0), čímž bude zabezpečena nižší vjemová viditelnost vodoznaku, vyšší kvalita obrazu s vodoznakem a nižší pravděpodobnost odstranění vodoznaku nepovolanou osobou..

Předpokládejme vložení vodoznaku W do první bitové roviny d_0. Prostorová rozlišovací schopnost vodoznaku W je dána $m_W \times n_W$; prostorová rozlišovací schopnost originálního obrazu I je $m_I \times n_I$, proto i vybraná bitová rovina d_0 bude $m_I \times n_I$. Rozměr vodoznaku W bývá zpravidla menší, než je rozměr obrazu I, do kterého se vodoznak vkládá, proto $m_W \leq m_I$; $n_W \leq n_I$. Předpokládejme navíc, že pro vložení vodoznaku se budeme uvažovat celý obraz I, nikoliv libovolnou jeho část s rozměry $m_W \times n_W$.

V rámci prvního kroku vložení vodoznaku W může být použita jeho obrazová permutace, tj. taková transformace vodoznaku W, která vykoná přeuspořádání obrazových prvků vodoznaku W použitím pseudonáhodného algoritmu. Použitý pseudonáhodný algoritmus může tvořit navíc uživatelský klíč. Přeuspořádáním obrazových prvků vodoznaku W získáme permutovaný vodoznak W_p. Matematicky je možné proces permutace vodoznaku obecně popsat relací

$$W_P = \nu(W)$$

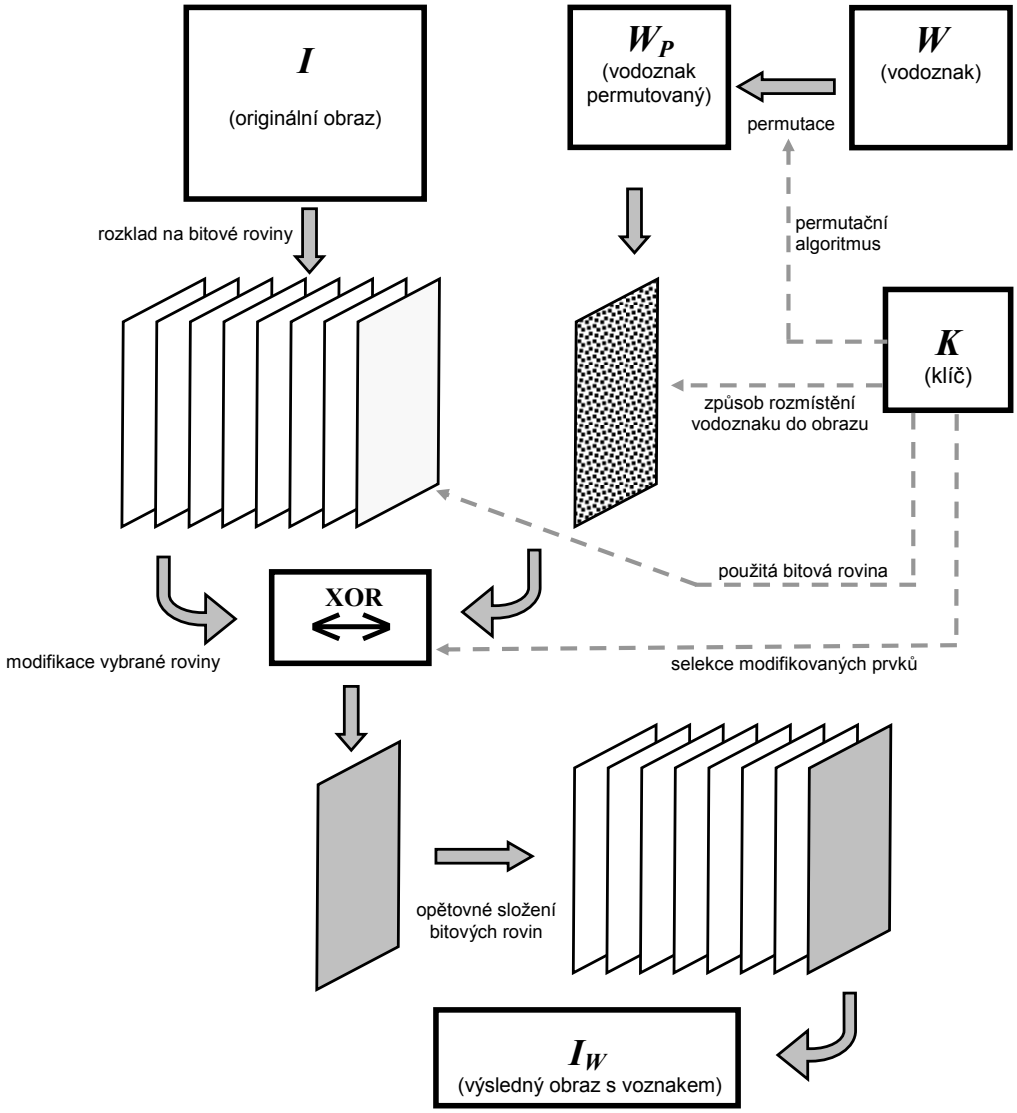
kde $\nu(.)$ je operace přeuspořádání obrazových prvků.

Následně je nutné určit jakým způsobem bude vodoznak rozprostřen do vybrané bitové roviny.

Vložení vodoznaku je realizováno tak, že vybrané obrazové prvky bloku bitové roviny jsou modifikovány podle hodnot prvků odpovídajícího permutovaného vodoznaku pomocí funkce *XOR*.

Takto upravená vybraná binární rovina se následně využije pro zpětné složení obrazu a vznikne výsledný obraz s vodoznakem I_W.[7]

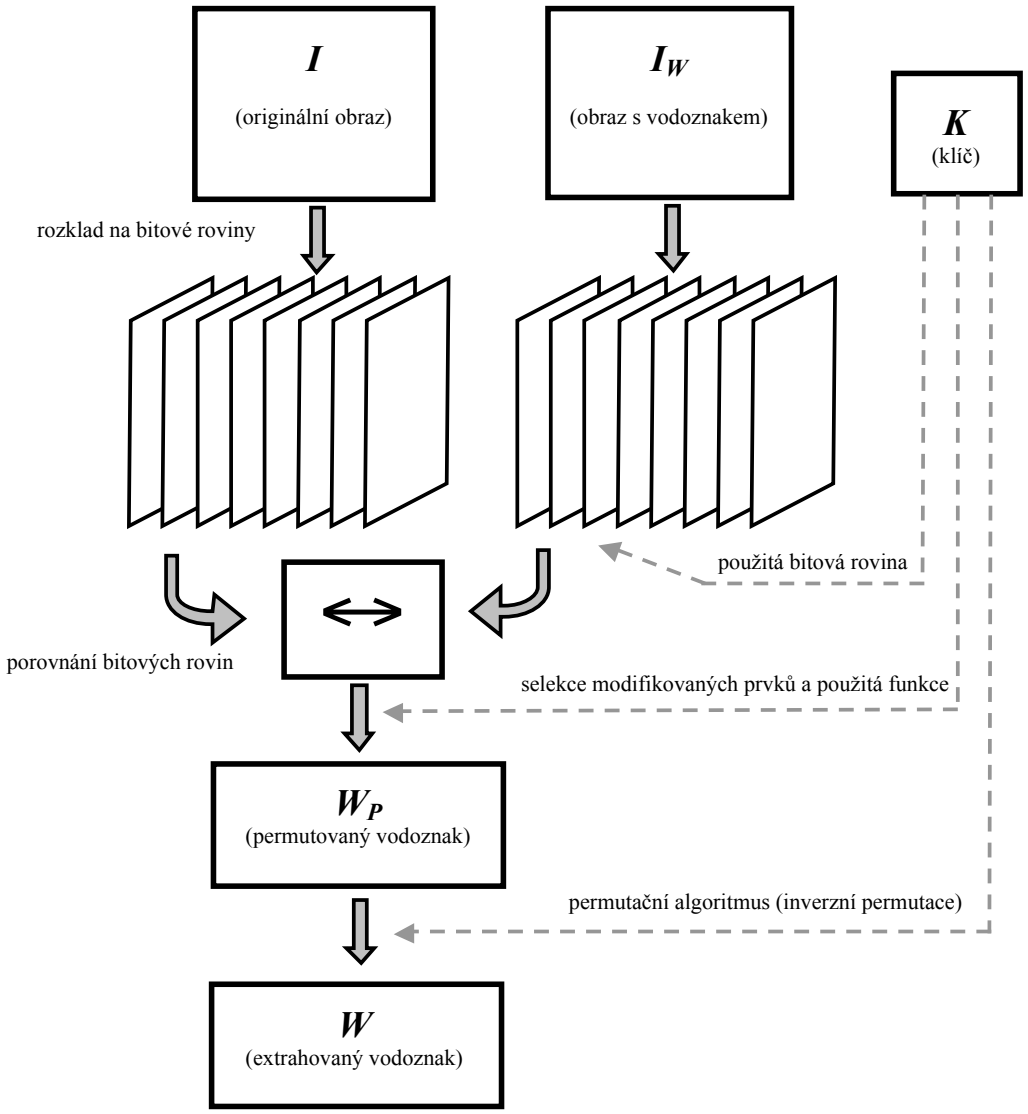
Algoritmus vkládání vodoznaku je naznačen na následujícím obrázku č. 4.3.



Obrázek č. 4.3 Algoritmus vkládání vodoznaku

4.1.2.3.2 Algoritmus extrakce vodoznaku

K extrakci vodoznaku je zapotřebí originální obraz *I* (bez vodoznaku) a obraz s vloženým vodoznakem I_W a uživatelský klíč *K*. Uživatelský klíč je tvořen informacemi o použité bitové rovině, použité obrazové permutaci vodoznaku a způsobu použité selekce obrazových prvků bitové roviny při vkládání vodoznaku. Originální obraz I rozložíme na bitové roviny. Obraz s vodoznakem I_W rozložíme taktéž na bitové roviny. Na základě uživatelského klíče *K* porovnáme vhodné bitové roviny a správnou selekcí prvků (na základě informace z uživatelského klíče *K*) získáme permutovaný vodoznak W_P. Použitím inverzního permutačního algoritmu (tzv. repermutačního algoritmu, nebo repermutace) modifikujeme permutovaný vodoznak W_P na vodoznak *W*, který byl do obrazu *I* vložen. Postup extrakce vodoznaku je graficky znázorněn na obr. 4.4. Extrahováním vodoznaku z obrazu se dokazují autorská práva k obrazu, do kterého byl vložen.[7]



Obrázek č. 4.4 – Postup extrakce vodoznaku

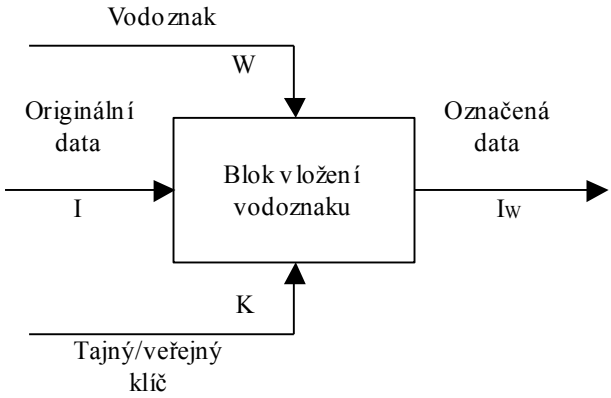
4.1.3 Systémy digitálního vodotisku

Stejně jako v steganografii data, která se vkládají do původních originálních, krycích dat se nazývají vodoznaky. Vodoznaky představují digitální signály přidané do krycích dat způsobující změnu původních dat za účelem jejich utajeného přenosu, resp. za účelem prokázání vlastnictví původních krycích dat. Vlastní vodoznak patří pouze jednomu vlastníkovi, on je jedinou osobou, která jej může spolehlivě a věrohodně detekovat a tak prokázat vlastnictví. Vlastník je taktéž jedinou osobou, která může odstranit vodoznak z digitálního obrazu. [1].

Metody digitálního vodotisku představují algoritmy, jimiž se vkládají vodoznaky do obrazů s cílem autentifikace obrazu, přičemž se uvažuje obraz i vodoznak v digitálním tvaru.

Technika digitálních vodoznaků je definovaná jako vložení přídavné informace (vodoznaku) do multimediálních dat tak, aby modifikace těchto dat byla smyslově nepostřehnutelná.

Všechny metody technik digitálních vodoznaků sdílí stejný algoritmus vkládání vodoznaků, viz následující obrázek. [42]



Obrázek č. 4.5 – Princip vkládání vodoznaku[35]

Originální data jsou data, do kterých vkládáme vodoznak. Mohou se označovat také jako krycí data nebo zdrojová data. Originálními daty mohou být audio signály, videosekvence, ale nejrozšířenějšími používanými originálními daty jsou digitální statické obrazy.

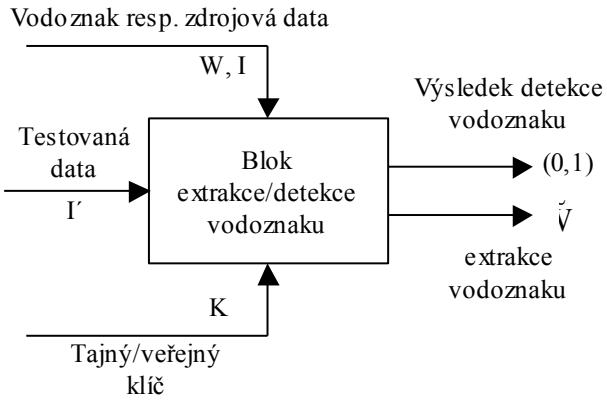
V závislosti na metodě vložení vodoznaku nám do procesu vkládání může, ale nemusí vstupovat tajný nebo veřejný klíč. Použití klíče zvyšuje odolnost vloženého vodoznaku, čímž se zároveň zvyšuje ochrana originálních dat před neautorizovanými operacemi. Většina praktických systémů využívá přinejmenším jeden klíč nebo dokonce kombinaci několika klíčů.

Výsledkem procesu vložení vodoznaku do originálních dat jsou data označená vodoznakem (watermarked data) nazývaná též označená nebo podepsaná data (signed data).

Extrakce vodoznaku – je to proces výběru vodoznaku z testovaných dat, tak aby ho bylo možné porovnat s vloženým vodoznakem. Shoda vodoznaků potvrzuje vložení vodoznaku do testovaných dat (autentizace dat). [33]

Detekce – je to binární rozhodovací proces, jehož výsledkem je zjištění, zda zdrojová data byla resp. nebyla označena vodoznakem. Modifikované detekční algoritmy poskytují trojhodnotový rozhodovací proces, a to: zda je vodoznak přítomný a současně detekovaný, resp. zda je vodoznak přítomný, ale nedetekovaný, resp. zda je vodoznak nepřítomný.[33]

Metody technik digitálních vodoznaků sdílejí stejný algoritmus extrakce/detekce vodoznaku, viz následující obrázek č. 16.



Obrázek č. 4.6 - Extrakce/detekce vloženého vodoznaku [35]

Data, ze kterých chceme extrahovat vodoznak, nebo zjistit, zda tato data byla označena vodoznakem (detekce vodoznaku) nazýváme testovaná data. V závislosti na použité metodě při vkládání vodoznaku jsou dalšími vstupy vodoznak resp. zdrojová data a tajný/veřejný klíč. Výstupem detekce přítomnosti vodoznaku je odpověď ano/ne (0,1). Výstupem extrakce je extrahovaný vodoznak W´. Extrahovaný vodoznak nemusí být shodný s vloženým vodoznakem W, neboť přenosová cesta může způsobit zkreslení označených dat a zároveň se předpokládá přítomnost nepovolané osoby, která může způsobit poškození, nebo odstranění vodoznaku z označených dat pomocí útoků. [42]

4.1.3.1 Rozdělení metod digitálního vodotisku

Techniky digitálních vodoznaků lze dělit z více hledisek. Podle vstupů a výstupů procesů vkládání a extrakce/detekce vodoznaku rozeznáváme tři systémy[30]:

- Soukromé systémy s vodoznakem používají na vložení vodoznaku W do originálních dat I, soukromý klíč K a při detekci resp. extrakci vodoznaku kromě soukromého klíče vyžadují přinejmenším také originální data. Lze je rozdělit do dvou skupin:

  - Systémy první podskupiny extrahují z testovaných dat I' vodoznak, přičemž vyžadují znalost originálních dat I a klíče K. Symbolicky je možné toto zapsat ve tvaru

$$\left\{I' \times K \times I \to \widetilde{W}\right\}$$

    Extrahovaný vodoznak $\widetilde{W}$ se porovnává s vloženým vodoznakem W, přičemž nejčastěji se jako míra podobnosti používá korekce mezi W a $\widetilde{W}$.

  - Systémy druhé podskupiny vykonávají pouze detekci přítomnosti vodoznaku W v testovaných datech I´. Obvykle vyžadují znalost vloženého vodoznaku W a znalost originálních dát, tzn. Je možné je symbolicky zapsat ve tvaru

$$\left\{I' \times K \times I \times W \to (0,1)\right\}$$

Výsledek detekce má binární formu, to znamená, že testovaná data obsahují vodoznak W (výstup „1“), resp. neobsahují vodoznak W (výstup „0“). Tyto systémy vzhledem k binárnímu výstupu se vyznačují větší robustností.

- Polosoukromé systémy s vodoznakem vykonávají detekci přítomnosti vodoznaku W v testovaných datech I´. Vyžadují znalost vloženého vodoznaku W a soukromého klíče K, ale nevyžadují znalost originálních dat. Symbolicky lze toto zapsat ve tvaru

$$\{I' \times K \times W \rightarrow (0,1)\}$$

Výstup je dvojhodnotový a odpovídá výsledku testu detekce přítomnosti vodoznaku.

- Veřejné systémy s vodoznaky používají veřejný klíč K, kterým se vkládá do originálních dát I n-bitová informace. Tato informce nemá charakter vodoznaku. Extrakce této n-bitové informace z označených dat I´ se realizuje veřejným klíčem K a nevyžaduje znalost originálních dát. Tyto systémy je možné symbolicky zapsat ve tvaru

$$\{I' \times K \rightarrow s\}$$

kde s je n-bitová informace vložená do originálních dat.

Hlavní využití soukromých a polosoukromých systémů s vodoznakem je přinejmenším v oblasti autentizace dat a ochrany autorských práv. Veřejné systémy s vodoznaky slouží k přenosu přídavné informace vložené do originálních dat, která jsou veřejně přístupná pomocí veřejného klíče.[7]

4.1.3.2 Rozdělení vodoznaků

V praxi používané vodoznaky je možné rozdělit podle jejich určení následovně[25]:

- **Viditelné vodoznaky** (visible watermarks) – jsou to viditelné obrazce vsunuté do jiných obrazců. Příkladem jsou např. loga. Představují analogii papírových vodoznaků. Slouží k zamezení použití určitých druhů označených dat (např. digitálních obrazů) ke komerčním účelům.
- **Skryté vodoznaky** (watermarks) – jsou přídavnou informací, která je vsunutá do původních informací bez toho, aby se podstatně narušil původní informační obsah, nejsou však běžně viditelné. Důležitým požadavkem je robustnost vodoznaku, čili odolnost vůči jeho odstranění nepovolanou osobou bez znalosti klíče.
- **Identifikační vodoznaky** (finger-printing) – jsou speciální třídou vodoznaků, které představují specifický kód autora série původní informace.
- **Proudové vodoznaky** (bitstream watermarking) – jsou to vodoznaky určené na označení komprimovaných dat, jako jsou komprimovaná video data.
- **Křehké vodoznaky** (fragile watermarks) – jsou to vodoznaky, které mají limitovanou robustnost. Proto slouží jako identifikátor narušení vodoznakem označených dat.

Z hlediska vnímatelnosti lze vodoznaky rozdělit na[18]:

- **Postřehnutelné** – obyčejně obsahují viditelný odkaz nebo logo společnosti.

- **Nepostřehnutelné** – krycí data s vloženým vodoznakem jsou vizuálně velmi podobná původním datům bez vodoznaku. Existence takového vodoznaku se dá dokázat jen jeho extrakcí či detekujícím algoritmem.

Z hlediska odolnosti lze vodoznaky rozdělit na[14]:

- **Křehké** – vodoznaky vložené takovouto metodou jsou lehko narušitelné jednoduchými operacemi s obrazem (například vodoznaky určené ke kontrole integrity musí být nutně křehké)
- **Robustní** – takto vložené vodoznaky odolávají manipulacím s obrazy (jsou užitečné při deklarování vlastnictví). Robustní vodoznaky je možné dále rozdělit na:
  - Soukromé, které vyžadují na extrakci/detekci vodoznaku původní obraz.
  - Veřejné, které nevyžadují na extrakci/detekci vodoznaku původní obraz.

Algoritmy vyžadující uživatelský klíč lze dělit na algoritmy[11]:

- **S tajným klíčem** – při těchto algoritmech se používá na vložení i extrakci/detekci stejný klíč (při přenosu klíče je pak nutné zabezpečit bezpečnou komunikaci mezi vlastníkem obrazu a příjemcem),
- **S veřejným klíčem** – při těchto algoritmech se používá dvou klíčů. Využívá se klíč veřejný a klíč soukromý.

4.1.3.3 Klasifikace metod obrazového vodotisku

Metody vkládání vodoznaku do obrazových signálů využívají na zabezpečení neviditelnosti nedokonalost lidského vizuální systému HVS (Human Visual Systém). Velké množství těchto metod je možné rozdělit do dvou základních skupin[7]:

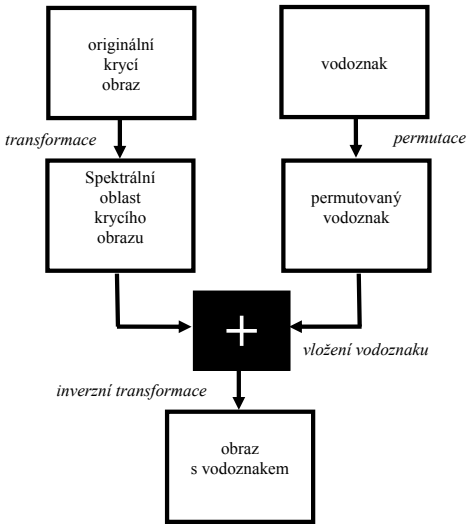
- Metody založené na korelaci – v obrazovém prostoru modifikují jasovou úroveň obrazových prvků pseudonáhodným obrazcem resp. pseudonáhodnou posloupností, která je odvozená od vodoznaku.
- Metody bez využití korelace – využívající modifikaci transformačních koeficientů vodoznakem. Tyto metody využívají transformaci na celý obraz nebo transformaci po blocích.

Techniky vložení vodoznaků využívají různé principy, přičemž je možné je rozdělit na:

- Techniky vkládání vodoznaků v obrazové oblasti – realizují modifikaci obrazových prvků. V případě neviditelných vodoznaků se využívá nedokonalosti lidského vizuálního systému v tom smyslu, že člověk rozpozná maximálně 90 přechodů jasových úrovní. Při vyšším počtu úrovní už není schopný zaregistrovat malé změny v těchto přechodech.
- Techniky vkládání vodoznaků v transformované oblasti – realizují modifikaci spektrálních, resp. sekvenčních koeficientů krycích dat. Tyto techniky využívají přinejmenším digitální obrazové vodoznaky. Zpětnou (inverzní) diskrétní ortogonální transformací modifikovaných koeficientů se získají původní data, ve kterých je vložený vodoznak.
- Techniky vkládání vodoznaků v parametrické oblasti – realizují vložení vodoznaku v procesu zpracování dat, přičemž využívají modifikaci tzv.

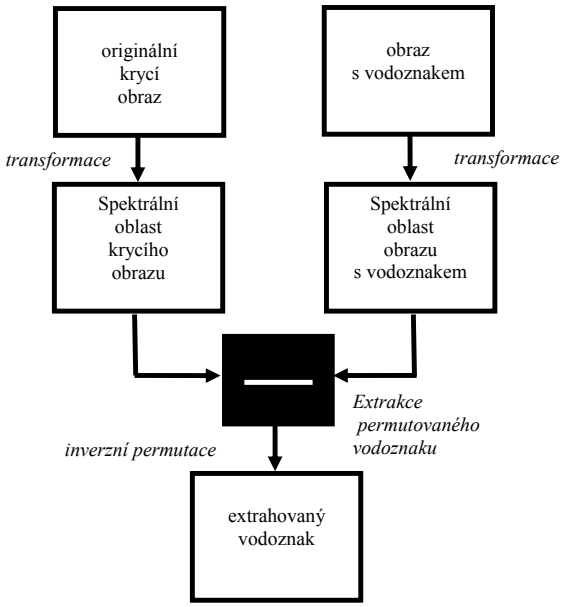
parametrického prostoru (parametrického popisu) krycího obrazu. Příkladem této techniky je vložení vodoznaku při fraktálovém kódování obrazu, kde je vodoznak vkládaný do koeficientů pro transformaci jasu v procesu konverze obrazu do formátu *.fif (fractal image format). [3]

Nejvíce využívanými technikami jsou techniky vkládání vodoznaků v transformované oblasti. Tyto algoritmy ve všeobecnosti využívají stejný postup implementace vodoznaku, jaký je znázorněný na obrázku č. 4.7. Liší se v použití diskrétních ortogonálních transformací a ve výběru a způsobu modifikace spektrálních koeficientů (aby byly splněny podmínky pro vizuální imperceptibilitu vloženého vodoznaku a jeho robustnost).



Obrázek č. 4.7 – Všeobecný algoritmus vložení vodoznaku do krycího obrazu[7]

Proces extrakce vyžaduje jako vstupní informaci originální krycí obraz, obraz s vodoznakem a uživatelský klíč. Tento proces je znázorněn na následujícím obrázku č. 4.8.



Obrázek č. 4.8 – Všeobecný algoritmus extrakce vodoznaku[7]

4.1.3.4 Požadavky na vodoznaky a metody vkládání vodoznaků

Vodoznaky v systémech digitálního vodotisku by měly splňovat následující vlastnosti[25]:

- **Imperceptibilita** – změny způsobené vkládáním vodoznaku by neměly zhoršovat vnímanou kvalitu obrazu.
- **Spolehlivá detekce** – vodoznak by měl přestavovat dostatečný a spolehlivý důkaz o vlastnictví produktu. Chyby detekce by se měly objevovat extrémně zřídka, v nejlepším případě nikdy.
- **Přidružený klíč** – vodoznaky by měly být přidružené s identifikačním číslem, nazývaným též klíč vodoznaku. Tento klíč je používaný na sestavení, detekci a odstranění vodoznaku. Potom tento klíč by měl být soukromý a měl by jednoznačně charakterizovat legálního vlastníka. Každý číslicový signál extrahovaný z digitálního obrazu je pokládán za platný tehdy a pouze tehdy, pokud je spojený s klíčem přes spolehlivě navrhnutý algoritmus. Tato podmínka zabraňuje vytváření falešných vodoznaků.
- **Statistická nedetekovatelnost** – vodoznaky by neměly být identifikovatelné použitím statistických metod. Například vlastnictví velkého počtu digitálních produktů, označených pomocí určitého vodoznaku, by nemělo dát možnost odhalit vodoznak použitím statistických metod. Pro zabezpečení statistické nedetekovatelnosti se používá pro modifikaci vodoznaků permutační algoritmy.
- **Vícenásobné vkládání vodoznaku** – při vkládání vodoznaku by jsme měli být schopni vložit do obrazu dostatečné množství rozdílných vodoznaků. Každý vodoznak by měl být detekovatelný použitím příslušného jedinečného klíče. Tato vlastnost je nevyhnutelná pro vkládání vodoznaku do obrazů, do kterých už v minulosti vodoznak vložený byl. Toto je taktéž vhodné v případě přenosu autorských práv z jednoho vlastníka na jiného.

- **Robustnost** – digitální obraz může podstoupit velké množství rozdílných modifikací, které úmyslně (pirátské útoky) nebo neúmyslně (komprese, filtrování pro odstranění šumu, apod.) ovlivňují vložený vodoznak. Vodoznak použitý jako ochrana autorských práv, by měl být detekovatelný až do bodu, kdy kvalita hostitelského obrazu zůstává v akceptovatelných hranicích. Robustnost je jednou z nejdůležitějších vlastností vodoznaků[6].

4.1.3.5 Všeobecný algoritmický model digitálních vodoznaků

Je-li uvažován digitální krycí obraz I_0 (tj. obraz, do kterého se vkládá vodoznak) s prostorovou rozlišovací schopností (t.j. s rozměry) $N_1 \times N_2$ a jasovou rozlišovací schopnost *8* bit/pixel, t.j. s $2^8=256$ jasovými úrovněmi. Potom pro krycí obraz I_0 lze napsat[30]:

$$I_0=\{i_0(i,j),\ 0 \le i < N_1,\ 0 \le j < N_2\},$$

kde $i_0(i,j) \in \{0, ..., 2^{\lambda}-1\}$ je intenzita obrazového prvku $i_0(i,j)$, λ je počet bitů použitých na vyjádření intenzity obrazového prvku a N_1, N_2 jsou přirozená čísla.

Vodoznak W může být reprezentovaný v nejjednodušším případě jako dvojrozměrný digitální obrazový signál W s prostorovou rozlišovací schopností (tj. s rozměry) $M_1 \times M_2$: $M_1 \le N_1$, $M_2 \le N_2$ a jasovou rozlišovací schopností *1* bit/pixel, tj. binární vodoznak (všeobecně ale může výt také uvažovaný víceúrovňový případ):

$$W=\{w(i,j),\ 0 \le i < M_1,\ 0 \le j < M_2\},$$

kde $w(i,j) \in \{0,1\}$, M_1 a M_2 jsou přirozená čísla.

Vodoznakové techniky v zásadě rozlišují dvě algoritmické fáze, kterými jsou:
- Vkládání vodoznaku
- Extrakce, případně detekce vodoznaku

Proces vkládání vodoznaku je definovaný jako superpozice dvojrozměrného digitálního (obrazového) signálu $W(i,j)$ do krycího obrazu $I_0(i,j)$. Označme tedy proces vkládání vodoznaku jako ε a definujme ho takto:

$$\varepsilon : I_0 \times W \times \Re \rightarrow I_W,$$

tzn. pro obraz s vloženým vodoznakem I_W bude platit

$$I_W = \varepsilon\,(I_0; W; l).$$

Parametr l, který nenabyde reálné hodnoty (z množiny reálných čísel $\Re$), je spojený s energií vloženého (embedding watermark energy). Funkce ε může být vyjádřená jako jednoduchá superpozice vodoznaku ve tvaru:

$$I_W(i,j) = I_0(i,j) \oplus L(i,j)W(i,j),$$

kde L představuje dvojrozměrnou masku na vložení vodoznaku a $\oplus$ definuje operátor superpozice obsahující zaokrouhlení a kvantizaci. Koeficienty $L(i,j)$ mohou být buď

konstanty pro všechny obrazové prvky, nebo se mohou měnit v závislosti na vlastnostech obrazu. Malé hodnoty $L(i,j)$ mohou garantovat neviditelnost vodoznaku. V takovémto případě ale bude energie vloženého vodoznaku malá a vodoznak může být odstraněný už mírným úsilím. Maska pro vložení vodoznaku by měla být specifická pro daný obraz a měla by brát v úvahu charakteristiky lidského vizuálního systému. Inverznost ε je požadovaná, ale není nevyhnutelnou podmínkou.

Procedura E extrakce vodoznaku je nejdůležitější částí algoritmu vodoznaku. Výstup extraktora/detektora může být binární výsledek (ano,ne). V takovémto případě se jedná pouze o tzv. *detekcu* vodoznaku. V případě, že bude z obrázku s vloženým vodoznakem I_W vyextrahovaný celý vložený vodoznak, jedná se o tzv. *extrakci* vodoznaku. [30]

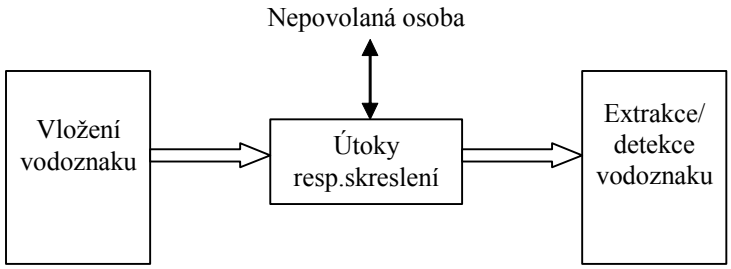
Výstup extraktora/detektora produkuje dostatečný důkaz vlastnických práv v případě, že je dostatečně věrohodný. Tento požadavek doporučuje, aby algoritmus detekce vyl veřejně známou a globálně akceptovanou procedurou. Použitím testovacích hypotéz mohou být možné chyby klasifikované ve dvou kategoriích:

- *Chyba I. druhu* – vodoznak je detekovaný, přestože v obraze není přítomný. Tato chyba je charakterizovaná kvantitativně pravděpodobností falešného poplachu (P_{fa}).
- *Chyba II. druhu* – vodoznak není detekovaný, přestože v obraze existuje. Vzniká chybová pravděpodobnost zamítnutí vodoznaku (P_{rej}).

Celková pravděpodobnost je $P_{err} = P_{fa}+P_{rej}$ a výkon detekce stoupá, pokud P_{err} klesá. Tyto dva druhy chyb se navzájem doplňují, jak stoupá P_{fa}, klesá P_{rej} a naopak.

4.1.4 Útoky na vodotiskové systémy

Útoky jsou procesy, jejichž cílem je buď odstranění vodoznaku respektive jeho poškození, aby se znemožnila jeho extrakce nebo aby po jeho extrakci nebylo možné potvrdit shodu vloženého a extrahovaného vodoznaku (viz. obrázek č. 4.9).



Obrázek č. 4.9 – Útoky na vodoznakové systémy

Systém vodotisku by měl být schopen odolat nejrůznějším útokům. Útokem je myšlena operace jejímž následkem je poškození vodotisku nebo znemožnění detekce. Je podstatné rozlišovat útoky neúmyslné a úmyslné. [27]

Za *neúmyslné útoky* se považuje běžná operace s daty, která vložený vodotisk poškodí neúmyslně, náhodou. Jedná se o operace, kdy poškození je vedlejším efektem.

Příkladem je ztrátová komprese, lineární filtrování, digitálně-analogová a analogově-digitální konverze, oříznutí, vytištění, skenování apod.

Naopak o *úmyslném útoku* se mluví, když útočníkovým cílem je vodoznak jakkoliv poškodit či znemožnit jeho funkci.

Známy jsou čtyři hlavní typy úmyslných útoků[7]:

- **Útoky na robustnost** – Cílem je poškodit nebo zcela znehodnotit vodoznak. Útoky na robustnost se dále dělí do dvou podtříd:
  - ***Útoky všeobecné*** – pracují různými způsoby a snaha odstranit vodotisk není závislá na konkrétních vlastnostech algoritmu. Mezi nejznámější patří:
    - *Útoky zpracováním signálu* (signal-processing attacks) – procují s běžnými a „nevinnými" manipulacemi s daty, jako je komprese, filtrovani, změna velikosti, tisk a skenováni. Typickým příkladem je útok šumem (attack with uncorrelated noise), který spočívá v přidání šumu do dat tak, aby se v nich vložený vodoznak nedal detekovat nebo extrahovat. Při tomto útoku však je nutné postupovat opatrně, aby se přidaným šumem data neznehodnotila pod akceptovanou úroveň.
    - *Útok přepsáním* (attack by overmarking) – útočník vloží do dat z kterých se snaží odstranit vodoznak dalším vodoznak, případně využije různé techniky, aby původní vodoznak přepsal (samozřejmě však při zachování kvality dat)
    - *Útok spiknutím* (collusion attack, attack by conspiracy, multiple document attack) – různé označené verze stejných originálních dat se zprůměrují a tak se vytvoří jejich nová neoznačená kopie. Čím víc verzí se na zprůměrování využije, tím by měla být výsledná kvalita dat lepší a bližší originálu.
    - *Iterativní útok* (iterative attack) – dá se využit jen tehdy, pokud jde o digitální vodotisk, na který pro extrakci respektive detekci nepotřebujeme znát tajný klíč a u kterého extrakční resp. detekční procedura je známá. Útočník pak může v datech udělat drobnou změnu a ze změněných dat se pokusit extrahovat vodoznak.
  - ***Útoky analytické*** – snaží se využít konkrétních vlastností algoritmu. Na rozdíl od předcházejících typů útoků je nutné znát, jak přesně algoritmus pracuje. Příkladem je útok invertováním (inversion attack), který je založen na principu přesného odhadnutí umístění vodoznaku a jeho následné odstranění za pomoci inverzního vložení (tzn. inverzní funkce k použité funkci vkládání vodoznaku).
- **Prezentační útoky** (presentation attacks, detection-disabling attacks, synchronization attacks) – nesnaží se vodoznak odstranit nebo poškodit, ale provádějí útok tak, že detektor nedokáže vodoznak najít. Příkladem efektivního prezentačního útoku je rozdělení označeného obrázku na malé části. Jednotlivé části je pak možné umístit na webovou stránku tak, aby byl poskládán příslušný obrázek.
- **Interpretační útoky** (interpretation attacks, ambiguity attacks, confusion attacks, deadlock attacks) – jsou založeny na vložení falešného vodoznaku. U takto označených dat může dojít k situaci, kdy se nedá dokázat, který vodoznak je pravý a útočník se může pokusit vydávat za (neoprávněného) majitele originálních dat.
- **Právní útoky** (legal attacks) – jsou netechnické útoky využívající nedokonalosti zákonných ochran autorských práv. Mohou například vycházet z rozdílné

interpretace zákona, různých soudech, pověsti vlastníka a útočníka, schopnosti útočníka zpochybnit danou vodoznakovou techniku apod. O právní útok se jedná, taktéž když vlastník originálních dat dokáže extrahovat vložený vodoznak, ale soud to nepovažuje za důkaz jejich vlastnictví.

4.2 Dílčí oblasti analýzy

4.2.1 Legislativa

Tato kapitola se bude zabývat právem autorským a trestním a zaměřuje se především na veřejně přístupná elektronická data, jejich užití, majetková práva s nimi související, ochranu těchto práv a v neposlední řadě i postihy spojené s porušením autorských práv.

Vzhledem k rozsahu autorského zákona a zákona trestního zde budou uvedeny pouze výňatky těchto zákonů s problematikou práce úzce související.

4.2.1.1 Autorský zákon

Autorské právo je v České republice upraveno autorským zákonem č. 121/2000 Sb. ve znění pozdějších předpisů. Autorský zákon je souhrn právních norem, které upravují vztahy, jejichž předmětem jsou autorská díla. Tato kapitola čerpá z [22].

Tento zákon **zapracovává příslušné předpisy Evropských společenství a** upravuje:

a) práva autora k jeho **autorskému** dílu,
b) práva související s právem autorským:
   1. práva výkonného umělce k jeho uměleckému výkonu,
   2. právo výrobce zvukového záznamu k jeho záznamu,
   3. právo výrobce zvukově obrazového záznamu k jeho záznamu,
   4. právo rozhlasového nebo televizního vysílatele k jeho vysílání,
   5. právo zveřejnitele k dosud nezveřejněnému dílu, k němuž uplynula doba trvání majetkových práv,
   6. právo nakladatele na odměnu v souvislosti se zhotovením rozmnoženiny jím vydaného díla pro osobní potřebu,
c) právo pořizovatele k jím pořízené databázi,
d) ochranu práv podle tohoto zákona,
e) kolektivní správu práv autorských a práv souvisejících s právem autorským.

4.2.1.1.1 Předmět práva autorského

Dle §2 je předmětem práva autorského, dílo literární a jiné dílo **umělecké** a dílo vědecké, které je jedinečným výsledkem tvůrčí činnosti autora a je vyjádřeno v jakékoli objektivně vnímatelné podobě včetně podoby elektronické, trvale nebo dočasně, bez ohledu na jeho rozsah, účel nebo význam (dále jen „dílo“). Dílem je zejména dílo slovesné vyjádřené řečí nebo písmem, dílo hudební, dílo dramatické a dílo hudebně dramatické, dílo choreografické a dílo pantomimické, **dílo fotografické** a dílo vyjádřené postupem podobným fotografii, dílo audiovizuální, jako je dílo

kinematografické, dílo výtvarné, jako je dílo malířské, **grafické** a sochařské, dílo architektonické včetně díla urbanistického, dílo užitého umění a dílo kartografické.

Fotografie a dílo vyjádřené postupem podobným fotografii, které jsou původní ve smyslu věty první, jsou chráněny jako dílo fotografické.

4.2.1.1.2 Autorství a obsah práva autorského

Dle § 5 je autorem je fyzická osoba, která dílo vytvořila a autorem díla souborného je fyzická osoba, která je tvůrčím způsobem vybrala nebo uspořádala, tím nejsou dotčena práva autorů děl do souboru zařazených.

Dle § 6 je autorem díla fyzická osoba, jejíž pravé jméno je obvyklým způsobem uvedeno na díle nebo je u díla uvedeno v rejstříku předmětů ochrany vedeném příslušným kolektivním správcem, není-li prokázán opak; to neplatí v případech, kdy je údaj v rozporu s jiným údajem takto uvedeným. Toto ustanovení se použije i tehdy, jeli toto jméno pseudonymem, pokud autorem přijatý pseudonym nevzbuzuje pochybnosti o autorově totožnosti.

Právo autorské k dílu vzniká okamžikem, kdy je dílo vyjádřeno v jakékoli objektivně vnímatelné podobě.

Právo autorské zahrnuje výlučná práva osobnostní (§ 11) a výlučná práva majetková (§ 12).

Mezi osobnostní práva se zahrnuje:

- autor má právo rozhodnout o zveřejnění svého díla
- autor má právo osobovat si autorství, včetně práva rozhodnout, zda a jakým způsobem má být jeho autorství uvedeno při zveřejnění a dalším užití jeho díla, jeli uvedení autorství při takovém užití obvyklé
- autor má právo na nedotknutelnost svého díla, zejména právo udělit svolení k jakékoli změně nebo jinému zásahu do svého díla, nestanoví-li zákon jinak
- a další zde neuváděná (netýká se přímo problematiky této práce)

Majetková práva

V rámci majetkového práva má autor právo své dílo užít a udělit jiné osobě smlouvou oprávnění k výkonu tohoto práva; jiná osoba může dílo užít v původní nebo jiným zpracované či jinak změněné podobě, samostatně nebo v souboru anebo ve spojení s jiným dílem či prvky bez udělení takového oprávnění pouze v případech stanovených tímto zákonem.

Poskytnutím oprávnění podle odstavce 1 právo autorovi nezaniká; autorovi vzniká pouze povinnost strpět zásah do práva dílo užít jinou osobou v rozsahu vyplývajícím ze smlouvy.

Autor má právo požadovat na vlastníku věci, jejímž prostřednictvím je dílo vyjádřeno, aby mu ji zpřístupnil, pokud je toho třeba k výkonu práv autorských podle tohoto zákona. Toto právo nelze uplatnit v rozporu s oprávněnými zájmy vlastníka; vlastník není povinen autorovi takovou věc vydat, je však povinen na žádost a náklady autora zhotovit fotografii nebo jinou rozmnoženinu díla a odevzdat ji autorovi.

Právem dílo užít je:

- právo na rozmnožování díla (§ 13)

- právo na rozšiřování originálu nebo rozmnoženiny díla (§ 14)
- právo na pronájem originálu nebo rozmnoženiny díla (§ 15)
- právo na půjčování originálu nebo rozmnoženiny díla (§ 16)
- právo na vystavování originálu nebo rozmnoženiny díla (§ 17)
- právo na sdělování díla veřejnosti (§ 18)

Sdělováním díla veřejnosti se rozumí zpřístupňování díla v nehmotné podobě, živě nebo ze záznamu, po drátě nebo bezdrátově.

Sdělováním díla veřejnosti podle odstavce 1 je také zpřístupňování díla veřejnosti způsobem, že kdokoli může mít k němu přístup na místě a v čase podle své vlastní volby zejména počítačovou nebo obdobnou sítí.

Sdělováním díla veřejnosti podle odstavců nedochází k vyčerpání práva autora na sdělování díla veřejnosti.

Další (ze zákona „jiná“) majetková práva

- Právo na odměnu při opětném prodeji originálu díla uměleckého
- Právo na odměnu v souvislosti s rozmnožováním díla pro osobní potřebu a vlastní vnitřní potřebu

Majetkových práv se autor nemůže vzdát. Tato práva jsou nepřevoditelná a nelze je postihnout výkonem rozhodnutí. Majetková práva jsou předmětem dědictví.

Majetková práva trvají, po dobu autorova života a 70 let po jeho smrti. Bylo-li dílo vytvořeno jako dílo spoluautorů, počítá se doba trvání majetkových práv od smrti spoluautora, který ostatní přežil.

4.2.1.1.3 Volná užití

Za užití díla dle autorského zákona se nepovažuje užití pro osobní potřebu fyzické osoby, jehož účelem není dosažení přímého nebo nepřímého hospodářského nebo obchodního prospěchu, nestanoví-li tento zákon jinak.

Do práva autorského tak nezasahuje ten, kdo pro svou osobní potřebu zhotoví záznam, rozmnoženinu nebo napodobeninu díla.

Do práva autorského nezasahuje ten, kdo užije dílo při vyučování pro ilustrační účel nebo při vědeckém výzkumu, jejichž účelem není dosažení přímého nebo nepřímého hospodářského nebo obchodního prospěchu, a nepřesáhne rozsah odpovídající sledovanému účelu. Vždy je však nutno uvést, jeli to možné, jméno autora, nejde-li o dílo anonymní, nebo jméno osoby, pod jejímž jménem se dílo uvádí na veřejnost, a dále název díla a pramen.

Do práva autorského nezasahuje vlastník ani osoba, která si od vlastníka vypůjčí originál či rozmnoženinu díla výtvarného, fotografie nebo díla vyjádřeného postupem podobným fotografii, vystavuje-li takové dílo nebo je k vystavení bezplatně poskytne, ledaže to autor při převodu vlastnictví k takovému originálu nebo takové rozmnoženině zapověděl a vlastníkovi nebo vypůjčiteli to bylo známo nebo známo být muselo, zejména proto, že zapovězení je zapsáno v rejstříku vedeném za tím účelem kolektivním správcem.

4.2.1.1.4 Ochrana práva autorského

Dle § 40 autor, do jehož práva bylo neoprávněně zasaženo nebo jehož právu hrozí neoprávněný zásah, může se domáhat zejména:

a) určení svého autorství,

b) zákazu ohrožení svého práva, včetně hrozícího opakování, nebo neoprávněného zásahu do svého práva, zejména zákazu neoprávněné výroby, neoprávněného obchodního odbytu, neoprávněného dovozu nebo vývozu originálu nebo rozmnoženiny či napodobeniny díla, neoprávněného sdělování díla veřejnosti, jakož i neoprávněné propagace, včetně inzerce a jiné reklamy

c) sdělení údajů o způsobu a rozsahu neoprávněného užití, o původu neoprávněně zhotovené rozmnoženiny či napodobeniny díla, o způsobu a rozsahu jejího neoprávněného užití, o její ceně, o ceně služby, která s neoprávněným užitím díla souvisí, a o osobách, které se neoprávněného užití díla účastní, včetně osob, kterým byly předmětné rozmnoženiny či napodobeniny díla určeny za účelem jejich poskytnutí třetí osobě; práva na informace podle tohoto ustanovení se autor může domáhat vůči osobě, která do jeho práva neoprávněně zasáhla nebo je neoprávněně ohrozila, a dále zejména vůči osobě, která

1. má nebo měla v držení neoprávněně zhotovenou rozmnoženinu či napodobeninu díla za účelem přímého nebo nepřímého hospodářského nebo obchodního prospěchu

2. využívá nebo využívala za účelem přímého nebo nepřímého hospodářského nebo obchodního prospěchu službu, která neoprávněně zasahuje nebo zasahovala do práva autora nebo je neoprávněně ohrožuje nebo ohrožovala

3. poskytuje nebo poskytovala za účelem přímého nebo nepřímého hospodářského nebo obchodního prospěchu službu užívanou při činnostech, které neoprávněně zasahují do práva autora nebo je neoprávněně ohrožují, anebo

4. byla označena osobou uvedenou v bodě 1, 2 nebo 3 jako osoba, která se účastní pořízení, výroby nebo distribuce rozmnoženiny či napodobeniny díla anebo poskytování služeb, které neoprávněně zasahují do práva autora nebo je neoprávněně ohrožují

d) odstranění následků zásahu do práva, zejména

1. stažením neoprávněně zhotovené rozmnoženiny či napodobeniny díla nebo zařízení, výrobku nebo součástky z obchodování nebo jiného užití

2. stažením z obchodování a zničením neoprávněně zhotovené rozmnoženiny či napodobeniny díla nebo zařízení, výrobku nebo součástky

3. zničením neoprávněně zhotovené rozmnoženiny či napodobeniny díla nebo zařízení, výrobku nebo součástky

4. zničením nebo odstraněním materiálů a nástrojů použitých výlučně nebo převážně k výrobě neoprávněně zhotovené rozmnoženiny či napodobeniny díla nebo zařízení, výrobku nebo součástky

e) poskytnutí přiměřeného zadostiučinění za způsobenou nemajetkovou újmu, zejména
1. omluvou

2. zadostiučiněním v penězích, pokud by se přiznání jiného zadostiučinění nejevilo postačujícím; výši peněžitého zadostiučinění určí soud, který přihlédne zejména k závažnosti vzniklé újmy a k okolnostem, za nichž k zásahu do práva došlo; tím není vyloučena dohoda o narovnání

f) zákazu poskytování služby, kterou využívají třetí osoby k porušování nebo ohrožování práva autora

Právo na náhradu škody a na vydání bezdůvodného obohacení podle zvláštních právních předpisů zůstává nedotčeno; místo skutečně ušlého zisku se autor může domáhat náhrady ušlého zisku ve výši odměny, která by byla obvyklá za získání takové licence v době neoprávněného nakládání s dílem. Výše bezdůvodného obohacení vzniklého na straně toho, kdo neoprávněně nakládal s dílem, aniž by k tomu získal potřebnou licenci, činí dvojnásobek odměny, která by byla za získání takové licence obvyklá v době neoprávněného nakládání s dílem.

Dle § 43 do práva autorského neoprávněně zasahuje ten, kdo obchází účinné technické prostředky ochrany práv podle tohoto zákona.

Do práva autorského neoprávněně zasahuje také ten, kdo vyrábí, dováží, přijímá, rozšiřuje, prodává, pronajímá, propaguje prodej nebo pronájem nebo drží k obchodnímu účelu zařízení, výrobky nebo součástky nebo poskytuje služby, které
a) jsou za účelem obcházení účinných technických prostředků nabízeny, propagovány nebo uváděny na trh,
b) mají vedle obcházení účinných technických prostředků jen omezený obchodně významný účel nebo jiné užití, nebo
c) jsou určeny, vyráběny, upravovány nebo prováděny především s cílem umožnit nebo usnadnit obcházení účinných technických prostředků.

Účinnými technickými prostředky podle tohoto zákona se rozumí jakákoli technologie, zařízení nebo součástka, která je při své obvyklé funkci určena k tomu, aby zabraňovala nebo omezovala takové úkony ve vztahu k dílům, ke kterým autor neudělil oprávnění, jestliže užití díla může autor kontrolovat uplatněním kontroly přístupu nebo ochranného procesu jako je šifrování, kódování nebo jiná úprava díla nebo uplatněním kontrolního mechanismu rozmnožování.

Dle § 44 **do práva autorského zasahuje též ten**, kdo bez svolení autora způsobuje, umožňuje, usnadňuje nebo zastírá porušování práva autorského tím, že:

a) **odstraňuje nebo mění jakoukoli elektronickou informaci** o správě práv k dílu, nebo
b) rozšiřuje, dováží nebo přijímá za účelem rozšiřování, vysílá nebo sděluje veřejnosti dílo, ze kterého byla informace o správě práv nedovoleně odstraněna nebo změněna.

Informací o správě práv k dílu je jakákoli informace určená autorem, která identifikuje dílo, autora nebo jiného nositele práva, nebo informace o způsobech a podmínkách užití díla a jakákoli čísla nebo kódy, které takovou informaci

představují. Totéž platí i pro informaci, která je připojena k rozmnoženině díla nebo se objevuje v souvislosti se sdělováním díla veřejnosti.

