Steganografická komunikace

Steganographic communication

Štefan Zigulec

Diplomová práce
2006

Univerzita Tomáše Bati ve Zlíně
Fakulta technologická

Děkuji vedoucímu mé diplomové práce Ing. Lubomíru Mackovi, Ph.D. za veškerou pomoc a cenné rady, které mi pomohly při jejím vypracování. Děkuji také Ing. Marku Čandíkovi, Ph.D. za podnětné připomínky a dále všem, kteří přispěli jakýmkoliv dobrým nápadem.

Prohlašuji, že jsem na celé diplomové práci pracoval samostatně a použitou literaturu jsem citoval.

Ve Zlíně, 20. 5. 2006 ….....

Štefan Zigulec

Abstrakt

Tato práce se zabývá obecným úvodem do problematiky steganografie se zaměřením na realizaci steganografických přístupů na binární digitální obrazy. Obsahuje základní pojmy z oblasti datové bezpečnosti a ochrany dat. Dále jsou popsány základní klasifikace steganografických přístupů, hlavně pak ve třetí a čtvré kapitole různých možností digitálního zpracování obrazu. V poslední části je uvedena základní praktická aplikace z prostředí MATLAB.

This Master Thesis deals with the general introduction into the steganography problematics with the focus on the practical realization of the binary digital images steganographic techniques. It contains the basic data security concepts. Furthermore the basic steganographic techniques classification is discussed, especially the various possibilities of digital image processing. In the last chapter there is the basic practical application in the MATLAB environment provided.

OBSAH

ÚVOD

Obrovský rozvoj ICT (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 top management, ale také pro pracovníky nižších útvarů podniku a všechny ostatní, kteří o ně projeví zájem. Po celém světě v různých zájmových sférách se 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. Internet je tedy dalším z řady médií, které firmy využívají pro svou prezentaci.

Relativně snadné získávání informací prostřednictvím prezentací (on-line či off-line) s sebou přináší i stinné stránky. Čím dál častěji se v souvislosti s distribucí veřejně přístupných informací (zejména na internetu) hovoří o problematice bezpečnosti. Týká se to především nelegálního šíření a zacházení s informacemi, které jsou vlastnictvím někoho jiného.

Zde vzniká otázka, jak je vůbec možné zabezpečit informace, které jsou záměrně poskytovány široké veřejnosti. Tuto otázku mohou částečně řešit metody utajené komunikace (tj. steganografie) a metody zabezpečení digitálních dat technikami digitálního vodotisku. Diplomová práce se zabývá právě steganografickými technikami.

I. TEORETICKÁ ČÁST

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.

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, které ulehčují 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 prezentací je tato problematika ztížena zejména díky základní funkci prezentací tj. prezentovat 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 nových pohledů a trendů v oblasti zabezpečení digitálních dat. Je potřeba 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 tato data používat.
- **Útočník** – osoba, která nevlastní data, resp. nemá od autora dočasné či trvalé právo tato data používat a snaží se data získat, upravit, nebo prezentovat tak,

aby buď nesloužila svému účelu, nebo aby byla interpretována jako data s dočasným nebo trvalým právem je používat.

Důležitým faktorem je autorizace, která stanovuje, zda je subjekt důvěryhodný pro určité činnosti.

Autorizace představuje vyhodnocování, zda je subjekt důvěryhodný k vykonávání určitých činností. Důvěryhodný informační systém, důvěryhodný objekt nebo subjekt představuje takovou entitu, která je implementována tak (je o tom pádný důkaz), že svou funkcí a specifikací splňuje kritéria tzv. bezpečnostní politiky.

Důvěryhodná entita se chová tak, jak očekáváme, že se bude chovat. Avšak v případě veřejně přístupných elektronických prezentací ve většině případů nelze bohužel autorizaci využít a rozpoznání útočníka je též značný problém.

1.1 Bezpečnost informací

Informace jsou aktiva, která mají pro organizaci hodnotu a potřebují být vhodným způsobem chráněna. Bezpečnost informací je zaměřena na širokou škálu hrozeb a zajišťuje jí kontinuitu podnikatelských činností, minimalizuje obchodní ztráty, maximalizuje návratnost investic a podnikatelských příležitostí.

Informace mohou existovat v různých podobách. Mohou být vytištěny nebo napsány ručně na papíře, ukládány v el. podobě, posílány poštou nebo elektronickou cestou, zachyceny na film nebo vyřčeny při konverzaci. Ať vezmeme jakoukoli formu informací, bez ohledu na způsob jejich sdělení či uložení, vždy by měla být odpovídajícím způsobem chráněna.

Bezpečnost je tedy charakterizována jako zachování:

- důvěrnosti – zajištění toho, že informace je dostupná pouze osobám s autorizovaným přístupem,
- integrity – zabezpečení správnosti a kompletnosti informací a metod zpracování,
- dostupnosti – zajištění toho, že informace a s nimi spjatá aktiva jsou dostupné autorizovaným uživatelům podle jejich potřeby.

Bezpečnost informací lze dosáhnout implementací soustavy opatření, která mohou existovat v podobě pravidel, natrénovaných postupů, procedur organizační struktury a programovaných funkcí. Tato opatření musí být zavedena proto, aby bylo dosaženo specifických cílů organizace.

Informace a podpůrné procesy, systémy a sítě jsou důležitými aktivy organizace. Zajištění jejich dostupnosti, integrity a důvěrnosti může být zásadní pro udržení konkurenceschopnosti, toku hotovosti (cash flow), ziskovosti, dodržování zákonných ustanovení a dobrého jména organizace.

Stále rostoucí měrou jsou organizace a jejich informační systémy vystavovány bezpečnostním hrozbám z různých zdrojů, včetně počítačových podvodů, špionáže, sabotáže, vandalizmu, požárů, výpadkům proudu nebo i povodním. Zdroje škod, jako jsou počítačové viry, útoky hackerů a útoky na odepření služby (denial of service) jsou stále častější, roste jejich nebezpečnost a sofistikovanost.

Z uvedených vlastností je možné zobecnit bezpečnost v informačních technologiích jako vlastnost systému popisující míru ochrany důvěrných objektů (systémových částí informačních technologií). Významnou vlastností bezpečnosti je její časová závislost (bezpečnost v informačních technologiích v závislosti na čase klesá), protože některé důvěrné informace o systémových částech se stávají známými a mohou způsobit ohrožení bezpečnosti celého systému, navíc dlouhodobým používáním každého systému se stávají známými jeho chyby, příp. nedostatky.

Základními pojmy v oblasti informační bezpečnosti jsou:

- **Riziko** – představuje možnost určité ztráty nebo škody,
- **Zranitelnost** – je slabé místo bezpečnostního systému, kterého může být užito při způsobení ztráty nebo škody.
- **Ohrožení systému** – jsou okolnosti, které mohou vést k potenciálním ztrátám nebo škodám.
- **Napadení** – je činnost, která směruje ke způsobení ztráty nebo škody.
- **Kontrola** – představuje ochranná opatření, resp. činnost, která minimalizuje ohrožení systému.

Ohrožení systému v informačních technologiích může být realizováno:

- **Přerušením** – představujícím ztrátu, nedostupnost, nebo nepoužitelnost některé systémové části.
- **Sledováním** – získáním přístupu nepovolané osoby (neautorizovaného subjektu) k systémové části.
- **Modifikací** – v případech, kdy neautorizovaný subjekt má nejen přístup k některé systémové části, ale může s ní i manipulovat. Některé modifikace programových prostředků, technických prostředků nebo dat je možné odhalit, některé modifikace nemusí být odhaleny.
- **Falzifikací** - představujícím schopnost nebo možnost zavést neautorizovanému subjektu do systémových částí falešná data, nebo realizovat falešné operace (záznamy, transakce, atd.)

Bezpečnost v informačních technologiích zahrnuje tři faktory, a to:

- **Utajení** - znamená, že informační obsah dat, resp. manipulace s nimi je dostupná jen autorizovaným subjektům, které znají klíč, nebo přístupové heslo. Utajení se realizuje šifrováním.
- **Integrita** – znamená, že systémové části mohou být modifikovány jen autorizovanými subjekty. Integrita se obvykle zabezpečuje digitálními podpisy.
- **Použitelnost** - znamená, že systémové části mohou být použity jen autorizovanými subjekty.

V souvislosti s autorizovanými přístupy je významným parametrem autentizace. **Autentizace** je ověření identity uživatele, že je opravdu tím, za koho se vydává. Metody používané pro zabezpečení autentizace uživatele můžeme rozdělit podle používaných postupů do následujících skupin:

- *autentizace přístupu tím, co člověk zná* – nejčastější aplikací tohoto přístupu je autentizace heslem. Požadavky na autentizační přístup heslem jsou:
  - pravidelná změna hesla,
  - kombinace alfanumerických znaků v hesle (písmena, číslice, jiné znaky),
  - zamezení možnosti opakovaného použití hesla.
- *autentizace přístupu tím, co má* – nejčastějším použitím tohoto přístupu je např. občanský průkaz, identifikační karta, atd.

- *autentizace přístupu tím, čím je* – mezi nepoužívanější klíčové prvky tohoto přístupu patří otisk prstu, dynamika podpisu, charakter hlasu, atd. Uvedený přístup je také nazýván autentizace pomocí biometrických parametrů. Biometrická autentizace se používá všude tam, kde je zapotřebí zajistit vysokou spolehlivost, bezpečnost a jednoduchost. Hlavní výhody biometrické autentizace jsou:
  - *neoklamatelnos*t – kontrolují uživatele, ne předmět (tedy nelze udělat kopii),
  - *nulové provozní náklady* – nejsou nutné režijní náklady na vytváření identifikačních předmětů,
  - *rychlost* – biometrické parametry uživatele jsou neustále k dispozici,
  - *praktičnost* – biometrické parametry nelze ztratit ani zapomenout,
  - *jednoznačnost* – identifikace je jednoduchá a jednoznačná,
- *autentizace přístupu použitím certifikátů veřejných klíčů* – jedná se o použití šifrovacích algoritmů.

Je nutné rozlišovat:

- **autentizaci entity**, tj. verifikace osob, nebo různých technických prostředků. Autentizace entity bývá někdy označována jako ***identifikace***.
- **autentizaci zprávy**, tj. verifikace původu a integrity (celistvosti) dat.

Útok na libovolnou systémovou část informačních technologií může ohrozit bezpečnost celého systému a může mít za následek únik nebo ztrátu cenných dat, nepříjemnou změnu těchto dat (např. www stránky), nebo znefunkčnění systému. Proto je vyžadováno, aby byl na systémové prostředky informačních technologií vykonáván bezpečnostní audit, výsledkem kterého je komplexní posouzení aktuálního stavu bezpečnosti systému a který pozůstává ze

- *stanovení možných bodů (vnějších i vnitřních) narušení bezpečnosti systému,*
- *analýze odolnosti těchto bodů vůči útokům,*
- *stanovení kritických míst bezpečnosti systému.*

Je zřejmé, že pro realizaci bezpečnostního auditu musí být specifikovány a deklarovány ty systémové prostředky informačních technologií, kterých se bezpečnostní audit bezprostředně týká.

Závislost organizací na informačních systémech a jejich službách znamená, že jsou zranitelné vůči bezpečnostním hrozbám. Propojení veřejných a privátních sítí i sdílení informačních zdrojů zvyšuje obtížnost kontroly přístupu. Trend směřující k distribuovanému zpracování oslabil efektivitu centrální kontroly prováděnou specialisty.

Mnoho informačních systémů nebylo navrženo tak, aby byly bezpečné.

Bezpečnost, která může být dosažena technickými opatřeními, je nedostačující a měla by být doplněna odpovídajícím řízením a postupy. Pro určení opatření, která je třeba přijmout, je nutný pečlivý rozbor problémů s důrazem na každý detail. Proto je nezbytné, aby organizace určila své bezpečnostní požadavky. K tomu existují tři základní důvody:

- První vyplývá z hodnocení rizik, která organizaci hrozí. Za pomoci hodnocení bezpečnostních rizik se určují hrozby působící vůči aktivům, zranitelnost vůči hrozbám i pravděpodobnost výskytu a provádí se odhad jejich potenciálního dopadu.
- Druhým zdrojem požadavků jsou požadavky zákonů, zákonných norem a smluvní požadavky, které organizace, její obchodní, smluvní a servisní partneři musí splňovat.
- Třetím zdrojem požadavků jsou konkrétní principy, cíle a požadavky na zpracování informací, které si organizace vytvořila pro podporu provozu.

Z důvodu eliminace nežádoucích vlivů je zapotřebí analyzovat účinnost a vlastnosti aktiv informačního systému, tj. jeho systémových komponent.

Z pohledu zabezpečení informačních systémů rozlišujeme

- **objekt informačního systému** – který představuje pasivní jednotku (entitu) obsahující/přijímající informace a která je zpřístupňována subjekty informačních systémů (udělováním přístupu subjektům),
- **subjekt informačního systému** – který představuje aktivní entitu, tj. osobu, proces, nebo zařízení činné na základě příkazu uživatele. Subjekt informačního systému je autorizovatelný pro získání informací z objektu informačního systému, vydávání příkazů ovlivňujících udělování práv přístupu k objektu, změnu stavu, režimu objektu apod.

Autorizace představuje určení, zda-li je subjekt důvěryhodný pro vykonávání jistých činností. Důvěryhodný informační systém, důvěryhodný objekt nebo subjekt představuje takovou entitu, která je implementována tak, že svou funkcí a specifikací splňuje kriteria

bezpečnostní politiky (je o tom podán důkaz). Důvěryhodná entita se chová tak, jak očekáváme, že se bude chovat. Zranitelné místo informačního systému představuje takovou slabinu informačního systému, kterou je možné využít ke způsobení škody na informačním systému, nebo ke způsobení ztráty (informací, dat), útokem na informační systém. Podstata zranitelného místa informačního systému může být:

- **fyzická** – umístění dostupné sabotáži,
- **přírodní** – objektivní důvody vyvolané přírodními katastrofami (záplavy, blesk, požár…),
- **informační** (informatická) a to:
  a) *Hardwarová* (fyzická) – např. nevhodné propojení bezpečnostních komponent, atd.
  b) *Softwarová* (logická) – např. nedokonalé zrušení dat na mediích, porucha ochrany paměti, atd.
- **fyzikální** – např. vyzařováním při komunikaci, apod.

