Využití hologramů pro vizuální zabezpečení osobních dokladů

Je možné rozlišit vizuální kontrolou originály od padělků během několika vteřin? Poskytují hologramy dostatečnou ochranu? Pokud ano, tak které hologramy a za jakých okolností?

Následující text se zabývá ochranou fyzických osobních průkazů proti padělání a hologramy. Nejprve zmíníme, proč jsou a nadále budou významným, i když často neprávem opomíjeným nástrojem autentizace a identifikace osoby. Budeme formulovat základní požadavky, které musí ochrana proti padělání splňovat, a probereme různé technologie, které jsou k dispozici. Druhá polovina článku se bude zabývat bezpečnostními hologramy jakožto nejpokročilejší technologií vizuální kontroly, jaká je v současné době k dispozici. Ukážeme si, jaký zde probíhá vývoj, že zastaralé hologramy nechrání dostatečně a shrneme obecné zásady, jaké musejí hologramy splňovat.

Požadavky na autentizační předmět

Jedna z klíčových a všeobecně akceptovaných bezpečnostních zásad říká, že autentizace osoby by měla být založena na třech faktorech: čím uživatel je (nějaký biometrický údaj), co ví (znalost nějakého hesla) a co vlastní (nějaká karta, token apod.).

Právě třetí faktor je v posledních letech výrazně podceňován. Spousta aktivit se točí kolem biometrie. Otázka hesel a zacházení s nimi se už stala téměř samostatným podoborem informační bezpečnosti. Ale pokud se řeší, jaký předmět je uživatelům vydáván, tak téměř výhradně z pohledu informačních technologií, tedy např. jaký čip by měl obsahovat a jaké šifrování použít. Jako by se úplně vytratilo ono základní intuitivní vizuální ověřování, které bylo po staletí na prvním místě. Člověk, který se chtěl dostat do nějaké klasifikované zóny, se musel prokázat správnou uniformou, správným odznakem a správným průkazem.

Možná se tak stalo v důsledku pocitu, že uniformy a průkazy jsou příliš snadno falšovatelné. Jenže technologie se vyvíjejí, takže v druhé dekádě 21. století je zase všechno jinak. Navíc se zdá, že současný trend informační bezpečnosti preferuje prostředky, které jsou pro uživatele přirozené a intuitivní, což opět nahrává vizuální kontrole.

Aby autentizační předmět hrál svou roli, musí být splněny dvě kategorie podmínek.

1) Musí být nemožné nebo alespoň velmi obtížné jej zfalšovat. Průkazy či karty, které lze okopírovat v každé kanceláři (nebo „jen“ vytisknout v profesionální tiskárně), jsou fakticky k ničemu.
2) Musí být velice snadno rozpoznatelné, zda se jedná o originál. Pokud by bylo zapotřebí zadávat číslo průkazu do nějakého rozhraní nebo by rozlišení vyžadovalo dlouhé a pečlivé zkoumání, ztratí se základní výhoda intuitivnosti.

Celková koncepce identifikačního průkazu se přitom odvíjí primárně od tří základních otázek:

- Z jakého bude materiálu? Tím jsou určeny i bezpečnostní prvky, protože některé prvky není možné na určité materiály připevnit. Otázce materiálu karty věnujeme Box 1.
- Jak bude vypadat personalizace? Jaké údaje o držiteli budou na dokladu uvedeny? Jak budou na kartu zapisovány?
- Jak bude vypadat proces vydávání?

Odpovědi jsou dány finančními možnostmi, potenciálním dopadem zneužití karty, ale i třeba tím, kolik karet bude vystavováno a jaká doba čekání je tolerovatelná. Pro úplnost uvádíme, že se nemusí striktně jednat o kartu, existují např. USB tokeny chráněné hologramem.

Nástroje vizuálního zabezpečení

Optické zabezpečovací prostředky, dnes využívané i na osobních dokladech, byly historicky většinou vyvinuty pro ochranu bankovek. V podstatě hned, jak se objevily první papírové peníze (resp. vládní směnky), objevily se také pokusy o jejich padělání. Americké kolonie, které vydáváním bankovek obcházely britský královský monopol na ražbu mincí, své papírové peníze chránily:

- vyhlášením, že padělání se trestá smrtí,
- dvoubarevným tiskem (vedle běžného černého inkoustu byl použit ještě dražší červený),
- obtiskem listu stromu s tím, že složitý předmět s jemnými vlákny se bude špatně napodobovat.