4.2.1.1.5 Licenční smlouva

Dle § 46 licenční smlouvou autor poskytuje nabyvateli oprávnění k výkonu práva dílo užít (licenci) k jednotlivým způsobům nebo ke všem způsobům užití, v rozsahu omezeném nebo neomezeném, a nabyvatel se zavazuje poskytnout autorovi odměnu.

Smlouva vyžaduje písemnou formu, poskytuje-li se licence jako výhradní.

Výhradní nebo nevýhradní licence

Licence může být poskytnuta jako licence výhradní nebo licence nevýhradní, nestanoví-li zvláštní právní předpis jinak. Nevyplývá-li ze smlouvy jinak, má se za to, že jde o licenci nevýhradní.

V případě výhradní licence autor nesmí poskytnout licenci třetí osobě a je povinen, není-li sjednáno jinak, se i sám zdržet výkonu práva užít dílo způsobem, ke kterému licenci udělil.

V případě nevýhradní licence je autor nadále oprávněn k výkonu práva užít dílo způsobem, ke kterému licenci udělil, jakož i k poskytnutí licence třetím osobám.

Nevýhradní licence získaná nabyvatelem před následným poskytnutím výhradní licence třetí osobě zůstává zachována, pokud není mezi autorem a nabyvatelem takové nevýhradní licence sjednáno jinak.

Jeli tak sjednáno ve smlouvě, může nabyvatel oprávnění tvořící součást licence zcela nebo zčásti poskytnout třetí osobě (podlicence).

Nabyvatel může licenci postoupit pouze s písemným souhlasem autora; o postoupení licence a o osobě postupníka je povinen autora informovat bez zbytečného odkladu.

Ve smlouvě musí být dohodnuta výše odměny nebo v ní musí být alespoň stanoven způsob jejího určení.

Nabyvatel licence nesmí upravit či jinak měnit dílo, jeho název nebo označení autora, ledaže bylo sjednáno jinak, nebo jde-li o takovou úpravu či jinou změnu díla nebo jeho názvu, u které lze spravedlivě očekávat, že by k ní autor vzhledem k okolnostem užití svolil; ani v takovém případě nabyvatel nesmí dílo nebo jeho název změnit, pokud si autor svolení vyhradil i pro tyto změny a nabyvateli je taková výhrada známa. To platí obdobně i při spojení díla s jiným dílem, jakož i při zařazení díla do díla souborného.

4.2.1.1.6 Přestupky

Dle § 105 se fyzická osoba, podnikající fyzická osoba nebo právnická osoba dopustí přestupku (správního deliktu) tím, že **neoprávněně užije autorské dílo**, umělecký výkon, zvukový či zvukově obrazový záznam, rozhlasové nebo televizní vysílání nebo databázi. Za přestupek lze uložit **pokutu do výše 150 000 Kč**.

4.2.1.2 Trestní zákon

Trestní právo je v České republice upraveno trestním zákonem č. 40/2009 Sb. § 270 trestního zákona je upravuje porušení autorského práva, práv souvisejících s právem autorským a práv k databázi. Tato kapitola čerpá z [23].

Dle tohoto paragrafu kdo neoprávněně zasáhne nikoli nepatrně do zákonem chráněných práv k autorskému dílu, uměleckému výkonu, zvukovému či zvukově obrazovému záznamu, rozhlasovému nebo televiznímu vysílání nebo databázi, bude potrestán odnětím svobody až na dvě léta, zákazem činnosti nebo propadnutím věci nebo jiné majetkové hodnoty.

Odnětím svobody na šest měsíců až pět let, peněžitým trestem nebo propadnutím věci nebo jiné majetkové hodnoty bude pachatel potrestán:

a) vykazuje-li čin znaky obchodní činnosti nebo jiného podnikání
b) získá-li takovým činem pro sebe nebo pro jiného značný prospěch nebo způsobí-li tím jinému značnou škodu, nebo
c) dopustí-li se takového činu ve značném rozsahu.

Odnětím svobody na tři léta až osm let bude pachatel potrestán:

a) získá-li činem uvedeným v odstavci 1 pro sebe nebo pro jiného prospěch velkého rozsahu nebo způsobí-li tím jinému škodu velkého rozsahu, nebo
b) dopustí-li se takového činu ve velkém rozsahu.

Skutková podstata trestného činu je, jako většina skutkových podstat v oblasti tzv. hospodářského trestního práva, normou blanketní. To znamená, že její obsah je vymezen jinými odvětvími práva, v tomto případě právem autorským.

4.2.2 Strategie EU 2020

Jednou z oblastí strategie Evropské unie 2020 je tzv. „Digitální agenda pro Evropu“ ustanovená v Bruselu dne 26.8.2010, kde je věnována taktéž pozornost problematice důvěry a zabezpečení.

Evropská komise v rámci sdělení Evropskému parlamentu, radě, evropskému hospodářskému a sociálnímu výboru a výboru regionů v tomto dokumentu v rámci kapitoly s názvem „Důvěra a bezpečnost“ uvádí[13]:

„Evropané nepřijmou technologii, které nedůvěřují – digitální věk není ani „velký bratr“, ani „kybernetický divoký západ“.

Uživatelé se musí po internetu pohybovat bezpečně a jistě. Stejně jako v reálném světě, ani v počítačovém světě nemůže být trestná činnost tolerována. „

Dále uvádí:

„Přibývá také případů krádeže identity a internetových podvodů. Útoky se stávají čím dál promyšlenější a často jsou motivovány finančními zájmy.“

Vypořádat se s hrozbami a posilovat bezpečnost v digitální společnosti je společným úkolem jednotlivců, stejně jako soukromých a veřejných subjektů doma i na celém světě.

Nezbytné jsou také vzdělávací činnosti a osvětové kampaně pro širší veřejnost. V tomto ohledu může EU a členské státy vynaložit větší úsilí a například v rámci programu Bezpečnější internet (Safer Internet) poskytovat informace a vzdělání dětem

a rodinám o bezpečnosti na internetu. Je také třeba povzbudit průmysl k tomu, aby vyvíjel a zaváděl samoregulační systémy.

Účinné a rychlé provedení akčního plánu EU na ochranu kritické informační infrastruktury přinese širokou škálu opatření na ochranu sítí a informací a pro boj proti kyberkriminalitě.

V zájmu účinného boje s ohrožením bezpečnosti a ke zmírnění takových hrozeb je třeba, aby spolupráce příslušných aktérů byla organizována na celosvětové úrovni. Diskuze v tomto směru se mohou stát součástí debaty o správě internetu. V operativní rovině by se mělo přistoupit k mezinárodně koordinovaným cíleným akcím na ochranu informací a ke společné akci v boji proti počítačové kriminalitě, za podpory obnovené Evropské agentury pro bezpečnost sítí a informací (ENISA).“

V rámci sdělení Evropské komise jsou k této problematice uvedena následující opatření:

- Klíčové opatření č. 6: v roce 2010 představit opatření zaměřená na posílenou politiku bezpečnosti sítí a informací a její vysokou úroveň, včetně takových legislativních iniciativ jako modernizování Evropské agentury pro bezpečnost sítí a informací (ENISA) a opatření umožňující rychlejší reakce v případě kybernetických útoků, zahrnující skupinu pro reakci na počítačové hrozby (CERT) pro instituce EU
- Klíčové opatření č. 7: do roku 2010 představit opatření, včetně legislativních iniciativ, k potírání kybernetických útoků na informační systémy a do roku 2013 odpovídající pravidla o soudní příslušnosti v kyberprostoru na evropské i mezinárodní úrovni.

V rámci sdělení Evropské komise v oblasti „Důvěra a bezpečnost“ jsou uvedena ještě další opatření:

- do roku 2012 vytvořit evropskou platformu pro varování před kyberkriminalitou
- do roku 2011 prozkoumat možnost vytvoření evropského centra pro boj proti kyberkriminalitě
- spolupracovat se zúčastněnými stranami z celého světa zvláště na posílení globálního řízení rizik v digitálním i fyzickém světě a podnikat mezinárodně koordinované cílené akce proti kyberkriminalitě a ohrožení bezpečnosti
- od roku 2010 podporovat v celé Evropě cvičení připravenosti týkající se kybernetické bezpečnosti
- podporovat dialog se zúčastněnými stranami z různých odvětví a samoregulaci evropských i světových poskytovatelů služeb (např. platforem pro vytváření sociálních sítí, mobilních operátorů), zvláště co se týče nezletilých, kteří využívají jejich služeb.

Dále jsou uvedena opatření pro členské státy. Ty by měly:

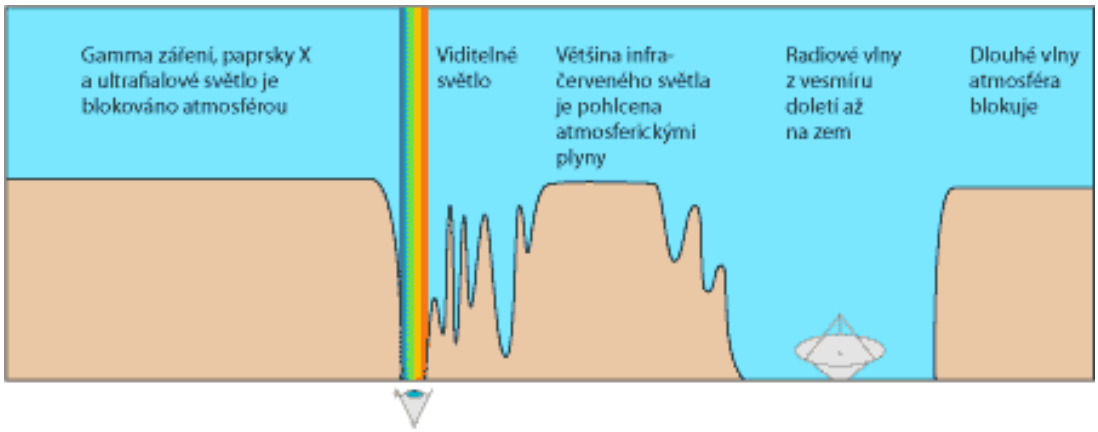
- vytvořit do roku 2012 dobře fungující síť CERT na vnitrostátní úrovni pokrývající celou Evropu
- od roku 2010 ve spolupráci s Komisí provádět simulace rozsáhlých útoků a vyzkoušet strategie zmírňování dopadů
- počínajíce rokem 2010 zřídit vnitrostátní platformy varování nebo je přizpůsobit platformě pro varování před kyberkriminalitou řízené Europolem do roku 2012.

4.2.3 Barvy a jejich vnímání lidským okem

Ač se na první pohled může zdát, že tato kapitola s tématem práce naprosto nesouvisí, je zde naprosto záměrně. Její úlohou je charakterizovat základní oblast teorie barev a jejich vnímání lidském okem. Poznatky z této kapitoly budou následně vyžity v rámci výzkumu v praktické části práce.

4.2.3.1 Teorie barevného vidění

Nejdříve je nutné uvést základní fyzikální teorii světla. Podle definice je světlo viditelná část elektromagnetického záření. Člověk je však schopen registrovat jen velmi malou část na zemi existujícího záření a ještě menší část záření existujícího ve vesmíru, jak je možné vidět z následujícího obrázku[29].

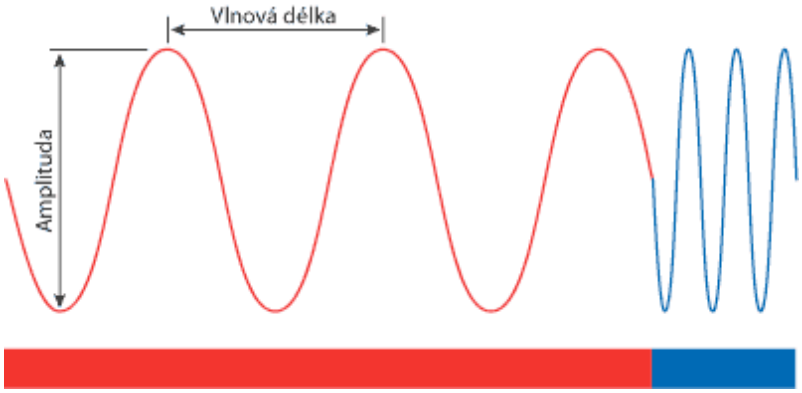


Obrázek č. 4.10 – Ukázka záření na Zemi a ve vesmíru [29]

Lidské vidění je citlivé na záření, které z celkového spektra našeho Slunce propouští zemská atmosféra. V tomto úzkém pásu se odehrává veškerý lidský vizuální svět (je možné vidět na obr. 4.10 – pouze malou část pro člověka viditelného spektra).

Základní charakteristiky světla jsou:

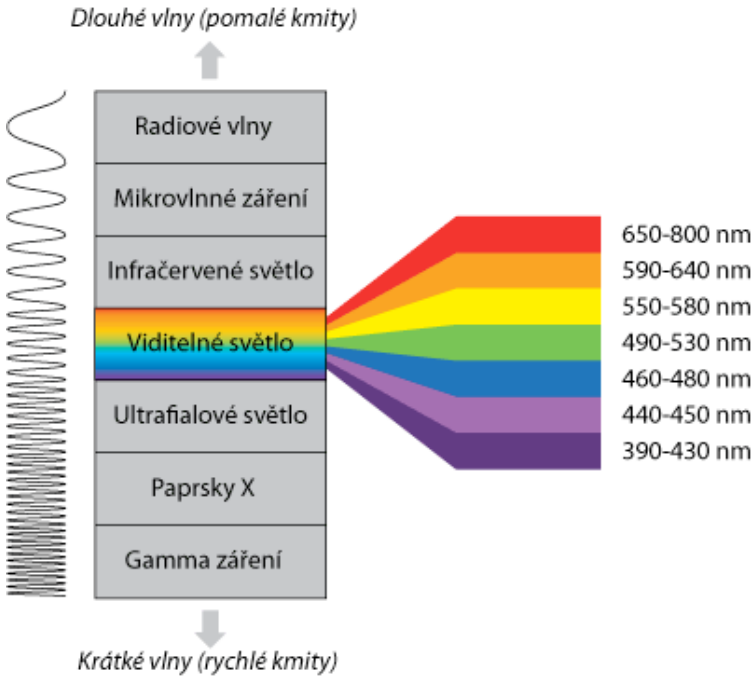
- Vlnová délka (neboli rychlost či frekvence kmitání)
- Intenzita (neboli síla či amplituda vlny)
- Polarizace (neboli směr kmitání)



Obrázek č. 4.11 – Kmitání světla a jeho charakteristiky[29]

Různé vlnové délky světla si lidé pojmenovali jako barvu světla. Každá jedna konkrétní vlnová délka světla bude okem vnímána jako jedna konkrétní barva. Barvy, které je takto možné vytvořit, jsou tzv. spektrální barvy. Spektrální barvy vytvoří známou barevnou stupnici od červené, což je barva světla, které do okem viditelné části vstupuje směrem od pomalých limitů, tedy dlouhé vlnové délky, přes žlutou a zelenou až po fialovou, kde spektrum vystupuje z viditelného rozsahu, jak je možné vidět na obrázku č. 4.12.

Jak je možné vidět z obrázku č. 4.11 rychlost kmitání světelného vlnění vnímá člověk jako barvu - pomalejší vlnění (s delší vlnovou délkou) vnímá jako červenou, kdežto rychlejší vlnění vnímá jako modrou až fialovou. Výška vlny (amplituda) odpovídá intenzitě světla, zjednodušeně řečeno jeho jasu.[29]



Obrázek č. 4.12 – Vlnové délky viditelného světla[29]

Člověk vnímá světlo zhruba od 400 do 700 nm, a tudíž vidí jen velmi malou část celkového elektromagnetického spektra. Avšak i uvnitř tohoto – z fyzikálního pohledu úzkého – spektra rozlišuje úžasné množství barev, jen pár z nich si ale i pojmenoval.

Barva v lidském smyslu

Většina reálných zdrojů světla nevysílá jen záření jedné jediné vlnové délky, ale směs různých vlnových délek. Lidské vidění přitom není schopné samostatně rozlišit jednotlivé složky spektra. Skvěle ale dokáže vnímat směs mnoha vlnových délek jako jednu barvu. Směs všech barev dohromady potom lidské oko vnímá jako bílou, tedy neutrální barvu[31].

Nespektrální barvy

Různým mícháním vlnových délek vzniká řada barev, které nikdy nemohou být vytvořeny jednou vlnovou délkou. Ty se nazývají nespektrální, protože nejsou obsaženy v čistém spektru světla. Typickými nespektrálními barvami jsou například desaturované

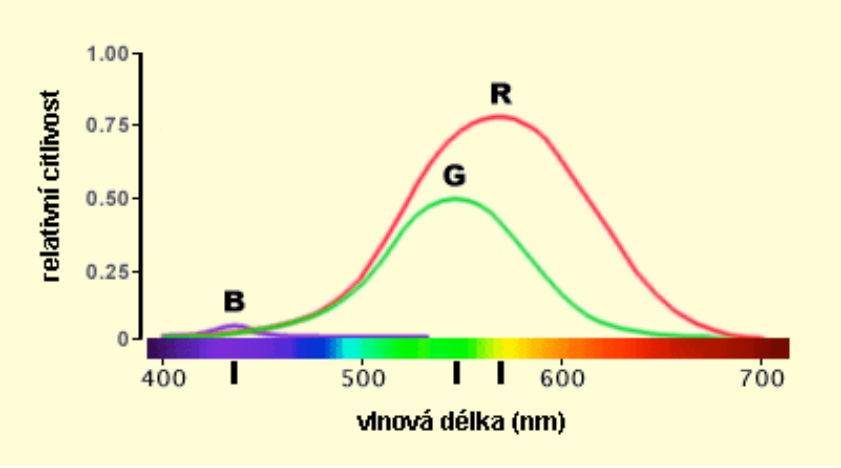
barvy, jako je šedá či bílá a např. růžová či purpurová, které jsou směsí červené a fialové z opačných konců spektra[31].

4.2.3.2 Fyziologie lidského zrakového systému

Lidské vidění je vysoce komplexní proces. I přes veškeré pokroky vědeckých znalostí v této oblasti není dosud dopodrobna známo, jak lidský zrak přesně pracuje, a to zdaleka nejen třeba co se vyšší sémantické analýzy zrakových signálů mozkem týká (tj. rozpoznávání tvarů, objektů apod.), ale i co se týká procesů, které stojí na úplném počátku vidění, neboli vidění v jeho nejprimitivnější formě – formace zrakových signálů okem[12].

Oko, a speciálně sítnice se svými světlocitlivými receptory a komplikovanými nervovými spojeními, vývojově patřící k mozku, je nesmírně složitý orgán. Popsání lidského oka není však účelem této kapitoly, zde se práce zaměří pouze na tzv. světločivné buňky – tyčinky a čípky, které se nacházejí na sítnici oka a jejichž vlastnosti jsou v rámci této práce podstatné.

Tyto buňky mají protáhlý tvar a lze si je představit tak trochu jako světelná vlákna, která vedou světlo. Barevné vidění je především záležitostí čípků, i když existují důkazy, že i tyčinky se na něm mohou za jistých okolností také částečně podílet. Barevné vidění je způsobeno tím, že existují tři druhy iodopsinu – fotoaktivního pigmentu, který čípky obsahují. Tyto pigmenty jsou spektrálně selektivní a každý druh je citlivý na poněkud jiný rozsah vlnových délek. Maximum citlivosti „modrých“ čípků se pohybuje někde kolem vlnové délky 440 nm, zatímco u „zelených“ čípků je to asi 540 nm a u „červených“ asi 570 nm. Graf přibližně zachycující spektrální citlivost jednotlivých druhů lze vidět na obrázku č. 4.13. Červené a zelené čípky jsou si navzájem hodně podobné. Vlastnosti modrých čípků jsou výrazně odlišné. V sítnici je jich mnohem méně, přibližně jen kolem 4 %. Zelených čípků je asi 32 % a zbylých 64 % je červených[36].



Obrázek č. 4.13 – Spektrální citlivost čípků[36]

Tyčinky se od čípků liší vedle rozdílné fyzické stavby a systému nervových propojení především pigmentem, který obsahují. Pigment obsažený v tyčinkách, rhodopsin, je citlivý více či méně na všechny vlnové délky viditelného spektra. Maximum citlivosti se u něj pohybuje někde kolem 500 nm. Dopadá-li na sítnici větší

množství světla, dochází k jeho kompletnímu vybělení a vidění pak zprostředkovávají pouze čípky (tzv. fotopická oblast vidění). Naopak, dolní práh citlivosti čípků je poměrně vysoký, takže za šera vidíme jen díky tyčinkám (tzv. skotopické vidění). Proto, jak ubývá světla, začínáme hůře vidět barvy, až nakonec za šera nevidíme barvy vůbec.

Tyčinek je v sítnici asi 20x více než čípků (uvádí se asi 120 miliónů tyčinek a 6 miliónů čípků) a jsou propojené ve větších skupinách. To zvyšuje citlivost zrakového vnímání při velmi nízkých hladinách světla, nicméně dochází k tomu na úkor prostorového rozlišení. Za tmy vidíme daleko méně ostře, a proto také třeba nejsme při nedostatku světla schopni číst. Dalším rysem zvyšujícím citlivosti tyčinek je i delší časová integrace dopadajícího světla. [12]

Z výše uvedených poznatků plynou následující závěry. Naprosto přesná reprodukce barev je v praxi nedosažitelná, nedostižná chiméra. Reprodukce barev může být pouze dostatečně či nedostatečně uspokojivá, což je samozřejmě ryze subjektivní hodnocení. Ačkoli si to zpravidla neuvědomujeme, tak barva ve skutečnosti není jednou z vlastností objektů kolem nás. Je pouhým výplodem našeho mozku. To, jakou barvu vidíme, závisí nejen na objektu samotném, ale na spoustě dalších faktorů - jakým světlem je nasvícený, co ho obklopuje, jaký je okamžitý stav adaptace našeho zraku, jaké jsou individuální charakteristiky našeho osobního zrakového aparátu, jestli objekt poznáváme a víme, jakou barvu má za denního světla, atd. Barvy na papírové fotce nebo na monitoru nejsou nikdy „přesně takové, jako byly ve skutečnosti“. Při reprodukci barev totiž nejde zdaleka jen o nějaké prosté okopírování barvy, ale obvykle o vytvoření zcela jiného zrakového podnětu, který se nám jeví, jako že má (aspoň přibližně) tutéž barvu, a to často navíc za zcela odlišných pozorovacích podmínek (např. reálná scéna venku versus obraz na monitoru nebo papírové fotografii prohlížené pod umělým světlem v místnosti), což situaci ještě dále komplikuje. Vzhledem k tomu, jak složitý proces barevné vidění je, modely které se při reprodukci barev v praxi používají, jsou jen velice hrubá zjednodušení, zahrnují jen ty nejzákladnější rysy zrakového systému, platí dostatečně přesně jen v jistém omezeném rozsahu pozorovacích podmínek a to ještě jen pro jakéhosi „průměrného“ diváka, od kterého se všichni více či méně lišíme.

Zajímavým poznatkem z této kapitoly je však vidění modré barvy. Dle obrázku č. 4.13 je vidění této barvy zcela odlišné od ostatních dvou barev díky odlišnosti modrých čípků. Navíc bylo uvedeno, že modrých čípků je pouze kolem 4% z celkového počtu všech čípků. Tyto uvedené fakty by měli mít za následek menší vjemovou schopnost člověka vůči modré barvě a díky tomu možnost využití tohoto poznatku v praktické části práce.

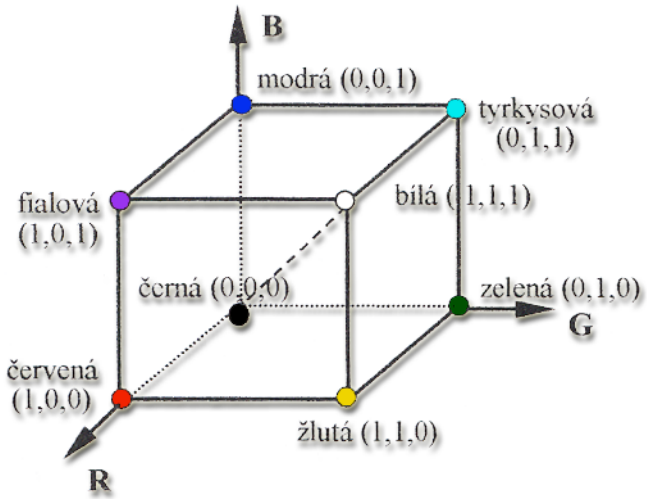
4.2.4 Model RGB

Lidské barevné vidění, zařízení na kterých jsou prezentovány veřejně přístupná data (monitory, projektory případně televize) a stejně tak nejužívanější formáty pro prezentace takovýchto dat využívají model RGB[16].

Obrázek č. 4.14 – Barevné spektrum

Barevný model RGB (Red, Green, Blue) je nejznámějším barevným modelem a je založen na třech základních barvách – červené, zelené a modré, jejichž mícháním lze získat přes 16 miliónů dalších barev, avšak ne

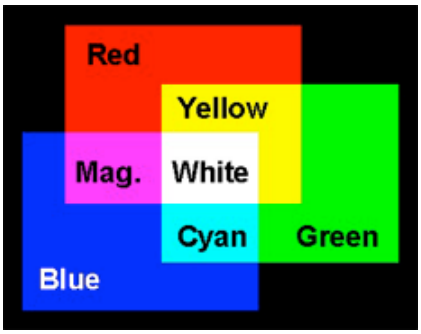
všechny barvy spektra (viz obr. č. 4.14). Tyto tři základní barvy jsou v RGB modelu dále nedělitelné. Barevný model RGB odpovídá fyziologii lidského oka, jež má na tyto tři barvy specializované receptory. Problém je však v tom, že modelem RGB ani jiným barevným modelem nelze popsat všechny barvy a odstíny, které dokáže vnímat lidské oko (lidské oko dokáže vnímat zhruba 15 000 až 60 000 odstínů každé základní barvy). Nelze tedy přesně zachytit a zobrazit čisté spektrální barvy ani některé jejich kombinace a tak již zde vzniká problém reálného zobrazení barev[15].



Obrázek č. 4.15 – Model RGB

Intenzita barev v tomto modelu se pohybuje v intervalu <0,1>. Model RGB se svým rozsahem běžně reprezentuje jako jednotková krychle umístěná v osách R, G, B, jak je vidět na obrázku č. 4.15. Z uvedeného znázornění vyplývá, že jemu odpovídající množina barev obsahuje 8 základních barev. Vrchol (0,0,0), tj. střed souřadnicového systému a odpovídá černé barvě. Opačně vrchol (1,1,1) odpovídá barvě bílé. Barvy ležící na diagonále mezi těmito vrcholy jsou odstíny šedi.

Barvy jsou v tomto systému vytvářeny aditivně, tj. přidáváním barev k barvě černé, jak je vidět na obrázku č. 4.16. Čím je přidáno více barvy, tím se výsledek více blíží k bílé. Absence základních složek dává barvu černou a naopak jejich plné zastoupení barvu bílou. Např. čistá červená je určena pouze 100 % červené a ostatní zůstávají na 0 %, tmavší odstín jedné barvy se získá snížením procenta této složky. Bílá barva je určena nastavením všech tří složek na 100 %, černá nastavením všech tří složek na 0 %.



Obrázek č. 4.16 – Aditivní vytváření barev[28]

V modelu RGB je každý prvek reprezentován třemi byty vyjadřujícími intenzitu tří barevných podílů, přičemž nejnižší intenzitě odpovídá hodnota 0 a nejvyšší 255. Tímto způsobem lze vytvořit celkem 256*256*256 = 16 777 216 kombinací (barevných odstínů).[33]

4.2.5 Vlastnosti barev

Je velmi užitečné poznat vzájemné souvislosti a vlastnosti jednotlivých barev a jak je správně používat. To však není účelem této práce. Pro tuto práci je důležité popsat alespoň základní vlastnosti barev, respektive základní složky z kterých se každá barva skládá. Tato problematika je uváděna na základě literárních zdrojů [4].

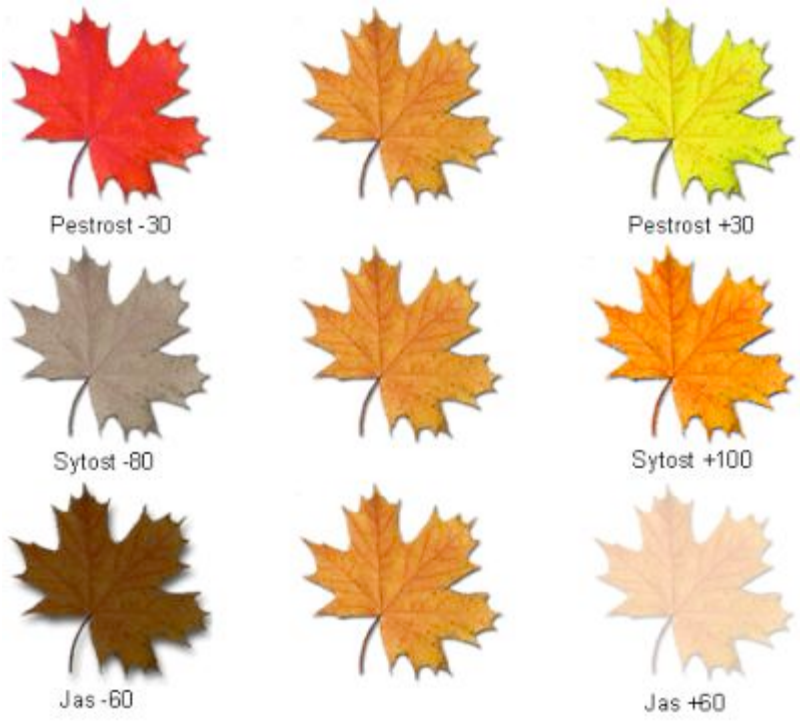
Všechny barvy se skládají ze tří základních složek:

Odstín (Hue) – je nejzřetelnější vlastností a podle něho se určují názvy barev. Každá barva spadá v rámci barevného spektra do kategorie odstínů neboli rozsahu barev.

Jas (Brightness) – určuje jasnost osvětlení barvy a její pozici ve vztahu ke stupnici šedi. Působí jako kdyby na list pokrytý daným odstínem bylo směřováno více či méně světla.

Sytost (Saturation) – určuje intenzitu odstínu. Syté barvy jsou intenzivní a tmavé, méně syté barvy jsou jakoby seprané a kalné.

Chování uvedených třech složek je možné vidět na následujícím obrázku č. 4.17, kde je znázorněna změna odstínu (neboli pestrost), sytosti a jasu.



Obrázek č. 4.17 - Barevné vlastnosti – pestrost, sytost, jas [20]

4.2.6 Obrazové formáty

Při uložení obrazu do souboru je potřeba držet se určitých pevně daných pravidel, aby jej později bylo možno opět načíst. Zmíněná sada pravidel se nazývá formát grafického souboru nebo zkráceně grafický formát.

Těchto formátů existuje několik desítek. Jednu skupinu tvoří formáty firemní, které byly vytvořeny pro různé programy, zpracovávající grafické informace. Jejich společnou nevýhodou je, že jim většinou rozumí právě a pouze program, pro nějž byly vytvořeny, případně další produkty téže firmy. Existují sice světlé výjimky, jimiž jsou například formáty BMP či PCX, které sice vznikly jako firemní, avšak jejich podpora je velmi rozšířena. Je však třeba podotknout, že zrovna tyto dva formáty jsou natolik primitivní, že jejich implementace představuje minimální úsilí. [15].

Daleko zajímavější jsou formáty univerzální. Byly zpravidla vytvořeny nezávisle na konkrétním programu jako nástroje pro výměnu grafických informací mezi nejrůznějšími programy pracujícími navíc na různých typech počítačů. Za nejvýznamnější lze považovat GIF, JPEG, TIFF a nejmladší PNG. Každý z nich má specifické vlastnosti, které do značné míry určují vhodnost jejich použití. Nevýhodou univerzálních formátů je, že zpravidla nedovedou uložit všechny vymoženosti grafického programu, který uživatel vlastní. Například GIF má omezený počet barev, JPEG je ztrátový a tak zkresluje obrázek[34].

Velké množství grafických formátů lze rozdělit do dvou již zmíněných základních kategorií podle druhu zpracovávané grafiky:

- bitmapové (rastrové, bodové) formáty grafických dat
- vektorové formáty grafických dat
- formáty umožňující kombinaci bitmapové i vektorové grafiky

Použití grafických formátů v multimediálních veřejně přístupných prezentacích představuje speciální skupinu se specifickými vlastnostmi v porovnání s klasickými grafickými formáty. Jejich nejdůležitějším kritériem, v podstatě „životní filozofií“, je velikost. Jde o to, aby použitá grafika byla co nejmenší při současném zachováním co nejlepší kvality. Pro prezentace prostřednictvím internetu je situace jasná, tvůrce se zde musí snažit optimalizovat grafiku tak, aby celková doba stažení dané stránky včetně obrázků byla co nejmenší. Pro ostatní prezentace, které nejsou určeny pro internet je však situace obdobná. Pro nezkušené tvůrce může být tento fakt zarážející. Říká si proč by mělo záležet na velikosti grafického souboru, když prezentace bude umístěna na pevném disku či na CD a nemusí se tedy nijak zdlouhavě stahovat. Odpověď je však prostá. Pokud by nebyla velikost grafických souborů optimalizována, mohlo by se například stát, že v průběhu prezentace by najednou začala animace trhat, zkrátka by najednou nestíhal počítač takový objem dat v požadovaném čase zpracovat. A tak právě z těchto důvodů se pro multimediální prezentace využívají především rastrové formáty GIF, JPEG a PNG. U vektorových formátů je situace jiná, zde se rozlišuje použití formátů pro prezentaci na internetu a mimo internet. Použití vektorových formátů mimo internet je zcela v souladu s používáním vektorových formátů v běžné praxi a je jich též celá řada. Avšak i přesto se doporučuje pro multimediální veřejně přístupné prezentace používat pouze ty vektorové formáty které dokáže zobrazit webový prohlížeč, aby nenastal problém s přenosem souboru, který nelze spustit z důvodu nepřítomnosti programu, který tento formát vytváří. Avšak pro zobrazování vektorové grafiky nebyl na internetu delší dobu akceptován všeobecně uznávaný a použitelný standard.

V posledních letech se však masově rozšířilo používání formátu SWF (Flash), který umožňuje kombinaci vektorové i bitmapové grafiky a využívá se především pro zobrazení animací.

Pro ukládání obrazových dat, především fotografií v rámci veřejně přístupných prezentací je nejrozšířenějším grafickým formátem formát JPEG. Jeho masové užívání je dáno zejména díky dosahování poměrně dobrého poměru velikosti a kvality. Navíc je to i nejrozšířenější formát, který využívají digitální fotoaparáty pro ukládání fotografií. Z těchto důvodů, ale taktéž z důvodu možnosti ochrany v rámci problematiky steganografie a digitálního vodotisku se práce bude zabývat zabezpečením právě tohoto grafického formátu. Podrobnější informace o formátu JPEG budou uvedeny v následující kapitole.

Dále bude uvedena charakteristika formátu BMP, který bude v praktické části práce využit pro ukládání vodoznaku.

4.2.6.1 JPEG

Počátky formátu JPEG se datují do roku 1990, kdy byl standardizován normou ISO, a roku 1991, kdy začal být hojně používán. Zkratka vznikla z názvu „The Joint Photographic Experts Group“. Jak je již z názvu patrné, je JPEG určen především pro ukládání fotografií nebo obecněji pro ukládání obrázků reálného světa.[38]

Pro fotografie je důležité umožnit zobrazení značného množství barev a jejich odstínů. Formát JPEG podporuje čtyřiadvacetibitovou grafiku, obrázek tedy může obsahovat až 16 777 216 barev. Všechny informace o jednotlivých barvách jsou ukládány v takzvaných RGB složkách, kdy každá barva je vyjádřena jako trojkombinace tří základních barev – červené (red), zelené (green) a modré (blue).

JPEG je grafický formát, který používá takzvanou ztrátovou komprimační metodu. U ztrátové komprese dochází ke ztrátám informace, to znamená, že data nejde obnovit přesně stejně. Uloží-li se tedy obrázek v tomto formátu, může být více nebo méně pozměněn. Tyto změny jsou prováděny tak, aby umožnily co největší komprimaci obrazových dat, ale zároveň aby byly co nejméně viditelné. Využívá se při nich specifických vlastností lidského oka, které je obecně citlivější na změny jasu, než na změny barvy. Proto si JPEG dovoluje občas nějaký ten bodík (pixel) lehce přebarvit, aby co nevíce ušetřil. Díky tomuto mechanismu, kombinovanému s komprimačním algoritmem, dokáže velmi výrazně zmenšit objem dat, nutných k reprezentaci fotorealistického obrázku. V případě formátu JPEG je možné dosáhnout komprimačního poměru 1:50 až 1:100 při zanedbatelné ztrátě informace. Většina programů, umožňujících ukládání ve formátu JPEG, nabízí nastavení kvality obrázku. Nejčastěji se zadává v podobě počtu procent.

JPEG definuje čtyři režimy činnosti, které kodér i dekodér provádí při komprimaci resp. dekomprimaci:

1. sekvenční kódování (nejméně náročné na paměť, nejpoužívanější)
2. progresivní kódování (více náročné, určeno pro přenos obrázků po síti)
3. bezeztrátové kódování (predikční kódování, není příliš známé)
4. hierarchické kódování (mnoho rozlišení, rychlé náhledy, podpora zobrazení, tisku, osvitu)

Základem komprimace vstupního číslicového signálu je transformační kódování, které převede prostorové souřadnice x, y na prostorové frekvence fx a fy. Matice signálových vzorků funkce g(x,y) se převede na matici frekvenčních koeficientů funkce G(fx,fy).

Nepříjemnou vlastností JPEG komprese je rozostřování hran. Obsahuje-li obrázek ostrý přechod dvou barev, dojde k jejich určitému promíchání a linie přechodu barev se rozmaže. To výrazně zhoršuje použitelnost JPEG pro obrázky typu perokresby či nápisů. Navíc v takových obrázcích bývají velké monotóní plochy, při jejichž ukládání není JPEG zdaleka tak efektivní jako GIF. Je bezesporu, že formát JPEG byl zkrátka navržen pro fotografie. Svůj obor zvládá velice dobře, ale za jeho hranicemi se mu příliš nedaří.

Je třeba si uvědomit, že ke snížení kvality dochází při každém uložení do formátu JPEG. Pokud obrázek již je uložen v tomto formátu, jsou v něm provedeny úpravy a znovu je uložen jako JPEG, snížení kvality se přičte k tomu, které již v obrázku bylo. JPEG je proto zcela nevhodný jako pracovní formát.

Nevýhodou formátu JPEG je, že neumožňuje průhledné části obrázku, animaci a ve své původní podobě ani nic podobného jako prokládání. Tyto nedostatky nahradila až novější varianta, tzv. progresivní JPEG. V tomto formátu je v jednom souboru obrázek uložen několikrát za sebou, vždy s rostoucí kvalitou. Na začátku je tedy uložen velmi nekvalitně, ale v malém počtu bytů. Jakmile jej klient ze sítě obdrží, je schopen zobrazit přibližnou podobu. Postupně mu ze sítě přicházejí další data a on je schopen zobrazovat přesnější a přesnější verze. Výsledkem je, že se obrázek na stránce zaostřuje.

JPEG se řídí dle standardů, kterých je několik. Za zmínku jistě stojí tzv. JPEG 2000. V oblasti komprese obrazu se stále více dostávají do popředí algoritmy založené na tzv. vlnové transformaci (Wavelet Transformation). I tento trend postih formát JPEG a vznikl tzv. JPEG 2000 založený právě na vlnové transformaci. Od tohoto standardu se očekávalo, že úspěšně nahradí originální standard, ale to se bohužel nakonec nepodařilo.[23]

Závěrem této kapitoly jsou přehledně uvedeny základní přednosti a nedostatky formátu JPEG.

Přednosti formátu JPEG jsou:

- Výborný pro fotografie a obrázky podobného charakteru (plynulé přechody barev)
- Plná barevná informace (24 bitů)
- Nastavitelná kvalita a s ní spojená velikost

Nedostatky formátu JPEG:

- Ztráta (zkreslení) části grafické informace
- Nevhodný pro kresby a nápisy
- Neefektivní pro souvislé jednobarevné plochy a obrázky malých rozměrů
- Neumí průhlednost a animaci

4.2.6.2 BMP

Formát BMP byl poprvé představen v roce 1988 jako součást nového systému OS/2 verze 1.10 SE. O něco později firma Microsoft trochu rozšířila jeho definici a zahrnula ho do svého tehdy nejprodávanějšího 16bitového grafického operačního systému MS Windows 3.0. Na počátku roku 1992 firma IBM uvedla na trhu první 32bitový systém OS/2 verze 2.0, který obsahoval vylepšenou variantu BMP s novou strukturou pro uskladnění vícenásobných bitových map v jednom souboru. Tento typ souboru se často obecně označuje jako bitmapové pole (BitMaP).

Výhodou tohoto formátu je jeho extrémní jednoduchost a dobrá dokumentovanost, navíc jeho volné použití není znemožněno patentovou ochranou. Díky tomu jej dokáže snadno číst i zapisovat drtivá většina grafických editorů v mnoha různých operačních systémech[37].

Obrázky BMP jsou ukládány po jednotlivých pixelech, podle toho, kolik bitů je použito pro reprezentaci každého pixelu je možno rozlišit různé množství barev (tzv. barevná hloubka):

- 2 barvy – 1 bit na pixel – dvoubarevné obrázky (používá se barevná paleta, nemusí se tedy jednat pouze o černobílé grafiky, ale o libovolnou kombinaci dvou barev),
- 16 barev – 4 bity na pixel (používá se barevná paleta o délce 64 bytů),
- 256 barev – 8 bitů na pixel (používá se barevná paleta o délce 1024 bytů), tyto obrázky mohou místo barev používat šedou škálu (256 odstínů šedi),
- 65 536 barev – 16 bitů na pixel,
- 16,7 milionů barev – 24 bitů na pixel – TrueColor obrázky (barevná paleta se nepoužívá, protože každý pixel je reprezentován přímo svou barvou).

Soubory ve formátu BMP většinou nepoužívají žádnou kompresi (přestože existují i varianty používající kompresi RLE – run-length encoding). Z tohoto důvodu jsou obvykle BMP soubory mnohem větší než obrázky stejného rozměru uložené ve formátech, které kompresi používají. Formát BMP je proto zcela nevhodný pro použití na Internetu, rovněž pro off-line prezentace, kde vzniká problém popisovaný v úvodu kapitoly „Obrazové formáty“.

4.3 Praktický příklad

Pro demonstraci hlavního aspektu, kterým se tato práce zabývá a který se bude snažit účinně řešit, je zde uveden praktický příklad, který jasně ukazuje na současný problém zabezpečení veřejně přístupných grafických dat.

Vezmeme-li v úvahu například fotobanky, které veřejně poskytují náhledy prodávaných fotografií. Není ojedinělou záležitostí, že grafičtí návrháři běžně stahují tyto náhledy a dále je využívají pro svá grafická díla (nejrůznější koláže, či pouze ořezy těchto náhledů), která posléze taktéž veřejně publikují.

Je sice pravda, že tyto fotobanky se často snaží označovat publikované náhledy tzv. viditelnými vodoznaky, ale upřímně řečeno častokrát naprosto neúčinně. Ve většině případů by ani pro naprostého laika nebyl problém tento vodoznak odstranit. Jako příklad jsou uvedeny následující obrázky s vloženým viditelným vodoznakem (stažené z veřejných fotobank).

Tabulka č. 4.1 – ukázka použití viditelných vodoznaků na obrázcích z různých fotobank

Z výše uvedených obrázku je jasné, že v některých případech by stačilo skutečně pouze jednoduché oříznutí (především u třetího obrázku) a hlavní motiv by zůstal zachován. Z tohoto jasně vyplývá, že nejméně účinné jsou viditelné vodoznaky v dolní či horní části obrázku nebo dokonce pouze v rozích. Naopak větší problém mohou působit vodoznaky větších rozměrů umístěné ve středu obrazu. Avšak i přes to je mnohokrát možné získat pouhým ořezem hlavní motiv (například u prvních dvou obrázků by to mohlo být poupě pivoňky a květ tulipánu).

Pokud budeme brát v úvahu zkušenější grafiky, tak jim však ani viditelný vodoznak umístěný na hlavní motiv obrázku nebude činit žádný velký problém. Jak je možné vidět na následujících třech obrázcích v kterých byl motiv vodoznaku odstraněn během pár minut.

Tabulka č. 4.2 – ukázka obrázků z fotobank, u kterých byl odstraněn viditelný vodoznak

Z výše uvedených příkladů vyplývá, že viditelný vodoznak je nedostatečným zabezpečením autorských práv a tedy v tomto případě fotobanky přicházejí o desítky až stovky tisíc.

Fotobanky nejsou však ojedinělými případy zneužívání digitálních grafických dat neboli tzv. narušením autorských práv. Mezi další případy lze uvést například oblast realitních internetových obchodů nebo různě specializované e-shopy, kde taktéž dochází k odcizování obrazových dat k jednotlivým realitám či produktům a objevují se v jiných realitních kancelářích či obchodech. Mnohdy si nikdo nedá práci ani s odstraněním viditelného vodoznaku. Takových to příkladů lze uvádět mnoho, dějí se dennodenně bez jakýchkoliv překážek a pohnutek a rozhodně nejde o legální činnost.

5 Metodika EZOD

„Nejdříve je třeba se naučit tomu, o čem píšeš, potom je třeba se naučit psát. Na jedno i druhé padne celý život.“
Ernest Hemingway

Tato stěžejní kapitola disertační práce se bude zabývat návrhem metodiky efektivního zabezpečení obrazových dat (EZOD).

Na tuto metodiku budou kladeny požadavky uvedené v rešeršní části práce a taktéž si klade dosažení určitých cílů.

5.1 Motivace pro tvorbu metodiky EZOD

V dnešní době jsou základním obchodním artiklem informace. Kdo je má, může dosáhnout úspěchu v podnikání dříve nebo lépe, kdo je nemá nebo o ně přijde, dostává se do konkurenční nevýhody. Z tohoto hlediska je nutné využívat nové manažerské a manažersko-technické přístupy v oblasti informačních a komunikačních technologiích a zajistit ochranu ekonomických vazeb na firmy, společnosti ale i jednotlivce přispívajících k zlepšení stavu ochrany veřejně přístupných dat.

V předešlé kapitole byl uveden příklad, který jasně demonstroval problematiku odcizení veřejně přístupných grafických dat. Vezmeme-li v úvahu navíc masový rozvoj sociálních sítí, digitalizace v nekomerční i komerční sféře výše popsaný problém se dostává do daleko širších rozměrů.

Jak je tedy možné digitální obrazy chránit a minimalizovat tak negativní důsledky odcizení – takové jsou otázky, které je nutné řešit v rámci veřejně distribuovaných prezentací.

V předešlých části práce byla věnována pozornost steganografii a vodoznakovým technikám. Z uvedené problematiky vyplývá možnost využití těchto technik v oblasti zabezpečení právě veřejně přístupných grafických dat. Tento fakt potvrzuje i současný rozvoj aplikací v této oblasti. Aplikace dostupné na současném trhu jsou však pro běžné nekomerční využití příliš drahé, nebo v opačném případě nejsou dostatečně ošetřeny proti různorodým útokům. Navíc neposkytují možnost implementace takovýchto metod v podnikových systémech.

Je nutné v této souvislosti však podotknout, že i drahé profesionální produkty z technického hlediska prostě nemohou poskytnout stoprocentní ochranu proti různorodým útokům. Tento fakt je zřejmý z obrázku č. 4.1, kde je možné vidět protichůdné mechanizmy, které na sebe vzájemně působí.

V rámci výše uvedených metod jsou v podstatě dva směry, jak zabezpečení veřejně přístupných dat v této souvislosti řešit. Jedním směrem se ubírají vodoznakové techniky, které využívají metod DCT (Diskrétní Cosínusová Transformace), Wavelet trasforamce a také KLT (Karhunenova - Loeveho Transformace). Tyto metody se

vyznačují vysokou robustností, avšak nízkou kapacitou (nízkou schopností vložení většího počtu dat).

Druhým směrem jsou steganografické techniky. Metoda rozkladu digitálního víceúrovňového obrazu na bitové roviny patří ke standardním steganografickým technikám. Tato metoda se ve srovnání s jinými metodami vyznačuje největší kapacitou (schopnost vložení největšího počtu vkládaných dat), její nevýhodou je však nižší robustnost (odolnost vůči ztrátovým operacím digitálního obrazu s vloženým vodotiskem). Vlastnosti této metody ale umožňují vícenásobné vkládání vodoznaku s cílem zvýšení robustnosti. Navíc, pro vícenásobné vkládání vodoznaku lze použít několik bitových rovin. Tato metoda má díky uvedeným vlastnostem velký potenciál v rámci rozvoje informačních a komunikačních technologií a jejího užití v nejrůznějších oblastech. Proto byla pro experimentální ověřování modifikací vodotiskových technik zvolena právě tato metoda.

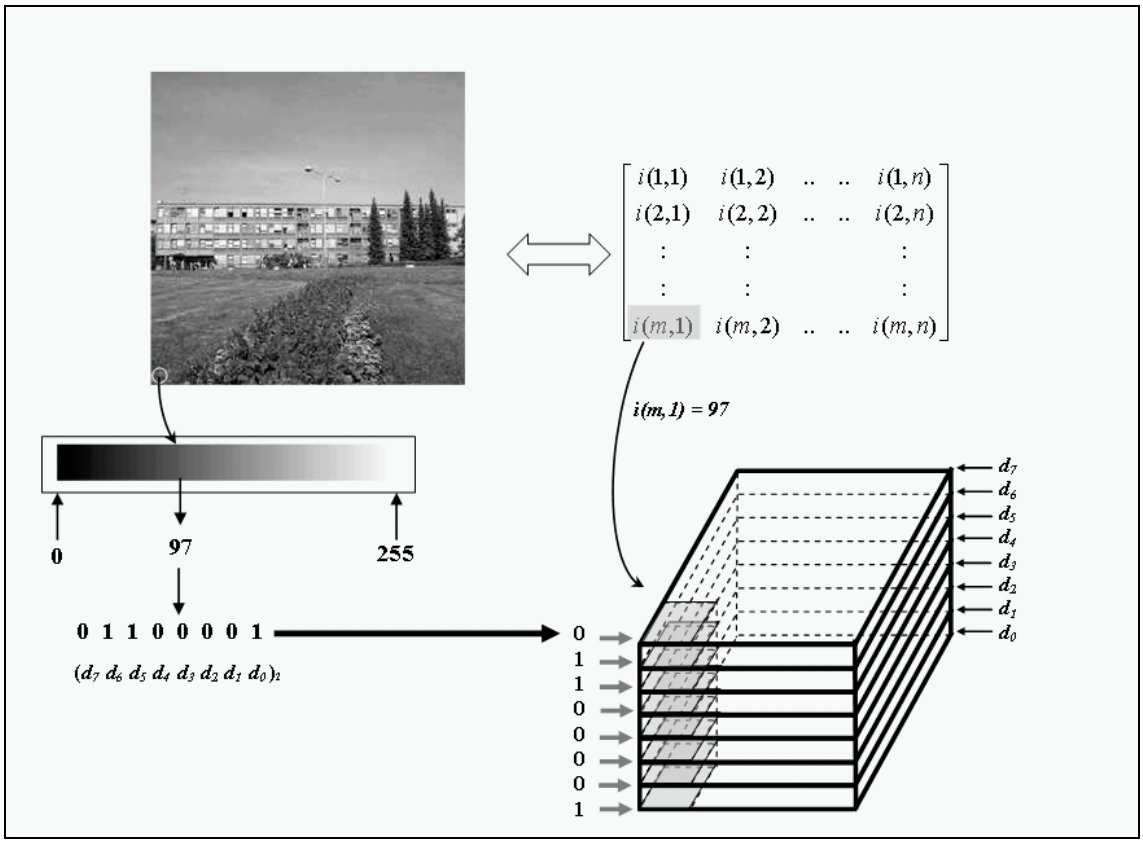
Pro názornější vysvětlení použití vybrané metody je následně uvedena ukázka rozkladu obrazu do bitových rovina a vložení samotného vodoznaku do obrazu.