Základními komponenty informačních systémů jsou počítačové jednotky a komunikační jednotky realizující přenosy dat mezi jednotlivými počítači (počítačovými jednotkami). Proto je bezpečnost systémů analogicky rozdělena na:

- **počítačovou (výpočetní) bezpečnost** – ochrana dat uchovaných v počítači,
- **komunikační bezpečnost** - ochrana dat při jejich přenosu,
- **fyzickou bezpečnost** - ochrana před přírodními hrozbami,
- **personální bezpečnost** - ochrana před vnitřními útočníky.

Potenciální možnost využití zranitelného místa k útoku na informační systém, ke způsobení škody na aktivech informačního systému, se nazývá hrozba. Hrozby lze kategorizovat na:

- **přírodní** - přírodní katastrofy (např. povodeň, požár), obtížná prevence, řešení bezpečnosti je zaměřené na minimalizaci dopadů na informační systém,
- **technické** – výpadek elektrického napětí, poruchy informačního systému, obtížná prevence, řešení bezpečnosti je zaměřené na minimalizaci dopadů na informační systém,
- **neúmyslné** – neúmyslný zásah uživatele do aktiv informačního systému,

- **úmyslné** – vědomý zásah uživatele do aktiv informačního systému s cílem narušit bezpečnost informačního systému nebo obdržet důvěryhodná data informačního systému, přičemž se rozlišují:

  a) *interní útočníci* – útočníci uvnitř organizace, útočníci s přístupem (i autorizovaným) k důvěryhodným datům,

  b) *externí útočníci* – útočníci mimo organizaci,

  c) *kombinace útočníků* – kombinace interních a externích útočníků, velmi efektivní z hlediska vedení útoků.

V oblasti bezpečnosti dat jsou specifikovány čtyři typy hrozeb namířených proti bezpečnosti informačního systému. Jsou to:

- ***přerušení***, kdy se aktivum informačního systému ztratí, stane se nepoužitelným nebo nepřístupným. Příkladem je zničení hardwarového zařízení, výmaz programu nebo datového souboru anebo selhání operačního systému při vyhledávání souboru na disku.
- ***odposlech,*** při kterém neoprávněná strana získá přístup k aktivu. Neoprávněná strana může být jak osoba, tak program nebo výpočetní systém. Příkladem je například nepovolené kopírování programů nebo datových souborů nebo tajný odposlech prováděný při datových přenosech po síti. Ztráta aktiva může být odhalena bezprostředně, ale „tichý“ odposlech nemusí zanechat stopy, podle nichž by byl odhalitelný.
- ***modifikace,*** kdy neoprávněná strana nejenže získá přístup k aktivu, ale také tohoto přístupu využije k jeho pozměnění. Příkladem může být nelegální provedení změn v datech v databázi, pozměnění programů tak, že se ovlivní jejich běh, nebo provedení změn na datech v průběhu jejich přenosu po síti. V některých případech se pozměnění aktiva projeví ihned, ale některé případy je téměř nemožné detekovat.
- ***vytvoření falsifikátu*** určitého objektu neoprávněnou stranou. Příkladem může být neoprávněné vložení falešných záznamů do databáze nebo vytvoření falešné zprávy a její následné odeslání po síti.

1.2 Hodnocení bezpečnostních rizik

Požadavky na bezpečnost jsou stanoveny za pomoci metodického hodnocení bezpečnostních rizik. Výdaje na bezpečnostní opatření by měly odpovídat ztrátám způsobeným narušením bezpečnosti. Hodnocení rizik může být aplikováno na celou organizaci nebo pouze na její část, stejně jako na jednotlivý informační systém, jeho určitou část nebo službu tam, kde to je praktické, reálné a užitečné.

Hodnocení rizik je zvažování:

- Poškození aktivit organizace, která mohou být selháním bezpečnosti, přičemž je nutné vzít v úvahu potenciální důsledky ze ztráty důvěryhodnosti, integrity nebo dostupnosti informací a jiných aktiv.
- Reálné pravděpodobnosti výskytu takových chyb z pohledu převažujících hrozeb, zranitelností a aktuálně implementovaných opatření.

Výsledky hodnocení rizik pomohou určit odpovídající kroky vedení organizace i priority pro zvládání bezpečnostních rizik u informací a pro realizaci opatření určených k zamezení jejich výskytu. Je možné, že proces hodnocení rizik a stanovení opatření bude třeba opakovat několikrát, aby byly pokryty různé části organizace nebo jednotlivé informační systémy.

Revizi bezpečnostních rizik a přijatých opatření je důležité provádět periodicky, aby bylo možné :

- Určit změny požadavků organizaci a priorit.
- Vzít v úvahu nové druhy hrozeb a slabin.
- Potvrdit vhodnost a účinnost přijatých opatření.

Revize by měly být prováděny do různé hloubky v závislostí na výsledcích předcházejících analýz a změn v úrovních rizik, které je vedení ochotno akceptovat.

Hodnocení rizik je často zpočátku realizováno na obecné úrovni, jako prostředek ke stanovení priority zdrojů v oblasti závažných rizik a až poté v detailnějších rovinách pro určení konkrétních rizik.

1.3 Řízení bezpečnosti IT

Je nutné vzít v úvahu kulturu a prostředí, ve kterém je organizace činná, protože tyto aspekty mohou mít významný vliv na celkový přístup k bezpečnosti. Navíc mohou mít vliv na ty, kdo jsou zodpovědní za ochranu specifických částí organizace. V některých případech je považována za odpovědnou vláda a ta se vyrovná s touto odpovědností přijetím a prosazením zákonů.

Pro identifikaci požadavků bezpečnosti IT uvnitř organizace je nutný systematický přístup. To platí rovněž pro implementaci bezpečnosti IT, a její stále probíhající správu. Tento proces je nazýván řízením bezpečnosti IT a zahrnuje následující činnosti:

- vývoj politiky bezpečnosti IT,
- identifikaci rolí a odpovědností uvnitř organizace,
- management rizik, včetně identifikace a odhadu:
    - aktiv, která je třeba chránit,
    - hrozeb,
    - zranitelností,
    - dopadů,
    - rizik,
    - ochranných opatření,
    - zbytkových rizik,
    - omezení,
- řízení konfigurace,
- řízení změn,
- havarijní plány a plánování obnovy po havárii,
- výběr a implementace ochranných opatření,
- povědomí o bezpečnosti
- údržby,
- bezpečnostního auditu,
- monitorování,
- revize, a
- zacházení s incidenty.

1.4 Cíle, strategie a politiky

Cíle, strategie a politiky bezpečnosti společnosti je třeba zformulovat jako základnu pro účinnou bezpečnost IT v dané organizaci. Podporují činnost organizace a společně zajišťují konzistenci mezi všemi ochrannými prostředky. Cíle identifikují co bude dosaženo, strategie identifikují jak těchto cílů dosáhnout, a politiky identifikují co je třeba udělat.

Cíle, strategie a politiky mohou být stanoveny hierarchicky od úrovně celé společnosti k operační úrovni organizace. Měly by odrážet organizační požadavky a vzít v úvahu jakákoliv organizační omezení, a měly by zajistit, aby na každé úrovni a přes všechny úrovně byla udržována konzistence. Bezpečnost je odpovědností všech úrovní managementu uvnitř organizace a vyskytuje se ve všech fázích životního cyklu systémů. Cíle, strategie a politiky by měly být udržovány a aktualizovány na základě výsledků periodických bezpečnostních revizí (např. analýzy rizik, bezpečnostních auditů) a změn obchodních cílů.

Popis úrovní bezpečnostních politik ve společnosti:

- Bezpečnostní politika celé společnosti zásadně zahrnuje bezpečnostní zásady a směrnice pro organizaci jako celek. Bezpečnostní politiky společnosti musí odrážet širší politiky společnosti, včetně těch, které se zabývají právy jednotlivců, právními požadavky a normami.
- Bezpečnostní politika IT celé společnosti musí odrážet základní bezpečnostní zásady a směrnice aplikovatelné na bezpečnostní politiku společnosti a všeobecné používání systémů IT uvnitř organizace.
- Bezpečnostní politika systémů IT musí odrážet bezpečnostní zásady a směrnice obsažené v bezpečnostní politice IT společnosti. Měla by také obsahovat podrobnosti specifických bezpečnostních požadavků a ochranných opatření, které mají být implementovány a návod, jak je správně používat, aby byla zajištěna adekvátní bezpečnost. Ve všech případech je důležité, aby přijatý přístup byl efektivní v relaci k obchodním potřebám organizace.

1.5 Hodnocení současné situace informační bezpečnosti v ČR

Průzkum stavu informační bezpečnosti v České republice v roce 2003 provedla společnost Ernst & Young ve spolupráci s národním bezpečnostním úřadem a specializovaným časopisem Data Security management již potřetí a díky tomu poskytuje nejen informace o současném stavu, ale nabízí také pohled na trendy v oblasti bezpečnosti firemních organizačních systémů.

Průzkum probíhal formou dotazníků s 56 otázkami soustředěnými do 14 skupin, osloveny byly střední a velké organizace s více než stem zaměstnanců. Největší zastoupení měl ve výzkumu státní sektor, následovalo strojírenství a energetické společnosti. Celkem společnost Ernst & Young získala pro další zpracování 362 vyplněných dotazníků, přičemž 72 % z nich byla vyplněna přímo lidmi, kteří za bezpečnost informačních systémů odpovídají.

1.5.1 Výsledky za rok 2003 a porovnání s rokem 2001

Výsledky průzkumu lze interpretovat následovně:

- Téměř polovina firem již řešila bezpečnostní problémy s přímým finančním dopadem, ale jen 13 procent českých firem má někoho, kdo se věnuje zejména bezpečnosti. Výsledky průzkumu nicméně naznačují pozitivní trendy.
- Česká republika není stranou problému s bezpečností počítačových systémů a sítí. Výzkum agentury Ernst & Young ukázal, že stejně jako ve světě i u nás jsou největším bezpečnostním rizikem pro informační systémy sami zaměstnanci a počítačové viry.
- V oblasti personálního a finančního zajištění bezpečnosti informačních systémů je nejvíce vidět rozdíl mezi bankami a ostatními organizacemi.
- Vyčleněný rozpočet na otázku bezpečnosti má v průměru 15 % organizací a tyto výdaje tvoří přibližně 8 % nákladů na IT jako celek. U finančních institucí v průzkumu mělo vlastní rozpočet na zabezpečení 67 % oslovených společností, ale jejich poměr k výdajům na informační technologie byl o procento nižší. Překvapivé je, že ani u bank a podobných společností není železným pravidlem existence plánů na obnovu funkce systému (87 % banky, 49 % průměr) nebo pravidelná analýza rizik (87 % banky, 61 % průměr).
- U poloviny organizací měly bezpečnostní incidenty v uplynulých dvou letech prokazatelný přímý finanční dopad (např. poškození nebo ztráta zařízení, cena opravy).

- Existence či neexistence bezpečnostní politiky pokrývající oblast informací a IS/IT je jedním ze základních ukazatelů toho, jak organizace k řešení informační bezpečnosti přistupují. Pod pojmem „bezpečnostní politika“ máme na mysli dokument schválený a vyhlášený nejvyšším vedením organizace. Neexistence bezpečnostní politiky ve většině případů signalizuje, že daná organizace přistupuje k řešení informační bezpečnosti nekoncepčně, bez definovaných pravidel a jasně definovaných zodpovědností. Vývoj za poslední čtyři roky ukazuje, že počet organizací s přijatou bezpečnostní politikou pomalu roste.
- Bezpečnost internetu :
    - Od roku 1999 se procento zaměstnanců s přístupem k internetu zvýšilo ze 17% na 47%.
    - Internet a elektronická pošta představují podle organizací stále největší hrozbu.
    - Za poslední dva roky došlo k výraznému nárůstu incidentů v podobě virů získaných ze souborů stažených z internetu.
    - Jen každá desátá organizace nebyla postižena viry z elektronické pošty.
- Od roku 1999 do roku 2003 se také výrazně změnil způsob zabezpečení internetu.
- Průzkum také ukázal překvapivý pokles finančních nákladů na informační bezpečnost vzhledem k ostatním odvětvím IT. Tato hodnota spíše než typický pokles vyznačuje stagnaci výdajů na informační bezpečnost než u jiných odvětvích IT.
- Nejčastějším problémem, se kterým se správci IS setkávají, je obyčejný výpadek elektrického proudu. Krátkodobé i delší výpadky zaznamenalo v roce 2003 89 % firem a stejně jako druhý nejrozšířenější problém – selhání hardwaru si udržuje setrvalou tendenci. Třetí největší hrozbou jsou počítačové viry. Chyby software potkaly méně než polovinu respondentů. Přibližně čtvrtina firem musela řešit i selhání administrátora, tento problém má ale podle zjištění E&Y klesající tendenci. Naopak nárůst problémů zaznamenaly firmy u nepovolených přístupů k systému zvenčí (7 %) a následky přírodních katastrof (20 %).
- Součástí analytické zprávy je také odhad budoucích rizik, který v podstatě opakuje již známé. Největší hrozbou jsou a budou uživatelé s přístupem k internetu. Internet je jako anonymní a nedůvěryhodné prostředí nejčastějším zdrojem problémů, ať už jde o nebezpečí počítačových virů, které i přes využívání antivirových systémů nadále zůstává i problémem pracovní hygieny uživatelů, nebo nezávislé útoky zvenčí. Nicméně i přes

rostoucí kvalitu technologií zůstává lidský faktor stále nejrizikovějším prvkem ve fungování informačních systémů, a brzkou změnu nelze očekávat.

