معیارهای طراحی و پیاده‌سازی یک سامانه پنهان‌نگاری امن با نگرش پدافند غیرعامل

رضا اصفهانی[۱]

تاریخ دریافت: ۹۰/۰۴/۲۰
تاریخ پذیرش: ۹۰/۰۶/۰۷

چکیده

مؤلفه‌های سرّی بودن و سرّی ماندن باعث کاهش آسیب‌پذیری و ارتقای پایداری و تسهیل مدیریت امنیت در برابر تهدیدات و اقدامات نظامی دشمن می‌شود. عادی جلوه‌کردن ارتباط، یکی از بارزترین و مهم‌ترین مسئله‌های پنهان‌نگاری است. از این‌رو پنهان‌نگاری، از اصول و ضوابط پدافند غیرعامل در مقابله با تهدیدات نرم‌افزاری و الکترونیکی و دیگر تهدیدات جدید دشمن به‌منظور حفظ و صیانت شبکه‌های اطلاع‌رسانی، مخابراتی و رایانه‌ای به شمار می‌رود. یک کانال ارتباطی ناامن که امکان ارسال رسانه‌های رقمی - صوت، تصویر و ویدئو - از طریق آن وجود دارد، و دسترسی به طرف مقابل ارتباط (همان گیرنده مورد نظر) از این کانال امکان‌پذیر است، عملاً پنهان‌نگاری روی چنین بستری قابل پیاده‌سازی است که با در نظرگرفتن شرایط و معیارهای ویژه و هم‌چنین مجموعه اقداماتی، صرف‌نظر از منشاءِ تهدید، از اطلاعات مورد نظر حفاظت می‌نماید. در این مقاله این شرایط و معیارهای ویژه که باید قبل از طراحیِ محصول پنهان‌سازی (محدودیت‌های طراحی) رعایت شود، به همراه ارائه یک مطالعه موردی، بررسی شده است.

کلیدواژه‌ها: پنهان‌نگاری، رمزنگاری، واترمارکینگ[۲]، سیستم فایل پنهان‌نگاری شده

۱- کارشناس ارشد مهندسی مخابرات گرایش رمز – مرکز تحقیقات امنیت و رمز (فتح) – دانشگاه جامع امام حسین(ع)، Email : isfahani@aryasys.com

2- Watermarking

۱- مقدمه

در بحث ارتباطات رقمی[1]، امنیت از اهمیت فوق‌العاده‌ای برخوردار است. سرمایه‌گذاری‌های کلان در این خصوص می‌تواند به تنهایی گویای این امر باشد.

بی‌شک در دنیای امروز که آن را عصر ارتباطات نامیده‌اند، بسیاری از امور که قبلاً به‌صورت حضوری و یا از طریق مکاتبات صورت می‌گرفت، از طریق سیستم‌ها و شبکه‌های مختلف ارتباطی صورت می‌گیرد. همین امر باعث می‌شود که بسیاری از افرادی که در گذشته شاید کوچک‌ترین ارتباطی با این شبکه‌ها نداشته‌اند، اکنون به یکی از مشتریان پر و پا قرص این تکنولوژی تبدیل شوند که به معنای افزایش چشم‌گیر تعداد کاربران شبکه است. تهدیدی که این افزایش تعداد کاربران می‌تواند با خود به همراه داشته باشد این است که شاهراه تبادل اطلاعات را که می‌توانست یک خیابان عادی باشد به یک پیست اتومبیل‌رانی تبدیل می‌کند که دور تا دور آن تماشاچیانی نشسته و نظاره‌گر اتومبیل‌های در حال گذر هستند.

در مطلوب‌ترین حالت، این کاربران تنها اطلاعات مورد نیاز و مربوط به کار خود را روی شبکه دنبال می‌کنند. اما همیشه این‌گونه نیست و بسیارند کسانی که روی چنین بستری به دنبال اطلاعات دیگران می‌گردند و یا مواردی وجود دارد که افراد به اطلاعاتی روی شبکه بر می‌خورند که اگرچه به آنها مربوط نمی‌شود اما حس کنجکاوی آن‌ها را برمی‌انگیزد و شاید اگر مختصر آشنایی با علوم مربوط به شبکه داشته باشند بتوانند به محتوای اطلاعات دسترسی پیدا کنند.

موضوع محرمانگی مخصوصاً در حوزه مسائل نظامی اهمیتی دوچندان پیدا می‌کند و در مواردی لازم خواهد بود که نوع ارتباط کاملاً عادی جلوه کند. به همین منظور در کنار سیستم‌های رمزنگاری مقولهٔ دیگری هم توسعه یافته و آن پنهان کردن اطلاعات از دید دشمن و یا افراد واسط است که در اصطلاح به این‌کار پنهان‌نگاری گفته می‌شود که یکی از مهمترین کاربردهای آن، مخابرات پنهان می‌باشد.

مسئله دیگری که به این مشکل دامن می‌زند، سرعت رشد تکنولوژی است که باعث شده تا ابزار دسترسی به اطلاعات بسیار زیاد و آسان باشد. شبکه‌های رایانه‌ای و اینترنت گسترده‌ترین بستر ارتباطی موجود در سرتاسر دنیا است که کاربران زیادی را به خود اختصاص داده است. شبکه‌های تلفنی، دستگاه‌های نمابر و غیره، جزء این شبکه گسترده محسوب می‌شوند.

بنابراین همواره افرادی وجود دارند که خواسته یا ناخواسته به منابع اطلاعات دسترسی پیدا می‌کنند و اگر هم این‌گونه نباشد فرض وجود آنها، فرض دور از ذهنی نیست و صاحبان و استفاده کنندگان از این اطلاعات را بر آن می‌دارد که راه‌کارهایی برای ایجاد امنیت و کنترل دسترسی افراد به اطلاعات ایجاد کنند. روش‌هایی که برای احراز هویت و تایید کاربری در شبکه‌ها وجود دارد ناظر به همین امر می‌باشد.

اما همواره راه‌هایی برای نفوذ به شبکه‌ها وجود دارد و سیستم‌ها و ابزار گوناگون کنترل دسترسی نمی‌تواند تنها راه ایجاد امنیت برای اطلاعات باشد. لذا باید به دنبال راه‌حل‌های دیگری رفت که یکی از راه‌کارهای حل این مشکل استفاده از رمزنگاری است. رمزنگاری اطلاعات اگرچه گام مهم و موثری در نیل به مقصود است ولی آن نیز یک ضعف عمده دارد و آن این‌که داده[2] را از حیث در بر داشتن اطلاعات مفید نشان‌دار می‌کند. به این معنا که اطلاعاتی که روی شبکه رد و بدل می‌شوند باید دارای معنی بوده و ترکیب خاصی داشته باشند و چنانچه این‌گونه نباشد، شک کاربران شبکه را بر می‌انگیزد و آنها را وادار به اعمال روش‌های دیگر بر روی اطلاعات تا رسیدن به محتوای آنها می‌کند. راه‌کار دیگری که به ذهن می‌رسد این است که موجودیت اطلاعات از دید افراد و کاربران غیرمرتبط مخفی بماند. برای این کار دو روش وجود دارد: یکی ایجاد یک شبکه ارتباطی که مستقیما افراد مرتبط با یک موضوع خاص را به هم‌دیگر وصل می‌کند و هیچ فرد دیگری امکان اتصال به چنین شبکه‌ای را ندارد و راه دیگر، استفاده از شبکه‌های ناامن موجود و ارسال اطلاعات از طریق آن به‌صورت پنهان است که با راه‌کارهای پدافند غیرعامل نیز همسو است چرا که ایجاد شبکه ارتباطی خصوصی یک هدف مشخص جهت حمله دشمن خواهد بود. از آنجا که ایجاد یک شبکه امن، بسیار هزینه‌بر و وقت‌گیر است، توسعه روش‌هایی که بر اساس آنها بتوان اطلاعات دارای طبقه‌بندی را از طریق کانال ناامن به‌صورت امن ارسال کرد، باصرفه‌تر خواهد بود و به همین دلیل نیز در چند سال اخیر پیشرفت‌های زیادی در این مسیر حاصل و روش‌های گوناگونی برای این کار ابداع شده است. مسایلی را که در این مسیر به آنها بر می‌خوریم، می‌توان تحت عنوان کلی

1- Digital

2- Data

«پنهان‌سازی داده[1]» جستجو کرد که در ادامه به شرح بیش‌تر آن خواهیم پرداخت.

