ZÁPADOČESKÁ UNIVERZITA V PLZNI
FAKULTA ELEKTROTECHNICKÁ

KATEDRA APLIKOVANÉ ELEKTRONIKY A TELEKOMUNIKACÍ

BAKALÁŘSKÁ PRÁCE

Digitální zabezpečení datových souborů a jejich správa

Tomáš Charvát **2013**

Originál (kopie) zadání BP/DP

Abstrakt

Předkládaná bakalářská práce se zabývá ochranou digitálních dat a určení jejich autorství. Popisuje současné metody využívané k ochraně digitálních souborů. Věnuje se digitálním vodoznakům, jejich funkci a aplikaci v různých typech datových souborů. Dále tato práce vysvětluje princip digitálního podpisu, jeho vytvoření a ověření pravosti. Část práce je určena metadatům a zabezpečení u speciálních typů datových souborů, jako je PDF či soubory kancelářského balíku MS Office. V další části bakalářské práce jsou porovnávány možnosti zabezpečení jednotlivých typů datových souborů. Nalézají se zde také možná doporučení k využití vybraných metod v univerzitním prostředí.

Klíčová slova

Certifikát, datový soubor, digitální podpis, digitální vodoznak, digitální zabezpečení, metadata, soukromý klíč, steganografie, veřejný klíč.

Abstract

Submitted bachelor's thesis deals with protection of digital data and determination of their authorship. It describes present methods, which are used to protection of digital files. It pursues to digital watermarks, their function and application in different types of data files. This thesis explains the principle of digital signature, its creation and verification. The part of thesis is dedicated to metadata and security at special types of data files like PDF or files from MS Office. In the next part of thesis, the options of security of different types of data files are compared. Also there are possible recommendations to using of selected methods at university.

Key words

Certificate, data file, digital security, digital signature, digital watermarking, metadata, private key, public key, steganography.

Prohlášení

Prohlašuji, že jsem tuto diplomovou/bakalářskou práci vypracoval samostatně, s použitím odborné literatury a pramenů uvedených v seznamu, který je součástí této diplomové práce.

Dále prohlašuji, že veškerý software, použitý při řešení této bakalářské/diplomové práce, je legální.

.....

podpis

V Plzni dne 5.6.2013 Tomáš Charvát

Obsah

Seznam symbolů a zkratek

AES ..... Šifrovací standard pro hesla

BMP, GIF, TGA ..... Grafické formáty pro ukládání rastrové grafiky

DRM ..... Digitální zabezpečení datových souborů (Digital Rights Management)

EAD ..... Kódovaný archivní podpis (The Encoded Archival Description)

IRM ..... Spravování přístupových práv u MS Office

JPG ..... Grafický formát pro ukládání ztrátové (fotorealistické) kvality

LSB ..... Nejméně významný bit (Least Significant Bit)

MSB ..... Nejvíce významný bit (Most Significant Bit)

PDF ..... Přenosný formát dokumentů (Portable Document Format)

RGB ..... Barevný model pro displeje schopný zobrazit jakoukoliv barvu pomocí červené, zelené a modré (Red, Green, Blue)

RMS ..... Správa přístupových práv v operačním systému Windows

SK ..... Soukromý klíč

VK ..... Veřejný klíč

XML ..... Rozšiřitelný značkovací jazyk (Extensible Markup Language)

fps ..... Snímková frekvence (frames per second)

pixel ..... Nejmenší obrazový prvek (picture element)

Úvod

V minulosti se významné dokumenty a umělecká díla chránily trezory a nejrůznějšími zabezpečovacími systémy. S nástupem a expanzí informačních technologií začaly takovéto dokumenty a díla vznikat i v elektronické podobě. Uložené ve formě souborů je mohl kdokoliv upravit a vydávat za své a jejich identické kopie mohly v nesčetném množství kolovat mezi uživateli. Zabezpečit jejich obsah nebo dokázat jejich autora bylo stejně důležité jako u jejich hmotných předchůdců. Začaly tedy vznikat metody, jejichž aplikací na daný soubor se zvýšila jeho ochrana. Tyto metody se souhrnně nazývají digitální zabezpečení datových souborů, zkráceně DRM, a právě jimi se tento dokument zabývá.

Práce se skládá ze dvou částí. První část obsahuje rešerši využívaných metod pro aplikaci DRM do souborů. Popisuje funkci těchto metod, jejich aplikaci a ve vybraných případech i ukázky jejich použití. Dále se věnuje zabezpečení u často využívaných datových souborů.

V druhé části této práce se nalézá porovnání možností zabezpečení jednotlivých typů datových souborů. Tato část také obsahuje příklady možného využití DRM v univerzitním prostředí, které vycházejí z předešlé rešerše.

Tuto práci jsem si vybral, protože mě dané téma zajímá. V minulosti jsem se problematikou zabezpečení datových souborů již zabýval a navíc je v poslední době toto téma hodně diskutováno, a to spíše v negativním smyslu jako nástroj pro omezování uživatelů. Proto bych si přál, aby tato práce sloužila jako objektivní pohled na problematiku DRM, odůvodnila jeho vnik a nastínila jeho další vývoj.

1 Digitální vodoznaky

V dnešní době se již běžně setkáváme se začleněním těchto vodoznaků do digitálních souborů. Z historického pohledu na věc tuto úpravu digitálních souborů provádíme z odlišných důvodů. Zprvu klasické vodoznaky sloužily k odlišení jednotlivých papírů z různých dílen, aby se dal snadno identifikovat původ papíru. Později se tato technika začala objevovat na poštovních známkách a následně na platidlech a speciálních listinách jako identifikační prvek.[1] Takovéto vodoznaky vznikaly a dále vznikají zeslabováním a zesilováním papírové hmoty v mokré fázi tvorby papíru.[2]

Běžné vodoznaky se snaží zabraňovat padělání, kdežto soubor, obohacený digitálním vodoznakem, může mít mnoho identických kopií. Hlavním úkolem digitálního vodoznaku je určit autora díla, tedy zabránit plagiátorství určením autorských práv.[3] V dnešní době se k takovýmto kopiím může dostat prakticky kdokoliv díky rozmachu BitTorrentů a nesčetných úložných serverů. Nejčastěji se jedná o textové, hudební, video a grafické soubory. Stahování těchto souborů poškozuje autora v podobě ušlého zisku. Vodoznaky zde mají za úkol skrýt autorská práva a sériová čísla (tzv. fingerprinting) do souborů, díky nimž se mohou následně vysledovat úniky dat z projektů a následně stíhat a identifikovat narušitele autorských práv.[4]

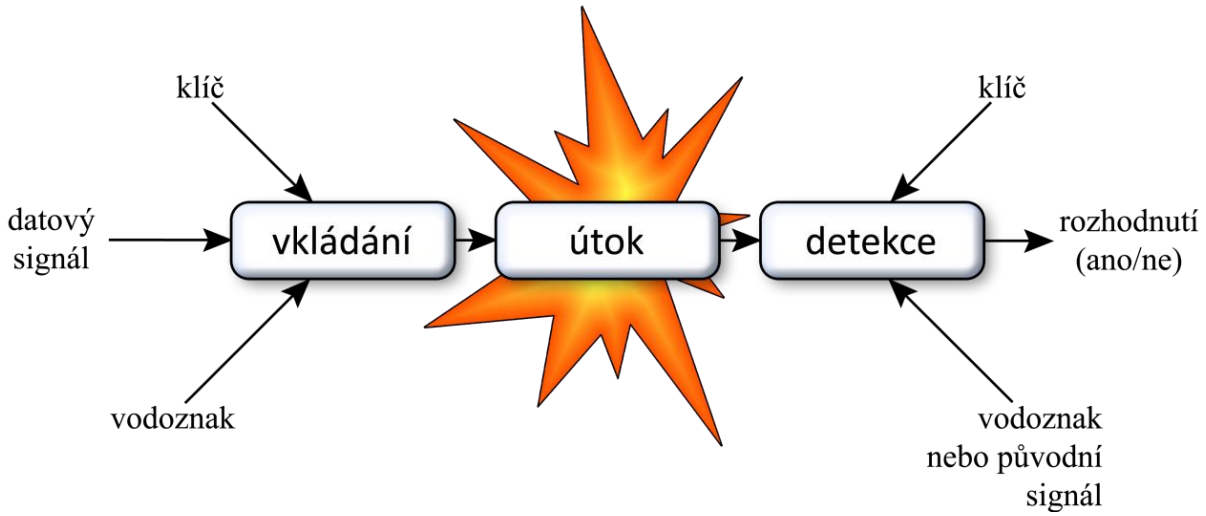
Pro ideální digitální vodoznak jsou charakteristická tato kritéria:

- Nenápadný na to, aby nesnižoval kvalitu souboru a zároveň aby zůstal skrytý před útočníkem,
- snadno zjistitelný pro majitele nebo kontrolní orgán,
- jednoznačný pro určení vlastníka údajů,
- nesčetný pro generování velkého množství rozlišitelných vodoznaků,
- robustný, přežije všechny útoky na soubor,
- pokud soubor obsahuje více vodoznaků, tyto vodoznaky se vzájemně nenarušují.[2]

Ideální vodoznak prakticky neexistuje, daný vodoznak vždy minimálně jednomu kritériu nevyhovuje. Podle jejich odolnosti je proto třídíme na slabé a silné (robustné). Slabý vodoznak se poruší i při minimální úpravě a díky tomu může například sloužit jako elektronický důkazní prostředek. Silný vodoznak zůstane patrný i po běžných operacích se souborem a zároveň jej nelze odstranit bez toho, aby nebyl porušen označený soubor.[4]

Tím se dostáváme k definici digitálního vodoznaku. Digitální vodoznak je digitální signál nebo vzor vložený do digitálního dokumentu a nese informace jedinečné pro vlastníka autorských práv, tvůrce dokumentu či jeho spotřebitele.[2]

Životní cyklus digitálního vodoznaku dělíme do tří fází; vkládání, útoku a detekce. Při fázi vkládání se k signálu datového dokumentu přidá za pomoci klíče signál vodoznaku. Ve fázi útoku se signál opatřený vodoznakem přenáší na jiné osoby nebo je uložen. Jako útok se bere libovolná modifikace např. ztrátová komprese, převod formátu, ořez či zvětšování šumu. Při detekci využíváme algoritmus, který se za pomoci klíče snaží dostat z atakovaného signálu původní signál vodoznaku. Ze signálu, který prošel fází útoku a nebyl modifikován, detekujeme původní vodoznak. Pokud proběhla modifikace, původní vodoznak se vytratí nebo byl-li vodoznak robustný, detekční algoritmus jej rozpozná a zrekonstruuje.[5] *Obr. 1.1* znázorňuje celý cyklus života digitálního vodoznaku.



