Dénes Tamás
matematikus-kriptográfus

email: tdenest@freemail.hu

SZTEGANOGRÁFIA

Rejtett információk rejtjelzés nélkül

"A történelem mindössze arra tanít meg bennünket,
hogy az emberiség semmit sem tanul a történelemből."
Albert Einstein

Néhány hónappal a 2001. szeptember 11-i terrortámadás előtt, *ECHELON az e-társadalom információpajzsa?* címmel megjelent [3] cikkemet az alábbi kérdésekkel fejeztem be:

„- Valóban teljesen kiszolgáltatottak vagyunk az ECHELON mindent behálózó információs pajzsának?
- Az e-társadalom szükséges velejárója az ECHELON?
- Védekezhetünk-e, és ha igen, akkor hogyan, a totális információs kiszolgáltatottság ellen?
- Kell-e az átlagembernek is védekezni a lehallgatás ellen?"

Maga a téma és e kérdésekre adható válaszok régóta foglalkoztatnak. Arra a koreográfiára azonban, hogy míg a fenti cikkemet leközlő folyóirat példányain éppen csak megszáradt a nyomdafesték, az élet történelmi választ produkált a szinte még fel sem tett kérdésekre, én sem számítottam. Pedig így történt: 2001. szeptember 11-én a Földünket körülvevő információpajzs, akárcsak a természetes védelmet nyújtó ózonpajzs, kilyukadt!
Az ECHELON szimbolikus jelentései (harcvonal, harcrend) valóságossá váltak, a fenti kérdések megelevenedtek és a sok milliárd dolláros titkos befektetés, amely a *„terrorizmus elleni védekezés zászlaja alatt”* az elmúlt két és fél évtizedben történt, nyilvánvaló kudarcot szenvedett.

> A titokról, a globális kommunikációról, az e-világ biztonságáról alkotott „egyértelmű képet” kényszerül az emberiség átfesteni. A történelem dupla felkiáltójellel hívta fel mindannyiunk figyelmét arra, hogy a jövendő információs társadalom kulcsfogalma a biztonság legyen!

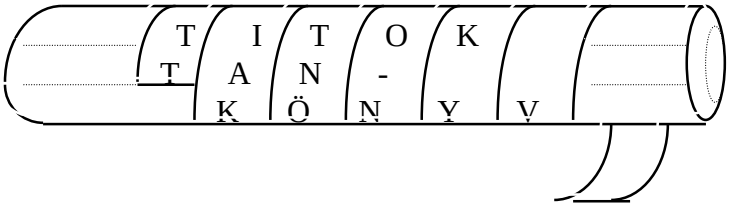
Ehhez szeretnék az itt következő gondolatokkal hozzájárulni, melyeket ajánlok a terrorkatasztrófa áldozatainak emlékére, azzal a meggyőződéssel, hogy e gondolatok hozzájárulhatnak ahhoz, hogy ne csak a terrorizmusnak, de a virtuális „információ pajzsnak” se legyenek újabb ártatlan áldozatai.

A titok rejtés gyökerei

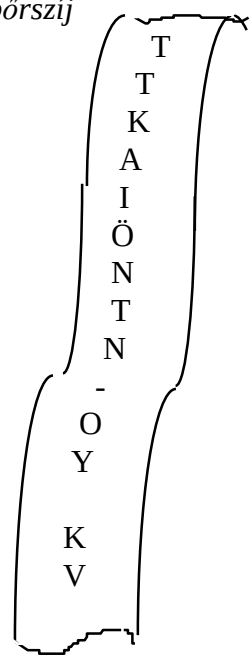
A kriptográfia (rejtjelzéstan) eszköztárában a titok elrejtésének és továbbításának ősi módja a *szteganográfia*. Ez egy görög eredetű szó, melynek jelentése: *„egy bizalmas közlést elrejtő, álcázó titkosírás”*, mondhatjuk *„rejtett írásnak”*, vagy inkább *„rejtett üzenetnek”* is. Tulajdonképpen e módszercsalád legősibb megoldásainál nem is igen beszélhetünk titkosírásról, csupán a titok (ami nem feltétlen írás, hanem bármely írásbeli, képi, vagy szóbeli üzenet) elrejtéséről és rejtett továbbításáról.
A szteganográfia modern, napjainkban is használatos megfelelőjét *„rejtett csatornának”*, vagy az angol nyelvű irodalomban *„subliminal channel”*-nek nevezik. Rejtett csatornát használtak a II. világháború folyamán azok a hírszerzők, akik beépültek a német katonai hírközpontba és német katonai üzenetek közé rejtették kémjelentéseiket.
A szteganográfia napjaink és a közeljövő e-társadalmában (elektronikus társadalom) is szerepet kap. A jövő új dokumentum védelmi korszakát a digitális ujjlenyomat elterjedése fogja jelenteni.