پنهان‌نگاری[2] در اصل کلمه‌ای است با ریشه یونانی که از دو کلمه ***استگانوس*** به معنای ***پنهان*** و ***گرافی*** به معنای ***نگاری*** تشکیل شده و به هنر مخفی نمودن یک پیام در پیام[3] دیگر اطلاق می‌گردد.

پنهان‌نگاری به لحاظ کاربردی، هم‌خانواده رمزنگاری به‌شمار می‌آید. امتیاز پنهان‌نگاری در مقایسه با رمزنگاری، عدم اطلاع شخص سوم از اصل وجود پیام است، حال آن‌که در رمزنگاری معمولاً شخص سوم از وجود پیام رمز شده مطلع بوده و چنانچه قادر به کشف پیام نباشد این امکان را دارد که آن را مخدوش نموده و گیرنده را از دریافت آن محروم نماید. هدف رمزنگاری حفظ امنیت است و در صورت لزوم، جهت محرمانگی و تمامیت پیام، از پروتکل‌های ارتباطی مانند توابع درهم‌ساز یا امضاهای رقمی و غیره استفاده می‌شود. پنهان‌نگاری هم همین اهداف را با پنهان‌سازی پیام دنبال می‌کند به‌علاوه در پنهان‌نگاری انتخاب مکان و ترتیب پنهان‌سازی پیام نیز با بهره‌گیری از نوعی رمز در چیدن بیت‌های پیام در میان بیت‌های رسانه پوششی صورت می‌پذیرد. هم‌چنین می‌توان پیام را قبل از جاسازی، به‌صورت رمز درآورد و سپس عمل پنهان‌سازی را انجام داد. همان‌طور که در شکل (۱) مشاهده می‌شود پنهان‌نگاری شاخه‌ای از دسته‌بندی پنهان‌سازی اطلاعات بوده که خود آن نیز به دو شاخه تقسیم می‌شود[۱].

۲- اطلاعات پنهان و دادهٔ میزبان

در پنهان‌نگاری، داده‌ها از دو قسمت تشکیل شده‌اند:

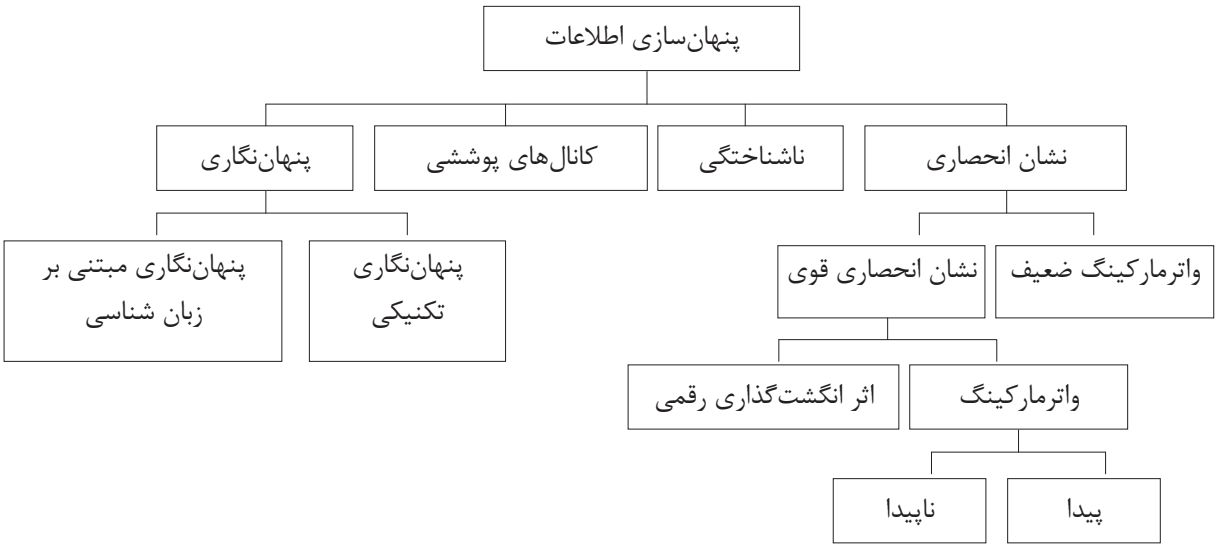
۱- اطلاعات پنهان

۲- داده میزبان

که ماهیت آن‌ها به‌شرح زیر است:

۲-۱- ماهیت اطلاعات پنهان

اطلاعاتی که امکان انتقال دارند و در مبحث پنهان‌نگاری، به آن «داده» اطلاق می‌شود از هر شکلی می‌توانند باشند، یعنی **متن، صوت، تصویر، فیلم و یا هر نوع دادهٔ دیگر** (شکل ۲)، که حجم این اطلاعات با توجه به نوع آن‌ها متفاوت خواهد بود. اما علیرغم تنوعی که در نوع اطلاعات وجود دارد، همه داده‌ها به شکل رشته‌های بیتی ارسال می‌شوند و در این‌جا «روش‌های پنهان‌سازیِ داده» است که اهمیت فراوانی دارند.

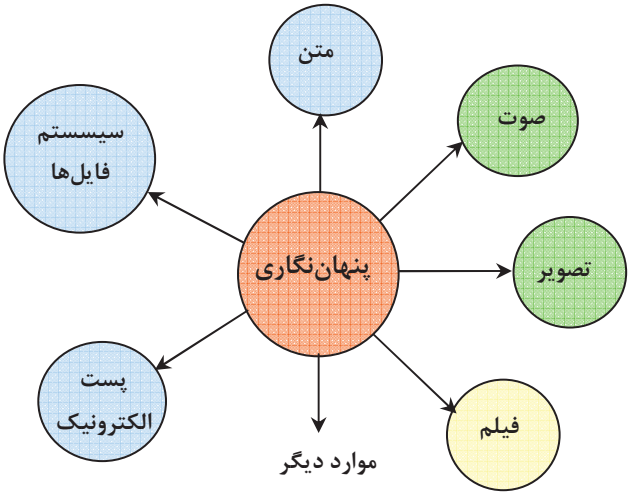


شکل ۱- دسته‌بندی پنهان‌سازی اطلاعات

1- Data hiding
2- Steganography
۳- به معنای پیام واقعی پنهان‌شده در پیام غیرواقعی ظاهرشده

۲-۲- ماهیت دادهٔ میزبان

به همین ترتیب بستری که برای پنهان‌سازی انتخاب می‌شود که به آن حامل[1] نیز گفته می‌شود نیز می‌تواند **متن، صوت، تصویر، فیلم و یا هر نوع دادهٔ دیگر** (شکل ۲) باشد که در اینجا نیز با توجه به بستر پنهان‌سازی، ظرفیت پنهان‌سازی افزایش یا کاهش می‌یابد. بنابراین هر داده‌ای را می‌توان درون متن، صوت و غیره پنهان کرد ولی محدودیت‌های مختلفی برای این‌کار در هر یک از بسترهای یاد شده وجود دارد که در بخش ۴ این مقاله به آن پرداخته می‌شود.



