

Systémy digitálního vodotisku

Digital Watermarking Systems

Simona PEJSAROVÁ

Česká zemědělská univerzita v Praze, Provozně ekonomická fakulta

Katedra informačních technologií

Kamýcká 129, Praha 6, Česká republika

E-mail: pejsarova@pef.czu.cz

Anotace

Systémy digitálního vodotisku představují speciální steganografickou techniku. Digitální vodotisk splňuje navíc ve srovnání se steganografií požadavek robustní komunikace. Metody digitálního vodotisku se využívají v utajené komunikaci, nebo jako důkaz vlastnictví (copyright).

Klíčová slova

Digitální vodotisk, vodoznak.

Abstract

Digital watermarking systems are one special part of steganography techniques. Digital watermarking satisfies in comparing with steganography furthermore requirements of robust communication. Digital watermarking methods are successfully used in hidden communication or in copyright data protection.

Key words

Digital watermarking, watermark.

Úvod

První zmínkou o použití ručně dělaných papírových vodoznaků jsou více než 700 let staré - nejstarší dokument s papírovým vodoznakem pochází z města Fabriano v Itálii z roku 1292 a sehrál významnou úlohu ve vývoji papírenského průmyslu. V dnešní době je možné se potkat s papírovými vodoznaky na různých úředních dokumentech, ale asi mezi nejběžnější patří jejich používání na bankovkách. Tyto vodoznaky inspirovali odborníky k používání vodoznaků také v souvislosti s digitálními daty. Forma vodoznaků (watermark) může být vzhledem k multimediálnímu charakteru dat různá - vodoznak může mít charakter textu, souboru čísel, audio signálu, binárního nebo víceúrovňového obrazu.

Steganografie a technika vodoznaků vzájemně velice úzce souvisí. Obě techniky popisují způsoby subjektivně nevnímatelného přenosu informace pomocí její vložení do krycích dat. Zatím co 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. Protože cílem steganografie je ukrytí skutečnosti, že tajná komunikace existuje, nekladou se na ni vysoké nároky na odolnost. Technika vodoznaků předpokládá velké množství příjemců a mezi nimi i takových

přijímatelů, kteří se snaží vloženou informaci odstranit nebo poškodit. Proto techniky vodoznaků kladou vyšší požadavky na odolnost vůči útokům nepovolaných osob. Poznamenejme, že vodoznakové techniky je možné využívat i jako technické steganografické techniky.

Cíl a metodika

Cílem práce je prezentace některých vlastností systémů digitálního vodoťisku s důrazem na digitální obrazová krycí data, přičemž vkládanou informací je digitální binární obraz.

Uvedené algoritmus slouží jako referenční (standardní) algoritmus pro komparaci dílčích výsledků v rozpracované výzkumné činnosti.

Základní vodoznakové techniky

Systémy digitálního vodoťisku je možné rozdělit z několika hledisek. Z hlediska postřehnutelnosti vodoťnaku se rozlišuje

- **Postřehnutelný vodoťisk** (perceptible) – data jsou označeny viditelným vodoťnakiem, kterým bývá nejčastěji logo společnosti. Používá se kvůli zamezení komerčních aktivit veřejně přístupných dat.
- **Nepostřehnutelný vodoťisk** (imperceptible) – data jsou označeny vizuálně nepostřehnutelným vodoťnakiem, vodoťnak se dá detekovat nebo extrahovat použitím speciálních procedur s označenými daty.

Z hlediska odolnosti (resp. citlivosti) rozlišujeme

- **Křehký vodoťisk** (fragile) – je analogií hašovacích funkcí používaných v digitálních podpisech. Cílem křehkých vodoťnaků je detekovat manipulaci s daty, tj. jakákoli modifikace dat musí způsobit změnu vodoťnaku.
- **Robustní vodoťisk** (robust) – vložený vodoťnak musí odolávat manipulacím s daty, do kterých je vložen. Robustní vodoťisk je vhodný na deklarování vlastnictví [2].

Z hlediska možnosti uživatelů detekovat, resp. extrahovat vodoťnak rozlišujeme

- **Veřejný vodoťisk** (public) – ve kterých detekce, resp. extrakce vodoťnaku je možná kterémukoli uživateli označených dat
- **Soukromý vodoťisk** (private) ve kterých uživatelé označených dat nejsou autorizováni k detekci, resp. extrakci vodoťnaku.