Obr. 1.1 Cyklus života vodoznaku, na jehož konci se dozvíme, zda byla či nebyla porušena autorská práva[6]

1.1 Vodoznaky v grafických formátech souborů

Nejběžnějším způsobem ochrany, se kterou se setkáme u digitálních fotografií a grafických děl je jejich překrytí transparentní vrstvou nesoucí vodoznak, která se následně stává součástí díla. Tato vrstva zpravidla obsahuje jméno autora, název/logo společnosti, kontaktní údaje či symbol copyright ©. K největším výhodám této metody patří její robustnost, protože odolá veškerým běžným útokům a dále bude rozpoznatelná. Mezi další výhody patří i její snadná aplikace. Pomineme-li software přímo určený pro práci s vodoznaky, jeho tvorbu zvládne běžný uživatel v každém základním grafickém editoru. To, že jiný obraz překrývá ten původní a tím odrazuje potencionální zloděje díla, zároveň tvoří hlavní nevýhodu, protože snižuje umělecký dojem. Často se tedy volí průhledné vodoznaky, které dílo narušují méně.[7] Na *Obr. 1.2* je znázorněn způsob použití této metody.

Obr. 1.2 Plný, průhledný a reliéfový vodoznak

Programy, které se snaží takovéto vodoznaky odstraňovat, využívají algoritmů pro klonování blízkého okolí, jimž následně překryjí vodoznak. S vyspělejším softwarem se útočníci snaží vytvořit masku podobnou vodoznaku, pod kterou se snaží úpravou křivek[1] vyčistit obraz od vodoznaku.[8]

Další možností ochrany grafického díla je jeho opatření nerozpoznatelným[2] vodoznakem. Metoda využívá toho, že lidský zrak není schopen tuto úpravu detekovat. Může se jednat o překrývání obrazu vodoznaky, jež mají nastavenou viditelnost v rozmezí 1 – 2 %. Jejich přítomnost se ověřuje odečtením originálu od označeného obrazu. Efektivnějším způsobem skrytí vodoznaku, je jeho zanesení pouze do jednoho kanálu RGB. Mezi přednosti toho skrývání vodoznaků patří jeho robustnost. Přežije většinu útoků (od ztrátové komprese po deformaci obrazu, přidávání šumu apod.) a zároveň vodoznak snadno detekujeme bez znalosti originálu (zobrazením pouze jednoho barevného kanálu). Nevýhoda této metody se skrývá v její tvorbě. Vlastnosti vkládaného vodoznaku se musí pro každý podklad nastavovat zvlášť. Proto je hromadná aplikace této metody téměř nemožná. Dále nemůže být použita přes černý či bílý podklad.[9] Příklad této metody je zobrazen na *Obr. 1.3*.

Jako speciální případ pro ochranu díla může posloužit steganografie[3]. Obvykle barevný pixel definuje 24bitů, tedy 8bitů pro každý barevný kanál RGB. Každý pixel tedy může zobrazit 16 777 216 ($2^8 \times 2^8 \times 2^8$) barev. Dále popisovaná metoda využívá neschopnosti lidského oka rozlišit takovéto množství barev tak, že u pixelu mírně změní hodnotu RGB kanálů, což ale v celkovém kontextu není rozpoznatelné. Jako nosič vodoznaku se používá nejméně významný bit (LSB) z každého barevného kanálu v pixelu. LSB využívá neschopnosti oka odlišit modifikovaný LSB pixel od pixelu původního.

[1] *Křivky ovlivňují jas, stíny, střední tóny a jednotlivé RGB kanály obrazu.*
[2] *Nerozpoznatelným, protože není stoprocentně neviditelným.*
[3] *Steganografie je vědní obor zabývající se ukrýváním zpráv v komunikaci.*

Obr. 1.3 Část fotografie s vodoznakem a. v normálním zobrazení b. pouze kanál B (modrý)

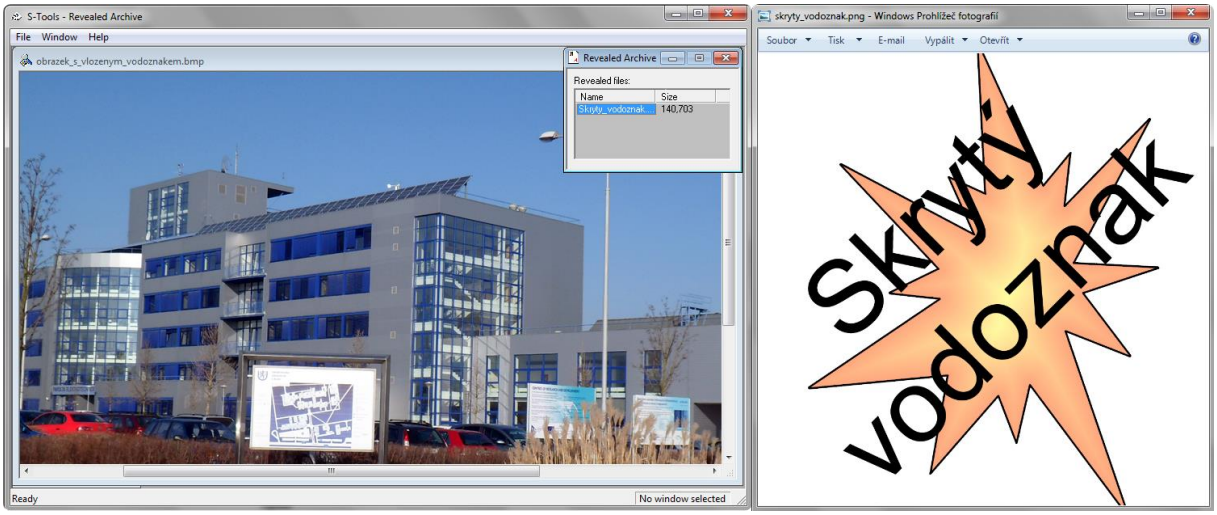
Vezmeme-li si například sytě červenou barvu z RGB modelu s 24 bitovou barevnou hloubkou, její hexadecimální zápis bude #FF0000. Převedením do binární soustavy získáme 1111111<u>1</u> 0000000<u>0</u> 0000000<u>0</u>. Podtržené bity si zabírá právě metoda LSB. Pixel nesoucí LSB informaci tedy bude moci zobrazit pouze 2 097 152 ($2^7 \times 2^7 \times 2^7$) barev, ale zároveň ponese skrytou informaci ve 3 bitech. LSB by bylo snadné odhalit, kdyby bylo aplikované na každém pixelu. Proto se v dnešní době tato metoda kombinuje společně s různými šifrovacími algoritmy, které náhodně vybírají pixely, na které se bude LSB aplikovat.

Tab. 1.1 Výpočet úložného prostoru vzorové fotografie

Vzorec	Popis
$1400 \times 1050 = 1470000\ px$	Rozlišení fotografie
$1470000 \times 24 = 35280000\ bitů$	Velikost fotografie v bitech
$35280000 \div 8 = 4410000 \doteq 538\ kBite$	Velikost úložného prostoru ($LST = 1/8$)

Fotografie tedy dokáže pojmout 538 kB libovolných dat, které kromě jiného mohou sloužit jako vodoznak. Takovýto vodoznak je ovšem slabý. Vyžaduje použití bezeztrátové

komprese (přípony typu TGA, BMP, GIF apod.) a jakýkoliv zásah může mít za následek ztrátu skrytých dat. Na *Obr. 1.4* se nalézá snímek grafického rozhraní freeware programu S-Tools 4.0, který touto metodou pracuje.[4]