شکل ۲- نوع فایل‌های مرتبط با پنهان‌نگاری: داده، حامل و سیستم فایل

از آن‌جا که پنهان‌سازی داده در یک رسانه یا داده‌های دیگر بر اساس محتویات فایل‌های آن رسانه صورت می‌گیرد، نمی‌توان با استفاده از هر روشی، پنهان‌سازی در صوت، متن، تصویر، فیلم و غیره را همزمان دنبال کرد. البته شاید بتوان روشی را پیدا کرد که در کلیات در مورد یک یا چند رسانه قابل بکارگیری باشد، اما همین روش‌ها نیز در جزئیات متفاوت از یکدیگر خواهند بود. به‌عنوان مثال روش LSB، هم در تصویر و هم در صوت وجود دارد و تقریباً مشابه هم هستند ولی بحث پردازش سیگنال صوت با پردازش تصویر متفاوت خواهد بود. لذا مسیری که از این به بعد دنبال می‌کنیم، بر اساس نوع رسانه بکار گرفته شده برای میزبانی، منشعب خواهد شد.

به‌همان میزان که در روش‌های پردازش داده پیشرفت حاصل می‌شود، روش‌های پنهان‌نگاری نیز دستخوش تغییر و تحول می‌شوند. بعضی از روش‌ها مانند روش *چیدن بیت‌های اطلاعات در بین بیت‌های میزبان به‌صورت یک در میان* منسوخ می‌شوند؛ امنیت[2] بعضی دیگر از روش‌ها مانند روش LSB[3] کم می‌شود و روش‌های جدید دیگری ابداع می‌شود. بنابراین ابزاری که برای این کار در نظر گرفته می‌شود باید به‌صورت نوبه‌ای بررسی و به روز شود و این امکان در آنها وجود داشته باشد که بتوان گزینه‌های دیگری به آنها افزود.

روش‌های پنهان‌نگاری بر روی حامل‌های مختلف هم مسئله‌ای مهم است که بایستی در طراحی و پیاده‌سازی در نظر داشت و این روش‌ها متفاوت می‌باشند؛ به عنوان مثال روش‌های پنهان‌نگاری داده در حامل‌های صوت و تصویر به شکل زیر می‌باشند:

الف) بعضی از روش‌های پنهان‌نگاری داده در صوت:

۱- پنهان‌نگاری به روش تبدیل بیت

۲- پنهان‌نگاری به روش LSB افزایش یافته

۳- پنهان‌نگاری داده با استفاده از تبدیل موجک[4]

۴-پنهان‌نگاری داده در پژواک صوت[5]

۵- پنهان‌نگاری داده در حوزه کپستروم[6] [۲]

۶- پنهان‌نگاری داده در صوت با استفاده از تبدیل فوریه[7]

1- Carrier

۲- طبق قاعده کیرشهف، امنیت یک سیستم رمزنگاری، مبتنی بر محرمانگی کلید بوده و نه محرمانگی الگوریتم رمزنگاری؛ که همین قاعده در مورد پنهان‌سازی داده نیز تقریباً در تمام کاربردها صادق است. یعنی امنیت سیستم‌های پنهان‌سازی باید مبتنی بر کلید باشد و چنانچه الگوریتم فاش شود نتوان به سادگی به اطلاعات پنهان دسترسی پیدا کرد. هرچند چنین اتفاقی برای مخابرات پنهان (پنهان‌نگاری) یک ضربه امنیتی محسوب می‌شود. البته امنیت در مواردی به معیار مقاومت در برابر تغییر و حملات خصمانه نیز اطلاق می‌شود.

3- Least Significant Bit

4- Wavelet

5- Echo hiding

۶- افزودن پژواک یا اکو به‌صورت مصنوعی در سیگنال علیرغم آن که از نظر شنیداری تأثیر قابل توجهی بر کیفیت سیگنال ندارد اما باعث ایجاد تغییراتی در انرژی سیگنال خواهد شد. ضرایب کپسترال (Cepstral) سیگنال صوتی یکی از معیارهای مناسب در این زمینه است. در حالتی که سیگنال دارای پژواک باشد، ضرایب کپستروم سیگنال در این نواحی دارای پیک‌های محلی (Local Picks) خواهند بود، که نشان‌دهنده میزان همبستگی بیش‌تر انرژی در این نواحی است.

7- Fourier Transform

ب) برخی روش‌های پنهان‌نگاری داده در تصویر:
۱- پنهان‌نگاری به روش LSB
۲- پنهان‌نگاری داده با استفاده از تبدیل موجک
۳- پنهان‌نگاری داده در حوزه DCT[1]
۴- پنهان‌نگاری داده با استفاده از تبدیل فوریه

۳- پنهان‌نگاری داده از دیدگاه مخابرات و پدافند غیر عامل

مباحث پنهان‌نگاری داده با دید مخابراتی از جمله مسائل مهم مرتبط با پدافند غیرعامل است که در این بخش، یک منظر مخابراتی از مسئلهٔ ارسال داده پنهان مورد نظر است. این مسئله، شباهت قابل توجهی با یکی از مسائل دیرینه مخابرات یعنی ارسال اطلاعات جانبی[2] در کدکننده و کدگشا دارد.
اساساً هدف، ارسال یک پیام است ولی داده میزبان و نیز اختلالی که مهاجم ایجاد می‌کند، هر دو به عنوان «اختلال» ایفای نقش می‌کنند که البته این امر، نقطه قرینه یا همتای کدگذاری کانال در پنهان‌سازی داده است. با این وجود، برای دست‌یابی به این هدف، باید پیام درون داده میزبان با مقدار معقول و منطقی از نویز جاسازی شود. بنابراین، این امکان وجود دارد که به این مسئله، یعنی مسئلهٔ پنهان‌نگاری داده، به عنوان یک مسئلهٔ کدگذاری تؤام کانال- منبع نگاه شود. این روش، امکان این که بتوان ظرفیت یک طرح پنهان‌نگاری را محاسبه کرد ایجاد می‌کند.
با تمام این شباهت‌ها، تفاوت مهمی بین نقطه نظرات و تصورات یک چارچوب مخابراتی سنتی و یک موقعیت پنهان‌نگاری دادهٔ مرتبط با امنیت وجود دارد. از نقطه نظر امنیتی و پنهان‌نگاری، دشمن متخاصم کانال حمله (یعنی فاصلهٔ بین گیرنده و فرستنده) را زیر نظر داشته و در واقع استراتژی دشمن (فردی با بدترین مقاصد) ایجاد اتفاقات خطرناک برای اطلاعات ارسالی است. از این‌رو، حملات هوشمندانه‌ای مدنظر است که جهت‌گیری آن‌ها به سمت یافتن موارد پنهان و مخفی در طرح‌ها و روش‌های طراحی شده می‌باشد [۳].
از سوی دیگر و از نقطه نظر مخابرات کلاسیک و سنتی (غیرخصمانه)، طبیعت، خود به عنوان یک مهاجم عمل می‌کند. از این‌رو حملات به تعداد کوچکی دسته‌بندی محدود می‌شود که زیرمجموعه‌ای از همهٔ حملاتی است که یک فرد متخاصم می‌تواند انجام دهد. به عبارت دیگر بررسی کامل از نقطه نظر امنیتی و پنهان‌نگاری، نقطه نظر مخابرات کلاسیک و سنتی (غیرخصمانه) را نیز پوشش خواهد داد و در نظر داشتن نقطه نظرهای مخابرات کلاسیک و سنتی با نگرش پدافند غیرعامل، مسلماً پیشگیری از حملات را دربر خواهد داشت.