5.2 Popis obecné steganografické metody

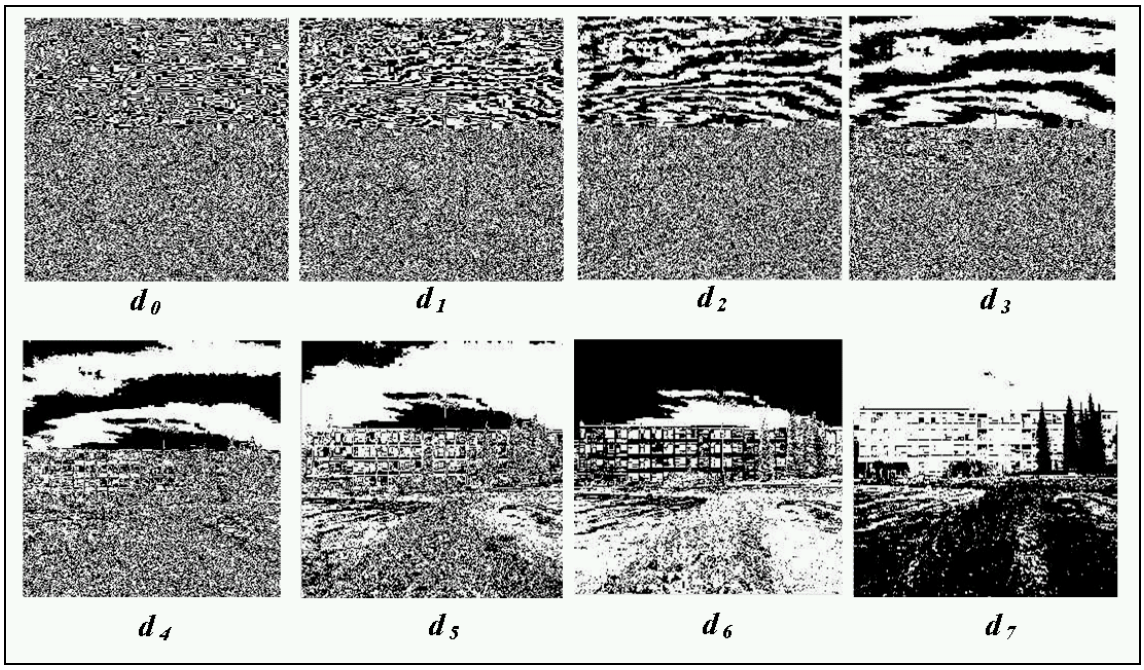
5.2.1 Rozklad obrazu do bitových rovin

Uvažujme-li zjednodušeně pro tuto ukázku pouze statický obraz s jasovou rozlišovací schopností 8 bit/op (obrazový prvek), tj. 256 jasovými úrovněmi, tedy obraz v odstínech šedi, potom tento obraz můžeme rozložit na 8 bitových rovin.

Obecný postup, jakým způsobem bude proveden rozklad statického víceúrovňového obrazu je znázorněn na obrázku č. 5.1 a ukázky binárních obrazů získaných rozkladem obrazu na bitové roviny je znázorněn na obrázku č. 5.2.



Obrázek č. 5.1 – Postup rozkladu statického víceúrovňového obrazu na bitové roviny



Obrázek č. 5.2 – Binární obrazy získané rozkladem víceúrovňového statického obrazu po bitových rovinách

Z obrázku je možné si všimnout, že informační obsah ve vyšších bitových rovinách narůstá, tzn. nejvyšší bitová rovina obsahuje nejvíce informací o vizuálním obsahu obrazu.

5.2.2 Metoda vložení vodoznaku do bitové roviny

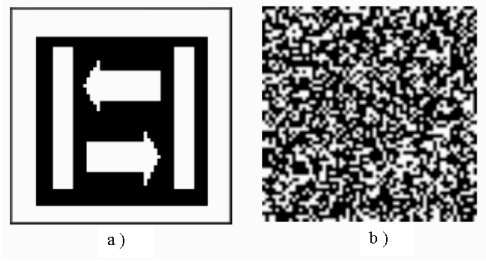
Pro jednoduchost předpokládejme vložení vodoznaku W do první bitové roviny d_0. Prostorová rozlišovací schopnost vodoznaku W je dána $m_W \times n_W$; prostorová rozlišovací schopnost originálního obrazu I je $m_I \times n_I$, proto i vybraná bitová rovina d_0 bude $m_I \times n_I$. Rozměr vodoznaku W bývá zpravidla menší, než je rozměr obrazu I, do kterého se vodoznak vkládá, proto $m_W \leq m_I$; $n_W \leq n_I$. Předpokládejme navíc, že pro vložení vodoznaku se budeme uvažovat celý obraz I, nikoliv libovolnou jeho část s rozměry $m_W \times n_W$.

Prvním krokem vložení vodoznaku W bude jeho obrazová permutace, tj. taková transformace vodoznaku W, která vykoná přeuspořádání obrazových prvků vodoznaku W použitím pseudonáhodného algoritmu. Důvodem použití pseudonáhodného algoritmu je potřeba zpětné rekonstrukce vodoznaku při jeho extrakci. Použitý pseudonáhodný algoritmus tvoří uživatelský klíč. Přeuspořádáním obrazových prvků vodoznaku W získáme permutovaný vodoznak W_p. Matematicky je možné proces permutace vodoznaku obecně popsat relací

$$W_P = \nu(W)$$

kde $\nu(.)$ je operace přeuspořádání obrazových prvků.

Názorný příklad permutovaného vodoznaku je znázorněn na následujícím obrázku č. 5.3.



Obrázek č. 5.3 – Příklad obrazové permutace vodoznaku: a) originální vodoznak; b) permutovaný vodoznak

Aby se některými ztrátovými operacemi (např. vystřižení části obrazu) vodoznak neodstranil, pro jeho vložení se využívá celá „plocha“ daná prostorovým rozlišením obrazu. To je zabezpečeno postupem, jež rozdělí selektovanou bitovou rovinu (v našem případě d_0) na vzájemně se nepřekrývající bloky, které pokryjí celou oblast (d_0). Permutovaný vodoznak W_p bude rozdělen analogicky, na stejný počet vzájemně se nepřekrývajících bloků pokrývajících celou oblast vodoznaku W_p. Přirozeně velikosti bloků v dané bitové rovině a velikosti bloků permutovaného vodoznaku nebudou stejné, nebude-li stejná velikost (prostorové rozlišení) obrazu I a vodoznaku W.

Rozdělme bitovou rovinu d_0 na h_V bloků ve vertikálním směru a h_H bloků v horizontálním směru. Požadujeme takové hodnoty h_V a h_H, aby $m = k_{I\text{-}V} h_V$ a $n = k_{I\text{-}H} h_H$, kde $k_{I\text{-}V} \times k_{I\text{-}H}$ je velikost jednoho bloku. Protože pro standardní obrazy platí $m = n$, nejčastěji bývá $k_{I\text{-}V} = k_{I\text{-}H}$ a $h_V = h_H$. Rozdělme permutovaný vodoznak W_p na stejný počet bloků v horizontálním směru (h_H) a stejný počet bloků ve vertikálním směru (h_V). Protože velikost vodoznaku není obecně stejná, jako je velikost obrazu, velikosti bloků vodoznaku nebudou stejné, jako velikosti bloku obrazu, resp. bitové roviny d_0, stejný bude jen počet bloků. Tak získáme dvojice korespondujících bloků – každému bloku bitové roviny d_0 bude odpovídat blok permutovaného vodoznaku

Vložení vodoznaku lze realizovat tak, že vybrané obrazové prvky bloku bitové roviny se modifikují podle hodnot prvků odpovídajícího bloku permutovaného vodoznaku.

Jedním z možných způsobů je pomyslné překrytí bloku bitové roviny blokem permutovaného vodoznaku (uprostřed bloku) viz. obrázek č. 5.4.

Dalším způsobem může být rozmístění prvků vodoznaku rovnoměrně do obrazu, tzn. dle velikosti vodoznaku vypočítáme počet řádků a sloupců které budeme vynechávat při vkládání viz. obrázek č. 5.5.

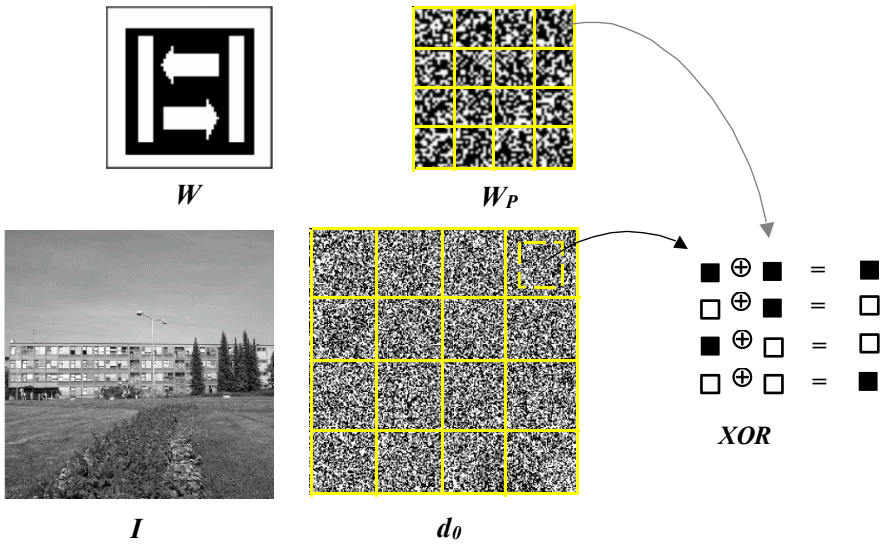
Dále je možné například vkládat vodoznak vícenásobně do obrazu – tzn. tolikrát kolikrát se do obrazu na výšku a šířku vejde.

Způsobů jak vodoznak vkládat do obrazů je mnoho. Avšak dle základních poznatků z literatury a učiněných pokusů bylo zjištěno, že vhodnější metodou jsou například první dvě výše uvedené. Třetí metoda by se mohla zdát účinnější z pohledu detekce vodoznaku a odolnosti vůči možným útokům, nicméně je nevhodná naopak z hlediska statistické detekovatelnosti, díky které by bylo dokonce možné vodoznak snadněji detekovat. Pro algoritmus v této práci dále uváděný byla vybrána a použita druhá z uvedených metod.

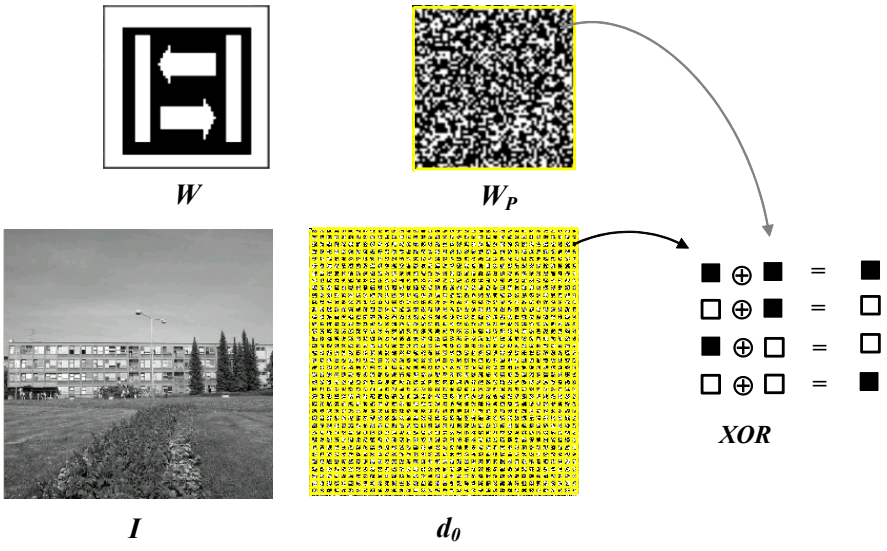
Další krokem vkládání vodoznaku je modifikaci bitové roviny vloženým vodoznakem na základě určité funkce. V literatuře je uváděna jako vhodná funkce pro tuto modifikaci funkce *XOR*.

Prvky bitové roviny v oblasti překrytí vodoznaku budou tedy modifikovány funkcí *XOR*. Příslušné hodnoty prvků bloku permutovaného vodoznaku W_P v takovém případě realizují „přirazení“: „0“ – žádná změna; „1“ – změna binární hodnoty příslušného prvku bitové roviny na převrácenou binární hodnotu (negace binární hodnoty příslušného prvku). Postup vkládání vodoznaku je znázorněn na obr. 5.4.

Takto upravená vybraná binární rovina se následně využije pro zpětné složení obrazu a vznikne výsledný obraz s vodoznakem I_W.



Obrázek č. 5.4 – Princip vložení vodoznaku v blocích



Obrázek č. 5.5 – Princip vložení vodoznaku rovnoměrným rozmístěním

5.3 Požadavky na navrhovanou metodiku

Jak již bylo uvedeno v úvodu tohoto oddílu, cílem této práce je navrhnout efektivní metodiku zabezpečení obrazových dat. Tato metodika by měla splňovat následující požadavky:

1. Poskytovat účinné zabezpečení obrazových dat.
2. Splňovat maximum požadavků na steganografické a vodoznakové systémy:

   (a) **Imperceptibilita** - změny způsobené vkládáním vodoznaku by neměly zhoršovat vnímanou kvalitu obrazu.
   (b) **Spolehlivá detekce** – vodoznak by měl představovat dostatečný a spolehlivý důkaz o vlastnictví produktu.
   (c) **Přidružený klíč** – vodoznak by měl být přidružený s tzv. klíčem vodoznaku, který je používán na sestavení, detekci a odstranění vodoznaku.
   (d) **Statistická nedetekovatelnost** – vodoznak by neměly být identifikovatelný použitím statistických metod.
   (e) **Vícenásobné vkládání vodoznaku** – algoritmus by měl umožňovat vkládání dostatečného množství rozdílných vodoznaků. Každý vodoznak by měl být detekovatelný použitím příslušného jedinečného klíče.
   (f) **Robustnost** – vodoznak použitý jako ochrana autorských práv, by měl být detekovatelný až do bodu, kdy kvalita hostitelského obrazu zůstává v akceptovatelných hranicích, tzn. měl by být imunitní (odolný) vůči neúmyslným i úmyslným operacím s daty.
   (g) **Bezpečnost** – vodoznak by neměl být extrahován z označených dat bez znalosti algoritmu vkládání a extrakce.

3. Minimalizovat důsledky odcizení obrazových dat.
4. Poskytovat jasný postup pro možnou implementaci v různorodých podnikových systémech i samostatně.
5. Umožňovat vkládání označení udělení oprávnění k dílu jiné osobě/osobám.

5.4 Východiska pro praktickou část práce

Výše popsanou obecnou steganografickou metodu, která byla vybrána pro další zpracování práce a která vytváří obecný základ metodiky EZOD, je možné v různých ohledech modifikovat.

Tyto modifikace je nutné založit na dílčích testováních, jež budou učiněny následně v praktické části práce. Nyní jsou zde uvedeny základní východiska důležitá právě pro zmíněné modifikace a postupy pro následné metodické využití.

V1: Možnosti variabilní implementace obecné metody

Pro vybranou metodu je možné využít mnoha modifikací, které se týkají:

- způsobu modifikace prvků bitové rovin
- způsobu selekce prvků bitové roviny, které mají být modifikovány
- výběru používané bitové roviny
- způsobu permutace vodoznaku

V2: Volba bitové roviny

Nejjednodušší již zmíněnou metodou kódování (vkládání vodoznaku) je tzv. LSB (Least Significant Bit = Nejméně důležitý bit). Běžné barevné schéma R,G,B, v kterém má každá barevná složka vyhrazený 1 byte, představuje možnosti pro přibližně 16 700 000 barev. Jak je patrné z kapitoly 4.2, lidské oko nedokáže tolik barev ani zdaleka rozlišit. V případě použití posledních a zároveň nejméně důležitých bitů každého n-tého bytu pro skrytí zprávy, dojde sice ke změně některých bodů, avšak je to změna natolik nepatrná a nezásadní, že lidské oko nemá šanci jí zaregistrovat a už vůbec nemůže kód odhalit a rozluštit.

Způsob kódování metodou LSB se bohužel vyznačuje tím, že není příliš odolný vůči manipulacím s obrázky. Často bývá porušen komprimací, ořízutím, úpravami barev, různými filtry apod. Každá z těchto úprav často nenávratně posune hladinu šumu za hladinu rozluštitelnosti.

Z výše uvedených důvodů je pro efektivní využití této metody nutné uvažovat vkládání vodoznaku do obrazu do dalších bitových rovin. Při vkládání do prvních čtyř bitových rovin (d_0 až d_3) bude pravděpodobně stále zabezpečena nižší vjemová viditelnost vodoznaku, vyšší kvalita obrazu s vodoznakem a nižší pravděpodobnost odstranění vodoznaku nepovolanou osobou.

Je možné však také využít i vyšších bitových rovin (d_4 až d_7), kde bude možno dosáhnout daleko nižší pravděpodobnost odstranění vodoznaku, ale bude nutné testovat imperceptibilitu obrazu a statistickou nedetekovatelnost.

V3: Vodoznak a jeho vkládání

Pro zvýšení odolnosti vodoznaku je vhodné do obrazu vkládat co největší množství informací. To může být realizované vkládáním vodoznaku s většími rozměry nebo vícenásobným vkládáním vodoznaku vždy do jiného obrazového prvku. Je to však limitované neviditelností vložené informace a statistickou nedetekovatelností. Při vkládání velmi velkého množství informací bude obraz do velké míry zkreslený, navíc se zvýší i vjemová viditelnost.

Důležitou úlohu zde hraje rovněž charakter vodoznaku, proto je nutné vytvářet vodoznak s ohledem na zvolenou metodu.

V4: Fyziologie lidského oka

Vezmeme-li v úvahu poznatky z kapitoly 4.2.3 týkající se fyziologických vlastností lidského oka, je zde možnost zajistit snížení vjemové viditelnosti vkládáním vodoznaku do vhodné barvy – v tomto případě modré. Tuto hypotézu je však nutné testovat v rámci testů imperceptiblity.

V5: Neúmyslné vs. úmyslné útoky

Vlastnost steganografických technik je zásadní v tom směru, že potencionální útočník nemá tušení o přítomnosti tajné zprávy, v tomto případě neviditelného vodoznaku. Tedy se v zásadě nepředpokládá, že by s obrazem, který je již graficky zpracován a upraven k prezentaci, prováděl nějaké zásadní manipulace, natož útoky záměrné. Avšak pro maximální odolnost metodiky EZOD bude nutné testovat i útoky úmyslné.

Výše prezentované předpoklady vycházejí z teoretické části práce a budou dále využity pro výzkumnou část práce.

5.5 Výzkumná část

V této části práce bude demonstrován postup a výsledky výzkumu při definování metodiky EZOD. Demonstrovány budou především postupy a výsledky vedoucí k pozitivním závěrům. Ostatní výsledky bude možné nalézt na přiloženém DVD.

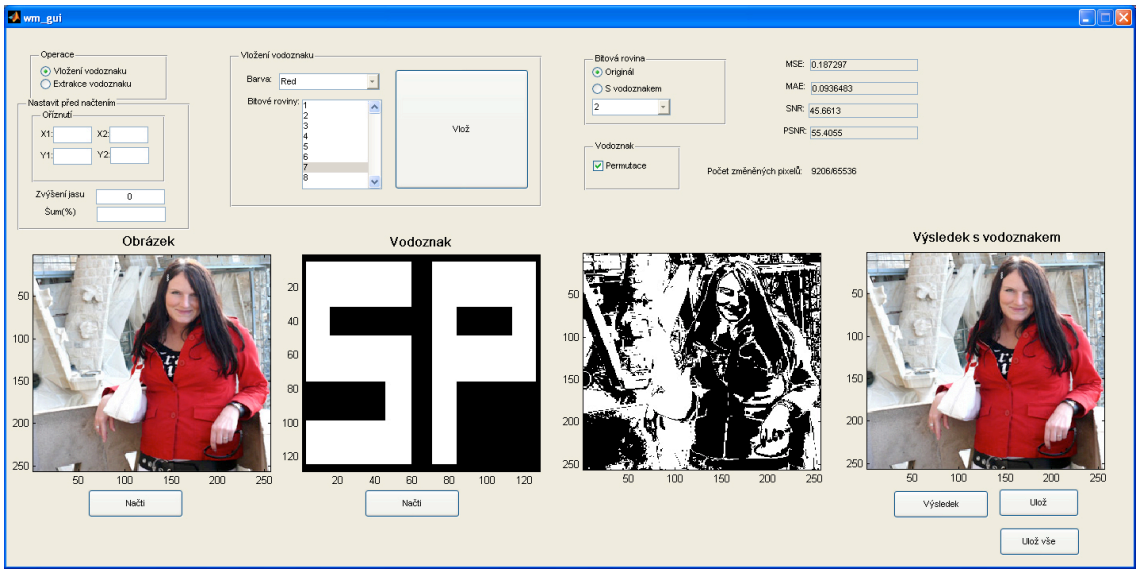
5.5.1 Použité nástroje

Výzkum řešené problematiky byl prováděn především v aplikaci zhotovené v programovém prostředí MATLAB od společnosti The MathWorks.

MATLAB je programové prostředí a skriptovací programovací jazyk pro vědeckotechnické numerické výpočty, modelování, návrhy algoritmů, počítačové simulace, analýzu a prezentaci dat, měření a zpracování signálů, návrhy řídicích a komunikačních systémů. Název MATLAB vznikl zkrácením slov MATrix LABoratory (volně přeloženo „laboratoř s maticemi“), což odpovídá skutečnosti, že klíčovou datovou strukturou při výpočtech v MATLABu jsou matice. Vlastní programovací jazyk vychází z jazyka Fortran.

Vzhledem k tomu, že v rámci dostupných knihoven program umožnuje efektivní práci s obrazovými daty a Česká zemědělská univerzita (dále ČZU) je nositelem licence tohoto programu, byl pro experimentální účely vybrán právě tento program.

Vytvořená aplikace v programovém prostředí MATLAB byla při výzkumu použita pro rozklad obrazu do bitových rovin, pro vložení a extrakci vodoznaku, pro výpočty kvalitativních ukazatelů, k simulaci útoků a v konečném důsledku k návrhu metodiky EZOD. Pracovní prostředí aplikace je znázorněno na následujícím obrázku.

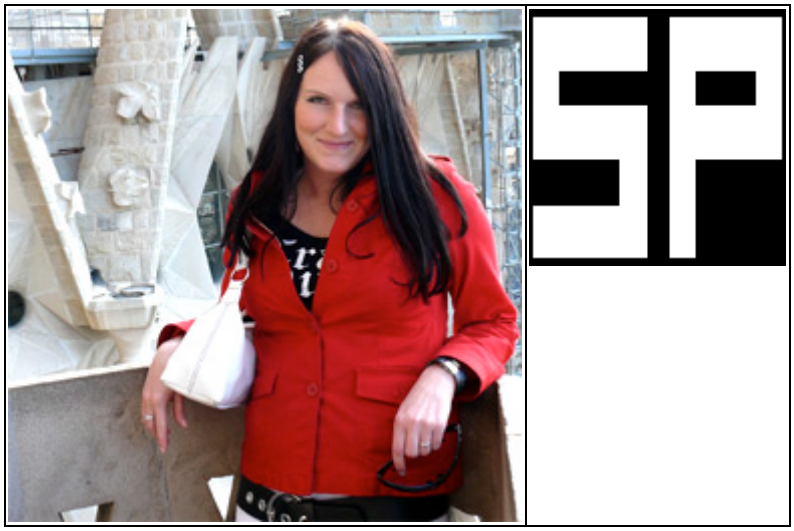


Obrázek č. 5.6 – Pracovní prostředí testovací aplikace

Pro některé další simulace útoků byl použit nejznámější profesionální grafický editor Adobe Photoshop od společnosti Adobe, který je na ČZU taktéž licencován.

5.5.2 Testovací grafické prvky

Pro valnou většinu testování byly zvoleny grafické prvky, které budou v následujících kapitolách opakovaně využívány. Tyto grafické objekty jsou zobrazeny v následující tabulce.



Tabulka č. 5.1 – Testovací grafické prvky

Pro vkládání vodoznaků byla zvolena fotografie autora práce, především z důvodu jednoznačného vlastnictví fotografie, nepopiratelnosti následných uváděných úprav a zkoumání autorem a také díky vhodným vlastnostem právě této fotografie, která není ani vyloženě vysokofrekvenční, ani nízkofrekvenční. Zvolená fotografie má nejen stejnobarevné plochy (nízkofrekvenční), ale obsahuje i mnoho detailů (vysokofrekvenční). Tzn. že je možné na jedné fotografii zkoumat a demonstrovat účinky vloženého vodoznaku na stejnobarevné plochy i na detaily.

Dále byl pro vhodnou demonstraci chování algoritmu vytvořen na základě poznatků z literatury a dílčích testování vhodný vodoznak. Vodoznak byl vytvořen z iniciálu autorova jména a úmyslně byla zvolena nízkofrekvenční povaha vodoznaku s přibližně stejným poměrem bílých a černých ploch. Důvodem jsou především dobré vlastnosti extrakce takovýchto nízkofrekvenčních vodoznaků.

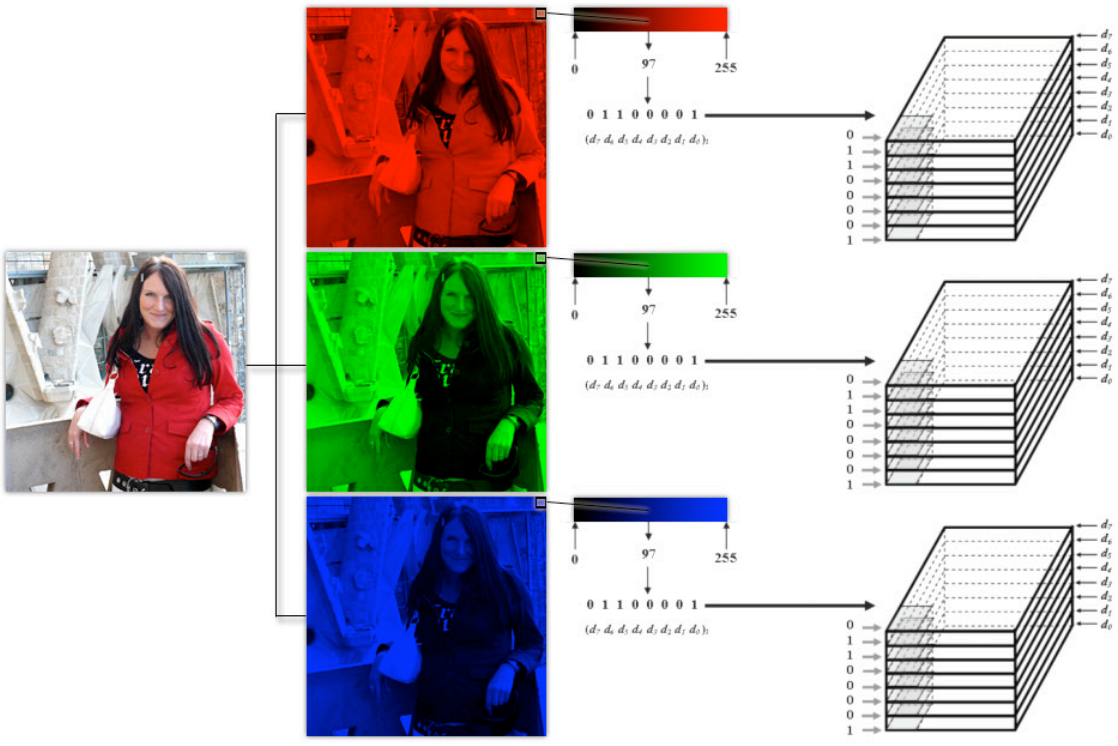
5.5.3 Rozklad obrazu a vkládání vodoznaku

V této kapitole bude demonstrován rozklad obrazu do bitových rovin a vkládání vodoznaku do jedné a následně dvou bitových rovin. Výsledky budou hodnoceny jak objektivními tak subjektivními metodami. V závěrečné části této kapitoly bude uveden výsledek testování imperceptibility při vkládání obrazu do různých bitových rovin a pro prostorové rozptýlení v několika bitových rovinách.

5.5.3.1 Rozklad a vložení vodoznaku do 1-8 bitové roviny

Tato kapitola se zabývá rozkladem obrazu do 8 bitových rovin v rámci všech barev barevného modelu RGB (R - red, G – green , B - blue), dále vložením vodoznaku do těchto rovin a výsledným obrazem získaným po vložení vodoznaku. Rovněž byly vypočteny objektivní ukazatele kvality pro každé vložení.

Rozklad obrazu uvedený v předešlé kapitole bral v úvahu jednoduchý model černobílé fotografie nikoliv fotografii barevnou. Z tohoto důvodu je následně uvedena ukázka, jakým způsobem probíhá rozklad v rámci barevného modelu RGB a tím vzniku 24 bitových rovin do kterých je možno následně vkládat vodoznak.



Obrázek č. 5.7 - Rozklad barevného obrazu do bitových rovin v modelu RGB

5.5.3.1.1 Kvalitativní ukazatele

V této části jsou vysvětleny základní charakteristiky objektivních ukazatelů kvality a následně uvedeny výsledné hodnoty při vkládání do různých bitových rovin s využitím již představených testovacích grafických prvků.

Pro objektivní analýzu kvality digitálních obrazů byla zvoleny následující uvedená kritéria.

Existuje-li digitální obraz i^+ a zkreslený digitální obraz i (oba s rastrem $N_1 \times N_2$) objektivní kritéria kvality tohoto obrazu lze vyjádřit pomocí následujících funkcí

1) Střední kvadratická chyba (*MSE - Mean Square Error*) - průměr kvadrátů rozdílů jasu obrazových prvků na příslušných pozicích.

$$MSE = \frac{1}{N_1 . N_2} \sum_{n_2=0}^{N_2-1} \sum_{n_1=0}^{N_1-1} e(n_1, n_2)^2 ,$$

kde e je odchylka rekonstruovaného obrazu $i(n_1,n_2)$ od originálu $i^+(n_1,n_2)$

$$e(n_1,n_2) = i^+(n_1,n_2) - i(n_1,n_2) ,$$

2) Střední absolutní chyba (MAE - *Mean Absolute Error*) – průměr absolutních rozdílů jasu obrazových prvků na příslušných pozicích.

$$MAE = \frac{1}{N_1 . N_2} \sum_{n_2=0}^{N_2-1} \sum_{n_1=0}^{N_1-1} \left| \; e(n_1, n_2) \; \right| ,$$

kde e je odchylka rekonstruovaného obrazu $i(n_1,n_2)$ od originálu $i^+(n_1,n_2)$

$$e(n_1,n_2) = i^+(n_1,n_2) - i(n_1,n_2) ,$$

U binárních obrazů (vodoznak) jsou MAE a MSE identické.

3) Odstup signálu od šumu (SNR – *Signal to Noise Ratio*) – odstup signálu od šumu. Šum je v podstatě míra zkreslení, která vypovídá o určité kvalitě obrazu. Velký šum ukazuje na malý odstup signálu a zároveň horší kvalitu.

$$SNR = 10 . \log_{10} \left\{ \frac{1}{\sigma} \sum_{n_2=0}^{N_2-1} \sum_{n_1=0}^{N_1-1} e\left(n_1, n_2\right)^2 \right\} ,$$

4) Vrcholový odstup signálu od šumu (PSNR - *Peak Signal to Noise Ratio*) – odstup špiček signálu od šumu.

$$PSNR = 10.\log_{10}\left\{\frac{1}{MSE}255^2\right\}.$$

Bitová rovina	MSE	MAE	SNR	PSNR
1	0.0468241	0.0468241	39.6407	61.4261
2	0.187297	0.0936483	45.6613	55.4055
3	0.749186	0.187297	51.6819	49.3849
4	2.99674	0.374593	57.7025	43.3643
5	11.987	0.749186	63.7231	37.3437
6	47.9479	1.49837	69.7437	31.3231
7	191.792	2.99674	75.7643	25.3025
8	767.167	5.99349	81.7849	19.2819

Tabulka č. 5.2 – Kvalitativní ukazatele

5.5.3.1.2 Ukázka bitových rovin

Následně je uvedena ukázka 5. a 7. bitové roviny modré barvy bez a s vloženým prozatím nepermutovaným vodoznakem a následně výsledný obraz. Ukázky všech bitových rovin této fotografie jsou uvedeny v příloze této práce (12.1), příklady dalších obrazů dále pak na přiloženém DVD.

Číslo bitové roviny	5	7
Barva	B	B
Rovina bez vodoznaku		
Rovina s vodoznakem		
Výsledný obraz		

Tabulka č. 5.3 – Ukázka bitových rovin a výsledného obrazu s vloženým vodoznakem

5.5.3.1.3 Zhodnocení a dílčí výsledky

Zhodnocení tabulkových údajů

Na základě objektivních kritérií kvality je možno vidět, že použitím 1. bitové roviny k rozložení vodoznaku dochází k nejmenší chybě (MSE, MAE) a obraz s vloženým vodoznakem má nejvyšší kvalitu (z pohledu zkreslení parametry SNR, PSNR).

Zdůvodněním tohoto jevu je skutečnost, že při binární reprezentaci mají bity 1. bitové roviny nejmenší váhu (2^0).

Zhodnocení ukázek bitových rovin a výsledného obrazu

Z ukázek rozkladu a vkládání vodoznaku do jednotlivých bitových rovin je patrné, že se kvalita výsledného obrazu postupně (od nejnižší bitové roviny k nejvyšší) zhoršuje.

Při vkládání do první až čtvrté bitové roviny není ve výsledném obrazu vodoznak viditelný v rámci všech barev (R – červená, G – zelená, B – modrá).

Dalším zajímavý výsledek poskytuje vkládání do modré barvy, kde je vodoznak vždy v rámci stejné bitové roviny méně patrný než u červené a zelené. Navíc při vložení vodoznaku do 5. a dokonce do 6. bitové roviny modré barvy je ve výsledném obrázku vodoznak stále ještě lidským okem nevnímatelný. Tento výsledek potvrzuje předpoklad vycházející z kapitoly „Fyziologie lidského zrakového systému“ (4.2.3.2).

Dílčí výsledky

Z analyzovaných podkladů vyplývá, že pro vkládání vodoznaku je výhodné při využití červené a zelené barvy vkládat vodoznak pouze do 1. až 4. roviny. U modré barvy je možné využít 1. až 6. bitovou rovinu. Je však nutné podotknout, že tento výsledek zahrnuje pouze obraz s nepermutovaným vodoznakem, kde jsou linie vodoznaku více viditelné.

Tento fakt však také částečně ovlivňuje barevnost a povaha obrázku (vysokofrekvenční, nízkofrekvenční), taktéž pak částečně povaha vodoznaku (vysokofrekvenční, nízkofrekvenční).

5.5.3.2 Vkládání vodoznaku do dvou bitových rovin zároveň

Jeden ze základních požadavků na vodoznaky je tzv. robustnost tzn. odolnost vodoznaku proti nejrůznějším modifikacím. Za účelem zvýšení robustnosti, byla konkrétní implementace algoritmus vkládání vodoznaku vytvořena tak, aby mohl být aplikován na více bitových rovin najednou. Pro ukázku byly zvoleny vždy dvě různé bitové roviny.

Tato kapitola prezentuje výsledky kvalitativních ukazatelů pro vkládání do dvou bitových rovin zároveň, dále pak ukázky výsledného obrazu po vložení do dvou bitových rovin zároveň a následně zhodnocení a dílčí výsledky.

5.5.3.2.1 Kvalitativní ukazatele

V následující tabulce jsou znázorněny výsledky kvalitativních ukazatelů pro vložení do dvou bitových rovin zároveň v rámci všech kombinací šesti bitových rovin a jednotlivých barev.

Číslo bitové roviny						Ukazatele kvality				
1	2	3	4	5	6	MSE	MAE	SNR	PSNR	
R	R					0.237376	0.0944621	46.6904	54.3764	9206/65536 = 0,1404724
G	G					0.238434	0.0947266	46.7097	54.3571	
B	B					0.240875	0.0953369	46.7539	54.3129	
R	G					0.234121	0.140472	46.6304	54.4364	
R	B									
G	R									
G	B									
B	R									
B	G									
R		R				0.79894	0.187663	51.9612	49.1057	9206/65536 = 0,1404724
G		G				0.807078	0.18868	52.0052	49.0616	
B		B				0.811717	0.18926	52.0301	49.0368	
R		G				0.79601	0.234121	51.9452	49.1216	
R		B								
G		R								
G		B								
B		R								
B		G								
R			R			3.07856	0.37678	57.8195	43.2473	9206/65536 = 0,1404724
G			G			3.05984	0.37561	57.793	43.2738	
B			B			3.05415	0.375254	57.7849	43.2819	
R			G			3.04357	0.421417	57.7698	43.297	
R			B							
G			R							
G			B							
B			R							
B			G							
R				R		12.0471	0.749603	63.7449	37.322	9206/65536 = 0,1404724
G				G		12.0699	0.750315	63.7531	37.3138	
B				B		12.0618	0.750061	63.7501	37.3167	
R				G		12.0338	0.79601	63.74	37.3268	
R				B						
G				R						
G				B						

B				R						
B				G						
R					R	48.0455	1.49917	69.7525	31.3143	9206/65536 = 0,1404724
G					G	48.0377	1.49904	69.7518	31.315	
B					B	48.1542	1.50086	69.7624	31.3045	
R					G	47.9947	1.5452	69.7479	31.3189	
R					B					
G					R					
G					B					
B					R					
B					G					
	R	R				0.947062	0.188619	52.6998	48.367	9206/65536 = 0,1404724
	G	G				0.956502	0.189799	52.7429	48.3239	
	B	B				0.953084	0.189372	52.7273	48.3395	
	R	G				0.936483	0.280945	52.651	48.4158	
	R	B								
	G	R								
	G	B								
	B	R								
	B	G								
	R		R			3.21139	0.376302	58.0029	43.0639	9206/65536 = 0,1404724
	G		G			3.19543	0.375305	57.9813	43.0855	
	B		B			3.23612	0.377848	58.0363	43.0306	
	R		G			3.18404	0.468241	57.9658	43.101	
	R		B							
	G		R							
	G		B							
	B		R							
	B		G							
	R			R		12.2771	0.752401	63.827	37.2398	9206/65536 = 0,1404724
	G			G		12.2745	0.752319	63.8261	37.2408	
	B			B		12.3077	0.753357	63.8378	37.229	
	R			G		12.1743	0.842834	63.7904	37.2764	
	R			B						
	G			R						
	G			B						
	B			R						
	B			G						
	R				R	48.1886	1.49921	69.7655	31.3014	9206/65536 = 0,1404724
	G				G	48.3553	1.50181	69.7804	31.2864	
	B				B	48.2524	1.5002	69.7712	31.2956	
	R				G	48.1352	1.59202	69.7606	31.3062	
	R				B					
	G				R					
	G				B					
	B				R					
	B				G					
		R	R			3.87093	0.382406	58.8142	42.2526	9206/65536 = 0,1404724
		G	G			3.74919	0.374797	58.6754	42.3914	
		B	B			3.88851	0.383504	58.8338	42.233	
		R	G			3.74593	0.56189	58.6716	42.3952	
		R	B							
		G	R							
		G	B							
		B	R							
		B	G							
		R		R		12.8664	0.753255	64.0306	37.0362	9206/65536 =

		G		G		13.0018	0.757487	64.076	36.9908	0,1404724
		B		B		13.0799	0.759928	64.1021	36.9648	
		R		G		12.7362	0.936483	63.9864	37.0804	
		R		B						
		G		R						
		G		B						
		B		R						
		B		G						
		R			R	48.8299	1.50045	69.8229	31.2439	9206/65536 = 0,1404724
		G			G	49.0487	1.50387	69.8423	31.2245	
		B			B	49.0695	1.50419	69.8441	31.2227	
		R			G	48.6971	1.68567	69.811	31.2558	
		R			B					
		G			R					
		G			B					
		B			R					
		B			G					
			R	R		15.6478	0.769938	64.8805	36.1863	9206/65536 = 0,1404724
			G	G		15.7077	0.77181	64.8971	36.1697	
			B	B		15.8275	0.775553	64.9301	36.1367	
			R	G		14.9837	1.12378	64.6922	36.3746	
			R	B						
			G	R						
			G	B						
			B	R						
			B	G						
			R		R	50.7155	1.49479	69.9874	31.0794	9206/65536 = 0,1404724
			G		G	52.1165	1.51668	70.1058	30.961	
			B		B	51.1686	1.50187	70.026	31.0408	
			R		G	50.9447	1.87297	70.007	31.0598	
			R		B					
			G		R					
			G		B					
			B		R					
			B		G					
				R	R	57.6849	1.46322	70.5466	30.5202	9206/65536 = 0,1404724
				G	G	65.1641	1.58008	71.0761	29.9907	
				B	B	54.1016	1.40723	70.2681	30.7987	
				R	G	59.9349	2.24756	70.7128	30.354	
				R	B					
				G	R					
				G	B					
				B	R					
				B	G					

Tabulka č. 5.4 – Kvalitativní ukazatele vkládání do dvou bitových rovin

5.5.3.2.2 Ukázka bitových rovin

V následující tabulce jsou zobrazeny ukázky pouze dvou kombinací výsledků získaných vkládáním vodoznaku do dvou bitových rovin zároveň. Některé další ukázky je možné vidět v příloze této práce (12.2), veškeré kombinace pak na přiloženém DVD.

5R6R	5B6B
	

Tabulka č. 5.5 - Ukázka výsledného obrazu po vložení vodoznaku do dvou bitových rovin zároveň

5.5.3.2.3 Zhodnocení a dílčí výsledky

Zhodnocení tabulkových údajů

Kvantitativní hodnoty míry zkreslení MSE a MAE vykazují větší chybu i nižší kvalitu, ale vzhledem k tomu, že byl vkládán stejný vodoznak na stejné pozice v různých rovinách, počet pixelů (obrazových prvků) které změnily hodnotu jasu, zůstávají stejné. Jak je patrné z tabulky, uvedeným postupem dochází k zvýšení odolnosti vloženého vodoznaku.

Zhodnocení ukázek výsledných obrazů po vložení do dvou bitových rovin zároveň

Z ukázek je patrný již známý trend zhoršující se kvality výsledného obrazu při vkládání do vyšších bitových rovin.

Současně je možné pozorovat, že kvalita se vložením dvou vodoznaků většinou nepatrně zhoršuje. Velmi zřídka je však možné pozorovat malé zlepšení – je to však závislé na určitých kombinacích barev v originálním obrazu, na kombinaci barev a vrstev do nichž je vodoznak vkládán a v neposlední řadě též na konkrétním vodoznaku a jeho vlastnostech.

Zároveň se v ukázkách vyskytuje podobný efekt jako při vkládání do jedné bitové roviny. Lze si povšimnout velmi dobrých výsledků při vkládání do modré barvy. Například podíváme-li se na ukázky 4G6G a 4R6R (viz. příloha 12.2), u výsledných

obrazů je kvalita značně zhoršená a vložený vodoznak začíná být již viditelný. Avšak v ukázce 4B6B nelze prakticky změny výsledného obrazu identifikovat. Taktéž pak lze pozorovat výborné výsledky dokonce i v ukázce 5B6B.

Zhodnocení a dílčí výsledky

Z výše uvedených výsledků plyne, že objektivní metody vykazují podobný trend jako subjektivní hodnocení. Nicméně je nutné subjektivnímu hodnocení přisuzovat větší významnost. Neboť podíváme-li se na kombinace ve stejných bitových rovinách při vkládání např. do dvou libovolných barev, výsledky jsou stále stejné. Nicméně subjektivní hodnocení hovoří o daleko lepších výsledcích při využití modré barvy. Tento jev je založen na fyziologických vlastnostech zrakového systému, kdy se skutečně potvrzuje menší citlivost na modrou barvu.

Navíc při subjektivním hodnocení obrazu je nutné si uvědomit, že zrakový systém je nelineární systém. Proto např. obraz s vyšším odstupem SNR, ale zkreslením na obrysech (hranách) se subjektivně může jevit horší v porovnání s obrazem s nižším odstupem SNR, ale se zkreslením textur (pozadí).

Z analyzovaných podkladů dále vyplývá a tím se částečně potvrzuje i předešlý výsledek, že pro vkládání vodoznaku do dvou bitových rovin a do červené a zelené barvy bude opět vhodné využívat pouze 1. až 4. roviny. U modré barvy je možné i v tomto případě využít 1. až 6. bitovou rovinu.

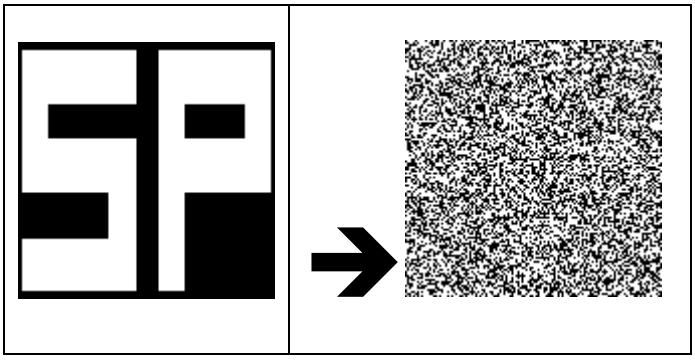
Pro další výzkum tento výsledek jednoznačně ukazuje, že vkládání do více bitových rovin je možné využít pro zvýšení odolnosti vodoznaku tzn. robustnosti. Navíc využije-li se modrá barva je možné vkládat vodoznak ještě do 5. a 6. bitové roviny a tím odolnost ještě zvýšit.

5.5.3.3 Rozklad a vložení permutovaného vodoznaku

V této kapitole bude demonstrován rozklad obrazu do bitových rovin s následným vložením permutovaného vodoznaku.

V tomto případě je nutné zajistit, aby se vodoznak do originálního obrazu nevkládal ve své původní podobě, ale byl modifikován. Modifikace spočívá v přidání tzv. permutačního algoritmu. V podstatě jde o přeuspořádání původních bodů obrazu. Proces vkládání a extrakce vodoznaku by měl toto reflektovat, tak aby byl vodoznak před vložením vždy permutován a při extrakci byla provedena zpětná permutace.

V následující tabulce je znázorněn původní vodoznak a následně jeho modifikace prostřednictvím permutačního algoritmu.



Tabulka č. 5.6 – Ukázka permutace vodoznaku

Kvalitativní ukazatele budou v tomto případě stejné jako v předešlém kapitole bez permutace, jelikož je modifikován stále stejný počet bodů.

5.5.3.3.1 Ukázka bitových rovin s permutovaným vodoznakem

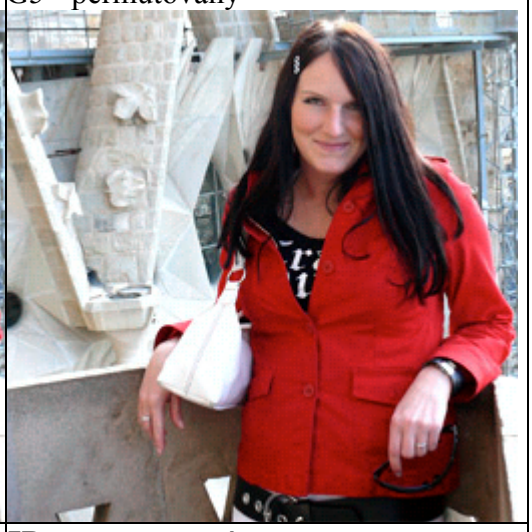
Následně je uvedena opět ukázka 5. a 7. bitové roviny modré barvy bez a s vloženým permutovaným vodoznakem a následně výsledný obraz s vodoznakem. Ukázky všech bitových rovin s permutovaným vodoznakem této fotografie jsou uvedeny v příloze této práce (12.3), příklady dalších obrazů dále pak na přiloženém DVD.

Číslo bitové roviny	5	7
Barva	B	B
Rovina bez vodoznaku		
Rovina s vodoznakem		
Výsledný obraz		

Tabulka č. 5.7. – Ukázka bitových rovin a výsledných obrazů s vloženým permutovaným vodoznakem

5.5.3.3.2 Ukázka srovnání výsledných obrazů bez a s permutovaným vodoznakem

V následující tabulce je možné vidět tři ukázky porovnání výsledných obrazů bez a s permutovaným vodoznakem. Další srovnání tohoto obrazu a jiných obrazů jsou uvedeny na přiloženém DVD.

R5 - nepermutovaný	R5 - permutovaný
	
G5 - nepermutovaný	G5 - permutovaný
	
7B - nepermutovaný	7B - permutovaný
	

Tabulka č. 5.8 - Srovnání výsledných obrazů bez a s permutovaným vodoznakem

5.5.3.3.3 Zhodnocení a dílčí výsledky

Zhodnocení ukázek výsledných obrazů vložením permutovaného vodoznaku a srovnání s nepermutovaným

Z ukázek je možné pozorovat, že kvalita výsledného obrazu se vložením permutovaného vodoznaku zlepšila. Je to dáno právě permutací nebo-li přeuspořádáním vodoznaku, tak že netvoří souvislé linie.

Lze si povšimnout velmi dobrých výsledků při vkládání do modré barvy. Například podíváme-li se na ukázky 7. bitové roviny modré barvy, ve výsledném vodoznaku není permutovaný vodoznak téměř patrný. Velmi dobrých výsledků dosahují i 5. a 6. bitové roviny zelené a červené barvy.

Podíváme-li se podrobněji na předešlé ukázky srovnání výsledných obrazů s permutací a bez permutace, je možné si všimnout následujících zlepšení:

1. V případě 5. roviny, kdy byl vodoznak vkládán do červené barvy je možné vidět velmi výrazné zlepšení, především je možné si jej všimnout na červeném kabátku, kde došlo k vyhlazení linie vodoznaku.
2. V případě 5. roviny, kdy byl vodoznak vkládán do zelené barvy, je taktéž možné si všimnout zlepšení, zejména v části obličeje a v levém dolním rohu obrázku.
3. V případě modré barvy bylo použito srovnání dokonce pro 7. bitovou rovinu, kde je v obrázku bez využití permutovaného vodoznaku, výrazně vidět linie vodoznaku, zejména ve vlasech a v levém dolním rohu obrázku. Avšak v 7. bitové rovině, kde bylo využito vložení permutovaného vodoznaku došlo k vyhlazení linií a přesto, že při detailnějším zkoumání jsou stále modifikované body viditelné, dalo by se uvažovat o využití této roviny a barvy pro praktické užití.

Zhodnocení a dílčí výsledky

Z analyzovaných podkladů vyplývá, že pro vkládání permutovaného vodoznaku lze využít vyšších bitových rovin nežli tomu bylo v předchozích ukázkách. Přesto že objektivní ukazatele vykazují stejné výsledky, subjektivně lze posoudit jednoznačné zlepšení výsledných obrazů s vodoznakem. Tzn. vkládání permutovaného vodoznaku má pozitivní vliv na výslednou kvalitu obrazu. Vkládání do 6. bitové roviny modré barvy je naprosto nepostřehnutelné. Stejně překvapivé výsledky vykazuje i 5. bitová rovina červené a zelené barvy.

Je možné dokonce uvažovat o vkládání do 7. bitové roviny modré barvy a 6. bitové roviny červené či zelené barvy. Samozřejmě použití těchto vyšších rovin bude vždy velmi závislé na konkrétním obrazu, zejména na jeho barevnosti a povaze - vysokofrekvenční či nízkofrekvenční. Bude-li však obraz pro vkládání vodoznaku vysokofrekvenční bude možné v těchto případech testovat dokonce i vyšší bitové roviny.

Obecně lze konstatovat, že ve vysokofrekvenčních částech obrazu je vodoznak vždy méně patrný, naopak u stejnobarevných ploch (nízkofrekvenční) vynikají rozdíly daleko více.

Pro další výzkum tento výsledek opět ukazuje, že vkládání do více bitových rovin je možné využít pro zvýšení odolnosti vodoznaku tzn. robustnosti.