Már Plutarkhosz, az ókori Rómában élt görög író részletesen ír a *spártaiak szkitalájáról*, az egyik legrégibb ismert titokrejtési módszerről: bizonyos vastagságú farúdra bőrszíjat tekertek fel az alábbi 1.ábra szerint úgy, hogy a menetek szorosan egymás mellé kerüljenek.

1. ábra *szkitala feltekert bőrszíjjal*



A letekert bőrszíj



A szöveget a rúd hossztengelyével párhuzamosan a szíjra írták egymás alatti sorokba úgy, hogy minden sorban minden menetre egy-egy betű kerüljön. Így a szíjat a rúdról letekerve, értelmetlen betűsorozatot láthatott az, akinek nem volt pontosan olyan rúd a birtokában, mint

a szöveg írójának. Az üzenet címzettjénél természetesen volt ilyen rúd, így a szíjat arra feltekerve a szöveg olvashatóvá vált.

Szintén az ókorból származó módszer, hogy *az üzenetet közvetítő futár fejét kopaszra nyírták, majd a fejbőrére tetoválták a rejtendő üzenetet.* Megvárták, míg kinő a haja és így küldték el a címzetthez. A címzett lenyíratta a futár haját és elolvasta a szöveget. Ez a módszer is túlélte az évezredeket és még a 20. század első felében is sikeresen használták a titkos üzenetek célbajuttatására.
Az eljárás elég hosszadalmas volt, így csak „ráérő üzeneteket" lehetett ily módon elküldeni, de ennél nagyobb hibája, hogy a haj visszanövéséig a titkos üzenet mindenki számára olvasható volt. Ezt persze igyekeztek megoldani a futár teljes elkülönítésével.

Ne gondolja senki, hogy eme szteganográfiai módszerek csak, mint történeti érdekességek léteztek! Az éppen csak elhagyott 20. század titkosszolgálati eszköztárának is fontos részét képezték a titkos üzenetek célbajuttatásának e módszerei.

A II. világháború angol titkosszolgálatának külön részlege foglalkozott a titkos üzenetek rejtjelzésével, illetve az ellenséges rejtjeles üzenetek megfejtésével. Ennek a rejtjelző csoportnak volt a vezetője Leo Marks, akinek különös ötlete támadt a titkos kódok ügynökökhöz való biztonságos eljuttatására. Azt tudjuk, hogy „nincs új a Nap alatt", csak a technika változik, mégis meglepő volt a gondolat, hogy a titkos kódot egy hétköznapi *selyemsál* egyik felére nyomtatták, amelynek másik oldala a szokásos mintákkal volt megfestve. Így az ügynökök, mint megszokott viselettel nyakukban, feltűnés nélkül mutatkozhattak a nyilvánosság előtt és juttathatták el a titkos kódot a címzettnek. A módszer jóval gyorsabb és biztonságosabb, mint a fejbőrre tetoválás, de csak akkor, ha sikerül teljes titokban tartani. Az angol titkosszolgálatnak ez annyira sikerült, hogy jóval a II. világháború után is még használták a selyemsál módszert, amely tulajdonképpen csak Leo Marks [9] memoár kötetében került nyilvánosságra.

