ISSN: 2745-3673
http://www.Rcsj.ir

مجلـه‌ی علمی پژوهش در علوم رایانه (سال سوم)
شماره ۹ / بهار ۱۳۹۷ / ص ۹- ۱

استگانوگرافی، واترمارکینگ و نقش آن در امنیت اطلاعات درفضای مجازی

افسون سروقد [۱]، پویا روزبه جوان [۲]، عرفانه نوروزی [۳]

[۱] دانشجوی کارشناسی ارشد مهندسی فن آوری اطلاعات، دانشگاه آزاد اسلامی واحد سپیدان.

[۲] دانشجوی کارشناسی ارشد مهندسی فن آوری اطلاعات، دانشگاه آزاد اسلامی واحد سپیدان.

[۳] استادیار، گروه کامپیوتر و فن آوری اطلاعات، دانشگاه آزاد اسلامی واحد سپیدان.

نام نویسنده مسئول:
افسون سروقد

چکیده

با توجه به گسترش فناوری در دنیای امروز و امکان انجام اکثر عملیات از راه دور ،با استفاده از شبکه‌های جهانی و محلی، همچنین عدم لزوم تمرکز همه داده‌ها در یک محل و نیاز به دستیابی به برخی از اطلاعات راه دور وهم چنین حفظ امنیت اطلاعات در زمان ارسال و دریافت، اهمیت مسئله نگهداری اطلاعات از دسترسی های غیر مجاز را دو بیش از پیش آشکار می سازد. پنهان نگاری اطلاعات روشی است که می‌توان اطلاعات مورد نظر را در قالب یک عامل پوشاننده و با بیشترین میزان دقت به امنیت، بین نقاط موردنظر جابجا نمود ، به گونه‌ای که حتی اگر در طی مسیر، اطلاعات از طریق افراد غیرمجاز مورد دسترسی قرار گرفت امکان دستیابی به داده‌های پنهان شده وجود نداشته باشند. در واقع پنهان‌نگاری هنر و علم جاسازی اطلاعات در یک رسانه حامل است که با توجه به پیشرفت قابل توجه ارتباطات دیجیتال استفاده از آن رو به افزایش می‌باشد. در پنهان‌نگاری هدف اصلی، امنیت به معنای عدم توانایی در اثبات وجود پیغام است.

واژگان کلیدی: استگانوگرافی، پنهان نگاری اطلاعات، واترمارکینگ.

مجلـه‌ی علمی پژوهش در علوم رایانه ، شماره ۹ ، بهار ۱۳۹۷، ص ۹- ۱

ISSN: 2745-3673
http://www.Rcsj.ir

مقدمه

Steganographyدر یونانی به معنای پوشیده شده یا نوشتن مخفیانه است. هدف steganography این است که پیغامی را در یک پیغام دیگرِ بی خطر به روشی ذخیره کند که دشمن پی به وجود پیغام اولی در پیغام دوم نبرد. جوهر های نامرئی یکی از عمومی ترین ابزارها برای steganographyهستند استگانوگرافی موضوعی است که به ندرت از طریق هواخواهان امنیتی فناوری اطلاعات مورد توجه قرار گرفته است. در حقیقت پنهان نگاری (نهان نگاری) پروسه ای است که در طی آن یک داده را در دیگر شکل های دیگر داده ای مثل فایل های عکس یا متن مخفی می کنند. معروف ترین و رایج ترین متد مخفی کردن داده در فایلها بکارگیری تصاویر گرافیکی به عنوان مکان‌هایی مخفی می باشد.

