# پنهان‌سازي اطلاعات

علیرضا احمدی باغکی. کارشناس ارشد مخابرات-رمز
دانشگاه شهيد ستاري : مهرآباد جنوبي
عضو دانشجويي انجمن رمز ايران

**چكيده**

تاكنون پنج كارگاه بين المللي با موضوع پنهان سازي[۱] اطلاعات برگزار شده كه اولين آن در ۱۹۹٦وآخرين آن دراكتبر۲۰۰۲بوده است.

موضوعاتي كه پنهان سازي اطلاعات دربرگيرنده آنها مي‌باشدعبارتنداز:

۱-مواردمربوط به حق مالكيت توليدات نرم افزاري والكترونيكي شامل نقش زمينه[۲] واثر انگشت[۳] كه جنبه تجاري از اين علم هستند .

۲-استفاده از پنهان سازي در ارسال ودريافت پيام به صورت غير محسوس كه در اين مقاله ازآن با نام پوشيده نگاري[٤] يادخواهيم كرد.

توجه به پنهان سازي اطلاعات از هر دومنظر فوق داراي اهميت است چرا كه با فراهم شدن زمينه هاي IT دركشورلزوم استفاده از قانون حق تكثير[٥] وحفظ حقوق مربوط به مالكيت محصولات نرم افزاري وتوليدات الكترونيكي اعم از موسيقي ،آثارهنري ،كتابهاي الكترونيكي و... شناخت واستفاده ازاين علم را ايجاب مي‌كند .

همچنين پوشيده نگاري در تركيب با رمزنگاري قدرت بسيار بالايي را درمقابل حملات مختلف پديد مي آورد .

شناخت پوشيده نگاري از جنبه هاي كنترلي براي پليس اينترنتي جهت جلوگيري وشناخت معبري براي ارتباطات غيرمجاز ومشكوك نيز داراي اهميت است .

دراين مقاله سعي شده به طور اجمالي و خلاصه به بررسي و معرفي اين علم پرداخته شود.

Key words: Steganography –watermarking –Information Hiding- Image

**۱ـ مقدمه**

در رمز نگاري براي جلوگيري از دسترسي غير مجاز به محتواي پيام از مخدوش نمودن آن استفاده مي‌شود بطوريكه اين پيام مخدوش وغير قابل درك شده توسط شخص مجاز و با استفاده از يك كليد سري قابل بازسازي است و اطلاعات به راحتي استخراج مي‌شود ليكن همين امر براي شخص غير مجازي كه به اطلاعات رمز شده و الگوريتم رمز نگاري دسترسي دارد بدون داشتن كليد(اصل كيرشهف[٦] در ۱۸۸۳) ناممكن است . [WP 2000]

ارسال پيام رمزشده روي كانال عمومي صورت مي پذيرد و همين امرموجب شكل گيري موج عظيمي ازحملات مختلف روي اين سيستم شده است بطوريكه ميتوان گفت جنگ سختي ميان طراحان الگوريتم هاي رمز نگاري از يك طرف و تحليل گران اين الگوريتم ها ازطرف ديگر همواره وجود داشته و دارد طراحان براي افزايش محافظت از محرمانگي وتماميت پيام سعي در پيچيده‌تر كردن الگوريتم ها براي مقاومت در برابر تحليلات مختلف را دارند و تحليلگران با نبوغ و استفاده از نقاط ضعف الگوريتم‌ها راههاي نفوذ را جستجو مي‌كنند .

اكنون بياييد از ديدگاه ديگري به اين مسئله نگاه كنيم اگر ما بتوانيم بگونه اي احتمال انجام شدن تحليل روي