۴- محدودیت‌ها و چالش‌های عملی

برای طراحی الگوریتم‌های پنهان‌سازی داده، بایستی از میان یک سری محدودیت‌های طراحی عبور کرد. این محدودیت‌ها با توجه به نوع کاربرد، متفاوت هستند. با این حال عمدتاً می‌توان آنها را به‌صورت زیر دسته‌بندی نمود. لازم به ذکر است که از این محدودیت‌ها در بعضی موارد تعبیر به خواص پنهان‌سازی داده نیز می‌شود. با درنظر گرفتن این خواص قبل از طراحیِ محصول پنهان‌سازی، در واقع یکی از راه‌کارهای مهم در به‌کارگیری اصول و ضوابط پدافند غیرعامل در طراحی و پیاده‌سازی صورت می‌پذیرد [۴].

۴-۱- شفافیت[3]

روش‌های پنهان‌سازی داده، نیازمند آن هستند که سطح خاصی از کیفیت ادراکی را در داده‌ای که پس از جاسازی تولید می‌شود، حفظ کنند. در غیر این‌صورت دادهٔ نشان‌گذاری‌شده یا دادهٔ پنهان‌شده، برای هر هدف عملی، غیرمفید خواهد بود. گفته می‌شود: زمانی "یک واترمارکینگ از درستی بالایی برخوردار است" که مشاهدهٔ افتی که از آن ناشی می‌شود، برای بیننده بسیار مشکل باشد.
ناگفته پیداست که مهمترین نقش را در این زمینه، نوع الگوریتم پنهان‌سازی ایفا می‌کند که باید کیفیت دادهٔ میزبان را تا آنجا که ممکن است، حفظ کند. با این حال فقط زمانی که رسانه‌ای مورد مشاهده قرار می‌گیرد، نیازمند دیده نشدن تغییرات و واترمارکینگ هستیم. اگر مطمئن شدیم که رسانه قبل از این که دیده شود یا مورد استفادهٔ ادراکی قرار گیرد، به‌طور جدی افت پیدا کرده یا خفیف شده است، می‌توان از این افت، برای کمک به پوشش واترمارکینگ، استفاده کرد. چنین موردی زمانی رخ می‌دهد که مثلاً یک محصول ویدئویی که

1- Discrete Cosine Transformation
۲- اطلاعات جانبی عبارت است از: دادهٔ میزبان و کلید مخفی
3- Fidelity

روی سیستم NTSC[1] یا یک محصول صوتی که روی سیستم AM[2] ارسال می‌شود را واترمارکینگ‌گذاری کرد. کیفیت دو سیستمی که از آنها یاد شد به قدری پایین است که صحت محصول واترمارکینگ‌گذاری شده (و شباهت داشتن آن به محصول اولیه) خیلی خوب به نظر برسد.

برعکس در سیستم‌های به ترتیب تصویری و صوتی HDTV[3] و DVD[4] ، سیگنال‌ها دارای کیفیت بسیار بالایی هستند و نیاز به واترمارکینگ‌های دقیق‌تر و ظریف‌تر داریم ولو این‌که کیفیت اولیه محتوا، بد باشد و همان‌طور باقی بماند چرا که یک فیلم با کیفیت پایین، چه روی نوار ویدئویی VHS[5] و چه روی DVD، بد خواهد بود.

در بعضی از کاربردها می‌توان واترمارکینگ‌هایی که به نرمی و ملایمت و با دقت زیاد، قابل تشخیص هستند در ازای این‌که استحکام بیش‌تری دارند یا بار محاسباتی کم‌تری تحمیل می‌کنند را پذیرفت. به‌طور مثال گزارش‌های روزانه‌ای که هالیوود در اختیار مراجع مختلف قرار می‌دهد، تولیدات نهایی این مؤسسه نیست و معمولاً نتایج تبدیلات ضعیف و نامرغوبی از فیلم به ویدئو هستند و هدفشان این است که نشان دهند تا آن مرحله، این صحنه‌ها در فیلم وجود داشته و تصویربرداری شده است. یک نویز ناچیز قابل رؤیت هم که در اثر واترمارکینگ بوجود می‌آید، شفافیت آنها را تقلیل نخواهد داد.

۴-۲- قوت[6]

به یک واترمارکینگ، زمانی مقاوم گفته می‌شود که بتواند در برابر عملیات عمومی و عادی پردازش مانند تبدیلات آنالوگ به رقمی و رقمی به آنالوگ و فشرده‌سازی با اتلاف[7]، از خود تحمل نشان دهد. در سال‌های اخیر، علاقه و نیز نگرانی فزاینده‌ای نسبت به اینکه واترمارکینگ‌های محصولات ویدئویی و حتی تصاویر، نسبت به تبدیلات هندسی هم مقاوم باشند، وجود داشته است. قوت و استحکام را اغلب به‌صورت یک بعدی در نظر می‌گیرند که به نظر می‌رسد تصور نادرستی است. واترمارکینگی که در مقابل یک نوع خاص از پردازش، مقاوم است، ممکن است در مقابل پردازش دیگری شکننده باشد. در بسیاری از کاربردها، تلاش برای رسیدن به استحکام در برابر تمام پردازش‌ها، هم افراط و هم کاری غیرضروری به نظر می‌رسد.

معمولاً یک واترمارکینگ، باید پردازش عمومی سیگنال را در مراحل جاسازی تا کشف، تحمل نماید. مثلاً در کار نظارت بر پخش رادیویی و تلویزیونی، واترمارکینگ فقط نیاز به تحمل فرآیند ارسال (انتقال) دارد که این فرآیند برای تلویزیون به معنی فشرده‌سازی با اتلاف، ارسال آنالوگ و در بعضی موارد مقداری جزیی انتقال یا برگردان عمودی یا افقی است و به تحمل فرآیند چرخش، پیمایش یا مقیاس‌گذاری، عبور از فیلتر بالاگذر یا هریک از عملیات موجود درگسترهٔ انواع نویزها که در خلال عملیات پخش اتفاق نمی‌افتد نیاز نیست. در بعضی موارد، ممکن است استحکام، کاملاً بی‌مورد یا حتی نامطلوب باشد. واترمارکینگ‌هایی که برای بررسی تمامیت تصویر از آنها استفاده می‌شود، هرگز نیازی به استحکام ندارند. در گذشته روش‌های پنهان‌سازی داده براساس معیار قوت، به دو شاخهٔ مقاوم و شکننده تقسیم می‌شد. اما امروزه یک حد وسط هم برای این تقسیم‌بندی قائل شده‌اند که به روش‌های «نیمه‌شکننده» معروف هستند.

یکی از برتری‌هایی که برای واترمارکینگ‌گذاری نسبت به رمزنگاری عنوان شد، تفاوت قائل شدن بین انواع مختلف تغییر است. هدف از بکارگیری واترمارکینگ‌های نیمه‌شکننده، تا حدودی به این وجه تمایز برمی‌گردد. چون در حوزهٔ تغییراتی که روی تصویر یا بطور عام، روی رسانه‌های رقمی صورت می‌گیرد، انگیزهٔ تغییرات مهم است. این تغییرات به دو دستهٔ قانونی و غیرقانونی یا به بیان دیگر، خصمانه و غیرخصمانه تقسیم می‌شود.