Z hlediska použití algoritmů pro detekci, resp. extrakci vodoťnaku rozlišujeme

- **Asymetrický vodoťisk** (asymmetric) – používá k extrakci vodoťnaku odlišný klíč, než jaký byl použitý při vkládání vodoťnaku.
- **Symetrický vodoťisk** (symmetric) – používá k extrakci vodoťnaku stejný klíč, jaký byl použitý při vkládání vodoťnaku.

Podle typu krycích dat, tj. dat, do kterých se vodoťnaky vkládají, rozlišujeme

- **textový vodoťisk** (text watermarking) – krycí představují textové data.
- **zvukový vodoťisk** (audio watermarking) – krycí představují zvukové data.
- **obrazový vodoťisk** (image watermarking) – krycí představují obrazové data, resp. obrazové sekvence.

Podle toho, jakým způsobem dochází k vložení vodoťnaku, rozlišujeme

- **vodoťiskové systémy využívající prostorový popis krycího signálu** (spatial domain watermarking) – kde pro vložení vodoťnaků slouží časová oblast (u audio signálů) resp. obrazová oblast u obrazových signálů.

- **vodotiskové systémy využívající frekvenční popis krycího signálu** (frequency domain watermarking) - kde pro vložení vodoznaku slouží frekvenční spektrum signálů (vodoznakem se modifikují vybrané spektrální koeficienty), resp. sekvenční spektrum signálů využívající diskretní ortogonální transformace (DCT, DWT), příp. hybridní transformace (Fourier-Mellinova transformace).
- **vodotiskové systémy využívající parametrický popis krycího signálu** (parametric domain watermarking) - kde pro vložení vodoznaku slouží parametrická oblast signálů. Příkladem této techniky je použití vodoznaků ve fraktálovém kódování obrazů, kde vodoznak modifikuje některé parametry fraktálového kódu obrazu.

Existují dva způsoby označení dat vodoznakem, které je možné vzájemně rozlišit v procesu extrakce vodoznaku, a to systémy:

- **vyžadující originální data** – které implementují do originálních dat vodoznak, a označená data jsou určena k distribuci. Autor si ponechává neoznačený originál. V případě potřeby důkazu autorských práv distribuované kopie se tato kopie porovná s originálními daty. Úspěšná extrakce vodoznaku v takovém případě slouží jako důkaz autorských práv.
- **nevyžadující originální data** – umožňují extrahovat vodoznak přímo z označených dat. Tyto algoritmy se vyznačují větší výpočetní složitostí a větší dobou extrakce vodoznaku. Některé algoritmy, které pro extrakci vodoznaku původní data vyžadují, je možné modifikovat i na algoritmy bez potřeby neoznačených dat pro extrakci vodoznaku.

Principy vkládání digitálního vodoznaku

Obecně lze techniky vkládání a extrakce digitálního vodoznaku popsat pomocí jednoduchých matematických funkcí, jak to naznačují relace (1) a (2).

Vložení vodoznaku lze matematicky popsat relací (1)

$$WOI = OI + W \quad (1)$$

kde

WOI představuje obraz s vloženým vodoznakem,

OI představuje originální obraz

W vodoznak

tj. obraz s vodoznakem je součet originálního obrazu a vodoznaku.

Pro výběr vodoznaku platí vztah (2):

$$W' = WOI - OI \quad (2)$$

kde

W' představuje extrahovaný vodoznak (Obecně $W' \neq W$ v případě silných ztrátových útoků na obraz s vloženým vodoznakem WOI.)

WOI představuje obraz s vloženým vodoznakem

OI představuje originální obraz tj. extrahovaný vodoznak je rozdíl obrazu s vodoznakem a originálního obrazu

Rozdělení vodoznakových technik pro obrazová krycí data

Digitální vodotisk dělíme podle typu použitého přístupu pro vkládání. V případě, kdy data, do kterých se vkládá vodoznak (tzv. krycí data), představují digitální obraz, rozlišují se vodoznakové techniky na základě toho, jak je do krycích obrazových dat vodoznak vkládán.