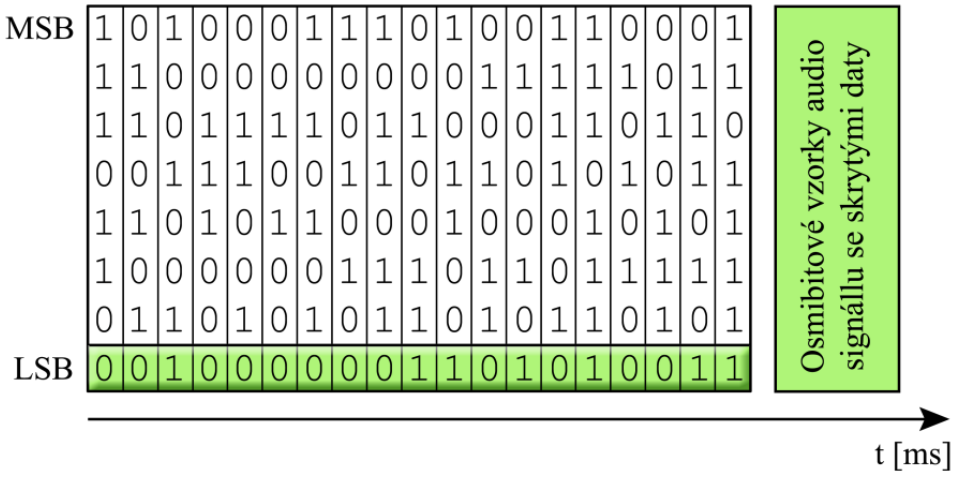
Obr. 1.4 Vlevo okno programu S-Tools se souborem obsahujícím ukrytá data, napravo vyextrahovaný vodoznak ve formě grafického JPG souboru (velikost hostitelského souboru se nezměnila)

Podobného principu (neschopnosti lidského oka rozpoznat málo odlišné barvy) dnes využívají některé novější laserové tiskárny. Při barevném tisku označí na vytištěnou stránku v podobě malých žlutých teček skryté informace. Jimi jde zjistit kde a kdy byl dokument vytištěn. Jedná se o velmi kompromitující funkci tiskáren, protože nejde vypnout a velmi narušuje soukromí. Díky tomu mohou osoby znající klíč k těmto vodoznakům odhalovat citlivé informace. V poslední době proto vnikají různá sdružení snažící se s výrobci tiskáren dohodnout o možnosti vypínání této funkce při tisku a také vznikají seznamy tiskáren, které tyto tečky tisknou.[10]

1.2 Vodoznaky v hudebních formátech souborů

Nejstarší metodou, která se používá pro skrývání informací do audio souborů je metoda využívající LSB, tedy nejméně významného bitu od libovolného vzorku. Díky tomu lze skrýt velké množství dat. Ideální kapacita takového prostoru v audio souboru je 1 kbit/s při frekvenci 1 kHz. Oproti LSB metodě v grafických formátech souborů lze u audio formátů využít dva nebo až čtyři nejméně významné bity. Tím několikanásobně vzrůstá velikost prostoru pro skrytí dat, ale zároveň se také zvětšuje detekovatelný hluk. Tato metoda je velice citlivá na úpravy audio signálu (filtrace, zesílení, odstranění šumu apod.). Proto se robustnost

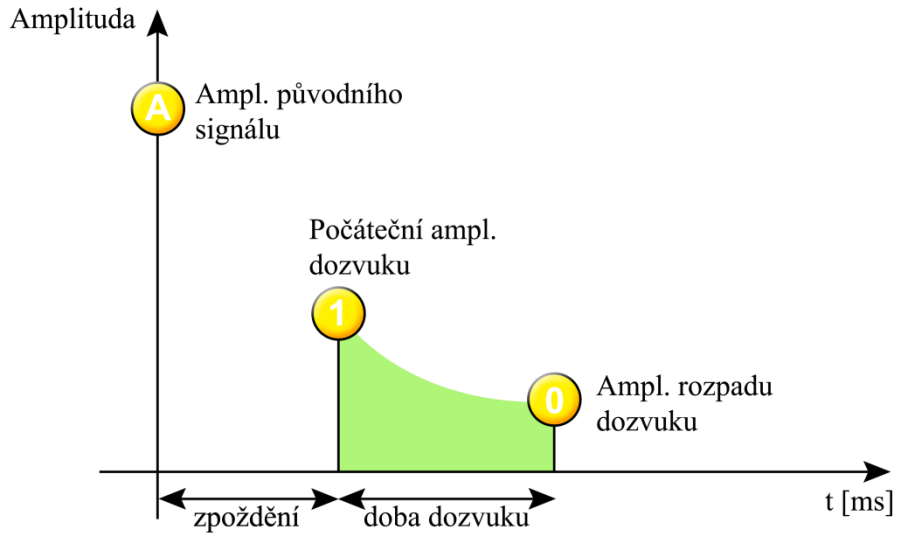
dat zvyšuje pomocí různých redundantních[4] technik, které sice sníží kapacitu ukrývaných dat, ale zaručí jejich lepší čitelnost.[11]



Obr. 1.5 Princip využití LSB u audio signálu[12]

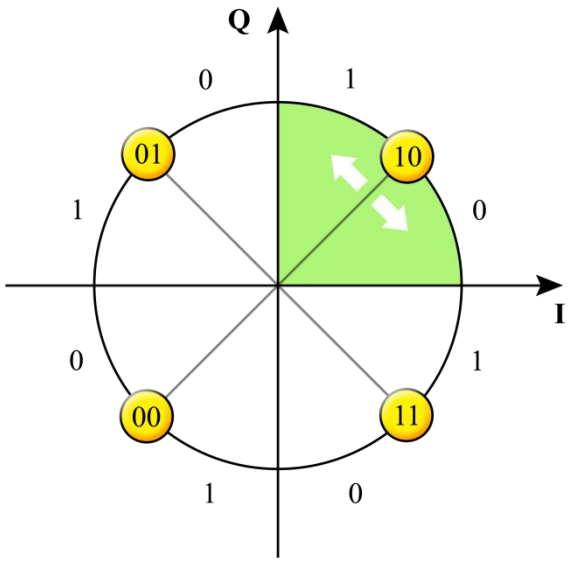
Často využívaným způsobem pro skrývání vodoznaků do hudebních souborů je metoda Echo hiding, pomocí které se data vodoznaku ukryjí do ozvěn. Princip této metody spočívá v tom, že zazní-li hlasitý zvuk, tak se o jeho dozvuk postará samo prostředí. Tudíž data, která zastupovala dozvuk na nahrávce, mohou být nahrazena jinými (v našem případě daty vodoznaku), aniž by lidský sluch poznal rozdíl. Velikost ukrytých dat signálu vodoznaku ovlivňují tyto tři parametry: velikost počáteční amplitudy, zpoždění a rychlost rozpadu dozvuku. Vliv parametrů na signál vodoznaku zobrazuje *Obr. 1.6*. Pro zpoždění do 1 ms je efekt této metody téměř k nerozpoznání. Navíc data signálu vodoznaku se volí tak, aby jejich přehrávaný zvuk ležel pod prahem vnímání lidského ucha. Echo hiding metoda značně závisí na kvalitě nahrávky. Kapacitu úložného prostoru také ovlivňuje počet a počáteční velikost ozvěn. [12]

[4] *Techniky sloužící ke zvyšování spolehlivosti a odolnosti opakováním informací.*



Obr. 1.6 Echo hiding (zelená oblast vyznačuje prostor pro ukrytí vodoznaku)[12]

Pakliže bychom hledali způsob, jak ukrýt vodoznak do přenosu audio signálu bez přidání dat vyvolávajících hluk, vhodnou volbou by jistě byla metoda fázového kódování. Tato metoda se opírá o skutečnost, že změny fáze jednotlivých složek neovlivňují zvuk vnímatelný lidským uchem. K zakódování skrytých dat používá jednoduché techniky fázového posunu. Princip je nejlépe patrný na IQ diagramu *Obr. 1.7*, kde je každá hodnota vysílaného signálu reprezentována jedním komplexním číslem. Dojde-li k výraznější výchylce u úhlu komplexního čísla, pak se jedná o zakódovanou hodnotu vodoznaku. Jedná se o robustnou metodu, která nedokáže ukrývat velké množství dat, a proto je nejpoužívanější právě pro skrývání vodoznaků.[11]



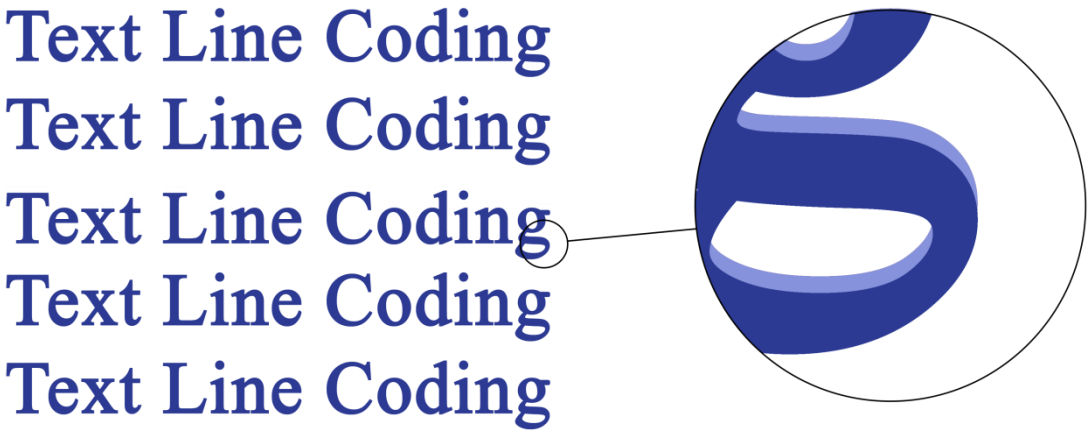
Obr. 1.7 IQ diagram čtyřstavového PSK (bude-li se úhel imaginárního čísla zastupující hodnotu 10 nalézat mezi 0° a 45°, zároveň se načte skrytá hodnota 0)[12]

