

A biztonsági nyomtatás

A DIGITÁLIS ADAT, A VÉDETT MÁRKA ÉS DOKUMENTUM, A CSOMAGOLT TERMÉK ÉS A FOGYASZTÓ VÉDELME

Eiler Emil

A vírustámadás, a hamisítás és a tudatos károkozás a mindennapjaink részévé vált! Mindenkinek van valami féltlenivalója, így személyesen mind érintettek lehetünk. Ez a cikk tehát mindenkihez szól! Abszolút és végleges megoldás nem létezik, mert a biztonság csak átmeneti állapot! A harc – amelynek a biztonsági nyomtatás egyik kiemelten fontos eszköze – olyan vég nélküli macska–egér játék, amelyben az egér a játékvezető! Tétlenül akkor sem ülhetünk! Mindig azt kell latolgatnunk, hogy mi okozza a nagyobb veszteséget, a védekezés többletköltsége vagy az annak hiányában fellépő kár. Ezt a cikket azért is érdemes végigolvasni, mert az alábbi védelmi eszközök – a nyomtatványok értéknövelt előállításával – extra profit szerzésre is alkalmasak!

Az információt előállító, tároló és feldolgozó számítógépek, az adatokat továbbító hálózatok és az általuk kezelt digitális adatok szüntelenül ki vannak téve az informatikai bűnözés (*Cyber Crime*) különféle támadásainak. A nyomtatott termék elleni támadások legismertebb formája a pénzhamisítás, amely egyidős a pénz megjelenésével. Veszélyeztetve vannak az írott, a nyomtatott, másolt adatok, a védett dokumentumok, a nagy értékű csomagolt és márkás termékek is. A világkereskedelmi forgalomban lévő termékek és árucikkek 5–10 százaléka hamisítvány. A digitális és nyomtatott információ elleni támadások főbb technikáit a 1. táblázat foglalja össze. A 2. táblázat a kiemelten veszélyeztetett nyomtatott termékcsoportokat ismerteti. A támadások elleni védekezés eszközeit pedig a 3. táblázatunk tartalmazza.

1. táblázat. Az információbiztonságot veszélyeztető főbb tényezők

Magyar megnevezés	Angol megnevezés
Adatcsere, kicserélés	Data Swapping
Crackertámadás (betörés)	Cracker Threat
Csalás, megtévesztés, félrevezetés	Deception
Dézsmálás (csomagé)	Pilfering
Egyszerre több helyre eljuttatott kéretlen küldemény	Spam
Fénykép-/ábracsere	Photo/picture substitution
Fogyasztási termékek hamisítása	Counterfeiting of consumer goods
Kalóztámadás	Hacker Threat/Piracy
Hamisítás (pénz /okmány, termék)	Forgery, Fake
Hitelkártya-hamisítás	Credit Card Fraudulance
Hozzáférésgátlás	Data Access Hindrance
Illetéktelen használat	Unauthorized Usage
Illetéktelen másolatkészítés	Unauthorized Photocopying
Kémprogram	Spyware
Kép-/ábrahamisítás	Photo Tampering
Eltulajdonítás, lopás	Theft
Másolás, duplikálás	PhotoCopying, Duplication
Hamisítás (pénz); megmásítás (okmányé, dokumentumé)	Tampering/Tampery

TRENDEK

Tendenciák, a folyamatban lévő fejlesztések és a jövő forgatókönyvei

Az IDTechEx előrejelzései szerint, a digitális és nyomtatott információ elleni támadások célja korábban a virtuskodás, a számítástechnikai ismeretek fitogtatása volt. Már most is érezhető, de a jövőben még kifejezettebben **a legnagyobb mértékű erkölcsi és anyagi károkozás, az ipari, kereskedelmi vonatkozásban pedig a megtámadott fél lejáratása, piaci ellehetlenítése és a haszonszerzés szerepel az elsőleges célok között!**

A nyomtatott biztonsági termékek piaci folyamatai a következőképpen alakulnak: folytatódik a küzdelem a kibernetikai bűnözés és a hamisítás ellen, az adat-, a márka- és a csomagolttermék-biztonság érdekében is; terjed az intelligens csomagolóanyagok (*Smart Packaging Materials*), a rádiófrekvenciás címkék (*RFID labels*), a függőcímkék (*RFID tags*), a mikrokódot tartalmazó, termékbe keverhető mikrocímkék (*Micro Taggants*) és a diagnosztikai címkék (*RFID Diagnostic Tools*) használata a szükséges távleolvasó készülékekkel együtt. (Magyar Grafika, 2004/7. 7–14. old.)

Ugyancsak az említett forrás becslései szerint, 2007-ben már közel kétmilliárd darab RFID-címkét hoznak forgalomba. Ezek forgalmi összértéke világviszonylatban – a hardvert, rendszereket és integrációt is beleértve – közelíti az ötmilliárd dollárt, amiből az USA-ban 58,4%, Európában pedig 33% kerül felhasználásra. Előrejelzések szerint az RFID-forgalom 2017-re eléri a 26,88 milliárd dollárt. (Részletesen lásd a www.idtechex.com/products/en/ honlap *Total RFID Market Projections 2007–2017* és az *RFID Forecasts, Players & Opportunities 2007–2017* linkjein.)

Az RFID-termékek főbb felhasználási területei ma: az árucikkek automatikus azonosítása; a csomagolt termékek és árucikkek ellátóláncon belüli nyomon követése, diagnosztikai feladatok ellátása, biztonsági iratkezelés, személyazonosítás, jogosultság-ellenőrzés, bűnüldözés és dokumentumvédelem.

Folytatódik a környezeti hatásoktól sérülékeny, érintkezésmentes és takart állapotban nem működőképes vonalkód kiváltása az RFID-technika és az automatikus távleolvasó szerkezetek segítségével. Alkalmazzák a termékcsomagok rongálásának, feltörésének, dézsmálásának, eltulajdo-

nításának és a hőérzékeny csomagolt termékek hőmérséklet-változási körülményeinek, esetleges megromlásának megakadályozására, dokumentálására is. Továbbá használják automatikus raktárkezelésre, távleltározásra és az áruházi polcok automatikus hiánypótlására, a gyártási folyamatok távfelügyeletére és a hulladék anyagok újrafelhasználásának nyomon követésére is.

Felgyorsul a globális biztonsági és megbízhatósági rendszerek kiépülése is. Új adatmentési, archiválási és titkosítási eljárások jelennek meg. Írishirosztika, digitális aláírás, digitális ujjlenyomat, új típusú digitális vízfestőszköz szolgálja a kibernetikai bűnözés visszaszorítását. Új típusú médiákat, információhordozó alap- és segédanyagokat fejlesztenek ki. Már csak viszonylag számítanak újnak a **humán biometrikai alkalmazások**, amelyeket részletesen ismertettünk.

Ez az írás az említett témákról szól. Megjegyzendő, hogy minden virtuális vagy létező anyag, eszköz, eljárás, termék és digitális adat – sőt még a leírt gondolat is – potenciális célpontja a *1. táblázatban* felsorolt támadásoknak!

A biztonság (Security) és a veszélyeztetés nélküli állapot (Safety) fogalma esetünkben a digitális, a nyomtatott és másolt adatbiztonságot, a márka- és a csomagolttermék-biztonságot (*Digital and/or Photocopied/Printed Data Security/Information Security*) jelenti a jogosulatlan hozzáférés, az illetéktelen módosítás, a részleges vagy teljes törlés, rongálás, illetve a megsemmisülés ellen. Más szóval: az adatok/termékek bizalmosságának, rendelkezésre állásának és sértetlenségének a teljes körű védelmét.

Olvasnivalók: IBM előrejelzések a biztonságot veszélyeztető károkozásokról (IBM Predicts2006 Security Threat Trends: www.eweek.com/article2/0,1895,1913864,00.asp); **A biztonság jövője: kétféle forgatókönyv** (*The Future of Security. Scenario: One & Two*: www.cio.com.au/index.php/id/); **Biztonsági trendek 2007-ben** (*Features: Trend sin Security For 2007*: www.itesecurity.com/features/security-trends-2007-010807/); **Az internetbiztonság jövője, pdf** (*Future Trends In Internet Security*: <http://csdl2.computer.org/comp/proceedings/>); **Biztonsági nyomtatás: A folyamatban lévő fejlesztések** (*Security Printing: Recent Developments*: www.poles.tarltd.com); **Biztonsági nyomtatványok nemzetközi jegyzéke** (*International Security Products*: www.isp-vft.com); **A biztonsági nyomtatás összefoglaló ismeretanyaga** (*Security Printing Resources*: www.security-printing.co.uk).

2. táblázat. Fokozott védelmet igénylő nyomtatványok és dokumentumok

- ◆ Adóügyi dokumentumok: zár- és adójegy
- ◆ Bizalmi dokumentumok (Fiduciary Documents): tanúsítvány, bizonylat (Voucher)
- ◆ Biztonsági okmányok, útiokmányok (ID & Travel Documents): személyazonossági és megszemélyesítő dokumentumok. Kártyák, vasúti és légi menetjegyek, vezetői engedélyek, zálog- és értékpapírok, szavazólapok
- ◆ Egyéb rendeltetésű nyomdai eredetű (kézirat, fotó, ábra), dokumentumok és nyomtatványok: belépőjegyek, ajándékutalványok, bélyegek, iskolai végzettségről igazolások
- ◆ Értékcikkek: bélyeg, részvény, értékpapír, jegyek, belépők, vásárlási utalványok és ajándék sorsjegyek, csekkfüzetek
- ◆ Kártyák: bank-, hitel-, mobilfeltöltő. Személyazonosító-, bank-, telefonkártyák
- ◆ Márkavédelmi és csomagoltermék-védelmi célú nyomtatványok: csomagolt fogyasztási cikkek (kiemelten gyógyszer) címkéi, csomagolóanyagai, zárjegyek, eredetiséget bizonyító (Authentication) eszközök, használati utasítások, szavatossági és garancialevelek
- ◆ Nyomtatott értékdocumentumok (Printed Value Documents)
- ◆ Okmánybiztonsági dokumentumok
- ◆ Pénz és pénzhelyettesítő nyomtatványok, banki nyomtatványok: bankjegy, csekk, részvény, bankkártya, átutalási dokumentumok, hitelkártyák
- ◆ Szerencsejáték-nyomtatványok: sorsjegyek, totó-, lottó- stb. szelvények
- ◆ Szerzői jogvédelemmel összefüggő dokumentumok
- ◆ Tulajdonjog-védelmi rendeltetésű nyomtatványok: lakás, gépkocsi tulajdonigazolások
- ◆ Üzleti és reklámnyomtatványok

AZ ADATBIZTONSÁGI ÉS VÉDELMI ESZKÖZÖK RENDSZERE

A védelmi eszközök – az észlelhetőség módjától és mértékétől függően – az alábbi csoportokba sorolhatóak:

- ◆ **szabad szemmel észlelhető** (*Overt Security Solutions*) típusok;
- ◆ **szabad szemmel nem észlelhető**, nagyítóval, mikroszkóppal érzékelhető (*Covert Security Solutions*) típusok, például a nyomtatott mikrokarakterek, mikrokódok;
- ◆ **csak gépi eszközök segítségével rekonstruálható** karakterekből, vonal-, szín-, mágneses vagy egyéb kódjelsorozatokból álló, megfelelő sugárzások (lézer-, UV-, infra-, rádió-, röntgen- és elektronsugár) segítségével, továbbá kémiai reagensekkel láthatóvá tehető karakterek és jelek.