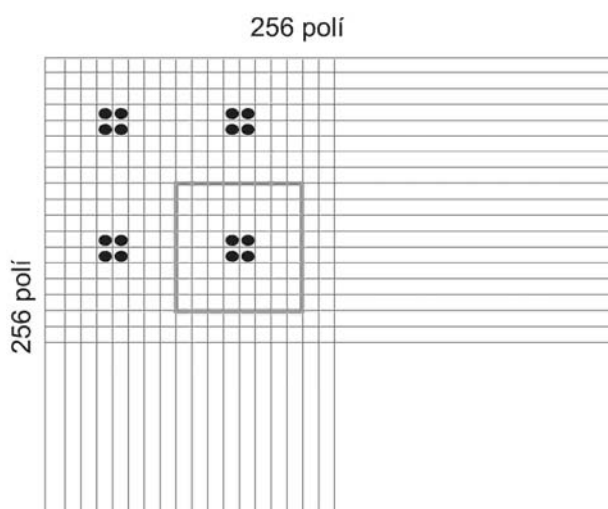
Vodoznaky se v případě obrazových krycích dat vkládají v:

1. Jasové oblasti obrazu,
2. V transformované oblasti obrazu,
3. V parametrické oblasti obrazu.

Vodoznaky vkládané v jasové oblasti

Slouží k označení, popřípadě k úmyslné degradaci obrazu – použití při ochraně autorských práv. Obraz je pozměněn jen z části, nebo úplně. Musíme vlastnit konkrétní vodoznak a znát metody vložení viditelného vodoznaku, abychom byli schopni rekonstruovat degradovaný obraz zpět do jeho původní podoby.

Jedná se o nejjednodušší metodu vkládání vodoznaku, v podstatě se ale využívá pouze při vkládání viditelných vodoznaků. Může ale posloužit jako základní schéma vkládání vodoznaku do obrazu. Mějme originální obraz OI o rozměrech $n \times n$, dále mějme vodoznak W o rozměrech $m \times m$, kde např. $m = n/4$; všeobecně je však jen nutné, aby $m \ll n$. Další nutná podmínka je aby počet barev W byl menší než počet barev OI . Rozdílný počet pixelů se projeví při vkládání vodoznaku, a to tak, že budeme měnit jen některé hodnoty v OI . Následující příklad platí pro $OI[256 \times 256]$ -256 odstínů šedi, $W[64 \times 64]$ -jednobitová barevná hloubka (Obr.1).



Obrázek č. 1: Modifikace hodnot originálního obrazu podle

- Tečky jsou pole, která budou měněna podle vztahu:

$$WOI = OI + k * W \quad (3)$$

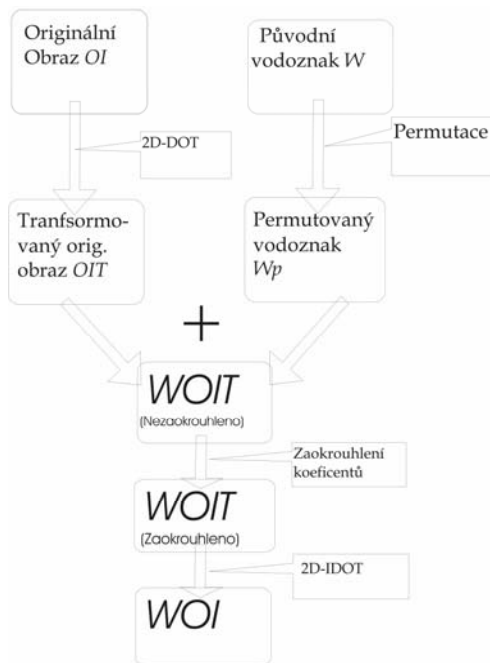
kde WOI je obraz s vodoznakem, k je koeficient, kterým se násobí hodnota ve vodoznaku a W představuje hodnotu konkrétního bodu ve vodoznaku (0 nebo 1).

Vodoznaky vkládané v transformované oblasti

Transformovaná oblast obrazových dat představuje jiný popis obrazových dat pomocí tzv. diskretních ortogonálních transformací. Ortogonální transformace umožňují reprezentovat

časové průběhy signálů ve formě jejich zobecněného spektra. V spektrální oblasti se pak realizují potřebné operace, které zajišťují např. rychlejší vyhodnocení signálů, atd. Některé operace se snadněji realizují v spektrální oblasti, jako v časové oblasti. Diskrétní ortogonální transformace nacházejí široké uplatnění v kompresi dat, rozpoznávání obrazů a jejich analýze, a pod. Jednou z běžných aplikací diskrétních ortogonálních transformací jsou právě vodotiskové techniky. Při těchto postupech se vodoznakem modifikují hodnoty transformačních (frekvenčních, či sekvenčních) koeficientů. Tyto metody jsou náročnější, ale tím také mnohem odolnější před možným odhalením.