A szteganográfiai módszerek tagadhatatlan gyöngyszeme a *„láthatatlan írás"*. Már Hérodotosz görög történetíró az i.e. 5. században említést tesz valamiféle *„láthatatlanná tett írás"*-ról, amelynek lényege, hogy a fakéregre, falevélre, papírra olyan folyadékkal (tintával) írták a szöveget, amely száradás után láthatatlanná vált, ám valamilyen eljárással a címzett újra olvashatóvá tudta tenni az üzenetet.
Ezeket a folyadékokat nevezik *szimpatetikus tintának*, a modern szóhasználatban *„vegytintának"*. A legegyszerűbb szimpatetikus tintát maga a természet szolgáltatja, ez *a tej és a citromlé*. Egyik sem hagy nyomot a papíron, legfeljebb ha a tollheggyel felkarcoljuk a papírt. Mindenki megpróbálhat otthon tejbe mártott tollal írni, majd száradás után meleg (nem forró!) vasalóval vasalja át a papírt és a rejtett szöveg halványan előtűnik.

A kémia fejlődésével egyre több szimpatetikus recept vált ismertté. Csak néhány mutatóba: kálium-hidroxiddal, nátrium-hidroxiddal, szódával irt szöveg fenolftaleinnel hívható elő (az írás vörös lesz). Vagy fordítva is csinálhatjuk, azaz a fenolftaleinnel irt szöveget szódával hívjuk elő, esetleg ammóniák fölé tartjuk. Ferro- vagy ferrición-kálium híg oldata is használható láthatatlan írásra, majd valamilyen ferro- vagy ferrisóval kezelve sötétkék betűk jönnek elő. Ferrocián-kálium és rézszulfát vörösbarna szint ad, a szulfocián-kálium és ferri-klorid karminvöröset, míg a szalicilsav és vas-klorid kékeslila színű írást eredményez (lásd [14]).

A kémia után az újabb fizikai eredmények is hasznosításra kerültek a *láthatatlan írás* előállításánál. Az *ultraibolya fény* bizonyos anyagokról úgy verődik vissza, hogy hullámhossza nagyobb lesz. Ha ez a hullámhossz már a látható fény tartományába esik, akkor az anyag a láthatatlan ultraibolya sugarakkal megvilágítva, látható (világító) sugarakat bocsát ki. Ezt a jelenséget használják fel napjainkban is a bankjegyek hamisítás elleni védelmére, amikor például színtelen kininoldattal írják meg a titkos szöveget (kódsorozatot), amit azután kvarclámpával világítanak meg. A kvarclámpa láthatatlan ultraibolya sugarai halványkék színben, látható fény alakjában verődnek vissza az írásról, így a szöveg olvasható.

A rejtett írásnak egy igen egyszerű változata a következő:
Egy könyv, vagy újság nyomtatott szövegében apró jelölésekkel, általában *pici pontokkal megjelölünk bizonyos betűket* úgy, hogy a megjelölt betűk összeolvasásából pontosan a kívánt rejtett üzenetet olvashassa ki a címzett. Például az alábbi szövegben a megjelölt betűk fölé pontot tettünk:

. . . .
„Ha sokszor eszel keveset, nem gyarapodik tested feleslegesen. Ezt tedd ha karcsúságot
. .
remélsz!” *(Az elrejtett szöveg: HOLNAP ITT LESZ A KÉS)*

Természetesen a komolyabb titkosírásokban a rejtett szöveg nyelve is titkot képez, ezért a csak a magyar nyelvre jellemző hosszú magánhangzókat célszerű a megfelelő röviddel helyettesíteni, amelytől a szöveg az olvasó számára még értelmes marad, hiszen például a számítástechnikában (pl. régebbi szövegszerkesztők) a magyar ékezetes betűk hosszú ideig nem léteztek, a szövegeket mégis mindenki megértette. Ugyanígy javasolt a rejtett betűk megjelölésére is kevésbé feltűnő jelölést használni (például pontok helyett apró tűszúrások). A pontozásnál jóval megbízhatóbb megoldás, ha például egy cérnaszálra a pontoknak megfelelő távolságokban csomókat kötünk. Így mód nyílik a szöveg és a *titkos kulcs* (ez a csomózott cérnaszál) szétválasztására, ami kriptográfiai szempontból nagy előny, hiszen ekkor lehetőségünk van az úgynevezett titok megosztásra. (Ez az ötlet, mint láttuk, a szkitaláknál már több ezer éve megszületett.) A titokmegosztás azt jelenti, hogy a titokhoz (a rejtett üzenethez) csak úgy lehet hozzájutni, ha a szöveg és a cérna (a titkos kulcs) egy kézben van.