5.5.4 Zpětná extrakce vodoznaku

Nutnou podmínkou použitelnosti a funkčnosti algoritmu je zajištění zpětné extrakce vodoznaku. Jak již bylo v teoretické části uvedeno, pro extrakci vodoznaku je nutné využít původní originální obraz, obraz s vodoznakem a samozřejmě také algoritmus, který je klíčem k získání vodoznaku.

V následující tabulce je znázorněn obraz s vloženým vodoznakem, originální obraz a výsledný vodoznak, který byl získán na základě zpětného algoritmu a obou obrazů.

Obrázek s vodoznakem vloženým do zelené barvy a do 2. bitové roviny 	
Originál 	

Tabulka č. 5.9 – Ukázka extrakce vodoznaku

Ukázka potvrzuje použitelnost a funkčnost zvoleného algoritmu pro extrakci vodoznaku.

5.5.5 Dílčí výsledky vkládání a extrakce vodoznaku

V předešlých kapitolách bylo ukázáno vkládání vodoznaku do bitových rovin a následná zpětná extrakce. Potvrzení funkčnosti tohoto algoritmu však nezajišťuje jeho použitelnost pro praxi.

Prozatím byly testovány vlastnosti imperceptibility (tzn. změny způsobené vkládáním vodoznaku) s využitím objektivních ukazatelů kvality a částečně i subjektivně. Výsledkem jsou určité hranice pro vkládání do jednotlivých barev.

Z výsledků plyne že objektivní metody vykazují podobný trend, jako subjektivní hodnocení. Nicméně díky vlastnostem zrakového systému je nutné subjektivnímu hodnocení přisuzovat větší významnost a proto by mělo být v práci dále provedeno rozsáhlejší testování imperceptibility.

Dalšími požadavky na vodoznaky jsou vícenásobné vkládání vodoznaku a tzv. přidružený klíč. Tyto požadavky byly taktéž dodrženy a splněny v předešlém výzkumu.

Ukázala se možnost zvýšení robustnosti vodoznaku s využitím vícenásobného vkládání vodoznaku. Tato možnost však musí být ověřena v následujících experimentech.

V dalších kapitolách bude nutné ověřit i další požadavky, které jsou kladeny na vodoznakové a steganografické systémy a především ověřit odolnost algoritmu proti útokům a jeho použitelnost v praxi.

Bude tedy nutné zabezpečit požadavek na statistickou nedetekovatelnost, robustnost a spolehlivou detekci (tu však samozřejmě i za podmínek provedeného/ých útoku/ů).

5.5.6 Testy odolnosti a zvyšování odolnosti algoritmu

V této kapitole budou prováděny testy odolnosti algoritmu zaměřené robustnost a spolehlivou detekci vodoznaku. Mezi tyto testy bude zařazeno testování odolnosti proti ořezu, šumu, změny jasu a ukládání obrazu do ztrátového formátu s nízkou kvalitou.

V případě nesplnění spolehlivé detekce bude kladen důraz na zlepšení vlastností algoritmu a tedy zvýšení odolnosti (robustnosti).

Následně budou provedena zkoumání statistické nedetekovaelnosti založené na porovnání histogramů.

5.5.6.1 Odolnost proti ořezu

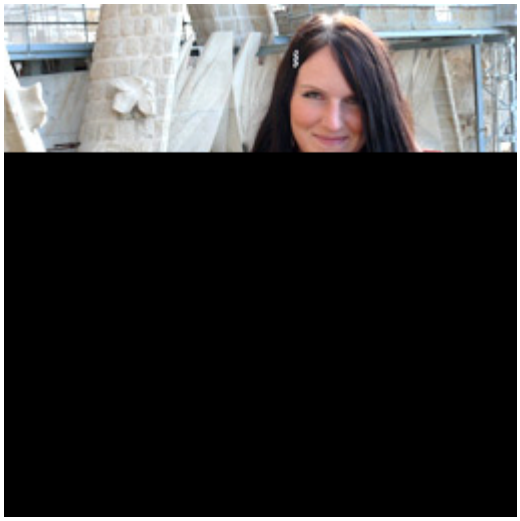
Tato kapitola se bude zabývat testováním odolnosti algoritmu proti útoku, konkrétně útokem s založeným na ořezu.

Nejdříve byl ověřen fakt nutnosti permutace vodoznaku. Není-li vodoznak permutován, jakýkoliv ořez znamená účinné narušení vodoznaku neboť nejsou z výsledné extrakce rozeznány základní obrysy vodoznaku. Tento jev je možné vidět v příloze této práce (viz. 12.4.1). Na vodoznak zapůsobil ořez vlastně stejným způsobem, jako na obrázek.

Tato kapitola dále demonstruje možnosti získání vodoznaku při různých procentech ořezu obrazu s využitím permutovaného vodoznaku.

5.5.6.1.1 Ukázka ořezu a výsledné extrakce vodoznaku

Následně je uvedena ukázka získání vodoznaku při 70% ořezu. Další ukázky je možné vidět v příloze této práce (viz. 12.4.2) či na přiloženém DVD. Pro ukázky byla využita 2. bitová roviny červené barvy.

Obrázek s vodoznakem a s ořezem 70%	
	

Tabulka č. 5.10 – Ukázka výsledku extrakce vodoznaku při 70% ořezu

5.5.6.1.2 Zhodnocení a dílčí výsledky

Výsledky testování odolnosti proti ořezu jasně znázorňují, že viditelnost extrahovaného vodoznaku se vzrůstajícím procentem ořezu snižuje, avšak je možné pozorovat že i při 80ti procentním ořezu je extrahovaný vodoznak stále ještě patrný.

Tedy na základě permutačního algoritmu je možno získat ne sice úplný vodoznak (se všemi body), ale základní obrysy a především rozeznatelnost iniciálu je čitelná.

Je nutné si ovšem uvědomit, že výsledky extrakce vodoznaku závisejí rovněž na výběru vhodného vodoznaku. V případě výběru vysokofrekvenčního vodoznaku, by výsledky byly určitě o horší (z důvodů častějších přechodů mezi bílou a černou).

Z hlediska využití je permutovaný vodoznak velmi vhodný. Nejen že díky němu získáváme lepší výsledky imperceptiblity obrazu, ale také odolnost proti ořezu až k osmdesáti procentní hranici.

5.5.6.2 Odolnost proti šumu

Odolnost proti šumu je jeden z možných útoků na digitální obrazy, kterým se útočník snaží o odstranění vodoznaku změnou náhodných bodů obrazu.

5.5.6.2.1 Ukázka odolnosti proti šumu

V této kapitole je demonstrován výsledek testování algoritmus z hlediska odolnosti proti šumu. Je zde uvedena ukázka 70% šumu a extrahovaného vodoznaku. Další ukázky 5%, 10%, 20%, 30%, 40%, 50%, 60% a 80% šumu jsou uvedeny v příloze této práce (viz. 12.4.3) nebo na přiloženém DVD.

Obrázek s vodoznakem + šum 70 %	
	

Tabulka č. 5.11 – Ukázka výsledku extrakce vodoznaku při 70% šumu

5.5.6.2.2 Zhodnocení a dílčí výsledky

Z uvedené ukázky a ukázek v příloze je patrné, že algoritmus je poměrně značně odolný i proti šumu. Lze pozorovat že při 70% šumu je extrahovaný vodoznak dobře viditelný. U 80% šumu je sice vodoznak stále částečně viditelný, ale již se postupně ztrácí.

Hranice odolnosti proti šumu se nachází mezi 70 a 80 procenty. Samozřejmě tato hranice je závislá na použitém vodoznaku.

Z hlediska praxe lze konstatovat, že algoritmus je dostatečně odolný proti útoku s využitím šumu neboť je nutno brát v úvahu, že případnému útočníkovi by s využitím 70ti procentního šumu z obrazu již příliš moc nezbylo.

5.5.6.3 Porovnání extrémního útoku s využitím šumu a ořezu

V práci byl taktéž porovnán extrémní útok s využitím šumu a ořezu. V příloze tohoto dokumentu (viz. 12.4.4) je znázorněno porovnání 80% útoku šumem a 80% útoku ořezem. Předpoklad byl, že extrahovaný vodoznak u šumu bude lépe viditelný, jelikož náhodný algoritmus nemusí nutně vybrat změněné body.

Avšak výsledek ukázal jen nepatrný, skoro neviditelný rozdíl. Tzn. útok ořezem i šumem poskytuje přibližně stejné výsledky. Samozřejmě však u šumu vždy závisí na výběru konkrétních bodů.

5.5.6.4 Odolnost proti zvýšení/snížení jasu

V této kapitole je demonstrována simulace útok snížením či zvýšením jasu a je zde uveden příklad zvýšení a snížení jasu o 140 jednotek.

Další příklady zvyšování a snižování jasu od 40 jednotek až po 200 jednotek jsou uvedeny v příloze této práce (viz. 12.4.5) nebo na přiloženém DVD.

5.5.6.4.1 Ukázka odolnosti proti zvyšování/snižování jasu

V tabulce je zobrazen obraz se sníženým jasem a se zvýšeným jasem o stejný počet jednotek – v tomto případě 140. Taktéž je zobrazen extrahovaný vodoznak.

Obrázek s vodoznakem - snížení jasu o 140 jednotek 	
Obrázek s vodoznakem - zvýšení jasu o 140 jednotek 	

Tabulka č. 5.12 – Ukázka výsledku extrakce vodoznaku při snižování a zvyšování jasu

5.5.6.4.2 Zhodnocení a dílčí výsledky

Z kompletních ukázek uvedených v příloze této práce je patrné, že algoritmus je poměrně značně odolný i proti snižování a zvyšování jasu.

Hranice odolnost proti zvyšování jasu je přibližně kolem 190 a 200 jednotek. V tomto stavu však obrázek již není téměř viditelný, tedy pravděpodobnost takto extrémního útoku je velmi nízká.

Hranice odolnosti proti snižování jasu vykazuje ještě o něco lepší výsledky. Vodoznak je zde možné získat ještě při snížení jasu o 210 až 220 jednotek. Opět je však nutné konstatovat, že obrázek je při tomto extrémním útoku již v podstatě nerozeznatelný (lze vidět pouze černý obraz). Tzn. pravděpodobnost takovéhoto extrémního útoku je opět velmi nízká.

Je nutné však konstatovat, že se občas u lichých bitových rovin nepodaří vyextrahovat vodoznak při snížení či zvýšení jasu o sudou hodnotu. Taktéž se občas u sudých bitových rovin nezdaří extrakce při snížení čí zvýšení jasu o lichou hodnotu. Tento jev se však vyskytuje velmi výjimečně. Samozřejmě by však bylo dobré i tento ojedinělý výskyt nějakým způsobem zabezpečit. Možností je vkládání vodoznaku jak do liché, tak sudé roviny.

Z hlediska dalšího výzkumu lze konstatovat, že algoritmus je dostatečně odolný proti útoku snižováním či zvyšováním jasu. Je však nutné zároveň vkládat vodoznak do liché i sudé bitové roviny.

5.5.6.5 Testování útoku opětovným ukládáním obrazu

V této kapitole bude uveden výsledek testování útoku opětovným ukládáním obrázku. Tento typ útok může na první pohled vypadat úplně nevinně, avšak přináší největší nároky na odolnost algoritmu.

Jedná se především o problémy znovu ukládání obrazových informací do formátu JPEG. Tento formát využívá ztrátovou kompresi, což zjednodušeně znamená, že při každém ukládání obrazu mění obrazové body. Tzn. v podstatě dochází k odstraňování některých částí vodoznaku.

Navíc je možné si u tohoto formátu volit kvalitu výsledného obrazu – tedy v podstatě hodnotu, dle které bude provedena komprese. Čím vyšší hodnota kvality, tím nižší komprese a tím menší ztráta jednotlivých bodů vodoznaku. A naopak čím nižší hodnota kvality, tím vyšší komprese a tím vyšší ztráta vodoznaku.

Nejčastěji se pro elektronické prezentace využívá 70% kvalita. Avšak to neznamená, že by algoritmus neměl zabezpečit zpětnou extrakci i s nižší kvalitou.

V rámci testování útoku opětovným ukládáním obrazu bylo provedeno mnoho pokusů a testování. Avšak pro přehlednost a následné zhodnocení jsou v příloze této práce (viz. 12.4.6) uvedeny pouze ty ukázky, které ke kvalitním závěrům přispívají a zároveň stanovují hranice použitelnosti bitových rovin k použité kvalitě opětovného ukládání.

Jelikož, při opětovném ukládání obrazu do formátu JPEG, dochází k přeuspořádání bodů vodoznaku do více bitových rovin (díky algoritmu komprese) bude v ukázkách zobrazena extrakce vodoznaku z více bitových rovin.

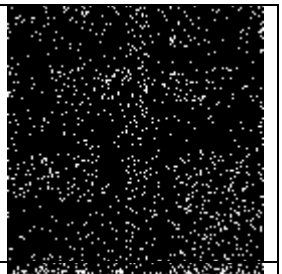
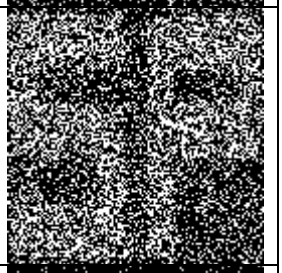
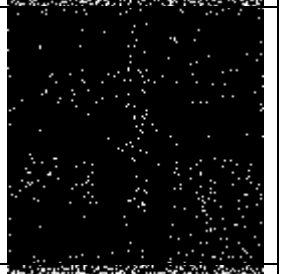
Předpokladem dalšího výzkumu a zkvalitňování extrakce vodoznaku po opětovném uložení, bylo následné vkládání vodoznaku do dvou bitových rovin zároveň v rámci jedné barvy. Na základě tohoto předpokladu byly taktéž prováděny rozsáhlá testování. Avšak původní předpoklad nebyl bohužel potvrzen a proto bude v příloze práce demonstrována jen velmi malá část tohoto experimentu, která je takzvaně jednou ze „slepých větví“, jež nemá pro tuto práci dalšího využití.

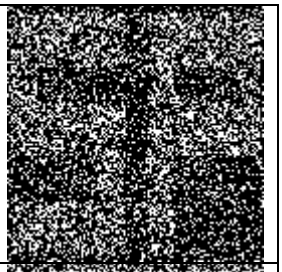
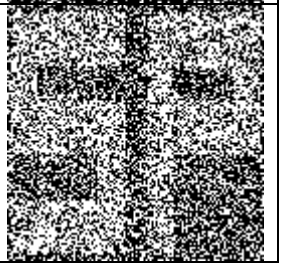
5.5.6.5.1 Ukázky testování útoku opětovným ukládáním obrazu

V rámci tohoto testování jsou zde uvedeny jen názorné ukázky některých výsledků. Ostatní ukázky, jak již bylo zmíněno výše lze nalézt v příloze této práce.

V tabulce je možné vidět použitou bitovou rovinu pro vložení vodoznaku, následné procento komprimace v rámci kterého byl obraz znovu uložen do formátu JPEG, následně pak extrakci vodoznaku z různých bitových rovin.

Ukázka extrakce vodoznaku za podmínek jeho vložení do dvou bitových rovin jedné barvy a následného znovu uložení do formátu JPEG byla z hlediska negativních výsledků umístěna pouze do příloh (viz 12.4.7).

5. bitová rovina – 55 %	Extrakce z 6. roviny	
6. bitová roviny – 55 %	Extrakce z 6. roviny	
	Extrakce z 5. roviny	
	Extrakce z 7. roviny	
6. bitová roviny – 70 %	Extrakce z 6. roviny	

7. bitová roviny – 50 %	Extrakce z 6. roviny	
	Extrakce z 5. roviny	

Tabulka č. 5.13 – Ukázky výsledků extrakce vodoznaku při opětovném ukládání obrazu

5.5.6.5.2 Zhodnocení a dílčí výsledky

Z výše uvedených ukázek a především ukázek v příloze této práce vyplývají následující poznatky. Čím je využita vyšší rovina pro vložení vodoznaku, tím je úspěšnost extrakce vodoznaku, v rámci znovu uložení a zhoršování kvality vyšší.

V úvodu této kapitoly jsem zmiňovala, že v běžné praxi se využívá pro ukládání obrázku do formátu JPEG nejčastěji 70% kvalita. To však samozřejmě neznamená, že útočník nemůže ať již neúmyslně či úmyslně uložit obrázek v horší kvalitě. Z těchto důvodů nebyly prezentovány ukázky z nižších bitových rovin (1., 2. a 3. roviny), kde při opakovaném uložení obrázku není možné zpětnou extrakcí vodoznak získat ani při ukládání s 80% kvalitou.

Pro názornou ukázku této situace byla prezentována zpětná extrakce, kdy byl vodoznak vložen do 4. bitové roviny a znovu uložen s 80% kvalitou. Z ukázek je možné pozorovat nepříjemný poznatek – ani z této bitové roviny při uložení v 80% kvalitě nebylo možné vodoznak získat v slušné kvalitě. Již o něco viditelnější vodoznak byl extrahován při ukládání v 85% kvalitě. Nicméně tyto výsledky slouží skutečně jen pro názornou ukázku a tedy nemohou být pro běžnou praxi využity.

Dále byly prezentovány ukázky zpětné extrakce při vkládání vodoznaku do 5. bitové roviny. Zde již je situace o něco lepší. Z této roviny již se podařilo vyextrahovat vodoznak, který byl poškozen opakovaným uložením s 70% kvalitou, jak je možné vidět v ukázce. Ale navíc byly zjišťovány limitní hranice, kde se podařilo vodoznak vyextrahovat i při ukládání s 55% kvalitou. V tomto případě je sice extrahovaný vodoznak ještě velmi řídký, nicméně již viditelný.

V další ukázce byla prezentována zpětná extrakce při vkládání vodoznaku do 6. bitové roviny. Zde již je situace výrazně lepší. Nejen, že z této roviny lze bez problémů vyextrahovat vodoznak, který byl poškozen opakovaným uložením s 70% kvalitou, jak je možné vidět v ukázce. Ale navíc se podařilo vodoznak vyextrahovat i při ukládání s 51% kvalitou, kdy je vodoznak jednoznačně čitelný.

V 7. bitové rovině byla situace dle předpokladu ještě daleko lepší. Zde byla zjištěna hranice pro opětovné ukládání obrázku v 35% kvalitě, kdy je možné ještě vodoznak identifikovat. Byly uvedeny i ukázky extrakce při 40 a 50% kvalitě, kde je vodoznak již bezesporu jednoznačně identifikovatelný.

Dále byly prezentovány výsledky z 8. bitové roviny, kdy však v běžné praxi již narážíme na vlastnosti imperceptibility. V této rovině bylo možno získat vodoznak již při opětovném ukládání v 20% kvalitě.

Podíváme-li se na ukázky testování zvýšení odolnosti proti opětovnému ukládání vložením vodoznaku do dvou bitových rovin jedné barvy (viz. příloha této práce 12.4.7), je možné si povšimnout, že ve většině případů se extrakce vodoznaku naopak nepatrně zhoršila. Je možné pozorovat, že v jednom případě se o něco skutečně zlepšila, ale z výzkumů, které byli prováděny je to spíše ojedinělý jev. Většinou bohužel dochází díky algoritmu JPEG komprese k nepatrnému zhoršení vlastností extrakce vodoznaku. V tomto případě je nutné konstatovat, že vícenásobné vkládání vodoznaku nezaručuje zvýšení jeho robustnosti proti útoku znovu ukládáním.

Z hlediska praxe se tedy jeví 1-4. bitové roviny v rámci opětovného ukládání obrazu bohužel zcela nepoužitelné.

Z tohoto experimentu plyne, že pro zabezpečení obrazu proti útoku znovu ukládáním do formátu JPEG (zachování vodoznaku), je nejvhodnější použít pro vkládání vodoznaku co nejvyšší rovinu. Nicméně zde musíme brát v úvahu další faktory, které nelze přehlížet. Jedná se zejména o vlastnosti imperceptibility, kdy je v podstatě u všech barev 8. bitová rovina málokdy využitelná.

Tedy pro užívání v běžné praxi lze doporučit 7., 6. a 5. bitovou rovinu. Kdy v případě využití vyšších rovin (7., 6.) je nutné testovat vlastnosti imperceptibility takto:

- u 7. bitové roviny na všechny barvy (R, G, B),
- u 6. bitové roviny na červenou a zelenou.

Ve výjimečných případech je možné využít i 8. bitovou rovinu – zejména u vysoce frekvenčních obrazů. Nicméně tento předpoklad je nutné skutečně vždy otestovat, tzn. Nelze jej procesně automatizovat.

Pro zachování zjištěných hranic opětovného ukládání obrazu je nutné si uvědomit, že vícenásobným vkládáním vodoznaku do jedné barvy, je možné naopak tyto hranice posunout ve prospěch útočníka.

5.5.6.6 Testování statistická nedetekovatelnosti

Testování statistické nedetekovatelnosti bylo v rámci tomto výzkumu prováděno srovnáváním histogramů originálního obrazu a obrazu s vodoznakem. Při tomto testování je důležité, aby se co nejvíce shodovaly porovnávané histogramy. Tzn. aby se co nejméně objevovaly zvýšené/snížené vrcholy (tzv. peaks).

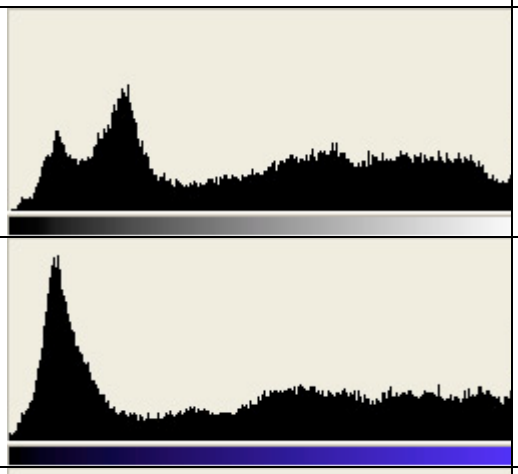
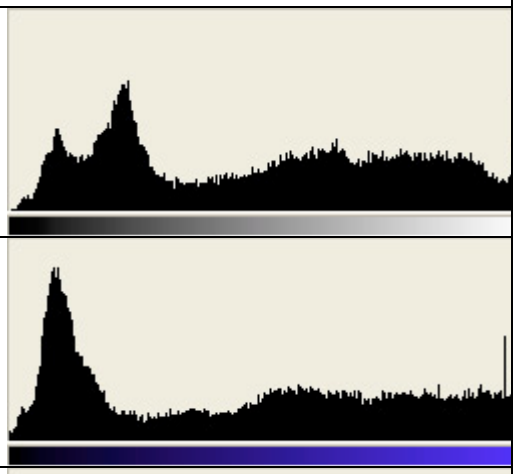
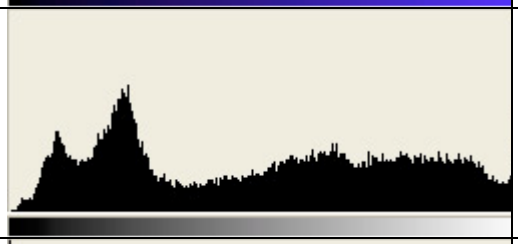
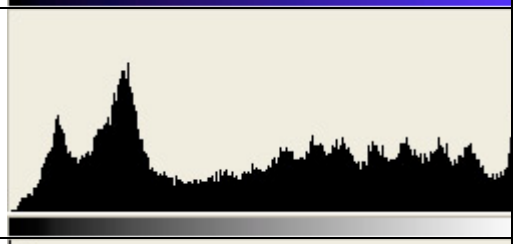
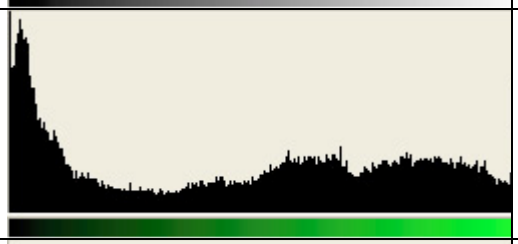
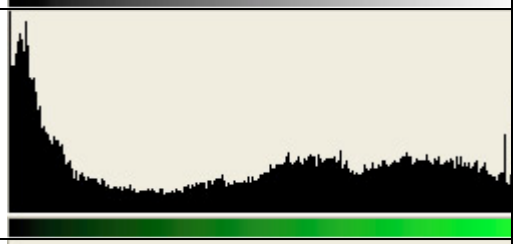
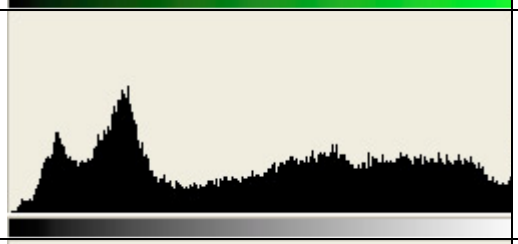
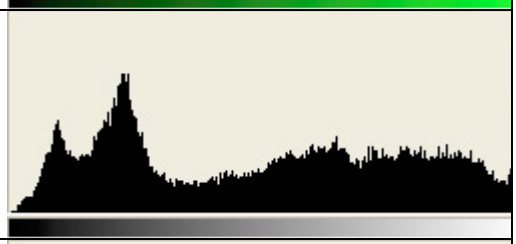
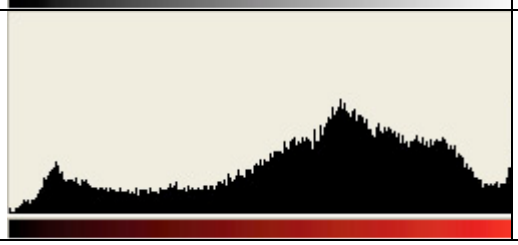
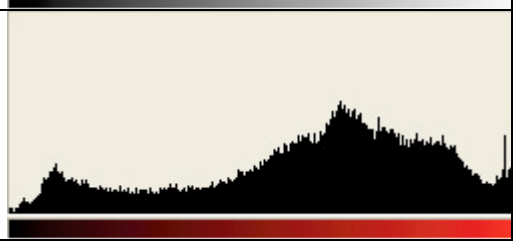
Barevný histogram reprezentuje rozložení barev v obrazu. Neboli je to graf, který pro každý jas od černé vlevo (R, G i B=0) do bílé vpravo (R, G i B=255) říká, jaká plocha obrazu (počet pixelů) jej obsahuje. Neboli říká, jaké je rozložení jasů v obraze.

V rámci demonstrace tohoto testování jsou zde uvedeny pouze některé ukázky histogramů obrazů při vkládání do jedné bitové roviny, následně ukázky histogramů obrazů při vkládání do dvou bitových rovin najednou. Další ukázky lze nalézt v příloze této práce (viz. 12.5.1, 12.5.2) nebo na přiloženém DVD.

5.5.6.6.1 Ukázky testování statistické nedetekovatelnosti při vkládání do jedné bitové roviny

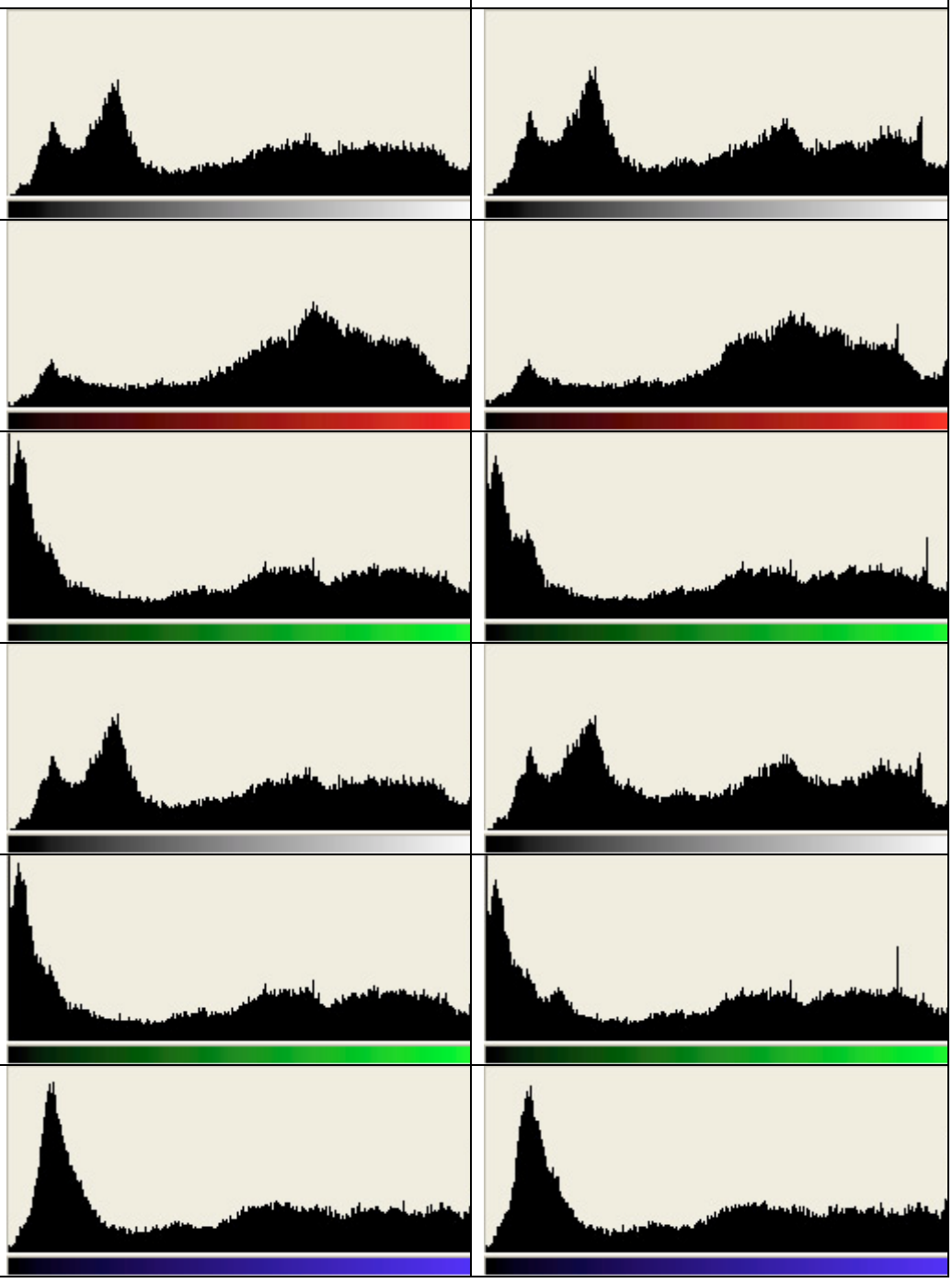
V rámci ukázky níže a samozřejmě i v rámci ukázek v příloze této práce jsou u každé bitové roviny jsou uvedeny dva histogramy – jeden je vždy za barvu, do které

byl vodoznak vkládán a druhý je výsledný histogram jasu (luminocity), který zahrnuje veškeré změny v obrazu.

Rovina / Barva	Histogram originálního obrazu	Histogram obrazu s vodoznakem
4B		
4G		
		
4R		
		

Tabulka č. 5.14 – Ukázky histogramů originálního obrazu a obrazu s vodoznakem při vkládání do jedné bitové roviny

5.5.6.6.2 Ukázky testování statistické nedetekovatelnosti při vkládání do dvou bitových rovin zároveň

Rovina / Barva	Histogram originálního obrazu	Histogram obrazu s vodoznakem
5G6R		

Tabulka č. 5.15 - Ukázky histogramů originálního obrazu a obrazu s vodoznakem při vkládání do dvou bitových rovin

5.5.6.6.3 Zhodnocení a dílčí výsledky

Z předešlých ukázek a ukázek v příloze této práce vyplývá:

1. Při vkládání vodoznaku do 1. až 3. bitové roviny lze v uvedených histogramech pozorovat pouze velmi malé nevýrazné změny.
2. Od 4. bitové roviny se začínají vyskytovat výraznější rozdíly v podobě tzv. peaks. Tohoto efektu si lze všimnout např. u histogramů 4B u modré barvy nebo 4G u zelené barvy. Výsledné změny se následně již v některých případech projevují výrazněji v celkovém histogramu luminocity (jasu) – např. u roviny 4G histogramu luminocity.
3. Se zvyšováním bitových rovin se dle předpokladu efekty zvyšování vrcholů nepatrně zhoršují.

Dle těchto zjištění se dalo předpokládat, že při několikanásobném vkládání do jedné barvy, se změny v histogramu této barvy ještě zvýrazní a následně se zvýrazní i ve výsledném histogramu luminocity. Taktéž pak při několikanásobném vkládání do více barev, se dalo předpokládat zvýraznění těchto změn ve výsledném histogramu luminocity. Z těchto důvodů obsahují ukázky i vkládání do dvou bitových rovin zároveň. Z ukázek následně vyplývá potvrzení uvedených předpokladů. Nicméně změny peaks v histogramech sice jsou nepatrně větší, ale při srovnání s vkládáním do jedné bitové roviny ne příliš výrazněji.

I když je statistická nedetekovatelnost jedním z požadavků na vodoznaky, je nutné si uvědomit, že ji lze provádět bez znalosti původního obrazu velmi obtížně. Jedinou možností se pak stává pro potencionálního útočníka analýza více obrazů s vloženým vodoznakem a na jejich základě odhalení změn. Avšak tento postup je poměrně obtížný a současně nezaručuje úspěšnost výsledku.

V rámci zabezpečení statistické nedetekovatelnosti pro praxi je možné doporučit využívání nižších bitových rovin a při vkládání do více rovin využít raději více barev aby se výsledná změna co nejvíce rozptýlila. Samozřejmě však využití nižších bitových rovin je na úkor zvyšování robustnosti (odolnosti) vodoznaku proti ostatním typům útoku. Je proto pak na zvážení, zda najít jakousi optimální úroveň statistické nedetekovatelnosti a robustnosti vodoznaku, nebo se snažit o maximální robustnost na úkor statistické nedetekovatelnost.

V praxi je samozřejmě však daleko více útočníků na robustnost (útok ořezem, šumem, jasem, znovu uložením apod.) než na statistickou detekci, proto bych v rámci dalších postupů doporučila spíše druhou variantu. Už jen proto, že statistická detekce obrazu je velmi náročná a nelze ji provést manuálně (jako u některých útoků na robustnost), ale naopak vyžaduje hlubší znalosti (programování, náročné matematické postupy) a navíc ani tato znalost nezaručuje výslednou úspěšnost.

Dále je pak možno pro praxi doporučit vkládání dvou rozdílných vodoznaků do různých bitových rovin, kdy tím můžeme dosáhnou většího rozptýlení změn a tím zvýšení statistické nedetekovatelnosti.

5.5.6.7 Dílčí testy odolnosti

V této kapitoly budou zmíněny další prováděná testování, které vzhledem k výsledkům není nezbytné uvádět samostatně.

Mezi další prováděné testy lze uvést testování odolnosti algoritmu proti rotaci a změně velikosti obrazu. Výsledky těchto testů jsou bohužel negativní a proto nebyly uvedeny v samostatné kapitole.

Nicméně je nutné uvést, že prezentované obrazy jsou ve většině případů upraveny do „dokonalosti“, proto není třeba provádět jakékoliv modifikace. Běžný uživatel tedy většinou s obrazem již nikterak nemanipuluje.

Útoky tohoto typu jsou ve většině případů úmyslné cílené útoky na odstranění neviditelných vodoznaků. V případě rotace je útok prováděn často otočením obrazu o pár stupňů, právě z důvodu narušení extrakce vloženého vodoznaku. V případě změny velikosti je situace obdobná, opět je prováděn útok zvětšením či zmenšením obrazu o pár obrazových bodů.

Prozatím byly v práci uváděny a testovány především útoky na robustnost, jejichž cílem je poškodit nebo zcela znehodnotit vodoznak. Nyní považuji za důležité zmínit také útoky prezentační, interpretační a právní.

Prezenční útoky se nesnaží vodoznak odstranit nebo poškodit, ale provádět útok například rozdělením obrazu na malé části. Pokud však chceme přeci jen vodoznak detekovat, není problém obraz zpětně složit, či detekovat vodoznak z oříznuté části obrazu.

Interpretační útoky jsou založeny na vložení falešného vodoznaku. V tomto případě se může snažit útočník vydávat za majitele originálního obrazu. Tento případ je ale možné eliminovat, neboť skutečný majitel má ve většině případů originální obraz bez vodoznaku a navíc ještě obraz v původní nezmenšené (velikostně) či nekomprimované (do formátu JPEG) kvalitě a tím je možné interpretační útoky dokazovat.

Právní útoky jsou netechnické útoky využívající nedokonalosti zákonných ochran autorských práv. O právní útok se jedná také v případě, kdy vlastník originálních dat sice dokáže extrahovat vložený vodoznak, ale soud to nepovažuje za důkaz vlastnictví. V souvislosti s legislativou byl v práci uveden výňatek z autorského a trestního práva. Český právní řád se řídí těmito zákony a extrahovaný vodoznak by měl být považován za dostatečný důkaz vlastnictví.

V rámci shrnutí této kapitoly je nutno uvést následující dílčí závěry. Navržený algoritmus není odolný proti útoku rotací a změně velikosti obrazu. Naopak se však není třeba obávat prezentačních, interpretačních či právních útoků.

5.5.7 Shrnutí testování odolnosti algoritmu

V předešlých kapitolách byly provedeny nejrůznější testy odolnosti. Byla testována odolnost proti ořezu, provedeny testy odolnosti proti šumu, zvyšování a snižování jasu, testy proti útoku opětovným ukládání obrazu a v neposlední řadě testy statistická nedetekovatelnosti.

V rámci těchto testování byly zjištěny následující výsledky:

- permutovaný vodoznak je nutností pro
  - zabezpečení odolnosti proti ořezu
  - pro zlepšení výsledků imperceptibility
- odolnost proti ořezu – až k 80ti procentům
- odolnost proti šumu – až k 80ti procentům
- odolnost proti zvyšování jasu – až k hranice 200 jednotek
- odolnost proti snižování jasu – až k hranici 220 jednotek
- nutnost vkládání vodoznaku do liché a sudé roviny pro záruku předešlých dvou bodů
- odolnost proti znovu uložení obrazu do ztrátového formátu JPEG
  - v 8. bitové rovině až k hranici 20% ztrátové komprese
  - v 7. bitové rovině až k hranici 35% ztrátové komprese
  - v 6. bitové rovině až k hranici 51% ztrátové komprese
  - v 5. bitové rovině až k hranici 55% ztrátové komprese
- vícenásobné vkládání vodoznaku do jedné barvy nezaručuje zvýšení robustnosti proti útoku znovu ukládáním do ztrátového formátu JPEG
- odolnost proti statistické nedetekovatelnosti bude však částečně narušena
- algoritmus není odolný proti útoku rotací obrazu a změny velikosti obrazu
- prezentační a interpretační útoky by neměly znemožnit extrakci vodoznaku
- dle českého právního řádu by extrahovaný vodoznak měl být považován za dostatečný důkaz vlastnictví – tzn. právní útoky by neměly ohrozit použití tohoto algoritmu

V rámci všech těchto kapitol byly popsány výsledky výzkumu a jejich využití v praxi. Následně bude v dalších kapitolách popsána konkrétní implementace výsledného algoritmu a na základě uvedených testování navrhnut konkrétní metodický postup pro co nejefektivnější zabezpečení obrazových dat.

5.5.8 Testování imperceptibility

Vzhledem k předešlým testováním je nutné ověřit nevnímatelnost vodoznaku při vkládání do vyšších bitových rovin. Částečné předběžné pokusy byli učiněny již v kapitole 5.5.3. Tyto pokusy však vycházeli pouze ze subjektivního hodnocení autora. Tvořily tak určité předpoklady pro vhodnost vkládání do konkrétních bitových rovin a pro zvyšování robustnosti algoritmu. Nyní po učiněných závěrech z předešlých kapitol je možné ověřit konkrétní kombinace na větším vzorku dat a s využitím většího množství respondentů.

V kapitole 4.1.2.2 „Kritéria na steganografické systémy“ bylo v rámci požadavku nevnímatelnosti citováno:

„Vložená informace je nevnímatelná, pokud průměrný člověk není schopný rozlišit originální data od dat obsahujících skrytou informaci. Nevnímatelnost se zkoumá na velkém vzorku dat, v němž buď je nebo není vložená informace, a to tak, že určité množství lidí porovnává tyto vzorky. Jako úspěšná hodnota neviditelnosti se považuje ta, pokud 50% zúčastněných lidí nedokáže odlišit označené vzorky od originálních.“

Bylo osloveno 100 osob ve věku od 15ti do 60ti let.

Dále bylo vybráno 100 fotografií a učiněno vložení vodoznaku do každé z nich v následujících kombinacích:

- 5. bitová rovina modré barvy a 4. bitová rovina červené barvy
- 5. bitová rovina modré barvy a 4. bitová rovina zelené barvy
- 6. bitová rovina modré barvy a 5. bitová rovina červené barvy
- 6. bitová rovina modré barvy a 5. bitová rovina zelené barvy
- 7. bitová rovina modré barvy a 6. bitová rovina červené barvy
- 7. bitová rovina modré barvy a 6. bitová rovina zelené barvy
- 8. bitová rovina modré barvy a 7. bitová rovina červené barvy
- 8. bitová rovina modré barvy a 7. bitová rovina zelené barvy

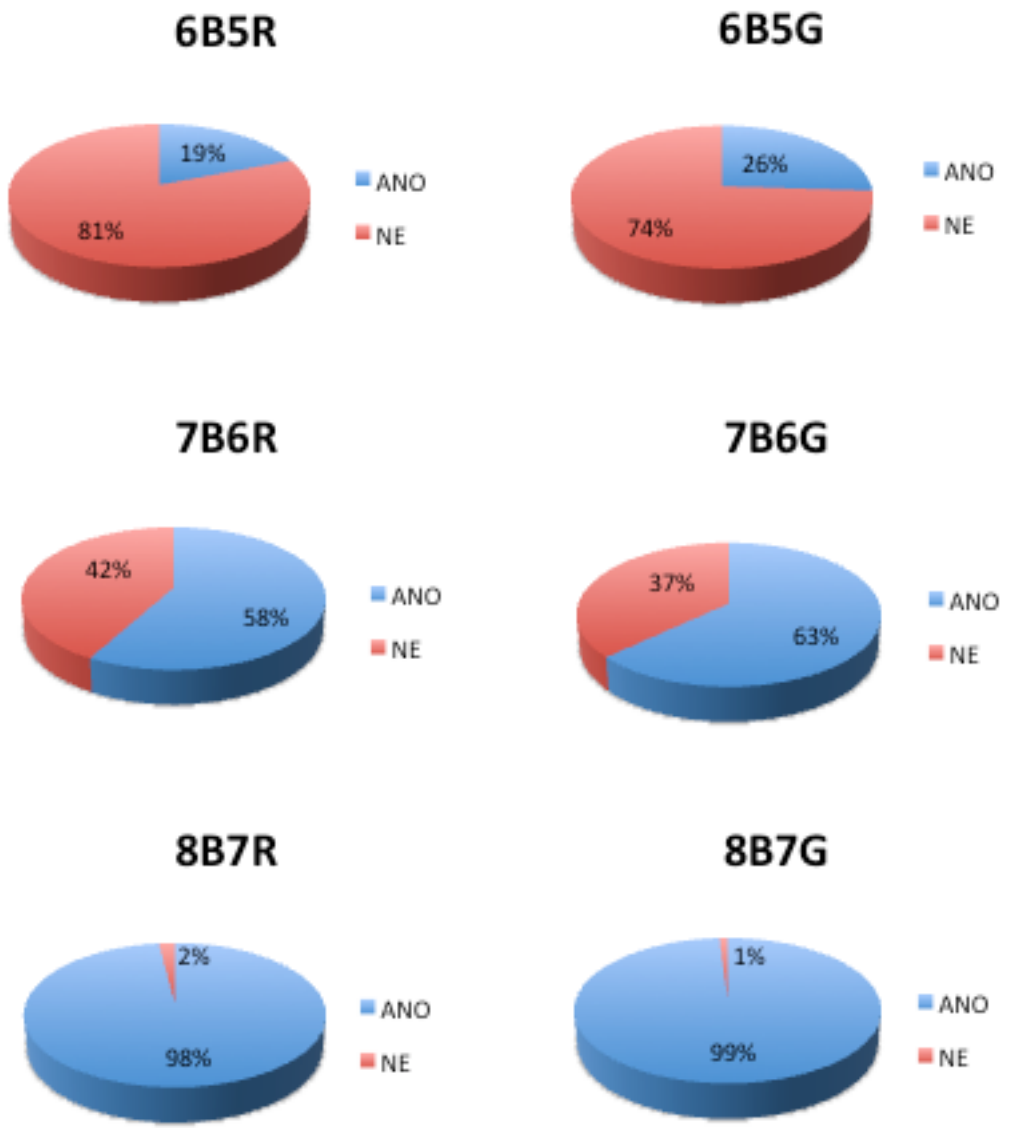
Tak vzniklo celkově 800 výsledných fotografií s vloženým vodoznakem. Jednotlivé vzorky byly distribuovány 50ti respondentům z nichž každý měl odpovědět na otázku, zda dokáže rozlišit označené vzorky od originálních.

Vzhledem k náročnosti tohoto testování byly respondentům distribuovány vzorky po 100 fotografiích, aby se zamezilo přílišné únavě a snížení soustředění.

5.5.8.1 Výsledky testování imperceptibility

Analýza výsledků byla prováděna pro každý obraz samostatně, tzn. bylo získáno 100 výsledků testování pro každý obraz, kde vznikl procentuální poměr pozitivních a negativních hodnocení. Takto postupně vzniklo 100 procentuálních poměrů v rámci jedné kategorie. Za konečný výsledek byl považován ten, který v rámci odpovědi „ano“ obsahoval nejvyšší hodnotu, jedině tak je možné zajistit požadavek iperceptibility. Takto postupně vznikaly výsledky pro všechny kategorie.

Výsledky testování imperceptibility jsou znázorněny na následujících koláčových grafech. Vzhledem k faktu, že pro 5. bitovou rovinu modré barvy a 4. bitovou rovinu červené či zelené barvy (tzn. 5B4R a 5B4G) byly výsledky nevnímatelnosti 100%, nebudou tyto dva grafy uváděny.



Graf č. 5.1- 5.6 – Ukázka výsledků testování imperceptibility

5.5.8.2 Zhodnocení

Výsledky testování imperceptibility potvrzují závěry učiněné již v kapitole 5.5.3 a potvrzují taktéž subjektivní vnímání imperceptibility autora práce.

Z učiněného testování je zřejmé, že využití 5. bitové roviny modré barvy a 4. bitové roviny červené či zelené barvy pro vkládání vodoznaku je naprosto spolehlivé neboť výsledkem je skutečně 100% nevnímatelnost vloženého vodoznaku.

Velmi dobrých výsledků bylo dosaženo taktéž u 6. bitové roviny modré barvy a 5. bitové roviny červené či zelené barvy, kdy více jak padesát procent respondentů není schopna rozlišit originální obraz od obrazu s vloženým vodoznakem. U kombinace 6B5R to byl nejhorší výsledek – dokonce pouze 81 % a u kombinace 6B5G 74 %. Tento výsledek jasně ukazuje na spolehlivé využití těchto kombinací pro automatické vkládání vodoznaku do obrazu.

Výsledky pro 7. bitovou rovinu modré barvy a 6. bitovou rovinu červené barvy či zelené barvy dopadly dle očekávání poměrně pozitivně. Nejhorší výsledek respondentů dosáhnul 42 % u červené a 37 % u zelené. Tento výsledek však nesplňuje minimální hodnotu 50 %. Tzn. automatické vkládání vodoznaku nelze pro tuto kombinaci využívat. Nicméně dle dalších výsledků dosahoval rozptyl varianty 7N6R 42 až 52 %, varianty 7B6G pak 37 až 48 %. Tyto výsledky ukazují, že obě varianty dosahují v rámci horních hodnot intervalu již zajímavější výsledky. Lze tedy uvažovat o možnosti využití této kombinace při manuálním vkládání vodoznaku, kdy je možné obraz subjektivně zhodnotit a rozhodnout se o konkrétní kombinaci.

Výsledky pro 8. bitovou rovinu modré barvy a 7. bitovou rovinu červené či modré barvy dopadly poměrně negativně. Nejhorší výsledek pro variantu s červenou barvou dosáhl 2 %. Zde je nutné však podotknout že v této kategorie měly hodnoty největší rozptyl – pohybovaly se od 2 do 31 %. Obdobně varianta se zelenou barvou se pohybovala od 1 do 27 %. Je patrné, že tato kategorie je značně subjektivní, nicméně je nutno brát v úvahu nejhorší výsledek. Z uvedeného vyplývá, že tato kategorie je pro vkládání vodoznaku nevhodná.

Obecně lze říci, že lepších výsledků dosahují vysokofrekvenční obrazy s velmi malým (nejlépe žádným) poměrem jednobarevných ploch. Pro manuální vkládání vodoznaků je možné doporučit testování i ve vyšších bitových rovinách, pro automatické však maximálně variantu 6B5R či 6B5G.

5.5.9 Popis výsledné metodiky EZOD

Na základě řady testování byla metodika EZOD od svého návrhu postupně upravována až ke kýženému výsledku.

Metodika EZOD se skládá z popisu konkrétní implementace algoritmu a následného postupu jeho efektivního využití.

5.5.9.1 Popis algoritmu

V této kapitole bude uveden detailní popis konkrétní implementace algoritmu, jako součást metodiky EZOD.

Program pro vkládání a extrakci vodoznaku byl tvořen v nástroji MATLAB – v. 7.0.1.24704 (R14) service pack 1. Tzn. Bude zde uveden popis implementace v tomto prostředí. Nicméně je nutné si uvědomit, že základní vlastnosti algoritmu vycházejí z provedených zkoumání a proto je dle následujícího popisu možné učinit implementaci i v jiném programovém prostředí, např. v programovacích jazycích JAVA, Python a dalších. Tzn. dle zásad a postupů následně uvedených vytvořit konkrétní implementaci metodiky EZOD ve vybraném programových prostředích organizace a s možností implementace metodiky do nejrůznějších podnikových systémů jako součást automatického či poloautomatického zpracování obrazových dat či samostatně.

Popis načtení obrazu a vodoznaku

Krok 1: Otevření obrazu

V prvním kroku je nutné učinit otevření obrazu, v rámci MATLABU je využita funkce „Uigetfile“.

Pro další popis je nutné definovat následující veličiny.
Velikost obrazu v pixelech (px):

m - výška obrázku
n - šířka obrázku
$o = 3$ (pro model RGB, tzn. barevný obraz)

Krok 2: Načtení obrazu

Dalším krokem je načtení obrazu – v programovém prostředí MATLABU je nutné použít funkci „imread“, která vrátí matici

$A = (a_{ij})$ typu $m \times n \times o$ pro barevný obrázek a matici
$A = (a_{ij})$ typu $m \times n$ pro černobílý obrázek

při

$a_{ij} \in \langle 0;255 \rangle$ pro barevný obrázek a
$a_{ij} \in \langle 0;1 \rangle$ pro černobílý

Krok 3: Vykreslení obrazu a jednotlivých bitových rovin

Po načtení obrazu vrátí funkce „imread“ rozložení obrazu do matice tzn. do binární soustavy. Vzniká 8 binárních matic

typu $m \times n \times o$ pro barevné obrázky
typu $m \times n$ pro černobílé obrázky

Zde bylo nutné ještě překonvertování datového typu „int8“ pomocí funkce „logical“. Následně dojde k vykreslení obrazu pomocí funkce „axes“ a jednotlivých bitových rovin dle volby combo boxu GUI v rámci konkrétní implementace GUI v MATLABU. Samozřejmě že pro implementaci v různých podnikových prostředích a automatizaci či poloautomatizaci tohoto procesu není třeba jednotlivé bitové roviny v GUI nutně vykreslovat.

Popis tvorby a implementace GUI není součástí tohoto popisu zejména z hlediska různých požadavků na automatizaci v rámci podnikových systémů a proto by tento popis nebyl účelný. Zde se skutečně práce zaměřuje pouze na popis implementace algoritmu.

Vytvoření permutované matice s vodoznakem

K vytvoření permutační matice se v programu využívá pomocná permutační matice, která obsahuje náhodně zpřeházené pozice matice vodoznaku na základě použití funkce „randn“, která je pseudonáhodná (tzn. při resetu vrací stejné hodnoty, lze ji tedy opakovaně použít pro vkládání a zpětnou extrakci vodoznaku,).