- Dalším znepokojujícím faktorem v oblasti internetu je výrazný nárůst spamu nebo-li nevyžádané pošty. Odhaduje se, že okolo 70 - 80% celé elektronické komunikace je spamového charakteru.
- 78 % dospělých uživatelů internetu dostává nevyžádanou poštu denně,
- 11 % dostává denně více než 40 nevyžádaných zpráv,
- 14 % z nich spamové zprávy před mazáním čte,
- 5 % uživatelů přiznalo, že v posledním roce pořídilo nějaký produkt na základě spamu.

Informační bezpečnost se v posledních letech v České republice zlepšila. Organizace si uvědomily hodnotu svých informací a potřebu je adekvátním způsobem chránit. Zejména finanční instituce jsou v tomto kroku napřed, dobrá bezpečnost systému je zárukou pro klienty. Ostatní instituce v tomto kroku mírně pokulhávají. Výdaje na informační bezpečnost stále neodpovídají dané potřebě.

Organizace si neuvědomují, že výdaje investované do bezpečnosti jsou mnohem menší než výdaje na odstranění následků bezpečnostních incidentů. Spousta organizací investovala jednorázově do nákupu firewallu, ale už neřeší další problémy s bezpečností a nesledují vývoj v oblasti IT.

Oblast informatiky se vyvíjí velice rychlým tempem, kromě nových technologií přibývají i nová nebezpečí. Roste počet virů, počet spamů v emailech je okolo 70-80%, roste počet útoků na informační systémy. Tento trend bude pokračovat i v dalších letech a je proto nutné do bezpečnosti investovat a zavádět nové technologie, jež zvýší bezpečnost IS v organizacích.

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.

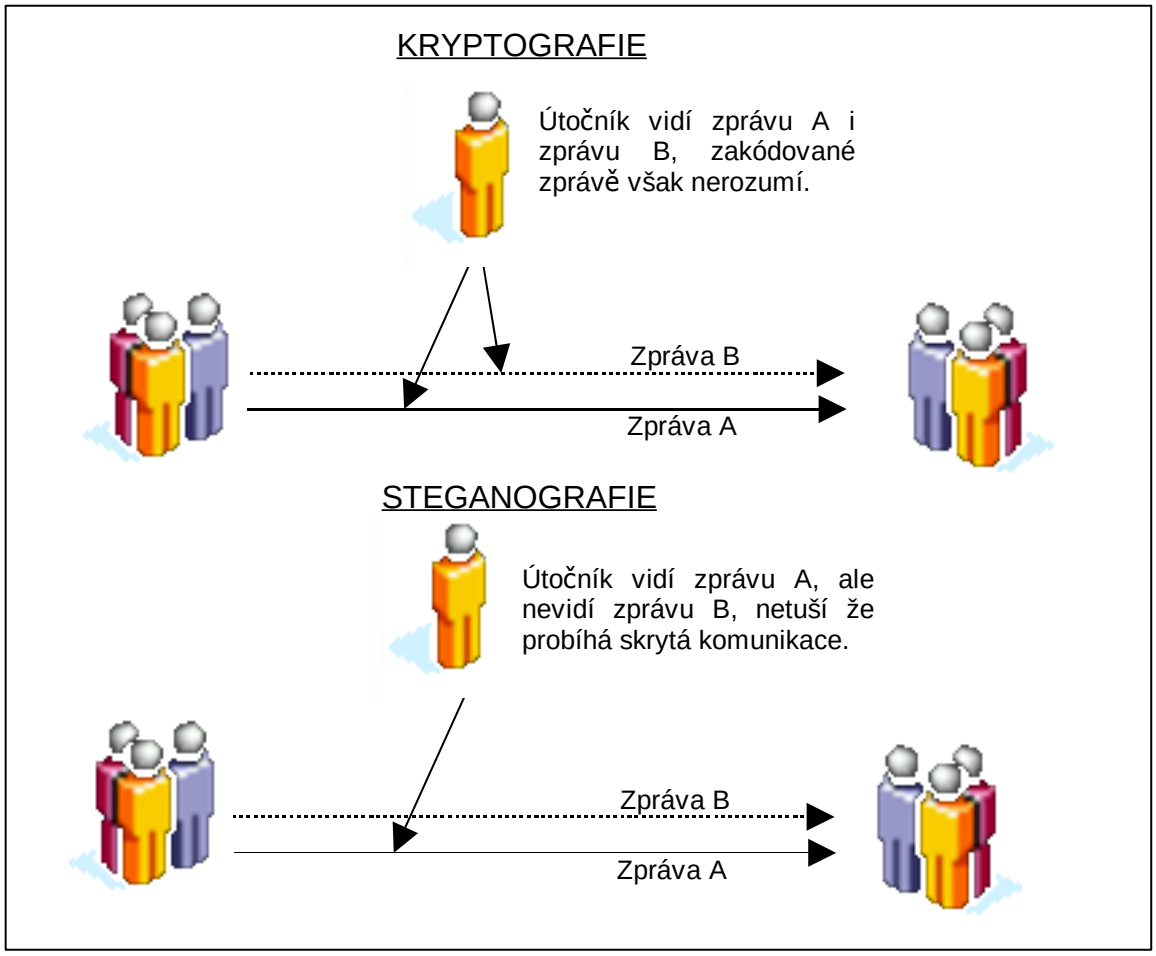
Ukrývání digitálních dat je umění a věda týkající se návrhu takových metod komunikace, které kromě zabezpečení důvěrnosti přenášených dat ukryjí také fakt, že jsme se důvěrnost něčeho snažili zabezpečit, případně ukryjí také samotnou komunikaci.

Problematikou ukrývání informací se zabývají následující oblasti**:**

- **Kryptografie** (cryptography) – zabývá se studiem matematických postupů, které 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 znát 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). Techniky křehkého vodotisku modifikují vodoznak při jakékoli operaci s daty, do kterých je vodoznak vložen. 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 navrhovány, ani nebyly pro přenos informací plánovány. Tato technika je používána některými softwarovými produkty, které 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 je ukrýt cestu přenosu zprávy použitím většího počtu anonymních osob, které přijatou zprávu poslaly další osobě a tím se postupně dostala až k adresátovi. Předpokladem použití byla zejména důvěra a spolehlivost jednotlivých anonymních osob.



Obr. 1: Kryptografie versus steganografie

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.

2.1 Rozdělení steganografických technik

Podle používaných metod v digitální steganografii je možné rozdělit steganografické techniky do tří odlišných skupin:

- **Injekční steganografie** (injection steganography) – využívá vložení dat do jiných dat, tzn. krycích dat, kterými 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 vložena tak, aby na straně příjmu byla klientskými programy nebo prezentačními algoritmy (prohledávače obrázků, audioprohledávače, textové editory) ignorována. Mnohé aplikace injekční steganografii umožňují. Data vložená do krycích dat bývají v steganografii označována 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 použity 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, která 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 vkládány. V zásadě rozlišujeme:

- **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 methods), které 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 realizováno 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, která je steganograficky přenášena, nazývaná 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 založeny 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, které jsou do obrazu vkládány. Nejčastější je použití nejméně významných bitů pro toto vložení.
  - *Metody digitálního halftoningu* – ukrytí dat je realizováno modifikací struktury aproximovaného šedého odstínu v pseudovíceúrovňových obrazech.

- *Subpásmový rozklad obrazů* – jestliže jsou krycí obrazová data frekvenčně rozdělena 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, kterými 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) je realizováno v procesu konverze do jiného obrazového formátu změnou některých jeho parametrů, resp. metadat.

- **Ukrývání dat v audiosignálech** – tyto metody jsou založeny 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 jsou modifikovány 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 průběhu 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 možno největší šířku. Tato technika je využívána při nízkých bitových rychlostech signálu.
- **Ukrývání datové odezvy** – tato technika realizuje ukrytí dat do audiosignálů zavedením odezvy signálu. Odezva signálu je definována třemi parametry – počáteční amplituda, opoždění, rychlost tlumení. Odezvy, které jsou charakterizovány 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 nastavena tak, aby byly 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:
  - **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 kvůli jehož extrakci není třeba spouštět ani simulovat. Statický vodotisk je však lehce atakovatelný transformacemi zachovávajícími sémantiku programu.

    Při statickém vodotisku mohou být vkládané informace vloženy do:

    - Segmentu inicializovaných dat (kde jsou uloženy statické řetězce).
    - Kódového segmentu (vykonávatelný kód).
    - Ladících informací.

- Dynamický vodotisk (dynamic watermark) – vodotisk je definován jako stav během vykonávání programu. Při dynamickém vodotisku aplikace běží na předurčeném vstupu, který 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 něj extrahován. Rozlišujeme tři techniky dynamického vodotisku – vodotisk se skrytou funkčností, vodotisk v datových strukturách a vodotisk v postupnosti vykonávání.

2.2 Klasifikace digitálních vodoznaků

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

- **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 vsunuta do původních informací bez toho, aby se podstatně narušil původní informační obsah, tedy není běžně viditelná. 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 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:

- **Postřehnutelné** – obyčejně obsahují viditelný odkaz nebo logo společnosti.
- **Nepostřehnutelné** – krycí data s vloženým vodoznakem jsou vizuálně velmi podobná původním datům bez vodoznaku. Existenci takového vodoznaku je možné dokázat jen jeho extrakcí či detekujícím algoritmem.

Z hlediska odolnosti lze vodoznaky rozdělit na:

- **Křehké** – vodoznaky vložené touto metodou jsou lehce 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, které vyžadují uživatelský klíč, lze dělit na algoritmy:

- **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 standardní algoritmus metody s veřejným klíčem.

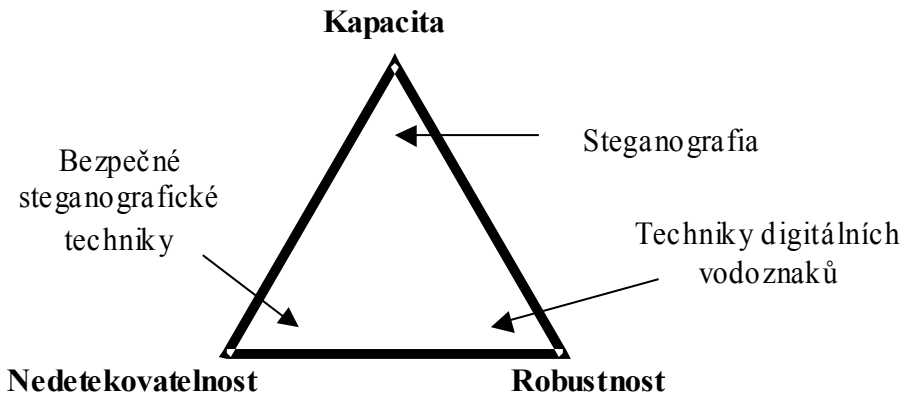
2.3 Kritéria na steganografické systémy

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

- **Robustnost** – vložená informace se nazývá robustní, pokud je lehce detekovatelná z krycích dat do kterých byla vložena, a to i v případě, kdy byla poškozena 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 vědět, že schopnost detekovat vložené informace ještě neznamená schopnost její extrakce.

- **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, ve kterém buď je nebo není vložená informace, a to tak, že určité množství lidí porovnává tyto vzorky. Jako úspěšná hodnota neviditelnosti se považuje ta hodnota, kdy 50% zúčastněných lidí nedokáže odlišit označené vzorky od originálních.
- **Bezpečnost** – o bezpečném algoritmu se hovoří tehdy, když vložená informace nemůže být extrahována z označených dat bez znalosti algoritmu vkládání a extrakce. Pojem bezpečnost také 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 je schematicky znázorněna tato situace a taktéž je znázorněno, jaké požadavky jsou upřednostňovány v jednotlivých oblastech skryté informace.



Obr. 2: Požadavky na steganografické systémy.

2.4 Imperceptibilita vložené informace

K analýze vlastnosti imperceptibility vložených vodoznaků se používají následující subjektivní a objektivní metody.

Objektivní metody

Pro objektivní analýzu kvality digitálních obrazů budou zvolena následující uvedená kritéria.

Existuje-li obraz s rastrem $n_1 \times n_{2:}$

1) Střední kvadratická chyba (*MSE-Mean Square Error*)

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

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

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

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

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

3) Odstup signálu od šumu (v [*dB*])

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

4) Vrcholový odstup signálu od šumu (*Peak Signal to Noise Ratio*)

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

Subjektivní metody

Subjektivní kritéria je možné popsat dvojím způsobem:

- kvantitativně neboli známkami,
- kvalitativně neboli slovně.

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

2.5 Útoky na steganografické přenosy

Analogicky, jako v kryptografii, je kryptoanalýza zaměřena na útoky na kryptosystémy, resp. na jejich bezpečnost vůči útokům, ve steganografii se útoky na steganografické systémy zabývá steganalýza (steganalysis) [5]. Steganalýza rozlišuje čtyři útoky na steganografické systémy, které do jisté míry korespondují s kryptoanalytickými útoky. Porovnání klasifikace steganalytických a kryptoanalytických útoků je uvedena v tab.1.

Útok se znalostí jen stego-objektu (stego-only attack) představuje takový útok, kdy steganalytik má k dispozici jen stego-objekt, tj. objekt s vloženými daty. V případě, že je kromě stego-objektu k dispozici ještě informace o tom, jakého algoritmu bylo použito při uložení krycích dat, jedná se o útok se znalostí stego-objektu a algoritmu (chosen-stego attack). Pokud jsou při stegoanalýze kromě stego-objektu k dispozici originální (původní) krycí data, půjde o útok se znalostí krycích dat (known-cover attack), bude-li při útoku se znalostí krycích dat navíc informace o použitém algoritmu, půjde o komplexní steganografický útok (known-stego attack).