S rozvojem dnešní komunikace se stále kladou větší nároky na ochranu či detekci případných úniků soukromých dat. Díky tomu dnes zažívá audio steganografie veliký rozvoj. Existuje řada dalších metod na skrývání dat, například ukrývání dat v intervalech ticha, kódování skrytých dat do audio hovorů, rozprostření spektra signálu a další, ale pro skrývání vodoznaků se využívají především výše uvedené metody, jelikož nejlépe vyhovují požadavkům vodoznaku.[12]

1.3 Vodoznaky v textových formátech souborů

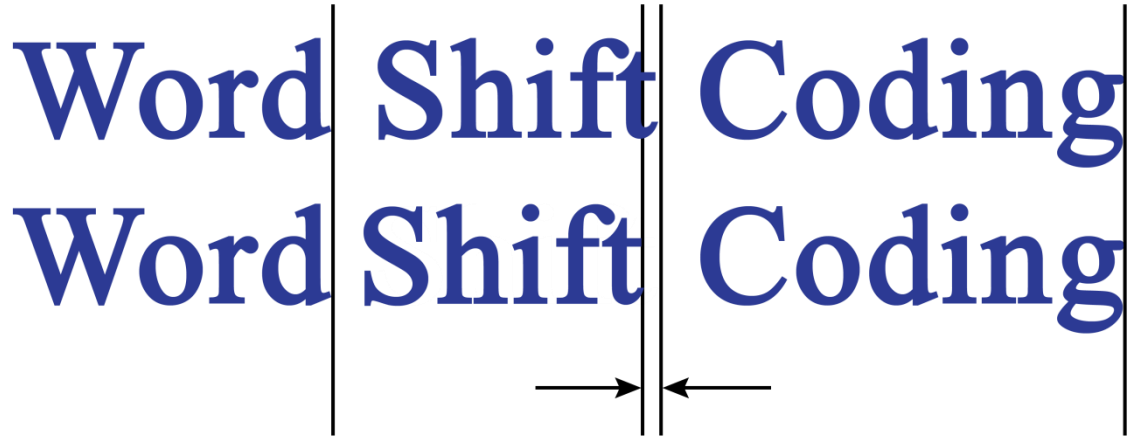
Pomineme-li vkládání obrázku do pozadí dokumentu, které využívají metod zmíněných u vodoznaků grafických formátů souborů, pro začlenění vodoznaků se nejčastěji používají tyto tři metody: Text Line Coding, Word Shift Coding a Character Encoding. Jedná se o slabé vodoznaky, ale lidským okem téměř nepostřehnutelné.[2]

Text Line Coding, volně přeloženo kódování v řádcích textu, upravuje prostor mezi jednotlivými řádky. Princip této metody spočívá pouze ve vertikálním posuvu řádků. Výhodou této metody je, že nemusí nabývat pouze jedné hodnoty (0 výchozí stav, 1 posunuto), ale i tří a více hodnot, pokud se neposunuje pouze o pixel (-1 posun nahoru, 0 výchozí stav, 1 posunuto dolu). Nutností k dekódování tohoto vodoznaku je znalost vzdáleností řádků v původním dokumentu.[13]



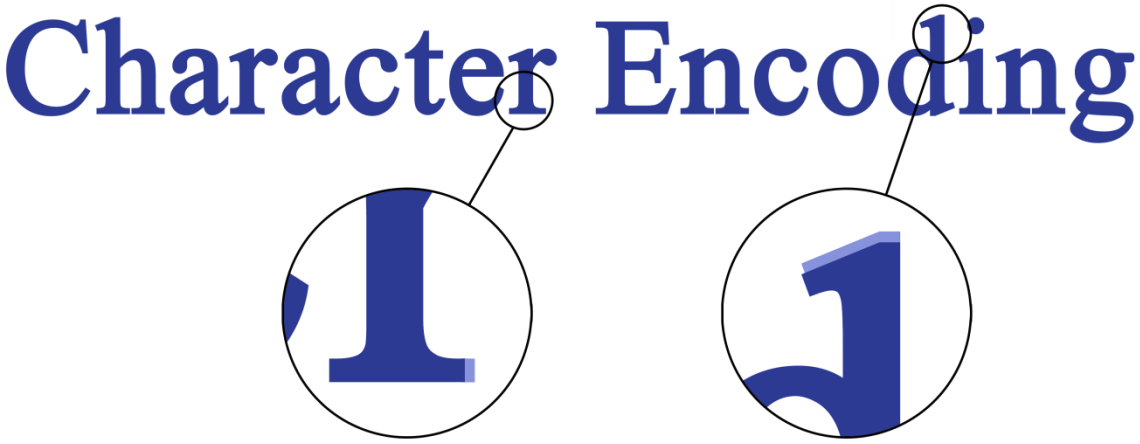
Obr. 1.8 Ukázka kódování v řádcích, světle modrá barva naznačuje původní pozici písmen v řádku

Word Shift Coding, volně přeloženo kódování posunem slov, upravuje velikost mezer mezi jednotlivými slovy. Výhodou je větší kapacita pro ukrytí dat než v předchozím případě. V dokumentech s pevnou mezerou se nepoužívá, jelikož ji v nich lze snadno odhalit. Pro její dekódování opět musíme znát původní dokument nebo se musíme řídit obecnými algoritmy pro tvorbu proměnlivých mezer.[13]



Obr. 1.9 Word Shift Coding (na prvním řádku se nalézá původní text)

Character Encoding, volně přeloženo kódování znaků, pozměňuje tvar písmen a tím nese datovou informaci. Změny mohou být ve formě změny délky horní dotažnice písmene (tj. vertikální linky, např. u písmen „d“ nebo „h“) nebo změnou šířky patky písmene. Skrytá informace tedy nabývá dvou stavů (0 výchozí tvar, 1 změněno), přičemž pro její identifikaci musíme znát původní tvar písmene.[13]



Obr. 1.10 Příklad využití kódování dat vodoznaku do jednotlivých písmen

Oproti kódování v grafických souborech, poskytuje kódování v textových souborech daleko méně úložného prostoru pro skrývání dat. Velikost tohoto prostoru závisí na počtu řádků, mezer či jednotlivých znaků nesoucích skrytou informaci.[13]

1.4 Vodoznaky v audiovizuálních souborech

Jedná se o soubory, které v sobě nesou video, jednu nebo více zvukových stop, případně i titulky. Takovéto multistreamové soubory se souhrnně označují kontejnery.[14] Podle toho,

jaká data obsahují, se k nim volí patřičné metody a kombinace metod (z výše uvedených) pro skrývání vodoznaků.

Aby se lidskému oku zdál obraz plynulý, musí mít video kanál alespoň 24 fps. To skýtá velkou výhodu vizuálním vodoznakům. Nemusí překrývat video po celou dobu jeho trvání a mohou být vloženy do jednoho či více snímků, které budou určitým způsobem rozprostřeny ve videu. Autor díla bude vědět, ve kterých časových intervalech se vodoznaky nacházejí, ale pro oko pozorovatele se objeví na tak krátkou dobu, že je stěží postřehne. Zpravidla se tyto vodoznaky vkládají do I-snímků, což jsou tzv. klíčové snímky, kódované nezávisle na okolních snímcích daným kodekem. Od I-snímků se vypočítávají tzv. rozdílové snímky (P-snímky). Rozdílové snímky se vypočítávají, a proto je obtížné do nich ukrýt vodoznak, ovšem v současné době již existují metody, které tento způsob skrývání dovedou.[15]

2 Digitální podpis

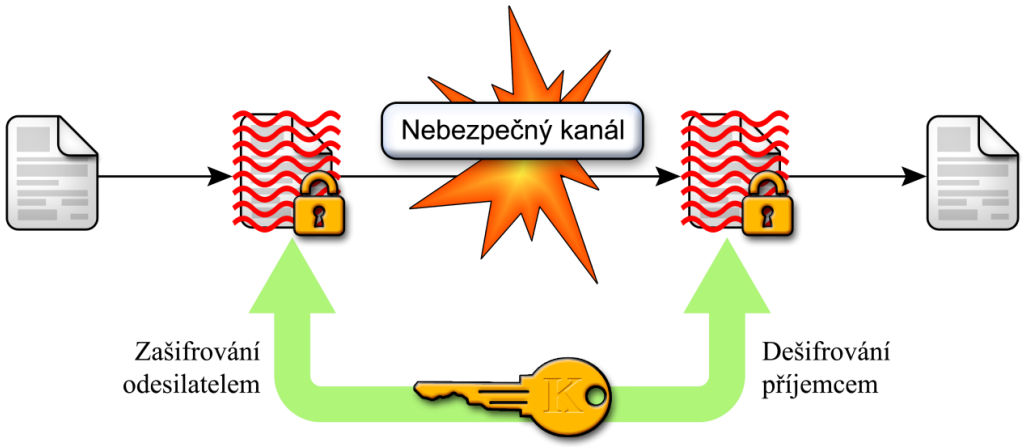
Digitální podpis byl vyvinut jako obdoba klasického podpisu. Zaručuje jednoznačnou identifikaci osoby, svojí jedinečnost a nezfalšovatelnost. Digitální podpis se již stal rovnocenným klasickému podpisu a v některých ohledej jej i předčil, protože se nedá zfalšovat a navíc i brání pozměnění dokumentu tím, že se vytváří na základě obsahu dokumentu.