Miután a digitális adatok, nyomtatványok és másolt dokumentumok ellen támadást intézők is folyamatos fejlesztéseket hajtanak végre, a támadások eszközei és módszerei folytonos változásban vannak. Ezért a védelmi eszközök sem lehetnek állandóak, hanem – a vírusirtó programokhoz hasonlóan – folyamatos frissítésükre van szükség.

A BIZTONSÁGI NYOMTATÁS (SECURITY PRINTING)

A védelmi eszközök alkalmazástechnikája

A *biztonsági nyomtatás* a fokozottan veszélyeztetett digitális, nyomtatott és másolt adat, a márka és csomagolt termékek támadásokkal szembeni védettségének folyamatos fenntartására irányuló eljárások összessége. Az egyéb nyomtatóeljárásoktól ez, főként a különleges biztonsági alap- és segédanyagok, a biztonsági nyomathordozók és nyomtató-/másolóeljárások, továbbá a speciális adatbiztonsági elemek alkalmazásában, az eredeti előállításában, a formakészítési eljárásokban és a termelőberendezések konstrukciós megoldásai-ban különbözik, a következők szerint.

BIZTONSÁGI ALAP- ÉS SEGÉDANYAGOK (*Security Rawmaterials & Auxiliary Products*)

Biztonsági festékek, pigmentek, tónerek, színezékek, lakkok és védőrétegek

Anti Forgery/Anti Counterfeit/Anti Thread Security Inks, Pigments, Dyes, Toners, Varnishes, and Covering Materials

Lapunk 2006/5. számában ezzel a témakörrel részben már foglalkoztunk. Az eltelt idő alatt azonban

3. táblázat. A biztonsági nyomtatás főbb védelmi anyagai és eszközei

- ◆ Biztonsági nyomathordozók: papír, karton, fémek, filmek, fóliák, védőbevonatok
- ◆ Digitális vízjelek: a papírba betervezett biztonság
- ◆ Biztonsági szálak és pelyhek
- ◆ Biztonsági festékek, pigmentek, tónerek, nanotermekek, lakkok, és egyéb nyomtatható bevonatok
- ◆ Különleges biztonsági nyomtató-, másolóeljárások és módszerek
- ◆ Nyomtatott grafikai és digitális biztonsági elemek, pl. Guilloche
- ◆ Optikai és nem optikai holografikus és optikailag változó eszközök
- ◆ Regisztrált képek, biztonsági elemek, logók
- ◆ Szelektíven, foltokban vagy teljesen „metallizált” felületelemek
- ◆ Másolásvédelmi megoldások, másolásvédtett nyomtatványok előállításának lehetősége
- ◆ Nyomtatható kódok: vonalkód, színkód, számkódok, mágneses, digitális kód
- ◆ Termékbe keverhető színkódok, MicroTaggant-megoldások
- ◆ Változóadat-nyomtatás (sorszámozás, változóképek)
- ◆ Másolásvédelmi elemek (Anti Copying Marks)
- ◆ Digitális aláírás
- ◆ Optikai mikrostruktúrák, mikroszövegek, mikroképek
- ◆ Csak gépileg olvasható elemek
- ◆ 3D-megoldások alkalmazása
- ◆ Változóadat-nyomtatás (sorszámozás, számkódok, megszemélyesítés)
- ◆ Biztonsági záró elemek
- ◆ Biometrikus eljárások
- ◆ Elektronikus védelmi megoldások: RFID, nyomtatható elektronikák (OLED), beépített mikrocsipek
- ◆ Nyomtatás és másolás után alkalmazható biztonsági eszközök
- ◆ Márka- és nagy értékű csomagolttermék-védelmi megoldások
- ◆ Nyomtatott banktechnológiai megoldások
- ◆ Copyright jogvédelmi megoldások
- ◆ Az alkalmazható biztonsági megoldások, eszközök kombinált használata

új anyagok, újabb ismeretek, termékcsoportok és alkalmazások láttak napvilágot, ezért indokolt e tanulmány keretében ismét áttekinteni az új helyzetet, a következők szerint.

Optikailag változó/színváltó festékek (*Color Change/Changing Inks; Color Shifting Inks; Optically Variable Printing Inks, OVPI*). Megszáradt rétegeik a megvilágító sugár természetétől, beesési szögétől és a szemlélés irányától függően, továbbá kémiai, hő-, illetve mechanikai behatásra színárnyalat-változással reagálnak.

Termokróm festékek (*Thermochromic/Thermochromic/Chroma Inks; Heat Sensitive Inks*). A folyékony kristály és a hőmérséklet-érzékeny *Leuko* színezék tartalmú száraz rétegük hőhatásra, hozzáérésre – tartósan vagy átmenetileg – színessé válik vagy megváltoztatja eredeti színét. Rejtett vagy szabad szemmel látható üzenetek (pl. *Érvénytelen!/Lejárt!/Hamisítvány!/Nem valódi másolat!/Nem hiteles!*) automatikus megjele-

nítésére képesek az illetéktelen másolaton. A kereskedelmi termokróm festékek 11 alapszínváltozatban kaphatóak.

A **fotokróm festékek** (*Photochromic Inks*) szintén láthatatlanok, de UV-besugárzás hatására láthatóvá válnak. Többek között a papírpénzek, a bank- és telefonkártyák, részvények gyártása során kerülnek alkalmazásra.

A **fluoreszkáló (fluoreszcens) nyomtató-, másoló-, bélyegzőfestékek** (*Fluorescent Inks*) a besugárzó fény gerjesztő hatására a besugárzás időtartama alatt különböző hullámhosszúságú fényt bocsátanak ki. Több változatuk ismert: a **Bi-fluoreszcens festékek** a 365/254 nm tartományban az UV-sugárzás hatására eltérő színekben fluoreszkálnak, könnyen ellenőrizhetőek és nehezen reprodukálhatóak. A **Trifluoreszcens** változatuk három különböző hullámhosszúságú UV-sugárzás hatására eltérő színekben fluoreszkál.

Hamisítás elleni jelölésre, színekódnyomatásra, márkavédelemre alkalmas anyagok. Csak optikai fehéritőmentes papír használata esetén működőképesek! Az ilyen típusú festék lehet teljesen láthatatlan, és a fényessége, illetve a színe UV-besugárzás hatására válhat szabad szemmel érzékelhetővé.

Infra-fluoreszcens (IF) festékek (*Infra-Fluorescent Inks*). Jelenlétük műszeres vizsgálattal mutatható ki. Ilyenek például az **Anti-Stokes** infravörös fényvel gerjeszthető és zöld színű fényt sugárzó festékek is, amelyek ideálisak rejtett információk elhelyezésére és gépi ellenőrző rendszerek kialakítására. (Bővebbet a www.allaminyomda.hu weboldalon.)

A foszforeszkáló/foszforeszcens festékek (*Phosphorescent Inks*) a besugárzó fény vagy UV-gerjesztés intenzitása és időtartama függvényében a sötétben még egy ideig világítanak.

Az **UV lumineszcens festékek** (*UV Luminescent Inks*) a bennük lévő pigment hatására, az UV-besugárzás után is még egy darabig világítanak (lumineszkálnak), és pedig a besugárzó fény hullámhosszától függő színekben. Célszerű vas-tag rétegben nyomtatni és a használat előtt mindig alaposan felkeverni őket, mert a pigmentjük ülepedésre hajlamos.

Infra fluoreszcens (IR) festékek (*Infra Fluorescent Inks / Infrared Inks*). A felsorolt színváltozásokat az infravörös sugárzás hatására hozzák létre.

Nulladrendű színváltó festékek (*First Order / Zero Order Security Inks*). A száraz festékrétegükben a belső rácsszerkezet és a létrejött vékonyrétegek együttes hatására, tükrözéssel, a megvilágítás minőségétől és a szemlélés irányától függően, a természetben nem létező színhatások jönnek létre.

A **kaméleon festékekkel** (*Cameleon Inks*) készült biztonsági nyomatok mozgatás hatására megváltoztatják a színüket.

Metamer-keverék festékek (*Metamer-mix Inks*). A különböző megvilágítás hatására eltérő színben megjelenő festékek. Másolásnehezítő/-gátló tulajdonságú anyagok, amelyek papírpénz, részvény és bankkártya gyártása céljára használhatóak.

Szikkasztó imitáló festékek (*Glittering Inks*). Fémes benyomást keltő, felvillanásokat imitáló *effektfestékek*. Ezek is másolásnehezítő, képesség- és másolatminőség-rontó hatású anyagok. Átlátszó színes vagy színtelen rétegükben tükröző pigmentet tartalmaznak.

Fémrészecskéket tartalmazó festékek (*Metal Inks*). Másolásnehezítő/-gátló nyomtatványok készítésére használható gyöngyházfényű anyagok.

Fémhatású festékek (*Metallic/Metalloid Inks*). Kitűnő nyomtathatósági tulajdonságú, fémfóliabenyomást keltő, aranyetál, ezüstetál, bronzetál színárnyalatú vagy tetszőlegesen színezett átlátszó rétegben csillogó fémrészecskéket tartalmazó festékek.

Vezetőképes/villamos vezetőképeségű/konduktív fémfestékek (*Conductive Metallic Inks*). Rádiófrekvenciás címkék, nyomdagéptermi módszerekkel előállítható integrált áramkörök gyártására szolgáló, magas fémtartalmú vagy vezetőképes polimer termékek. Utóbbiakat már korábban is használták a nyomdaiparban a felület anti-sztatikussá tétele céljából, de eddig tökéletesen átlátszó festék – az Agfaén kívül – még senkinek nem állt rendelkezésére. Az Agfa ilyen típusú terméke szitanyomatásra korábban nem terjedt el. A mobiltelefonok átlátszó billentyűinek fejlesztése során adódó lehetőség elvezetett a szitanyomatásra alkalmas transzparens, vezetőképes festékek gyártásához is. Vezetőképes bevonatok, gyártói és termékei a www.thomasnet.com/products/conductive-coatings és a **Transparent Conducting Screen Printing Inks**: www.idtechhex.com honlapokon találhatóak. Utóbbi festéktípus biztonsági nyomtatás céljaira széles körben alkalmazható.