Tabulka 1: Rozdělení steganalytických a kryptoanalytických útoků

Steganalýza		**Kryptoanalýza**	
Anglicky	*Česky*	*Anglicky*	*Česky*
stego-only attack	*Útok se znalostí jen stego-objektu*	**ciphertext-only attack**	*Luštění se znalostí jen zašifrované zprávy*
chosen-stego attack	*Útok se znalostí stego-objektu a **algoritmu***	**chosen-plaintext attack**	*Luštění se znalostí vybraných otevřených textů*
known-cover attack	*Útok se znalostí krycích dat*	**known-plaintext attack**	*Luštění se znalostí otevřené zprávy*
known-stego attack	*Komplexní steganografický útok*		

Přirozeně, útoky na steganografické systémy nejsou realizovány jen ze strany steganalýzy. V kontextu steganografické komunikace rozlišujeme tři typy útočníků:

- **aktivní útočníci** (active attackers) – sledují komunikaci mezi dvěma stranami – odesílatelem a příjemcem zprávy a snaží se odhalit způsob tajné komunikace mezi nimi, tj. hledají v krycích datech ukryté tajné zprávy.
- **pasivní útočníci** (passive attackers) – jsou útočníci, kteří netuší o tajné komunikaci a změní krycí data dřív, než se dostanou k přijímateli, nebo při zkoumání krycích dat náhodně objeví ukryté tajné zprávy.
- **zlomyslní útočníci** (malicious attackers) – zachytávají zprávy od odesílatele, získané tajné zprávy modifikují a posílají přijímateli bez toho, aby si toho přijímatel všiml, nebo posílají vlastní zprávy předstírajíc, že jsou pravým odesílatelem.[2]

II. PRAKTICKÁ ČÁST

3 OBECNÝ POPIS DIGITÁLNÍCH OBRAZŮ

Předpokládáme, že originální obraz, do kterého chceme vložit vodoznak, bude statický víceúrovňový (šedý) obraz *I*. Statické obrazy jsou charakterizovány prostorovým a jasovým rozlišením, resp. prostorovou a jasovou rozlišovací schopností. Tato podkapitola čerpá z literatury [30].

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.

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 taky 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

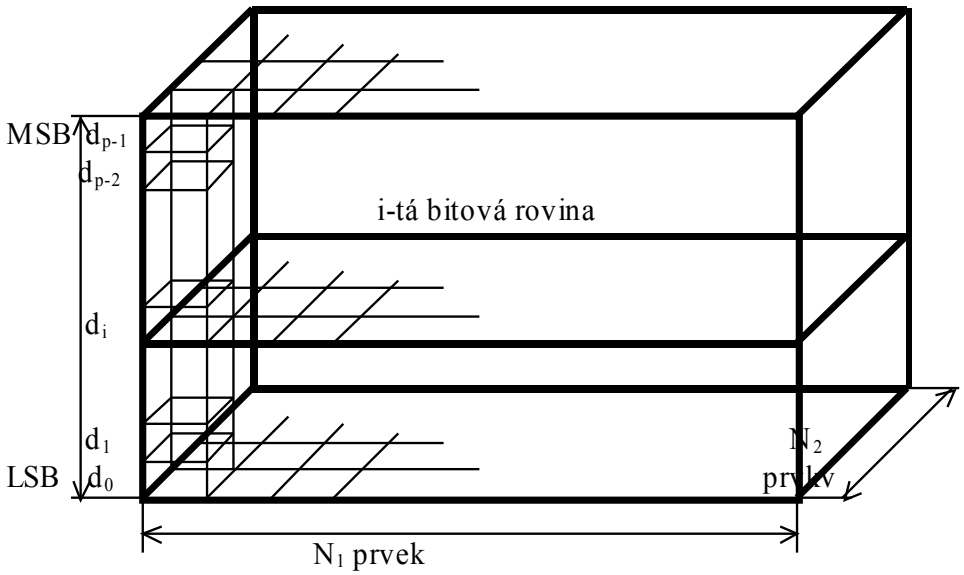
černými a bílými obrazovými prvky, odstín šedé barvy je dán „koncentraci“ bílých a „koncentraci“ černých obrazových prvků v dané oblasti obrazu).

3.1 Možnosti využití rozkladu krycího obrazu na bitové roviny ve steganografii

Víceúrovňový statický obraz je možné interpretovat taky 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.

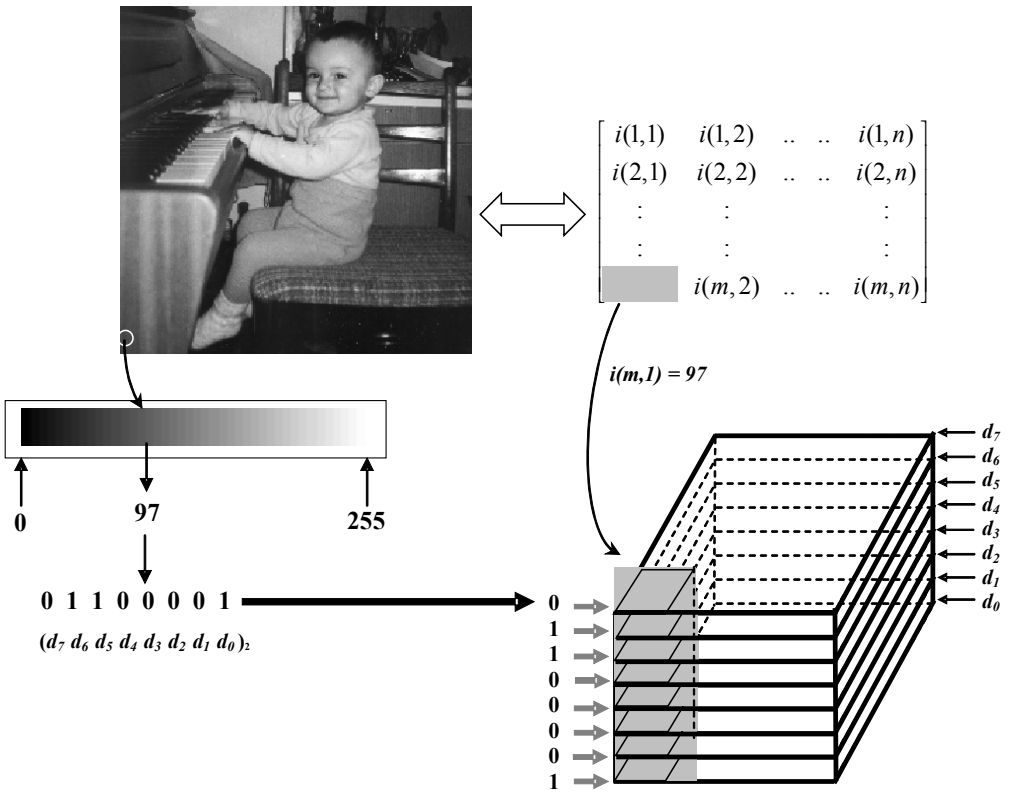
Popíšeme-li všechny obrazové body jejich binárními reprezentacemi, získáme třírozměrný model originálního obrazu I, kde osy x a y udávají velikost (rastr) obrazu, tedy $n_I \times m_I$ a osa z udává bitovou reprezentaci každého obrazového prvku. Z takového modelu získáme p – bitových rovin obrazu I, 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.

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 obr. 3.

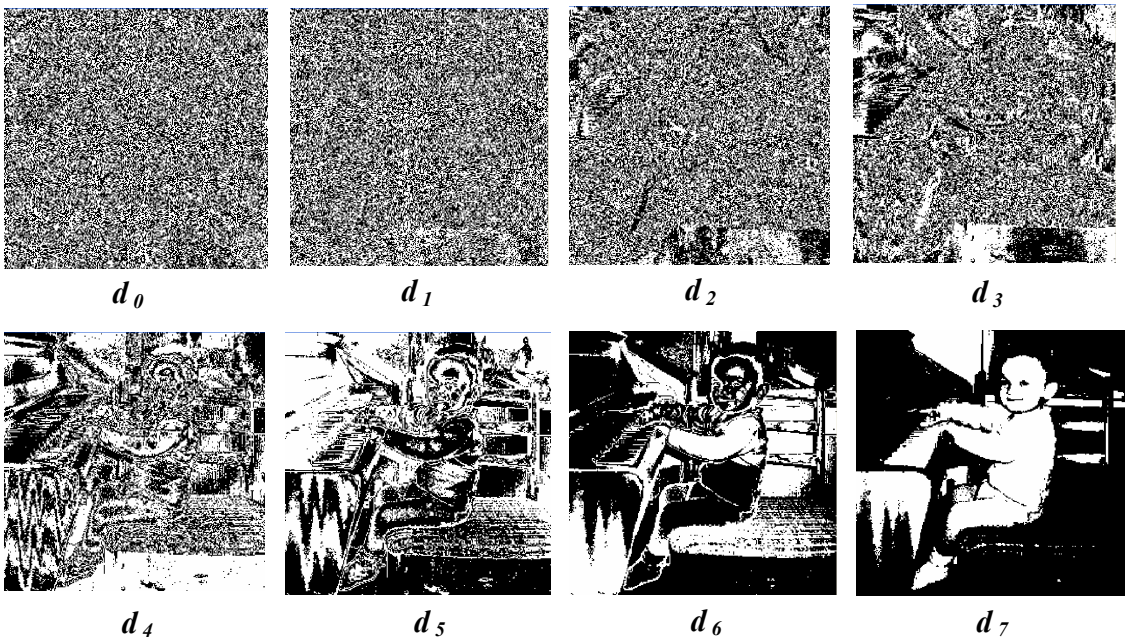


Obr. 3: Trojrozměrný model krycího obrazu.

Postup rozkladu statického víceúrovňového obrazu je znázorněn na obr. 4 a ukázky binárních obrazů získaných rozkladem obrazu na bitové roviny je znázorněn na obr. 5.



Obr. 4: Postup rozkladu statického víceúrovňového obrazu na bitové roviny.



Obr. 5: Binární obrazy - rozklad víceúrovňového statického obrazu po bitových rovinách.

3.2 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) a způsobující změnu původních dat za účelem jejich utajeného přenosu, resp. za účelem prokázání vlastnictví původních krycích dat (digitální vodotisk).

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 je vhodné vodoznak vkládat nejvíce do prvních čtyř bitových rovin (d_0 až d_3), čímž bude zabezpečena nižší vjemová viditelnost vodoznaku, vyšší kvalita obrazu s vodoznakem a nižší pravděpodobnost odstranění vodoznaku nepovolanou osobou. Je možné také použít více bitových rovin – různé části vodoznaku W je možné vkládat do různých bitových rovin (to může

představovat součást uživatelského klíče), čímž získáme prostorové rozptýlení vodoznaku v třírozměrném prostoru našeho (uvažovaného) modelu.

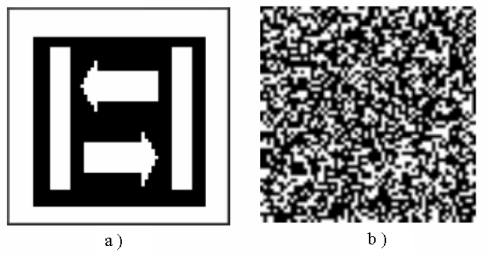
Pro jednoduchost předpokládejme vložení vodoznaku W do první bitové roviny d_0. Prostorová rozlišovací schopnost vodoznaku W je dána $m_W \times n_W$; prostorová rozlišovací schopnost originálního obrazu I je $m_I \times n_I$, proto i vybraná bitová rovina d_0 bude $m_I \times n_I$. Rozměr vodoznaku 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 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

$$W_P = v\left(W\right)$$

kde $v(.)$ je operace přeuspořádání obrazových prvků.

Názorný příklad permutovaného vodoznaku je znázorněn na následujícím obr. 6.



Obr. 6: Obrazová permutace vodoznaku: a) originální vodoznak; b) permutovaný vodoznak.

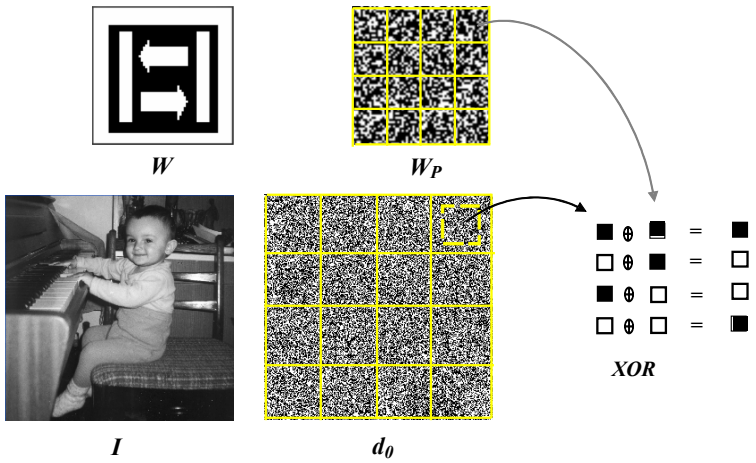
Aby se některými ztrátovými operacemi (např. vystřižení části obrazu) vodoznak neodstranil, pro jeho vložení se využívá celá „plocha“ daná prostorovým rozlišením obrazu. To je zabezpečeno postupem, který rozdělí selektovanou bitovou rovinu (v našem případě d_0) na vzájemně se nepřekrývající bloky, které pokryjí celou oblast (d_0). Permutovaný vodoznak W_p bude rozdělen na analogicky, na stejný počet vzájemně se nepřekrývajících

bloků, které pokryjí 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 realizujeme tak, že vybrané obrazové prvky bloku bitové roviny modifikujeme podle hodnot prvků odpovídajícího bloku permutovaného vodoznaku. Jedním z možných způsobů je pomyslné překrytí bloku bitové roviny blokem permutovaného vodoznaku (uprostřed bloku) a prvky bloku bitové roviny v oblasti překrytí bloků se modifikují funkci *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 vložení vodoznaku je znázorněn na obr. 7.