Permutační matice:

$$P_z(p_{ij}) = \sum_{k=1}^{m \times n} k$$

$$P = randn(P_z)$$

Dojde tedy k přeuspořádání matice vodoznaku dle permutační matice:

$$A_p(a_{ij}) = A(P(p_{ij}))$$

Tato operace je prováděna 100x. Neboť následně vzniká skutečně optimální rozmístění prvků (pixel) vodoznaku. Stonásobné použití funkce „randn“ je součástí permutačního a depermutačního klíče.

Dále dochází k vykreslení vodoznaku v GUI a možnostem zobrazování jednotlivých bitových rovin s a bez vodoznaku na základě combo boxu, check boxu a radio buttons.

Vložení vodoznaku

Krok 1: Rozprostření vodoznaku

Je nutné si uvědomit, že obrázek má jiné rozměr ($m \times n$) než vodoznaku ($k \times l$). O způsobech rozprostření vodoznaku bylo již zmiňováno v teoretické i praktické části práce. Pro optimální rozprostření vodoznaku byla využito již popsaná metoda z kapitoly 5.2.2 a znázorněna na obr. 5.5. tzn. je nutné zajistit maximální rozprostření vkládaného vodoznaku do obrazu.

Vodoznak (v našem případě permutovaný) je proložen prázdnými obrazovými body (tzn. černou barvou, která následně nevytváří změnu při vkládání vodoznaku).
Je tedy vloženo tolik prázdných sloupců (řádků), tak aby se vodoznak co nejvíce roztáhl (přizpůsobil velikosti obrazu, do kterého bude vkládán).

Podmínkou je aby vodoznak byl nejvýše tak velký jako obrázek. Dle zjištěných testování je vhodné vkládat vodoznak o přibližně polovičních rozměrech než je samotný obrázek a důležitou vlastností vodoznaku by měl být jeho nízkofrekvenční charakter.

Pro demonstraci bylo zvoleno:

- obraz o velikost $m \times n$, kde m=256 px, n=256 px

- vodoznak o velikosti $k \times l$, kde k=128 px, l=128 px

Pro definici počtu vynechaných řádků (sloupců) je využita funkce „Fce floorů“, užívaná pro zaokrouhlení dolů na celá čísla.

$floor\left(\frac{m}{k}\right) - 1$ a následné zaokrouhlení dolů na celá čísla

$floor\left(\frac{n}{l}\right) - 1$ a následné zaokrouhlení dolů na celá čísla

Počet vynechaných sloupců i řádků se pak odvodí následovně:

$$\left(\frac{256}{128}\right) - 1 = 1$$

Krok 2: Samotné vložení vodoznaku

Nyní bereme v úvahu dvě binární matice

- matici rozprostřeného vodoznaku (A_{rp}) a
- matici originálního obrazu (konkrétní bitová rovina a barva) (A_{rb}).

Na tyto matice následně aplikujeme funkci „XOR“ a získáme výslednou binární matici *Z* (pokud vkládáme do více rovin, získáme více těchto matic).

$$A_{rbx} = A_{rb} xor A_{rp}$$

Krok 3: Kompletace obrazu

Maticí A_{rbx} nahradíme matici A_{rb} a provedeme složení bitových rovin zpět do výsledného obrazu (s vodoznakem).

$$A_{rb} = A_{rbx}$$

Extrakce vodoznaku

Při extrakci vodoznaku se provede načtení obrázku s vodoznakem a načtení originálního obrazu stejným způsobem, jako již bylo popsáno výše tzn. **Krok 1 – 3: Popis načtení obrazu a vodoznaku**.

Krok 4: Použití klíče pro zpětnou extrakci

V tomto kroku jsou zvoleny důležité parametry pro úspěšné provedení následné extrakce - tzn. je nutné zvolit barvu (popřípadě více barev), bitovou rovinu (popřípadě různé bitové roviny v rámci jedné barvy či více barev), způsob vložení v našem případě permutovaného vodoznaku a velikost vodoznaku.

Následně je provedena extrakce vodoznaku na základě zvolených parametrů a zpětného algoritmu (symetrický klíč).

Zpětný algoritmus:

Na základě parametrů: barvy a bitové roviny – při zpětné extrakci pracujeme pouze s touto bitovou rovinou jak u obrázku s vodoznakem, tak u originálního obrazu. Následně se provede ořez těchto bitových rovin na oblast, do které byl vložen vodoznak.

Velikost ořezu ve směru osy x :

$$= k \times floor\left(\frac{m}{k}\right)$$

Velikost ořezu ve směru osy y:

$$= l \times floor\left(\frac{n}{l}\right)$$

Dále je provedeno vyjmutí řádků a sloupců, které byly při vkládání vodoznaku vynechány dle výše popsaného algoritmu „vynechaných řádků (sloupců)“.

Takto vzniknou dvě upravené binární matice

- upravená matice originálního obrazu O_y a
- upravená matice obrazu s vodoznakem P_y

z kterých aplikací zpětné funkce XOR získáme extrahovaný vodoznak.

$$W = P_y xor O_y$$

Pokud byl vkládán permutovaný vodoznak, je nutné provést ještě tzv. depermutaci. Ke zpětné depermutaci se v programu využívá pomocná depermutační matice, která vychází z pomocné permutační matice.

$$A_{dp}(a_{ij}) = \sum_{i=1}^{i \times j} A_p(a_{ij})$$

Následně dojde k zpřeházení matice vodoznaku dle depermutační matice a tak vzniká výsledný extrahovaný vodoznak (v nepermutované podobě).

Pro názornější demonstraci je následně uveden konkrétní příklad.

Příklad:

Matice obrázku: $A_o = \begin{pmatrix} 9 & 216 \\ 113 & 84 \end{pmatrix}$

Vytvoření permutační matice A_p:

Permutační matice: $A_p = randn\begin{pmatrix} 1 & 3 \\ 2 & 4 \end{pmatrix} = \begin{pmatrix} 3 & 4 \\ 1 & 2 \end{pmatrix}$

Permutace obrázku: $A_{op} = A_o(A_p) = \begin{pmatrix} 216 & 84 \\ 9 & 113 \end{pmatrix}$

Vytvoření depermutační matice A_{dp}:

$$A_p = \begin{pmatrix} 3 & 4 \\ 1 & 2 \end{pmatrix} \Rightarrow 1 \rightarrow A_{dp}(a_{12}), 2 \rightarrow A_{dp}(a_{11}), 3 \rightarrow A_{dp}(a_{22}), 4 \rightarrow A_{dp}(a_{21})$$

$$A_{dp} = \begin{pmatrix} 2 & 1 \\ 4 & 3 \end{pmatrix}$$

Depermutace obrázku: $A_o = A_{op}(A_{dp}) = \begin{pmatrix} 9 & 216 \\ 113 & 84 \end{pmatrix}$

5.5.9.2 Metodický postup efektivního užití algoritmu

Způsob efektivního zabezpečení obrazových dat je nejlépe rozdělit do dvou základních skupin:

- Dávkové (hromadné) zpracování obrazů
- Postupné (manuální) zpracování jednotlivých obrazů

Obě tyto skupiny se snaží o co nejlepší zabezpečení dat, avšak první skupina navíc upřednostňuje automatizaci tohoto procesu. Automatizace však s sebou logicky přináší snížení efektivity zabezpečení. Je to především z důvodu nemožnosti kontroly imperceptibility (vnímatelnosti vodoznaku) každého obrazu zvlášť.

5.5.9.2.1 Dávkové zpracování

Fáze 1: Vkládání viditelného vodoznaku

Viditelný vodoznak by měl chránit obrazy před většinou typických uživatelů. Proto je určitě účelné jej pro prvotní zabezpečení a odrazení potencionálních útočníků použít. Jak již bylo zmíněno v předešlé části práce lze použít viditelný vodoznak, který zakrývá co největší plochu obrazu, nebo použít pouze viditelný vodoznak např. v dolní části obrazu.

Druhá varianta může samozřejmě přilákat daleko větší množství potencionálních útočníků, jelikož pro odstranění takovéhoto vodoznaku stačí pouhý jednoduchý ořez části obrazu s vodoznakem.

Zde je však také otázka k jakým účelům budou prezentované obrazy sloužit. Zda budou použity pro soukromé účely v rámci soukromé fotogalerie či pro komerční účely tedy například pro nějaké fotobanky, realitní kanceláře, e-shopy, firemní portály a podobně.

Pokud vezmeme v úvahu soukromou fotogalerii bude zřejmě základním účelem fotogalerie prezentovat fotografie svým známým a snažit se jim pochlubit s co nejlepšími a pokud možno co nejlépe viditelnými fotografiemi. Pro tyto účely pak bude jistě rozumnější zvolit vodoznak překrývající menší plochu obrazu např. jej umístit v některém z dolních rohů obrázku. Avšak je tu samozřejmě stále riziko útoku i když se pravděpodobně na soukromé stránky dostane méně potencionálních útočníků než na známou veřejnou fotobanku.

Pro komerční účely, kde panuje nemilosrdný konkurenční boj a kde je daleko větší potencionální možnost útoků, bych však přeci jen doporučila viditelný vodoznak překrývající větší část obrazu.

Fáze 2: Vkládání neviditelného vodoznaku

Krok 1: Volba vodoznaku

Vodoznak je nutné volit co nejuváženěji, jelikož špatná volba vodoznaku s sebou nese riziko nefunkčnosti zpětné extrakce v extrémních hranicích.

Pro volbu vodoznaku lze tedy doporučit:

- Zaměřit se na nízkofrekvenční vodoznak – tzn. pokud možno spíše volit větší stejnobarevné plochy a vyhnout se detailům
- Volit přibližně stejný poměr bílých a černých ploch – při extrémních útocích lépe vyniknou základní obrysy vodoznaku
- Volit vodoznak přibližně poloviční velikosti výsledného obrazu

Při dávkovém zpracování je předpoklad následné prezentace velkého počtu dat (obrazů). Proto zde doporučuji volbu několika vodoznaků s výše uvedenými vlastnostmi, které se budou náhodně vkládat do obrazů, aby byla maximálně omezena možnost statistické detekce vodoznaku eventuálními útočníky.

Taktéž je nutné použít permutovaný(é) vodoznak(y) pro zabezpečení odolnosti vodoznaku proti ořezu.

Krok 2: Volba bitové roviny

Dle provedených výzkumů je nutné vkládat vodoznak minimálně do dvou bitových rovin – a to minimálně jedenkrát do liché bitové roviny a jedenkrát do sudé bitové roviny. Důvodem jsou výkyvy při eventuálním útoku změnou jasu, kde při vložení do sudé i liché roviny pokryjeme i tyto sic zřídka se objevující výkyvy.

Dále je otázkou do jakých rovin vkládat. Samozřejmě pro zabezpečení odolnosti vodoznaku potřebujeme vkládat do co nejvyšších rovin. Pro dávkové zpracování však je nutné volit takovou nejvyšší rovinu, aby byly vždy zabezpečeny taktéž vlastnosti imperceptibility vodoznaku. V tomto případě lze doporučit vkládání nejvýše do 6. bitové roviny a jako lichou rovinu zvolit 5. bitovou rovinu.

Taktéž je třeba určit barvu, do které vodoznak vkládat. Dle učiněných testování, které odpovídají popsaným vlastnostem citlivosti lidského oka na jednotlivé barevné složky, lze jednoznačně doporučit pro vyšší bitovou rovinu (tedy 6.) vkládání do modré barvy a pro nižší bitovou rovinu (tedy 5.) vkládání do červené barvy. Využití pouze modré barvy je nevhodné pro možný útok znovu uložením obrazu.

Tato volba bitových rovin a barev by neměla být závislá na vlastnostech obrazu tzn. zda je vysokofrekvenční či nízkofrekvenční. U obou typů by měly být zachovány vlastnosti imperceptibility vodoznaku. Zároveň by zde měla být zachována maximální odolnost algoritmu pro 6. a 5. bitovou rovinu.

Obraz s vloženým vodoznakem bude mít tedy následující vlastnosti při užití této metodiky:

- Odolnost proti ořezu – až k 80ti procentům,
- odolnost proti šumu – až k 80ti procentům,
- odolnost proti zvyšování jasu – až k hranice 200 jednotek,

- odolnost proti snižování jasu – až k hranici 220 jednotek,
- odolnost proti znovu uložení obrazu do ztrátového formátu JPEG – až k hranici 51% ztrátové komprese,
- odolnost proti statistické nedetekovatelnosti bude však částečně nikoliv však výrazně narušena,
- nebude odolný proti rotaci a změně velikosti,
- neohrožují jej prezentační a interpretační útoky,
- neměli by jej ohrozit ani právní útoky,
- imperceptibilita zajištěna.

5.5.9.2.2 Manuální zpracování jednotlivých obrazů

V dnešní době, kdy je snaha o co největší efektivitu práce je vůbec otázkou zda by někdo volil postupné (manuální) zpracování od volby dávkového zpracování (automatizace). Avšak v tomto případě je nutné podotknout že postupné zpracování s sebou přináší možnost vyššího zabezpečení obrazu – tzn. větší odolnost proti potencionálním útokům.

Samozřejmě opět zde záleží na oblasti užití. Pokud budeme potřebovat upravit denně tisíce obrazů, jistě zvolíme dávkové zpracování. Pokud však budeme potřebovat upravovat několik fotografií týdně, volba již může být rozdílná.

A protože i autor této práce upřednostňuje maximální zabezpečení veřejně přístupných grafických dat, bude zde popsán postup manuálního zpracování jednotlivých obrazů.

Fáze 1: Vkládání viditelného vodoznaku

Tato fáze vkládání viditelného vodoznaku se od dávkového zpracování nikterak neliší, proto rozhodnutí o konkrétní aplikaci viditelného vodoznaku bude stejné.

Fáze 2: Vkládání neviditelného vodoznaku

Krok 1: Volba vodoznaku

Vodoznak je nutné volit co nejuváženěji, jelikož špatná volba vodoznaku s sebou nese riziko nefunkčnosti zpětné extrakce v extrémních hranicích. Pro volbu vodoznaku lze doporučit stejné zákonitosti uvedené v dávkovém zpracování.

Pokud nebylo zvoleno dávkové zpracování, ale výsledný soubor prezentovaných obrazů bude rozsáhlejší, opět bych zde doporučila volbu několika vodoznaků s výše uvedenými vlastnostmi, které se budou náhodně vkládat do obrazů pro maximální omezení statistické detekovatelnosti vodoznaku eventuálními útočníky. Taktéž je nutné použít permutovaný(é) vodoznak(y), pro zabezpečení odolnosti vodoznaku proti ořezu.

Krok 2: Volba bitové roviny a barvy

Dle provedených výzkumů je nutné vkládat vodoznak opět minimálně do dvou bitových rovin – a to minimálně jedenkrát do liché bitové roviny a jedenkrát do sudé

bitové roviny. Důvodem jsou výkyvy při eventuálním útoku změnou jasu, kde při vložení do sudé i liché roviny budou pokryty i tyto sic zřídka se objevující výkyvy.

Dále je otázkou do jakých rovin vkládat. Samozřejmě pro zabezpečení odolnosti vodoznaku potřebujeme vkládat opět do co nejvyšších rovin.

Pro postupné manuální zpracování obrazu bych zde doporučila zaměřit se na výsledky imperceptibility i v 8. a 7. rovině zejména u modré barvy. U vysokofrekvenčních obrazů je vysoká pravděpodobnost, že by mohla být právě jedna z těchto dvou rovin využita.

Následně dle výběru vyšší bitové roviny provést následný výběr doplňkové nižší sudé či liché bitové roviny. To znamená opět testování imperceptibility v rámci další barvy ve vyšších rovinách. Zde bych doporučila zaměřit se především na červenou barvu, která při testech imperceptibility vykazovala lepší výsledky. Nicméně je možné vyzkoušet i výsledky při vkládání do zelené barvy, neboť jsou výsledky závislé i na samotné barevnosti obrazu.

Mohou tedy nastat následující možnosti:

- 8. bitová rovina modré barvy a 7. bitová roviny červené či zelené barvy. Toto je samozřejmě ideálním případ pro nejvyšší zabezpečení obrazu, nicméně jeho výskyt bude velmi řídký.
- 8. bitová rovina modré barvy a 5. bitová rovina červené či zelené barvy.
- 7. bitová rovina modré barvy a 6. bitová rovina červené či zelené barvy. Toto bude pravděpodobně jedna z častějších variant manuálního zpracování, avšak je samozřejmé, že u některých obrazů nebude taktéž možná vzhledem k nízkofrekvenčním povahám obrazů.
- 7. bitová rovina modré barvy a 4. bitová rovina červené či zelené barvy. Tento postup by však z hlediska volby sudé roviny nebyl příliš žádoucí.
- Poslední možností je základní doporučení dávkového zpracování – tzn. 6. bitová rovina modré barvy a 5. bitová rovina červené barvy (eventuálně zelené barvy).

Volba bitových rovin a barev bude v tomto zpracování závislá na vlastnostech obrazu – tzn. zda je vysokofrekvenční či nízkofrekvenční. U obou typů by po volbě bitových rovin a barev měly být zachovány vlastnosti imperceptibility vodoznaku.

Obraz s vloženým vodoznakem bude mít tedy následující vlastnosti při užití této metodiky:

V rámci volby nejvyšší 8. bitové roviny:

- Odolnost proti ořezu – až k 80ti procentům,
- odolnost proti šumu – až k 80ti procentům,
- odolnost proti zvyšování jasu – až k hranice 200 jednotek,
- odolnost proti snižování jasu – až k hranici 220 jednotek,
- odolnost proti znovu uložení obrazu do ztrátového formátu JPEG – až k hranici 20% ztrátové komprese,
- odolnost proti statistické nedetekovatelnosti bude však částečně narušena,
- nebude odolný proti rotaci a změně velikosti,
- neohrožují jej prezentační a interpretační útoky,
- neměli by jej ohrozit ani právní útoky,
- imperceptibilita bude pravděpodobně zhoršena.

V rámci volby nejvyšší 7. bitové roviny:

- Odolnost proti ořezu – až k 80ti procentům,
- odolnost proti šumu – až k 80ti procentům,
- odolnost proti zvyšování jasu – až k hranice 200 jednotek,
- odolnost proti snižování jasu – až k hranici 220 jednotek,
- odolnost proti znovu uložení obrazu do ztrátového formátu JPEG – až k hranici 35% - 40% ztrátové komprese,
- odolnost proti statistické nedetekovatelnosti bude však částečně narušena,
- nebude odolný proti rotaci a změně velikosti,
- neohrožují jej prezentační a interpretační útoky,
- neměli by jej ohrozit ani právní útoky,
- imperceptibilita bude pravděpodobně zhoršena.

V rámci volby nejvyšší 6. bitové roviny (shodné s dávkovým zpracováním):

- odolnost proti ořezu – až k 80ti procentům,
- odolnost proti šumu – až k 80ti procentům,
- odolnost proti zvyšování jasu – až k hranice 200 jednotek,
- odolnost proti snižování jasu – až k hranici 220 jednotek,
- odolnost proti znovu uložení obrazu do ztrátového formátu JPEG – až k hranici 51% ztrátové komprese,
- odolnost proti statistické nedetekovatelnosti bude však částečně narušena,
- nebude odolný proti rotaci a změně velikosti,
- neohrožují jej prezentační a interpretační útoky,
- neměli by jej ohrozit ani právní útoky,
- imperceptibilita zajištěna.

6 Aplikace metodiky EZOD

„Práce bývá často matkou radosti.“
Voltaire

Tato kapitola demonstruje výsledky aplikace navržené metodiky zabezpečení veřejně přístupných grafických dat na konkrétních příkladech. Následně se věnuje srovnání tohoto řešení s obdobnými postupy a v neposlední řadě poukazuje na konkrétní oblasti vhodné pro aplikaci metodiky.

6.1 Demonstrace na praktických příkladech

Pro demonstraci metodiky EZOD byly použity čtyři autorské obrazy různé povahy a čtyři obrazy, které jsou obecně využívány pro výzkumy a hodnocení v oblasti steganografie a vodotisku v odborných literárních zdrojích.

Tabulka č. 6.1 – Původní autorské obrazy pro demonstraci metodiky EZOD

Předešlá tabulka zobrazovala čtyři autorské obrazy. V další tabulce jsou uvedeny známé obrazy využívané nejčastěji pro testování kvality obrazů v odborné literatuře, které se nazývají lenna, house, mandrill a pepers.

Tabulka č. 6.2 – Původní obrazy lenna, house, mandrill a pepers využité pro demonstraci metodiky EZOD

Následně budou uvedeny výsledky aplikace metodiky EZOD pro postupného zpracování jednotlivých obrazů.

Autorské fotografie: obraz 1

První demonstrace je zobrazena na fotografii která byla v této práci využívána nejvíce. Nejdříve byl vložen viditelný vodoznak do dolní časti obrazu. Následně se podařil vložit neviditelný vodoznak do 6. bitové roviny modré barvy a 5. bitové roviny červené barvy při zachování vlastností imperceptibility. Výsledek je možno vidět v následující tabulce.

Originální obraz	Obraz s viditelným a neviditelným vodoznakem – 6B5R
	

Tabulka č. 6.3 – Demonstrace výsledku po vložení vodoznaků

Autorské fotografie: obraz 2

Dále byl vložen vodoznak do fotografie ČZU (nebo spíše do koláže), kde byla použita průhlednost (ve smyslu průhledného červeného pruhu), která je velmi náchylná na vkládání přídavných informací. Opět byl nejdříve vložen viditelný vodoznak, tentokrát na hlavní motiv fotografie. I přes náchylnost průhlednosti se podařilo vložit neviditelný vodoznak do 6. bitové roviny modré barvy a 5. bitové roviny červené barvy. Výsledek je znázorněn v tabulce níže.

Originální obraz	Obraz s viditelným a neviditelným vodoznakem – 6B5R
	

Tabulka č. 6.4 – Demonstrace výsledku po vložení vodoznaků

Autorské fotografie: obraz 3

Pro třetí demonstrativní ukázku byla vybrána vysokofrekvenční fotografie výřezu hlavy kočky. Byl vložen viditelný vodoznak do dolní části obrazu. Neviditelný vodoznak se v tomto případě podařilo vložit dokonce do 7. bitové roviny modré barvy a 6. bitové roviny červené barvy, samozřejmě při zachování vlastnosti imperceptibility. Výsledný obraz je možné vidět v následující tabulce.

Originální obraz	Obraz s viditelným a neviditelným vodoznakem – 7B6R
	

Tabulka č. 6.5 – Demonstrace výsledku po vložení vodoznaků

Autorské fotografie: obraz 4

Následně byla vybrána fotografie z přírody, kde je možné vidět jak vysokofrekvenční, tak nízkofrekvenční oblasti. Viditelný vodoznak byl zde vložen přes hlavní motiv obrazu. Neviditelný vodoznak se podařilo vložit do 6. bitové roviny modré barvy a 5. bitové roviny červené barvy. Výsledek je možné vidět v následující tabulce.

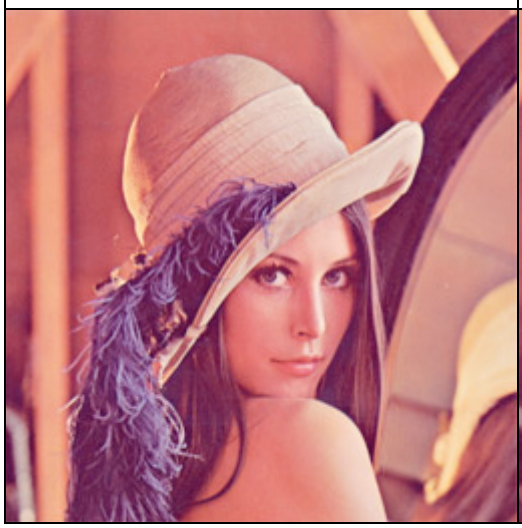
Originální obraz	Obraz s viditelným a neviditelným vodoznakem – 6B5R
	

Tabulka č. 6.6 – Demonstrace výsledku po vložení vodoznaků

V další části je demonstrováno vložení neviditelných vodoznaků do známých obrazů, které jsou využívány k testování v odborných literárních zdrojích. Do těchto obrazů byly vloženy i příklady viditelného vodoznaku, pouze však pro názornou demonstraci.

Obraz 1: Lenna

Prvním obrazem je fotografie lenny. Po vložení viditelného vodoznaku se podařil vložit neviditelný vodoznak do 6. bitové roviny modré barvy a 5. bitové roviny červené barvy. Výsledný obraz je možné vidět v tabulce níže.

Originální obraz	Obraz s viditelným a neviditelným vodoznakem – 6B5R
	

Tabulka č. 6.7 – Demonstrace výsledku po vložení vodoznaku do obrazu „lenna“

Obraz 2: House

Dalším obrazem je fotografie domu. Viditelný vodoznak byl zde vložen přes celý motiv obrazu. Neviditelný vodoznak byl následně vložien do 6. bitové roviny modré barvy a 5. bitové roviny červené barvy. Výsledný obraz je možné vidět v tabulce níže.

Originální obraz	Obraz s viditelným a neviditelným vodoznakem – 6B5R
	

Tabulka č. 6.8 – Demonstrace výsledku po vložení vodoznaku do obrazu „house“

Obraz 3: Mandrill

Dalším obrazem je fotografie „mandrill“. Nejdříve byl opět vložen viditelný vodoznak přes celý motiv obrazu a následně vložen neviditelný vodoznak dokonce do 7. bitové roviny modré barvy a 6. bitové roviny červené barvy. Do vyšších bitových rovin se vodoznak podařilo vložit díky vysokofrekvenční povaze obrazu. Samozřejmě byla zachována vlastnost imperceptibility. Výsledný obraz je možné vidět v tabulce níže.

Originální obraz	Obraz s viditelným a neviditelným vodoznakem – 7B6R
	

Tabulka č. 6.9 – Demonstrace výsledku po vložení vodoznaku do obrazu „mandrill“

Obraz 4: Pepers

Dalším obrazem je fotografie paprik. Zde po vložení viditelného vodoznaku se podařil vložit neviditelný vodoznak do 6. bitové roviny modré barvy a 5. bitové roviny červené barvy při zachování vlastnosti imperceptibility. Výsledný obraz je možné vidět v tabulce níže.

Originální obraz	Obraz s viditelným a neviditelným vodoznakem – 6B5R
	

Tabulka č. 6.10 – Demonstrace výsledku po vložení vodoznaku do obrazu „pepers“

6.2 Porovnání s obdobnými postupy

Navržená metodika EZOD je v této části práce srovnávána s profesionálním nástrojem Digimarc od stejnojmenné firmy a s freeware nástrojem SignMyImage.

Program od společnosti Digimarc je v tomto oboru naprostou jedničkou a poskytuje buď samostatný program nebo jej lze využívat jako plugin v programu Adobe Photoshop. Je však ale také poměrně drahým řešením pro ochranu velkého počtu grafických dat.

SignMyImage je program který lze využívat rovněž samostatně i jako plugin do programu Adobe Photoshop. Z dostupných freeware nástrojů je jedním z nejužívanějších.

Oba uvedené nástroje poskytují možnost ochrany dat technikami digitálního vodotisku. Avšak na rozdíl od metodiky EZOD využívají metody založené na tzv. DCT (Diskrétní Cosínusova Transformace). O této metodě lze obecně říci, že se vyznačuje vysokou robustností, avšak nízkou kapacitou (nízkou schopností vložení většího počtu dat).

Pro srovnání s metodikou EZOD byla využita nejvyšší možná ochrana v obou nástrojích. Byla testována:

- odolnost proti ořezu,
- odolnost proti šumu,
- odolnost proti zvyšování jasu,
- odolnost proti snižování jasu,
- odolnost proti znovu uložení obrazu do ztrátového formátu JPEG,
- odolnost proti rotaci,
- odolnost proti změně velikosti,
- statistická nedetekovatelnost,
- možnost vkládání více vodoznaků.

V rámci všech testování byla zajištěna vlastnost imperceptibility. Výsledky srovnání jsou uvedeny v následující tabulce.

testování/srovnávané postupy	Digimarc	SignMy Image	EZOD (dávkové zpracování)	EZOD (manuální zpracování)
ořez	do 80 %	není	do 80 %	do 80 %
šum	až 20 %	není	až 200 %	až 200 %
snížení jasu	do 200	není	do 200	do 200
zvýšení jasu	do 190	není	do 220	do 220
ukládání do JPEG	až 30 %	až 50 %	až 50 %	až 35 %
rotace	ano	ne	ne	ne
změna velikosti	ano	ano	ne	ne
statistická nedetekovatelnost	výrazné změny	výrazné změny	nevýrazné změny	nevýrazné změny
možnosti vkládání více vodoznaků	ne	ne	ano	ano

Tabulka č. 6.11 – Srovnání výsledků odolnosti proti možným útokům

Z výsledků v tabulce je možné vidět, že v rámci testování ořezu a snižování jasu poskytuje metodika EZOD srovnatelné výsledky s profesionálním nástrojem Digimark. V testování odolnosti proti šumu, zvyšování jasu a statistické nedetekovatelnosti poskytuje navrhovaná metodika dokonce ještě lepších výsledků než tento profesionální program. Srovnání výsledků statické nedetekovatelnosti pomocí histogramů je explicitně uvedeno v tabulce č. 6.12, kde je možné pozorovat u obou programů skutečně výrazné změny.

V rámci srovnání útoku opětovným ukládáním do ztrátového formátu JPEG poskytuje metodika EZOD u dávkového zpracování horších výsledků než Digimark, při manuálním zpracování a případné možnosti vkládání do 7. bitové roviny modré barvy a 6. bitové roviny červené barvy, je však výsledek srovnatelný.

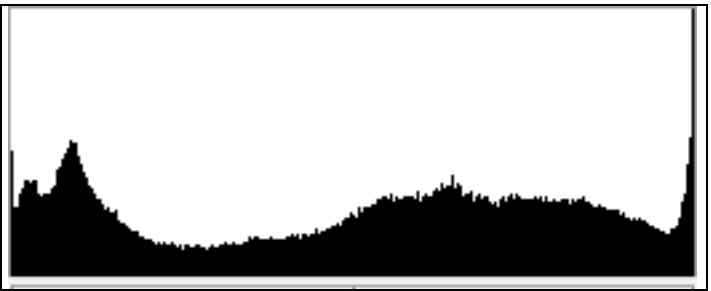
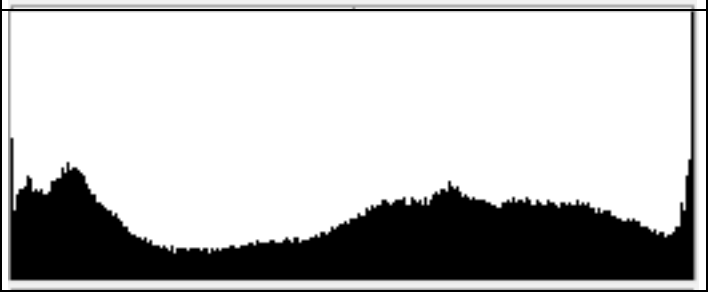
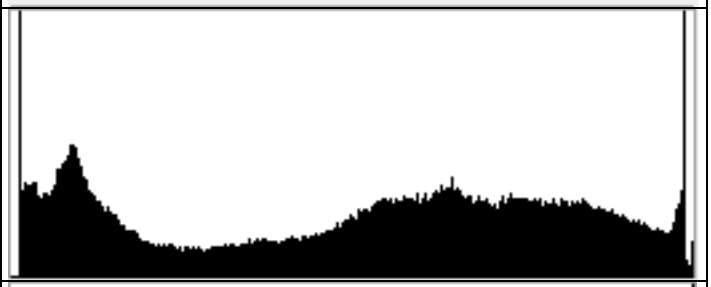
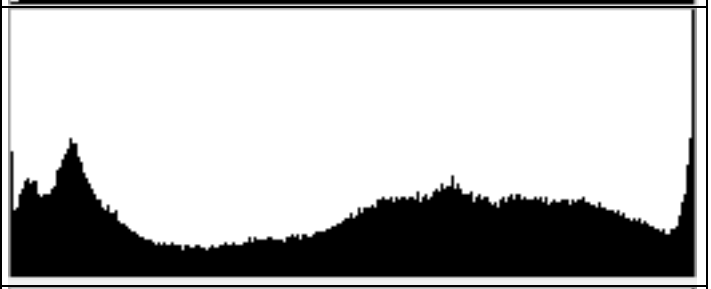
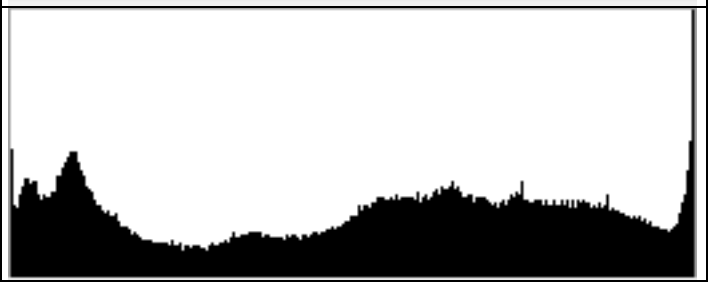
Výsledky rotace a změny velikosti jsou však na rozdíl od metodiky EZOD u profesionálního nástroje zajištěny.

Ve srovnání s nástrojem SignMyImage dosahuje metodika EZOD ve většině případů lepších výsledků. Ve dvou případech dosahuje stejného výsledku a v případě testování odolnosti proti změně velikosti horšího výsledku. Zarážející však je že SignMyImage neposkytuje odolnost proti základním útokům, zejména ořezu, ale také šumu a snižování a zvyšování jasu.

Navíc metodika EZOD poskytuje možnost vícenásobného vkládání vodoznaku či více různých vodoznaků. Tím je možné nejen zvyšovat robustnost algoritmu, ale také vkládat přídavné informace např. udělení oprávnění k dílu jiné osobě.

Z uvedených výsledků považuji za nutné rovněž uvést že srovnávané nástroje nezajišťují některé zásadní požadavky na systémy digitálního vodotisku. Zejména se jedná o vícenásobné vkládání vodoznaku, statistickou nedetekovatelnost a u nástroje SignMyImage i významné narušení požadavku robustnosti (vzhledem k nezajištění odolnosti proti základním útokům). U profesionálního nástroje jako je Digimarc, který je prezentován jako robustní řešení, využitelné pro velké množství obrazů, je nesplnění statistické nedetekovatelnosti až zarážející.

Na rozdíl od srovnávaných nástrojů se metodika EZOD snažila dosáhnout co nejefektivnějšího výsledku ochrany obrazových dat za předpokladu naplňování pokud možno všech požadavků na systémy digitálního vodotisku a dokonce i na samotné steganografické systémy.

Histogram originálního obrazu	
Histogram nástroje Digimark	
Histogram nástroje SignMyImage	
Histogram označeného obrazu dle metodiky EZOD – v rámci automatického zpracování – tzn. vkládání do 6. bitové roviny modré barvy a 5. bitové roviny červené barvy	
Histogram označeného obrazu dle metodiky EZOD – v rámci manuálního vkládání do 7. bitové roviny modré barvy a 6. bitové roviny červené barvy	

Tabulka 6.12 – Ukázka srovnání histogramů (v rámci statistické detekce vodoznaku) obdobných postupů

Na základě uvedených výsledků testování, lze závěrem této kapitoly konstatovat, že navržená metodika EZOD je jednoznačně konkurenčním řešením. Navíc s využitím několikanásobného ukládání vodoznaku poskytuje širší využití při označování grafických dat. Taktéž díky konkrétnímu popisu algoritmu a postupu pro efektivním zabezpečení obrazových dat, poskytuje možnost implementace do různorodých

podnikových systémů, tzn. neomezuje se pouze na integraci do čistě grafických nástrojů, jako např. Adobe Phostoshop, ale poskytuje širší využití v rozmanitých oblastech práce s grafickými informacemi.

6.3 Doporučené oblasti aplikace metodiky

Předešlá kapitola již zmiňovala širší využití navržené metodiky EZOD. Jaké jsou tedy vhodné oblasti jejího užití, se pokusí objasnit tato kapitola.

Její primární využití je samozřejmě stejné, jako u srovnávaných nástrojů, tzn. především v oblasti grafického průmyslu při zpracování velkého množství fotografií. Zde se samozřejmě dostává do popředí užití pro fotobanky a fotogalerie, ale také v nejrůznějších internetových obchodech, kde se často úmyslně odcizují obrazová data. Podobná situace nastává v internetových nabídkách realitních kanceláří a u nejrůznějších on-line prezentací. Samozřejmě je zde možné využití metodiky i pro off-line prezentace distribuované na různých médiích.

Kromě standardního využití poskytuje metodika EZOD i další možnosti. Jednou z nich je možnost vkládání označení udělení oprávnění k dílu jiné osobě/osobám dle autorského zákona. Díky možnosti vkládání přídavných informací do obrazu, je možné vložit například informace o udělení výhradní či nevýhradní licence, podlicence a dalších údajů, které jednoznačně identifikují autora a zároveň definují oprávnění užití díla.

Využití může metodika poskytnout v současné době i z hlediska digitalizace v komerční i nekomerční sféře. Významnou roli by mohla hrát v této souvislosti ve státní správě. Příkladem může být například automatické označování skenovaných dat datem a dalšími potřebnými údaji, které mohou pomáhat v boji s korupcí a případnými podvrhy.

Díky možnostem navržené metodiky lze uvažovat její využití i v dalších oblastech a oborech které jsou v současné době aktuální. V bankovním sektoru je možné uvažovat např. vkládání přídavných informací do fotografií náležících k hypotečním případům.

V tomto sektoru je aktuálním trendem umožnit klientovi výběr jeho soukromé fotografie a její následná aplikace na kreditní kartu. V této souvislosti by bylo možné tímto způsobem zasílat klientům skryté výpisy v jejich vlastních obrázcích, či tímto způsobem zasílat samotný pin.

Dalším trendem v této oblasti je vytváření klientských portálů v rámci služeb přímého bankovnictví. V některých bankách se uvažuje o zavádění skutečně robustních portálů na kterých budou moci klienti komunikovat, sdílet různorodé informace, fotografie a v neposlední řadě také obchodovat. V tomto ohledu by bankovní ústav měl poskytovat zabezpečení takovýchto sdílených informací. V případě obrazových dat například metodikou EZOD.

Další využití poskytuje metodika v poměrně aktuální oblasti tzv. Digital rights management (DRM), v českém překladu také známé pod pojmem systémy (nebo management) pro řízení digitálních práv. Tyto systémy se používají k řízení digitálního obsahu a jeho ochraně proti neoprávněnému použití. Existuje množství různých druhů systémů DRM. Jsou integrovány jak do fyzických nosičů (CD či DVD) tak i do obsahů šířených online, jako např. do hudebních dat, elektronických knih (eBook), textů,

obrázků a her či do tzv. Video On Demand (video na vyžádání, VOD). Šíření online obsahů se může dít prostřednictvím internetu, interaktivních televizních sítí nebo i mobilní komunikací. DRM využívá rozmanitých technických řešení k řízení a kontrole použití digitálního obsahu, především tzv. kódování, kde je nutné vlastnictví nějakého klíče a značkování, kde vlastník práv označuje soubory před prodejem tak, aby bylo možné získat informace o obsahu, tedy např. zda je soubor chráněn proti kopírování, kdo je vlastníkem práv a které formy použití jsou povolené. Uvedené dvě techniky je možné metodikou EZOD zajistit a v této oblasti lze tedy nalézt její vhodné užití.

Pro aplikaci metodiky EZOD je taktéž možné uvažovat i oblast lékařství. Například v případě zasílání lékařských předpisů od lékaře přímo pacientům v případě, že nemají možnost vyzvednout si předpis osobně. Zaslání v obrazových datech by mělo funkci zabezpečení před potencionálními útočníky. Tento způsob lez samozřejmě řešit i řadou jiných přístupů, nicméně se k nim metodika EZOD může připojit.

Podnětů pro využití navrhované metodiky a její integrace do různých podnikových systémů, je celá řada. Jde především o zefektivnění práce, kdy by se mohla obrazová data označovat automaticky, bez jakýchkoliv dílčích úkonů. Např. při tvorbě nejrůznějších prezentací, označování fotografií a užití v dalších již uvedených oblastech, kdy by se mohly potřebné informace vkládat do obrazových dat automaticky, bez nutnosti tohoto úkon v jiném programovém prostředí než v kterém probíhají primární práce. Toto je kouzlo integrace, kterou díky podrobnému popisu navržené metodiky, lze v podnikových systémech zajistit.

Navrhovaná metodiky by tak mohla napomáhat opatření Evropské unie zaměřené na posílení politiky bezpečnosti sítí a informací a v boji proti kyberkriminalitě v rámci strategie EU pro rok 2020.

7 Závěr

Dynamický rozvoj informačních a komunikačních technologií, masové využívání internetu, stále více rostoucí obliba sociálních síti, digitalizace v komerční a nekomerční sféře s sebou přináší i negativní jevy v oblasti bezpečnosti a ochrany dat.

Stále častěji vzniká problém zabezpečení veřejně distribuovaných grafických dat, které nemají parametry chráněné komunikace a jejichž zabezpečení je tím daleko složitější.

Předložená disertační práce se proto zabývala technikami ukrývání digitálních dat a steganografií jako možností zabezpečení veřejně přístupných grafických dat.

Hlavním cílem práce bylo nalézt, navrhnout a detailně popsat takový způsob zabezpečení veřejně přístupných grafických dat, který zajistí vyšší ochranu autorských práv a současně bude minimalizovat negativní důsledky při případném odcizení těchto dat. Navržený způsob (metodiku) bude možné implementovat jak v rámci různorodých podnikových systémů, tak samostatně.

Tento hlavní cíl byl postupně naplňován prostřednictvím řešení dílčích cílů, které byly seskupeny do tří logických celků.

1) Teoretická východiska související s problematikou práce

V teoretické části práce byla především analyzována problematika steganografických a vodoznakových systémů. Pozornost byla věnována zejména možnostem zabezpečení obrazových dat pomocí těchto metod. Mezi dílčí teoretická východiska disertační práce patřily také oblasti:

- Legislativa autorských a trestních práv,
- strategie EU pro rok 2020,
- problematika barev a jejich vnímání lidským okem,
- grafický model RGB,
- specifikace grafických formátů.

Na základě získaných poznatků a dílčích závěrů z teoretické části práce byly učiněny předpoklady a východiska pro část praktickou. Mezi základní oblasti východisek byly uvedeny:

- Variabilní možnosti implementace obecné metody,
- volba bitové roviny,
- vlastnosti vodoznaku a variabilita jeho vkládání,
- vlastnosti fyziologie lidského zrakového systému,
- základní vlastnost steganografických systémů.

2) Návrh metodiky EZOD (Efektivní Zabezpečení Obrazových Dat)

Stěžejní částí předkládané disertační práce byl návrh metodiky EZOD (Efektivní Zabezpečení Obrazových Dat), která vychází z teoretických poznatků a přináší širší možnosti při zabezpečení grafických dat.

V následujícím výčtu jsou shrnuty požadavky na metodiku EZOD, jež byly v práci stanoveny a kterých mělo být návrhem metodiky dosaženo. U každého požadavku je uvedeno jakým způsobem bylo zajištěno jeho naplnění:

1. *Poskytovat účinné zabezpečení obrazových dat*
   Účinné zabezpečení obrazových dat bylo zajištěno na základě řady testování v rámci plnění jednotlivých kritérií na steganografické a vodoznakové systémy. Je však nutné v této souvislosti podotknout, že tyto systémy z technického hlediska prostě nemohou poskytnout stoprocentní ochranu proti různorodým útokům. Tento fakt je zřejmý z obrázku č. 4.1, kde je možné vidět protichůdné mechanizmy, které na sebe vzájemně působí.

2. *Splňovat maximum požadavků na steganografické a vodoznakové systémy*

   (h) ***Imperceptibilita*** *- změny způsobené vkládáním vodoznaku by neměly zhoršovat vnímanou kvalitu obrazu.*
   Imperceptibilita byla analyzována při vkládání vodoznaku do různých bitových rovin na základě objektivních i subjektivních kritérií. Výsledná hranice nevnímatelnosti lidským zrakem byla stanovena na 6. bitovovou rovninu modré barvy a 5. bitovou rovinu červené či zelené barvy (lépe vkládat do červené). V těchto rovinách je jistota nevnímatenosti vodoznaku. V určitých případech je možné dosáhnout nevnímatenosti i ve vyšších bitových rovinách, nicméně zde už je nutné testovat každý výsledný obraz zvlášť.

   (i) ***Spolehlivá detekce*** *– vodoznak by měl představovat dostatečný a spolehlivý důkaz o vlastnictví produktu.*
   V rámci výzkumné části byl demonstrován rozklad na bitové roviny, vkládání a zpětná extrakce vodoznaku, která poskytuje jednoznačný důkaz vlastnictví.

   (j) ***Přidružený klíč*** *– vodoznak by měl být přidružený s tzv. klíčem vodoznaku, který je používán na sestavení, detekci a odstranění vodoznaku.*
   Pro vkládání a zpětnou extrakci vodoznaku je v modifikovaném algoritmu nutné znát permutační a depermutační funkci, bitovou rovinu(y) a barvu(y) do které(kterých) byl vodoznak vložen, způsob rozmístění vodoznaku do obrazu a funkci pro samotné vkládání a extrakci.

   (k) ***Statistická nedetekovatelnost*** *– vodoznak by neměl být identifikovatelný použitím statistických metod.*
   Statistická nedetekovatelnost byla testována na základě histogramů. Histogram obrazu s vloženým vodoznakem a histogram originálního obrazu by neměly vykazovat výrazné odlišnosti. Z výsledků testování vyplývá, že až do 3. bitové roviny nelze prakticky rozeznat jakékoliv změny. Od 4. bitové roviny již lze pozorovat drobné změny. Nutno však podotknout že, případný útočník

k dispozici originální obraz nemá, tedy tyto drobné změny nejsou nikterak zásadní.

(l) ***Vícenásobné vkládání vodoznaku*** *– algoritmus by měl umožňovat vkládání dostatečné množství rozdílných vodoznaků. Každý vodoznak by měl být detekovatelný použitím příslušného jedinečného klíče.*
Výsledný modifikovaný algoritmus umožňuje vkládání jednoho vodoznaku vícenásobně a taktéž vkládání různých vodoznaků do jednoho obrazu. Výsledná metodika navíc dokonce doporučuje vkládání vodoznaku do dvou bitových rovin zároveň – konkrétně vždy do liché a sudé bitové roviny pro zvýšení robustnosti vodoznaku a spolehlivou detekci.

(m) ***Robustnost*** *– vodoznak použitý jako ochrana autorských práv, by měl být detekovatelný až do bodu, kdy kvalita hostitelského obrazu zůstává v akceptovatelných hranicích, tzn. měl by být imunitní (odolný) vůči neúmyslným i úmyslným operacím s daty.*
V rámci výzkumné části práce byla ověřována odolnost algoritmu proti možným útokům. Byla testována odolnost proti ořezu, šumu, zvyšování a snižování jasu, odolnost proti opětovnému ukládání obrazu do formátu JPEG, rotaci obrazu, změnu velikosti a taktéž již zmíněné statistické nedetekovatelnosti vodoznaku. V rámci těchto testování a za předpokladu platnosti požadavku imperceptibility dosahuje vodoznak při vkládání do 7. bitové roviny modré barvy a 6. bitové roviny červené barvy následující **pozitivní výsledky:**
- Odolnost proti ořezu – až k 80ti procentům,
- odolnost proti šumu – až k 80ti procentům,
- odolnost proti zvyšování jasu – až k hranice 200 jednotek,
- odolnost proti snižování jasu – až k hranici 220 jednotek,
- odolnost proti znovu uložení obrazu do ztrátového formátu JPEG – až k hranici 35% ztrátové komprese,
- odolnost proti statistické nedetekovatelnosti je částečně narušena od 4. bitové roviny.

Algoritmus však neposkytuje odolnost proti:
- Rotaci,
- změně velikosti.

(n) ***Bezpečnost*** *– vodoznak by neměl být extrahován z označených dat bez znalosti algoritmu vkládání a extrakce.*
Tento požadavek je zajištěn částečně statistickou nedetekovatelností. Taktéž bylo doporučeno pro velké množství obrazů vkládat různé vodoznaky, tím je možné zajistit odolnost proti útokům založeným na poznání části procesu vkládání.

3. *Minimalizovat důsledky odcizení obrazových dat*
Minimalizace důsledků odcizení je naplněna v případě jednoznačného určení autorství k danému dílu, tzn. vodoznak je možné z odcizených obrazových dat účinně detekovat. Tento požadavek byl naplněn, nicméně v případě možných útoků je třeba si uvědomit již uvedená omezení.

4. *Poskytovat jasný postup pro možnou implementaci v různorodých podnikových systémech i samostatně*
   Na základě řady testování, poznatků a dílčích závěrů byl v práci uveden výsledný popis metodiky EZOD, nejdříve samotného algoritmu a posléze postupu jeho efektivního využití. Samotný algoritmus je popsán v kapitole 5.5.9.1, na jehož základě lze možnou implementaci v podnikových systémech uskutečnit v různých programovacích jazycích s využitím podobných funkcí těmto jazykům náležícím.
   Samotný metodický postup byl rozdělen na tzv. dávkové neboli hromadné zpracování obrazů a postupné neboli manuální zpracování. Tento postup se liší především tím že u manuálního způsobu lze testovat možnost vkládání do vyšších bitových rovin pro zvýšení odolnosti vodoznaku. Základní postup pro tyto způsoby je možné shrnout do následujících dvou fází:
   - **Fáze 1: Vkládání viditelného vodoznaku –** zahrnuje výběr vhodného viditelného vodoznaku a jeho vložení. Tato fáze je stejná pro oba způsoby (dávkové i manuální zpracování).
   - **Fáze 2: Vkládání neviditelného vodoznaku –** zahrnuje volbu vhodného vodoznaku nebo i více vodoznaků, volbu bitových rovin, barev a samotného vkládání. U dávkového zpracování je dle předešlých testování zvolená automatická volba 6. bitové roviny modré barvy a 5. bitové roviny červené barvy. U manuálního zpracování obrazu je možnost testování i vyšších bitových rovin, dokonce zřídka i 8. bitové roviny modré barvy. U vysoko frekvenčních obrazů je vkládání do 7. bitové roviny modré barvy téměř vždy možné (podrobnosti viz. kapitola 5.5.9.2.2).

     V rámci dávkového zpracování dosahuje výsledný obraz následujících vlastností:
     - Odolnost proti ořezu – až k 80ti procentům,
     - odolnost proti šumu – až k 80ti procentům,
     - odolnost proti zvyšování jasu – až k hranice 200 jednotek,
     - odolnost proti snižování jasu – až k hranici 220 jednotek,
     - odolnost proti znovu uložení obrazu do ztrátového formátu JPEG – až k hranici 51% ztrátové komprese,
     - odolnost proti statistické nedetekovatelnosti bude však částečně nikoliv však výrazně narušena,
     - nebude odolný proti rotaci a změně velikosti,
     - neohrožují jej prezentační a interpretační útoky,
     - neměli by jej ohrozit ani právní útoky,
     - imperceptibilita zajištěna.

   Z výše uvedeného vyplývá že při manuálním zpracování mohou být hodnoty ještě příznivější (viz. opět kapitola 5.5.9.2.2)

5. *Umožňovat vkládání označení udělení oprávnění k dílu jiné osobě/osobám*
   Tento požadavek byl s plněn možností vkládat několik vodoznaků do obrazu. Tzn. v tomto případě by bylo možné vložení vodoznaku autora a vodoznaku osoby, které autor udělil oprávnění k dílu. Dokonce je možné vkládat i další informace vztahující se k tomuto oprávnění, jako např. datum udělení oprávnění, doba platnosti, informaci zda je licence výhradní či nevýhradní apod.

V rámci návrhu metodiky EZOD byly naplněny dílčí cíle. A je možné říci, že tato metodika splňuje základní kritéria na steganografické a vodoznakové systémy a její implementace v podnikových systémech nebo i samostatně zajistí jednoznačný důkaz autorství.