Mágneses festékek (*Magnetic Inks*). Mágneses rendszerű leolvásokkal, karakterfelismerő berendezésekkel (*Magnetic Ink Character Recognition, MICR*) érzékelhető festéktípus. Mágneskód és csak géppel rekonstruálható mágneses jelek elhelyezésére alkalmasak. (Bővebbet a www.barcodersource.com/micr/shtml és a www.troygroup.com/SecurityPrinting/Products/micr.asp weboldalon.)

Dörzsérzékeny/ledörzsölhető/lekapható festékek (*Erasable Ink*). Alacsony tónusértékű összefüggő vagy rácsszerkezetű háttérként nyomtatva, vizuálisan egyértelműen jelzik, ha valaki megpróbálja megváltoztatni a nyomtatott adatokat. Előfordulhat, hogy már a színes másoló hőjétől is leválik a rétegük. Többféle színben gyártják, és kapható a fluoreszkáló változatban is. Hasonló anyagot használnak a kaparós sorsjegyek gyártására is.

A nyomathordozóba mélyen beszívódó festékek (*Penetrating Inks*). Az ilyen festék nyomata a dokumentum vagy pénzfény blokk hátoldalán



Mikroszöveg rácsból létrehozott CMYK kép (MICON)

is megjelenhet, kizárva ezzel a hamisítás lehetőségét.

Reaktív festékek (Reactive Inks). Olyan festékcsalád megnevezése, amelynek tagjait az jellemzi, hogy valamely fizikai, kémiai, mechanikus, sugárzóenergia, pl. hőhatásra fény-, színgyengüléssel, -eltűnéssel vagy színváltozással reagálnak.

Oldószerérzékeny biztonsági festékek (Solvent Sensitive Security Inks, Chemical Solution Reactive Inks). Az e festékekkel készült nyomatok gyengén sárga fényvel fluoreszkálnak, de fényük oldószer hatására jelentősen felerősödik, ezért a dokumentumhamisításra, jogosulatlan adattartalom-változtatásra irányuló kísérletet hamar felfedezhetővé teszik.

Vízalapú színehagyó (fugitív) festékek (Water Based Fugitive Inks; Water-Fugitive Inks). Ezek is oldószerérzékenyek, de azzal a különbséggel, hogy a víz vagy bármely vizes oldat nem erősíti a színt, hanem elmaszatolja, kihalványítja a nyomatképet, jelezve ezzel a dokumentumot ért hamisítás szándékú beavatkozást.

Transzparens festékek (Transparent Security Inks). Áttetsző, átlátszó, láthatatlan szintetikus rétegük védőhatást fejt ki, de tartalmazhat olyan rejtett üzenetet is, amely csak valamilyen kémiai, dörzsölés, oldószer, hő vagy más sugárzóenergia hatására – például fluoreszkálással – válik láthatóvá.

Szabad szemmel láthatatlan és eltűnő festékek (Invisible Inks). UV- vagy IR-fluoreszcens festékek, ezért nevezik őket láthatatlan festékeknek.

Sötétben a gerjesztő sugárzás utal a festék jelenlétére és a rejtett üzenet vagy kód megjelenítésére. Viszonylag olcsó és sokféle színben kapható termékek. A *Nude Ink* és a *Glowe-in-the-Dark (GID) Inks*, márkájú „meztelen”, illetve „sötétben világító” elnevezésű termékcsalád jó példája az ilyen típusú alkalmazásnak. Többféle típusa ismeretes. A skóciai *Andrews Egyetem* bizonyította, hogy az anyagnak létezik egy olyan láthatatlan állapota is, amely a fény elterelésével idézhető elő. Az *eltűnő* és a *valóban láthatatlan festék* tehát már nem illúzió. Katonai célokra a láthatatlan dokumentumok és eszközök kifejlesztése már folyamatban van. (Bővebbet a http://en.wikipedia.org/wiki/Invisible_ink weboldalon.)

Lézerrel kódolható festékek és lakkok (Laser Codable Inks & Varnishes). Színváltó festék, lakk, lamináló és felrétegezzhető, nyomtatható anyagok, amelyeket csomagoló gépsoron történő alkalmazásra fejlesztettek ki. Víz- és szerves oldószer alapú változatban kaphatóak.

Biometrikus festékek (Biometric Inks). A genetikai információk átörökítő anyagát, a DNS-t (angolul *DNA*) utánzó részecskéket tartalmazó nyomó-, bélyegző-, másolófesték, amely gépileg leolvasható, kémiai oldattal pedig reagáltatható. A különböző dokumentumok eltérő biometrikus tulajdonságokat hordozó festékekkel jelölhetőek meg. Az ellenőrzés eredményének értékelését csak specialista végezheti, és a kapott vizsgálati eredményt hitelesíteni is kell.

Elektronikus festékek (E-Inks). Folyadékban diszpergált, pozitív töltésű *fehér* és negatív töltésű *fekete* részecskéket tartalmazó mikrokapszulából álló anyag, amely a ráható mágneses vagy villamos erőter polaritásától függően válik fehérre, illetve feketévé, annak síkbeli eloszlásától függően pedig értelmezhető vizuális információvá.

Folyékony rádiófrekvenciás (RFID) festékek (RFID Ink Solutions). A *Cross ID Communication Materials* által kifejlesztett anyag az általa leadott rádiófrekvenciás jelek révén azonosítja azt az anyagot, terméket, amelyhez hozzákeverik. Nyomtató- és másolófestékbe keverten, hamisíthatatlan, biztonsági nyomdatermék előállítását teszi lehetővé. (www.intertechpira.com)

Másolásnehezítő/másolásgátló anyagok (No Copy Inks/Hard to Reproduce Inks/CopyProof Inks & Materials). Olyan anyagok, amelyeket a legtöbb szkennel, másoló, nyomtató, fényképezőgép nem érzékel, ezért hatékony másolás- és hamisításgátló hatásúak.

Az **Invisible Taggant Ink** biztonsági festék védett termékbe keverhető, csak mikroszkóppal észlelhető méretű (*Micro Taggant*) olyan részecskét tartalmaz, amelynek minden darabja kódot képvisel.

Biztonsági nyomathordozók

Természetes és mesterséges alapanyagú papír, karton, textil, bőr, film, fólia, fémréteg és többrétegű szendvicsszerkezetek

Ezt a témakört a részletes felsorolás ellenére, az egyszerűség kedvéért, a következőkben a papírok és kartonok példáján tekintjük át.

A biztonsági nyomathordozók (*Security/Safety Paper/Board; Print Media, Copy Free Media; No-Print Media*), olyan anyagok, amelyek felépítése, valamint fizikai, kémiai és nyomtathatósági tulajdonságai következtében az alábbi jellemzőkkel rendelkeznek:

- ◆ az előállításához olyan bonyolult és költséges technológiákat igényelnek, amelyek az engedély nélkül előállító/felhasználó számára – technikailag, műszakilag és/vagy gazdaságilag is – lehetetlenné, megvalósíthatatlanná teszik a gyártást, az alkalmazást;
- ◆ az engedély nélküli hozzáférés esetén a nyomathordozóként történő felhasználást, továbbá a másolással/szkenneléssel történő duplikálást, hamisítást, a védett információ tartalom megváltoztatását, sokszorosítását *felfedezhetővé teszik*.

A biztonsági célok elérése érdekében a gyártók részére különféle kémiai, optikai, mechanikai felületnemesítő és másolás, szkennelés ellen védő rétegek, bevonatok, lamináló filmek, fóliák, az anyag felületén elhelyezhető vagy a nyomathordozóba beépített ún. *biztonsági elemek* állnak rendelkezésre. Ezek egy részét itt egyenként, külön is tárgyaljuk, de a gyakorlatban az alkalmazásukra – a fokozott biztonság érdekében – általában párhuzamosan kerül sor, a következők szerint.

Optikailag változó felületű biztonsági nyomathordozók

A festékekkel foglalkozó fejezet részben az UV- és IR-fluoreszcencia, lumineszcencia és a foszforeszcencia jelenségével kapcsolatos megállapítások a nyomathordozók vonatkozásában is érvé-

nyesek. Ezért a festékekhez hasonlóan beszélhetünk színváltó, UV- és IR-fluoreszcens, lumineszcens, illetve foszforeszcens nyomathordozókról is (*UV/IR Substrates*).

Termál papírok (*Thermal Security Papers*). A másolás során keletkezett hő vagy nyomás hatására színváltozással hívják fel a figyelmet az illetéktelen beavatkozásra, megnehezítve ezzel a hamisítók munkáját.

Kémiai védőréteggel ellátott papírok (*Chemically Coated Papers*). A fluoreszkáló/lumineszkáló/foszforeszkáló/pH-módosító/lekarparható külső védőréteggel papírgyártmányok másolhatósága, szkennelése nagyon megnehezített vagy eredménytelen. Hasonló a helyzet, ha a hordozó maga az anyagában színezett és/vagy kémiaileg módosított.

Hidegen/melegen laminált felületű nyomathordozók, nyomatok és másolatok (*Laminated Substrates, Prints and Copies*). Az illetéktelen másolás, szkennelés, hamisítás ellen a nyomtatott, másolt és fényképezett információ védelmére alkalmazott optikailag változó fólia- és fémrétegek igen hatékony nyomtatott információvédelmet biztosítanak.

Beépített biztonsági rostokat, textil- vagy fémszálat, fonalakat, pelyheket tartalmazó papírok (*Embedded/Internal Security Threads, fibres, flakes, planchettes*). A rendszerint szemmel is látható, keverten többféle színű betétanyagok alkalmazása a papír alapú okmányok biztonságosabbá tétele érdekében alkalmazott megoldás. Az Állami Nyomda ilyen célra például különféle méretű, hosszúságú, Dtex számú, színtelen, színes, UV-, illetve IR-fluoreszcens és nem fluoreszkáló, poliamid és viszkóz alapú rostokat, holografikus biztonsági száalakat kínál. Felületük lehetőséget ad rejtett, titkos jelek, szövegek felvitelére is. (Az eljárás neve *Encryption*, azaz titkosítás, amely meggátolja a nyomtatott adathoz az illetéktelen hozzáférést.) A titkosító kódoláshoz az *USA Data Encryption Standard*-ben meghatározott valamely *kulcs* szükséges. Enélkül a visszafejtés is lehetetlen. A biztonsági száalal védett hordozóra készült nyomdatermékeket rendkívül nehéz vagy csak nagyon költséges eszközökkel lehet másolni, szkennelvel feldolgozni.