Digitální podpis lze charakterizovat těmito vlastnostmi:

- Jednoznačnou identifikací, vždy musí prokázat původce podpisu,
- zajištění integrity obsahu, příjemci musí dokument dorazit kompletní a nepozměněný,
- zaručení nepopiratelnosti, odesilatel nemůže popřít, že mu podpis nepatří,
- nenapodobitelnost, podpis nelze napodobit ani zneužít pro jiný dokument.

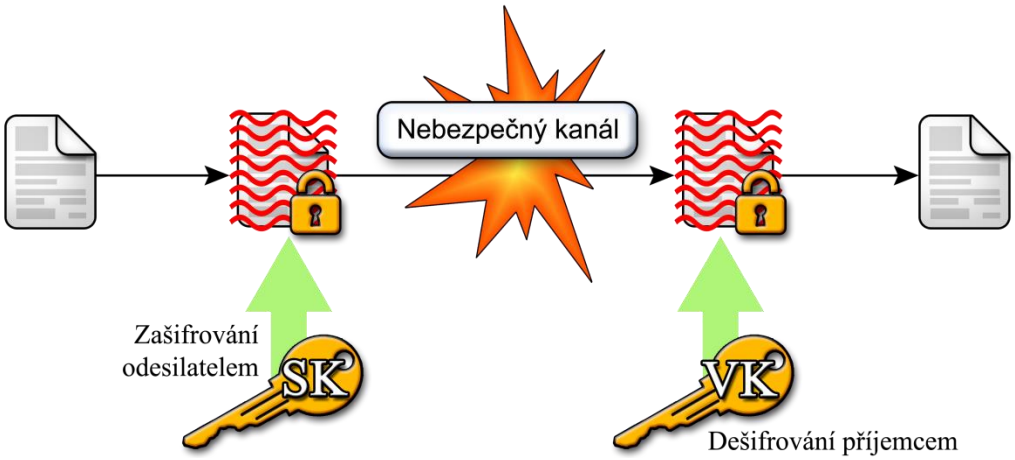
Šifru, ochranu proti zfalšování podpisu, tvoří velmi velké číslo (dlouhé minimálně 1024 bitů), které se vždy vztahuje ke konkrétnímu dokumentu. Generování tak velkého čísla by bez pomoci hašovacích funkcí (hash function) zabralo spoustu času.[16] Jedná se o jednosměrné funkce, přesněji algoritmy, které za přítomnosti klíče vygenerují z obsahu dokumentu dané číslo.[17] Klíče se tedy používají při šifrování a zpětném odšifrování. Podle toho, jaké klíče použijeme, dělíme podepisovací algoritmy na symetrické a asymetrické.

Při symetrickém způsobu šifrování se k zašifrování i odšifrování používá stejný klíč. Takovýto klíč musí vlastník důkladně zabezpečit a utajovat. Nevýhodou této metody je, když dojde k prozrazení společného klíče. Snadno pak může dojít k úniku informací a nepůjde ani určit zda klíč unikl příjemci či odesilateli. Jedinou výhodou symetrického šifrování je rychlost, s jakou algoritmy pracují.[16]



Obr. 2.1 Symetrické šifrování[16]

V asymetrických šifrovacích algoritmech se nalézá soukromý a veřejný klíč. Veřejný klíč se určitým způsobem zveřejní a privátní klíč se ponechává v tajnosti. Veřejný klíč může kdokoliv použít pro zašifrování dokumentu určenému pro nás a jen my budeme schopni dokument dešifrovat. Druhou možností je, že vytvoříme dokument a zašifrujeme jej naším soukromým klíčem. Pak kdokoliv kdo za pomoci veřejného klíče dokument otevře, bude mít jistotu, že dokument pochází právě od nás. U asymetrických systémů tedy nespočívá nebezpečí ve vyzrazení veřejného klíče. Jediným bezpečnostním rizikem je možná snaha podvrhnout jej.[17]



Obr. 2.2 Asymetrické šifrování[16]

2.1 Podepisování dokumentu

Podepisování dokumentu v jednoduchosti probíhá tak, že dokument vložíme do speciálního programu, který z dokumentu a našeho soukromého klíče vygeneruje posloupnost znaků, kterou připojí k dokumentu jako jeho digitální podpis. Takovýto dokument je zaslán příjemci, který si za pomoci veřejného klíče ověří pravost podpisu a integritu obsahu.

Z výše uvedeného principu vyplývá série několika kroků, které musí odesilatel vždy podstoupit při generování digitálního podpisu:

1. Odesilatel musí vlastnit počítačový program pro vytváření a ověřování elektronického podpisu,
2. programem si vytvoří dvojici soukromého a veřejného klíče,
3. poskytovateli certifikačních služeb předloží veřejný klíč a prokáže svoji totožnost,
4. nechá si vystavit certifikát certifikační autoritou, kterým se zaručí, že veřejný klíč náleží právě jemu,

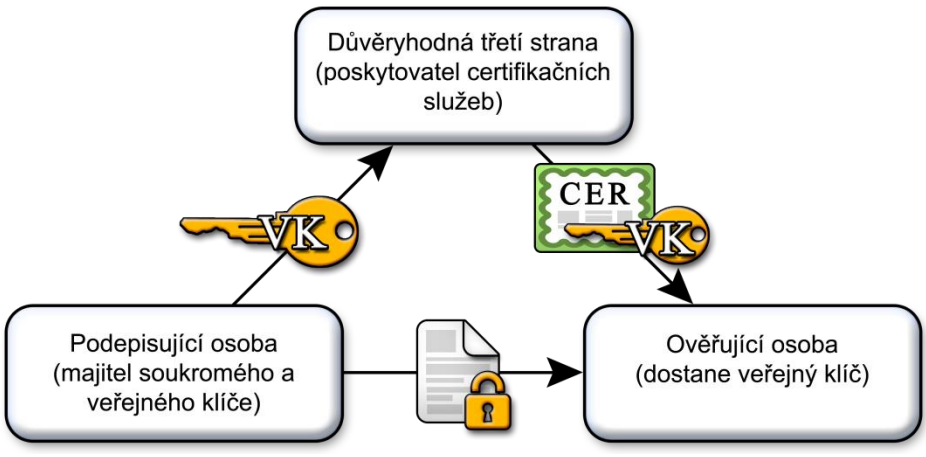
5. svým soukromým klíčem může vytvářet elektronické podpisy u jednotlivých dokumentů a příjemci si za pomoci veřejného klíče mohou ověřovat pravost odesilatelovo podpisu.

Klíče jsou při svém použití vzájemně závislé. Veřejný klíč se zpřístupňuje komukoliv, kdo potřebuje ověřit digitální podpis odesilatele, či potřebuje zašifrovat vzájemnou komunikaci. Soukromý klíč musí zůstat utajen, vlastník jej využívá pro tvorbu digitálních podpisů a dešifrování dokumentů zašifrovaných pomocí veřejného klíče.[16]

2.2 Ověřování podpisu

Ověřování podpisu se provádí za pomoci veřejného klíče a opět počítačovým programem. Výstupem tohoto ověřování je buď potvrzení, že podpis patří odesilateli a obsah nebyl během doručení pozměněn, anebo zamítnutí, protože se s dokumentem manipulovalo, či nebyl ověřen podpis odesilatele.

Veřejný klíč může příjemce získat přímo od odesilatele. Častěji ale bývají zveřejňovány v přístupných internetových databázích společně s údaji, komu daný klíč patří. U takto sdíleného veřejného klíče si ovšem nemůže být příjemce jist, že se jedná o pravý klíč. Proto je zapotřebí, aby někdo zaručil jeho pravost. O to se stará certifikační autorita, což je třetí strana, poskytovatel certifikačních služeb. Ta svým certifikátem připojeným k veřejnému klíči potvrzuje jeho pravost, protože odesilatel musel doložit svoji totožnost při registraci svého veřejného klíče.



Obr. 2.3 Význam třetí strany, certifikování klíče[16]

Certifikační autoritou je tedy nezávislý subjekt potvrzující pravost totožnosti majitele soukromého a veřejného klíče. Každý certifikát který vydá, obsahuje také podpis certifikační

autority, kterým potvrzuje, že údaje v certifikátu jsou pravdivé. Její hlavní úkol spočívá ve vydávání certifikátů, veřejných klíčů a vytváření důvěry mezi subjekty.[16]

Certifikát obsahuje údaje týkající se klienta a digitální podpis certifikační autority. Často se přirovnává k občanskému průkazu, na rozdíl od něj ovšem certifikát obsahuje veřejný klíč. Struktura certifikátu a jednotlivé položky jsou psány v jazyce ASN.1. Položky obsahují údaj o verzi certifikátu, jeho unikátní sériové číslo, algoritmus (kterým certifikační autorita vytvořila svůj podpis), podpis certifikační autority, dále obsahují platnost certifikátu, položku pro jedinečná jména (obsahuje identifikátory, jejichž atributy lze popsat klienta) a veřejný klíč.[17]

3 Metadata

Jedná se o strukturovaná data, která popisují, vysvětlují, lokalizují nebo jinak zjednodušují určení obsahu daného souboru. Následně se využívají ke katalogizaci či třídění elektronických dat. V DRM se především používají k určení autorství a práv duševního vlastnictví.