الگوريتم راكاهش دهيم آيا اين كار منجر به افزايش در محافظت از محرمانگي و تماميت پيام نخواهد شد؟
بدون شك اگر ما بتوانيم اين احتمال را محتمل كنيم پاسخ پرسش فوق مثبت خواهد بود .
ايده استفاده از پنهان سازي اطلاعات راهي است در جهت نيل به هدف فوق كه در ۱۹۸۳ توسط سيمونز[۷] تحت عنوان مسئله زندانيان[۸] مطرح شد: [AP 97]
آليس[۹] وباب[۱۰] زنداني هستند وبراي طرح نقشه فرار آليس ميخواهد پيامي را براي باب ارسال كند ارتباط آليس وباب از طريق ارسال ودريافت نامه هايي با محتواي مجاز كه توسط ويلي[۱۱] زندانيان چك مي‌شود ممكن مي‌شود بديهي است در صورتيكه ويلي ارسال پيامي غير مجاز راتشخيص دهد به سرپرست زندان اطلاع خواهد داد واين موجب قطع ارتباط آليس وباب خواهد شد بنابراين آليس باید پيام خود را در قالب يك پيام عادي وپنهان شده درآن براي باب ارسال نمايد طوريكه سوءظن ويلي برانگيخته نشود وباب هم قادر به فهم كامل پيام آليس باشد.

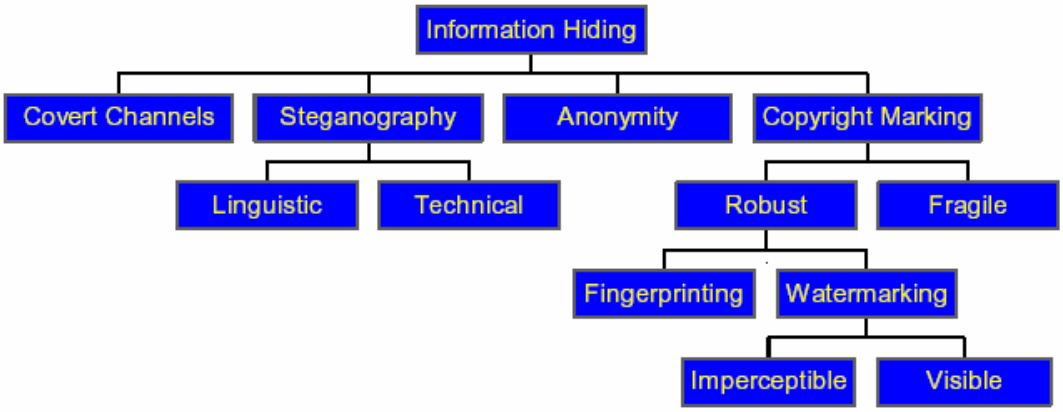
**۲ـ تاريخچه اي كوتاه [DK 96]**

استفاده از پنهان سازي اطلاعات در گذشته داراي سابقه اي طولاني است سربازان يوناني براي انتقال پيام بجاي آنكه طبق روال عادي آن زمان كه روي موم كشيده شده بر لوح پيام نوشته ميشد پيام رابنويسند روي خود لوح مي نوشتند وسپس روي آن را با موم مي پوشانيد واكنون ازاين لوح مثل يك لوح عادي استفاده مي كردند وروي آن يك پيام عادي مي نوشتند ويا اينكه براي ارسال پيام از ميان نيروهاي دشمن سر بردگان را مي‌تراشيدند وروي پوست سر آنان نقشه ياپيام را خال كوبي مي كردند ومدتي بعد كه موي سر اين بردگان بلند ميشد وروي پيام را مي گرفت آنها مي توانستند به راحتي از ميان سرزمين ها و اراضي مربوط به دشمن عبور كنند ودر مقصد با تراشيدن مجدد موي سر آنان پيام استخراج ميشد.همچنين استفاده از جوهرهاي نامرئي از زمانهاي بسيار دور در نقاط مختلف دنيا مرسوم بوده است .
در طول دهه۱۹۸۰مارگارت تاچر كه از نشت اطلاعات و اسناد كابينه اش بسيار ناراحت بود توانست بااستفاده از يك پردازشگر كلمات مشخصات هر وزير را در فاصله بين كلمات به نحوي ثبت كند وبنابراين وزراي خائن رااز اين طريق رديابي نمايد [ AP 97] در حال حاضر نيز تكنيكي مشابه در رديابي انتشارات الكترونيكي مورد استفاده قرار مي گيرد كه به عدد سريال[۱۲] مي توان اشاره كرد .