Rejtett jeleket tartalmazó papírok. A hagyományos papírra nyomtatott és gyakran hamisított nyomtatványok ellenőrzésére alkalmazott megoldás. Segítségével a papírhoz érintett kézi ellenőrző eszköz egyértelműen kimutatja a hamisítást.

sítás tényét. Másolás vagy szkennelés alkalmával a másolaton megjelenhet többnyelvű üzenet, például a *VOID* szó, ami azt fejezi ki, hogy a másolat hamis!

Biztonsági tollal írt láthatatlan jelöléseket tartalmazó papír (*Invisible Marks on Paper made with Security Pen*). Hamisítás elleni védelmet biztosítanak a papírra olcsón beszerezhető biztonsági tollal írt jelölések is, amelyek szabad szemmel nem, csak megfelelő eszközzel tehetőek láthatóvá. (www.securitymanagement.com/library/001540.html)

Szendvics szerkezetű nyomathordozók. Ívben és tekercsben egyaránt kapható többretegű struktúrák, amelyek külső papír/karton vagy műanyag rétegei között azonosításra alkalmas színes és/vagy UV-fluoreszcens réteg helyezkedik el. Ez a megoldás egyben eltérhetlenné is teheti a papírt. Viszonylag olcsó és biztonságos.

A tónert az átlagos papírnál lényegesen jobban megkötő felületű ún. **Toner Fusing** papír nagyon megnehezíti a nyomat (pl. csekk-) felületről a szövegtávolítást.

Másolás, hamisítás ellen védett papírtípusok (*AntyCopy, NoCopy, Anti Alteration/AntiScanning Papers*).

Támadási kísérletet vagy sikeres támadást (Thread), káreseményt regisztráló/jelző papírok (*CopyEvident/TamperEvident/FraudEvident/Papers*).

Az „intelligens” papír (*The Smart Paper*). A jövő nyomathordozó-típusa, amely az anyagában, illetve a felületén elhelyezett félvezető polimerek, mikrocsipek, rádiófrekvenciás eszközök, nyomdai úton előállított integrált elektronikai elemek segítségével programozható. [Bővebben: *Az intelligens papírokkal kapcsolatos fejlesztések állása* című *Pira* kiadású szakkönyvben. (*Development in Smart Papers*: www.intertechpira.com/publicationSearch.asp?step=2.)]

Nyomatott és digitális vízjelek az írott, a nyomtatott és a másolt információ biztonságát szolgáló módon

A vízjel és vízjelzett papír (angolul: *Fingerprint, Watermark, illetve Watermarked Paper/Substrate*, az alkalmazás pedig: *Watermarking*) a biztonsági nyomtatás, az írott, nyomtatott és másolt információ védelmének a leghatékonyabb eleme, mivel másolása, szkennelése, duplikálása mai ismereteink szerint kizárt. A köztudatban a papír

és karton fogalmához kötődik, de már hosszú ideje nem ezek a kizárólagos nyomathordozók, ezért a biztonsági vízjelek más anyagok esetében is alkalmazhatóak.

A vízjelalkalmazás célja: elsősorban a bankjegyek, továbbá a fokozottan védett írott, nyomtatott vagy másolt információ, a nagy értékű, csomagolt termékek, illetve márkák védelme és eredetiségük tanúsítása (*Authentication*).

A vízjelek főbb kivitelezési alaptípusai

◆ **Nedvesen vagy szárazon préselt/ prégelt vízjel.** Papír és kartonfélék esetében a gyártás során még nedves állapotú anyagban képzett (*Cylinder Mould Watermark*) vagy később szárazpréseléssel/prégeléssel lehet előállítani. Az eredmény *vízjeles* papír/nyomathordozó.

◆ **Nyomatott vízjel** (*Printed Watermarks/Fingerprints*).

◆ **Digitális vízjel.** Ez utóbbi legelőször 1992-ben jelent meg a nyomtatott, másolt termékek piacán. Állhat például csak géppel rekonstruálható szám- vagy kódkombinációkból és digitális aláírásból.

A nyomathordozó-felületen elhelyezett vagy annak anyagába beépített (*embedded*), látható vagy nem látható vízjel és annak információ-tartalma, a védelmi céltól függően, lehet a következő:

- ◆ szoftver által védett, gépi karakterfelismerő (OCR) eszközökkel értelmezhető;
- ◆ optikailag változó (UV-, IR-fluoreszcens, foszforeszcens) nyomat;
- ◆ RFID-festékkel nyomtatott;
- ◆ a közfelhasználás részére elérhetetlen speciális (pl. nano-) festékkel nyomtatott;
- ◆ mágneses kód és *jelkép* (logo), vonalkód vagy színkód;
- ◆ holografikus/OVID-elem;
- ◆ beépített vagy nyomtatott mikrocsip;
- ◆ beépített vagy nyomtatott mikro-RFID;
- ◆ digitális vízjelek esetében: digitális aláírás, digitális szám-, mikro-karakterkombináció (mikroszöveg), digitalizált mikrokép;
- ◆ végül lehet integrált rövid audio- és videotartalom is, illetve a felsorolt lehetőségek kombinációiból álló megoldás is.

A digitális vízjel által hordozott információ-tartalom, a védett nyomtatvány rendeltetésétől függően, vonatkozhat személyazonosításra, a fokozot-

tan veszélyeztetett nyomdatermékek védelmére, eredetiségük tanúsítására, különféle termékek megnevezésére, szerzői jogvédelmi tudnivalókra. Tartalmazhat a termék megvásárlójára, felhasználójára utaló információkat (név, cím, elérhetőség stb.), fényképet, grafikai elemeket, digitális aláírást, rejtett (ún. *steganográfiás*) és mikroszövegeket, mindezt anélkül, hogy a vevőnek, felhasználónak tudomása lenne a vízjel jelenlétéről, illetve annak információtartalmáról, amely lehet például tömörített JPEG fájl formájában rögzített is. Mágneses vagy integrált elektronikus elemek használata esetén lehetnek kódolt jelsorozatok is.

A nyomtatott vízjel előállítás elvben történhet bármely nyomtatóeljárással, azonban egyes eljárások, például az *Intaglio nyomtatás*, a *festékszóró digitális nyomtatóeljárások* és a *szitanyomó eljárás* is ilyen célra első helyen állnak.

Olvasnivalók: *A védett papír* (www.protectedpaper.com); *Biztonsági nyomtatás, biztonsági papír* (www.security-printing.co.uk/security-paper.php); *Szakkönyv: A jövő nyomathordozója* (*The Substrate of the Future*: www.intertechpira.com/publicationSearch.asp?step=2); *A digitális vízjelek* (*Digital Watermarks*: http://en.wikipedia.org/wiki/Digital_watermark weboldalon.)

A NYOMTATÁS

Biztonsági nyomtató-, bélyegző-, másolóeljárások, eszközök és módszerek

E témakör teljes részletességű ismertetéséhez lapunk egész terjedelme sem lenne elegendő. Állandóan újabb és újabb eljárásokat dolgoznak ki, amelyek egyre bonyolultabbak, és az alkalmazásuk egyre drágább felszereléseket és egyre nagyobb szaktudást igényel (pl. a nanotechnológiai és a szintén új, biometrikai eljárások stb.).

A maximális biztonságra törekvés azt igényli, hogy *egyidejűleg minél több nyomtatóeljárás alkalmazására kerüljön sor*, mert a hamisító annál kevésbé és/vagy annál költségesebben képes a céljait elérni.

Hagyományos eljárások

Elvben a hagyományos nyomtatóeljárások (magas-, ofset-, szita-, flexó-) mindegyike alkalmas biztonsági nyomatok gyártására, de nem egyenlő eséllyel, hiszen a védett nyomtatvány értékétől, bonyolultságától függően kritikus jelentősége

lehet az eredititervezésben és a formakészítésben alkalmazott egyedi eljárásoknak, a maximális festékréteg-vastagságnak, a felbontóképességnek, az eljárással elérhető illeszkedési pontosságának, a legújabb típusú biztonsági festékek, lakkok és a változóadat-nyomtatás alkalmazhatóságának, hogy csak néhányat említsünk a valóban kritikus tényezők közül.

Digitális eljárások

- ◆ Egyenesen a nyomathordozóra nyomtató eljárások: *inkjet, elektrosztatikus, elektrofotografikus és termotranszfer*.
 - ◆ Fix nyomóformát használó nyomtatóeljárások: *Computer to Press*.
 - ◆ Újraírható nyomóformát használó eljárások: *elektrofotografikus, ionsugaras, Direct Imaging* (Océ), *elkografikus* és *magnetografikus*.
- (Részletesen lásd a lapunk előző számának 7. oldalán lévő 1. ábrán.)

Termotranszfer nyomtatás (*Thermotransfer Printing*). Digitális egyszínnyomtató eljárás, amely állandó hőmérsékletű nyomtatótűk és festékszalag segítségével juttatja fel a festéket a nyomathordozóra, majd ott beégeti. A biztonsági kártyagyártás során logó-, fotó-, szöveg- és kódfelvitelre használják.

Termoszublímációs nyomtatás (*Thermo Sublimation Printing*). Az előbbi eljárástól abban különbözik, hogy a nyomtatófej és a CMYK alapszíneket tartalmazó festékszalagok hőmérséklete a nyomtatás folyamán változik, elősegítve, hogy a festék szükség szerint diffundáljon be az akár PVC anyagú kártyafelületbe is. Színes- és monokróm nyomtatáshoz egyaránt használható.

RE-transzfer nyomtatás (*Re-Transfer Printing*). Az információfelvitel először speciális, ún. *RE-transzfer* fóliára történik, majd ezt a nyomtatott fóliát laminálják rá a kártyafelületre. Így a festékréteg a fólia belső felületén helyezkedik el, amely csak a fólia roncsolása árán teszi lehetővé a nyomtatott információ megváltoztatását. Előnye a gyors nyomtatás, a kártyaalapanyag függetlenség, a nagy felbontás, a kiváló kopásállóság és a hologramfelvitel lehetősége is. Az eljárás személyi dokumentumok, jogosítványok nyomtatására is használható.

A ClearJet technológia (*ClearJet Printing*). Ez is nagyfelbontású, két színt nyomtató hőtranszfer nyomtatóeljárás, amely szintén speciális fóliára nyomtat, de ez utóbbi, festékszalag használata

nélkül. Előnye, hogy képes a nyomtatott adatok újraírására, törlésére, ami kártyák esetében, például a személyi adatok változásakor vagy az évváltások alkalmával előnyös lehet.