Metadata se většinou nacházejí uvnitř souboru ve speciálním záhlaví a dají se aplikovat téměř na jakýkoliv formát souboru. Metadata tvoří elementy, které jsou navrhnuty pro konkrétní použití a následně je jim přiřazena vhodná informace (např. jméno autora, organizace, datum vytvoření, apod.). Zprvu existovalo 13 elementů sloužících pro identifikaci webových dokumentů pojmenovaných Dublin Core. S rozvojem digitální komunikace se tyto prvky začaly rozrůstat a začaly se vytvářet speciální skupiny elementů pro specifické účely (např. umění, technické výkresy, apod.). V současné době se s oblibou používá kódovaný archivní popis, zkráceně EAD, který vychází z XML (každý element je uzavřen v tagu, hierarchická struktura kódu). Syntaxe přiřazení a nejužívanější elementy pro identifikaci jsou znázorněny v *Tab. 3.1*.[18]

Tab. 3.1 Syntaxe elementů metadat podle Dublin Core a EAD

Syntaxe Dublin Core	Syntaxe EAD
`Title="DRM"`	`<Title>DRM</Title>`
`Creator="Charvat,Tomas"`	`<namePart type="family">Charvat</namePart>` `<namePart type="given">Tomas</namePart>`
`Date="2013"`	`<dateIssued>2013</dateIssued>`
`Type="Text"`	`<typeOfResource>text</typeOfResource>`
`Format="application/pdf"`	`<format>application/pdf</format>`
`Language="cz"`	`<language>cz</langure>`

Metadata jsou užitečným nástrojem pro třídění, vyhledávání či určování autorství. Nejedná se však o silnou ochranu dokumentu, jelikož tato data mohou být snadno přepsána či úplně odstraněna. Často se navíc stává, že aplikace, jimiž vytváříme dokumenty a ostatní soubory, ukládají do metadat citlivé informace, které zjišťují z autorova počítače. Snadno pak dochází k úniku těchto informací, aniž by autor něco tušil. Proto je vždy důležité vědět, jak dané aplikace pracují nebo jak jsou nastaveny.[19]

4 DRM ochrana u speciálních typů souborů

4.1 Zabezpečení PDF souborů

Jedná se o přenositelné soubory vyvinuté společností Adobe. Díky své schopnosti substituce a objektově orientovanému skládání prvků si dokument uložený v tomto formátu zachovává svoji integritu. Na všech zařízeních se tedy dokument zobrazuje stejně. Společnost Adobe zaměřila svůj datový formát především na produktivitu pracovního postupu pro firemní uživatele, obohatila jej o funkce jako například digitální podpisy a formuláře, vkládání metadat, zvýraznění, přeškrtnutí, apod. PDF také může obsahovat video, zvuk, spustitelné aplikace makra a různé přílohy. Tím se stal tento formát dokumentů velice oblíbeným a začal být využíván ve velkém.[20]

S následnou expanzí tohoto formátu dokumentů musela společnost Adobe začít řešit i zabezpečení obsahu PDF dokumentů. Začali se tedy implementovat jak relativně jednoduchá tak i značně složitá opatření, kterými se dala navýšit bezpečnost dat v dokumentu dle potřeby uživatele.

Nejjednodušším opatřením jak ochránit obsah svého dokumentu je zaheslovat jej. Tuto možnost zvolíme, pokud chceme, aby obsah mohly vidět pouze vybrané osoby. Do verze PDF 1.3 existovalo pouze 40 bitové zabezpečení. Nyní je běžné 128 bitové zabezpečení s AES kódováním, ovšem stávající verze PDF 1.7 a vyšší již zvládají 256 bitové zabezpečení s AES kódováním. Protože však starší verze kódování nejsou kompatibilní s vyššími, musíme vždy správně zvolit jeho verzi. Hesla v PDF dokumentech jsou dvojího druhu, uživatelské heslo a heslo správce. S uživatelským heslem si můžeme otevřít dokument a provádět základní operace dle nastavení daného dokumentu. S heslem správce, neboli s heslem pro práva můžeme nastavovat různá oprávnění pro příjemce dokumentu. Může se jednat například o omezení tisku, omezení úprav a kopírování obsahu. Pro vyšší úroveň zabezpečení by měl dokument obsahovat oba typy hesel. Navíc ve stávajících verzích Acrobatu se již objevuje i index a komentář o síle hesla.

Další možností jak chránit obsah svého dokumentu je nastavení práv pro tisk, změny, kopírování a šifrování. Nutností pro aplikaci těchto nastavení je znalost hesla pro správu na daném dokumentu. U práva pro tisk můžeme zcela zakázat tisknutí dokumentu. Další možností jak omezit tisk je nastavení nízkého rozlišení (pouze 150 dpi). Změny můžeme také úplně zakázat nebo můžeme povolit jen některé. Na výběr máme několik možností:

- Vložení, odstranění a natočení stránek,

- vyplnění polí formulářů a podepsání existujících polí podpisu,
- přidávání poznámek, vyplnění polí formulářů a podepsání existujících polí podpisu,
- vše kromě vyjmutí stránek.

Kopírování textu, polí a obrazů můžeme v dokumentech povolit či zakázat, stejně tak jako přístup čtecích zařízení pro slabozraké. Zašifrovat můžeme nechat celý obsah dokumentu, celý dokument bez metadat (ty jsou často ponechávány pro vyhledávací programy) nebo můžeme nechat zašifrovat pouze přílohy.

Pakliže bychom chtěli, aby měl příjemce jistotu, že dokument pochází právě od nás, můžeme dokument namísto hesel obohatit digitálním identifikátorem. Digitální identifikátor funguje jako digitální podpis, tedy identifikuje osobu podepisující dokument. Obsahuje zašifrované, pro podepisující osobu jedinečné informace, jako například jméno a příjmení, email, sériové číslo či datum ukončení platnosti. Může také obsahovat obraz podpisu. Digitální identifikátor obsahuje soukromý klíč a certifikát s veřejným klíčem. Soukromý klíč se využívá při tvorbě podpisu založeném na daném certifikátu, který se následně aplikuje na celý dokument. Využívá se přitom hašovacího algoritmu, který dané informace zašifruje. Takto vytvořený podpis se pak ověřuje za pomoci certifikátu s veřejným klíčem pokaždé, když příjemce otevře dokument.

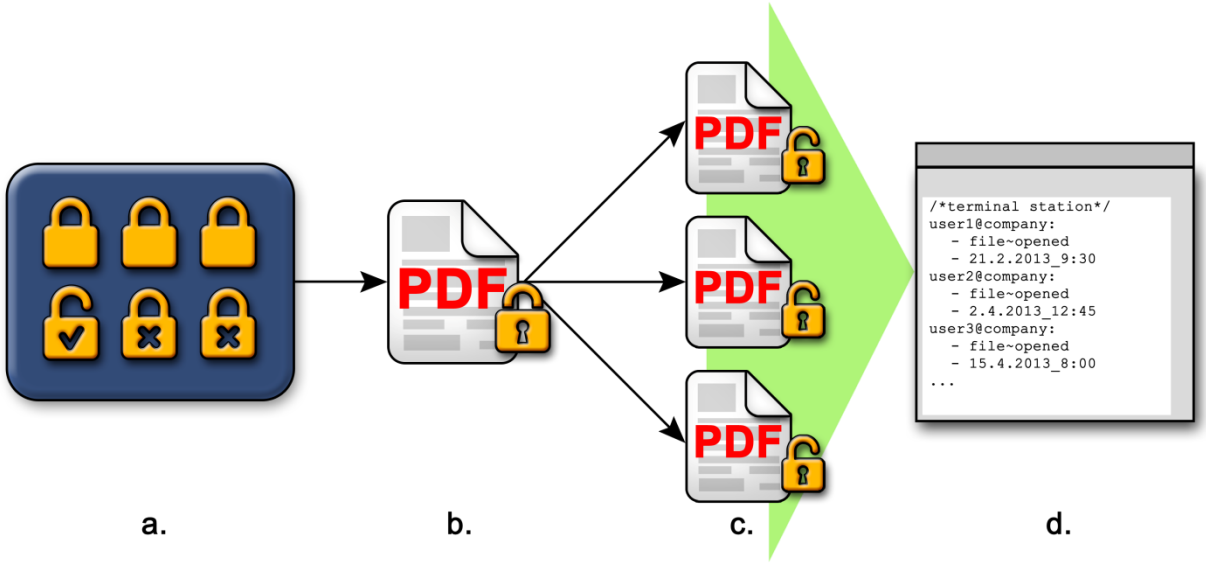
S tvorbou PDF dokumentů je důležité hlídat si citlivý obsah. Jde o údaje, které se automaticky vyplňují a narušují autorovo soukromí. Může se jednat o citlivý text a obrázky, metadata, nebo mohou nežádoucím způsobem změnit vzhled dokumentu (JavaScript, akce a pole formulářů). Proto je vhodné využívat software, který dokáže takovéto prvky najít a eliminovat, případně redigovat[5].

Veliký vliv na bezpečnost tohoto formátu dokumentů má i vlastní čtecí software od společnosti Adobe. Disponuje řadou zabezpečení, díky kterým uživatel lépe ochrání svá data. Dokáže detekovat potencionální hrozby a upozornit na ně. Důležitou, ovšem defaultně vypnutou funkcí, je funkce chráněného režimu. PDF soubor se otevře ve chráněném prostředí, tzv. sandboxu, který je izolován od okolního prostředí a nic, co se v něm nalézá, nemůže poškodit systém. Další výhodou je možnost zablokování internetových vazeb, které často představují potencionální bezpečnostní riziko.