**۳ـ روشهاي پنهان سازي اطلاعات**

**!Error**

# Classification of Hiding Techniques




*Ref:* F.A.P. Petitcolas, R.J. Anderson, and M.G. Kuhn, "Information Hiding - A Survey," in *Proc. Of the IEEE*, vol. 87, No. 7, July 1999, pg. 1063

روشهاي پنهان سازي اطلاعات رامي توان به صورت زير دسته بندي كرد: [MP 2002 ]

بلوك دياگرام و تعاريفي كه در اولين كارگاه بين المللي پنهان سازي اطلاعات براي انجام اين عمل عنوان شد به شرح زير است :[ BP ٩٦]

cover-medium : شئ اي كه پيام در قالب آن منتقل مي شود و ميتوان شامل تصوير ،متن و...باشددراين مقاله به آن ميزبان گفته مي شود.

Embedded-message : داده اي كه بايدبه صورت پنهاني منتقل شود وداخل ميزبان جاسازي مي گردد در اين مقاله به آن پيام گفته مي شود.

Stego-medium : حاصل تركيب پيام در ميزبان است در اين مقاله به آن شيئ تركيبي گفته مي شود.

Stego-key : اطلاعات سري است كه مشترك بين فرستنده و گيرنده است وبه منظور جاسازي و باز يابي اطلاعات از آن استفاده مي‌شود.

(Embedder(E : تابع جاسازي كننده پيام .

extractor(E-1 ) : تابع بازسازي كننده پيام .

براي انجام هر روش پنهان سازي دو كار زير بايد صورت پذيرد: [FR 2000 ]

الف) در آنچه به عنوان ميزبان بكار ميرود اين تحقيق بايد انجام شود كه چه تغييراتي را مي توان روي آن اعمال نمود بدون اينكه تفاوت قابل دركي بين نمونه اصلي ونمونه اي كه در آن تغييرات ايجاد شده بوجود آيد اين تحقيق براي انجام عمليات فشرده سازي نيزجهت حذف اجزاء زائدي كه وجود يا عدم وجود آنها در كيفيت تاثير چنداني ندارد انجام مي شود.

ب) از مشخصه تحقيق شده در قسمت (الف)براي پنهان كردن اطلاعات استفاده شود.

اگرخواسته باشيم پنهان سازي اطلاعات رابه صورت فرمولي عنوان كنيم مي توان گفت :[ M 99] براي

قطعه اي اصلي از داده d كه به عنوان ميزبان مطرح است حد آستانه اي وجود دارد t كه چنانچه زير اين حد آستانه ،تغيراتي در d بوجود آوريم قابل تشخيص براي حسگرهاي انساني نيست اين حد آستانه از راه آزمايش بدست مي آيد ودرافراد مختلف متفاوت است ليكن كمترين مقدارآن از لحاظ حس انساني مي تواند براي t در نظر گرفته ميشود بنابراين ماهمواره مي توانيم تغيير c در d را زير حد آستانه t بوجود آوريم طوري كه قابل تشخيص بوسيله احساس نباشد

$t>d+c$

**مواردي كه در طراحي يك روش پنهان سازي داراي اهميت هستند:** [ AP 97]

۱ـ شفافيت [۱۳]: شفافيت سيستم بيان ميدارد كه موضوع ميزبان قبل وبعد از جاسازي در پيام نبايد تفاوت محسوسي داشته باشد چراكه هدف غير قابل حس كردن انتقال پيام است و در حقيقت امنيت يك سيستم پنهان سازي در همين مسئله شفافيت نهفته است وهر چقدر كه شباهت موضوع ميزبان پيام در هردو حالت عاري وحاوي پيام بيشتر باشد امنيت اين سيستم در سطح بالاتري قرار دارد.

۲ـ مقاومت[۱٤] : مقاومت يك سيستم پنهان سازي به معناي اين است كه پيام پنهان شده درمقابل اعمال تغيرات ناخواسته و غير عمدي كه وجود نويز در طول مسير انتقال بوجود مي آورد و يا اعمال تغييرات عمدي كه توسط حمله كننده فعال به منظور تغيير پيام ياازبين بردن آن انجام مي گيرد مقاومت لازم راداشته باشد.