تغییرات قانونی (غیرخصمانه)، به تغییراتی گفته می‌شود که در اثر نوع کاربرد خاص و برای فشرده‌سازی و یا احیاناً بهبود رسانه، مخصوصاً تصویر صورت می‌گیرد که منجر به تغییر محتوایی تصویر نمی‌شود و گاهی ناچار از انجام این نوع پردازش‌ها هستیم و امکان انجام آنها، قبل از جاسازی واترمارکینگ وجود ندارد. واضح است که این تغییرات پذیرفتنی است امّا هدف تغییرات غیرقانونی، درست عکس موارد گفته شدهٔ قبلی است؛ یعنی در اینجا کسی که تصویر را دست‌کاری می‌کند، در پی تغییر در محتوای رسانه و یا اطلاعات پنهان

1- National Television Standards Committee
2- Amplitude Modulation
3- High Definition Television
4- Digital Video Disk
5- Video Home System
6- Robustness
۷- معمولاً در فشرده‌سازی داده‌ها کمی اتلاف داده وجود دارد

شده در آن است و این تغییر را عمداً انجام می‌دهد. ذکر این نکته هم لازم است که تغییر در اطلاعات تصویر، تغییر اطلاعات پنهان را به خودی خود به‌همراه دارد. لذا برای آن‌که بتوان اطلاعات پنهان را بعد از تغییرات غیرعمد، بازیابی کرد و در صورت بروز تغییر محتوایی، این‌کار قابل انجام نباشد، به واترمارکینگ‌های نیمه شکننده روی می‌آوریم.

در مقولهٔ خاص پنهان‌نگاری (کانال امن) بایستی روش ارائه شده کاملاً مقاوم باشد یعنی در صورت بروز هرگونه پردازش، اطلاعات پنهان، دستخوش تغییر و حتی کشف، قرار نگیرد و استخراج آن برای افراد مجاز نیز، بدون مشکل باشد.

۴-۳- مقاومت در برابر تغییر[1]

مقاومت یک سیستم واترمارکینگ‌گذاری در برابر حملات خصمانه، با پدافند غیرعامل ارتباط مستقیم دارد. انواع مختلفی از این نوع مقاومت وجود دارد. بسته به نوع کاربرد، انواع خاصی از حمله نسبت به سایر حملات، از اهمیت بالاتری برخوردار هستند. در واقع، کاربردهای متعددی وجود دارد که در آنها، واترمارکینگ، دشمن متخاصمی ندارد و مقاومت در مقابل تغییر، برای آنها از جایگاه خاصی برخوردار نیست. بعضی از انواع اساسی حمله عبارتند از:

- ***حملات فعال***: در این نوع حمله، هکر تلاش می‌کند که واترمارکینگ را حذف کند یا تغییر دهد تا آن را غیر قابل کشف نماید که برای بسیاری از کاربردها نیز خطرناک محسوب می‌شود. مثلاً تشخیص هویت شخص، اثبات مالکیت، اثر انگشت و کنترل کپی که نتوان نشان مورد نظر را پیدا کرد. در این‌صورت، هدف این کاربردها با شکست مواجه می‌شود. با این‌حال، حملات فعال در مورد تصدیق یا مخابرات پنهان، یک مسئلهٔ جدی به شمار نمی‌رود.
- ***حملات غیرفعال***: در حملات غیرفعال، هکر به دنبال حذف نشان نیست بلکه در پی مشخص کردن این موضوع است که آیا نشانی وجود دارد یا خیر؟ یعنی به دنبال آن است که بفهمد آیا یک ارتباطات پنهان در جریان است یا نه؟ بیشتر سناریوهایی که در بالا گفته شد با این حمله در نظر گرفته نمی‌شوند. در واقع ممکن است حتی وجود نشان اعلان شود و واترمارکینگ به‌عنوان یک عامل بازدارنده نقش ایفا کند. اما برای مخابرات پنهان، تلاش و هدف اصلی این است که از مشاهده شدن دادهٔ پنهان جلوگیری شود.
- ***حملات سازشی***: در واقع نوعی از حملات فعال هستند که در آن‌ها، هکر از چند کپی یک قطعه رسانه که هرکدام، واترمارکینگ متفاوتی دارند، استفاده می‌کند تا یک کپی بدون واترمارکینگ بسازد. مقاومت در برابر این حمله می‌تواند در مورد کاربرد اثر انگشت، بحرانی و حیاتی باشد. چون این کاربرد مستلزم قرار دادن یک نشان متفاوت در هر کپی مربوط به یک قسمت از رسانه می‌باشد. با این‌حال، تعداد کپی‌هایی که هکر می‌تواند فراهم کند، از یک کاربرد به کاربرد دیگر به شدت تغییر می‌کند. به‌طور مثال در کاربرد DiVX[2] یک هکر، هر تعداد پخش‌کنندهٔ DiVX که بخواهد می‌تواند بخرد و یک فیلم را با تمام آنها پخش کند تا هر تعداد کپی که با واترمارکینگ‌های مختلف لازم داشته باشد، در اختیار بگیرد. از طرف دیگر، در کاربرد ثبت روزانهٔ مراحل فیلم‌برداری، هر کارمند، فقط می‌تواند یک نسخه از مورد واترمارکینگ‌گذاری شده را در اختیار داشته باشد. برای اجرای چنین حمله‌ای، لازم است چندین کارمند، در نقشهٔ توطئه شریک شوند تا به مقصود خود برسند و آن را بدست آورند که آن هم بعید به‌نظر می‌رسد.
- ***حملات جعل***: در این نوع حمله، هکر تلاش می‌کند تا به‌جای حذف واترمارکینگ، یک واترمارکینگ معتبر را در دادهٔ غیرمعتبر جاسازی کند و این مقوله در کاربردهای تصدیقی یک هدف امنیتی است. چون اگر هکر بتواند نشان‌های معتبر تصدیق و تأیید را جاسازی کند، این

1- Tamper resistance

۲- نام اختصاری عبارت Digital Video Express، یک فرمت جدید DVD-Rom است که از سوی چندین شرکت بزرگ فیلم‌سازی همچون Paramount، Dreamworks SKG، Disney و Universal ارائه شده است. با استفاده از این فرمت، یک فیلم (یا هر اطلاعات دیگری) که در داخل DVD-Rom قرار می‌گیرد، تنها برای زمان محدودی قابل پخش است. بنابراین به محض این‌که DVD مذکور را در داخل دستگاه پخش قرار می‌دهید، یک شمارنده شروع به شمارش می‌کند. هر پخش‌کننده DivX امکان اتصال به خط تلفن و برقراری ارتباط با سرور اصلی شرکت پخش کننده را دارد تا بتواند اطلاعات مربوط به هزینه خدمات را دریافت کند. این فرمت جدید تنها از سوی چند شرکت ارائه می‌شود و بالطبع هنوز از سوی تمامی شرکت‌های سازنده تجهیزات پخش کننده مورد استقبال قرار نگرفته است. بنابراین بر روی برخی از دستگاه‌های پخش DVD عبارت DivX نقش بسته است. فرمت DivX یک فرمت فشرده‌سازی تصویری است که بر اساس فناوری MPEG-4 بنا شده است.

نشان‌ها می‌توانند باعث شوند که آشکارساز، رسانهٔ جعلی یا تغییر یافته را بپذیرد. هم‌چنین، این نوع حمله یک نگرانی جدی برای اثبات مالکیت شخصی محسوب می‌شود.