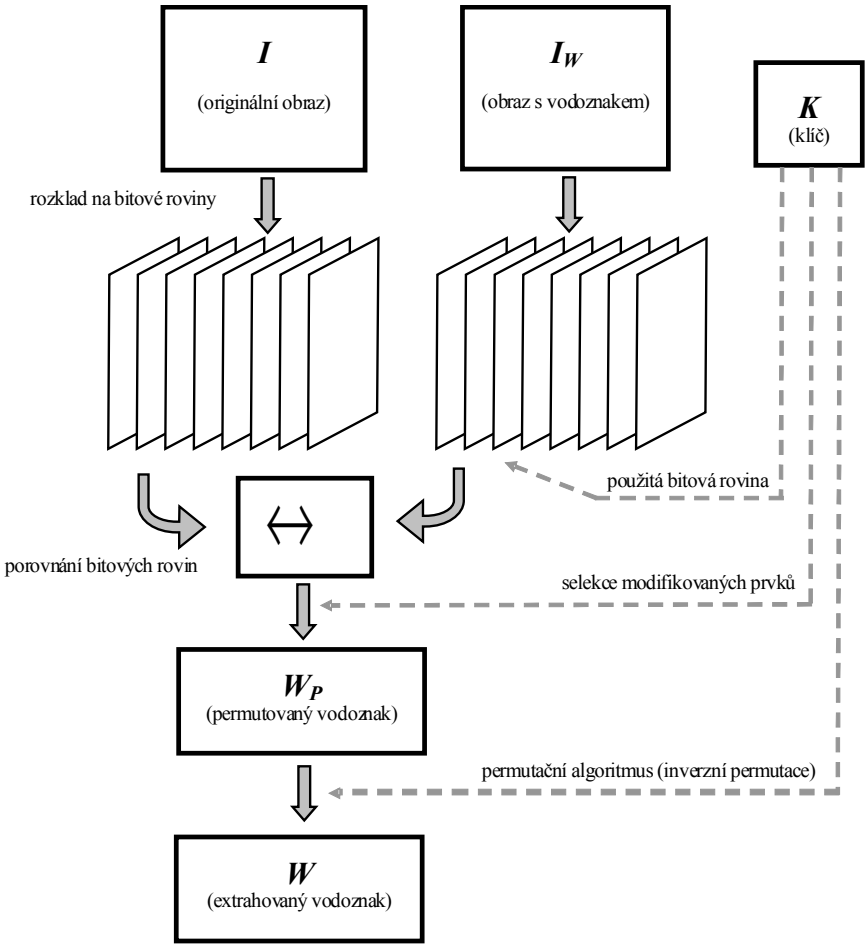
Obr. 7: Princip vložení vodoznaku.

Poznamenejme, že existuje mnoho modifikací tohoto přístupu, které se týkají:

- způsobu modifikace prvků bitové roviny (je možné použít např. nahrazení vybraných prvků bitové roviny prvky permutovaného vodoznaku),
- způsobu selekce prvků bitové roviny, které mají být modifikovány,
- výběru používané bitové roviny (nebo bitových rovin - prostorové rozptýlení vodoznaku v třírozměrném prostoru),
- způsobu permutace vodoznaku (bývá používán např. algoritmus vodoznaku na bloky, ve kterých se uskuteční vnitřně-bloková permutace obrazových prvků a potom se vykoná permutace celých bloků, tzv. mezibloková permutace).

3.3 Algoritmus extrakce vodoznaku

K extrakci vodoznaku bude 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 také 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. 8. Extrahováním vodoznaku z obrazu dokazujeme autorská práva k obrazu, do kterého byl vložen.



Obr. 8: Postup extrakce vodoznaku.

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

4 VYBRANÉ STEGANOGRAFICKÉ TECHNIKY

Pro vkládání digitálních vodoznaků do obrazů bylo vyvinuto několik přístupů. Zajímavým přístupem k vkládání vodoznaků do pseudovíceurovňových obrazů pomocí digitálního halftoningu. Tento přístup nachází větší použití jako steganografická technika (utajený přenos informace - vodoznaku), v porovnání s technikami digitálních vodoznaků používaných jako důkaz autorských prav, a to hlavně z důvodu menší robustnosti, tj menší odolnosti vodoznaku vůči ztrátovým operacím s obrazem s vloženým vodoznakem.

Pseudovíceúrovňové obrazy jsou binární (dvojúrovňové) obrazy imitující víceúrovňové (šedé) obrazy technikou označovanou jako halftoning. Halftoning je proces, kterým jsou víceúrovňové obrazy konvertovány na binární obrazy tak, aby vzniklé obrazy co nejvíce imitovaly původní víceúrovňový obrazový dokument. Halftoning simuluje šedý odstín víceúrovňových obrazů hustotou černých a bílých teček (obrazových bodů), umístěných podle definovaných pravidel na stanovené částí obrazu. Důvodem pro používání této techniky je, že většina tiskáren umožňuje tisknout jen v černo-bílém režimu, tj. tisknout jen bílé resp. černé body. Tato technika je založena na vlastnosti prostorové integrace zrakového vnímání člověka (lidské oko při vnímání zanedbá jemnou strukturu těchto teček a zaznamená jen intenzitu šedé, která odpovídá poměru černých a bílých teček – větší počet černých teček koresponduje s tmavším odstínem šedé, větší počet bílých teček koresponduje se světlejším odstínem šedé barvy).

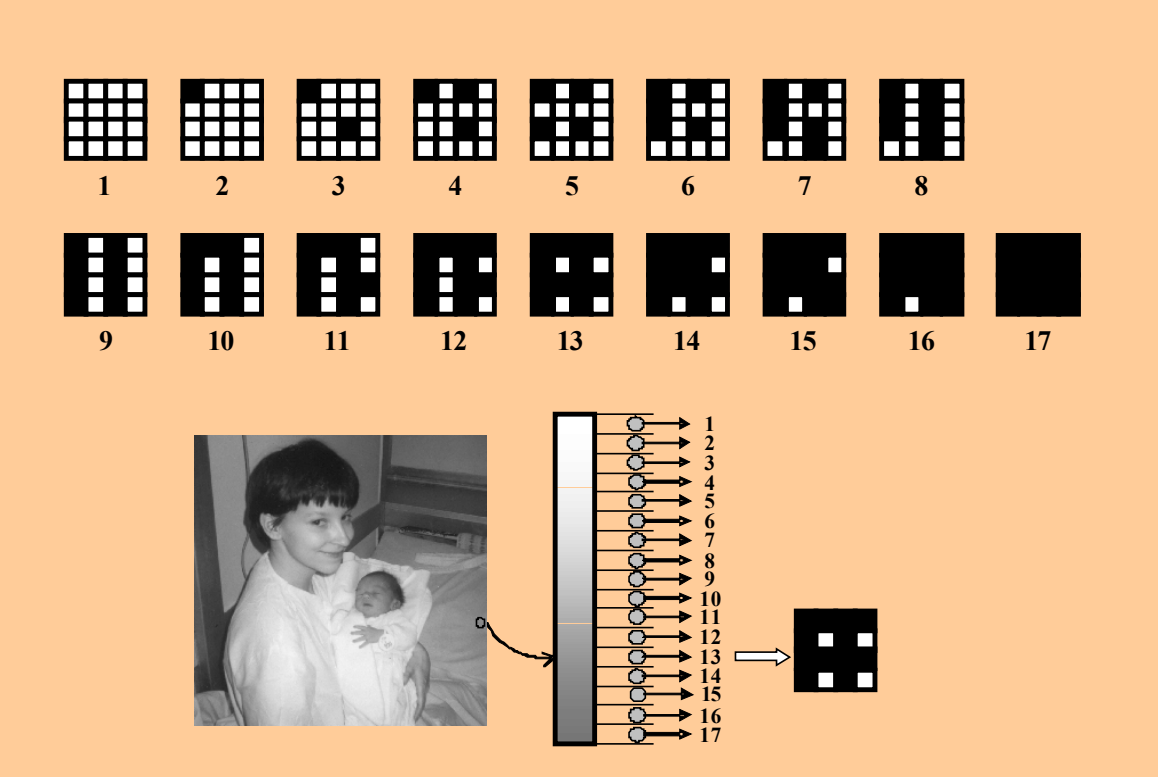
Digitální halftoning (digital halftoning) využívá dekompozice digitálního obrazu na bloky, které jsou nahrazeny odpovídajícími halftoningovými buňkami. Pro použití digitálního halftoningu se používá pět základních přístupů, a to

- patterning,
- dithering,
- maskování (masking, resp. screening),
- difuze chyby,
- náhodné prahování.

4.1 Patterning

Patterning je nejsnadnější technikou pro generování obrazů metodou digitálního halftoningu. Tato technika generuje binární obraz větších rozměrů, než měl původní šedý obrazů. Šedé obrazy používají jasové rozlišení 8bit/pixel, tj. 2^8=256 jasových úrovní (256

odstínů šedé). Tento interval je rozdělen na 17 částí (17 subintervalů). Rozdělení intervalů odstínů, obecně, nemusí být rovnoměrné, ve většině případů se ale setkáváme s rovnoměrným rozdělením (snadnější a rychlejší implementace). Každý obrazový prvek šedého obrazu je nahrazen buňkou velikosti 4×4, proto výstupní obraz bude zvětšen v horizontálním i vertikálním směru čtyřnásobně. Pro každý subinterval je definována jiná buňka. Na obr. 9 jsou znázorněny buňky vytvořené Rylanderovým rekurzivním algoritmem.

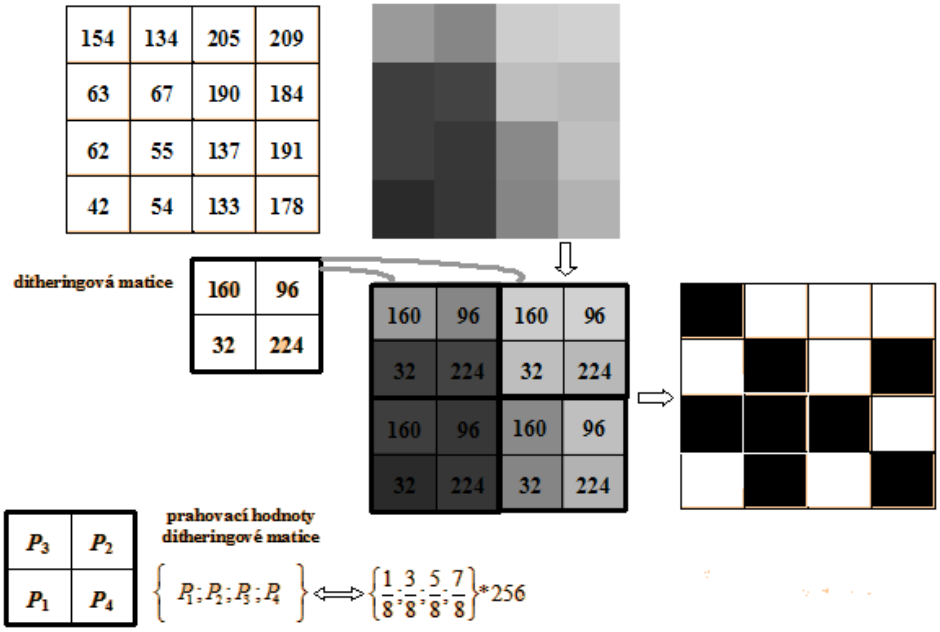


Obr. 9: Princip patterningu.

4.2 Dithering

Jiná technika pro vytváření obrazů pomocí digitálního halftningu je dithering. V porovnání s patterningem produkuje dithering výsledný obraz se stejnou velikostí, jako byl původní šedý obraz. Dithering obrazu je realizoíván prahováním obrazových prvků zdrojového šedého obrazu na základě ditheringové masky, tzv. ditheringové matice (dither matrix), která se opakovaně používána na celý zdrojový obraz. Každý obrazový prvek zdrojového obrazu se porovnává s hodnotou ekvivalentního prvku ditheringové matice. Má-li prvek nižší hodnotu, než příslušný prvek ditheringové matice, bude nahrazen černým obrazovým bodem, má-li hodnotu vyšší, bude nahrazen bílým obrazovým bodem. Uvedený postup náhrady šedého obrazového prvku bílým, nebo černým obrazovým prvkem se

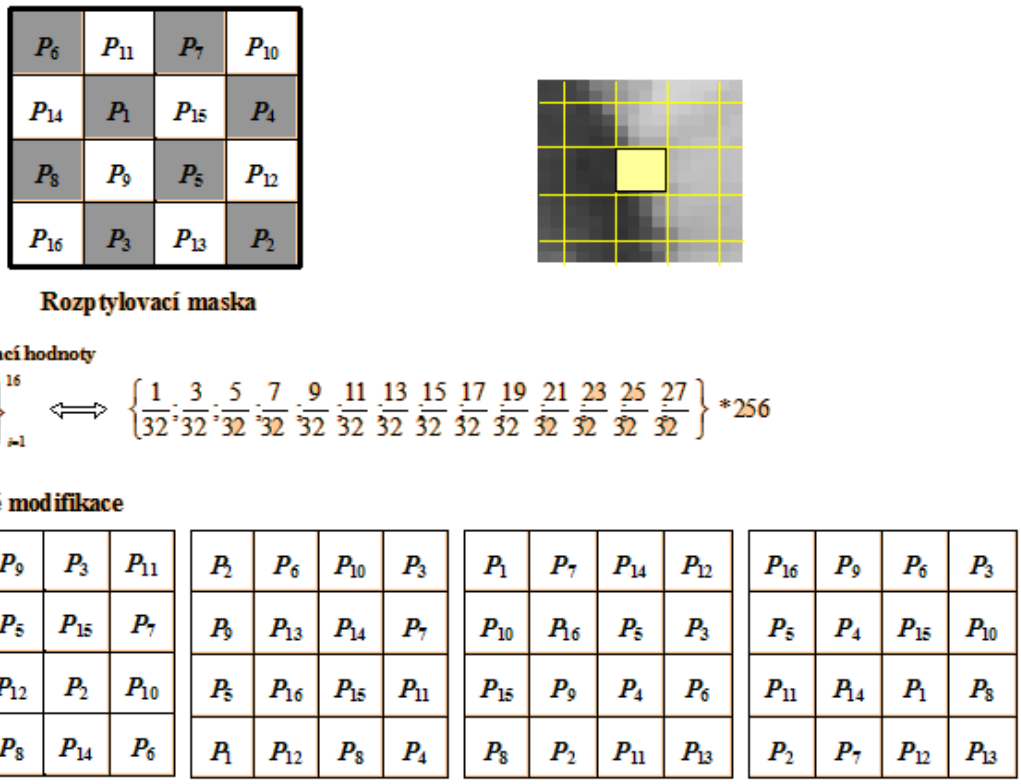
nazývá binarizace obrazu a proces porovnávání hodnot se nazývá prahování. Princip ditheringu je znázorněn na obr.10. Popsaným postupem dochází k nahrazení každé čtveřice (2×2) šedých obrazových prvků čtveřicí (2×2) binárních prvků.