۳ـ ظرفيت [۱٥]: در يك سيستم پنهان سازي هر چقدر بتوان پيام بيشتري را در يك ميزبان مخفي نمود اين سيستم مناسب تر خواهد بود حجم دادهاي كه مي توان در يك ميزبان ذخيره كرد دقيقا بستگي به ماهيت ميزبان دارد و اين كه تاچه حدي مي توان داده در آن پنهان كرد بدون اينكه در شفافيت آن تا ثيري جدي بگذارد. سه ويژگي فوق بطور بسيار

تنگاتنگي در ارتباط با يكديگر هستند بدين معني كه باثابت فرض كردن ويژگي اول وافزايش ويژگي دوم ويژگي سوم حتما كاهش خواهد يافت

ثابت =مقاومت*ظرفيت

۳ـ ۱ـ پوشيده نگاري[۱٦]

متشكل از دو كلمه يونانيstego به معني مخفي و graphos به معناي نوشته كه روي هم معني نوشته مخفي را تداعي مي كنند . دراين مقاله من از ترجمه پوشيده نگاري براي آن استفاده كرده ام.

در رمز نگاري دسترسي به محتواي پيام براي فرد غير مجاز ناممكن مي گردد ليكن درپوشيدهنگاري موجوديت پيام انكار مي شود هدف رمزنگاري حفظ محرمانگي وتماميت پيام است كه با رمز كردن آن حاصل مي شود پوشيده نگاري هم همين اهداف را با پنهان نمودن پيام دنبال مي كند بعلاوه در پوشيده نگاري انتخاب جا و ترتيب پنهان نمودن پيام نيز با بهرهگيري از نوعي رمز در چينش بيت هاي پيام لابه لاي بيت هاي ميزبان صورت ميپذيرد. همچنين مي توان پيام راقبل از جا سازي داخل ميزبان بااستفاده از الگوريتم هاي رمز نگاري به صورت رمز در آورد و سپس عمل پنهان سازي راانجام داد.

بطوريكه ميتوان گفت با استفاده از پوشيده نگاري در حقيقت سه لايه حفاظتي بسيار محكم در دسترسي به پيام ايجاد خواهد شد: [ M 99] اول اينكه وجود ارتباط نامحسوس است و اين هدف اصلي در پوشيده نگاري است و بنابراين گذشتن از اولين مانع كار چندان ساده اي نخواهد بود در صورتيكه وجود اطلاعات دريك ميزبان مورد سوءظن واقع شود مرحله دوم پيدا كردن الگوريتم پنهان سازي است طوريكه بايد جا و ترتيب پنهان شدن اطلاعات معلوم شود ليكن در اين مرحله نيز چون از يك كليد بنام stego_key براي جاسازي پيام

استفاده شده دانستن اين كليد ضروري است و بنابراين گذشتن از اين مرحله نيز با دشواري همراه خواهد بود و چنانچه دو مرحله قبلي با موفقيت پشت سر گذاشته شوند اكنون به متن رمزي دسترسي پيدا شده است كه تازه در اين مرحله مسائل مربوط به رمزنگاري مطرح مي گردند .

علاوه بر اين استفاده از پنهان‌سازي اطلاعات در امور ارتباطات گاها گريزناپذير است همان طور كه در سناريوي مطرح شده در اين مورد عنوان گرديد آليس مجبور به استفاده از اين روش است.

در دنياي واقعي كنوني نيز استفاده از رمزنگاري قوي در ارتباطات شخصي توسط دولت‌ها محدود شده است[M 99] علت اين محدوديت سوء استفاده از اين علم براي انجام فعاليت‌هاي جنايي و تروريستي و ساير امور مرتبط با اين موضوعات مي‌باشد و به شدت توسط ارگانهاي مربوطه كنترل مي‌گردد و در صورت انجام تخلف از فرستنده و گيرنده پيام رمزي توضيح خواسته مي‌شود. [M 99 j ]

اساس كار روش‌هاي موجود در پوشيده‌نگاري را مي‌توان به دو دسته كلي زير تقسيم كرد: [ MP ۲۰۰۲]

۱ـ روش هايي كه بر پايه نقص در سيستم بينايي انسان [17](h hvs]) استواراست.

۲ـ روش هايي كه بر پايه نقص در سيستم شنوايي انسان [۱۸]( hos) استوار است.

سيستم شنيداري انسان آنقدر دقيق نيست كه تغيرات جزئي ايجاد شده در قطعات صوت را تشخيص دهد وبنابراين از همين نقطه ضعف مي توان استفاده نمود وداده اي را لابه لاي قطعات صوت جا سازي كرد همچنين سيستم ديداري انسان داراي خصوصياتي است كه بر مبناي آنهاروش هاي پنهان سازي متفاوتي در قالب تصاوير خصوصا تصاوير ثابت ابداع شده اند.