A szteganográfia, mint módszer alapgondolata tehát, hogy a nyílt üzenetből (amely önmagában is értelmes szöveg) egyáltalán nem érzékelhető, tartalmaz-e rejtett üzenetet, vagy sem!

Akárcsak a mimikrinél a rejtett üzenet észrevehetetlenül beleolvad környezetébe, a nyílt szövegbe. Ebből következik, hogy az így rejtett üzenetnek nem csak a megfejtése reménytelenül nehéz, hanem annak kiderítése is, hogy egyáltalán `titokkal` állunk szemben. Hiszen így tulajdonképpen minden nyílt szöveg "gyanús" lehet, és valóban bármely szöveget alkotó betűkből számtalan másik értelmes szót, mondatot elő lehet állítani.

Hogy valóban nincs új a nap alatt, arra igazi szemléltető példa, hogy a fenti *szöveg a szövegben titkosítás* már 450 évvel ezelőtt Girolamo Cardano (1501-1576) intervallum rejtjelzésében megjelent. Cardano *intervallum rejtjelzés*-e ugyanis éppen a betűk közötti távolságokon, azaz a 2.ábrán látható rejtjelző táblán alapult.

2.ábra

A	a e	r n	c b
B	i o	d l	g q
C	u s	m f	p t

A módszert az egyszerűség kedvéért egy példán mutatjuk be. Legyen az üzenet: *csacsi*. (a lépéseket a 3.ábrán követhetjük)

- Írjuk egy üres levélpapír bal felső sarkába az A,B,C betűk bármelyikét. Ez csupán a szöveg kezdetét jelöli (C).
- Helyezzük a táblázat üres négyzetét a megjelölt betűre, majd a *csacsi* első betűjét *(c)* tartalmazó, nagybetűvel jelzett mező jelét *(A)* írjuk a papírra pontosan a *c* betű fölé (lásd 3.ábra).
- Most helyezzük a táblázat üres négyzetét az utoljára felirt nagybetűre és keressük ki a táblázatból a következő betűt az *s*-et. Ezzel ugyanúgy járunk el, mint az előzőkben, azaz a táblázatbeli *s* betű fölé írjuk a papírra a mező jelét *(C).*
- A fenti lépéseket addig folytatjuk, míg van hely a levélpapír adott sorában, majd a legelső lépést megismételve új sort nyitunk és az eljárást folytatjuk a küldendő üzenet végéig.
- A megfejtő dolgát azzal nehezítjük meg, hogy az üresen maradt helyeket tetszőleges betűkkel töltjük ki ! (lásd 3.ábra)

Természetesen jó, ha értelmes szöveggé egészítjük ki a rejtett szöveget, de nem feltétlenül szükséges.

3.ábra

CSOROGATEAAFALONAMIGACSIGAMACSUDALASSANHALADHATNACSENDBEN

↓ ↓ ↓ ↓ ↓ ↓ ↓

kezdőpont (c) (s) (a) (c) (s) (i)

Az üzenet fogadójánál természetesen ugyanolyan táblázat volt (lásd 2.ábra), mint a küldőnél. Így a fenti eljárást a kezdőponttól elvégezve olvashatóvá vált a rejtett üzenet.