Intaglió nyomtatás (Intaglio Printing). Klasszikus és drága nyomtatóeljárás. A galvanoplasztikai úton, maratással, kézi vagy gépi véséssel előállított mélynyomóformája a rajzi elemeket bemélyítve tartalmazza. A nyomóhenger-felületre felhordott viszkózus intaglió festéktöbbséget törőhengerrel távolítják el. A nyomtatás rendkívül nagy nyomóerő alkalmazásával történik, miközben a festék a nyomóforma mélyedéséből átkerül a hordozófelületre. A nyomtatott elemek, a hordozófelület szabad szemmel láthatóan és kézzel is jól érezhetően kiemelkednek. Az eljárás alkalmas az ábrán látható ún. *Guilloche* rajzelemek, továbbá hologramok és optikailag változó elemek (*Optically Variable Devices, OVID, DOVID*) nyomtatással történő előállítására is. Az intaglio eljárás fő alkalmazási területei: a bankjegyek, bélyegek, csekkok, útlevelek, kormányzati dokumentumok előállítása. (Utóbbiról bővebben a *HOLOTEK Technology Co. Ltd* cég www.holotek.com.cn honlapján. Lásd még a *Chan Wanich Security Printing Co. Ltd* www.chanwanich.com/tec/technology_01.htm weboldalát is.)

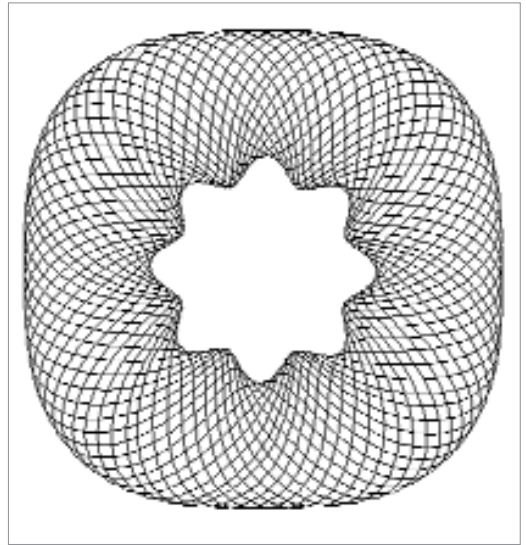


Színes *Guilloche*-rozetták (www.maa.org)

Dombornyomtatás (Embossing). Hitelkártyákról régóta ismert eljárás. Préshatás alkalmazásával, hideg eljárással domború nyomatot hoznak létre, majd a nyomatsíkból kiemelkedő felületelemeket festékszalag segítségével színessé teszik.

Lézervésés, lézergravírozás (Laser Engraving). Lézerforrás segítségével karakter- vagy rácsponterületen átégetik a védőfóliát, és a biztosítandó nyomtatvány (pl. kártya) felületén akár árnyaltos képet is létrehozhatnak.

A korábbi és az itt felsorolt újabb eljárások többsége egyaránt használható különféle adatvédelmi, hamisítás-, másolás- és szkennelésgátló



Matematikai rendszerű *Guilloche*-rozetta (www.maa.org)

biztonsági elemek (Anticopy, NoCopy Marking, Anti-Photocopying/Uncopyable Marks) nyomtatására, a következők szerint:

Kódnymtatás. Fekete-fehér és/vagy színes vonalkód, háromdimenziós kód, mágneses kód, elektronikus termékkód, nanokód, mikrokód, digitális kód vagy a termékbe keverhető színes vonalkód (*Multi Color Code; MicroTaggant*) alkalmazása. Ez és a szintetikus *DNS* (angolul *DNA*) molekuláris kód (*Synthetic DNA Molecular Code*, pl. a *CodeSafe* gyártmány) ma a legbiztonságosabbnak tűnnek.



Termékbe keverhető, márka azonosító szín-kódolt, *MicroTaggant*-részecskék több százszoros nagyításban. A valódi részecskeméret 20 mikrométer körüli (www.microtaggant.com/microtaggant.htm)

Mikrostruktúra-nyomtatás (Micro Printing). Rendkívül kicsiméretű, ezért szabad szemmel nem látható karakterekből, képekből, grafikákból álló nyomtatott információ. Ha a felületen foltokban eltérőek a fontok és a karakterméretek is, akkor a hamisítás még jobban nehezített. Ma főként bankjegy-, csekk- és bankkártyagyártás esetén alkalmazott eljárás.

Változóadat-nyomatás (*Variable Information Printing, VIP*). Megszemélyesítés, sorszámozás (*Personalization, Serial Numbering*), elsősorban a felület laminálása előtt, tintasugaras- vagy lézernyomatató segítségével.

Nyomathordozó vágottéljelölés (*Authentication with Docu Edge Encoding; Perimeter Side Marking; Cut Edge Marking*). Védendő dokumentum, nagy értékű/márkás csomagolt termék hitelességét, eredetét, tulajdonjogát tanúsító nyomtatott információ (*digitális mikrokód/mikroszöveg/mikroszínkód*) felvitele a nyomathordozó vágott élére. Nehezen felfedezhető, hamisításképző és nagyon költségemelő eszköz. Felhasználható a megkísérelt vagy végrehajtott hamisítás tényének ellenőrzésére és bizonyítására is. Változóadat nyomtatására alkalmas megoldás. A technológia részletes leírását például a *United States Patent 20070119950* is tartalmazza.

A nyomathordozó mindkét oldalán pontosan illeszkedő nyomatkép előállítás. Az így készült nyomat kifogástalan másolása lehetetlen.

Optikai karakterfelismerő eszközökkel, gépekkel, programokkal olvasható elemek nyomtatása (*Machine Readable Devices for Security Documents/Optical Character Recognition*).

Az angolul **Prismatic Printing** (*Fountain Printing*)-nek nevezett technika alkalmazása. Több, egymástól független és méretben egyre csökkenő nyomatképek felvitele egymásra.

Kriptogramok (rejtett szövegek) (Cryptograms) nyomtatása.

Többszörös lézerképek/Lencserácsképek alkalmazása. A hologramhoz hasonló effektust biztosító eljárás főként bankkártyagyártási célokra. A hengerlencsés és a két lézersugárral létrehozott különböző képeket vagy sztereoképpárt tartalmazó nyomatot a lamináláskor egyesítik.

Végül, de nem utolsósorban megemlítendő a mindennapos gyakorlat, a **több biztonsági védőelem egyidejű alkalmazása** (*Mixed Security Elements*), amely még inkább nehezíti a hamisító tevékenységét.

Olvasnivalók a biztonsági nyomtatás témaköréből: **Biztonsági nyomtatás. A jelenlegi fejlesztések** (*Security Printing: Recent Developments*: www.polestarltd.com/tg/securityprint.html). **A globális biztonság jövője** (*The Future of Global Security*: www.intertechpira.com/publicationsearch.asp); **Biometrika** (*Biometrics*: <http://en.wikipedia.org/wiki/Biometrics>).

NYOMTATÁS UTÁN

Security Postpress: nyomtatás utáni információbiztonsági műveletek

A kiemelten védett nyomtatott/másolt dokumentumok, a nagy értékű csomagolt termékek esztétikai, mechanikai, környezetállósági, tartósági, kiemelten pedig alkalmazástechnikai/védelmi jellemzőinek javítása a nyomtatás utáni műveletekkel, az illetéktelen másolás/felhasználás/hamisítás ellen.

A továbbfeldolgozás (Converting) jellegű feladatok közös jellemzője, hogy a biztonsági termék az adott készültiségi állapotában még nem alkalmas arra, hogy a megrendelőnek átadhassák (például még nem kódolt, védőfólia nélküli, elektronikája még programozatlan).

A kikészítés, nyomdatermék-befejezés, konfekcionálás (Finishing) jellegű feladatok célja pedig a termékmegrendelőnek/felhasználónak átadható, végleges biztonsági állapotra hozása az alábbiak szerint:

◆ **Biztonsági védőrétegek felvitele a nyomatfelületre (lakkozás, filmbevonás, fedő/védőfóliázás, hideg- vagy melegeljárású laminálás (Hot Stamp Foiling/Lamination).** Idetartoznak a színváltó, UV-, IR-fluoreszcenciás és lumineszcens anyagok, köztük a különböző fóliák, másolásgátló fluoreszcens nyomathordozók és védőfóliák is.

◆ **Hologram/optikailag változó eszköz, holofólia-felvitel (Holograms/Optically Variable Devices, OVID, DOVID) beragasztása.** A hologram ragasztással vagy a fóliával együtt, ragasztással vihető fel a védendő nyomatra. Erre a célra asztali hologramfólia-felviteli berendezéseket is forgalmaznak. A nyomat védett információtartalmának elérését biztosító ragasztott hologram roncsolás nélkül nem távolítható el. Egyes hologramok – másolásvédelmi és eredetiségbizonyítási célból – lézergravírozott azonosító sorszámot is tartalmaznak. (Bővebben a márka- és csomagoltermék-védelmi tárgyú fejezetben.)

◆ **Két- vagy háromdimenziós információkat, mozgásélményt keltő lencserácsos (Lenticular) biztonsági elemek integrálása a nyomatba.** A létrehozott kép hologramszerű, de a létrehozása nem holográfiai eljárással történik!

◆ **Biztonságicímke-felvitel (Security Labels/Tags/Taggants) felragasztása a kész nyomdatermékre.**

◆ **Mikroperforálás (Micro Perforation).** Szabad szemmel nem érzékelhető méretű szövegerforálás.

◆ **A termék mikro- és makrodomborzati jellemzőinek megváltoztatása.** Például vaknyomatással/prégléssel (*Security Embossing*).

◆ **Mágnescsíkok felragasztása.**

◆ **Elektronikus biztonsági elemek integrálása a nyomtatott termékbe.** Mikrocsipek, rádiófrekvenciás eszközök, nyomtatással előállított integrált áramköri elemek, nyomtatott áramforrások stb.

◆ **Biztonsági záróelemek rögzítése a nyomaton.** Öntapadó, bepattanó, kapcsos, roncsolásmentesen nem nyitható rögzítőelemek, OVID-jelölésű biztonsági zárószálak alkalmazása.

A következő biztonsági megoldás viszonylag új, de alkalmazását nemzetközi hatályú törvények teszik kötelezővé!

Biometrikus biztonsági elemek felvitele a védett nyomatfelületre (*Security Biometrics/ Human Biometric Characteristics*). A biztonságtechnikai macska–egér játék javában zajlik. A hamisítás elleni harcban már a nyomathordozó vágott élére nyomtatás is egy csúcscsökzeli eredménynek számít. (Ha valaki évtizedekkel ezelőtt ezt javasolja, valószínűleg elmebetegnek nézik...)