Obecně platí, že vydavatelé bankovek mívali k dispozici podstatně lepší vybavení než padělatelé, takže hlavní ochranou byl dostatečně kvalitní tisk. Jednu z mála výjimek představuje období americké občanské války, kdy padělatelé v severních státech pracovali s lepšími tiskárnami než konfederační ministerstvo financí, a padělky tudíž měly vyšší kvalitu než pravé konfederační bankovky.

Až po 2. světové válce došlo k tomu, že i velmi kvalitní tiskové technologie se staly všeobecně dostupnými. Vydavatelé bankovek začali masově nasazovat prostředky vizuální ochrany proti padělání, což bylo zpětně impulzem k jejich dalšímu rozvoji. O významu, jaký centrální banky přikládají této oblasti, svědčí např. skutečnost, že náklady na výrobu jedné pětilibrové bankovky činí sedm liber.

Co přichází po papíru **BOX 1**

Osobní doklady byly tradičně vyráběny z papíru. V 70. letech se objevily první plastové karty a dnes se už jen zřídka stane, že by někdo vydával třeba papírové klubové karty, natož důležitější doklady. I papírové cestovní pasy dnes obsahují plastové stránky. A některé centrální banky již uvedly do oběhu plastové bankovky. Plast je praktičtější, odolnější, omyvatelný, pohodlnější pro uživatele a je obtížnější jej kopírovat.

Nejlevnější variantou je PVC (především klubové průkazy, karty zákaznických věrnostních programů, zdravotních pojišťoven atd.). Pokročilejší karty se vyrábí z kompozitů, střídají se v nich různé vrstvy plastů nebo se jedná o proprietární materiály jednotlivých výrobců.

Po všech stránkách nejperspektivnější se ukazuje polykarbonát. Stárne tak pomalu, aby bylo možné garantovat dobu používání minimálně 10 let. Vydrží teploty od -100 do +135 C°. Má velmi dobré optické vlastnosti, lze do něj provádět nevratné zápisy laserovým paprskem (třeba fotografie a jméno držitele karty). Polykarbonát podporuje bezpečnostní prvky, např. různé bezpečnostní inkousty. Záporem je relativně vysoká cena. Určité problémy mohou být způsobeny také tím, že polykarbonát se špatně spojuje s jinými materiály, což vytváří těžkosti např. při přidávání hologramu z jiného materiálu nebo čipu.

Změny urychlily události 11. září 2001. Do té doby vydávala řada amerických států i jiné pokročilé země (včetně ČR) jednoduché průkazy z papíru nebo PVC přetažené laminační vrstvou. Takové řešení bylo jednoduché, levné a stačilo k ochraně proti hlavní skupině relativně primitivních padělatelů. Po útocích ale vzrostlo povědomí o tom, že možnost padělání dokladu totožnosti představuje obrovské riziko a že se možnosti padělatelů rychle zvyšují. V roce 2003 bylo vydáno ISO 2810:2003, o rok později schválil americký Kongres tzv. Real ID Act, v roce 2006 vyšla norma EU [5], v témže roce i norma Světové asociace civilního letectví (ICAO), která tuto oblast řeší v souvislosti se strojovým čtením pasů (ICAO 9303). Žádná ze zmíněných norem nepředepisuje konkrétní materiál, ale klade takové požadavky na odolnost a trvanlivost, že levné plasty vyřazuje ze hry. Soukromí vystavitelé, na které se uvedené normy přímo nevztahují, si osvojují stejné technologické změny s určitým zpožděním.

V podstatě všechny ochranné technologie, původně vyvinuté pro bankovky, jsou dnes používány i pro ochranu identifikačních průkazů. Jedná se zejména o následující:

Tisk iridescentními inkousty – tyto inkousty jsou duhově proměnlivé a je velmi obtížné je okopírovat. Můžete je najít na některých ceninách nebo bankovkách, kde jsou jimi vyvedeny speciální grafické ochranné prvky, tzv. giloše (viz obr. 1).

Tisk OVI inkousty – zkratkou OVI (Optical Variable Ink) se označují inkousty, které mění barvu v závislosti na úhlu světla dopadajícího na dokument. Ani tento druh tisku prakticky nelze kopírovat.