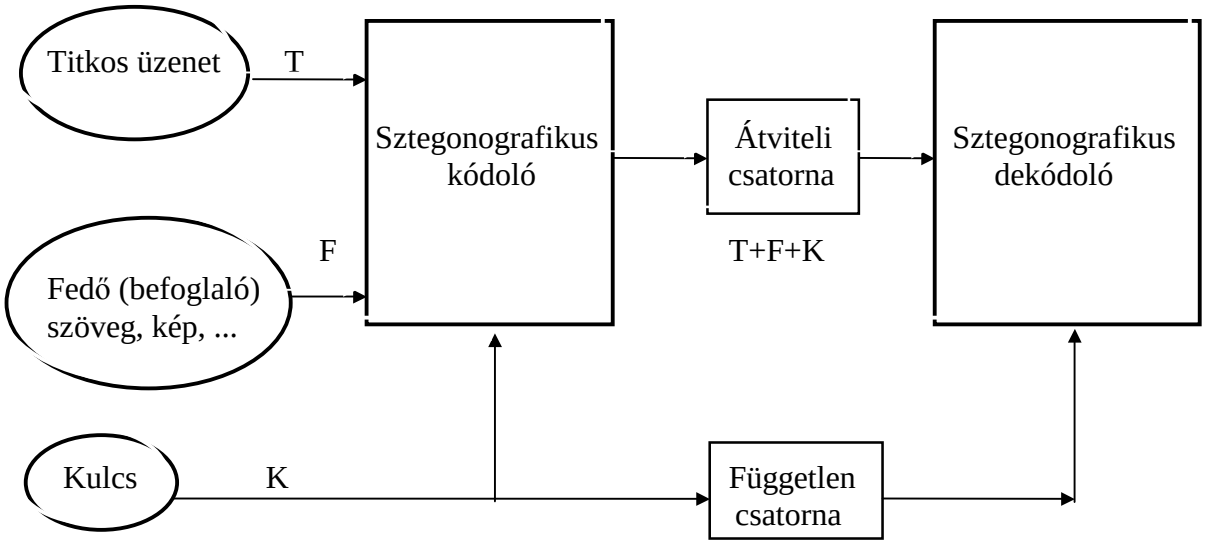
Mai szemmel ez az eljárás érdekes, de nem túl praktikus, mivel elég nehézkes a táblázat használata, sok helyet használ az információtartalomhoz képest. Cardano a nehéz érthetőség kritikáját több kortársától meg is kapta, akik akkor még nem tudhatták, hogy Cardano ezzel messze megelőzte korát és elvetette a modern, táblázaton alapuló rejtjelzés, valamint a *modern szteganográfia* magjait.

Szintén a szteganográfia módszercsaládjába tartoznak azok az eljárások, amelyek fotózási technikákat alkalmaznak a szöveg, vagy ábra elrejtésére. Ilyen a *mikropont módszer*, ahol a rejtett szöveget akkorára kicsinyítik, hogy az a normál szövegben egy pontnak feleljen meg (például mondatvégi pontnak, vagy a szöveg végén levő felkiáltójel alatti pontnak, vagy bármely *i, ö, ü* betű ékezetének). Így a címzettnek elég azt tudnia, hogy hol helyezkedik el a nyílt szövegben az a pont, amely a rejtett üzenetet tartalmazza és azt megfelelő nagyítással olvashatóvá kell tennie.

Szteganográfia a digitális világban

A szteganográfia tehát az adatok elrejtésének művészete és tudománya egyszerre, amelyhez napjaink digitális technikája igen kedvező megvalósítási feltételeket teremtett. Mindezt úgy éri el, hogy az úgynevezett *„fedő, vagy hordozó adatok”* között a tulajdonképpeni rejtett adat (üzenet) nem is észlelhető. A szteganográfia általános modelljét mutatja a 4.ábra, melynek természetesen számos algoritmikus és technikai megvalósítása lehetséges.

4.ábra



Ez a modell lényegesen különbözik a kriptográfiáétól, hiszen ott a rejtés (rejtjelzés) nyilvánvalóan felismerhető. Egy rejtjeles szöveg ugyanis teljesen értelmetlen, illetéktelenek számára értelmezhetetlen (zajszerű) karaktersorozat, hiszen a rejtjelzési eljárásnak pontosan az a célja, hogy illetéktelenül ne lehessen a rejtjeles szöveg tartalmát elolvasni.

A szteganográfiai módszerek közös jellemzője, hogy a titkot (az üzenetet) *nem módosítják, csupán csak eredeti formájában elrejtik, álcázzák.*

Azonban ezeknek az eljárásoknak gyengéje, hogy *ha a rejtési módszer típusát ismerjük, akkor aránylag könnyen hozzájuthatunk a titkos üzenethez*, amely már közvetlenül megérthető (nyíltan olvasható). Tehát jelentős értéket képviselő titok esetén (vagy éppen olyan esetekben, amikor, mint a terrortámadás esetén élet-halál függ tőle), akkor *nagyon megnő az árulás veszélye*. Ezért célszerű napjaink modern technikája mellett a szteganográfiai és kriptográfiai módszerek együttes alkalmazása, amellyel igen magasfokú biztonság érhető el.