Biztonságot nélkülöző világunkban az igazi csúcs azonban a *biometrikus eljárások* kidolgozása és alkalmazása. Ennek lényege az, hogy egyes kiemelten védett nyomtatott biztonsági azonosító dokumentumok (útlevél, vízum, személyazonosság igazolvány stb.) által rögzítendő információnak tartalmaznia kell a dokumentumtulajdonos alábbi jellemzőit is:

◆ **humán fizikai és méretjellemzők;**

◆ **fiziológiai jellemzők** – az arc geometriai adatai és hőfényképe, az ujjlenyomatok, a kézre vonatkozó geometriai adatok, a szírvárványhártya (írisz) retinaszkenneres fényképe (amely ellenőrzéskor írisz-szkennerrel azonosítható), a testi illatjellemzők (!), továbbá az illető genetikai információit átörökítő anyaga (a személyi DNS) által hordozott fontosabb biometrikus adatok;

◆ **személyiségjellemzők** (*Behaviometrics*) – viselkedéssellemzők, emberi magatartás, hangjellemzők, aláírás és a személy billentyűleütési dinamikája (*Keystroke*).

A dokumentumkivitelezési technológiákról, a biometrika fejlődési irányairól bővebben a Pira www.intertechpira.com/publicationresearch.asp honlapján, az egyes országok – köztük az **Euró-**

pai Biometrikus Útlevél – 2006 óta érvényben lévő biztonsági és nyomdatechnikai előírásai pedig a http://wikipedia.org/wiki/Biometric_passport honlapon találhatóak. Ezzel kapcsolatban nyomdászokat érintő aktuális információk is olvashatóak a *Journal of the International Biometric Society* című szaklapban.

Egy külföldi karikatúra szerint – amelynek közlésére nem kaptunk engedélyt –, a kiemelten védett személyi iratok terén a *felülmúlhatatlan, abszolút biztonságot* az jelentené, ha a dokumentum jogos tulajdonosát digitálisan lekisebbitve, préselten és kiszáritottan beragasztanák a dokumentum biometrikus oldalára, és testének karakteres illatjellemzőit apró polietilén tasakokban tárolva helyeznék el mellette, a nyomozókutyák nagy örömére.

Nyomtatott integrált áramköri elemek felvitele a védett nyomatfelületre (*Printable Integrated Electronics*). Ez a megoldás is rohamosan terjed! A nyomdagéptermi eszközökkel előállítható és/vagy felragasztható integrált elektronikai elemek és eszközök részletes gyártás- és alkalmazástechnológiája lapunk 2007/2. számában olvasható. Elterjedése fokozatosan kiválthatja a korábbi integrált áramköri elemeket és áramkörgyártmányokat, alapjaiban megváltoztatva a mai technológiai gyakorlatot, végképpen elektronikai jellegű iparaggá átformálva a nyomdaipart is.

Ajánlott olvasnivaló: *Nyomatás után* (Magyar Grafika, 2005/5., www.mgonline.hu).

MÁRKAVÉDELME, A NAGY ÉRTÉKŰ CSOMAGOLT TERMÉKEK ÉS KÍSÉRŐ DOKUMENTUMAIK VÉDELME

Biztonsági címkék, jelölők és csomagolóanyagok

Az alábbiakban a témakör főbb **védelmi rendeltetésű nyomtatványtípusait** ismertetjük rendeltetés, működésmód és felhasználási terület szerinti szempontok szerinti értékelve.

Működési cél (funkció, rendeltetés) alapján a márkákat, csomagolt termékeket és kísérő dokumentumokat veszélyeztető támadások ellen védelmet biztosító **jelölő-, címke- és csomagolóanyagok** következő nyomtatványtípusait különböztethetjük meg:

- ◆ *eredetiséget/hitelességet ellenőrző, tanúsító, ún. **Authentikus (Authentic)** típusúakat és kémiai, biológiai, rádiófrekvenciás és nyomtatással előállított egyéb integrált elektronikai és molekuláris jelölőket (Molecular Markers);*
- ◆ *a bűncselekmény elkövetését nehezítő ún. **Anti- és No/Non-típusúakat**: például **AntiTheft, Anti-Forgery** címkéket és csomagolóanyagokat (**Anti-Forgery, AntiCopy, NoCopy Labels**);*
- ◆ *az illetéktelen szkennelés, másolás és felhasználás ellen védelmet biztosító **Proof (Counterfeit Proof, CopyProof, TamperProof, PhotoCopyProof Labels)** típusúakat;*
- ◆ *a támadást, az illetéktelen cselekmény elkövetésének tényét érzékelő **Sensor/Detector** típusúakat;*
- ◆ *a szándékos károseményt regisztráló, jelző és tanúsító, ún. **Evident** típusúakat (**Tamper Evident, Forgery Evident Labels**);*
- ◆ *a terméklejáratból, természetes elhasználódásból, a környezeti hőmérsékleti, légnedvességi, pH-változások miatt bekövetkező minőségromlási folyamatokat érzékelő, regisztráló, ún. **Diagnosztikus** típusokat;*
- ◆ *az illetéktelen másolás, termék- vagy dokumentumhasználat tényére figyelmeztető **Void, Nem eredeti, Hamisítvány, Lejárt, Érvénytelen, Engedély nélküli másolat** figyelmeztető szöveget közlő típusúakat;*
- ◆ *a csak roncsolással bontható öntapadós címkéket, **nyomtatott zárjegyeket (Security Seals)**;*
- ◆ *végül – de nem utolsósorban – a felsorolt védelmi anyagok, eszközök és elemek felhasználásával létrehozott ún. **kombinált biztonsági-nyomtatvány-rendszereket (Combined Security Printed Materials/Matters)**, köztük kiemelten az **intelligens címke- és csomagolóanyag (Smart Labels/Smart Packaging Materials)** típusú következő nyomdatermékeket.*

Intelligens, okos (Smart) címke- és csomagolóanyag-rendszerek. A *Smart* kifejezés valójában az önállóan megfigyelő, elemző és rádióadás formájában jelentéstételre képes rendszerű (*Self Monitoring Analysis and Reporting Technology*) angol kifejezésből képzett mozaikszó = **SMART**, ugyanakkor ez a kifejezés az *intelligens, okos* jelentéssel is rendelkezik. Az ilyen termékek a felhasználó által védetten programozhatóak! (A címke- és csomagolóanyag-rendszer kifejezés itt arra utal, hogy az ilyen termékekhez nyomtatott rádióadó-antenna, elektronikus író- és távleolvasó készülék is hozzá tartozik.)

A rádiófrekvenciás azonosító, ún. RFID-címke (Radio Frequency Identification Label) olcsón előállítható, mikrocsipet és adó-vevő antennát tartalmazó eszköz, amelynek – energiaellátás alapján – háromféle típusát különböztetjük meg: a **passzív RFID**-címketípus áramforrás nélküli; a **fél-passzív RFID** és az **aktív RFID**-címketípus beépített elemet is tartalmaz. Az utóbbi típus fémplé méretű. Az RFID-rendszerelemek: a címkére, csomagolóanyagra nyomtatott *antenna*, továbbá a rendszert működtető *író- és táv-adatkiolvasó szerkezet*. (Bővebbet: Magyar Grafika, 2004/7., www.mgonline.hu.)

E rendszerek alkalmazási területei:

- ◆ A környezeti hatásokra sérülékeny vonalkód kiváltása, a be- és kiléptető rendszerek, hozzáférési jogosultságot reprezentáló kártyák, elektronikus fizetőkártyák érintkezésmentes (*Contactless*) kezelése.
- ◆ Márka- és csomagoltermék-védelem terén: a nagy tömegű biztonságidokumentum- és árukészlet-védelem.
- ◆ Automatikus termékazonosítás, megfigyelés, dokumentummozgás követése nagy távolságból is.
- ◆ Információ elleni támadás- és kármegelőző funkció ellátása: a fentebb felsorolt márka és csomagolt termékek veszélyeztetettségének, az ellenük irányuló támadásoknak (rongálás, dézsmálás, lopás, kicserélés, illetéktelen dokumentumhasználat, másolás stb.) megfigyelése, jelzése.
- ◆ Árukövetés az ellátóláncban nagy távolságról is, ellenőrzés, irányítás, raktári alap-, segédanyag és értékesítésre váró árukészlet felügyelete, érintkezés nélküli rendkívül gyors leltározása, készletfogyások jelzése.
- ◆ A felsoroltakkal kapcsolatos nyilvántartások, elemzések, jelentések készítése és továbbítása.
- ◆ A megfigyelt dokumentum/árुकészlet eredetiségének, valódiságának, épségének, darabszámának, fizikai, kémiai, biokémiai állagának és mechanikai változásainak, spontán romlásának figyelemmel kísérése és – veszélyhelyzetben – az önmegsemmisítés kezdeményezése.
- ◆ Bank- és egyéb kártyák, jegyek személyi és pénzügyi változóadatainak kezelése, termékek garancia-, szavatossági- és felhasználhatósági idejének folyamatos figyelemmel kísérése, időbeni figyelmeztető kijelzése.

A rádiófrekvenciás eljárás előnye a vonalkóddal szemben az, hogy takart helyzetben is működik, falon keresztül is leolvás, beázás és elszennyeződés esetén is helyes adatokat állapít meg, egyidejűleg nagy tömegű megfigyelést, mérést képes elvégezni, érintkezés nélkül, nagy távolságból is.

HOLOGRAMOK ÉS MÁS OPTIKAILAG VÁLTOZÓ ESZKÖZÖK

Alkalmazás a márka, a nagy értékű csomagolt termékek és dokumentumok védelmére

A háromdimenziós (térhatású, sztereo) nyomtatványok, a lencserácsos termékek, a hologramok és az optikailag változó, diffrakciós azonosító eszközök (*Optically Variable Identification Devices, OVID, DOVID*) gyártás- és alkalmazástechnológiáit nyolcrészes cikksorozatban már részletesen ismertettük (hologram és OVID: Magyar Grafika, 1998/1). Ezért most az újabb fejlesztési eredményekkel és alkalmazásokkal foglalkozunk.

A **hologram** a ráeső fény jellemzőit és diffrakcióját befolyásoló, olyan optikailag változó eszköz, amelyet a művészeti célú felhasználáson és a dekoratív csomagoláson kívül a *márkák*, a nagy értékű *csomagolt termékek*, a dokumentumeredetiség/-hitelesség tanúsítására (*Authentication*), a hamisítás elleni védelemre, és a biztonsági nyomtatványok (címkék, jelölő- és csomagolóanyagok), továbbá védett dokumentumok gyártására is felhasználnak.