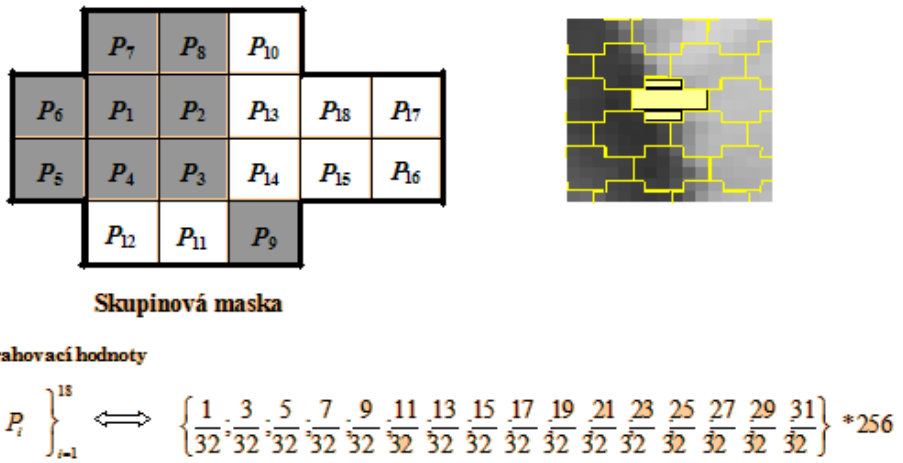
Obr. 10: Princip ditheringu.

4.3 Maskování

Maskování je analogická technika k ditheringu, vylepšuje některé jeho nevýhody, využívá masky větších rozměrů a větší množinu prahovacích hodnot. Rozlišuje me dvě techniky maskování, a to používání rozptylovací masky bodů (dispersed dot mask), která produkuje obraz s vysokým prostorovým rozlišením a používání skupinové masky bodů (clustered dot mask), kterou je možné dosáhnout vysoké rezistence proti rozpíjení inkoustu u inkoustových tiskáren. Princip použití rozptylovací masky pro tvorbu pseudovíceúrovňového obrazu je znázorněn na obr. 11, princip použití skupinové masky je znázorněn na obr. 12. Rozdíl použití rozptylovací masky a skupinové masky je zřejmý z obr.11 a obr. 12 (levá horní část obou obrázků), kde je tmavě šedým odstínem v masce znázorněna distribuce černých a bílých bodů pro stejnou prahovací úroveň. Skupinová maska snižováním prahové úrovně produkuje černé obrazové body ležící „u sebe“, rozptylovací maska má černé a bílé body vzájemně „prostřídané“.



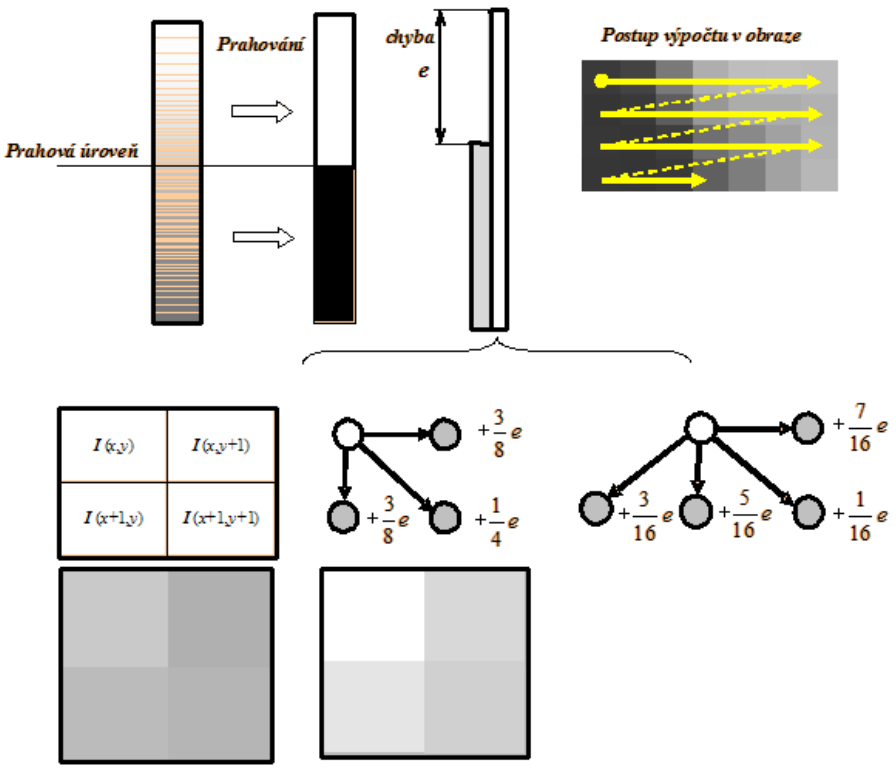
Obr. 11: Princip maskování rozptylovací maskou.



Obr. 12: Princip maskování skupinovou maskou.

4.4 Prostorový dithering

Difuze chyby je další technikou digitálního halftoningu. Bývá také označována termínem prostorový dithering (spatial dithering). Z matematického pohledu minimalizují kvantizační chybu vytvořenu halftoningem. Každý obrazový prvek je porovnáván s prahovou hodnotou. V případě, že bude hodnota obrazového prvku vyšší než prahová úroveň, obrazový prvek bude zaměněn za bílý (hodnota jasu 255), v opačném případě bude nahrazen černým obrazovým prvkem (hodnota jasu 0). Chyba, tj. rozdíl mezi původní hodnotou jasu a výstupní (binární) hodnotou bude rozptýlena k nejbližších „sousedům“, tj. šedé obrazové prvky v okolí aktuálního obrazového prvku budou modifikovány tak, že celková chyba bude distribuována (po částech) do okolních obrazových prvků. Nejčastěji bývá používána fixní prahovací úroveň (fixed thresholding) pro všechny obrazové prvky šedého obrazu (např. střední hodnota jasu celého obrazu), existují různé modifikace využívající adaptivní prahování (adaptive thresholding), měnící se v závislosti od obrazové informaci v jednotlivých částech obrazu, nebo prahování podle náhodných čísel (random thresholding). Distribuce chyby bývá realizována Floyd–Steinbergovým algoritmem, nebo Jarvis-Robertsovým algoritmem. Floyd-Steinbergův algoritmus je schématicky znázorněn na obr. 13.

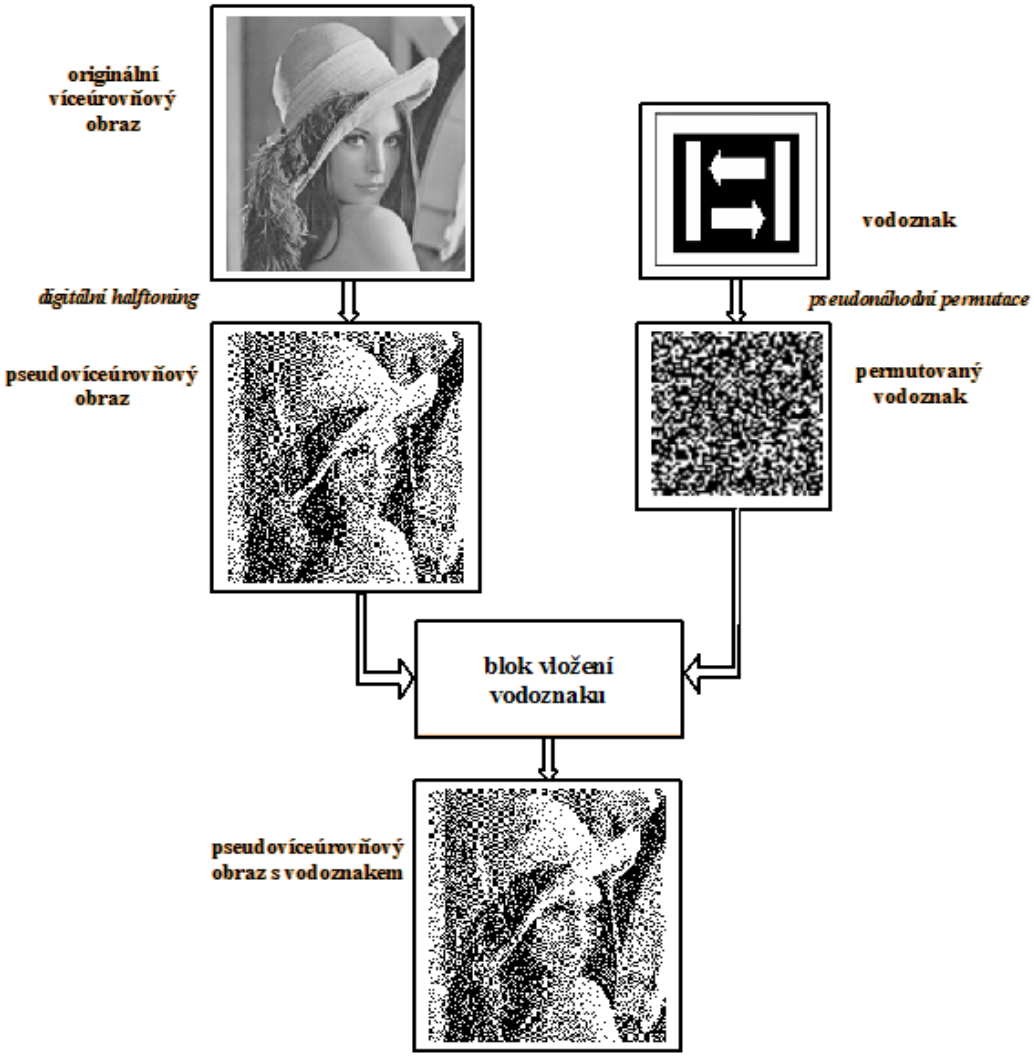


Obr. 13: Floyd-Steinbergův difuzní algoritmus.

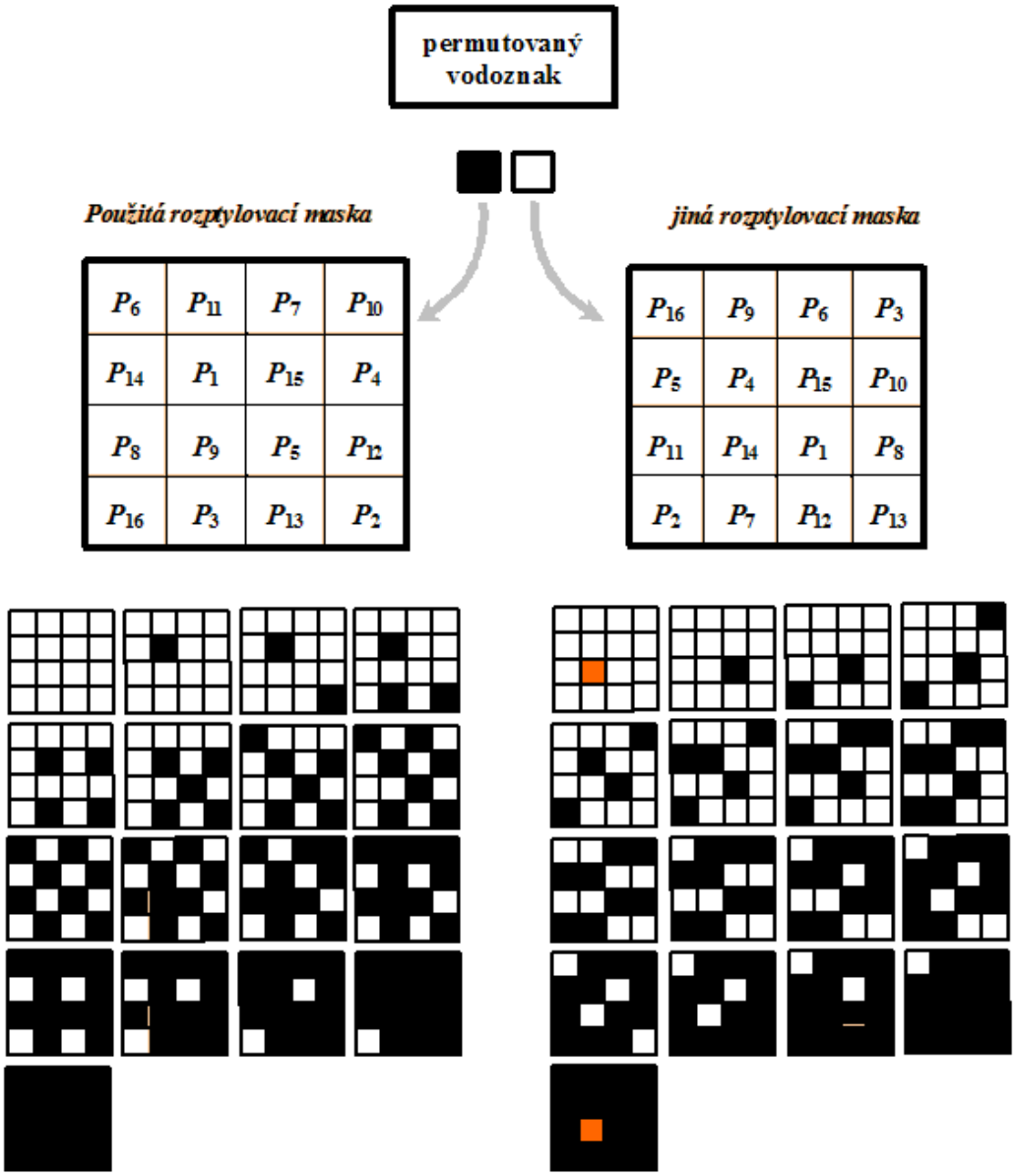
Metody digitálního halftoningu založeny na náhodném prahování využívají ke konverzi šedých obrazů generátory náhodných čísel. Tyto generátory obvykle generují náhodná čísla z intervalu $< 0;1 >$. Výstup z generátoru (náhodné číslo) je násobeno konstantou rovnou maximální hodnotě jasu zdrojového obrazu. Každý obrazový prvek zdrojového obrazu je porovnáván s takovouto hodnotou. Je-li jeho hodnota nižší, než náhodná hodnota (modifikována), bude obrazový prvek nahrazen černým obrazovým prvkem (hodnotou 0), bude-li jeho hodnota vyšší, bude nahrazen bílým obrazovým prvkem (hodnotou 255). Pro každý obrazový prvek zdrojového obrazu je generováno jiné náhodné číslo. Tyto metody se někdy označují termínem dithering s bílým šumem (dithering with white noise).