Vklad vodoznaku



Obrázek č. 2: Vkládání vodoznaku v transformované oblasti obrazu

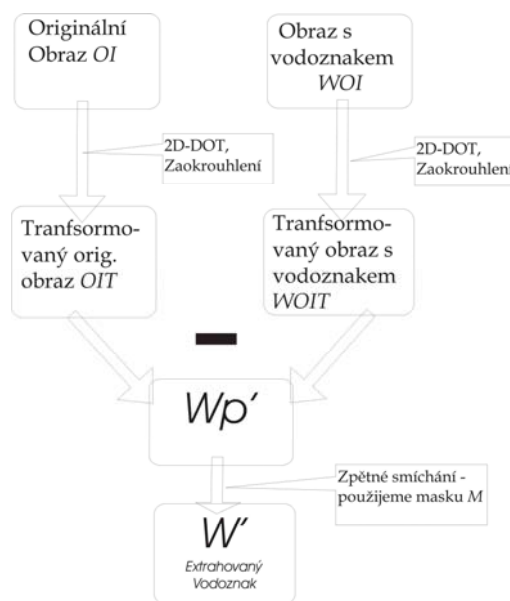
$WOIT$ = Transformovaný originální obraz s vodoznakem.

WOI = obraz s vodoznakem⁸⁶

Postup:

1. Transformace OI , vznikne OIT
2. Přeuspořádání obrazových prvků vodoznaku (Permutace) W , vznikne Wp
3. Vložení permutovaného vodoznaku do krycích dat: $Wp + OIT$, vznikne $WOIT$
4. Výpočet inverzní (diskrétní ortogonální) transformace.

Výběr vodoznaku



Obrázek č. 3: Extrakce vodoznaku v transformované oblasti

Postup:

1. Transformace OI a WOI , vznikne OIT , resp. $WOIT$.
2. Rozdíl frekvenčních spekter obou obrazů je permutovaný vodoznak – děleno konstantou robustnosti.

$$Wp' = (OIT - WOIT) / k \quad (4)$$

3. Na základě klíče (masky M) realizujeme inverzní permutaci (použitá permutace má být tzv. pseudonáhodná, t.j. náhodné generování v procesu extrakce je stejné, jako v procesu vkládání vodoznaku.) a tak dostaneme extrahovaný vodoznak:

$$W' = \text{Repermutace}(Wp') \quad (5)$$

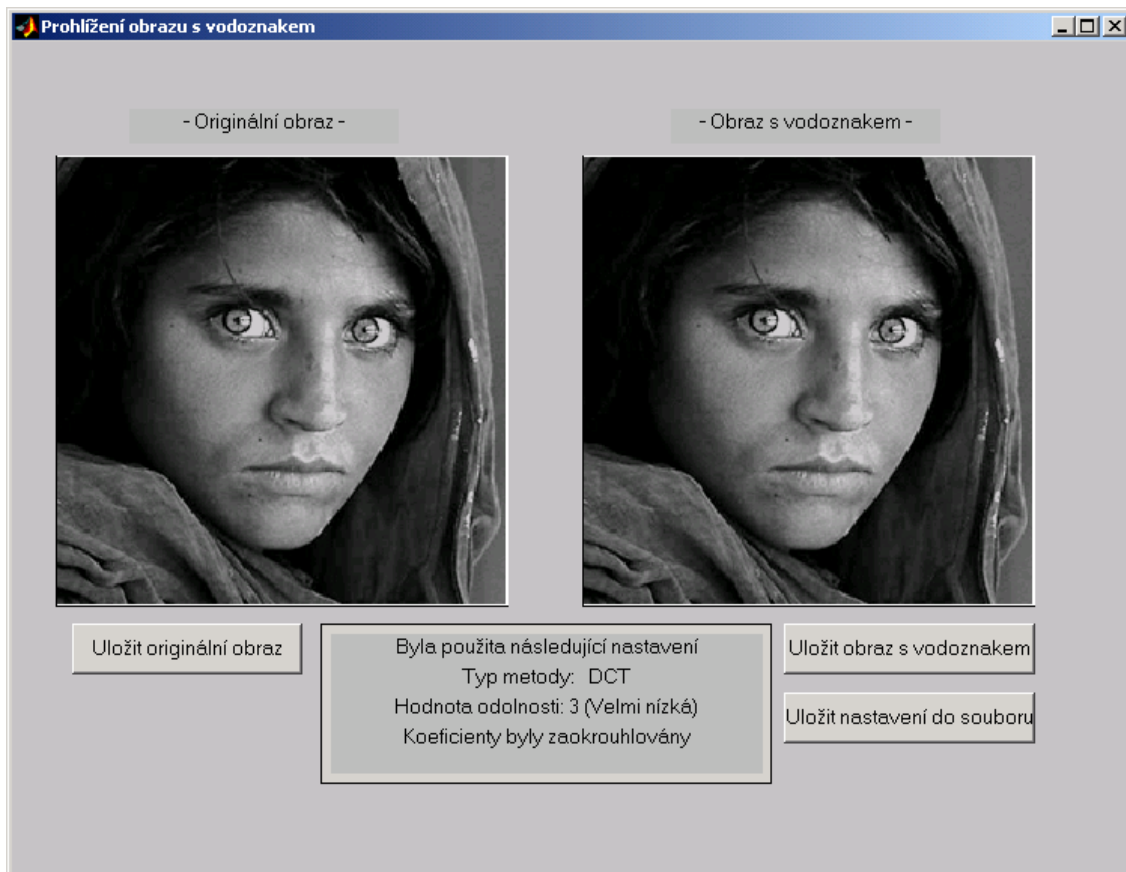
Vodoznaky vkládané v parametrické oblasti