A védett nyomtatványokra a **biztonsági hologram** felvitele fólia formájában történik. A hologram nem másolható és nem hamisítható, tehát eredményes márka-, áru- és dokumentumvédelmi eszköz. *Statikus* (álló) és *dinamikus* (mozgást szimuláló) változatai léteznek.

Főbb biztonságifólia-típusok és alkalmazási területeik:

- ◆ arany-, ezüstbevonatú holografikus fóliák;
- ◆ nagy reflexiós indexű (*High-Reflective Holographic, HRI*) fóliák;
- ◆ részlegesen fémbevonat, félig áteresztő fóliák (*Partly metallized semi-transparent foil*), az általa takart szöveg részbeni elolvasását engedő típus;
- ◆ lekaphartható („kaparós”) többrétegű lapfóliák/fóliatekerccsek;

- ◆ márkavédelmi eszközök (audio-, videokazeták, fényképek) kicserélés elleni védelme;
- ◆ csomagolt, nagy értékű termékek védelme (pl. audio/video adathordozók, gyógyszerek, cigaretták, alkohol stb.);
- ◆ promóciós cikkek hologramfóliás védelme;
- ◆ azonosító dokumentumok (*Identifying Documents*) fénykép- és bizalmas adatainak védelme fóliával;
- ◆ utazási, közlekedési jegyek hamisítás elleni védelme.

A fóliákat a biztonsági nyomtatás gyakorlatában a fólia anyaga/típusa, a rajta lévő grafikai motívum és a felhasználási cél szerint szokták rangsorolni.

A tekercsben és lapban kapható, melegen sajtoló, vaknyomtatással/dombornyomással feldolgozható (*Hot Stamping Foil*) fóliából a biztonsági nyomtatással foglalkozó nyomdászok jelentős mennyiséget használnak. A papír vagy műanyag (polimer) előrenyomtatott hordozón lévő védett adatok, csekkek, biztonsági címkék, jegyek, pénzügyi dokumentumok és a *Hologram Image Register* által nemzetközileg elismerten nyilvántartott képek bevonására is alkalmazva.

A biztonsági hologram tervezése

A vonalas, árnyalatos/monokróm vagy színes hologramok tervezéséhez a megfelelő elképzelés, a technika (hologramtípus) kiválasztásán és a szükséges felszerelésen kívül, megvásárolható regisztrált kép, eredeti tárgy, mikromodell (makett) és/vagy hologramtervező szoftverben rögzített képeredeti szükséges. Az – a kívánt rendeltetéstől függően – lehet akár folytonos, tapétajellegű, végtelenített felépítésű (*Wallpaper type*) vagy zsugor-sleeve (*Holographic Shrink Sleeve*) is. Utóbbira a csomagolóanyag-gyártás esetén lehet szükség.

Hologramtípusok

2D hologramok. – Lézerrel létrehozott kétdimenziós információrögzítő eszközök.

2D/3D hologramok. – Lézerrel generált, háromdimenziós és látszólagos elmozdulás érzetét is keltő több kép egyidejű rögzíthetőségét biztosítja.

3D hologramok. – Lézerrel és/vagy számítógéppel, tárgyeredeti vagy mikromodell segítségével létrehozott képeket, szövegeket, grafikákat tartalmazhatnak 1:1 méretarányban.

Mozgófilmes 3D hologram (*Filmed Stereogram*).

– Lefilmezett tárgyról készült mozgó, térbeli képeket tartalmaz. Számítógéppel, modell nélkül is előállítható. Másolás, hamisítás ellen nagy biztonságú védelmet nyújtó eszköz.

Pontmátrix hologramok (*Dot Matrix Holograms*).

– Alapjában sík (2D), de erős mozgásérzetet keltő, a szemlélési iránytól függően különböző (kinetikus) hologramképeket tartalmaznak.

CLRI (*Covert Laser Readable Image*). – *Forensic* védelmi típusú lézerrel előállított megoldás. Rejtett képtartalma csak lézerrel rekonstruálható. Mikroszövegek rögzítésére is alkalmas technika.

A fémbevonatot az egész felületen, részlegesen vagy csak szelektíven tartalmazó hologram-típusok (*Metallic/Metallized/Demetallized/Selectively Demetallized Holograms*). – Hordozó-alapja, a végtermék rendeltetésétől függően, lehet öntapadó fólia, laminálásra alkalmas film, de lehet szilárd alap is. Ezt vákuumgőzölés segítségével, vékony fémréteggel vonják be. A hologram az alkalmazott fémtől függően, arany-, alumínium-, ezüstszerű vagy tetszőlegesen színeztet, fémszerű megjelenést nyer. A fémréteg vastagsága meghatározza, hogy a termék átlátszó, fedett vagy – a személyazonossági (ID) dokumentumok esetében – a fénykép és írott adatok részleges takarásához kedvezően, áttetsző legyen-e. Lehetőség van a fémréteg szelektív eltávolítására is. Ez történhet meghatározott foltokban, de szövegszerű eloszlásban is. Egy ilyen hologrammal védett dokumentum megfelelő minőségben nem hamisítható!

Számítógéppel létrehozott hologramok (*ComputerSynthesized/Generated Holograms*).

Kombinált képtartalmú hologramok. – A felsorolt technikák kombinált alkalmazásával létrehozott, több, egymástól független, mozgó és térszerű képtartalmat rögzíthetnek.

OVDs hologramok. – A legkorszerűbb hologramgyártási technológiával létrehozott, *overt/covert* típusú, másoláságtól, CD-ROM-on vagy audio diszken tárolt, „hologramszerű” eszközök, amelyek a kereskedelmi forgalomban megrendelhetők. Csak géppel olvasható információkat tartalmazhatnak, sorszámozottak, és – kérésre – vonalkóddal is ellátottak. Információtartalmukat a szemlélés irányától függően változtatják. Megjegyzendő, hogy az OVD fogalma nem korlátozódik a szóban forgó termékekre, hiszen például a színváltó

festékek is ebbe a kategóriába sorolhatóak, és minden más olyan anyag, termék, aminek a színe a fénybeesés szögétől és a szemlélés irányától is függő. A közös bennük az, hogy a változó információtartalmuk és színváltó tulajdonságuk miatt megfelelő minőségben nem reprodukálhatóak, tehát megbízható eszközei a védelemnek.

DOVID (*Diffraction Optical Variable Image Device*). *Optikailag változó diffrakciós kép megjelenítő eszköz*, síkfelületen két- vagy háromdimenziós fénykép megjelenítésére alkalmas esztétikai és dokumentumbiztonsági célú, eredetiséget, hitelességet, valódiságot tanúsító, az illetéktelen másolás, hamisítás elleni védelmet biztosító termékváltozat. (A diffrakció kifejezés az elnevezésben a fényhullámoknak a nyomathordozó-felületen történő elhajlására utal.) Megjegyzendő, hogy az OVID mozaikszóval jelölt kifejezést a lézertechnika fejlődése, a színváltó festékek, lakkok, fóliák megjelenése következtében a korábbinál szélesebb értelemben használjuk, és például a színváltó festékekre, fóliákra és fluoreszkáló/foszforszkáló anyagra is vonatkoztatjuk.

Kinegramok (*Kynegrams*). – Számítógéppel létrehozott nagy felbontású hologramfélék. Több önálló képet tartalmaznak rögzítve, amelyek a szemlélés irányától függően válnak láthatóvá. Ha a képek egy teljes mozgássorozat részei, akkor a szemléléskor a néző mozgásban lévő tárgyat, képet érzékelhet. *Overt, covert* és *forensic* változatban is kaphatóak.

Flip-Flop effektus hologramok. – Jellemzője az, hogy két különböző képet rögzítenek, és ezek egymástól függetlenül, a szemlélés irányától függően külön-külön észlelhetők. Nem másolható védőeszközök.

Digitális hologramok. – A hologramkészítés egyik technikai alternatívája: a felvételhez a hagyományos film helyett CCD kamerát használnak. Ebben az esetben a hologramtartalom rekonstrukciójához szabványos számítógépet kell használni. A 3D kép annak monitorán vagy a tv-képernyőn jeleníthető meg.

Nagy felbontású vonalas ábrákat tartalmazó holografikus képek (*High Resolution Line Patterns*).

Holografikus lemezek (*Holographic Discs*).

– A nemzetközileg regisztrált hologram-eredetik és a biztonsági célokra előre gyártott, kereskedelmi forgalmazásra szánt, optikailag

változó diffrakciós képeredetik tárolására használt eszközök.

Holografikus záróelemek, tépőzárak (*Hologram Security Seal*). – Az áru vagy dokumentum illetéktelen használatának meggátlására szolgáló védelmi célú eszközök.

Holografikus biztonsági védőszálak (*Security Threads*).

Stock Hologram Labels. – A *Tamper Evident* kategóriába sorolható, raktárról rendelhető, kész címkék, ívben/tekercsben szállítva. NovaVision Inc.: kcrea@novavisioninc.com.

A nem fényoptikai holográfia termékei

Akusztikus hologramok (*Acoustic Holograms*).

– A kívánt szöveges és képi információ tartalmat a hagyományos technológiákhoz hasonlóan, de hanghullámok segítségével rögzítik.

Elektron hologramok (*Ebeam Holograms*). – Rendkívül erős háromdimenziós mozgásérzetet keltő, lézer nélkül, elektronsugár-generátor segítségével létrehozott, nagy védelmet nyújtó, igen drága hologramtípus. Felbontása 12 000 dpi. Ellenőrzése és rögzített információ tartalmának rekonstrukciója csak elektronmikroszkóppal lehetséges.

A biztonsági hologramok, előre gyártott és kereskedelmi forgalomban árusított hologramos biztonsági címkék, zárjegyek és kitűzők főbb alkalmazási területei

Márkavédelem. – Kosmetika, gyógyszer, alkohol, cigaretta, drog, autó és elektronikai alkatrészek stb. címkéi.

Termék és védett dokumentum esetében az **eredetiség, hitelesség tanúsítása** (*Security Authentic Holograms*):

Jegyvédelem (színházi, koncert, kiállítási, sportmérkőzési, autóbusz, vonat, repülő céljára).

Garancia- és szavatosságilevel-védelem.

Nyereményjáték-szelvények adatvédelme.

Holografikus adattárolás (*Holographic data Storage*). – A jelenlegi csúcs másodpercenként 1000 különböző kép rögzítése 1024×1024 bit felbontással. Polimerek esetében ez másodpercenként 1 gigabit írási sebességnek felel meg. Feltételezések szerint hamarosan elérhető lesz vele az 1 terabit (=10¹² bit) per sec. kiolvasási sebesség is.