Vhodnou volbou pro větší organizace je systém Adobe LiveCycle Rights Management ES. Jedná se o zabezpečovací systém založený na serveru, který dynamicky kontroluje PDF

[5] *Proces trvalého odstranění grafiky či textu z dokumentu začerněním a odstraněním.*

dokumenty. Na takovýto server se nahrávají zásady zabezpečení, které jsou následně hromadně aplikovány na vybrané dokumenty. Zásada obsahuje kombinace výše uvedených bezpečnostních opatření. Takováto zásada zajišťuje jednotné zabezpečení pracovního postupu a navíc šetří čas strávený nastavováním zabezpečení jednotlivých dokumentů. Server také umožňuje kontrolovat platnost dokumentů, jejich odvolávání a spravuje přehled o odpovědnosti kontrolou uživatelů otevírajících chráněné dokumenty. Nemalou výhodou tohoto serveru je i jeho variabilnost, díky které je schopen spolupracovat s dalšími podnikovými systémy.[21] *Obr. 4.1* znázorňuje princip fungování serveru.



Obr. 4.1 a. zásady uložené na serveru b. aplikace zásad na PDF c. uživatelé splňující zásady mohou pracovat s dokumenty d. zaznamenávání událostí na serveru[22]

4.2 Zabezpečení souborů kancelářského balíku MS Office

Tento kancelářský balík obsahuje sadu aplikací pro práci s různými typy dokumentů. Je vyvíjen společností Microsoft od roku 1989, ovšem první aplikace MS Word přišla na trh již v roce 1983.[23] Jedná se o velice využívaný kancelářský software, proto disponuje řadou bezpečnostních opatření. V závislosti na druhu dokumentu jsou aplikovatelná i další nastavení, která zvyšují bezpečnost daného typu dokumentu.

Novější aplikace tohoto balíku umožňují zabezpečit dokument řadou různých opatření. Uživatel může svůj finální soubor označit jako konečný, čímž zamezí jakýmkoliv úpravám a od daného okamžiku bude dokument sloužit pouze pro čtení. Standardní možností je také ochrana dokumentu pomocí hesla, podle kterého se zároveň zašifruje celý obsah dokumentu.

V aplikaci MS Word můžeme vymezit typy změn, které v dokumentu půjdou provádět. Tyto změny se dělí na omezení formátování a omezení úprav. Omezení formátování se využívá u dokumentů, kde chceme zachovat původní vzhled. V nastavení této funkce můžeme přesně nastavit, jaké styly povolíme. V omezení úprav můžeme přesně určit, zda půjde dokument upravovat, či jaké úpravy budou povoleny. Dále v této aplikaci můžeme použít jednoduchý zámek, který nám dokument uzamkne heslem nebo nastaví ověřování uživatelů.

Aplikace MS Excel nabízí funkci zamčení aktuálního listu. Tím na daný list může autor aplikovat ochranu heslem a povolit zda ostatní uživatelé budou moci vybírat, vkládat, odstraňovat a upravovat oblasti daného listu. Další možnost jak zabránit ostatním uživatelům ve změnách dokumentu je zamčení struktury sešitu. Jedná se o funkci, kde můžeme nastavit ochranu heslem a vybrat možnosti zabraňující uživatelům měnit, přesouvat a odstraňovat důležitá data.

Stejně tak, jako v případě PDF dokumentu, můžeme i do souboru aplikace MS Office přidat digitální podpis s ověřovacím certifikátem, který zaručí koncovému uživateli, že je soubor pravý a nebyl v průběhu doručování pozměněn. Zároveň se ale do metadat souboru mohou dostat citlivá data, která následně mohou uniknout.

Pro velké organizace je jistě důležitou funkcí spravování přístupových práv k informacím (IRM). Tato technologie je přístupná od verze MS Office 2010 a umožňuje správcům a uživatelům stanovovat jednotlivá přístupová opatření k souborům této sady. Nutným požadavkem této funkce je přítomnost služby Správa přístupových práv ve Windows (RMS) nebo Windows live ID. Tato služba umožní definování IRM šablon jak pro společnost, tak pro různé skupiny cílových uživatelů. Jednou z možností je například omezení otevření souborů a pošty pouze v rámci emailové domény společnosti. Jakmile se souboru nastaví omezení oprávnění technologií IRM, nastavení se uloží přímo do souboru a od daného okamžiku bude vynucováno pokaždé bez ohledu na to, kde se soubor nachází. Při prvním pokusu otevřít takovýto soubor se požadovaná služba připojí k licenčnímu serveru a ověří uživatelovo pověření k tomuto souboru. Danému uživateli pak bude přidělena licence s příslušnými právy.

S funkcí IRM mohou následně autoři využívat omezení oprávnění obsahu souborů pro jednotlivce i skupiny. Navíc mohou jednotlivým oprávněním nastavovat jejich životnost. Na výběr mají ze tří úrovní oprávnění, a to čtení, změny a úplné řízení. Při výběru čtení je dokument určen pouze pro prohlížení. Úpravy, kopírování a tisk jsou zakázané. Při výběru změny může uživatel dokument měnit, ale nemá oprávnění k tisku. Při úplném řízení má uživatel stejná oprávnění jako autor.[24]

5 Možnosti zabezpečení datových souborů

Metadaty můžeme opatřit jakýkoliv soubor. Stejně tak je tomu i u skrytých vodoznaků. S využitím skrývání informací do LSB můžeme skrýt do grafických, audio a video souborů libovolná data, ať už se jedná o skrývání textu, obrázků či celých souborů. Výhodou takového skrývání dat je, že se nemění velikost hostitelského souboru a jeho obsah se změní nerozpoznatelně pro lidské smysly. Další možnosti skrytí dat v audio souborech nám nabízí metoda skrývání dat do ozvěn a metoda fázového kódování určená pro přenos audio signálu. Skryté vodoznaky v dokumentech pak zastupují metody jako text line coding, word shift coding a character encoding.

V grafických a video formátech soborů se ovšem nejčastěji setkáváme s viditelnými vodoznaky, jelikož chrání dílo nejlépe, a to tím, že jej znehodnotí. S viditelnými vodoznaky se také můžeme setkat u dokumentů, kde se mohou nalézat na pozadí dokumentu či v jeho obsahu. Nejbezpečnější ochranu však nabízejí digitální podpisy, které díky svým jednosměrným hašovacím funkcím a certifikaci od třetích stran zaručují pravost a integritu obsahu dokumentu.

Tab. 5.1 Možnosti zabezpečení jednotlivých typů souborů

Typ souboru	Grafický	Hudební	Audiovizuální	Dokument
Metadata	Ano	Ano	Ano	Ano
Digitální podpis	Ne	Ne	Ne	Ano
Viditelný vodoznak	Ano	Ne	Ano	Ano
Skrytý vodoznak	Ano	Ano	Ano	Ano

6 Využití DRM v univerzitním prostředí

Vytváříme-li dokument pouze pro vybranou skupinu uživatelů a chceme, aby se mimo tuto skupinu nemohl šířit, je vhodné jej zabezpečit heslem. Nesmíme ale zapomenout vytvořit heslo pro správu dokumentu. Druhému heslu, tedy heslu pro uživatele můžeme nastavit různá omezení, která se týkají například úprav nebo kopírování obsahu.

Studenti si také často upravují univerzitní dokumenty. Dopisují do nich poznámky z přednášek, což nevadí, ale často mění i jejich původní obsah, který dále šíří. Tím často dochází k nesprávným úpravám, které mění význam obsahu a často vedou k nesprávným výrokům. Pro omezení takovýchto editací je vhodné nastavovat dokumenty jako finální. Neumožní již s dokumentem žádné úpravy ani kopírování, povolené bude pouze čtení a tisk. Alternativním způsobem ochrany dokumentu je jeho export do PDF. Adobe Reader navíc podporuje vkládání poznámek do PDF dokumentů, díky čemu si student nemusí tisknout dokument pro zapisování poznámek z přednášek.

Významné a důležité dokumenty z univerzitního prostředí se mohou opatřovat digitálním podpisem, který příjemcům zaručí jejich pravost a integritu obsahu.

U dokumentů i jiných souborů je vhodné vyplňovat patřičné elementy metadat. Tímto způsobem lze vhodně sdělit uživateli, odkud dokument pochází (univerzita, fakulta, apod.), kým a kdy byl dokument vytvořen i bez toho, aniž by dokument otevřel. Takto vyplněná metadata navíc ulehčí vyhledávání a archivaci souboru.

U kancelářského balíku MS Office by se mohla funkce IRM využívat při psaní znalost ověřujících prací na počítači. Z IRM by se konkrétně využívalo především nastavení životnosti oprávnění vybraných uživatelů (studentů), kteří by psali test do připraveného formuláře. Studenti by měli nastavené právo zapisovat do tohoto formuláře pouze po dobu testu, tuto dobu by si nastavoval vyučující.

Grafické soubory (schémata, nákresy, apod.) se v určitých případech jistě vyplatí obohatit viditelnými vodoznaky. Vhodnou variantou vodoznaku může být logo fakulty, musí však splňovat podmínky jednotného vizuálního stylu. Podmínky jsou dostupné na webové adrese http://www.zcu.cz/about/vyznamne-dokumenty/Manual_jednotneho_vizualniho_stylu.pdf.

U grafických souborů, kde není vhodné vkládat viditelný vodoznak, můžeme patřičným softwarem skrýt vodoznak jednou z metod, která využívá nedokonalosti lidského oka, například kódování do LSB, které se může aplikovat i na audio soubory, protože ani lidské ucho nerozpozná tak jemné rozdíly ve zvukové stopě. Další metodou, kterou lze snadno aplikovat do audio nahrávek je skrývání dat do ozvěn.