A digitális ujjlenyomat

A jelenlegi számítógépes biztonsági problémák közül az egyik legégetőbb az, hogy el lehessen dönteni egy dokumentumról, hogy az eredeti, vagy hamisított. A hagyományos módszerek (vízjel, fémszál, különleges papír, hologram, stb.) mindegyike az eredetit igyekszik megkülönböztetni a hamistól.

A digitális ujjlenyomat az egyedi azonosítást teszi lehetővé, vagyis képes egy dokumentumot nemcsak a hamistól, hanem egy másik eredetitől is megkülönböztetni.

A probléma eredete az USA és a Szovjetunió közötti fegyverzetellenőrzési szerződések megkötése idején merült fel, nevezetesen oly módon, hogy a számbavett rakétákat egy eltávolíthatatlan matricával kellett megjelölni, hogy azok bármikor egyedileg azonosíthatók legyenek. Ugyanakkor a jogellenesen másolt szoftverek digitális hang- és képanyag felismerése is oly módon lehetséges hatásosan, hogy a hamisítás könnyű felismerhetősége érdekében az adathordozót egyedi azonosítóval látják el.

Általában a nyomdatechnikában bármilyen biztonsági papír előállítása olyan ismertető jelekkel történik, amelyek az egyedi azonosítást nem teszik lehetővé. Azt a biztonsági gyakorlatot, amivel az előzőkben leírt biztonsági fenyegetettségek megszüntethetők, *digitális ujjlenyomat*nak nevezzük. J. Simmons több mint két évtizedig vezette az Egyesült Államok nukleáris fegyvereinek elektronikáját gyártó legnagyobb cég, a Sandia National Laboratoriesban a digitális ujjlenyomatok kutatását (lásd [12],[13]). A Sandia laboratórium eredményeit, amelyek alapvető alkalmazási területe a fegyverzetellenőrzés és a felügyelet nélküli szeizmográfok kifejlesztése volt, más területeken is igyekeztek felhasználni. Ilyen terület a pénzhamisítás megakadályozása, amely például az 1999-ben kiadott, új százdolláros bankjegyekben valósult meg. A Sandia által javasolt megoldás a következő:

A bankjegyek papír anyagának gyártása közben, tehát még pépes formában, árnyékolt üvegszálakat különböző hosszúságban a pépbe kevernek, ezek természetesen megszáradásuk után rögzítődnek, és egy véletlenszerű irányultságot vesznek fel (a szteganográfiai modellnek megfelelően „elrejtőznek" a papír anyagában). Ezután egy sor érzékelővel el lehet érni, hogy a sorban lévő, és adott sorral egyező végponttal rendelkező üvegszálak, mivel azok megfelelő burokkal vannak ellátva, a fényt csak saját végpontjukig vezetik. Mivel az üvegszálak hossza véletlenszerű, ezért egy vonali megvilágításból egy véletlenszerű ponthalmaz adódik. Ezt természetesen több vonalon meg lehet ismételni. Az eredményként létrejövő ponthalmaz megfelelő kódolásával el lehet érni, hogy az adott bankjegyre jellemző kód, vagy kódsorozat jöjjön létre. Ez a kódolási eljárás a hibajavító kódokat is magában foglalja. Ezeket a kódokat digitális aláírással, esetleg más adatokkal, például sorszámmal, kiadási időponttal kiegészítve a kibocsátó bank hitelesíti. Ilyen módon az aláírt sorozat és a bankjegyben lévő, véletlenszerűen elszórt üvegszálak kölcsönösen megfeleltethetők egymásnak. Ha az üvegszálak száma és hosszúságuk megfelelően van meghatározva (ami nem egyszerű és mély matematikai meggondolásokat igényel), akkor a bankjegyeken lévő kódok egyértelműen meghatározzák a bankjegyet. Egy ilyen eljárás, szemben a különböző nem egyedi nyomdai megoldásokkal, az egyediségből adódóan számos előnnyel bír. A papír anyagában lévő jellemzők pedig másolhatatlanná teszik a bankjegyeket.