۴-۴- حجم محاسبات

کاربردهای مختلف نیاز دارند که جاسازها و آشکارسازها در سرعت‌های مختلف، کار کنند. در کار نظارت بر پخش، جاساز و آشکارساز هر دو، باید به‌صورت آنی یا زمان واقعی کار کنند. جاسازها نباید زمان‌بندی تولید رسانه را کند کرده و به تأخیر بیندازند و آشکارسازها هم باید همگام با پخش‌های زمان‌واقعی پیش بیایند و تحمل این سرعت را داشته باشند. از طرف دیگر برای اثبات مالکیت شخصی، اگر یک آشکارساز روزها وقت صرف کند، باز هم ارزشمند خواهد بود. چنین آشکارسازی فقط در جریان منازعه‌ای که بر سر مالکیت شخصی پیش می‌آید استفاده خواهد شد که این موارد هم کمیاب هستند و نتیجهٔ آن مبنی بر این‌که آیا واترمارکینگ وجود دارد یا خیر، بقدری برای کاربر مهم است که حاضر است هر چقدر طول بکشد، صبر کند.

در ضمن، کاربردهای مختلف، به تعداد جاساز و آشکارسازهای مختلفی نیاز دارند. مثلاً نظارت پخش، به تعداد کمی جاساز نیاز دارد ولی شاید چند صد آشکارساز در موقعیت‌های جغرافیایی مختلف، مورد نیاز آن باشد. یا کنترل کپی ممکن است تعداد انگشت شماری جاساز لازم داشته باشد، اما میلیون‌ها آشکارساز را شامل شود. برعکس در کاربردهای مربوط به اثر انگشت که توسط DiVX اجرا شده و در آن، هر پخش‌کننده‌ای، یک واترمارکینگ مجزا را جاسازی می‌کند، میلیون‌ها جاساز وجود خواهد داشت ولی تعداد محدودی آشکارساز وجود دارد. به‌طور کلی، هرچه تعداد بیشتری از یک وسیله مورد نیاز باشد، هزینه و بار محاسباتی آن باید کمتر باشد. به‌عنوان مثال تغییرات وسیع در ارزش دلار و نیز در سرعت تقاضاها، به این معنا است که تغییرات وسیعی در بازده و کارایی محاسباتی جاسازها و آشکارسازهای واترمارکینگ مورد نیاز است.

۴-۵- نرخ مثبت کاذب[1]

یک «مثبت کاذب» به واقعهٔ کشف واترمارکینگ در قطعه رسانه‌ای گفته می‌شود که به طور واقعی شامل آن واترمارکینگ نیست. زمانی که از نرخ چنین وقایعی صحبت می‌شود، به معنی "نرخ مثبت کاذب"، منظور تعداد چنین اتفاقاتی در تعداد مشخصی از عملیات آشکارسازی واترمارکینگ است. مثبت کاذب را می‌توان خطای مثبت هم تعبیر کرد که در مقابل آن خطای منفی (منفی کاذب) [2] قرار دارد و به معنای عدم تأیید واترمارکینگ در یک رسانهٔ محتوی واترمارکینگ می‌باشد.

۴-۶- ظرفیت[3]

یکی دیگر از خواص روش‌ها و الگوریتم‌های پنهان‌سازی داده، ظرفیت است. در مورد تصاویر، معمولاً این پارامتر را به‌صورت درصدی از دادهٔ خام موجود در تصویر بیان می‌کنند. در یک دید کلی، ظرفیت عبارت است از حداکثر اندازهٔ پیامی که می‌تواند درون دادهٔ میزبان قرار گیرد. راه‌های مختلفی برای اندازه‌گیری ظرفیت، تاکنون ارائه شده که بعضی بر تئوری اطلاعات، بعضی بر روش‌های مبتنی بر احساس و ادراک و نهایتاً بعضی بر تئوری کشف استوار هستند. ممکن است تصور شود که ظرفیت، هم ناظر به بحث پنهان‌نگاری است و هم در واترمارکینگ‌گذاری مطرح می‌شود و ممکن است نتوان واترمارکینگ با هر اندازه‌ای را درون رسانهٔ مورد نظر جاسازی کرد، یا چنان‌چه جاسازی شود، کیفیت تحت‌الشعاع قرار می‌گیرد.

۴-۷- قابل درک یا غیرقابل درک بودن

همان‌طور که در بحث تقسیم‌بندی مسائل مربوط به پنهان‌سازی داده مطرح شد، بعضی از شاخه‌ها، خود به مرئی و نامرئی تقسیم می‌شوند. شاید این پرسش مطرح شود که اگر پنهان‌سازی مطرح است، مرئی و نامرئی بودن چه معنایی دارد یا به عبارت بهتر مرئی بودن بی‌معناست. در جواب باید گفت، این اصطلاح به اصل وجود پیام پنهان برمی‌گردد. به‌طور مثال در بعضی موارد، باید وجود واترمارکینگ، مشخص و پیدا باشد؛ ولی در بعضی موارد هم اثری از وجود واترمارکینگ نباید باشد. در عین حال در هر دو مورد، اطلاعات مربوط به خود واترمارکینگ، نباید در دسترس قرار گیرد.

1- FPR (False-Positive Rate)

2- FNR (False-Negative Rate)

3- Capacity

۴-۸- عمومیت

با توجه به تنوعی که در میان رسانه‌ها وجود دارد، روش‌هایی که معمولاً برای پنهان‌سازی ارائه می‌شود، منحصر به نوع خاصی از این رسانه‌ها است. بعضی از این رسانه‌ها همان‌طور که در مطالب قبلی اشاره شد عبارتند از: متن، صوت، تصویر، فیلم و غیره.

به تازگی به این مجموعه، فایل‌های اجرایی، صفحات وب، آدرس‌ها و محتوای پست‌های الکترونیکی نیز اضافه شده است. انحصاری که از آن یاد شد، بعضاً در میان خود شاخه‌های هر رسانه هم وجود دارد. به‌طور مثال اگر روشی برای پنهان‌نگاری در تصویر یا واترمارکینگ‌گذاری تصویر ارائه شود، ممکن است همهٔ انواع تصویر را در بر نگیرد و فقط شامل تصاویر دودویی[1] یا فقط شامل تصاویر ۲۴ بیتی شود [۵]. لذا اگر بتوان از یک الگوریتم در مورد رسانه‌های مختلف استفاده کرد، معیار عمومیت بالا رفته است و این مزیت حاصل می‌شود که در مواقع ضروری، می‌توان بین رسانه‌های مختلف سوئیچ کرد.

همان‌طور که گفته شد، تقابل موجود بین نکات گفته شده، این اجازه را نخواهد داد که همه مشکلات به طور همزمان برطرف شود. در این میان اگر در یک روش پنهان‌نگاری بتوان از فایل‌های میزبان مختلفی استفاده نمود، این روش‌ها از عمومیت بالایی برخوردار هستند و در مواردی که نسبت به یک نوع میزبان خاص، حساسیت ایجاد شود، می‌توان از انواع دیگر آنها استفاده نمود.

علاوه بر معیارهای مطرح‌شده فوق، طراحی و پیاده‌سازی سیستم‌های پنهان‌نگاری براساس استانداردهای مرتبط مانند ISO10006 ، PMBOK2004 و غیره نیز مهم و لازم‌الاجرا است.

۵- سیستم فایل پنهان‌نگاری شده[2]

در علوم رایانه، سیستم فایل روشی است برای ذخیره‌سازی و مدیریت فایل‌های رایانه‌ای و داده‌هایی که آن فایل شامل می‌شود تا پیدا کردن و دسترسی به آن اطلاعات، مخصوصاً در حالت‌های بحرانی، آسان گردد. بیش‌تر سیستم‌های فایل از یک ابزار ذخیره داده اساسی مثل هارد دیسک یا CDROM استفاده می‌کنند که دسترسی به آرایه‌ای از بلوک‌های با طول ثابت را عرضه می‌کند. به این بلوک‌ها گاهی سکتور نیز گفته می‌شود و اندازه آنها معمولاً توانی از ۲ است (۵۱۲ بایت یا ۱، ۲ یا ۴ کیلوبایت مقادیر معمول‌تر این اندازه‌ها هستند). نرم‌افزار سیستم فایل مسئول مدیریت این سکتورها برای فایل‌ها و دایرکتوری‌ها است و این موضوع را دنبال می‌کند که کدام سکتورها به کدام فایل‌ها مربوط هستند و کدام سکتورها مورد استفاده قرار نگرفته‌اند.