Tisk fluorescenčními inkousty – vytištěné nápisy nebo tvary nejsou viditelné při ozáření běžným světlem, ale objeví se při nasvícení ultrafialovým zářením.

Obr. 1: Jemné čáry, jimiž jsou vyvedeny, tzv. giloše, představovaly historicky hlavní ochranu proti kopírování.

O všech uvedených metodách tisku platí, že útočník není schopen bezpečnostní prvek přímo okopírovat. Pokud si ovšem pořídí tiskárnu s kompletním vybavením, může si koupit i bezpečnostní inkoust s potřebnými vlastnostmi a vytisknout velmi přesnou napodobeninu.

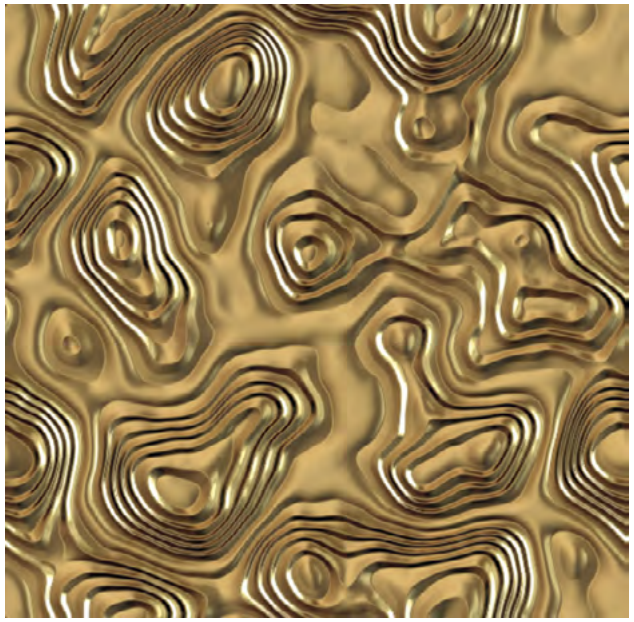
Další možností je bezpečnostní hologram. Nebudeme zdržovat čtenáře historií ani vysvětlováním technického principu. Připomeneme jenom, že výroba hologramů probíhá tak, že jemné difrakční struktury jsou pomocí raznice vytlačovány do nějakého materiálu, nejčastěji do plastové fólie. Na to se váže základní bezpečnostní otázka. Za jakých okolností je možné hologram padělat? Pokud má útočník k dispozici stejnou raznici, jakou byl vyroben původní hologram.

Způsoby vytváření raznice můžeme rozdělit do dvou skupin. Buď je skládána z nějakých standardizovaných bloků (nejpoužívanější je dot matrix), nebo je hologram do podkladu zapsán přímo – laserovým paprskem nebo svazkem elektronů.

Technologie dot matrix – grafik zadá požadovaný vizuální efekt a software vypočte pro každý jednotlivý pixel o rozměrech 10–20 mikronů parametry difrakční mřížky, na které se světlo láme a tvoří požadovanou iluzi. Pro každý pixel jsou určeny dva parametry – šířka mezer a orientace. Následuje fyzická výroba raznice. Metodou dot matrix je dnes vyráběna většina hologramů. Je to relativně snadné, rychlé a dostupné.

Z hlediska bezpečnosti ale narážíme na problém spočívající v tom, že zkušený útočník dokáže odhadnout, z jakých stavebních kamenů se hologram skládá, případně v některých částech parametry mřížky změřit difrakčním mikroskopem. Je tak možné rekonstruovat raznici a začít sériově vyrábět padělky hologramů.

Elektronová litografie – nejedná se vlastně o proces podobný tradiční fotografii, můžeme se dokonce setkat s tvrzením, že už se fakticky nejedná o holografii, ale o nanooptiku [1]. Velmi úzký fokusovaný svazek elektronů (šířka desítky



Obr. 2: Struktura hologramu vytvořeného metodou elektronové litografie. Algoritmy vytvářející difrakční struktury jsou natolik komplikované, že vytváří dojem nepravidelnosti. Není možné je reverzně odvodit z hologramu.

až stovky nanometrů) exponuje bod po bodu vrstvu rezistu nanesenou na křemíkovém substrátu. Následuje vyvolávání ve vývojce, kdy je rezist částečně vyleptán (citlivost rezistu závisí na předchozím působení svazku elektronů), a vzniká raznice. Také elektronový litograf pracuje s daty vytvářenými pomocí matematických algoritmů. Tyto algoritmy však jsou řádově složitější a není možné je odvodit zpět z hologramu [2, 3]. To je vidět i na velmi komplikovaných a zdánlivě nepravidelných strukturách hologramu (viz obr. 2). Elektronová litografie je tedy bezpečná, oproti metodě dot matrix je však řádově komplikovanější, a tudíž také nákladnější.