Vodoznaky vkládané v parametrické, neboli systémové oblasti, modifikují tzv. parametrický prostor obrazu, t.j. příznaky (metadata), které slouží k jeho zobrazení. Příkladem vkládání vodoznaků do parametrického prostoru je fraktálový popis obrazu, ve kterém mohou být modifikovány např. parametry pro transformaci kontrastu a jasu.

Jiným příkladem modifikace parametrického prostoru obrazu je např. úprava matice palety u direct color RGB.

Výsledky

Pro naši simulace jsme využili statický víceurovňový obraz Shrabat v pgm (portable gray map) formátu s jasovou rozlišovací schopností 8bitů/pixel a prostorovou rozlišovací schopností 256x256. Vkládané vodoznaky byly statické binární obrazy s prostorovou rozlišovací schopností 64x64. Pro vložení vodoznaku byla použita dvourozměrná diskretní kosinová transformace (2DDCT). Obr. 4 ukazuje vizuální nepostřehnutelnost vložené informace (imperceptibilitu algoritmu).



Obrázek č. 4: Porovnání originálního (krycího) obrazu a obrazu s vodoznakem

Změny nejsou prakticky pozorovatelné, lze je ale zvýraznit například tím způsobem, že obrazové body (pixely), které se v jasové oblasti od originálu liší více jak o 1 jasovou hodnotu budou změněny na bílou barvu (obr.5).



Obrázek č. 5: Zvýrazněné rozdíly mezi krycím obrazem *OI* a obrazem s vodoznakem *WOI*

Závěr

Metody utajení komunikace patří mezi zajímavá odvětví digitálního zpracování obrazové informace. V průběhu posledních deseti let bylo v této oblasti vyvinuto velké množství sofistikovaných přístupů. Jednou z prvních a nejsnadnějších steganografických metod, které slouží také k zabezpečení obrazové informace je digitální vodotisk.

Příspěvek prezentuje některé vlastnosti systémů digitálního vodotisku s důrazem na digitální obrazová krycí data, přičemž vkládanou informací byl digitální binární obraz. Uvedený algoritmus slouží jako referenční (standardní) algoritmus pro komparaci dílčích výsledků v rozpracované výzkumné činnosti.

Literatura

- [1] 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.
- [2] LUKÁČ, R., ČANDÍK, M. The Influence of Noise Corruption to Image Watermarking in DCT Domain. *Journal of Electrical Engineering*, No.3-4, Vol.52, 2001, pp. 81-87.
- [3] PODILCHUK, CH. I., DELP, E.J. Digital Watermarking: Algorithms and Applications. *IEEE Signal Processing Magazine*. July, 2001. pp. 33-46.
- [4] ČANDÍK, M. *Bezpečnost informačních systémů, steganografia a digitální vodotlač*. Ostrava: OFTIS, 2005, ISBN 80-239-5962-X.
- [5] HSU, CH. T., WU, J. L.: Hidden Digital Watermarks in Images, *IEEE trans. On Image Processing*. Vol.8, No.1, 1999, pp.58-68.