سیستم فایل پنهان‌نگاری شده نوعی سیستم فایل است که اولین بار توسط راس اندرسون[3]، راجر نیدهام[4] و ایدی شامیر[5] ارائه شد [۶]. مقاله‌ای که این سه نفر ارائه کردند دو روش اصلی برای مخفی کردن داده معرفی می‌کند:

۱- فایل‌های مربوط به کاربر در دنباله‌ای از فایل‌های با طول ثابت که اساساً حاوی بیت‌های تصادفی هستند قرار داده می‌شود. این دنباله از فایل‌ها بواسطه یک کلمه عبور انتخاب خواهند شد. فرض کنید مجموعه‌ای از فایل‌های با طول ثابت با محتوای بیت‌های تصادفی به نام‌های $C_0, C_1, ..., C_{k-1}$ وجود دارد. هم‌چنین برای اولین گام، فایل کاربر F و کلمه عبورش نیز P در نظر گرفته می‌شود. حال فایل‌های C_j به ازای مقادیری از j که jامین بیت کلمه عبور، مقدار ۱ دارد را انتخاب کرده و محتوای فایل‌ها با استفاده از XOR بیتی ترکیب می‌شوند. حاصل را با فایل کاربر XOR کرده و نتیجه این مرحله نیز با یکی از C_jها مجدداً XOR می‌شود. آنچه حاصل می‌گردد فایل کاربر است که با زیرمجموعه‌ای از C_jها XOR شده است. به‌صورت ریاضی می‌توان فرآیند را به‌صورت زیر نشان داد:

$$F = \bigoplus_{P_j=1} C_j$$

یکی از خاصیت‌های مهم این سیستم این است که اگر یک دسترسی خطی سلسله مراتبی وجود داشته باشد[6] آنگاه می‌توان بدون ایجاد اختلال در فایل‌هایی که در حال حاضر مخفی شده‌اند، به‌صورت طبیعی فایل‌های دیگری نیز اضافه کرد.

1- Binary
2- Steganographic file system

3- Ross Anderson
4- Roger Needham
5- Adi Shamir

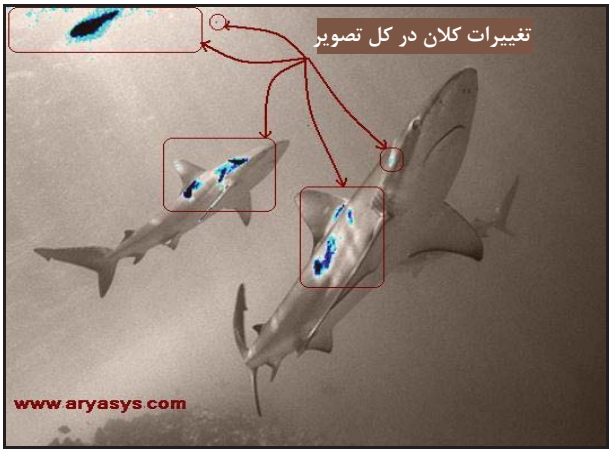
۶- یعنی کاربری که با سطحی از امنیت فایلی را ذخیره می‌کند، کلمات عبور تمام فایل‌های ذخیره شده با سطوح امنیت پایین‌تر را می‌داند.

۲- در روش دوم، کل یک اِفراز[1] از هارد را با بیت‌های تصادفی پر کرده و فایل‌های کاربر در آن پنهان می‌شوند. در این روش، نه فایل‌های کاربر و نه رمزشده آن هیچ‌کدام ذخیره نمی‌گردند بلکه کل اِفراز تصادفی می‌شود. زیرا فایل‌های رمزنگاری شده به شدت شبیه به بخش‌های تصادفی شده اِفراز هستند و بنابراین وقتی فایل‌ها روی اِفراز ذخیره می‌شوند راه آسانی برای تمایز قائل شدن بین فایل‌های نامفهوم فاقد معنی و فایل‌هایی که واقعاً رمز شده‌اند وجود ندارد. علاوه بر این، موقعیت فایل‌ها از کلید فایل استخراج شده و موقعیت‌ها پنهان می‌شوند و تنها در اختیار برنامه‌هایی قرار دارند که همان رمز عبور را دارند. این مسئله منجر به این می‌شود که فایل‌ها به سرعت روی همدیگر بازنویسی شوند که این مسئله هم با نوشتن تمام فایل‌ها در چندین مکان جبران می‌شود و احتمال از دست دادن داده را تقلیل می‌دهد.

۶- مطالعهٔ موردی بر روی معیارهای طراحی و پیاده‌سازی پنهان‌نگاری

در مطالعه موردی با روش LSB، استفاده و یا عدم استفاده معیارهای مطرح شده، مورد بررسی قرار می‌گیرند. اگر بدون در نظر گرفتن هیچ محدودیتی پنهان‌نگاری پیاده‌سازی گردد، مسلماً حامل از حالت اصلی خود خارج شده و تغییرات زیادی در حامل رؤیت خواهد شد. روش جایگزینی کم ارزش‌ترین بیت، ساده‌ترین روش برای پنهان‌نگاری است. در این روش کم ارزش‌ترین بیت (یا دومین بیت کم ارزش) پیکسل‌های تصویر حامل که به عنوان نویز تصویر شناخته می‌شوند، با دنباله بیت پیام جایگزین می‌شود. به طور متوسط می‌توان گفت حدوداً ۵۰٪ احتمال دارد که در اثرگذاری هر بیت پیام، LSB پیکسل‌های تصویر از مقدار صفر به یک یا بالعکس بدل[2] شوند. برای ایجاد امنیت، محل جاگذاری (پیکسل‌ها) به‌صورت شبه تصادفی[3] انتخاب می‌شود. پس از جاگذاری، گیرنده از روی محل پیکسل‌ها که به صورت کد در اختیار او قرار داده می‌شود می‌تواند پیام را به‌طور سریال از LSBها استخراج کند. در مورد تصاویر رنگی که هر پیکسل شامل سه کانال رنگ قرمز، سبز و آبی است، می‌توان ظرفیت را بالا برد و سه بیت در هر پیکسل جاگذاری نمود. همان‌طور که ملاحظه می‌گردد این روش ظرفیت خیلی بالایی دارد و در صورتی که تصویر قبل از جاگذاری فشرده شود، این ظرفیت افزایش خواهد یافت. اما در عوض نسبت به کوچک‌ترین تغییرات، حوزه تصویر بسیارحساس و شکننده است. هم‌چنین روش پنهان‌نگاری LSB امنیت بالایی ندارد و پنهان‌شکن می‌تواند وجود پیام را به سادگی تشخیص دهد؛ چرا که به دلیل جاگذاری مستقیم در مقادیر شدت پیکسل‌ها، اولاً کیفیت بصری تصویر پایین می‌آید و ثانیاً پس از جاگذاری، به دلیل ثابت ماندن شدت برخی از پیکسل‌ها که LSB آن‌ها با بیت پیام برابر بوده و احتمال یکسان در تبدیل شدن صفر و یک به هم در LSB پیکسل‌های مخالف بیت پیام (با تبدیل شدت روشنایی[4] فرد به زوج به صورت کاهشی و شدت روشنایی زوج به فرد به صورت افزایشی)، تعداد پیکسل‌های با شدت روشنایی یکسان بالا می‌رود و در نتیجه در هیستوگرام شدت‌ها، جفت مقادیر[5] (Pov) خواهیم داشت که آن‌را می‌توان به وسیله حمله آماری مربع خی[6] آشکار نمود.