Závěr

Funkce digitálního vodoznaku a kritéria na něj kladená jsou popsány v kapitole 1. Díky těmto kritériím můžeme vodoznaky dělit na silné a slabé. Životní cyklus vodoznaku je znázorněn na *Obr. 1.1*. Dále jsou v této kapitole popsány nejvyužívanější metody pro aplikaci vodoznaků pro různé typy datových souborů.

Kapitola 2 se zabývá digitálním podpisem a jeho charakteristickými vlastnostmi. Je zde vysvětlen význam hašovacích funkcí v digitálním podpisu a rozdíl mezi symetrickým a asymetrickým šifrováním dokumentu. Dále je zde nastíněn postup podepisování a následné ověřování dokumentu, úloha třetí strany, význam a obsah certifikátu. Pro názornost je vše zpracováno graficky na *Obr. 2.1 – Obr. 2.3*.

Další kapitola je věnována metadatům. Vysvětluje důvod jejich vzniku, výhody i možná úskalí. Věnuje se také jejich syntaxi a příkladům zápisu v *Tab. 3.1*.

Následující kapitola se zabývá zabezpečením u konkrétných typů souborů a to konkrétně PDF soubory a soubory kancelářského balíku MS Office. PDF nabízí řadu zabezpečení jako zabezpečení heslem pro správu dokumentu a odlišným heslem pro uživatele, nastavení práv pro práci s dokumentem, či připojení digitálního podpisu. Velkou výhodu PDF tvoří i jeho čtecí aplikace společnosti Adobe, která dokáže v dokumentu rozpoznat různá bezpečnostní rizika a upozornit na ně. Pro velké společnosti navíc Adobe vyvinulo serverový zabezpečovací systém, který umožňuje hromadně spravovat zabezpečovací oprávnění a dynamicky kontrolovat soubory PDF. Princip této serverové aplikace znázorňuje *Obr.4.1*. Dokumenty ze sady MS Office disponují heslováním, podle kterého se následně šifruje celý dokument. Dále umožňují nastavit dokument jako finální, čímž znemožní jakékoliv další úpravy. Také nabízí omezení formátování či úprav daného souboru, připojení digitálního podpisu a hromadné spravování přístupových práv přes funkci IRM.

Další kapitola této práce se věnuje porovnání zabezpečení jednotlivých typů soborů, kde nejvýstižněji toto porovnání zachycuje *Tab. 5.1*.

Poslední kapitolu tvoří návrhy využití DRM v univerzitním prostředí, které byly sestaveny na základě poznatků z rešeršní části této práce.

S rozvojem informačních technologií nabízí dnešní doba vysoké uplatnění DRM. Se stále se navyšujícím počtem digitálních děl je potřeba zaručit jejich nezfalšovatelnost, či majitele duševních práv, tedy autora. V dnešní době se můžeme běžně setkat s aplikováním DRM na soubory a programy, například u služby iTunes od Apple, speciální ochranou pro elektronické knihy Adobe DRM nebo online autentizací před spouštěním programů či

her. S DRM se můžeme setkat také u záznamových zařízení v televizích či rekordérech, které své nahrávky ukládají do speciálních typů souborů opět spustitelných pouze v nich, nebo se můžeme setkat se záznamem, který lze přehrát pouze jednou. Do budoucna můžeme počítat, že společnosti a autoři digitálních děl budou stále více přecházet na DRM nebo svoje stávající zabezpečení budou více prohlubovat. Díky tomu můžeme počítat s velkým uplatněním a dalším vývojem DRM a digitální steganografie, vědního oboru, který se zabývá skrýváním informací.

Seznam literatury a informačních zdrojů

[1] Průsvitka. In: *Wikipedia: the free encyclopedia* [online]. San Francisco (CA): Wikimedia Foundation, 2001-, 9.3.2013 [cit. 2013-03-09]. Dostupné z: http://cs.wikipedia.org/wiki/Pr%C5%AFsvitka

[2] LEE, Insup. *Watermarking* [online]. 19.1.2000 [cit. 2013-03-09]. Dostupné z: http://www.cis.upenn.edu/~lee/00emtm553/watermark.ppt

[3] HÁJEK, Petr. *Trendy v technologii digitálních vodoznaků*. In: Http://www.root.cz [online]. 3.8.2010 [cit. 2013-03-09]. Dostupné z: http://www.root.cz/clanky/trendy-v-technologii-digitalnich-vodoznaku/

[4] Kryptologie: Univerzita Hradec Králové. RYŠÁNKOVÁ, A. *Steganografie* [online]. 2003 [cit. 2013-05-05]. Dostupné z: http://kryptologie.uhk.cz/81.htm

[5] Digital watermarking. In: *Wikipedia: the free encyclopedia* [online]. San Francisco (CA): Wikimedia Foundation, 2001-, 22.2.2013 [cit. 2013-03-09]. Dostupné z: http://en.wikipedia.org/wiki/Digital_watermarking

[6] AMIT6. *Watermark_life_cycle*. 5.1.2010. Dostupné z: http://upload.wikimedia.org/wikipedia/en/thumb/0/0e/Watermark_life_cycle.svg/800px-Watermark_life_cycle.svg.png

[7] POLÁŠEK, Roman. *Zabraňte krádežím - chraňte fotografie vodoznakem*. In: Stahuj.cz [online]. 11.10.2009 [cit. 2013-03-09]. Dostupné z: http://magazin.stahuj.centrum.cz/zabrante-kradezim-chrante-fotografie-vodoznakem/

[8] BRICHTA, Martin. *Úprava fotografie nástrojem Křivky - 1. díl.* In: Www.fotoradce.cz [online]. 05.08.2009 [cit. 2013-03-09]. Dostupné z: http://www.fotoradce.cz/blog/uprava-fotografie-nastrojem-krivky-1-dil-idc80

[9] OPRINCA, Andrei. *Create an invisible watermark in Photoshop*. In: Http://www.psdbox.com [online]. 6.5.2011 [cit. 2013-03-09]. Dostupné z: http://www.psdbox.com/tutorials/create-an-invisible-watermark-in-photoshop/

[10] *Seeing yellow* [online]. 2012[cit. 2013-03-09]. Dostupné z: http://seeingyellow.com/

[11] ADHIYA, K. P. a S. A. PATIL. *Hiding Text in Audio Using LSB Based Steganography* [online]. 2012 [cit. 2013-05-04]. Dostupné z: http://www.iiste.org/Journals/index.php/IKM/article/download/1782/1735

[12] DJEBBAR, F., B. AYAD, K. A. MERAIM a H. HAMAM. Comparative study of digital audio steganography techniques. *EURASIP Journal on Audio, Speech, and Music Processing*. 2012, vol. 2012, issue 1, s. 25. DOI: 10.1186/1687-4722-2012-25. Dostupné z: http://asmp.eurasipjournals.com/content/2012/1/25#

[13] Hiding Information in Text. HIP: Hiding Information Perfectly [online]. [cit. 2013-03-10]. Dostupné z: http://www.cs.virginia.edu/~wm2a/text.html

[14] MIKE. *Kontejner není kontejner*. In: TVFreak.cz [online]. 10.5.2005 [cit. 2013-05-16]. Dostupné z: http://www.tvfreak.cz/recenze-kontejner-neni-kontejner/600

[15] NOORKAMI, M. a R. M. MERSEREAU. *Digital Video Watermarking in P-Frames with Controlled Video Bit-Rate Increase* [online]. 2008 [cit. 2013-05-16]. Dostupné z: http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=04578707

[16] Kryptologie: Univerzita Hradec Králové. BERÁNEK, M., T. LÍPA a O. PODZIMEK. *Elektronický podpis* [online]. 2003 [cit. 2013-05-05]. Dostupné z: http://kryptologie.uhk.cz/54.htm

[17] DOSTÁLEK, Libor. *Velký průvodce protokoly TCP/IP: Bezpečnost*. 1.vyd. Praha: Computer Press, 2001, 565 s. ISBN 80-722-6513-X.

[18] *Understanding metadata* [online]. Bethesda, MD: NISO, 2004 [cit. 2013-05-20]. ISBN 18-801-2462-9. Dostupné z: http://www.niso.org/publications/press/UnderstandingMetadata.pdf

[19] Internetová bezpečnost a anonymita: Zachovejte si soukromí. *Metadata* [online]. 2012 [cit. 2013-05-29]. Dostupné z: http://anonymita.e-riki.net/?cat=4

[20] DENNIS, Anita. *Tvorba PDF pomocí Adobe Acrobat: průvodce pro profesionály DTP a pre-press.* Vyd. 1. Brno: Computer Press, 2003, xiii, 287 s. ISBN 80-722-6718-3.

[21] ADOBE. *Nápověda pro Acrobat: Nápověda a výukové lekce* [online]. 2013 [cit. 2013-04-24]. Dostupné z: http://helpx.adobe.com/cz/acrobat/topics.html

[22] ADOBE. *Zásady zabezpečení*. 2013. Dostupné z: http://help.adobe.com/cs_CZ/acrobat/using/images/se01.png

[23] CRT. *Historie Microsoft Office* [online]. 2007 [cit. 2013-04-26]. Dostupné z: http://www.ctr.cz/microsoft_office/historie_office.htm

[24] MICROSOFT. *Podpora: Office* [online]. 2013 [cit. 2013-04-26]. Dostupné z: http://office.microsoft.com/cs-cz/support