3) Praktická aplikace metodiky

V rámci naplnění dílčího cíle v oblasti praktické aplikace metodiky EZOD bylo uvedeno osm ukázek, z toho 4 autorské obrazy a 4 obrazy využívané pro testování obrazových dat v odborné literatuře. Na těchto obrazech byly demonstrovány výsledky manuální aplikace metodiky díky které bylo možné dosáhnout vložení vodoznaku u dvou vysokofrekvenčních obrazů až do 7. bitové roviny modré barvy a 6. bitové roviny červené barvy kdy odolnost proti útokům dosahovala následujících výsledků:

- Odolnost proti ořezu – až k 80ti procentům,
- odolnost proti šumu – až k 80ti procentům,
- odolnost proti zvyšování jasu – až k hranice 200 jednotek,
- odolnost proti snižování jasu – až k hranici 220 jednotek,
- odolnost proti znovu uložení obrazu do ztrátového formátu JPEG – až k hranici 35% - 40% ztrátové komprese,
- odolnost proti statistické nedetekovatelnosti bude však částečně nikoliv výrazně narušena,
- nebude odolný proti rotaci a změně velikosti,
- neohrožují jej prezentační a interpretační útoky,
- neměli by jej ohrozit ani právní útoky,
- imperceptibilita zajištěna.

U ostatních šesti obrazů byl vodoznak vkládán do 6. bitové roviny modré barvy a 5. bitové roviny červené barvy. Zde odolnost dosáhla těchto výsledků:

- Odolnost proti ořezu – až k 80ti procentům,
- odolnost proti šumu – až k 80ti procentům,
- odolnost proti zvyšování jasu – až k hranice 200 jednotek,
- odolnost proti snižování jasu – až k hranici 220 jednotek,
- odolnost proti znovu uložení obrazu do ztrátového formátu JPEG – až k hranici 51% ztrátové komprese,
- odolnost proti statistické nedetekovatelnosti bude však částečně narušena,
- nebude odolný proti rotaci a změně velikosti,
- neohrožují jej prezentační a interpretační útoky,
- neměli by jej ohrozit ani právní útoky,
- imperceptibilita zajištěna.

Navržená metodika EZOD byla v práci porovnána s profesionálním nástrojem Digimarc od stejnojmenné firmy a s freeware nástrojem SignMyImage. Pro srovnání s metodikou EZOD byla využita nejvyšší možná ochrana v obou nástrojích. V rámci metodiky EZOD bylo nejdříve srovnání prováděno pro dávkové zpracování (tzn. 6. bitová rovina modré barvy a 5. bitová rovina červené barvy) a následně pro manuální zpracování, kde byla využita 7. bitová rovina modré barvy a 6. bitová rovina červené barvy. Při testování byla zajištěna vlastnost imperceptibility. Výsledky srovnání jsou uvedeny v následující tabulce, podrobně jsou rozebírány v kapitole 6.2.

testování/srovnávané postupy	Digimarc	SignMy Image	EZOD (dávkové zpracování)	EZOD (manuální zpracování)
ořez	do 80 %	není	do 80 %	do 80 %
šum	až 20 %	není	až 200 %	až 200 %
snížení jasu	do 200	není	do 200	do 200
zvýšení jasu	do 190	není	do 220	do 220
ukládání do JPEG	až 30 %	až 50 %	až 50 %	až 35 %
rotace	ano	ne	ne	ne
změna velikosti	ano	ano	ne	ne
statistická nedetekovatelnost	výrazné změny	výrazné změny	nevýrazné změny	nevýrazné změny
možnosti vkládání více vodoznaků	ne	ne	ano	ano

Na základě výsledků srovnání, lze konstatovat, že navržená metodika EZOD je jednoznačně konkurenčním řešením. Navíc s využitím několikanásobného ukládání vodoznaku poskytuje širší využití při označování grafických dat. Taktéž díky konkrétnímu popisu algoritmu a postupu pro efektivním zabezpečení obrazových dat, poskytuje možnost implementace do různorodých podnikových systémů, tzn. neomezuje se pouze na integraci do čistě grafických nástrojů, ale poskytuje širší využití v rozmanitých oblastech práce s grafickými informacemi.

Závěrečná část práce poukazuje na konkrétní oblasti vhodné pro aplikaci navržené metodiky. Tuto metodiku je možné využívat v různorodých oblastech a oborech, z nichž byly definovány následující (podrobněji popsáno v kapitole 6.3):

- Webové stránky s různého zaměření,
  - Fotobanky
  - Fotogalerie
  - Různorodé internetové obchody
  - Realitní kanceláře
  - Nejrůznější on-line prezentace
    - Firem a nejrůznějších organizací
    - Výrobků a služeb
    - Osob atd.
- Off-line prezentace distribuované prostřednictví různých médií,
- Vkládání označení udělení oprávnění k dílu jiné osobě/osobám v rámci autorského zákona (udělení licence),
- Oblast digitalizace v nekomerční i komerční sféře. Významnou roli by mohla hrát metodika zejména ve státní správě. (Označování skenovaných dat datem a dalšími potřebnými údaji, které mohou pomáhat v boji s korupcí a případnými podvrhy),
- Bankovní sektor (ukládání přídavných informací k obrazům k hypotečním případům, zasílání výpisů či pinů v obrazových datech – tzn. trend výběru fotografií klientů, další využití v rámci klientských služeb přímého bankovnictví – klientské portály),

- Digital rights management (DRM) - management digitálních práv. Tzn. využití metody jako jednu z technik DRM,
- Lékařství – např. zasílání lékařských předpisů.

Samotná integrace navrhované metodiky do různých podnikových systémů může přinést zefektivnění práce, kdy by bylo možné obrazová data označovat automaticky, bez jakýchkoliv dílčích úkonů, tzn. bez nutnosti označování dat v jiném programovém prostředí než v kterém probíhají primární práce. Toto je možnost, kterou díky podrobnému popisu navržené metodiky, lze v podnikových systémech zajistit.

Na základě naplnění dílčích cílů, je možné konstatovat i naplnění hlavního cíle disertační práce.

Prezentace veřejně přístupných grafických dat představuje velice účinný marketingový nástroj pro různé společnosti, firmy, státní správu a mnoho dalších institucí, avšak pouze za podmínek minimalizace rizika zneužití poskytovaných dat, jež by mohlo v opačném případě vést k negativním ekonomickým efektům.

Implementace navržené metodiky EZOD by měla pomáhat soukromým osobám, manažerům a pracovníkům na různé úrovni řízení ve společnostech a institucích s nejrůznějším zaměřením zabezpečit jejich prezentovaná veřejně přístupná grafická data a jejich další legální distribuci.

Navrhovaná metodiky by tak mohla také napomáhat opatření Evropské unie zaměřené na posílení politiky bezpečnosti sítí a informací a v boji proti kyberkriminalitě v rámci strategie pro rok 2020.

8 Seznam odborné literatury

[1] ARNOLD, M., SCHMUCKER, M., WOLTHUSEN, D. S. *Techniques and Applications of Digital Watermarking and Content Protection*. Boston: Artech House Publishers, 2003. ISBN: 1-58053-111-3.

[2] AUERBACH: *Investigator's Guide to Steganography*. c2004 Auerbach Publications 2004. Greg Kipper. ISBN:084932433

[3] BOLAND, F. M., RUANAIDH, J. J., DAUTZENBErg, C. *Watermarking Digital images for Copyright Protection.* Proc. of the 5th IEE International Conference on Image Processing and its Applications, no.410, Edinburgh, July 1995, pp.326-330.

[4] CEDERHOLM, D. *Webdesign s webovými standardy*. Přel. Jaroslav Blažek. 1. vyd. Brno: ZONER software, 2004. 255 s. Přel. z Web standards solutions: the markup and style handbook. ISBN 80-86815-15-3.

[5] COX, I. J., KILIAN, J., LEIGHTON, T., SHAMOON, T. *A Secure, Robust Watermark for Multimedia.* Information Hiding, Lecture Notes in Computer Science, vol.1174, pp.183-206, 1996.

[6] COX, I. J., MILLER, M. L., BLOOM, J. A. *Watermarking applications and their properties In: Proc. of the Int. Conf. on Information Technology'2000*, Las Vegas, 2000, pp.6-10.

[7] ČANDÍK, Marek. *Bezpečnosť informačných systémov, steganografia a digitálna vodotlač.* 1. vyd. Ostrava: OFTIS, 2005. 117 s. ISBN 80-239-5962-X.

[8] CHUN-SHIEN, L. *Multimedia Security: Steganography and Digital Watermarking Techniques for Protection of Intellectual Property*. Hershey: Idea Group Publishing, 2004. ISBN: 1-59140-275-1.

[9] DECKER, S. E*ngineering Considerations in Commercial Watermarking.* IEEE Communications Magazine, August 2001, vol.39, no.8, pp.128-133.

[10] DITTMANN, J., *Steganography and steganalysis in voice over IP scenarios*. Proc. of SPIE, Vol. 5681, Security, Steganography and Watermarking of Multimedia Contents VII, San Jose. pp. 607 - 618. 2005.

[11] DOBDA, L. *Ochrana dat v informačních systémech.* 1. vyd.. - Praha : Grada Publishing, 1998. 286 s. ISBN 80-7169-479-7.

[12] DZIK, P. *Teorie barevného vidění*[online]. 17.6.2001, [cit. 2010-11-03]. Dostupné z: <http://www.paladix.cz/clanek.php?aid=10012>.

[13] EVROPSKÁ KOMISE, P. *Strategie EU 2020* [online]. c2010, [cit. 2011-01-23]. Dostupné z: <http://ec.europa.eu/index_cs.htm>

[14] FLEET, D. J., HEEGER D. J. *Embedding Invisible Information in Color Images*, IEEE International conference on Image Processing, vol.1, pp.532-535, Santa Barbara, 1997.

[15] GRAY, Daniel. *Profesionální design na webu*. Přel. Tamara Váňová. 1. vyd. Brno: Soft Press, 2000. 223 s. Přel. z Looking good on the web. ISBN 80-902824-1-5.

[16] HAMLIN, J. Scott., *Grafika, animace, kouzla na Webu*. Přel. Ivana Kollingerová, et. al. 1. vyd. Brno: UNIS, 2000. 336 s. Přel. z Effective Web Animation: Advanced Techniques for the Web. ISBN 80-86097-45-5.

[17] HERINGOVÁ, B., HOR, P., *Matlab* [online]. c2005. Dostupné z : <http://www.cdm.cas.cz/czech/hora/vyuka/mvs/tutorial.pdf>.

[18] HOŠEK, J., *Vodoznačení video obsahu. Elektrorevue* [online]. c2007 [cit. 2010-08-16]. Dostupné z : <http://www.elektrorevue.cz/cz/download/vodoznaceni-video-obsahu/>.

[19] HSU, CH. T., WU, J. L., *Hidden Digital Watermarks in Images*, IEEE trans. On Image Processing. Vol.8, No.1, 1999, pp.58-68.

[20] JANČOVIČ, A., *Vnímání barev* [online]. c2005, [cit. 2010-08-11]. Dostupné z: < http://www.ped.muni.cz/wphy/publikace/Jancovic1.html>.

[21] JUSTICE. *Autorský zákon* [online]. c2010, [cit. 2010-10-26]. Dostupné z: <http://www.justice.cz>.

[22] JUSTICE. *Trestní zákon* [online]. c2010, [cit. 2010-10-28]. Dostupné z: <http://www.justice.cz>.

[23] KOŘÍNEK, David. *Svět multimediálního internetu.* c2000, roč. IIIX, č. 19, s. 12-15. ISSN 1210-8790.

[24] LÁTAL, I. *Ochrana informací, dat a počítačových systémů.* 1. vyd.. - Praha : Eurounion, 1996. 238 s. ISBN 80-85858-32-0.

[25] LUKÁČ, R., ČANDÍK, M. *The Influence of Noise Corruption to Image Watermarking in DCT Domain. Journal of Electrical Engineering*, No.3-4, Vol.52, 2001, pp. 81-87.

[26] MATHWORKS. *Product Documentation* [online]. c2010. Dostupné z: <http://www.mathworks.com/help/techdoc/>.

[27] METEŇKO, J. a kol.: *Kriminalistické metódy a možnosti kontroly sofistikovanej kriminality*. 1. vyd. Katedra kriminalistiky a forenzných disciplín, Akadémia PZ

v Bratislave. Bratislava 2004. s. 356. ISBN: 80-8054-336-4, EAN: 9788080543365.

[28] PELIKÁN Josef, SOCHOR Jiří. *Barva a barevné vidění* [online]. 15. 3. 2000, [cit. 2010-11-27]. Dostupné z: <http://www.fi.muni.cz/usr/sochor/M4730/>.

[29] PIHAN, R., *Vše o světle* [online]. 26.1.2007, [cit. 2010-12-27]. Dostupné z: <http://www.fotografovani.cz/art/fozak_df/rom_1_01_cojetosvetlo.html>.

[30] PODILCHUK, CH. I., DELP, E.J. *Digital Watermarking: Algorithms and Applications*. IEEE Signal Processing Magazine. July, 2001. pp. 33-46.

[31] POWELL, Thomas. *Web design Kompletní průvodce*. 1. vyd. Brno: Computer Press, 2004. 818 s. ISBN 80-7226-949-6.

[32] RODRYČOVÁ, D., STAŠA, P., *Bezpečnost informací jako podmínka prosperity firmy*. 1. vyd. Praha Grada Publishing, 2000. 143 s. ISBN 80-7169-144-5.

[33] SEITZ, J*., Digital Watermarking for Digital Media. Hershey: Information Science Publishing,* 2005. ISBN: 1-59140-518-1.

[34] STUCHLÍK, Petr, PEGNER, Martin a DVOŘÁK, Martin. *Marketing a reklama na internetu*. 1. vyd. Praha: Grada, 1998. 198 s. ISBN 80-7169-630-7.

[35] SWANSON, M. D., ZHU, B., TEWFIK, A. H.: *Transparent robust image watermarking.* In Proc. 1996 Int. Conf. Image Processing, vol. III, pp. 211-214.

[36] TEZAUR, R., *Barevné vidění: druhý pohled* [online]. 7.5.2003, [cit. 2010-12-12]. Dostupné z: <http://www.paladix.cz/clanky/barevne-videni-druhy-pohled.html>.

[37] TIŠNOVSKÝ, P., *Grafický formát BMP* [online]. 19.10.2006, [cit. 2010-10-12]. Dostupné z: <http://www.root.cz/clanky/graficky-format-bmp-pouzivany-a-pritom-neoblibeny/>.

[38] TIŠNOVSKÝ, P., *Programujeme JPEG* [online]. 25.1.2007, [cit. 2010-10-14]. Dostupné z: <http://www.root.cz/clanky/programujeme-jpeg-interni-struktura-souboru-typu-jfifjpeg/>.

[39] WATKINS, J., *Steganography - Messages Hidden In Bits. In: Proc. of the 2nd Int. Annual Conference on Multimedia Systems* [online] c2002, cit. [cit. 2011-01-14], Dostupné z: <http://mms.ecs.soton.ac.uk/mms2002/papers/6.pdf>.

[40] WANG, Z., LU, L., BOVIK, ALAN C. *Video Quality Assessment Based on Structural Distortion Measurement, Signal Processing: Image Communication,* Vol. 19, No. 2, P. 121-132, 2004.

[41] WAYNER, Peter, *Disappearing cryptography : information hiding: steganography & watermarking*. 2nd ed. Amsterdam : MK/Morgan KaufmannPublishers, 2002. 413 s. ISBN 1558607692.

[42] XIE, L., ARCE, G. R. *A Class of Authentication Digital Watermarks for Secure Multimedia Communication.* IEEE Transactions on Image Processing, vol.10, no.11, November 2001, pp.1754-1764.

[43] ŽÁRA, Jiří, BENEŠ, Bedřich a FELKEL, Petr. *Moderní počítačová grafika*. 2. vyd. Praha: Computer Press, 2006. 448 s. ISBN 80-7226-049-9.

[44] ŽIVĚ, *Steganografie - ukryjte, že máte tajemství* [online]. c2008, [cit. 2010-12-21]. Dostupné z: < http://uzivatel.blog.zive.cz/2008/10/steganografie-ukryjte-ze-mate-tajemstvi/>.

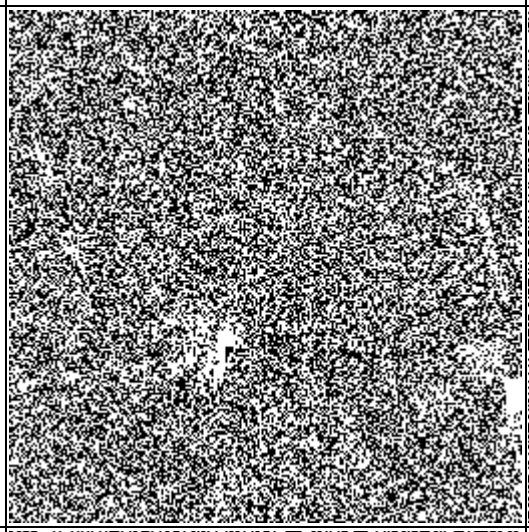
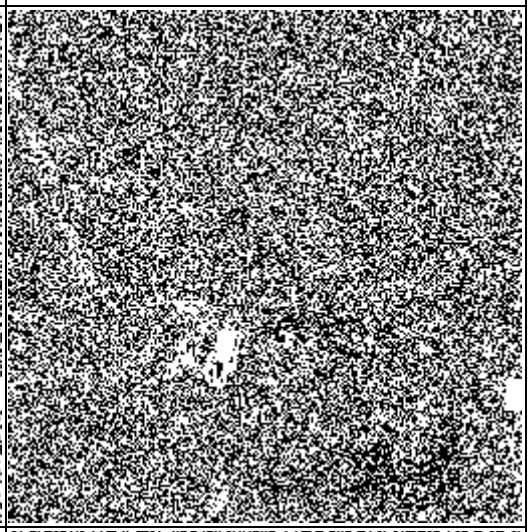
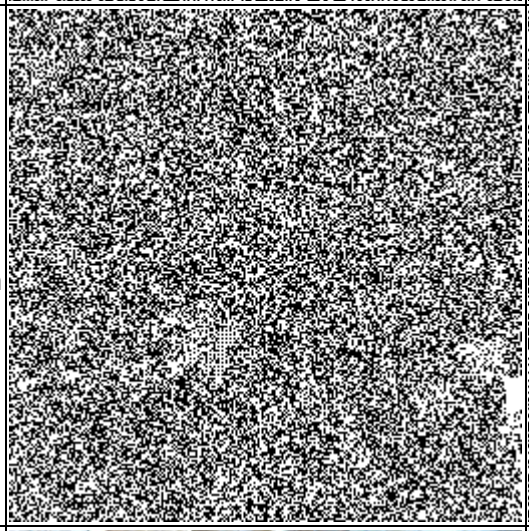
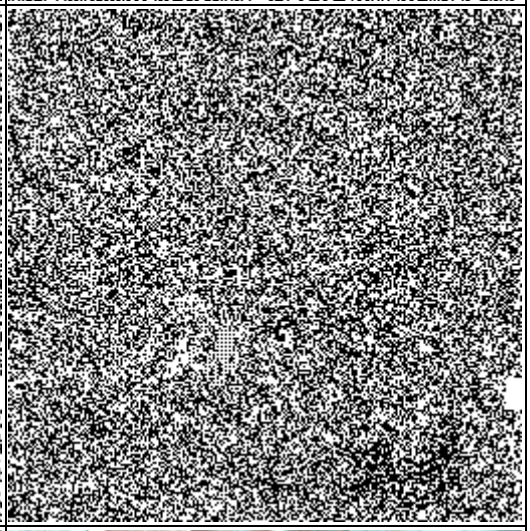
9 Seznam obrázků

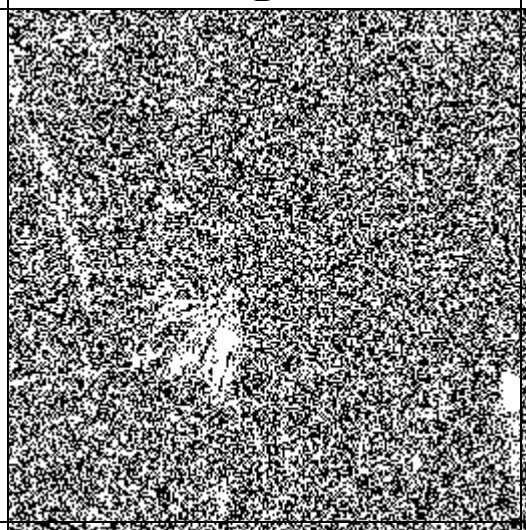
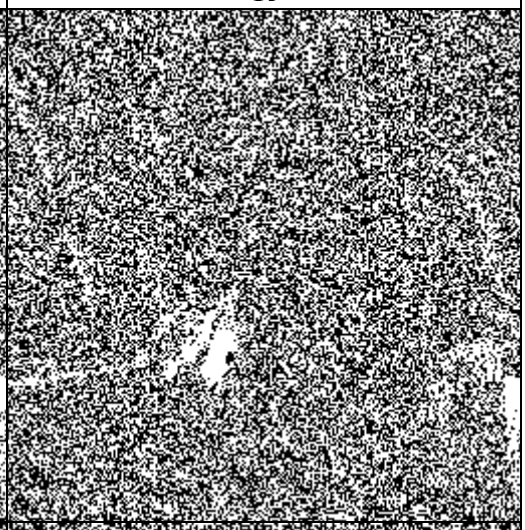
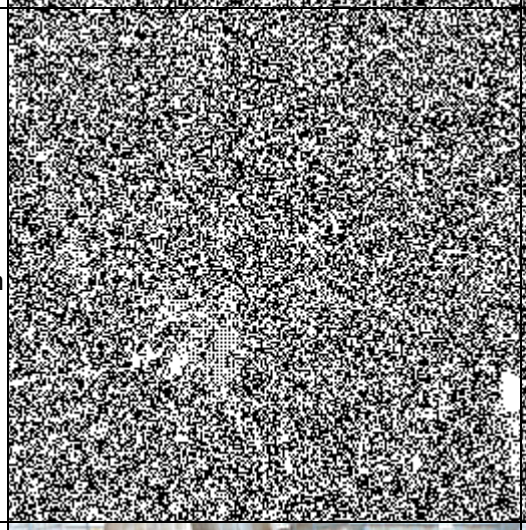
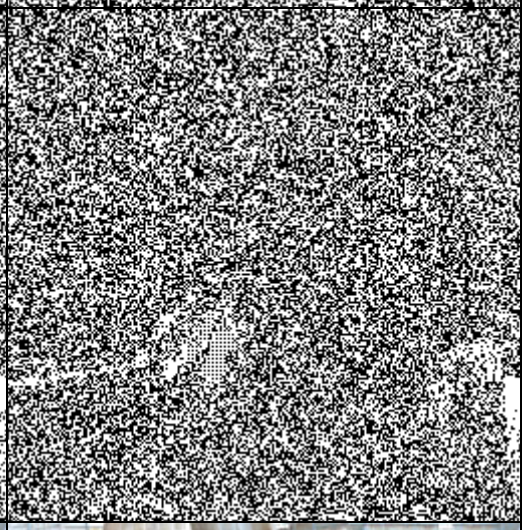
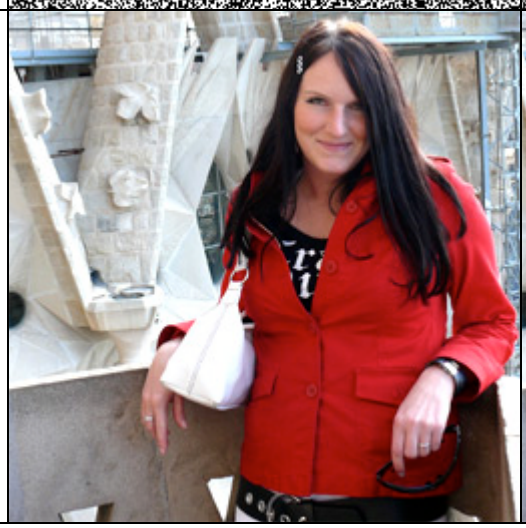
10 Seznam tabulek

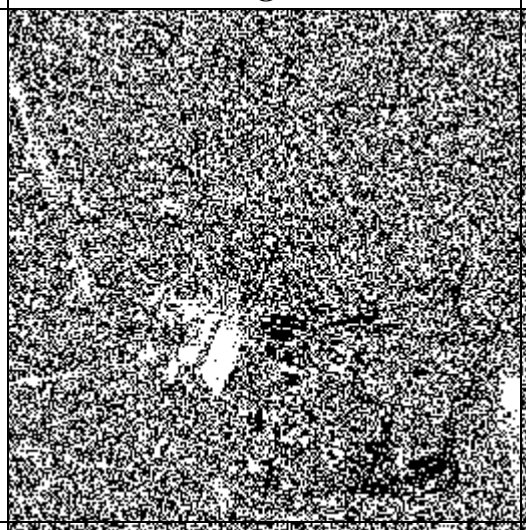
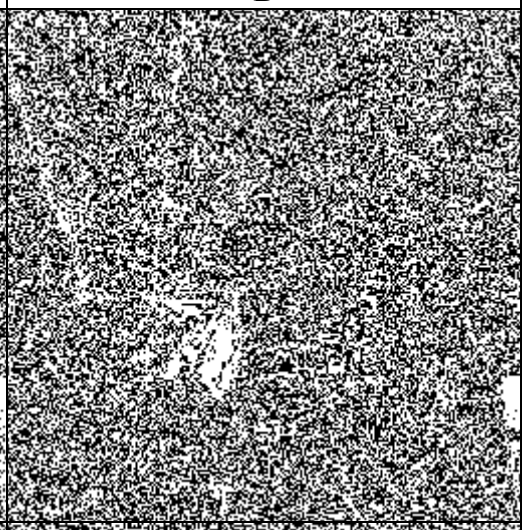
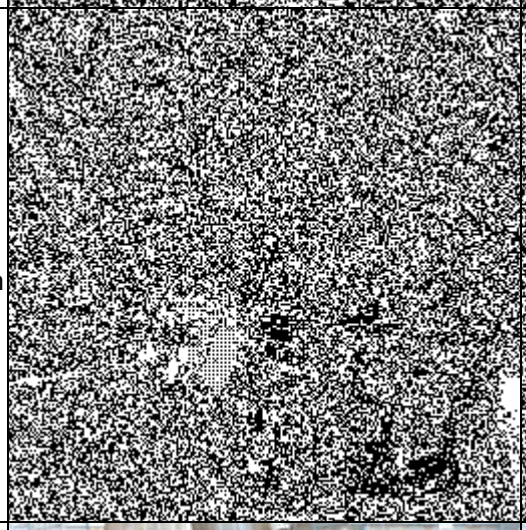
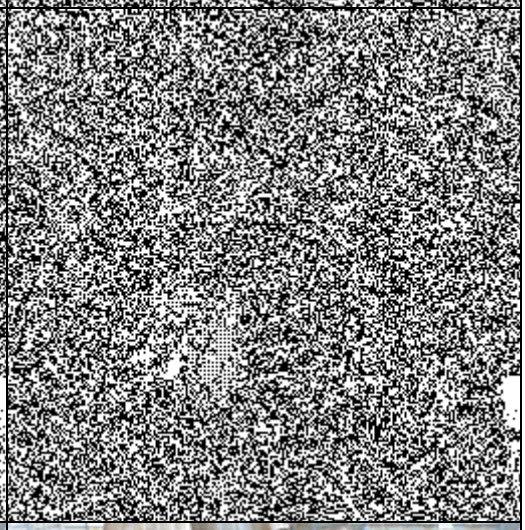
11 Seznam grafů

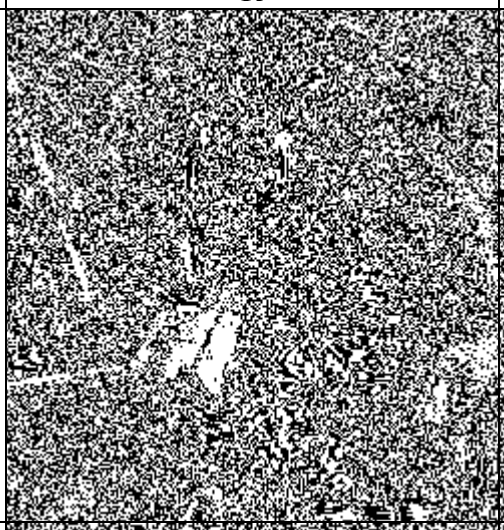
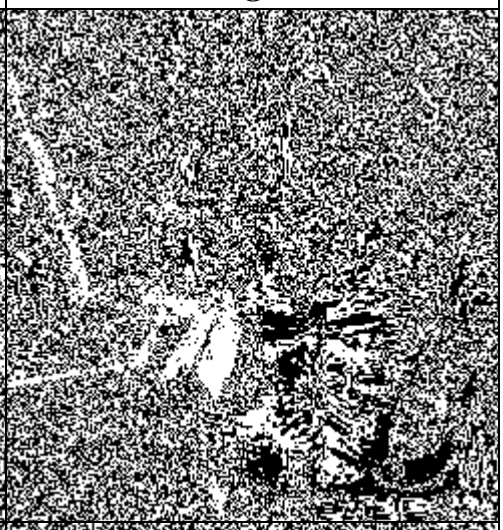
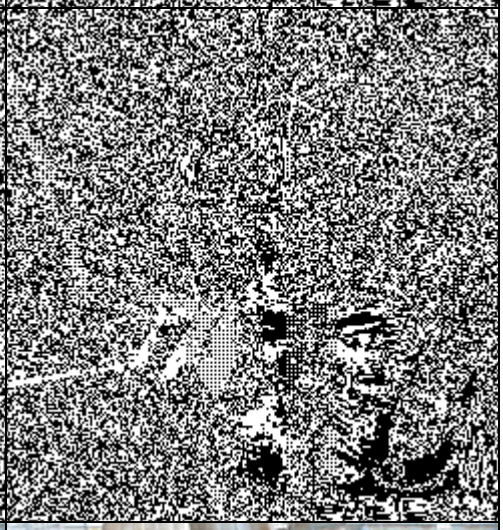
12 Přílohy

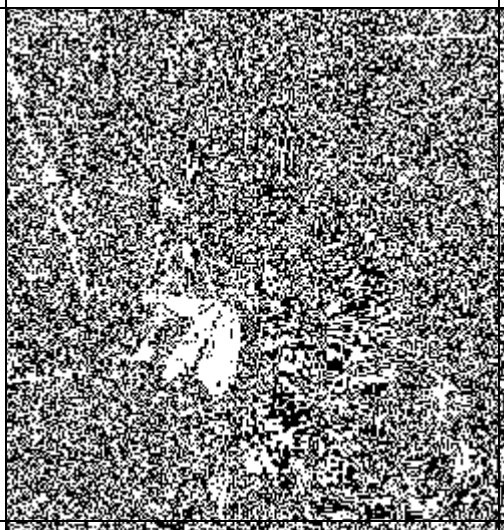
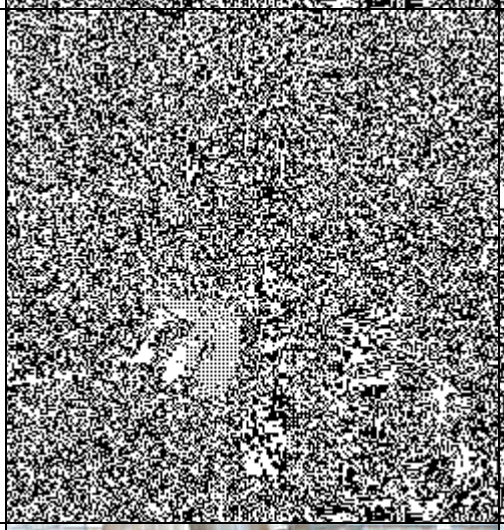
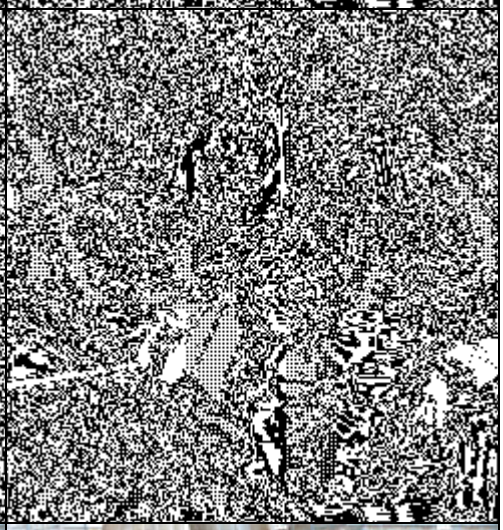
12.1 Vkládání vodoznaku do 8 bitových rovin

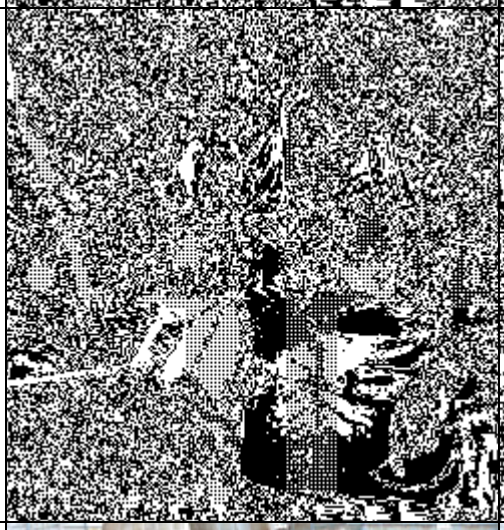
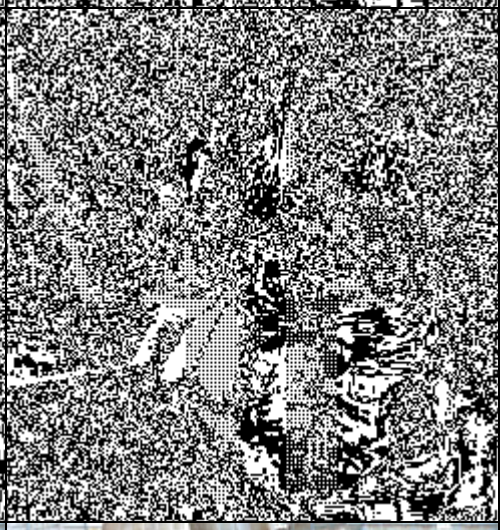
Číslo bitové roviny	1	1
Barva	R	G
Rovina bez vodoznaku		
Rovina s vodoznakem		
Výsledný obraz		

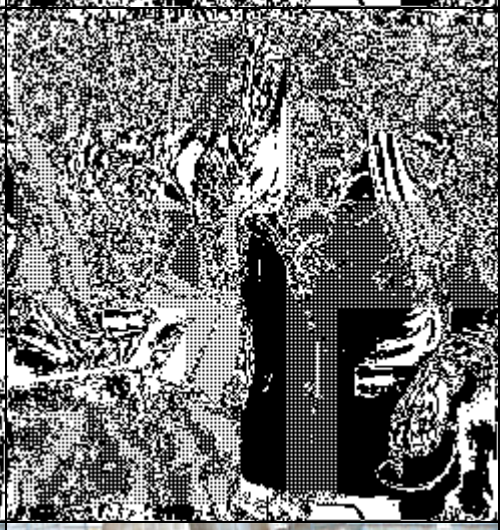
Číslo bitové roviny	1	2
Barva	B	R
Rovina bez vodoznaku		
Rovina s vodoznakem		
Výsledný obraz		

Číslo bitové roviny	2	2
Barva	G	B
Rovina bez vodoznaku		
Rovina s vodoznakem		
Výsledný obraz		

Číslo bitové roviny	3	3
Barva	R	G
Rovina bez vodoznaku		
Rovina s vodoznakem		
Výsledný obraz		

Číslo bitové roviny	3	4
Barva	B	R
Rovina bez vodoznaku		
Rovina s vodoznakem		
Výsledný obraz		

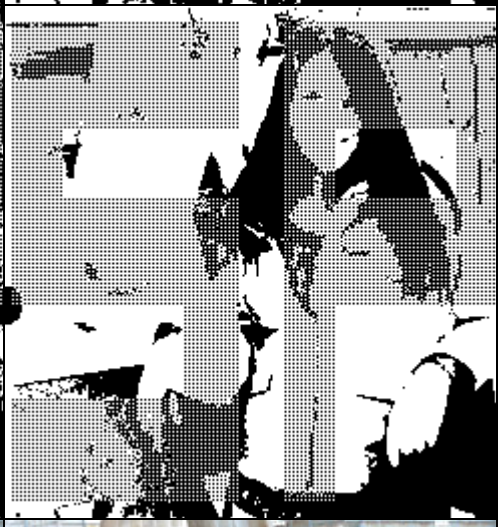
Číslo bitové roviny	4	4
Barva	G	B
Rovina bez vodoznaku		
Rovina s vodoznakem		
Výsledný obraz		

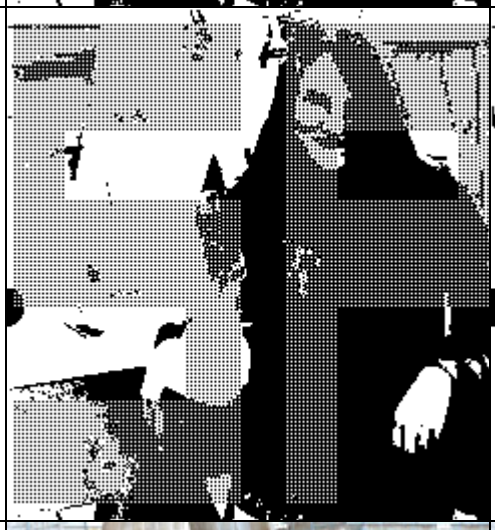
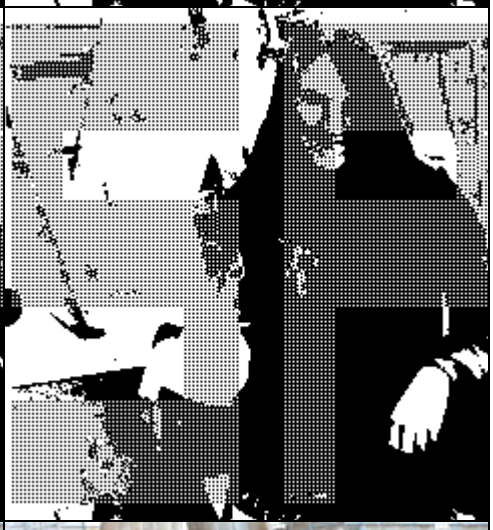
Číslo bitové roviny	5	5
Barva	R	G
Rovina bez vodoznaku		
Rovina s vodoznakem		
Výsledný obraz		

Číslo bitové roviny	5	6
Barva	B	R
Rovina bez vodoznaku		
Rovina s vodoznakem		
Výsledný obraz		

Číslo bitové roviny	6	6
Barva	G	B
Rovina bez vodoznaku		
Rovina s vodoznakem		
Výsledný obraz		

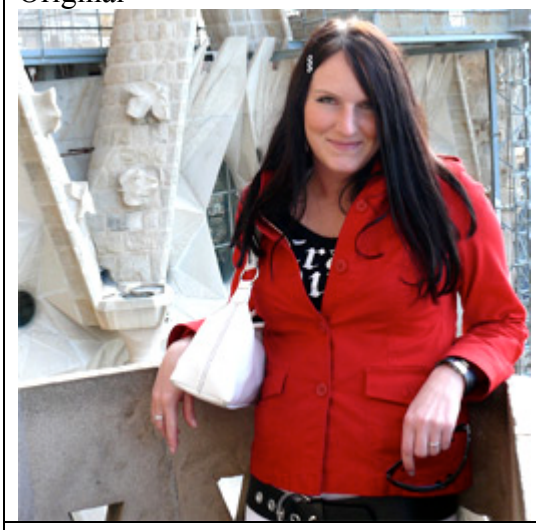
Číslo bitové roviny	7	7
Barva	R	G
Rovina bez vodoznaku		
Rovina s vodoznakem		
Výsledný obraz		

Číslo bitové roviny	7	8
Barva	B	R
Rovina bez vodoznaku		
Rovina s vodoznakem		
Výsledný obraz		

Číslo bitové roviny	8	8
Barva	G	B
Rovina bez vodoznaku		
Rovina s vodoznakem		
Výsledný obraz		

12.2 Vkládání do dvou bitových rovin zároveň

Originál



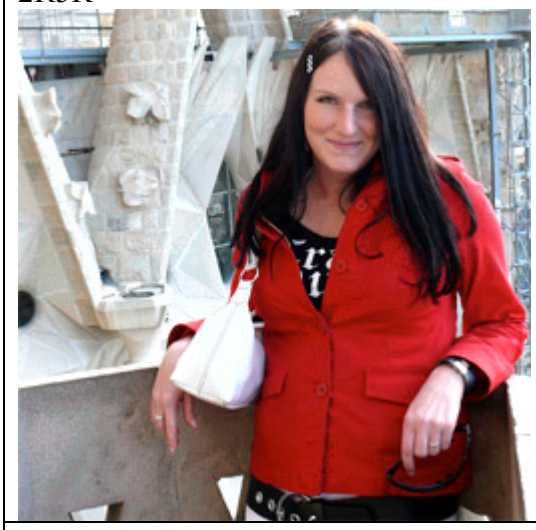
5R

1R2R

1R3G

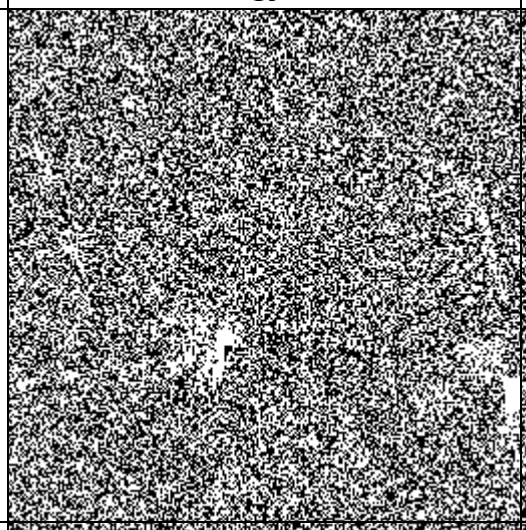
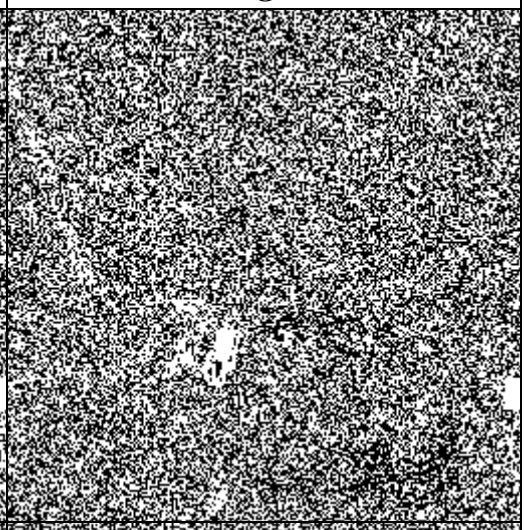
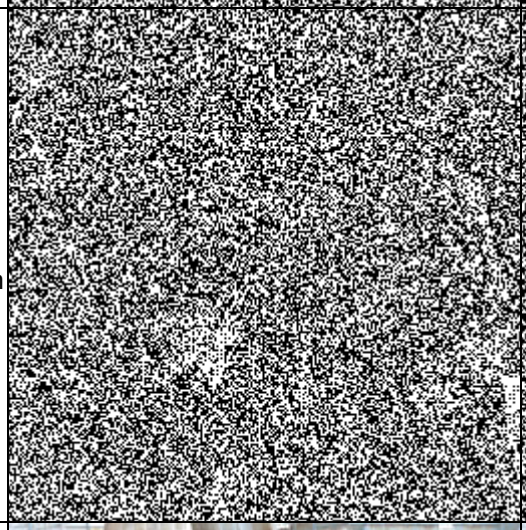
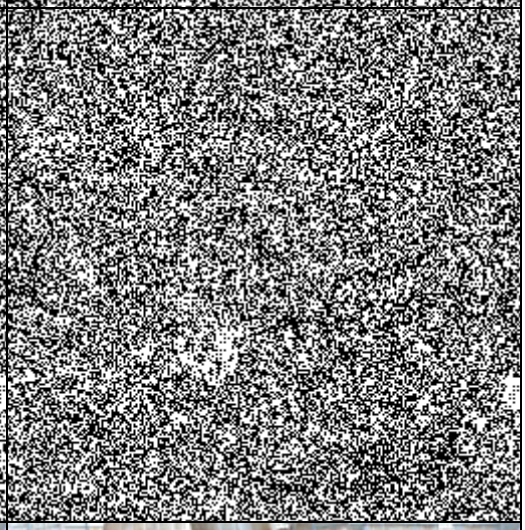
1G4G

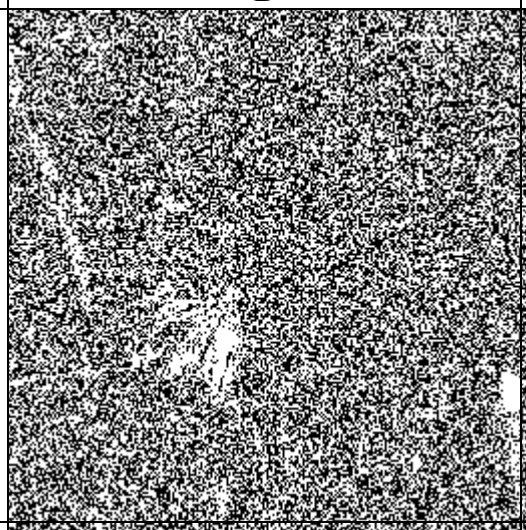
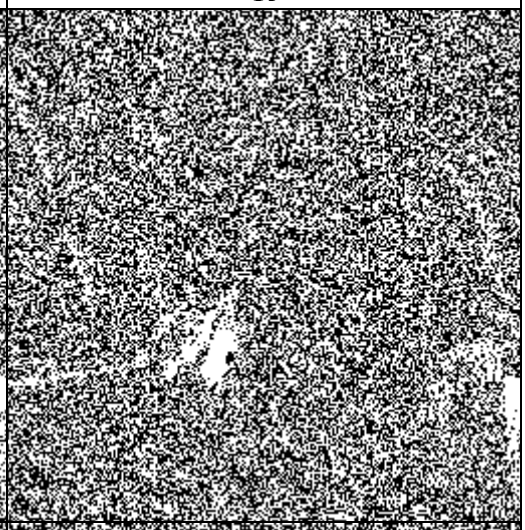
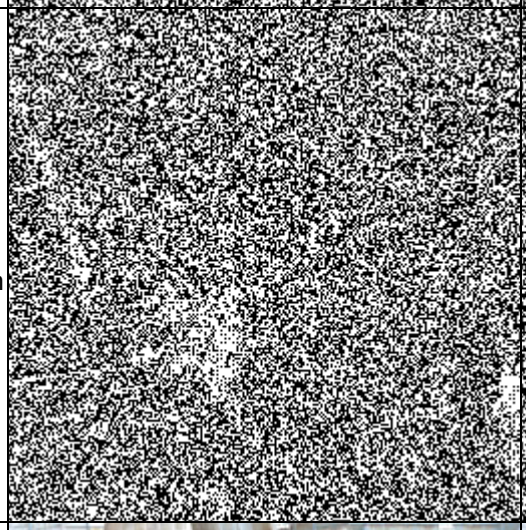
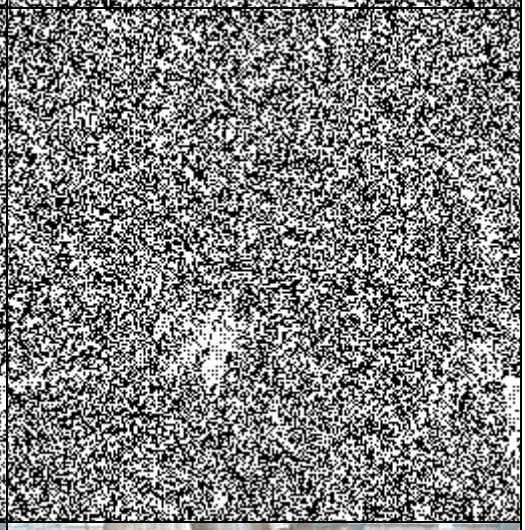
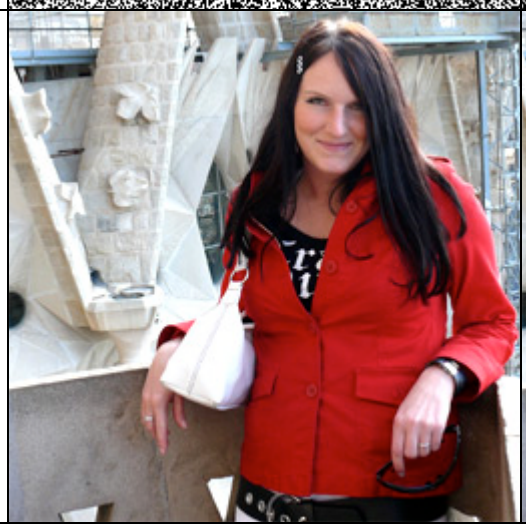
1R5R

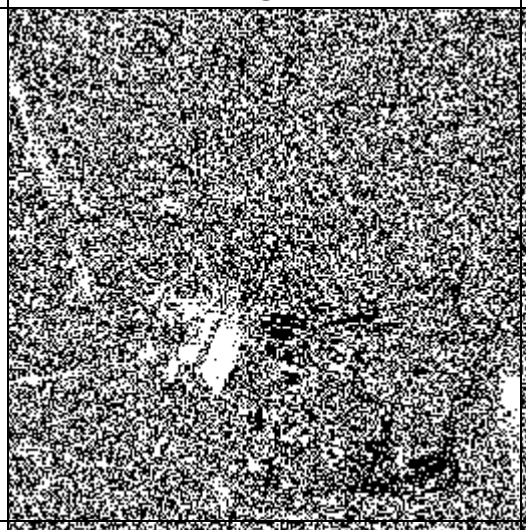
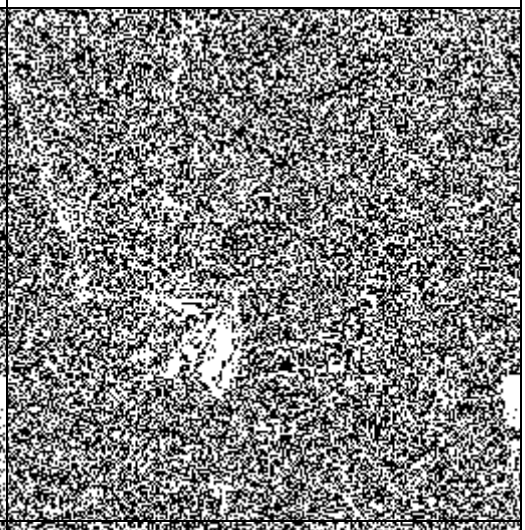
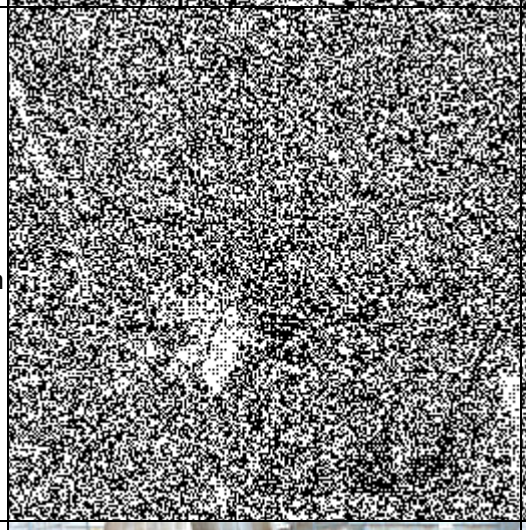
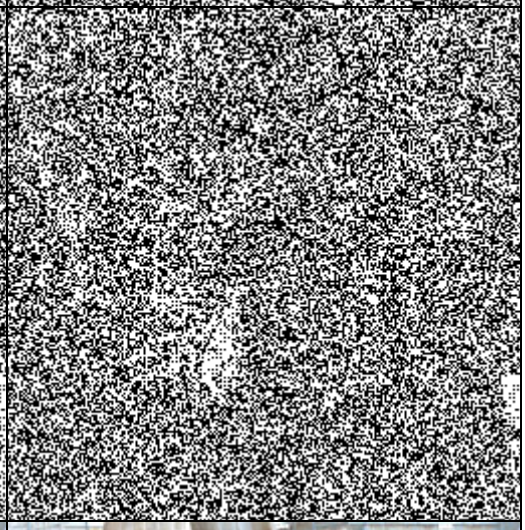
2B3B 	2B4R 
2R5R 	3G4G 
4B5B 	3G5G 