همان‌طور که در شکل (۳) مشاهده می‌شود درصورت اضافه کردن اطلاعات به بیت‌های کم ارزش، بدون رعایت معیار ظرفیت، تغییرات کلی در تصویر حاصل می‌شود که با حملات بسیار ساده می‌توان به اطلاعات پنهان شده در تصویر دست یافت.

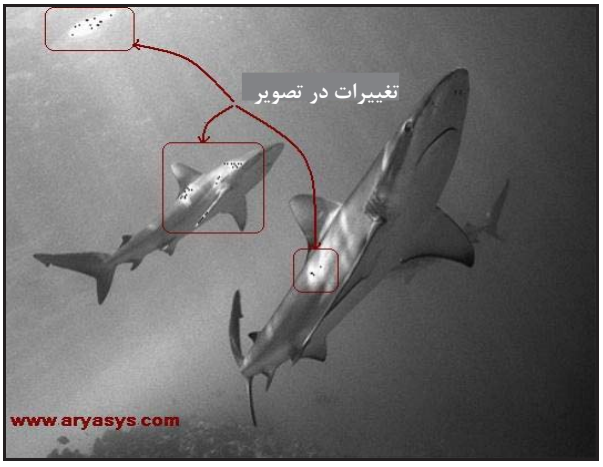


شکل ۳- پنهان‌نگاری به روش LSB بدون رعایت هیچ معیاری

1- Partition
2- Flip
3- Pseudo-Random
4- Luminance
5- **Pair of Values**
6- Chi-Square

حجم تصویر خام (بدون اضافه کردن اطلاعات) ۵۸۱۳۳۲۸ بیت است که حداکثر ۷۲۶۶۶۶ بیت کم ارزش جهت بارگذاری اطلاعات شناسایی شده است. البته برخی از بیت‌های کم ارزش هم با توجه به موقعیت پیکسل، درصورت بارگذاری، تغییرات بر روی تصویر مشاهده خواهد شد که به این بیت‌ها، بیت کم ارزش غیرقابل تغییر گویند. در این مطالعه موردی ۹۰۰۰۰۰ بیت داده اطلاعات بارگذاری شده است که ۱۷۳۳۳۴ بیت اضافی بارگذاری شده است. با توجه به شکل (۳) با سرریز داده‌های پیام بر روی داده‌های پر ارزشِ حامل، تغییرات کلان در کل تصویر مشاهده می‌گردد.

حال اگر در معیار ظرفیت به اندازه بیت‌های کم ارزش، یعنی ۷۲۶۶۶۶ بیت اطلاعات بارگذاری شود تغییرات کم‌تری در تصویر مشاهده خواهدشد و کمتر جلب توجه می‌کند (شکل ۴). ولی اگر در معیار ظرفیت، بیت‌های کم ارزش غیرقابل تغییر هم شناسایی شود و بارگذاری نگردد، تغییرات در تصویر به حداقل رسیده و با چشم غیرمسلح قابل رؤیت نخواهد بود. در شکل (۵) میزان اطلاعات بارگذاری به ۲۰۰۰۰۰ بیت تقلیل یافته است.



شکل ۴- پنهان‌نگاری به روش LSB با رعایت فقط معیار ظرفیت

۷- نتیجه‌گیری

این مقاله بعد از معرفی اجمالی پنهان‌نگاری و اهمیت استفاده آن در پدافند غیرعامل، به برخی از معیارهای مهم که در هنگام طراحی و پیاده‌سازی سامانه‌های پنهان‌نگاری بایستی در نظر گرفت، اشاره می‌کند. با توجه به این‌که ذات پنهان‌نگاری یک فعالیت در زمینه پدافند غیرعامل است (حفاظت از اطلاعات و بطور کلی تمام اشیاء و پدیده‌ها)، عدم رعایت معیارهای طراحی و پیاده‌سازی، مشکلاتی را به‌خصوص در مواقع بحرانی، دربَر داشته و ممکن است نتیجه معکوس و مخرّبی داشته باشد. در چنین حالتی با تصوّر این‌که کانال امن است اقدام به ارسال و دریافت اطلاعات مهمی می‌شود. در حالی‌که به‌خاطر عدم رعایت معیار ظرفیت و نشت اطلاعات، کانال تحت شنود نامحسوس دشمن بوده و هرگونه تخریبی امکان‌پذیر است.

از این‌رو رعایت معیارهای طراحی و پیاده‌سازی جهت امنیت سامانه‌های پنهان‌نگاری به‌خصوص با دیدگاه پدافند غیرعامل امری لازم و ضروری می‌باشد. ضمن این‌که مواردی چون رعایت **اصول امنیتی پیاده‌سازی نرم‌افزاری یا سخت‌افزاری و رمزنگاری** پیام قبل از پنهان‌نگاری نیز بسیار مهم و ضروری است که می‌تواند موضوع تحقیقات مستقل در این زمینه باشد.

شکل ۵- پنهان‌نگاری به روش LSB با رعایت تمام معیارها

مراجع

1. M. Kivanc. M. "Information hiding codes and their application to images and audio". PHD thesis. University of Illinois at Urbana - Champaign, (**2002**).
2. Chien-Chang Lin, Shi-Huang Chen, Trieu-Kien Truong, Fellow and Yukon Chang, "Audio Classification and Categorization Based on Wavelets and Support Vector Machine", IEEE TRANSACTIONS ON SPEECH AND AUDIO PROCESSING, VOL. 13, NO. 5, SEPTEMBER (**2005**).
3. I. J. Cox, Matthew L. Miller, Jeffrey A. Bloom, Jessica Fridrich, "Digital Watermarking and Steganography", ISBN 978-0-12-372585-1, (**2007**).

4. I. J. Cox, M. L. Miller and J. A. Bloom, "Watermarking applications and their properties", Published in the Int. Conf. on Information Technology'2000, Las Vegas, (2000).
5. E. Kawaguchi and R. Taniguchi, "Complexity of binary pictures and image thresholding - An application of DFExpression to the thresholding problem", Proceedings of 8th ICPR, vol.2, pp.1221-1225, (**1986**).
6. Ross Anderson (Cambridge University), Needham (Microsoft Research Ltd) and Adi Shamir (Weizmann Institute) "The Steganographic File System", (**1998**).

Design and Implementation Criteria for a Secure Steganography System from the Passive Defense Perspectives

Reza Esfahani[1]

Abstract

The parameters of being secret and remaining secret contribute to the mitigation of vulnerability and enhancement of resistance and facilitation of security management against enemy's military threats and actions. Apparent normalization of communications is one of the most significant and obvious issues of steganography. Therefore; steganography is inclusive of the principles and laws of passive defense in countering software and electronic threats and enemy's other new threats in order to maintain and safeguard information, communications and computer systems. An unsafe communication channel by which the transmission of sound-digital, image and video medias is possible and access to the communication of the other side(the same relevant receiver) is made possible, as well, steganography can also be practically implemented on such a domain which safeguards the relevant information considering the special conditions and criteria, regardless of the origin of threat.

This article is intended to review the special conditions and criteria which have to be observed before designing the steganography product(design limitations) accompanied by a case study.

Key Words: *Steganography, Cryptography, Watermarking, Steganography File System*

1- Email: isfahani@aryasys.com