۳ـ۲ـ علامت حق تكثير[۱۹]

در حقيقت علامت هاي حق تكثير جنبه تجاري استفاده از پنهان سازي اطلاعات هستند كه براي جلوگيري از استفاده هاي غيرمجاز توليدات الكترونيكي اطلاعات به صورت نا محسوس وغيرقابل تفكيك از محصول داخل آن جا سازي مي شود كه در مواقع لزوم براي پيگيري استفاده غير مجاز واثبات حق مالكيت از طريق قانون مي تواند به مالك واقعي محصول كمك كند .

علامت حق تكثير را مي توان به دو دسته تقسيم كرد: [ NM 99]

الف ) نقش زمينه[۲۰] : علامت نقش زمينه اطلاعاتي هستند كه داخل محصول الكترونيكي جا سازي مي شوند و يا بهتر بگوئيم تركيب مي شوند طوري كه از مقاومت بسيار بالايي برخوردار مي باشند و معمولا اين اطلاعات شامل آرم يا علامت مخصوص شركت يا مالك است كه به آن لوگو[۲۱] گفته ميشود فرقي كه پوشيده نگاري بانقش زمينه دارد اين است كه در پوشيده نگاري آنچه مهم است پيامي است كه داخل ميزبان پنهان شده است وميزبان در حقيقت سدي است براي محافظت ازپيام ليكن درنقش زمينه آنچه كه مهم است ميزبان است و پيام براي محافظت از ميزبان داخل آن جاسازي شده است يكي از خصوصيات ضروري نقش زمينه داشتن مقاومت بسيار بالا است طوري كه به هيچ وجه قابل تفكيك از ميزبان نباشد و از بين بردن آن منجر به از بين رفتن ميزبان شود.

ب ) اثر انگشت[۲۲] : اثر انگشت اطلاعاتي است كه براي محافظت در مقابل استفاده غير مجاز از محصولات نرم افزاري داخل آن پنهان مي شود طوري كه استفاده كننده مجاز با وارد كردن آنها به صورت عدد شناسايي[۲۳] قادر به استفاده از آن خواهد بود .همچنين اين عدد شناسايي براي پيگيري كپي‌هاي غير مجاز از نرم افزار نيز مي تواند مورد استفاده قرار گيرد.

**٤ـ الگوريتم‌هاي پنهان‌سازي اطلاعات**

تا كنون الگوريتم‌هاي گوناگوني براي پنهان‌سازي اطلاعات طراحي شده‌اند. پوشيده‌نگاري در دو حوزه زمان و تبديل انجام مي‌شود :

حوزه زمان شامل آن دسته از الگوريتم‌هايي مي‌شود كه بيت‌هاي پيام عيناً لا به لاي بيت‌هاي ميزبان گنجانيده مي‌شوند به عنوان مثال در حالتي كه از تصوير به عنوان ميزبان استفاده مي‌شود در تكنيك LSB كه يكي از ساده‌ترين آنها مي‌باشد بيت‌هاي پيام در كم ارزش‌ترين بيت هر پيكسل گنجانيده مي‌شوند .[ AP 97]

حوزه تبديل شامل آن دسته از روش‌هايي است كه اطلاعات بيت‌هاي پيام روي تمام يا قسمتي از بيت‌هاي ميزبان پخش مي‌گردد . در اين روش‌ها از تبديلاتي همچون DCT وDFT استفاده مي‌شود . به عنوان مثال در همان حالت قبلي براي پنهان‌سازي در قالب تصوير ابتدا تصوير به بلوك‌هاي ٨ x 8 پيكسل تقسيم شده سپس روي اين بلوك‌ها تك تك DCT گرفته مي‌شود بيت‌هاي پيام با دستكاري ضرائب بدست آمده از اين تبديلات روي اين ضرائب پياده شده و در پايان DCT-1 گرفته مي‌شود . و يا در تكنيك SS با شبيه‌سازي پيام به صورت نويز آن را روي طيف فركانسي ميزبان مي‌گسترانند (گسترش باند باريك روي باند وسيع ) .[ MBR 99]