A digitális ujjlenyomat tehát a digitális aláírás egy olyan speciális esete, amikor az aláírásra kerülő üzenet egy része, vagy egésze, a hordozó anyag fizikai jellemzőiből adódik. Ez pontosan a szteganográfia és a kriptográfia egyesítése.

A digitális ujjlenyomat tehát nem teszi lehetetlenné a másolást, azonban az eredeti és a hamis bankjegy, csupán a bankjegy felhasználásával megkülönböztethetővé válik, mert az egyedi sajátosságok (a bankjegy anyagába bevitt jelző elemek) elhelyezkedése nem másolható.

A pénzhamisítás megakadályozására egy ugyancsak digitális ujjlenyomatokra visszavezethető módszer került kidolgozásra és felhasználásra Németországban, a német márka bankjegyek védelmére (lásd [1]).

Érdekes megjegyezni, hogy míg a Sandia-nál az elméleti eredmények sokkal hamarabb rendelkezésre álltak, mint Németországban, a gyakorlati alkalmazásra később került sor.
Az 1990-es években kiadott német márka (DEM) bankjegyek az összes címletekben, kivéve az ötmárkást, már digitális ujjlenyomattal voltak védve.

Tehát a digitális ujjlenyomat alkalmazásával a hamisítókat egyrészt el lehet rettenteni a hamisítástól, másrészt a hamisítást könnyen és gyorsan föl lehet ismerni, hiszen maga a dokumentum tartalmazza az ehhez szükséges összes információt. Így a hamisítás ténye helyben, azonnal megállapítható.

A digitális ujjlenyomat biztonsági papírok előállítására is alkalmas, sőt egy újonnan vizsgált és bevezetéshez közel álló területe a digitalizált analóg jeleknek, például digitális hangszalag, CD lemez, vagy videoszalag másolás elleni védelme.

A képbe rejtett üzenet

A. Einstein cikkem elején idézett gondolatának mély gyökerei vannak a tudomány és technika történetében, hiszen minden jelentős tudományos, technikai eredmény felhasználása kockázatokat rejt magában, mivel az emberi fantázia a pozitív és negatív alkalmazásokat tekintve is korlátlan.
Amint az az eddigiekből kiderül, a szteganográfiai módszereknek igen kedvező tehnikai hátteret biztosít a „digitális világ”. *A digitális ujjlenyomat véletlen eloszlású, papír anyagába bevitt szennyeződéseinek megfeleltethetünk például egy digitális képbe tudatosan elrejtett üzenetet, amelynek bináris kódolása éppen a több millió képpont között észrevehetetlen idegen szennyeződéseknek felel meg!*

Íme a rejtjelzés nélküli információrejtés egyik lehetősége, ahol a hordozó, vagy fedő képhez hozzáadjuk a titkos üzenet binárisan kódolt alakját, így a szteganogram egy digitális kép lesz. Az 5.ábrán szereplő bináris jelsorozat valóban az EZ A TITKOS SZÖVEG! nyílt üzenet ASCI kódjának binárisan kódolt alakja (19x8=162 bit), amely így a szteganogram majdnem 1 millió képpontja között észrevétlenül rejtőzködik.

5. ábra

(Hordozó, vagy Fedő kép)

Szteganografikus kódoló

EZ A TITKOS SZÖVEG!
(binárisan kódolva)

0 1 0 0 0 1 0 1 0 1 0 1 1 0 1 0
0 0 1 0 0 0 0 0 0 1 0 0 0 0 0 1
0 0 1 0 0 0 0 0 0 1 0 1 0 1 0 0
0 1 0 0 1 0 0 1 0 1 0 1 0 1 0 0
0 1 0 0 1 0 1 1 0 1 0 0 1 1 1 1
0 1 0 1 0 0 1 1 0 0 1 0 0 0 0 0
0 1 0 1 0 0 1 1 0 1 0 1 1 0 1 0
1 0 0 1 1 0 0 1 0 1 0 1 0 1 1 0
0 1 0 0 0 1 0 1 0 1 0 0 0 1 1 1
0 0 1 0 0 0 0 1