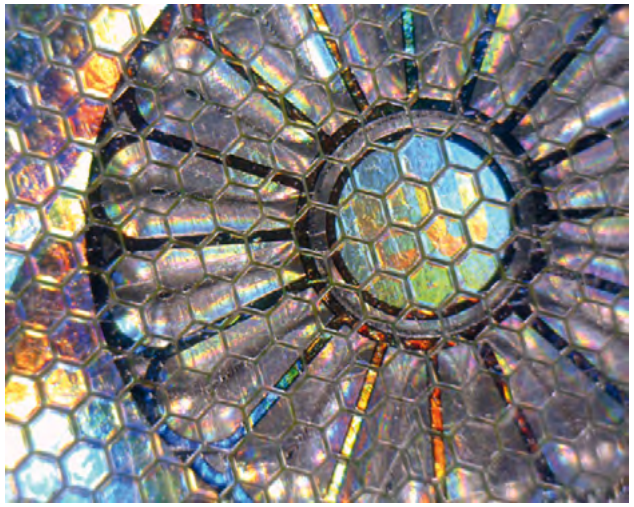
Vedle těchto dvou nejpoužívanějších metod existuje řada metod proprietárních. Liší se mírou obtížnosti zvládnutí a mírou bezpečnosti.

Možné způsoby útoku na hologram

Pokud není možné vyrobit stejný hologram, může se útočník pokusit o hologram s velmi podobným vizuálním efektem. I zde se hologramy navzájem výrazně liší. Čtenáři se již možná setkali s hologramy, kde veškerá grafika spočívá v tom, že když se změní úhel dopadajícího světla, tak např. stříbrná písmena zčernají. Patří do kategorie, kde sestavení velmi podobného hologramu je otázkou studentského cvičení. Proti tomu stojí složité hologramy s plastickými objekty, které rotují, jsou animovány, zanořují se, z pozadí vystupují jiné, případně se dokonce vynořují QR kódy. Podle toho, jak hologram naklápíte a v jakém úhlu jej osvětlujete, případně jakou barvou světla a zda jde o laserové světlo. Takové sofistikované hologramy jsou fakticky nenapodobitelné (viz Box 2 na následující straně).

Pokud není možné hologram zkopírovat ani napodobit, zbývá ještě třetí možnost. Vyjmout jej z průkazu a využít pro výrobu padělku. To vede k otázce, jakým způsobem je ochranný prvek ke kartě připojen. I zde existuje několik možností s různou úrovní bezpečnosti:

1) Hologram může být nalepen na kartu a přetažen krycí fólií. To je řešení poměrně jednoduché z hlediska výroby, nicméně zranitelné vůči vyjmutí hologramu. Variantou téhož je zatavení hologramu dovnitř polykarbonátové karty.



Obr. 3. Hologram (produkt Optaglio OVMesh Unlimited) je složen z miniaturních částí. Při vyjmutí z chráněného předmětu se rozpadne.

2) Další možností je hologram na samodestruktivní nálepce nebo samodestruktivní hologram. Vždy jde o to, že vrstva nemá samonosnost, takže po ztrátě opory (odlepení nebo vyjmutí z karty) se rozpadá. Byť i zde je přinejmenším teoreticky myslitelné, že by ji útočník před vyjmutím překryl nějakou nosnou fólií.

3) Nejbezpečnější je rozdělení hologramu do miniaturních částí (viz obr. 3), mezi nimiž jsou drobné mezery. Pokus o vyjmutí pak znamená nevratný rozpad na jednotlivé dílky.