دسته ديگري از تكنيك‌هاي پنهان‌سازي كه تنها در پوشيده‌نگاري كاربر دارند به تكنيك‌هاي زباني[٢٤] معروف هستند در اين روش‌ها پيام در قالب يك متن عادي پنهان مي‌گردد روش كار به اين صورت است كه با استفاد از يك ديكشنري كه كلمات آن به دسته‌هاي مختلفي تقسيم مي‌گردند و يك متن انتخابي مي‌توان بيت‌هاي پيام را به صورت يك متن كاملا عادي به عنوان مثال يك متن ادبي پنهان كرد. Nicetext يكي از الگوريتم‌هايي است كه در اين مورد پياده سازي شده است.

**٥ـ جمع بندي**

در اين مقاله به لحاظ اهميتي كه شاخه پنهان‌سازي اطلاعات در ارتباط با تجارت الكترونيك و مسائل مربوط به ايجاد امنيت و اطمينان براي عرضه محصولات نرم‌افزاري و الكترونيكي روي شبكه اينترنت دارد همچنين به لحاظ آشنايي با ارتباطات مخفي و پوشيده‌اي كه به مدد اين علم قابل حصول مي‌باشند به معرفي و بررسي آن پرداخته شد ليكن به خاطر محدوديت حجم نوشتار توضيح جزئيات امكان پذير نبود .

كاربرد اين علم در امور تجاري بسيار زياد است و در كشوهايي كه متعهد به اجراي قانون حق تكثير مي‌باشند خدمات خوبي براي صاحبان توليدات الكترونيكي روي شبكه اينترنت ارائه نموده است . در كشور ما در حال حاضر متاسفانه به دليل عدم رعايت قانون ذكر شده شايد اهميت كاربردي اين علم زياد مورد توجه نباشد ليكن با پيشرفت صنعت IT در آينده‌اي نه چندان دور توجه بيشتر به آن گريز ناپذير خواهد بود.

همچنين به لحاظ ارتباط اين علم با مسائل امنيتي در برقراري ارتباطات پوشيده توجه ارگان‌ها و نهادهاي ذيربط و ذي نفع را مي‌طلبد و غفلت از آن زيان‌هاي جبران ناپذيري را متصور مي‌سازد.

**پانوشتها:**

[1] -information hiding

[2] -watermarking

[3] -fingerprinting

[4] -steganography

[5] -copyright

[6] - Kerckhoffs

[7]-simmons

[8] -prisoner's problem

[9] -alice

[10] -bob

[11] -willie

[12] -sereal number

[13] -tranceparencey

[14] -resistance

[15] -capacity

[16] -steganography

-[17] human video system

2-human audio system

[19] -copyright marking

[20] -watermarking

[21] -logo

[22] -fingerprinting

[23] -ID Number

[24] -Lingustic

---

**References**

[DK 96] David Kahn , " The History of Steganography " , Lecture Notes in computer science 1174 , 1996 , pp 1-7

[BP 96] Birgit Pfitzman , " Information Hiding Terminology " , Lecture Notes in computer science 1174 , Springer , 1996 , pp . 347-358

[WP 2000] Andreas Westfeld , Andreas Pfitzman , " Attacks On Steganigraphic Systems " , Department of computer science , IH'99 , LNCS 1768 , pp. 61-76 , 2000

[MP 2002] Michael Panczenko , " Steganography-An Introduction to Data Hidig Techniques " , The Windermere Group , Us Census Bureau Annual Security Day , Suitland , maryland , 2002

[JFR 2000] Jiri Fridrich , Rui Du , " Secure Steganographic Methods For Palette Images " , Center for Intelligent Systems , Dept .of , SS&IE , 2000

[MBR 99] Lisa M.Marvel , Charles G.Boncelet , Chrles T.Retter , " Spread Spectrum Image Steganography " , IEEE Transaction on image processing , vol 8 , No 8 , 1999

[NM 99] Norishige Morimoto , " Digital Watermarking Technology With Practical Applications" , Inform Science Special Issue on Multimedia , vol 2 , No 4 , 1999

[AP 97] Ross J.Anderson , Fabien A.Petitcolas , " On the Limits of Steganography " ,

[M 99] Matteo Fortini , "Steganography and Watermarking : A Global View"