Azonosító kártyák. – Útlevel, vízum, ID, jogosítvány, belépőkártyák, utazási csekkék és egyéb dokumentumok védelme.

Értékhordozók. – Értékjegy, értékpapír, bankjegy, bélyeg, csekk, kötvény, részvény, hologramos műanyag alapú bankkártya, hitelkártya stb. védelmére.

Hologramot is tartalmazó intelligens/okos nyomathordozók, címkék és csomagolóanyagok (*Holographic Smart Labels*). – A rádiófrekvenciás (RFID) címkékhez hasonló márka-, termék- és dokumentumvédelmi eszközök.

Holografikus tépőzárak/tépőszalagok (*Tear-off Holographic Tapes*).

Hologramos műanyag kártyák (*Plastic Cards with Hologram*).

Hologramos öntapadó címkék gyártása (*Holographic Self-adhesive Labels*).

Olvasnivalók: **A hologramok és optikailag változó eszközök** (*Holograms & Optically Variable Devices*: www.security-printing.co.uk/holograms-ovds.php); **Az OVD és a csak géppel leolvasható védelmi eszközök használata biztonsági dokumentumok védelmére. Részletes technológia leírás** (www.patentstorm.us/patents/5403040-fulltext.html); **Vaknyomású OVD hologramok** (*Embossed Optically Variable Devices*: www.freepatentsonline.com/20060151989.html); **Hologramalkalmazás ügyben gyakran feltett kérdésekre adott válaszok** (www.lightimpressions.com/holograms.html honlap FAQ linkje); **A holografikus csomagolás és jövője** (*Holographic Packaging – The Next Dimension?* (www.cfcintl.com/newsletter/holographic_packaging); **Az öntapadó holografikus címke** (*Self Adhesive Holographic Label*: www.optaglio.cz); **Holnapai eszközök a mai hamisítás ellen** (*Tomorrow's Security Solutions for Today's Fraud*: www.isp-vft/index.htm); **A holográfia teljes ismeretanyaga tömören** (<http://en.wikipedia.org/wiki/Holography>); **Hamisítás-ellenőrző detektor-készülékek** (*Counterfeit Detectors*: www.idhouse.com/detect1.htm).

A BIZTONSÁGI NYOMTATÁS SZOFTVEREIBŐL

Giotto Security in Design: Biztonsági nyomtatványtervező szoftver: www.pitagora.ch/giotto.htm

Szoftver hologramos biztonsági fólia nyomtatáshoz: www.hagueprint.com/SOFTWARESOLUTIONS/tabid/62/Default.aspx

TrustMarking Basic: Fuji – Xerox szoftver, a rejtett szövegek előállítására: www.fujixeroc.co.jp/eng/headline/2004/1213_fxps.html

4. táblázat. Nyomtatott és elektronikus szaklapok

Lapcím	Témakör	Elérhetősége a világhálón
Packaging Design Magazine	Csomagolástervezés	www.packagedesignmag.com
Packaging Digest	Tallózás a megjelent irodalomban	www.packagedigest.com
Packaging Digest China	Tallózás a megjelent irodalomban	www.packagedigestchina.com
RFID Journal Live	Élő online RFID újság	www.rfidjournal.com
Grafics Arts Monthly	Nyomdaipari havilap	www.graficartsmonthly.com
Converting	Postpress	www.converting.com

Troy Group Security Printing szoftverek a mikrokarakterek, rejtett digitális aláírások előállítására: www.troypgroup.com/SecurityPrinting/Products/Paymentsoftware/index.asp

FraudOne SOFTPRO's flagship fraud detection solution: védelem a csekkhamisítók ellen: www.signplus.com/en/solutions/fraudone.php

SAKKÖNYVEK

Pira kiadványok (www.intertechpira.com)

A vízjelhasználat fejlődési irányai (Developments in Watermarking)

Nanotechnológia a papír- és kartoncsomagolásban (Nanotechnology in Paper & Board Packaging)
Intelligens és okos csomagolás (Intelligent & Smart packaging – USA 2005), 104 £

A nyomtatott RFID fejlődése (Developments in Printed RFID), 280 £

Bevezetés a mai elektronikus csomagolásba (Packaging Electronics: Understanding of Packaging Electronics Today), 285 £

Biztonsági címkék (Security Labels & Tags), 280 £

Biometrikai fejlesztések (Developments in Biometrics)

Diagnosztikus (hibafelismerő) csomagolás (Diagnostic Packaging), 280 £

Intergraf kiadványok

(www.intergraf.eu/Publications.htm)

A nyomdaipar fejlődése (Evolution of the Graphic Industry)

Információbiztosítási hírlevél (InfoSecure Newsletter)

Amazon kiadványok

A címke- és a címkézés technológia enciklopédiája (Michael Fairly: Encyclopedia of Labels and Label Technology), 151.99 £

Optikai dokumentumbiztonság (Rudolf L. Van Renesse, Optical Document Security), 139 £

Bevezetés a biztonsági nyomtatásba (Richard D. Warner, Introduction to Security Printing), 45 £

3M kiadványok

(www.3m.com/security/en/sec_products.html)

Biztonságitermék-katalógus (Security Product Catalog): Márkavédelem. Adat-, infrastruktúra- védelem, Dokumentumvédelem. Biztonsági laminálás. Megszemélyesítő rendszerek

Biztonsági azonosító kártyák (Security ID Cards)

A Vandagraf Kiadó ajánlata

(www.vandagraf.com)

Márkavédelem a nemzetközi piacokon. Átfogó műszaki, gazdasági és biztonságtechnikai eljárás ismertető. Csomagolt márkás termékek ellen elkövetett bűnesetek elemzése. A márka- védelmi, a biztonsági címkézést és csomagolást érintő eljárások fejlődési trendjei és jövője. (*The International Market for Brand Protection Solutions – A Comprehensive Techno-Economic Report*) USD \$ 4,399

HASZNOS INTERNETCÍMEK

A digitális információtechnikai és nyomtatási biztonsági szakemberek weboldala: Security Management Online, www.securitymanagement.com/library/

Biztonsági információfigyelő: www.securityInfoWatch.com

A témakör definícióinak gyűjteménye: www.SearchSecurity.com.Definitions

Minden tudnivaló, ami a biztonsági nyomtatással kapcsolatos: http://en.wikipedia.org/wiki/security_printing

Holotek hologramgyártó vállalat: www.holotek.com.cn

Állami Nyomda (www.allaminyomda.hu). Az ország legnagyobb, nemzetközileg elismert, biztonsági termékeket gyártó, fejlesztő vállalata. Főbb termékei: a műanyag bankkártyák, okmánybiztonsági termékek, értékcikkek, elektronikus dokumentumok, rádiófrekvenciás (RFID) címkék stb.

Pénzjegynyomda (www.penzjegynyomda.hu).

A hamisítás elleni védelem legigényesebb nyomdatechnikai eljárása a metszet-mélynyomatás. Magyarországon ezzel a technológiával kizárólag a *Pénzjegynyomda Rt.* rendelkezik, amelynek egyik metszetmélynyomatással készült termékcsoportjával – a bankjegyekkel – mindennap találkozunk.

Diósgyőri Papírgyár, DIPA (www.dipa.hu). Az ország egyetlen biztonságipapír-gyártó vállalata.

Főbb termékei: bankjegy, okmány, értékcikk és jegy alappapír; vízjeles nyomópapírok, biztonsági kartonok, vízjeles számlapapír, közhi-teles okmányok és az öntapadós biztonsági papír.

5. táblázat. Nemzetközi konferenciák, kiállítások, szemináriumok és kísérőrendezvények

Megnevezés	Tárgykör	Hely és időpont	Elérhetőség a világhálón
CSI 2007 Annual Conference	Mai biztonsági technikák, anyagok és eszközök	2007. nov. 4–6., Virginia (USA)	www.CSIannual.com
Emerging technologies (The Game of Cat and Mouse)	A feltörekvő új technológiák. (A macska–egér játék)	2007. aug. 13–15., Melbourne, Convention Centre	www.cio.com.au
Security Printing & Alternative Solutions	Biztonsági nyomtatás és alternatív megoldások Közép-Kelet-Európában és Oroszországban	2008. január 22–23., Ljubljana (Jugoszlávia)	www.pyrabelisk.com
Watermark Conference 2007	Vízjel konferencia	2007. Suzdai (Oroszország)	www.watermark-conference.com
14. Pan-European High Security Printing Conference	14. Pán-európai biztonsági nyomatás konferencia	2007. március 28–29., Budapest Hotel	www.goingtomeet.com/ conventions/
European Biomarkers Summit	Európai biometriai konferencia	2007. szept. 4–5., Amszterdam	www.selectbio sciences.com/
4. Annual Security Printing Conference	Biztonsági nyomtatás. Anya- gok, technológiák, ellenőrzés.	2007. március 28–30., San Francisco	www.gotomeet.com/ details/7206
Annual Printable Electronics & Displays Conference & Trade Fair	Nyomtatható elektronikák és diszpléjek/monitorok konferenciája	2007. október 17–19., San Francisco	http://imi.maine.com/ completed/printelt07/html
Security & Risk Management Trade Show	Biztonság és kockázatkezelés	2007. november 7–10., Velece (Olaszország)	www.pcsi2007.org
NIP 23 International Conference on Digital Printing Technologies	Biztonsági nyomtatás. Eljárás-összehasonlító	2007. szept. 16–21., Alaszka	www.imaging.org/ conferences
Commercializing Printed RFID	Az RFID-technika széles körű bevezetésének a feltételei	2007. szeptember 5–7., Chicago	Letölthető brosúra: sophie.sipsma@pira- international.com
2nd Annual Fine Particle Application Conference	Mikrorészecskék, mikroírások, MicroTaggants-alkalmazások	2006. október 18–20., Las Vegas (Nevada)	http://imi.maine.com/ completed.html
1st RFID Technology Integration Symposium	Az RFID széles körű bevezeté- sének a feltételei	2007. május 23–24., Arizona	http://imi.maine.com/ completed.html
Holo Pack –Holo Print	A holografikus termékek cso- magolóstechnikai alkalmazásai	2007. nov. 14–16., Hongkong	www.eventseye.com/fairs/ event_tc12_40_1.html
További rendezvények nyilvántartója: www.eventsseye.com/fairs/trade_fair . A már lezajlott rendezvények honlapjaira azért irányítjuk olvasóink figyelmét, mert a konferencia utáni időkből már könnyebben és általában térítésmentesen lehet hozzájutni az elhangzott előadások és kísérőrendezvények anyagához.			