Postup vložení vodoznaku do pseudovíceúrovňového obrazu je možno popsat na základě obr. 14. Největší možnosti a implementačně nejsnadnější techniky využívají maskování víceúrovňových obrazů. Pro jednoduchost předpokládejme vložení vodoznaku, kterého prostorová rozlišovací schopnost (rozměry v horizontálním a ve vertikálním směru) korespondují s počtem ditheringových masek (matic) v horizontálním a vertikálním směru, kterých bylo použito ke konverzi obrazu na pseudovíceúrovňový obraz. Stejně, jako v případě autentizačních technik bývají vodoznaky permutovány, tj. jejich obrazové prvky bývají vzájemně přeuspořádány podle zvoleného pseudonáhodního permutačního algoritmu. Bude-li splněna podmínka, že velikost vodoznaku odpovídá počtu ditheringových masek v horizontálním a vertikálním směru, bude algoritmus vložení velice jednoduchý. Podle hodnoty intenzity příslušného obrazového prvku (černý nebo bílý) permutovaného vodoznaku modifikujeme použitou masku v pseudovíceúrovňovém obrazu, tj. obecně řečeno, když bude aktuální hodnota obrazového prvku permutovaného vodoznaku 0 (černý obrazový prvek), nedochází k žádné změně, když bude aktuální hodnota obrazového prvku permutovaného vodoznaku 255 (bílý obrazový prvek), změníme pořadí bílých a černých prvků v dané masce (matici) tak, aby poměr černých a bílých bodů zůstal zachován. Popsaný přístup je jednoduchý i proto, že existuje několik druhů ditheringových masek, proto je např. možné pro hodnotu permutovaného vodoznaku 0 použít jeden typ masky a pro hodnotu permutovaného vodoznaku 255 použít jiný korespondující typ masky (např. obr.11). Jiným přístupen může být použití afinních transformací masky (pro hodnotu permutovaného vodoznaku 255), jakými jsou např. rotace masky ($o \pm 90^o$), horizontální, vertikální, nebo diagonální zrcadlení apod. – tento přístup ale vyžaduje použití vhodných typů masek (např. při použití rotace nesmí být maska rotačně invariantní, tj. otočením masky musí vzniknout odlišná maska ve smyslu distribuce černých a bílých obrazových bodů pro danou prahovací úroveň). Problémem použití afinních transformací, jako i záměny

ditheringové masky jsou krajní hodnoty prahovacích úrovní – celý blok bílý, nebo černý (vyznačují se rotační invariancí). Tuto skutečnost je možno eliminovat záměnou jednoho vhodného prvku masky na inverzní hodnotu – viz obr. 15. Změna prvku v masce je naznačena jiným odstínem.



Obr. 14: Princip vložení vodoznaku do pseudovíceúrovňového obrazu.



Obr. 15: Záměna masky pro vložení binárního vodoznaku.

K extrakci vodoznaku je obecně potřebná jen původní ditheringová maska a algoritmus obrazové permutace vodoznaku, jsou-li obrazové prvky pseudovíceúrovňového obrazu totožné s možnými případy prvků původní ditheringové masky, výstupem je černý obrazový prvek permutovaného vodoznaku, nejsou-li příslušné obrazové prvky totožné, výstupem je bílý obrazový prvek permutovaného vodoznaku. Aplikováním inverzní permutace obrazových prvků permutovaného vodoznaku získáme vodoznak, který byl do pseudovíceúrovňového obrazu vložen.

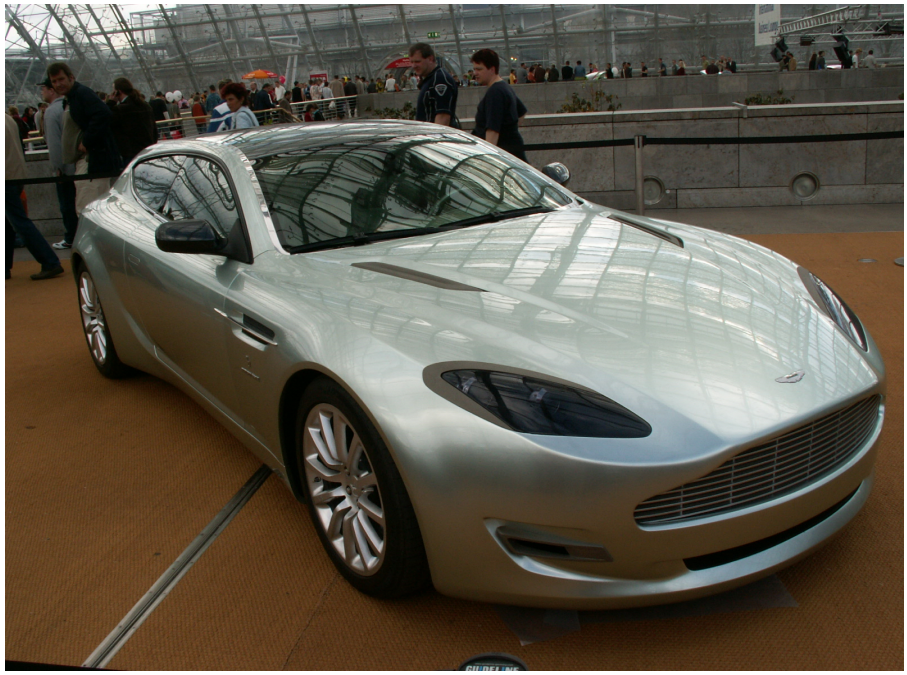
Použití vkládání digitálních vodoznaků do pseudovíceúrovňových obrazů nesplňuje požadavky robustnosti, tj. odolnosti vloženého vodoznaku vůči operacím s pseudovíceúrovňovými obrazy, proto je tato technika používána jako steganografická technika.

5 PRAKTICKÝ PŘÍKLAD

V této části diplomové práce předvedu praktickou ukázku rozložení statického víceúrovňového obrazu na bitové roviny, zakódování dat a prezentace výsledků včetně subjektivního hodnocení výsledků. Ještě před samotným příkladem je nutno podotknout, že pro faktickou realizaci jsem si vybral prostředí GNU Octave, což je kompatibilní free klon jinak známého prostředí MATLAB.

První podmínkou pro úspěšný pokus je vhodný „testovací objekt“, v našem případě tedy obraz o definovaném horizontálním a vertikálním rozlišení, v 8-bitové barevné hloubce, resp. ve 256ti odstínech šedi. Chceme-li tento obraz nějakým způsobem zpracovat, musíme zadat určitou posloupnost příkazů, které postupně provedou s naším obrazem dané operace. Tuto posloupnost příkazů je možné uložit do souboru, tzv. skriptu, a tento je možné spouštět dávkově přímo z daného prostředí Octave, popř. MATLAB.

Náš skript je vytvořen takovým způsobem, že umí zpracovat obraz o (v zásadě) libovolné velikosti. Je ovšem potřeba brát v úvahu paměťové a výkonové nároky na hardware při zpracování velkého obrazu, proto jsem pro tuto praktickou ukázku zvolil obraz poměrně malý, a to o velikosti 256x256 pixelů. Původní obraz dle mého výběru (obr. 16; soubor PICT0069.JPG) jsem pomocí grafického editoru (můžeme použít libovolný editor, který nám dokáže vyrobit obraz v námi požadovaném formátu) zmenšil na danou velikost a zkonvertoval na nižší barevnou hloubku (obr. 17; soubor car.bmp).



Obr. 16: Původní obraz před zpracováním.

Tím jsem si připravil vhodný testovací objekt (obraz s hodnými vlastnostmi):

Obr. 17: Obraz připravený pro rozklad na bitové roviny.

Ten nyní můžeme zpracovat pomocí našeho skriptu:

```
%nahrajeme originalni obrazek
[obr,cmap]=loadimage('C:\\PROGRAMS\\GNUOctave\\scripts\\car.bmp', 'bmp');

%zkonvertujeme hodnoty 0..255 (odstiny sedi) na radu 8mi bitovych hodnot
binarni = mdec2bin(obr,8); %65536x8, po sloupcich
```

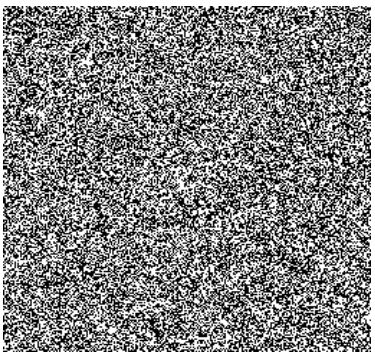
V těchto krocích jsme načetli připravený obraz do paměti. Odstíny šedi jsou definovány jako kombinace osmi bitů, tj. 2^8=256 jasových úrovní šedé. Celou matici obrazu jsme překonvertovali na matici binárních hodnot.

Následující částí algoritmu vytvoříme osm matic, každá bude obsahovat jednu složku obrazu, jednu bitovou rovinu:

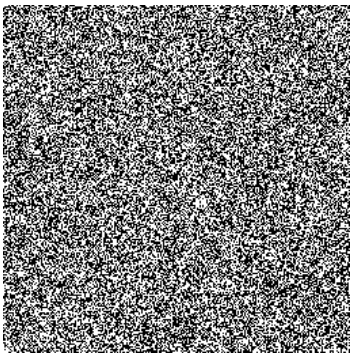
```
%rozlozime do 8mi bitovych rovin, kazdou do vlastniho pole
for m=1:256
for n=1:256
      %(8)10=(00000101)2 => prvni hladina (d0) je 8. pozice
      prvni(n,m)   = binarni(n+((m-1)*256),8); % konverze (65536x8)->
(256x256), hladina d0
      if prvni(n,m)==0                         % konverze znaku '0','1'
na cisla 0,255
                     prvni(n,m)=0;
         else
                     prvni(n,m)=255;
      end;
      druhy(n,m)  = binarni(n+((m-1)*256),7);
      if druhy(n,m)==0
                     druhy(n,m)=0;
         else
                     druhy(n,m)=255;
      end;
      treti(n,m)  = binarni(n+((m-1)*256),6);
      if treti(n,m)==0
                     treti(n,m)=0;
         else
                     treti(n,m)=255;
      end;
```

```
      ctvrty(n,m) = binarni(n+((m-1)*256),5);
      if ctvrty(n,m)==0
                     ctvrty(n,m)=0;
         else
                     ctvrty(n,m)=255;
      end;
      paty(n,m)  = binarni(n+((m-1)*256),4);
      if paty(n,m)==0
                     paty(n,m)=0;
         else
                     paty(n,m)=255;
      end;
      sesty(n,m) = binarni(n+((m-1)*256),3);
      if sesty(n,m)==0
                     sesty(n,m)=0;
         else
                     sesty(n,m)=255;
      end;
      sedmy(n,m) = binarni(n+((m-1)*256),2);
      if sedmy(n,m)==0
                     sedmy(n,m)=0;
         else
                     sedmy(n,m)=255;
      end;
      osmy(n,m)   = binarni(n+((m-1)*256),1);
      if osmy(n,m)==0
                     osmy(n,m)=0;
         else
                     osmy(n,m)=255;
      end;
 end
end
```

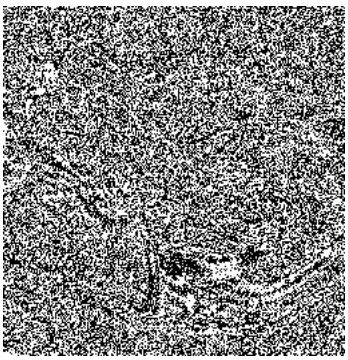
Takto získané bitové roviny jsem zároveň i uložil do nových souborů, námi zkoumaný obraz rozložený do osmi bitových rovin vypadá následovně:



Obr. 20: 1. bitová rovina.



Obr. 19: 2. bitová rovina.

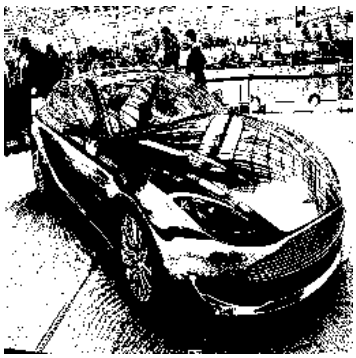


Obr. 18: 3. bitová rovina.

Obr. 21: 4. bitová rovina.

Obr. 22: 5. bitová rovina.

Obr. 23: 6. bitová rovina.



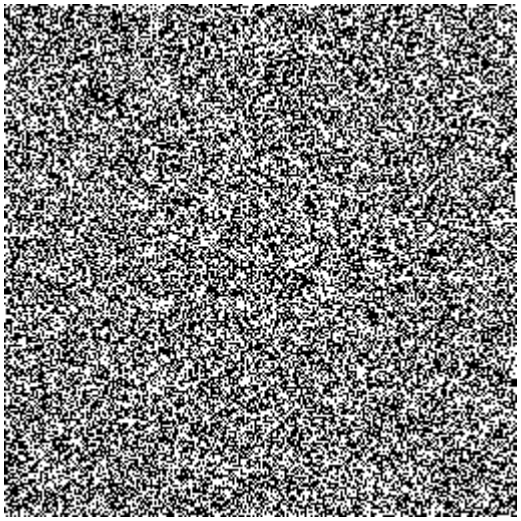
Obr. 24: 7. bitová rovina.