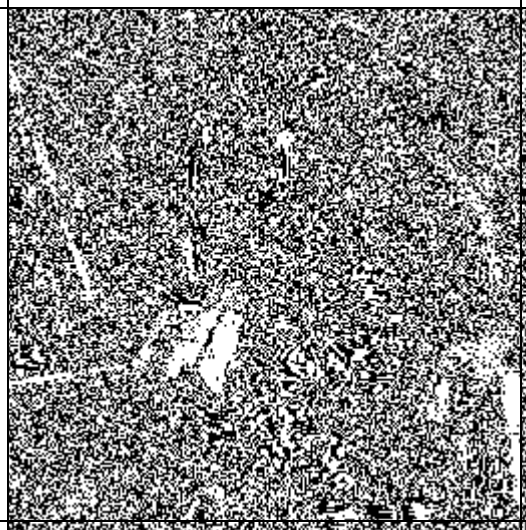
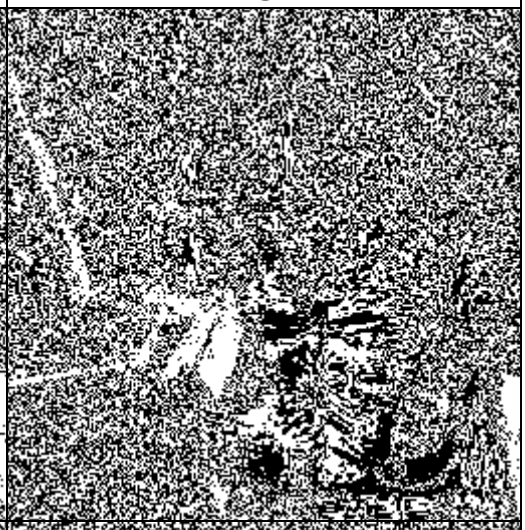
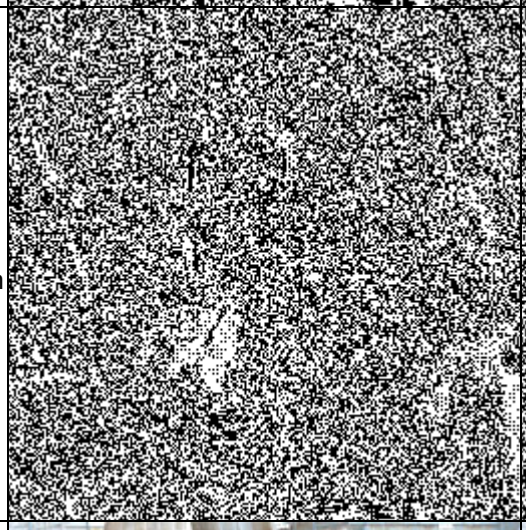
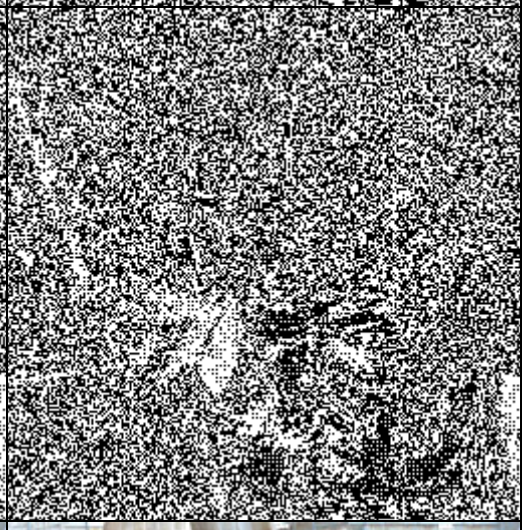
4G6G 	4R6R 
4B6B 	5G6G 
5R6R 	5B6B 

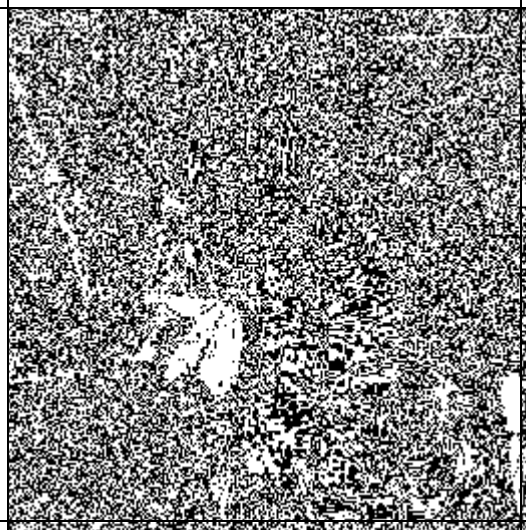
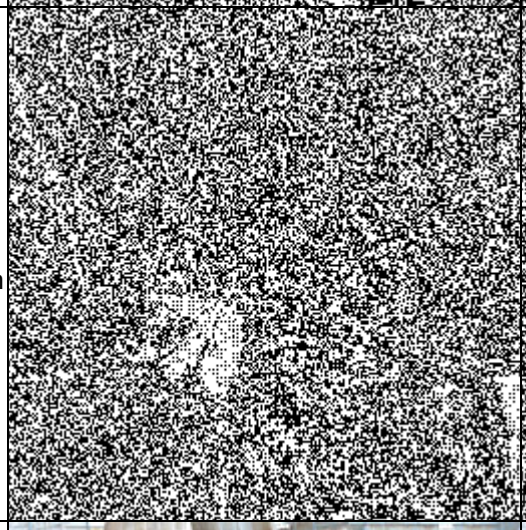
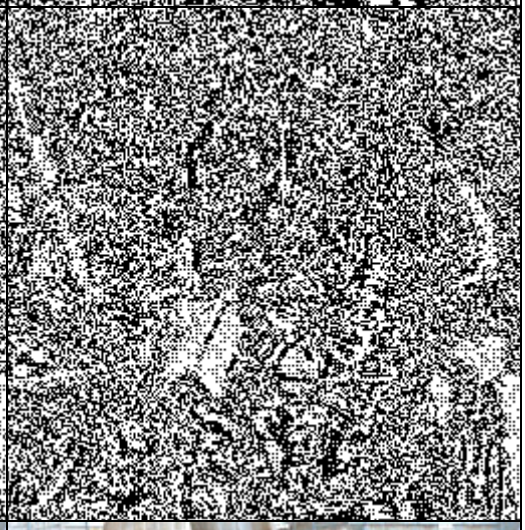
12.3 Rozklad obrazu na bitové roviny při využití permutovaného vodoznaku

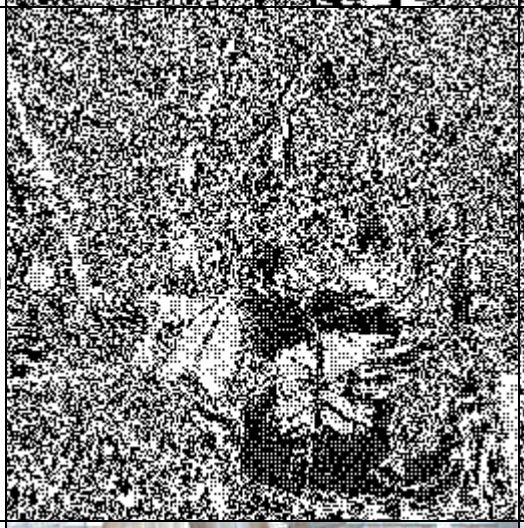
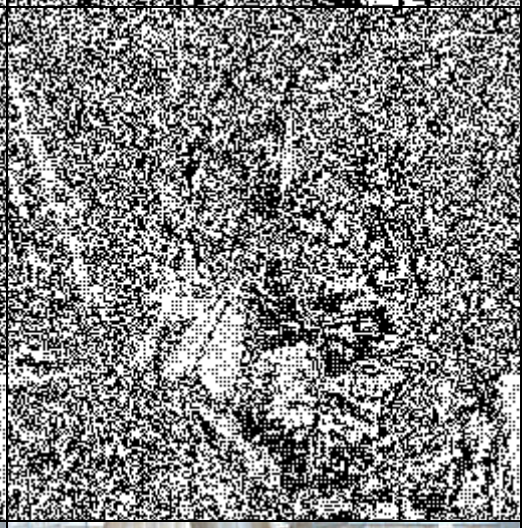
Číslo bitové roviny	1	1
Barva	R	G
Rovina bez vodoznaku		
Rovina s vodoznakem		
Výsledný obraz		

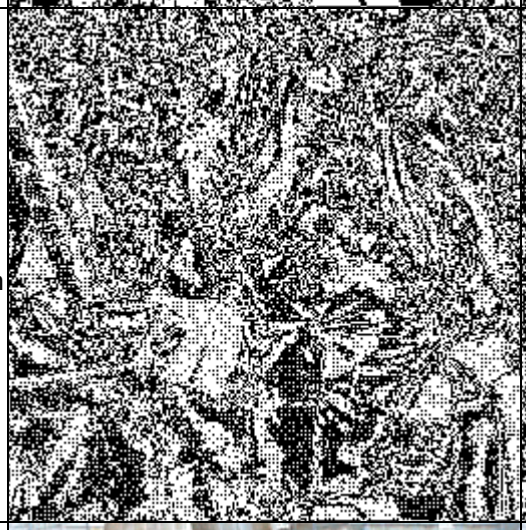
Číslo bitové roviny	1	2
Barva	B	R
Rovina bez vodoznaku		
Rovina s vodoznakem		
Výsledný obraz		

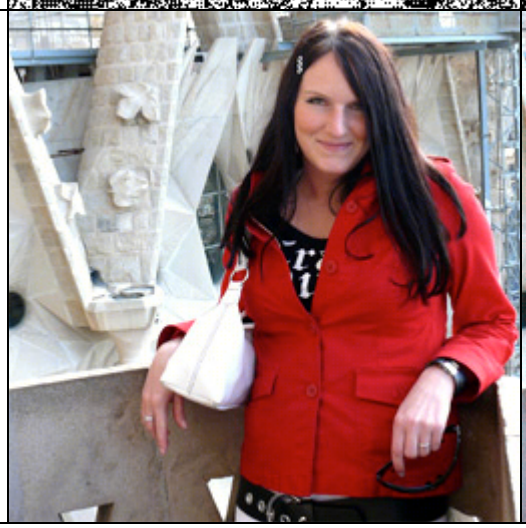
Číslo bitové roviny	2	2
Barva	G	B
Rovina bez vodoznaku		
Rovina s vodoznakem		
Výsledný obraz		

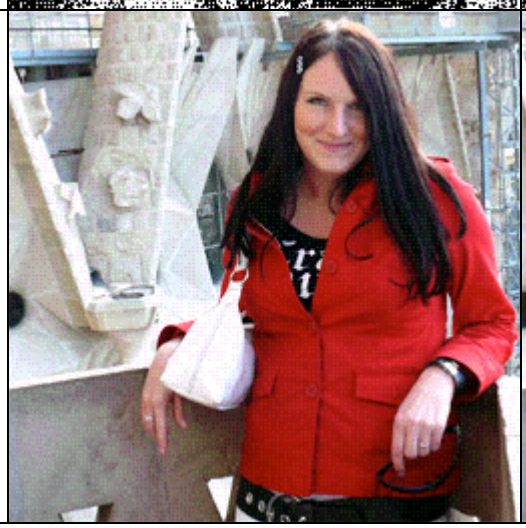
Číslo bitové roviny	3	3
Barva	R	G
Rovina bez vodoznaku		
Rovina s vodoznakem		
Výsledný obraz		

Číslo bitové roviny	3	4
Barva	B	R
Rovina bez vodoznaku		
Rovina s vodoznakem		
Výsledný obraz		

Číslo bitové roviny	4	4
Barva	G	B
Rovina bez vodoznaku		
Rovina s vodoznakem		
Výsledný obraz		

Číslo bitové roviny	5	5
Barva	R	G
Rovina bez vodoznaku		
Rovina s vodoznakem		
Výsledný obraz		

Číslo bitové roviny	5	6
Barva	B	R
Rovina bez vodoznaku		
Rovina s vodoznakem		
Výsledný obraz		

Číslo bitové roviny	6	6
Barva	G	B
Rovina bez vodoznaku		
Rovina s vodoznakem		
Výsledný obraz		

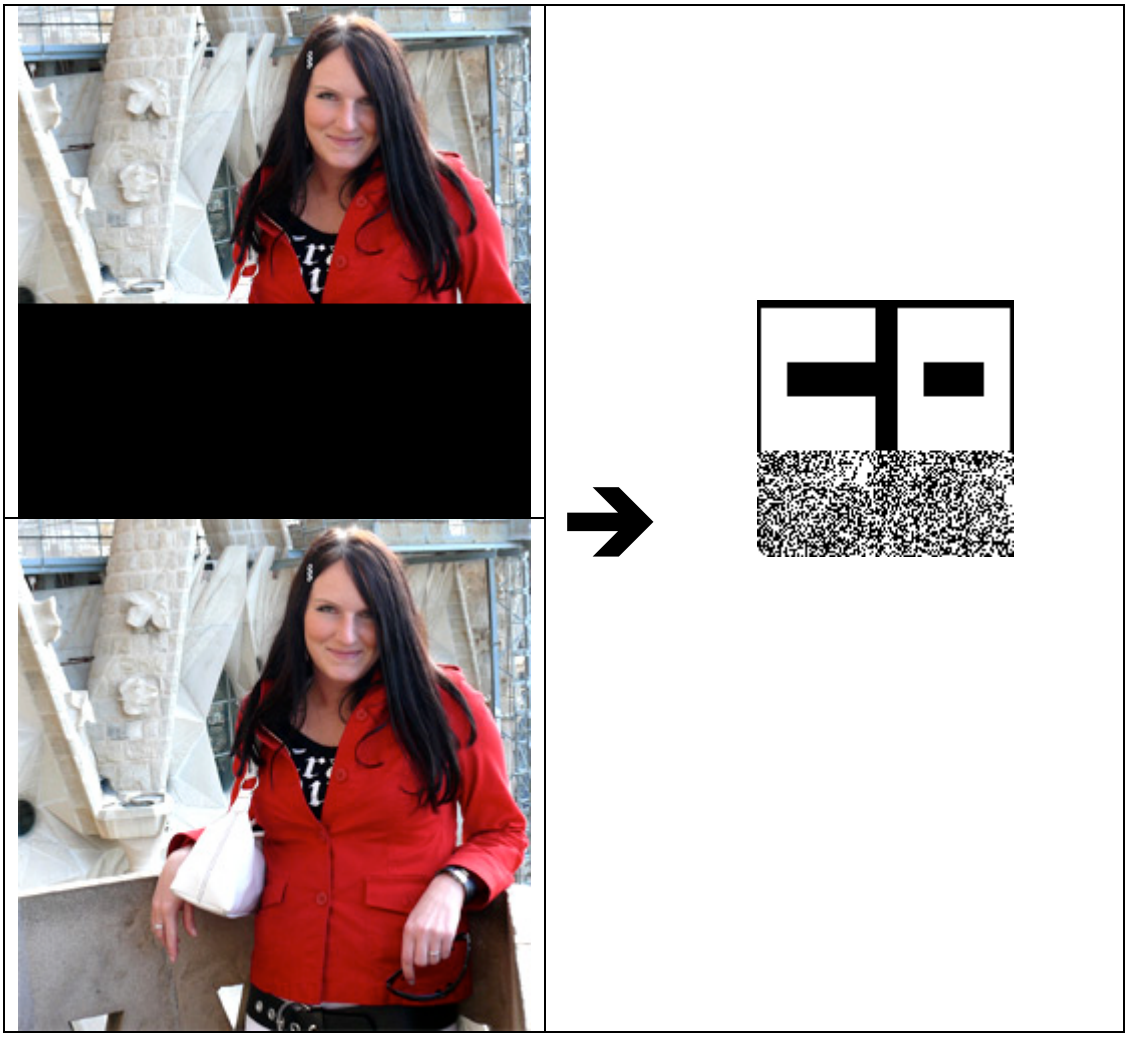
Číslo bitové roviny	7	7
Barva	R	G
Rovina bez vodoznaku		
Rovina s vodoznakem		
Výsledný obraz		

Číslo bitové roviny	7	8
Barva	B	R
Rovina bez vodoznaku		
Rovina s vodoznakem		
Výsledný obraz		

Číslo bitové roviny	8	8
Barva	G	B
Rovina bez vodoznaku		
Rovina s vodoznakem		
Výsledný obraz		

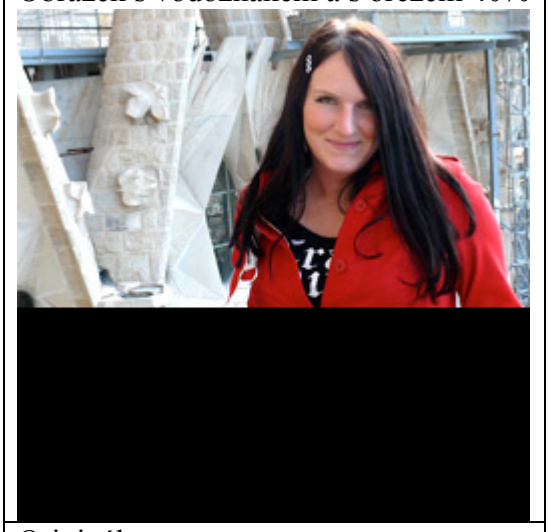
12.4 Tetování robustnosti

12.4.1 Ukázka neúčinné extrakce nepermutovaného vodoznaku

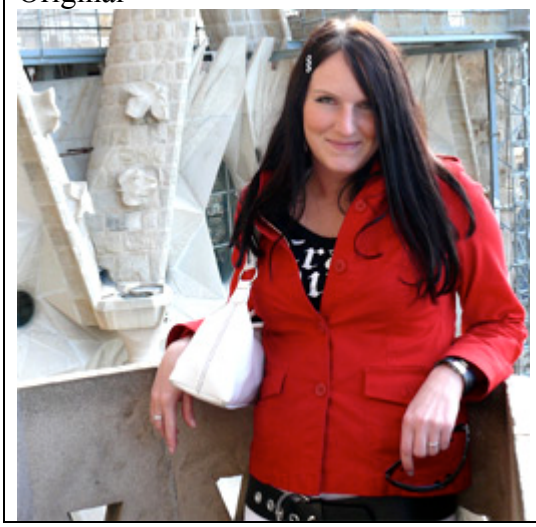


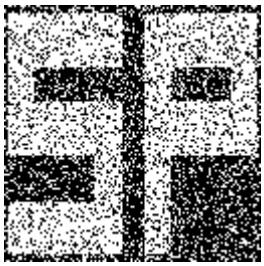
12.4.2 Odolnost proti ořezu

Obrázek s vodoznakem a s ořezem 40%

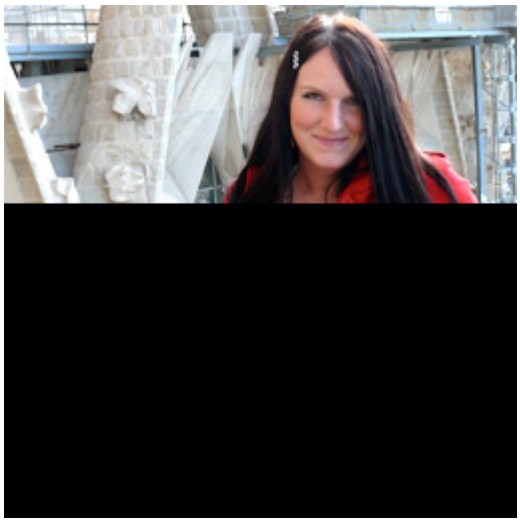


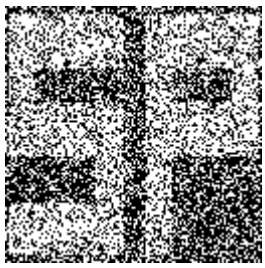
Originál



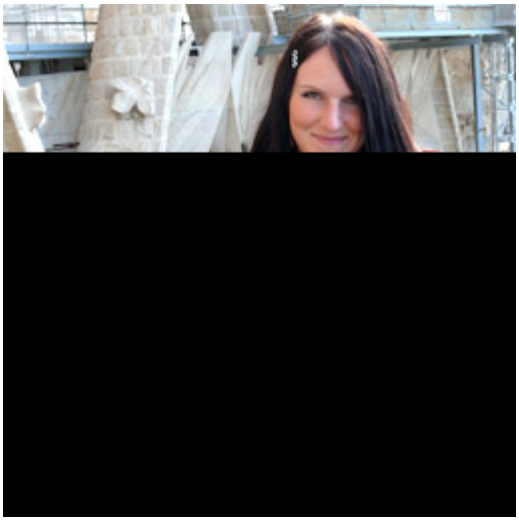


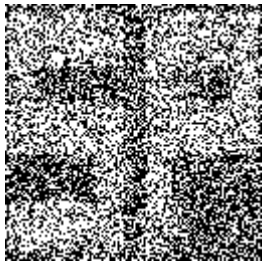
Obrázek s vodoznakem a s ořezem 60%



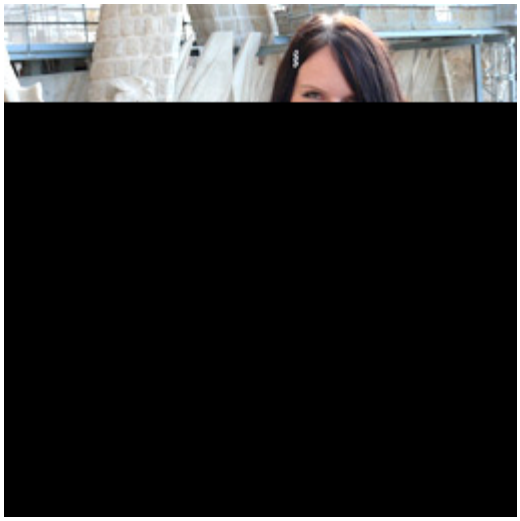


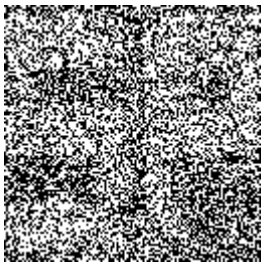
Obrázek s vodoznakem a s ořezem 70%





Obrázek s vodoznakem a s ořezem 80%

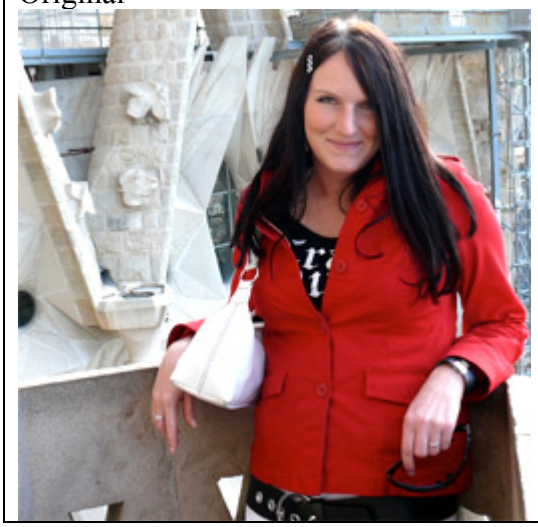




12.4.3 Odolnosti proti šumu

Obrázek s vodoznakem + šum 5%

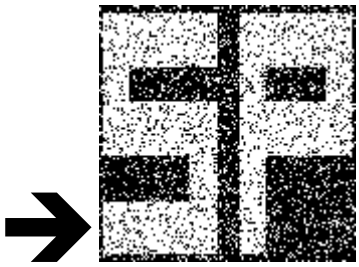
Originál



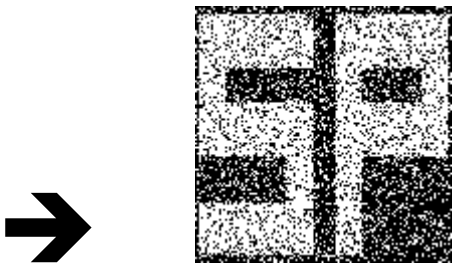
Obrázek s vodoznakem + šum 10%

Obrázek s vodoznakem + šum 20%

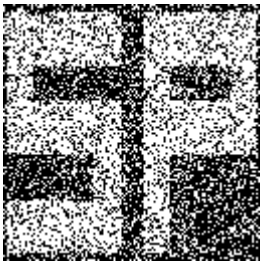
Obrázek s vodoznakem + šum 30%



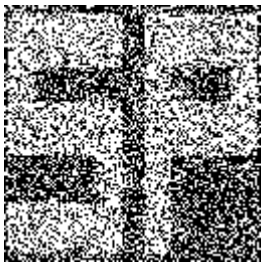
Obrázek s vodoznakem + šum 40%



Obrázek s vodoznakem + šum 50%



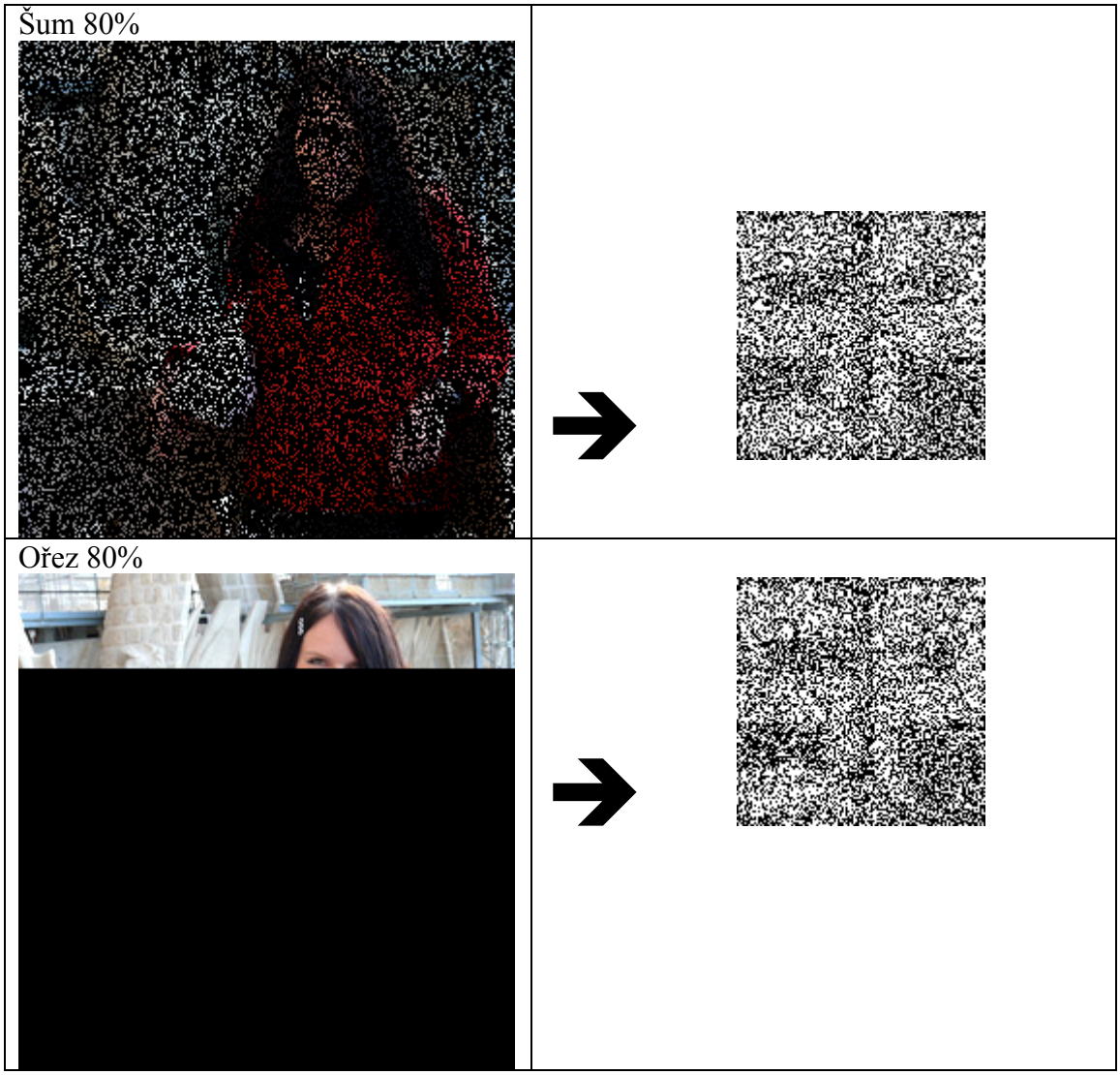
Obrázek s vodoznakem + šum 60 %



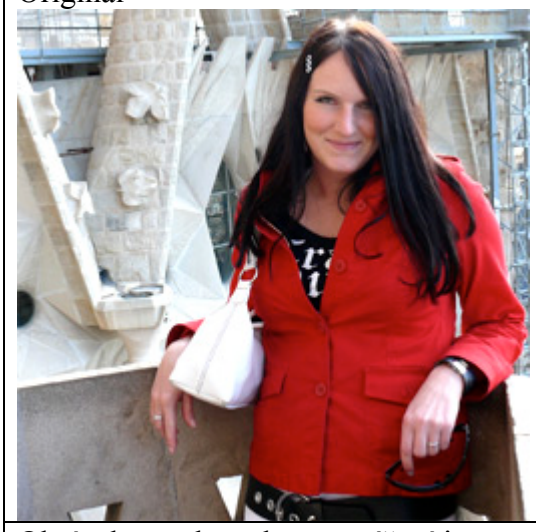
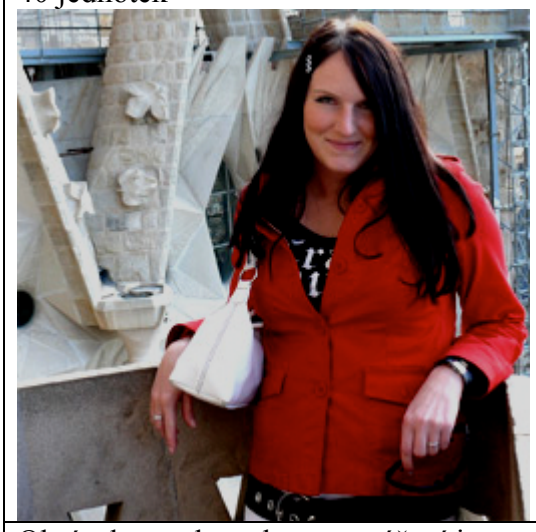
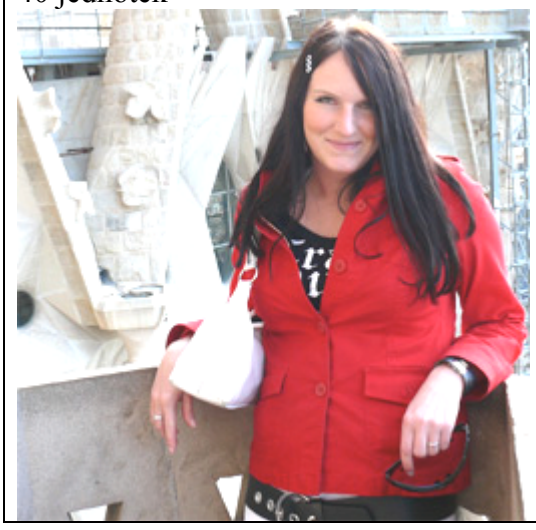
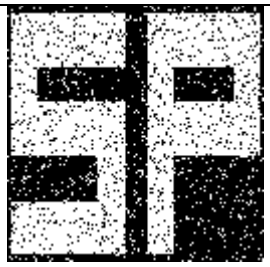
Obrázek s vodoznakem + šum 70 %

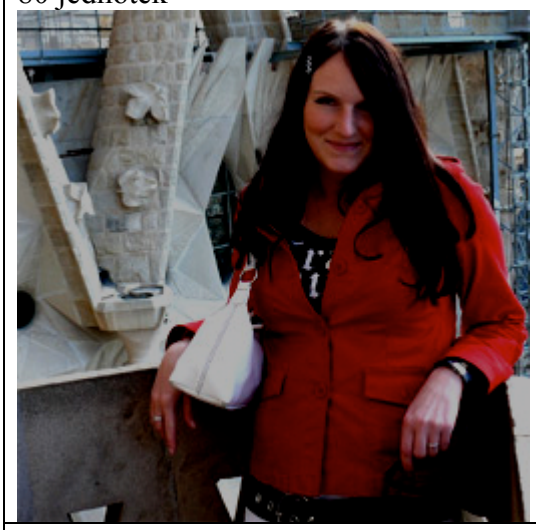
Obrázek s vodoznakem + šum 80 %

12.4.4 Porovnání extrémního útoku s využitím šumu a ořezu



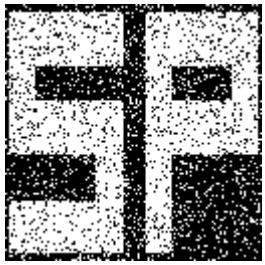
12.4.5 Odolnosti proti zvyšování/snižování jasu

Originál 	
Obrázek s vodoznakem - snížení jasu o 40 jednotek 	 
Obrázek s vodoznakem – zvýšení jasu o 40 jednotek 	 

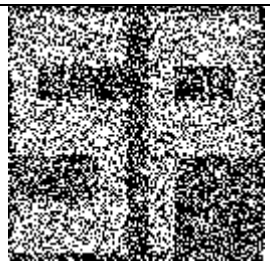
Originál 	
Obrázek s vodoznakem - snížení jasu o 80 jednotek 	
Obrázek s vodoznakem - zvýšení jasu o 80 jednotek 	

Originál

Obrázek s vodoznakem - snížení jasu o 120 jednotek

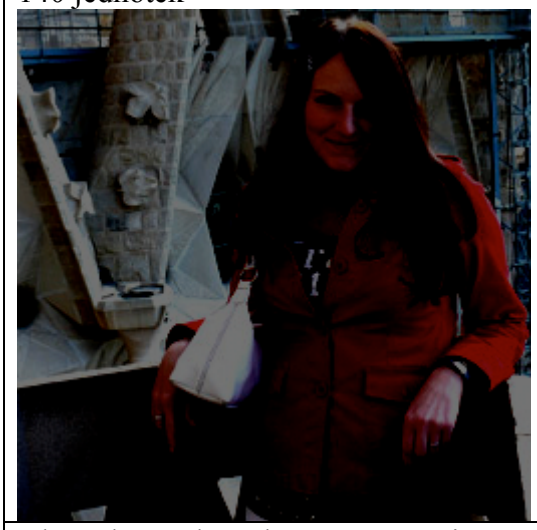


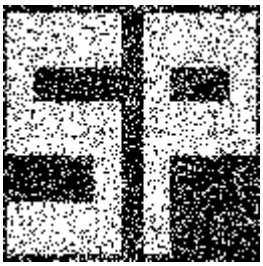
Obrázek s vodoznakem - zvýšení jasu o 120 jednotek



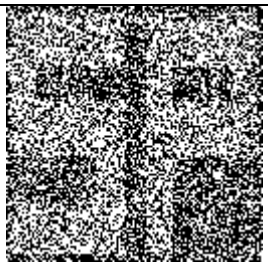
Originál

Obrázek s vodoznakem - snížení jasu o 140 jednotek



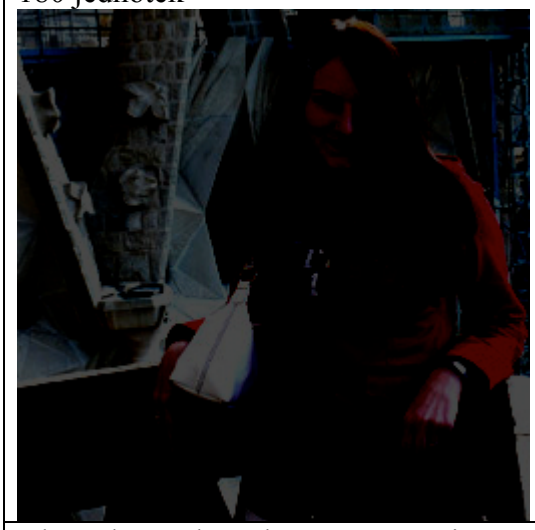


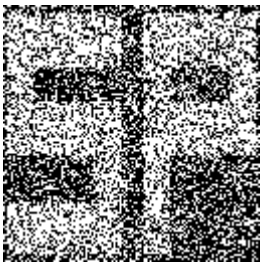
Obrázek s vodoznakem - zvýšení jasu o 140 jednotek



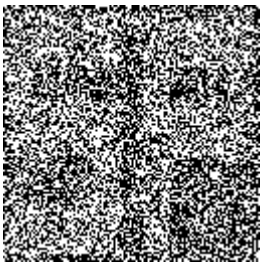
Originál

Obrázek s vodoznakem - snížení jasu o 180 jednotek



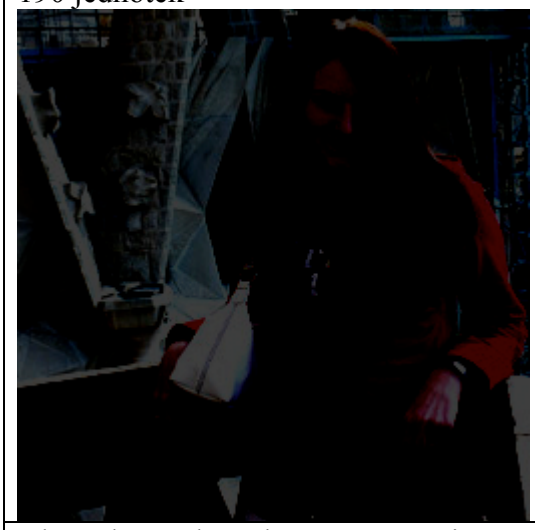


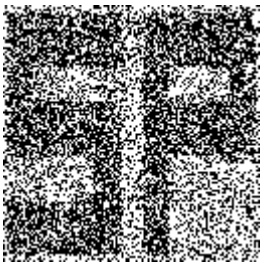
Obrázek s vodoznakem - zvýšení jasu o 180 jednotek



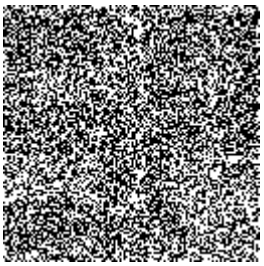
Originál

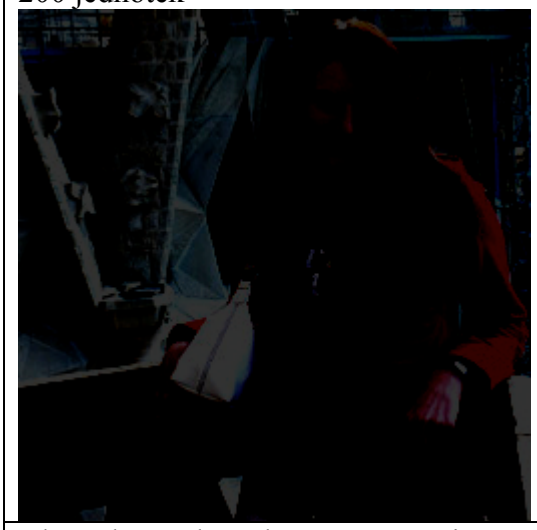
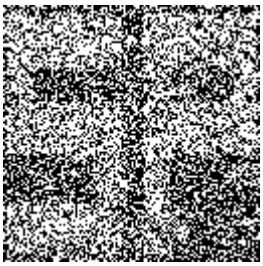
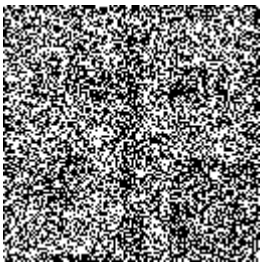
Obrázek s vodoznakem - snížení jasu o 190 jednotek

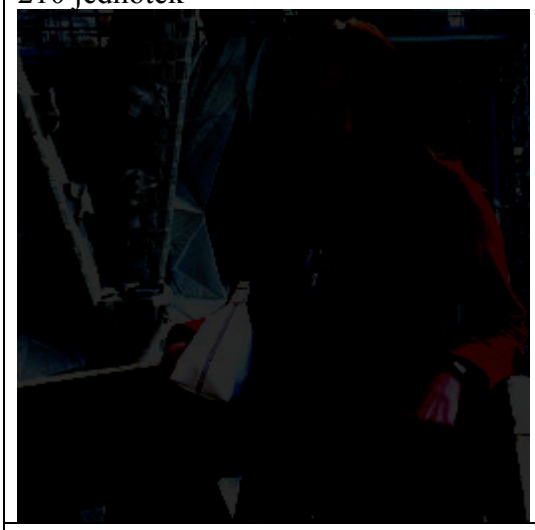
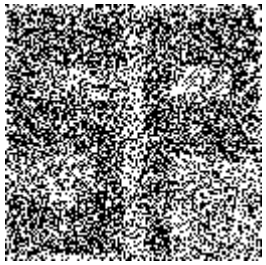
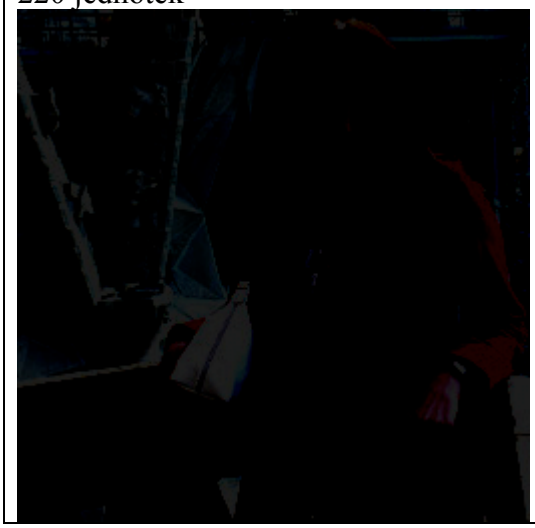
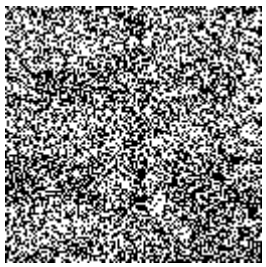




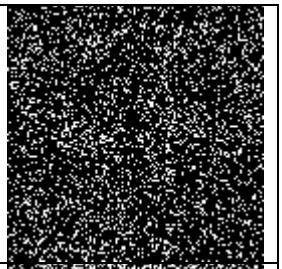
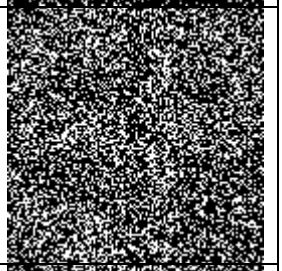
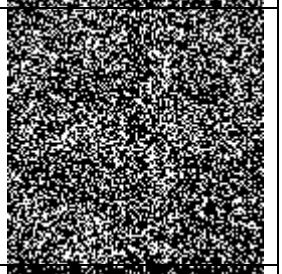
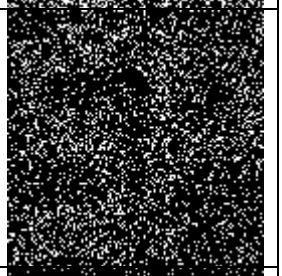
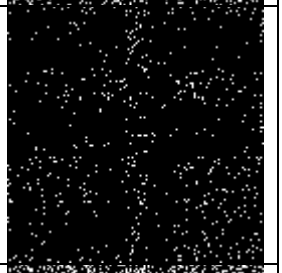
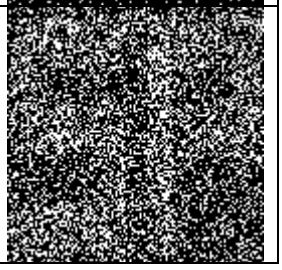
Obrázek s vodoznakem - zvýšení jasu o 190 jednotek

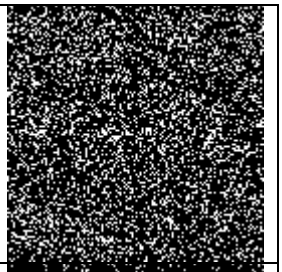
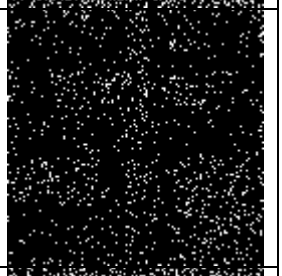
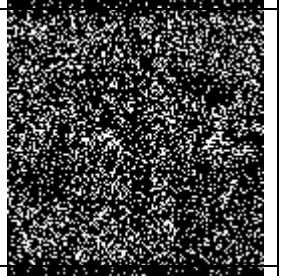
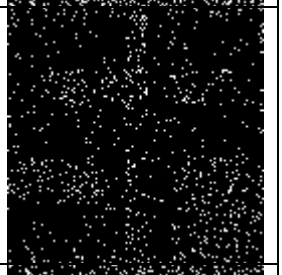
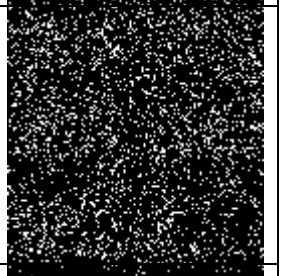
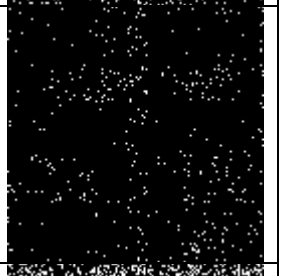
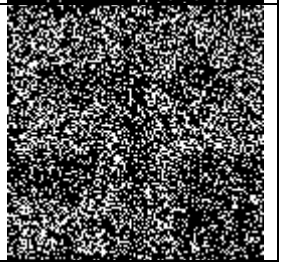


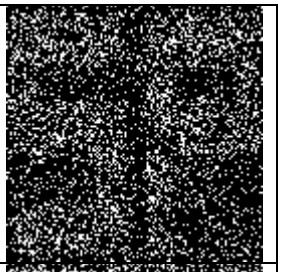
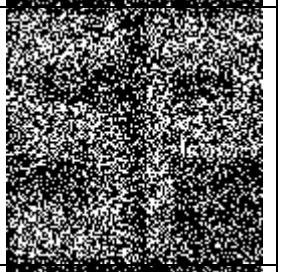
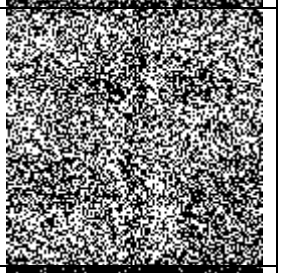
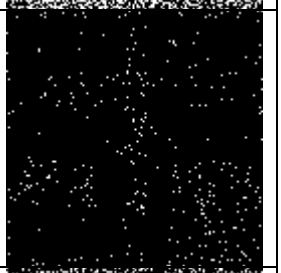
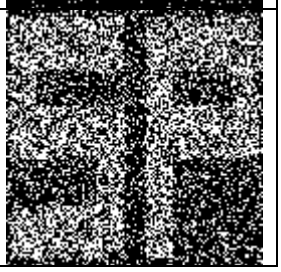
Originál 	
Obrázek s vodoznakem - snížení jasu o 200 jednotek 	 
Obrázek s vodoznakem - zvýšení jasu o 200 jednotek 	 

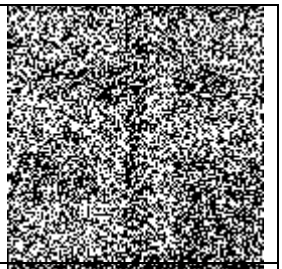
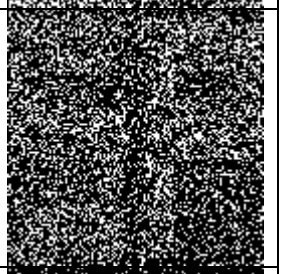
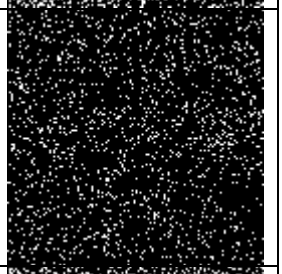
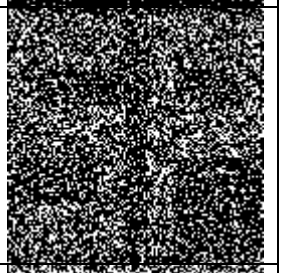
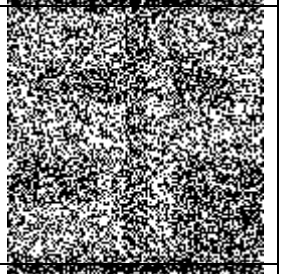
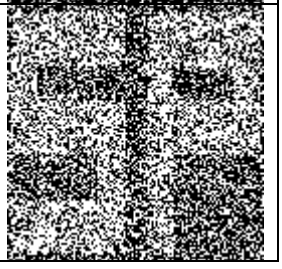
Originál 	
Obrázek s vodoznakem - snížení jasu o 210 jednotek 	 
Obrázek s vodoznakem - snížení jasu o 220 jednotek 	 

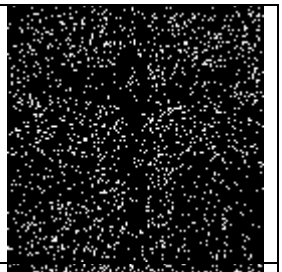
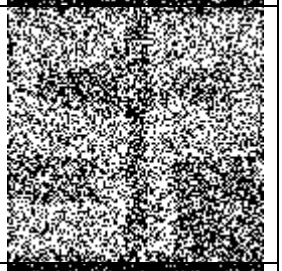
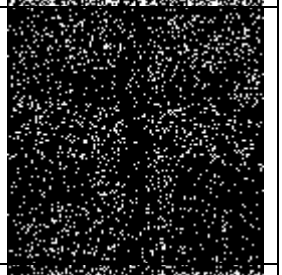
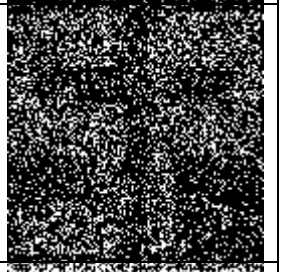
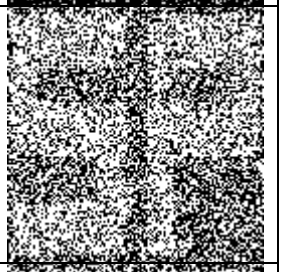
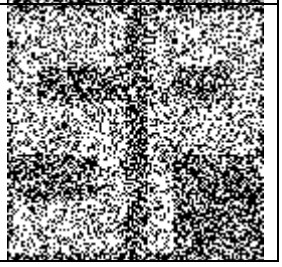
12.4.6 Odolnost proti opětovnému ukládáním obrazu do formátu JPEG

4 bitová rovina – 80 %	Extrakce z 4. roviny	
	Extrakce z 5. roviny	
	Extrakce z 3. roviny	
4. bitová roviny – 85 %	Extrakce z 4. roviny	
	Extrakce z 5. roviny	
	Extrakce z 3. roviny	

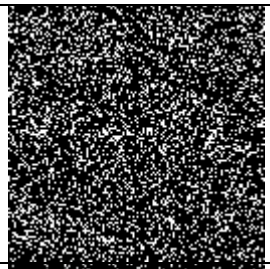
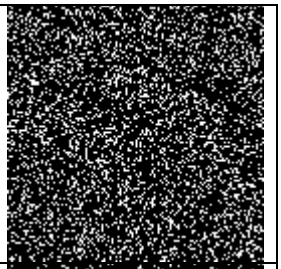
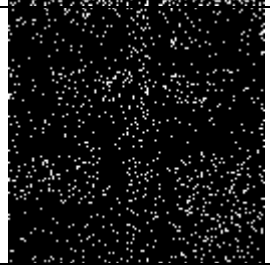
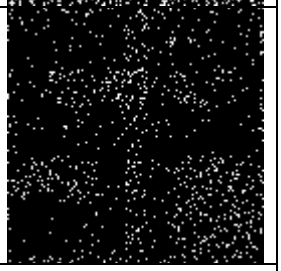
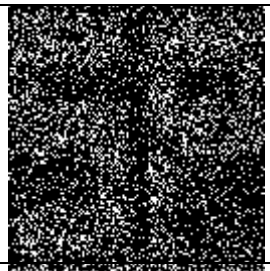
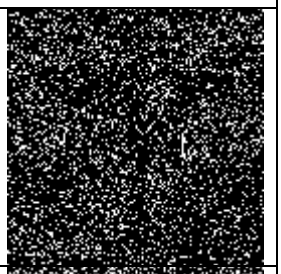
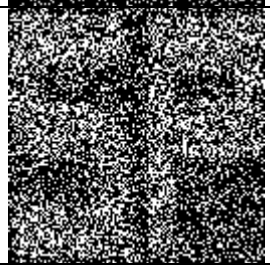
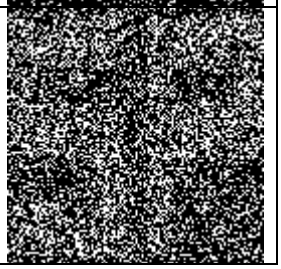
5. bitová rovina – 55 %	Extrakce z 5. roviny	
	Extrakce z 6. roviny	
5. bitová roviny – 60 %	Extrakce z 5. roviny	
	Extrakce z 6. roviny	
5. bitová roviny – 70 %	Extrakce z 5. roviny	
	Extrakce z 6. roviny	
	Extrakce z 4. roviny	