Posledním zranitelným místem je proces výroby a vydávání karet včetně navázaných podpůrných procesů, např. evidence a skladování „polotovarů“. Zde je na výběr mezi řadou variant. Na jedné straně centralizovaná – osobní údaje jsou posílány na centrálu, kde se karty vyrábí. Tak tomu bývá např. u cestovních pasů. Tento centralizovaný model znamená velmi nízké riziko odcizení polotovarů a zneužití tiskáren, ale také ztrátu flexibility, což přináší rizika nová (uživatelé musí čekat na vystavení, spontánně uvádějí do provozu neautorizovaná náhradní řešení apod.). Druhou krajní variantou je umístění „laminovačky“ nebo laserového zapisovače na každou pobočku spolu se zásobou nedokončených karet. To je model velmi flexibilní, nicméně zase náchylný k odcizení či zneužití na místní pobočce. Může být také velmi nákladný, pokud by např. měla být každá pobočka vybavena laserovým zapisova-

BOX 2

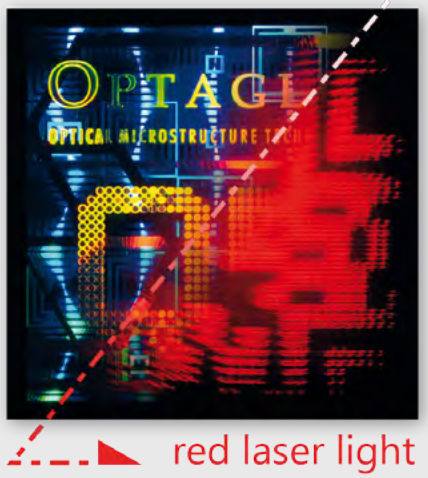
Vizuální efekty

Vytváření zajímavých optických iluzí není samozřejmým rysem holografie. I vizuální efekty jsou předmětem technologického výzkumu, podléhají patentové ochraně a řadu z nich nemůže napodobit ten, kdo nemá totožné přístrojové vybavení. V této souvislosti připomínáme, že neexistuje něco jako standardní stroj na hologramy. Špičkové firmy mají vlastní aparatury, které si přizpůsobily a využívají trochu jinak než konkurence.

Jako příklad uvádíme nejzajímavější vizuální efekty, jaké používá firma Optaglio:

- Iluzní 3D reliéf s matným povrchem, který je dobře viditelný i při nekvalitním rozptýleném světle (produkt Nanogravure).
- Iluzní 3D reliéf, který svítí ostrými barvami. Při otáčení hologramu se barvy mění podle úhlu dopadajícího světla (produkt Kinetic3D).
- Objekty, které se plynule posouvají v jiné ose, než je natáčen hologram (produkt Real3D).
- Krátké animace (produkt Real3D).
- Zdánlivě „běžný“ hologram. Po nasvícení světlem jedné konkrétní barvy nebo laserem QR ovšem vyjede z pozadí další objekt nebo QR kód (produkty Hidden3D a HiddenQR).

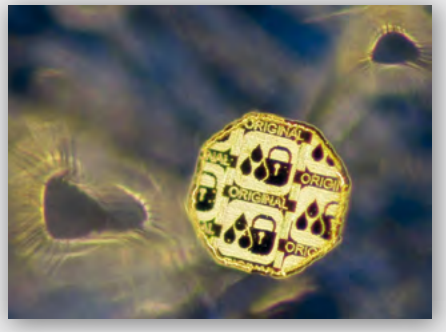
Využití takových možností vyžaduje výtvarníka specializovaného na hologramy, který dokáže vytvořit zajímavé dílko odpovídající grafické prezentaci vystavitele karty.



Mikrohologramy

Česká firma Optaglio přišla ještě s další možností, jak s hologramy pracovat. Vyvinula tzv. mikrohologramy – maličké částice kovu s hologramem na povrchu. Velikost částice určuje zákazník, ty nejmenší začínají na 40 mikrometrech. Mikrohologramy mají pravidelný tvar rovněž určený zákazníkem. Nejčastěji se objednávají šestiúhelníky a čtverce. Přes holografický povrch mohou být vyleptány alfanumerické znaky.

Pokud se hologramy používají v identifikačních kartách, bývají zataveny přímo do polykarbonátu. Pouhým okem je pak možné zkontrolovat přítomnost čehosi na způsob kovového prachu. S lupou zjistíte tvar, vyleptaná písmena a přítomnost hologramu. Pod mikroskopem pak můžete hologram prohlížet včetně všech detailů a vizuálních efektů.



čem. Mezi tím existuje řada kompromisů, např. koncentrace vystavování do několika center, decentralizovaný model s centrálním řízením personalizačních tiskáren apod.