Obr. 25: 8. bitová rovina.

Teď potřebujeme vygenerovat naše nada, která se pokusíme zakódovat do bitových rovin. Pro tento účel můžeme využít funkcí, které nám vygenerují pseudonahodná data:

```
%vygenerujeme matici bitu, kterou budeme kodovat do obrazu
% matice ma rozmer (256:256)
% je pseudonahodna - pri stejne zadane hodnote "seed" vygeneruje vzdy
stejne "nahodnou" matici
a = 0;
b = 1;
rand("seed",10);
x=round(a+(b-a)*rand(256));
```

Námi vygenerovaná pseudonáhodná data vydapají následovně:

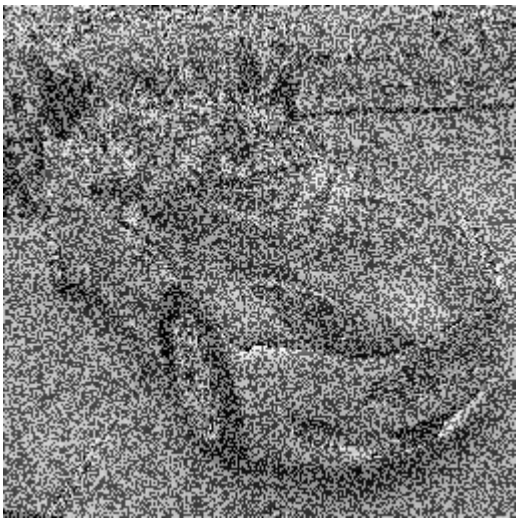


Obr. 26: Pseudnáhodná data.

Tato data zakódujeme to všech bitových rovin pomocí logocké funkce XOR (eXclusive OR):

```
%ted zakodujeme vygenerovanou matici dat do vybrane bitove roviny naseho
obrazu
% promenna bitrovina urcuje ktera bitova rova bude "prekodovana"
% data se koduji do bitove roviny pomoci fce XOR
bitrovina=1;
for b=1:256
 for a=1:256
  binarni( a+((b-1)*256),bitrovina )=xor( binarni( a+((b-1)*256),4 ),
x(a,b));
 end
end
```

Výsledné obrazy po zakódování dat do první (MSB), střední, a poslední (LSB) bitové roviny:



Obr. 28: Změna 1. bitové roviny.

Obr. 27: Změna 4. bitové roviny.

Obr. 30: Změna 8. bitové roviny.

Obr. 29: Původní obraz.

5.1 Hodnocení

Z obrázků je patrné, že výběr bitové roviny pro kódování dat je viditelný na první pohled. V zásadě se lze držet pravidla, že pokud modifikujeme tzv. LSB (Least Significant Bite), rozdíl mezi originálním obrazem a zpracovaným obrazem nelze normálním okem pozorovat. Naopak čím více se v modifikacích „blížíme“ prvnímu bitu (MSB – Most Significant Bit) o to více je na výsledném obrazu vidět sebemenší změna.

Co se týká kapacity přenosu dat – v tomto případě pro tento obraz – tak lze říci, že na každý pixel obrazu můžeme změnit (překódovat) jeden bit informace. Takový obraz má potom přenosovou kapacitu rovnu celkovému počtu pixelů.

5.2 Poznámky k provozu

Některé příkazy mezi systémy Octave a MATLAB nejsou co se týká syntaxe úplně vždy kompatibilní. Nicméně zpravidla vždy existuje za danou funkci funkce náhradní s podobnou syntaxí a podobnými vlastnostmi.

Ve skriptu pro tento příklad jsou cesty pro obrázky nastaveny absolutně, v plné délce. Dále jsou použity zdvojené zpětné lomítka „\\“ a to hlavně kvůli tomu, že Octave je původně vytvořen pro platformu UNIX/Linux a tím pádem používá specifické znaky. V případě potřeby je nutno tyto cesty změnit, popř. zkusit použít cesty relativní.

ZÁVĚR

Z dostupných zdrojů jsem zpracoval komplexní úvod do problematiky steganografie. Jelikož je dnes steganografie nedílnou součástí bezpečnosti a ochrany dat, hodnocení bezpečnostních rizik a řízení bezpečnosti, zabývám se v první části právě těmito obory.

Steganografické techniky používají lidé již od nepaměti, proto je tato problematika značně rozsáhlá. Proto když se v druhé kapitole podrobněji zabývám klasifikacemi steganografie, je patrné, že výčet daných technik není ani zdaleka konečný. Stále důmylsnější technické prostředky umožňují používat stále důmyslnější postupy nejen pro ochranu a utajování informací, ale také pro utajování samotného přenosu informací.

V dnešní době nám dává hlavně informatika velké pole působností pro efektivní použití steganografických technik. Jednou z mnoha disciplin je v informatice i digitální zpracování obrazu. Ve třetí a čtvrté kapitole se věnuji výčtu základních přástupů při digitálním zpracování obrazu včetně zákiladního popisu algoritmů a vybraných steganografických technik. Jsou zde také uvedeny základní vlastnosti těchto přístupů, jako robustnost a možná přenosová datová kapacita.

Na závěr jsem vybral jednu z výše uvedených steganografických metod, kterou jsem implementoval v prostředí Octave. Tento příklad jsem vybíral i podle toho, aby byl co nejjednodušší a tím nezabíhal zbytečně do podrobností co se týká informatiky. Přitom byl vybrán tak aby podával hmatatelné výsledky z oboru steganografie a zároveň byl i jednoduše modifikovatelný pro případné zájemce o aplikace tohoto oboru.

Steganografie je moderní přístup k ochraně dat a také k utajení přenosu dat, jehož význam dnes nabývá na významu právě dohromady s informačními systémy.

SEZNAM POUŽITÝCH ZDROJŮ

[1] BAHARAV, Z., SHAKED, D. Watermarking of dither halftoned images. *Hewlett-Packard Development Company, L.P. technical report.* 1999, Haifa, Israel, pp. 1–14,

[2] COX, I. J., MILLER, M. L. The first 50 years of electronic watermarking. *Journal of Applied Signal Processing*, 2002, 2, pp. 126-132.

[3] 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.

[4] COX, I. J., KALKER, T., PAKURA, G., SCHEEL, M. Information Transmission and Steganography In: *Proc. of the Int. Workshop on Digital Watermarking* (IWDW), Sept, 2005.

[5] CURRAN, K., BAILEY, K. An Evaluation of Image Based Steganography Methods. *International Journal of Digital Evidence* (IJDE) Vol. 2, No. 2, November 2003, Economic Crime Institute, 2003.

[6] ČANDÍK, M. Základy informační bezpečnosti. Zlín: UTB-Academia centrum, 2004, 107s.

[7] ČANDÍK, M. Význam simulácií útokov na systémy digitálnej vodotlače. *Krízový manažment* 1/2005, str. 15-19.

[8] ČANDÍK, M., MATÚŠ, E., LEVICKÝ, D. Digital Watermarking in Wavelet Transform Domain. *Radioengineering*, Vol. 10, No. 2, 2001, pp. 1-4.

[9] ČANDÍK, M., LEVICKÝ, D., KLENOVIČOVÁ, Z. Fractal image coding with digital watermarks. *Radioengineering*, Vol. 9, No. 4, 2000, pp. 22-26.

[10] ČANDÍK, M. Digital Watermarking using Karhunen-Loève Transform. *Jemná mechanika a optika*, č. 5/2003, roč. 48, str. 135-137.

[11] ČANDÍK, M. Digitální vodotisk založen na rozkladu obrazu do bitových rovin. *Jemná mechanika a optika*, č. 4/2004, roč. 49, str. 121-123.

[12] ČANDÍK, M., KRÁL, P. Some properties of digital image watermarking based on discrete cosine transform. *Jemná mechanika a optika*, č. 7-8/2004, roč. 49, str. 218-222.

[13] ČANDÍK, M.: *Metódy číslicovej vodotlače vo fraktálovom kódovaní obrazov.* In: Zborník z vedeckej konferencie Informatika a algoritmy `2000, Fakulta výrobných technológií Prešov, Prešov, 2000, str.159-161.

[14] ČANDÍK, M.: *Možnosti využitia Karhunenovej–Loèveovej transformácie pre vkladanie číslicových vodoznakov.* In: Zborník z vedeckej konferencie Informatika a

algoritmy `2002, Fakulta výrobných technológií Prešov & Slovenská spoločnosť pre kybernetiku a informatiku INFORMATECH Košice, Prešov, 2002, str. 99-102.

[15] ČANDÍK, M.: *Digitální halftoning obrazů v steganografické komunikaci*. In: Ochrana osôb a majetku 2003, III. vedecká konferencia s medzinárodnou účasťou, Košice, Multiprint Košice, str. 24-28.

[16] ČANDÍK, M. : *Bezpečnost informačních systémů jako nový trend edukace informatiky.* In: Sborník příspěvků z mezinárodní konference Trendy technického vzdělávání 2005, Olomouc, 2005, str.274-276.

[17] ČANDÍK, M. *Digitální vodotisk jako moderní fenomén datové bezpečnosti*. In: Sborník přednášek 28. mezinárodní konference TD 2005 – DIAGON 2005. Zlín (26.4.2005), Vyd. UTB-Academia centrum Zlín, 2004, str.107-110.

[18] DAVERN, P., SCOTT, M. Fractal Based Image Steganography. In: *Proc. of the First International Workshop on Information Hiding*, p.279-294, May 30-June 01, 1996.

[19] GONZALEZ, R.C., WINTZ, P. P. Digital Image Processing. New York: Addison-Wesley publishing Company, 1987.

[20] HAVLÍČEK, Z. Internetové technologie I. Praha: Reprografické studio PEF ČZU, 2003. 193s.

[21] JAIN, A. K. Fundamentals of Digital Image Processing. London: Prentice - Hall, 1989.

[22] JOHNSON, N. F., JAJODIA, S. Steganalysis: The Investigation of Hidden Information. In: *Proc. of the 1998 IEEE Information Technology Conference*, Syracuse, 1.-3.9. 1998, New York, USA, pp. 1-4.

[23] JOHNSON, N. F., JAJODIA, S. Steganalysis of Images Created Using Current Steganography Software. In: Proc. of the 2nd Information Hiding Workshop, Portland, Oregon, USA (15.-17.4.), 1998.

[24] KESSLER, G. C. Steganography: Hiding Data Within Data. *Windows & .NET Magazine* (April 2002).

[25] KLÍMA, M., BERNAS, M., HOZMAN, J., DVOŘÁK, P.Zpracování obrazové informace. Praha: ČVUT, 1996.

[26] KOTULIAKOVÁ, J., ROZINAJ, G. Číslicové spracovanie signálov I. Bratislava: FABER, 1996.

[27] KUNDUR, D., HATZINAKOS, D. A robust digital image watermarking scheme using the wavelet based fusion. In: Proc. of the IEEE International Conference on Image Processing ICIP´97, vol.1, pp. 544-547, Santa Barbara, USA, 1997.

[28] MIHALÍK, J. Číslicové spracovanie signálov. Bratislava: Alfa, 1987.

[29] MOHANTY, S. P. Digital Watermarking : A Tutorial Review. Report, Dept. of Electrical Engineering, Indian Institute of Science, Bangalore, India, 1999.

[30] PAQUET, A. H., WARD, R. K. Wavelet-based Digital Watermarking for Image Authentication. In: *IEEE Canadian Conference on Electrical and Computer Engineering*, Vol. I, Winnipeg, Manitoba, May 2002, pp. 879-884.

[31] PETITKOLAS, F. A. P., ANDERSON, R. J., KUHN, M. G. Information Hiding – A Survey. *Proceedings of the IEEE*, special issue on protection of multimedia content, July 1999, vol. 87, pp. 1062 - 1078.

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

[33] POLEC, J., PAVLOVIČOVÁ, J., ORAVEC, M.: Vybrané metódy kompresie dát. Bratislava: FABER, 1996.

[34] PROVOS, N., HONEYMAN, P. Hide and Seek: An Introduction to Steganography. *IEEE Security & Privacy*, May/June 2003, pp. 32-44.

[35] PŘIBYL, J. Informační bezpečnost a utajování zpráv. Praha: ČVUT, 2004. 239s.

[36] PŘIBYL, J., KODL, J. Ochrana dat v informatice. Praha:ČVUT, 1996. 299s.

[37] PUATE, J., JORDAN, F. Using fractal compression scheme to embed a digital signature into an image. In: *Proc. of the SPIE Video Techniques and Software for Full-Service Networks* (Tzicker Chiueh & Andrew G. Tescher eds.), vol. 2915, pp.108 – 118. SPIE, 1997.

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

ICT (Information and Communication Technologies) - informační a komunikační technologie

CD (Compact Disc) – datové záznamové médium

DVD (Digital Versatile/Video Disc) - datové záznamové médium

denial of service (DoS) - odepření služby

IT - informační technologie, informatika

IS - informační systém(y)

copyright marking - označování autorských práv

fragile watermarking - křehký vodotisk

robust watermarking - robustní vodotisk

dynamic watermarking - dynamický vodotisk

bitstream watermarks - proudové vodoznaky

fragile watermarks - křehké vodoznaky

fingerprinting - technika identifikačních vodoznaků

MSE (Mean Square Error) - střední kvadratická chyba

SNR (Signal to Noise Ratio) - poměr signál/šum

pixel (picture element) - jednotkový obrazový prvek; obrazový bod

DPI (dots per inch) - rozlišovací schopnost udávaná počtem pixelů na jednotku délky

MSB (Most Significant Bit) - nejvíce důležitý bit

LSB (Least Significant Bit) - nejméně důležitý bit

XOR (eXclusive OR) - logická funkce

SEZNAM OBRÁZKŮ