6. bitová rovina – 51 %	Extrakce z 6. roviny	
	Extrakce z 5. roviny	
6. bitová roviny – 55 %	Extrakce z 6. roviny	
	Extrakce z 5. roviny	
	Extrakce z 4. roviny	
	Extrakce z 7. roviny	
6. bitová roviny – 70 %	Extrakce z 6. roviny	

7. bitová rovina – 35 %	Extrakce z 5. roviny	
	Extrakce z 6. roviny	
7. bitová roviny – 40 %	Extrakce z 7. roviny	
	Extrakce z 6. roviny	
	Extrakce z 5. roviny	
7. bitová roviny – 50 %	Extrakce z 6. roviny	
	Extrakce z 5. roviny	

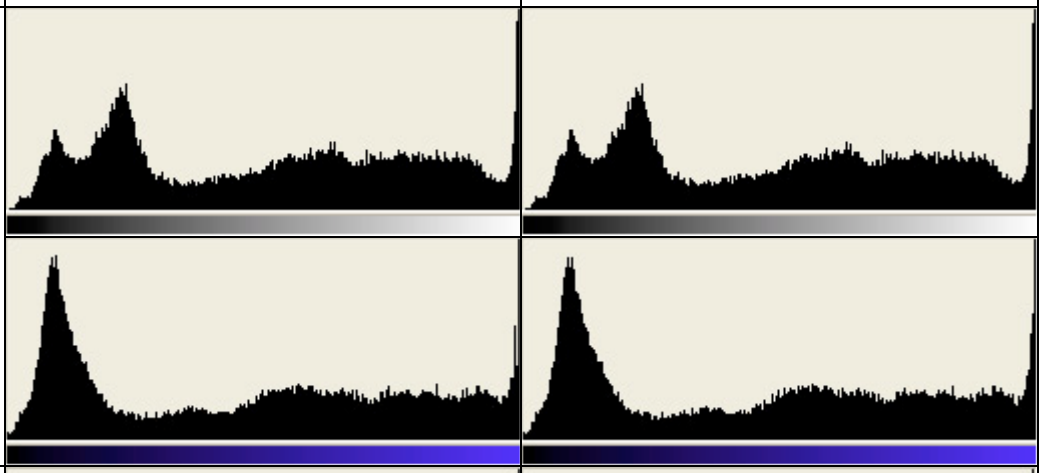
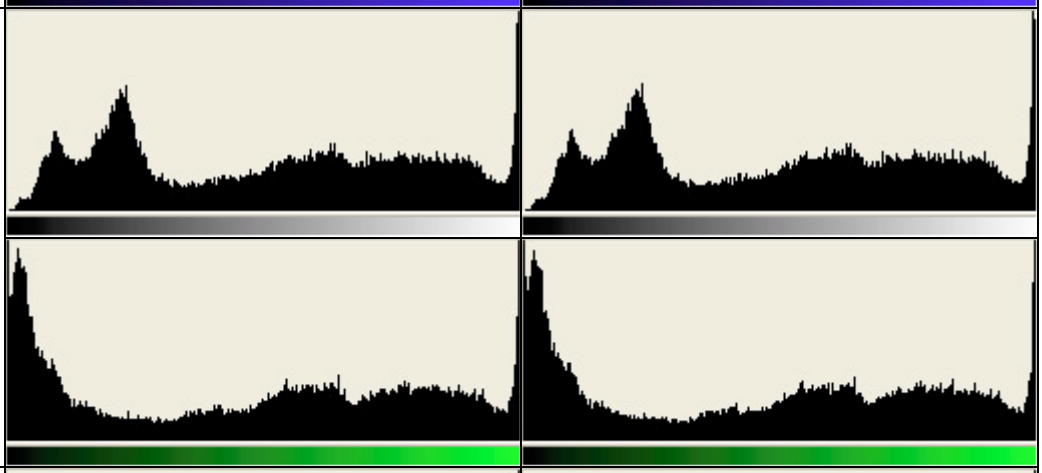
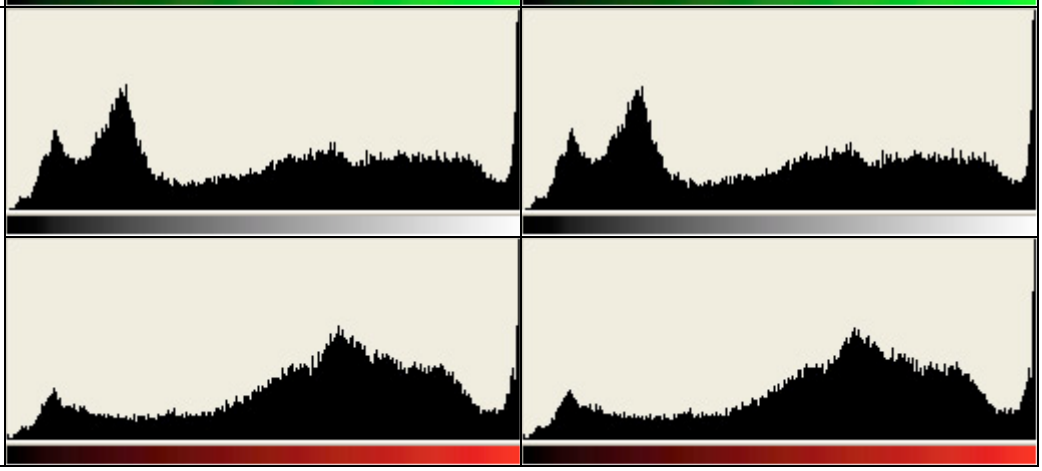
8. bitová rovina – 20 %	Extrakce z 8. roviny	
	Extrakce z 7. roviny	
	Extrakce z 6. roviny	
8. bitová roviny – 25 %	Extrakce z 8. roviny	
	Extrakce z 7. roviny	
	Extrakce z 6. roviny	
8. bitová roviny – 25 %	Extrakce z 6. roviny	

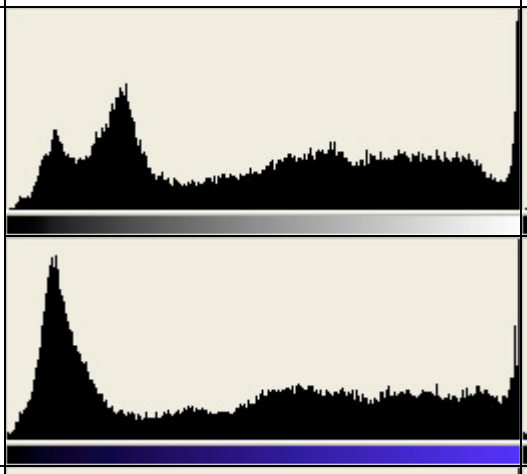
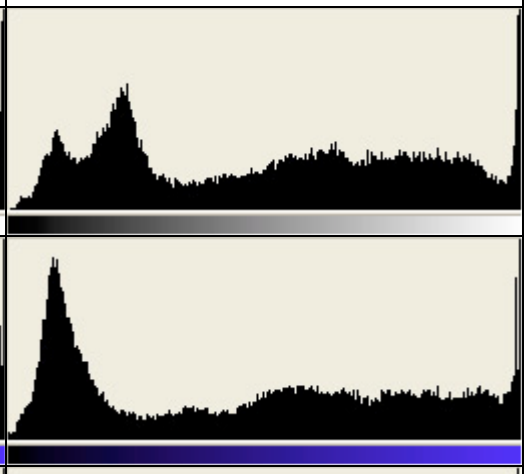
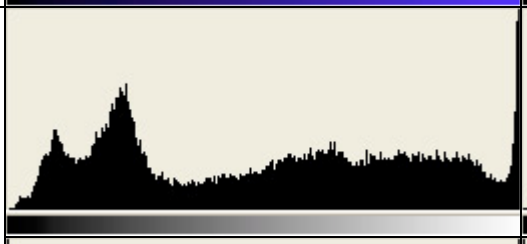
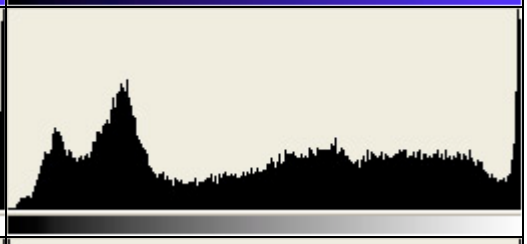
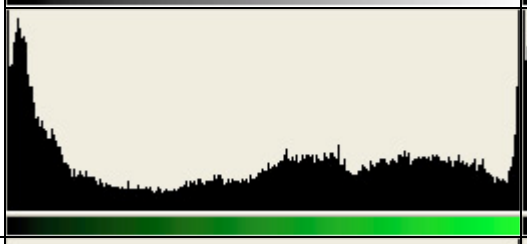
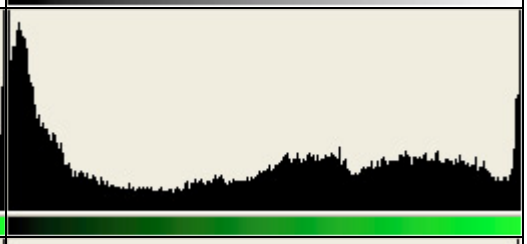
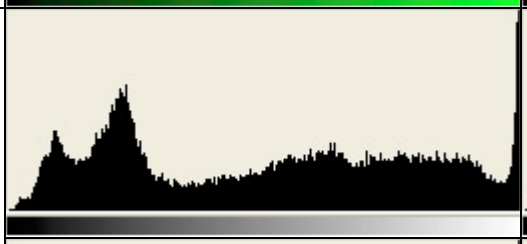
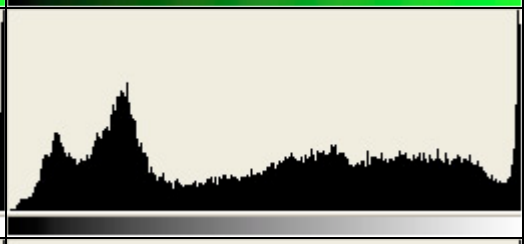
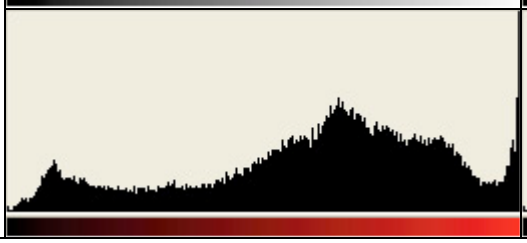
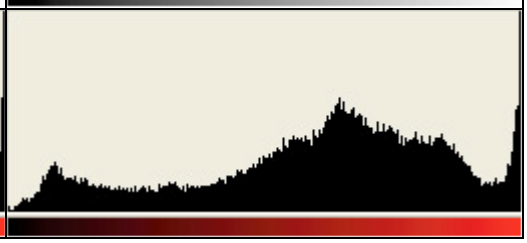
12.4.7 Pokus o zvýšení odolnosti vkládáním vodoznaku do dvou bitových rovin stejné barvy

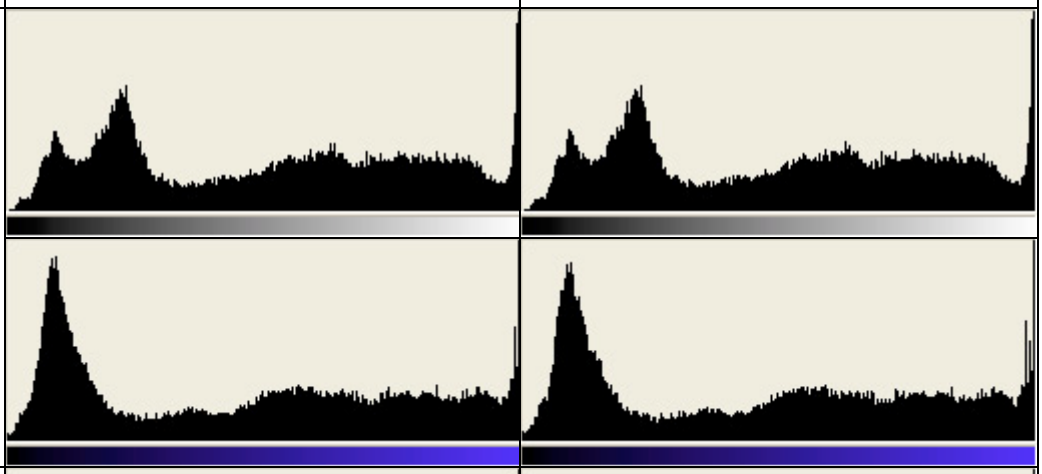
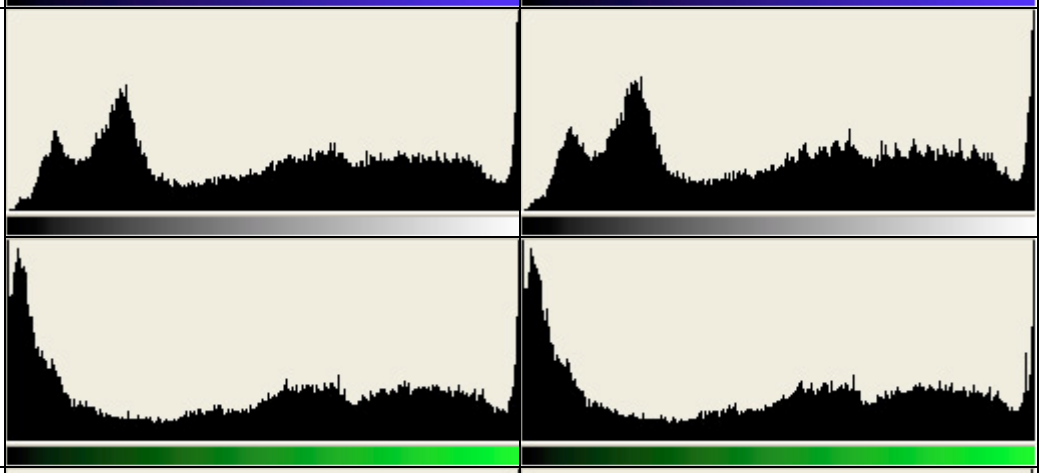
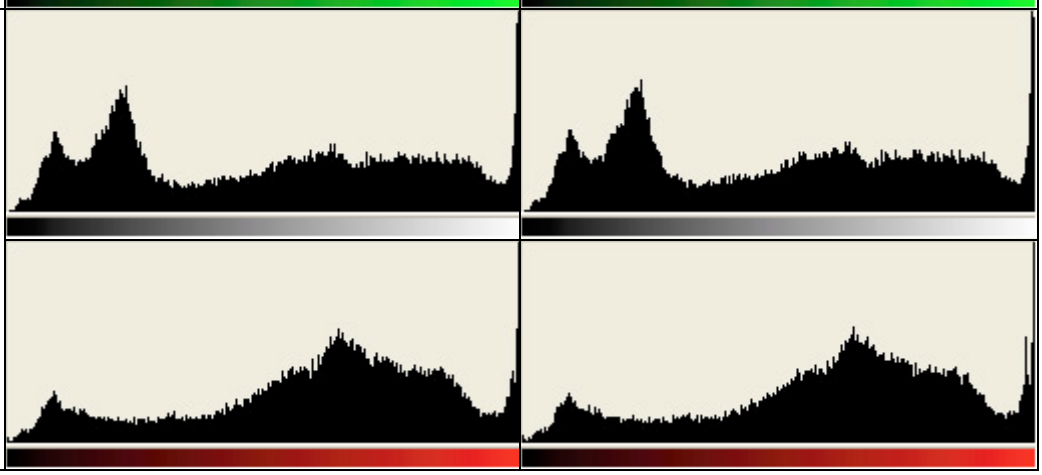
Srovnání vložení do 5. bitová roviny a vložení do 5. a 4. roviny zároveň – 55 %	Extrakce z 5. roviny		
	Extrakce z 6. roviny		
Srovnání vložení do 6. bitová roviny a vložení do 6. a 5. roviny zároveň – 51 %	Extrakce z 6. roviny		
	Extrakce z 5. roviny		

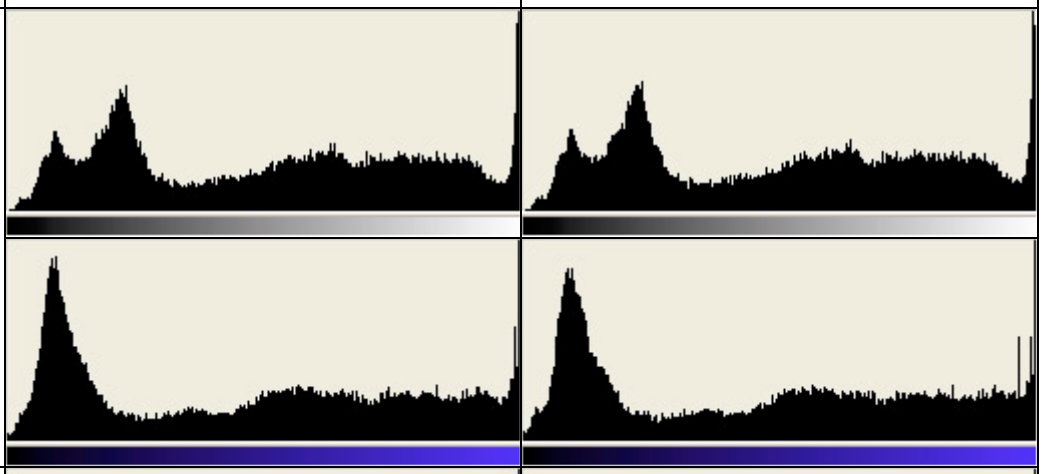
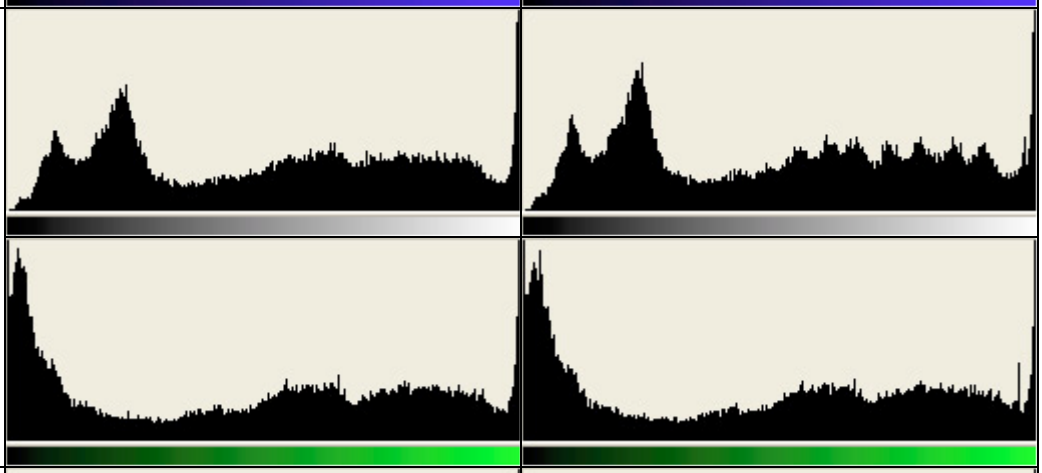
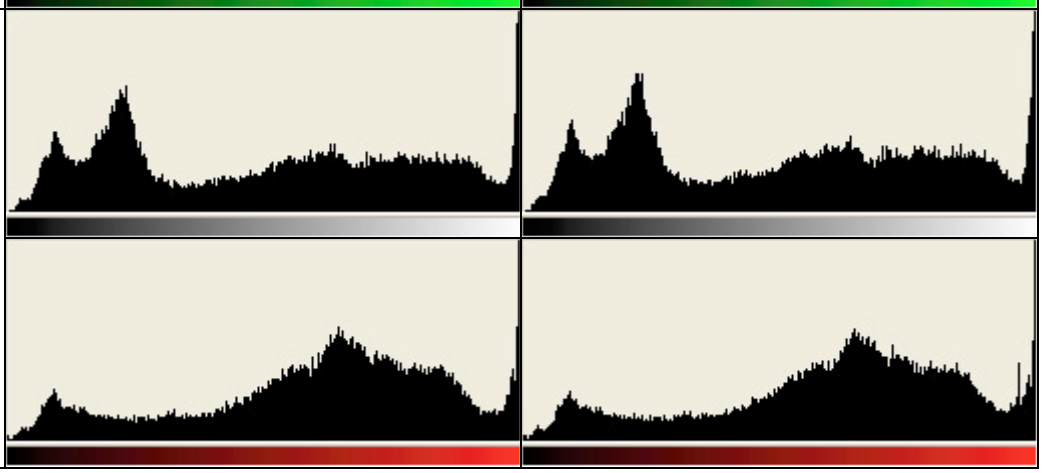
12.5 Testování statistické nedetekovatelnosti

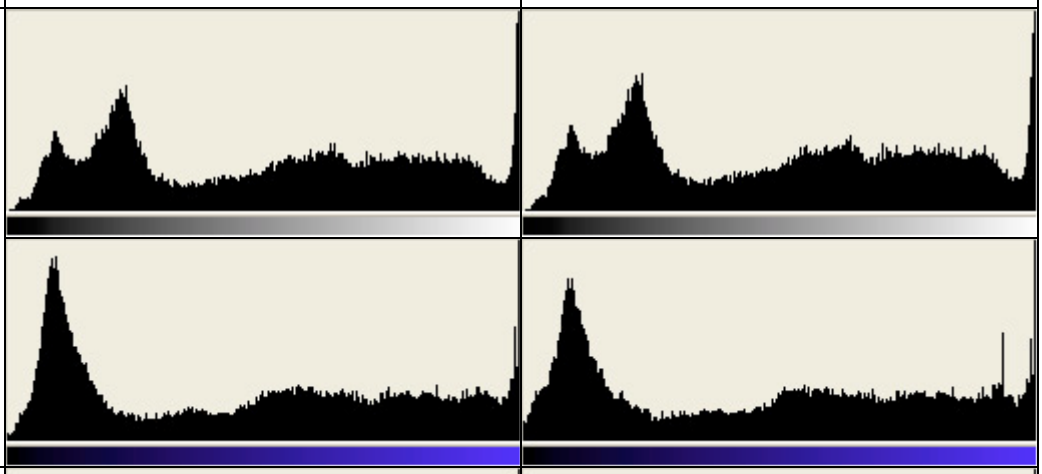
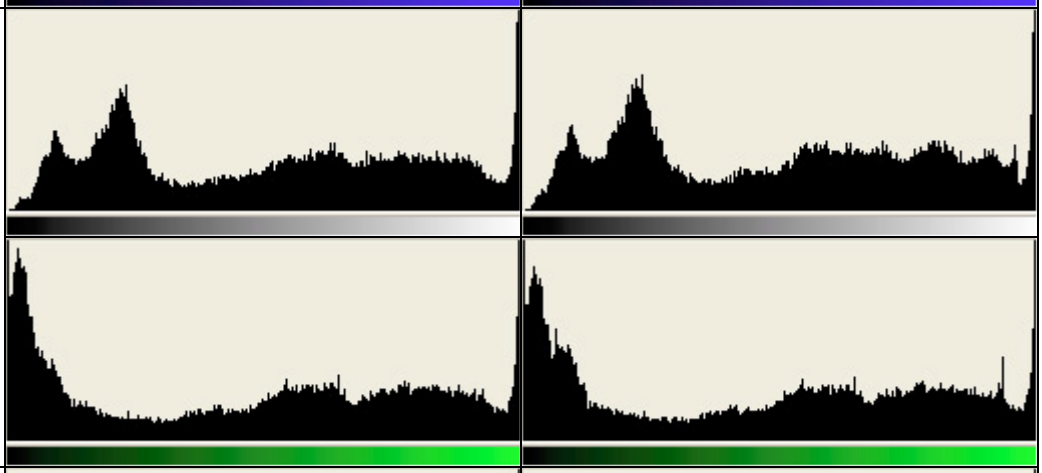
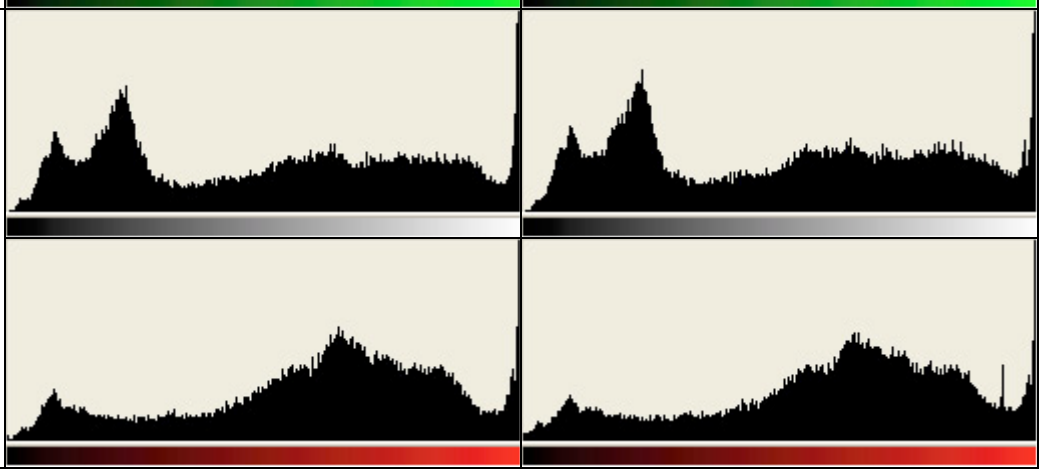
12.5.1 Vkládání do jedné bitové roviny

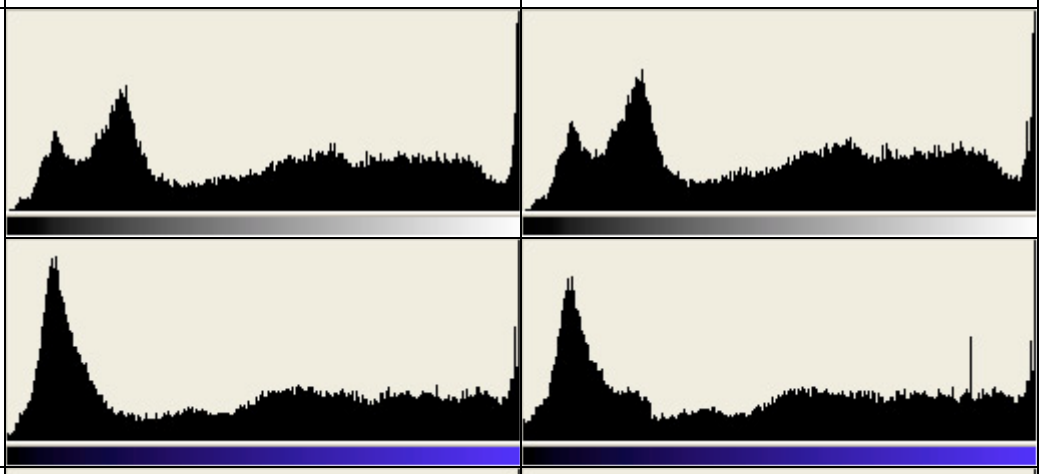
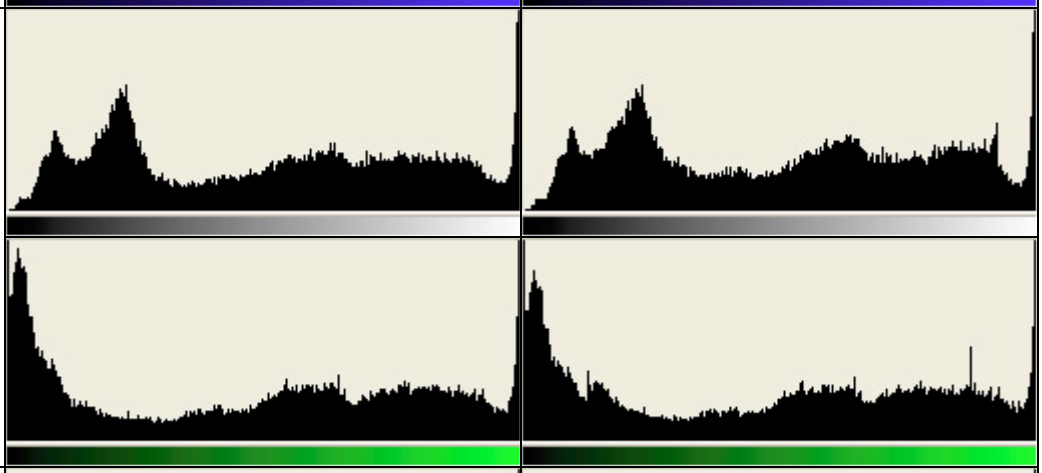
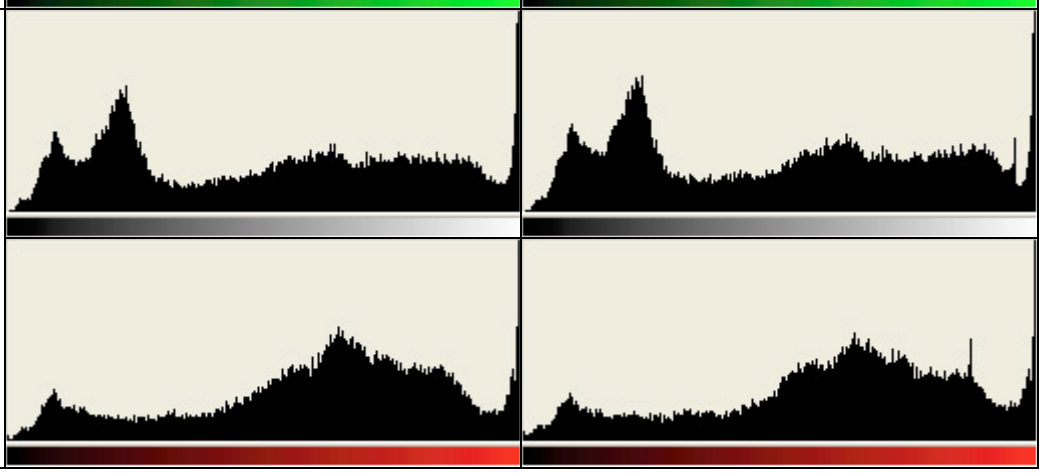
Rovina / Barva	Histogram originálního obrazu	Histogram obrazu s vodoznakem
1B		
1G		
1R		

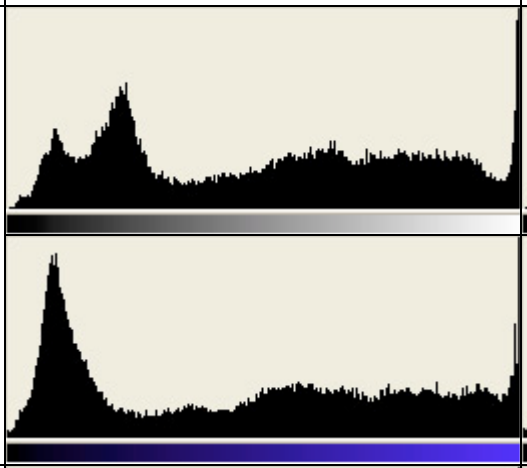
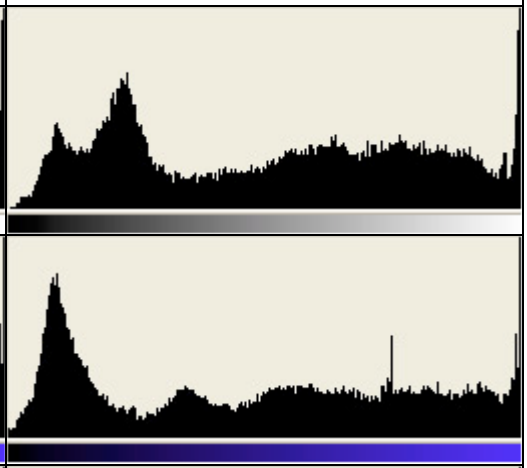
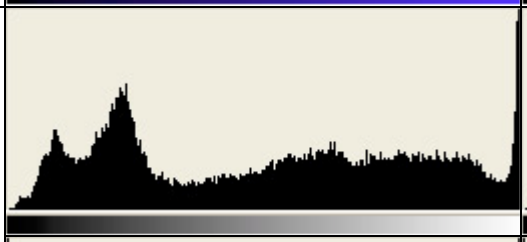
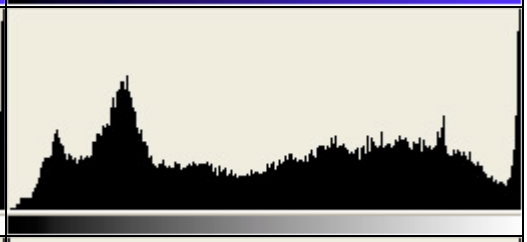
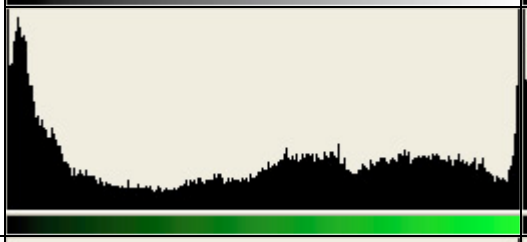
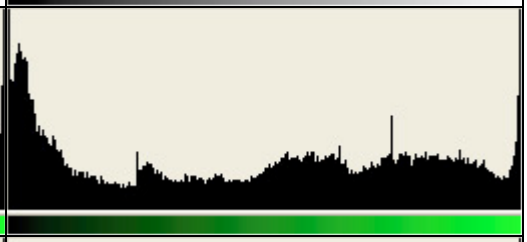
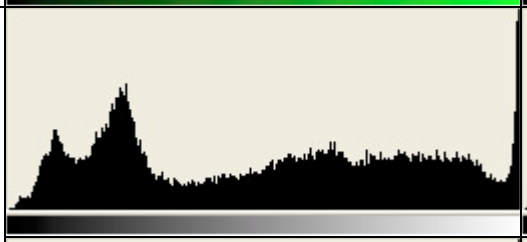
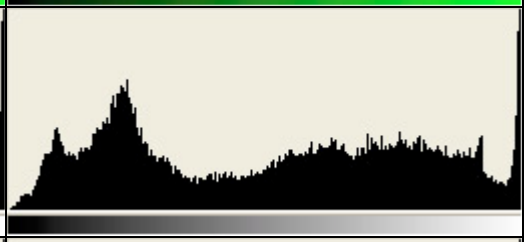
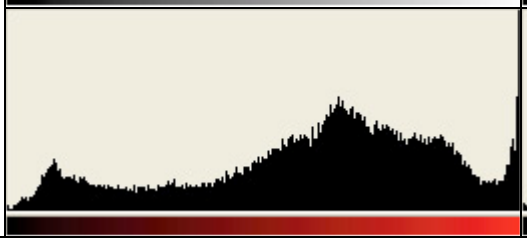
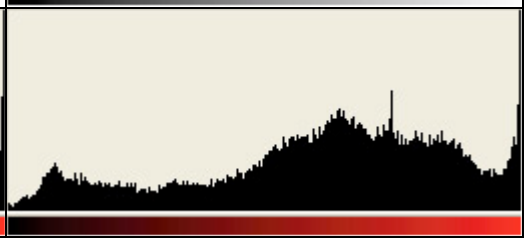
Rovina / Barva	Histogram originálního obrazu	Histogram obrazu s vodoznakem
2B		
2G		
		
2R		
		

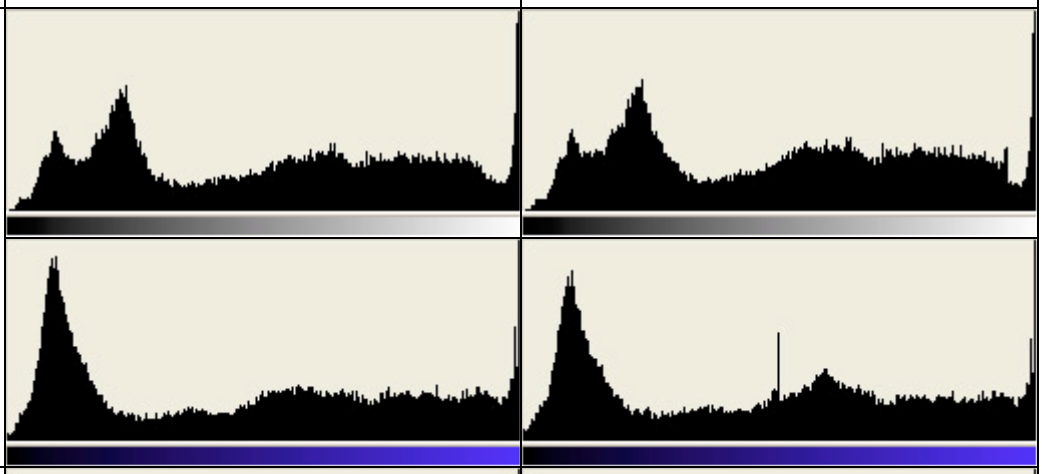
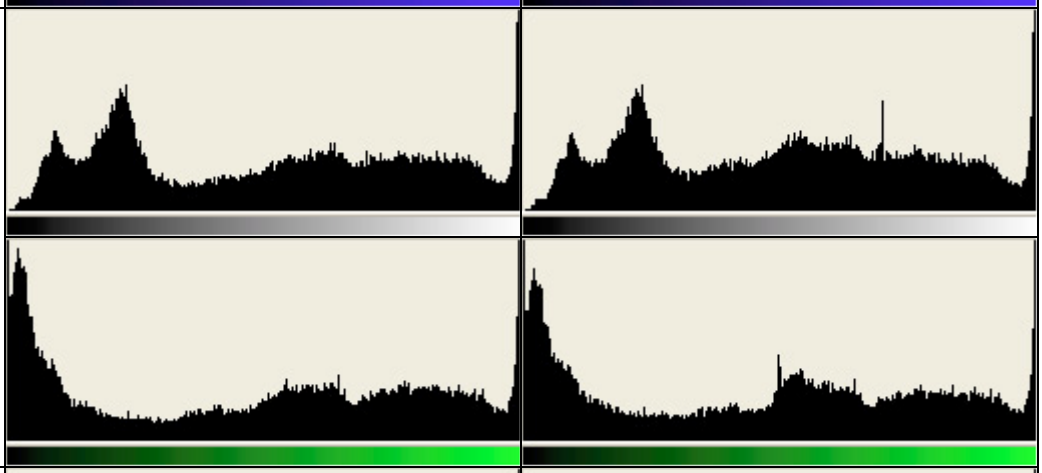
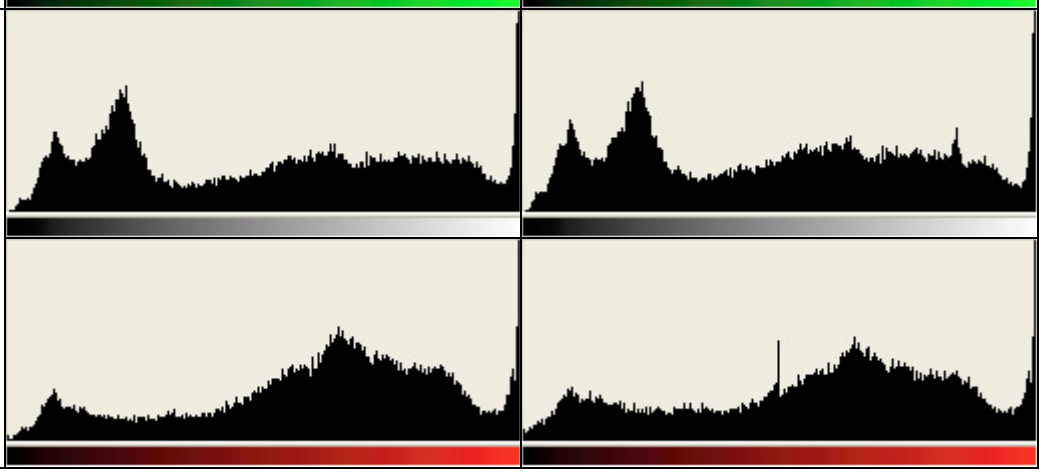
Rovina / Barva	Histogram originálního obrazu	Histogram obrazu s vodoznakem
3B		
3G		
3R		

Rovina / Barva	Histogram originálního obrazu	Histogram obrazu s vodoznakem
4B		
4G		
4R		

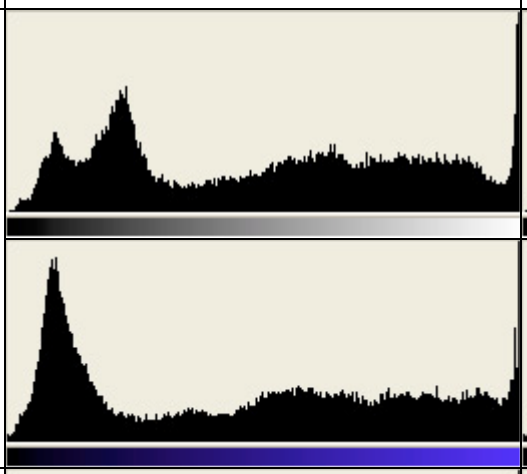
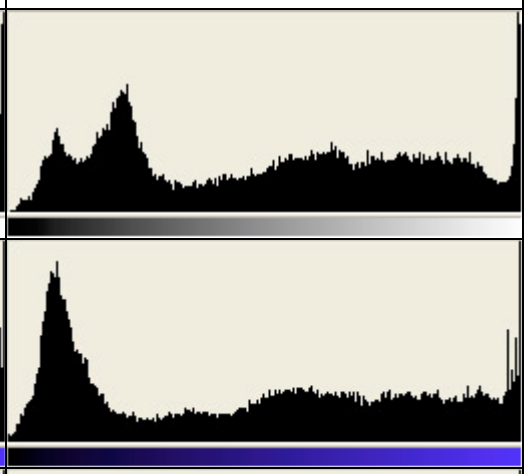
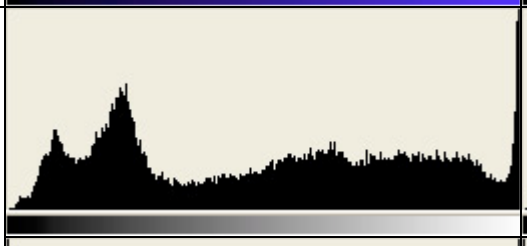
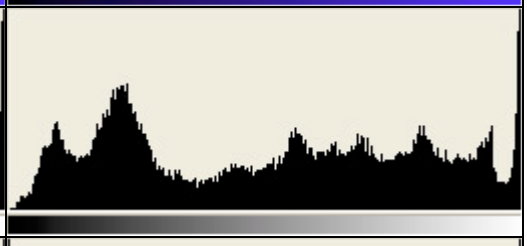
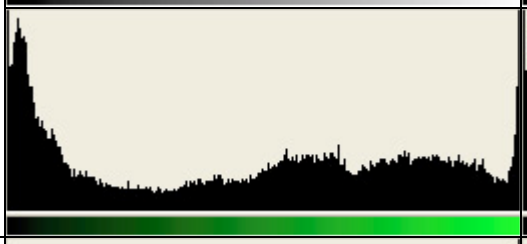
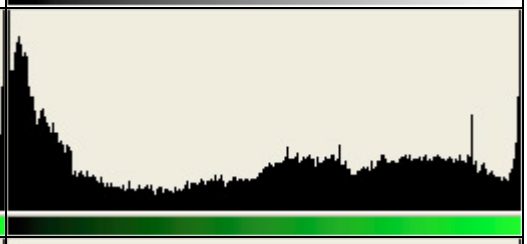
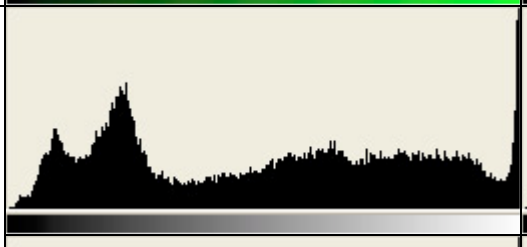
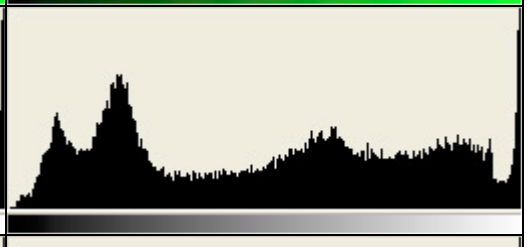
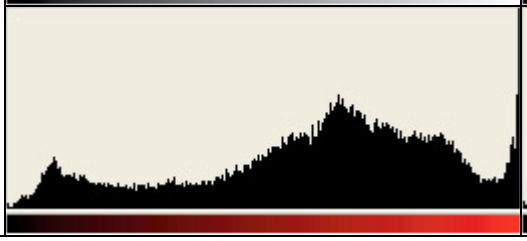
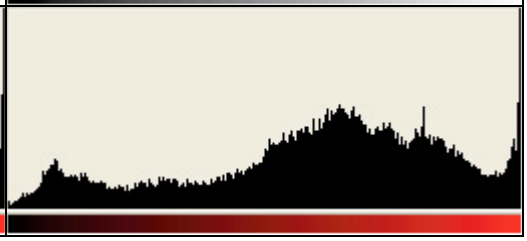
Rovina / Barva	Histogram originálního obrazu	Histogram obrazu s vodoznakem
5B		
5G		
5R		

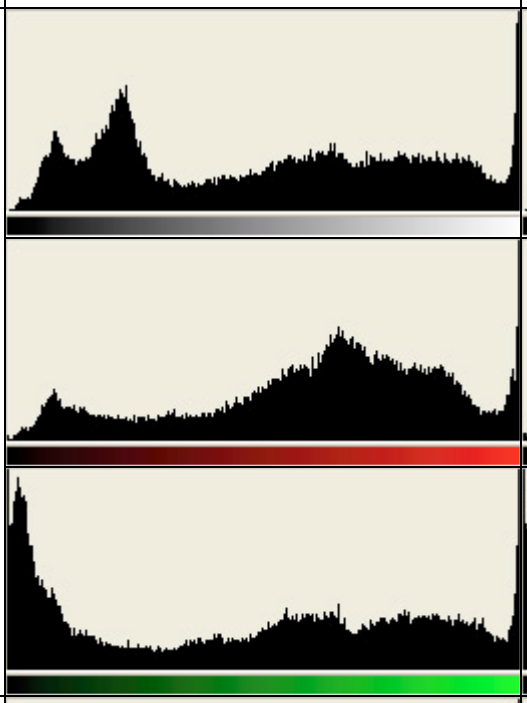
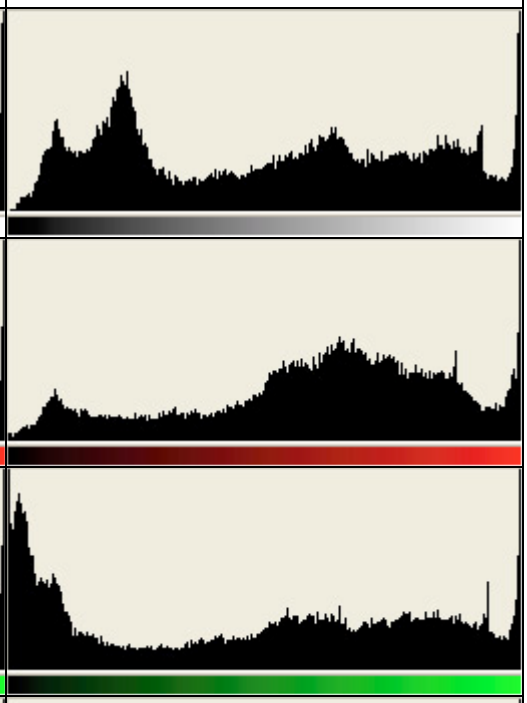
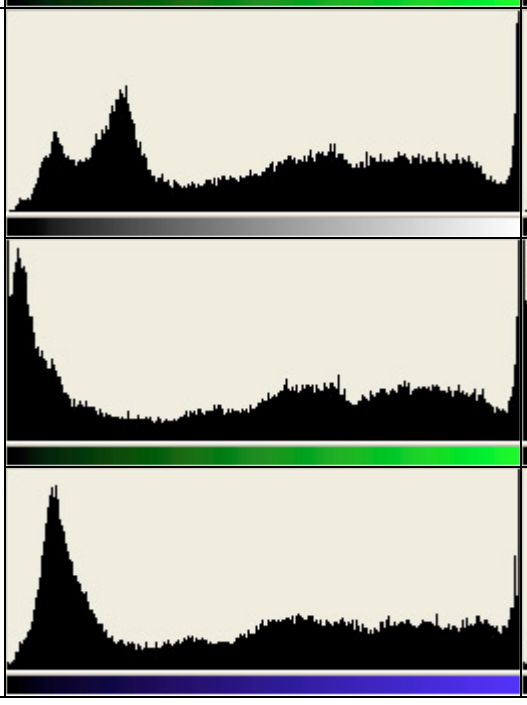
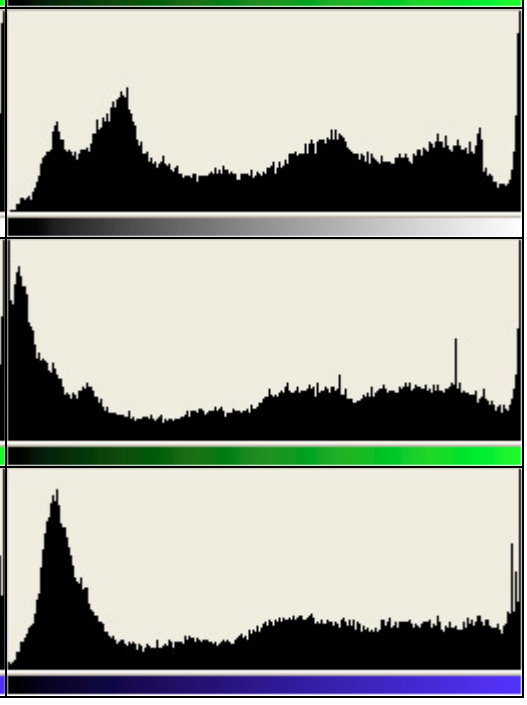
Rovina / Barva	Histogram originálního obrazu	Histogram obrazu s vodoznakem
6B		
6G		
6R		

Rovina / Barva	Histogram originálního obrazu	Histogram obrazu s vodoznakem
7B		
7G		
		
7R		
		

Rovina / Barva	Histogram originálního obrazu	Histogram obrazu s vodoznakem
8B		
8G		
8R		

12.5.2 Vkládání do dvou bitových rovin zároveň

Rovina / Barva	Histogram originálního obrazu	Histogram obrazu s vodoznakem
2B3B		
4G5G		
		
5R6R		
		

Rovina / Barva	Histogram originálního obrazu	Histogram obrazu s vodoznakem
5G6R		
		

12.6 DVD

Přiložené DVD obsahuje:

- Elektronickou podobu disertační práce
- Testování v rámci výzkumné části práce
  - Ukázky vkládání do 8 bitových rovin s nepermutovaným a permutovaným vodoznakem
  - Testování vkládání do dvou bitových rovin zároveň
  - Testování robustnosti
  - Testování statistické nedetekovatelnost
- Ukázku praktických příkladů po aplikaci metodiky EZOD
- Ukázky dílčích výsledků testování při srovnávání metodiky s obdobnými postupy
- Ukázku zdrojového kódu testovací aplikace
- Další materiály vzniklé při testování a zpracování práce, které buď nevedly k pozitivním výsledkům, nebo jsou to dílčí výsledky explicitně neuváděné