SZTEGONOGRAM

A titkos üzenet fedőképbe rejtve

Sztegonografikus Dekódoló

0 1 0 0 0 1 0 1 0 1 0 1 1 0 1 0
0 0 1 0 0 0 0 0 0 1 0 0 0 0 0 1
0 0 1 0 0 0 0 0 0 1 0 1 0 1 0 0
0 1 0 0 1 0 0 1 0 1 0 1 0 1 0 0
0 1 0 0 1 0 1 1 0 1 0 0 1 1 1 1
0 1 0 1 0 0 1 1 0 0 1 0 0 0 0 0
0 1 0 1 0 0 1 1 0 1 0 1 1 0 1 0
1 0 0 1 1 0 0 1 0 1 0 1 0 1 1 0
0 1 0 0 0 1 0 1 0 1 0 0 0 1 1 1
0 0 1 0 0 0 0 1

EZ A TITKOS SZÖVEG!

Egy fentihez hasonló részletgazdag képben, főleg, ha színes, a néhány száz *rejtett pont*, amely akár életbevágóan fontos üzenetet is takarhat, mint csepp a tengerben tűnik el. Ugyanez vonatkozik a digitalizált hanganyagokra, vagy videofelvételekre is, mint a szteganogramok fedő információhordozójára. Mindezek ismeretében akár a mikropont módszer modern, digitális változatát is könnyen elképzelhetjük, hiszen a fenti kép egy lényegtelen részlete is több száz képpontból áll.

A rejtjelzéshez képest tehát igen különös módszerrel állunk szemben, amelynek lehetőségei beláthatatlanok és a digitális technika rohamos fejlődésével méginkább azok lesznek. A szteganogramokba rejtett üzenetek lehallgatása csak a digitális kommunikáció megszüntetésével lenne elérhető. Ezzel nem csupán fél évszázadot lépnénk vissza, a számítástechnika előtti korba, hanem megrendülne az előttünk álló információs társadalom alapja, a globális kommunikáció.

Az ECHELON információs pajzsán pillanatnyilag tátongó lyukat tehát csak egy olyan „dugóval" lehet betömni, amelyik annyira régi, hogy már szinte egészen új. *A szteganográfia eszköztára az információ biztonság régi-új perspektívája.*

Irodalomjegyzék

[1] A. Beutelspacher: Cryptology. The Mathematical Association of America, 1994.

[2] Dénes Tamás: DIGITÁLIS UJJLENYOMAT (A dokumentumvédelem új korszaka)
Magyar Távközlés, XI.évf. 5.szám, 2000. május

[3] Dénes Tamás: ECHELON az e-társadalom információpajzsa ?
Híradástechnika, 2001/6

[4] Dénes Tamás: Cardano és a kriptográfia
KÖMAL, 51.évf. 2001/6.

[5] Dénes Tamás: Biztonságos információ (s) társadalom?
INFO-Társadalomtudomány, 53.szám 2001. augusztus

[6] Dénes Tamás: Titok Tan avagy Kódtörö ABC (Kriptográfia Mindenkinek)
Bagolyvár Könyvkiadó, 2002.

[7] Doris A.Paul: The Navajo Code Talkers
Dorrance Publishing CO., INC. Pittsburgh, Pennsylvania, 1973.

[8] S. Katzenbeisser, F.A.P. Petitcolas (Ed.): Information Hiding
Techniques for Steganography and Digital Watermarking, Artech House Books, 2000.

[9] Leo Marks: Between Silk and Cyanide, The story of S.O.E.'s code war
Harper Collins Publishers, London, 1998.

[10] Löfvenberg: Random Codes for Digital Fingerprinting.
Linköping Studies in Science and Technology., Thesis No 749, Linköping, 1999.

[11] A. Pfitzmann (Ed.): Information Hiding
Proceedings of Third International Vorkshop, IH'99, Dresden, Germany Sept. 29 - Oct. 1., 1999.

[12] G. J. Simmons (ed): Contemporary Cryptology. , *IEEE Press, New York, 1991*

[13] G. J. Simmons: Identification of data, devices, documents and individuals.
Proc 25th Annual IEEE Carnahan Conf. On Security Technology 1991, IEEE, New York, pp. 197-218.

[14] Svékus Olivér: Titkosírások, *Móra Ferenc Könyvkiadó, 1989.*