Je tedy zapotřebí definovat proces tak, aby odpovídal konkrétním potřebám a situaci organizace. Připomínáme také, že je dobré věnovat dostatek pozornosti pořízení portrétních fotografií. Rozmazaný snímek ze studentských let není dobrou pomůckou pro autentizaci osoby.

Dostatek pozornosti musí být věnován i komunikaci. Aby ochranné prvky fungovaly, musí je uživatelé znát a musí vědět, co na identifikačních průkazech hledat. Stejně jako pokladník v bance nebo prodavačka v obchodě si občas pozorněji prohlédnou bankovku, protože jsou dobře instruováni, jak rozpoznat pravou od nepravé. Ostatně pro centrální banky je samozřejmostí, že když uvedou do oběhu novou bankovku, zveřejní zároveň také videa a další návody popisující ochranné prvky. S průkazy totožnosti by se mělo dít totéž.

Závěrem

V textu jsme ukázali, že osobní karta může výrazně zvýšit jistotu autentizace osoby, ovšem za předpokladu, že je dostatečně odolná vůči padělání. Formulovali jsme také požadavek, aby ověření pravosti karty bylo snadné, rychlé a intuitivní. V další části byly probrány různé možnosti a nástroje, jak chránit předměty proti padělatelům. Největší prostor byl věnován bezpečnostním hologramům. Zabývali jsme se jejich vlastnostmi a technologií jejich výroby z hlediska ochrany proti padělání. Závěrečná část článku pak zmínila navazující procesy – komunikaci a vydávání karet.

Výrobci bezpečnostních hologramů **BOX 3**

Na světě dnes působí desítky nebo možná dokonce stovky firem zabývajících se výrobou bezpečnostních hologramů. Naprostá většina z nich se zaměřuje na levné jednoduché hologramy vytvářenou technologií dot matrix, vesměs určené pro ochranu spotřebního zboží. Kromě nich najdete firmy se zajímavými, byť možná poněkud kuriózními inovacemi, jako např. čokoládové hologramy.

Nejvyšší třídě hologramů určených primárně pro bankovky, cestovní pasy a osobní průkazy dnes dominují tři firmy:

Kurz (Německo)
– jeden z největších světových výrobců obalových fólií zaměstnává 5 000 lidí, hlavně v Malajsii a Číně. V roce 2000 koupil Kurz malou švýcarskou firmu Kinegram zabývající se výrobou bezpečnostních hologramů a začlenil ji do svého portfolia.

OPTAGLIO (Česká republika)
– skupina lidí původně pracujících v Akademii věd se začátkem 90. let osamostatnila, založila s. r. o., později získala britského investora (s ním také název OPTAGLIO), nicméně charakterem zůstává českou firmou. Zaměřila se na elektronovou litografii a dokázala se v ní dostat do světové špičky. Její hologramy jsou využívány ve více než 50 zemích světa. Sídlí v Lochovicích u Berouna.

SURYS (Francie)
– korporace, která za posledních 30 let postupně provedla akvizici asi desítky firem zabývajících se výrobou bezpečnostních hologramů.

I v oblasti identifikačních karet platí, že technologická pokročilost útočníků roste, a je tudíž zapotřebí, aby obránci investovali do udržení náskoku.

Čestmír Hradečný
cestmir.hradecny@optaglio.cz

Čestmír Hradečný

Prom. fyz. Čestmír Hradečný, CSc., vystudoval fyziku na Běloruské státní univerzitě. V roce 1994 byl jedním ze spoluzakladatelů firmy Czech Holograms, s.r.o., která dnes působí pod názvem OPTAGLIO, s.r.o., a kde pracuje jako technolog.

POUŽITÉ ZDROJE

[1] GONCHARSKY A., DURLEVICH S..: E-beam origination technology: Current state and development prospects. In: Holography Times, Issue 19 (2012), str. 15–18
[2] MATĚJKA F.: Praktická elektronová litografie. Ústav přístrojové techniky AV ČR, Brno. 2012.
[3] MANFRINATO V.: Resolution Limits of Electron-Beam Lithography toward the Atomic Scale. American Chemical Society. 2013.
[4] RABIA R., EL HAJJI M., DOUSI H., HARBA R.: Evaluation of a Fourier Watermarking Method Robustness to Cards Durability Attacks. In: Image and signal processing. Springer International Publishing. 2014.
[5] Draft Resolution of the Representatives of the Governments of the Member States meeting within the Council on common minimum security standards for Member States' national identity cards. Council of European Union, 15356/06. 2006.