در زمینه پزشکی، استگانوگرافی، به عنوان یک ابزار توانمند، اطلاعات شخصی بیمار را روی یک سیگنال حامل که در اینجا همان تصاویر پزشکی است، مخفی کرده و با در اختیار قرار دادن یک تصویر استگانوگرافی شده که یک فایل توأم تصویر پزشکی و اطلاعات خصوصی بیمار است، تنها به افرادی که کد مخصوص نهان‌سازی اطلاعات را در اختیار دارند، اجازه دسترسی به اطلاعات بیمار را می‌دهد. استگانوگرافی در تصاویر پزشکی با توجه به ویژگی‌های خاص این تصاویر، مستلزم تمهیدات خاصی است. وجود پس‌زمینه بسیار زیاد و همچنین اهمیت خاص کیفیت تصویر در تشخیص بیماری، از ویژگی‌های مهم همه تصاویر پزشکی است .بنابراین روش‌های بکار گرفته شده در مورد این تصاویر باید به گونه‌ای باشد که ضمن استفاده بهینه از پس‌زمینه، کمترین آسیب را به تصویر وارد کند.

۱-تاریخچه

تاریخچه استگانوگرافی به ۵ قرن قبل از میلاد مسیح و کشور یونان برمی گردد، در آن زمان مردی به نام هیستایاکاس می خواست پیغامی را به صورت محرمانه برای شخص دیگری بفرستد. وی برای فرستادن پیغام مورد استفاده از این روش استفاده کرد: او برده ای را برای این کار انتخاب کرد و موهای سر برده را تراشید و پیغام محرمانه را بر روی پوست سر برده خالکوبی کرد و سپس مدتی صبر کرد تا موهای فرد رشد کرده و به حالت اول برگشت و بعد او را به سمت مقصد (گیرنده) روانه کرد در مقصد، گیرنده ی پیغام دوباره موهای برده را تراشید و پیغام را بر روی پوست سر او مشاهده کرد .

۲-استگانوگرافی چیست؟

استگانو گرافی از لغت یونانی استگانوس (پوشاندن) و گرافتوس (نوشتن) گرفته شده است . در واقع استگانوگرافی دانشی است برای پنهان کردن داده یا فایلی در فایل دیگر، بطوری که فقط افراد آگاه با ابزار لازم بتوانند به آن دست یابند.استفاده از این روش در مواردی بسیار عالی و کاربردی است. برخلاف رمزگذاری که فایل حفاظت شده را کاملاً حساس جلوه می‌دهد و جلب توجه می کند، این روش از ناآگاهی افراد، برای جلوگیری از دستیابی آن‌ها به اطلاعات خاص بهره می برد. این کار شبیه پنهان کردن اشیای گرانبها در قوطی بیسکویت، داخل کابینت آشپزخانه است؛ جایی که معمولاً هیچ دزدی احتمالش را نمی‌دهد. پنهان نگاری خود شاخه ای از دانشی به نام ارتباطات پوشیده است. دانش ارتباطات پوشیده خود شامل چندین شاخه از جمله رمز نگاری، ته نقش نگاری و ... می باشد.

۳- تفاوت پنهان نگاری (steganogrphy)و رمزنگاری(Cryptography)

۳-۱- تفاوت اصلی رمزنگاری و پنهان نگاری

آن است که در رمز نگاری هدف اختفاء محتویات پیام است و نه به طور کلی وجود پیام، اما در پنهان نگاری هدف مخفی کردن هر گونه نشانه‌ای از وجود پیام است. در مواردی که تبادل اطلاعات رمز شده مشکل آفرین است باید وجود ارتباط پنهان گردد. به عنوان مثال اگر شخصی به متن رمزنگاری شده‌ای دسترسی پیدا کند، به هر حال متوجه می‌شود که این متن حاوی پیام رمزی می‌باشد. اما در پنهان نگاری شخص سوم ابدا از وجود پیام مخفی در متن اطلاعی حاصل نمی‌کند. در موارد حساس ابتدا متن را رمزنگاری کرده، آنگاه آن را در متن دیگری پنهان نگاری می‌کنند. اما با وجود بهتر بودن استگانوگرافی در مقابل رمز گذاری همچنان بسیاری از افراد می گویند:رمزنگاری بهتر از استگانوگرافی (stganography)عمل می کند(۱).

۴- شمای کلی استگانوگرافی

برای جاسازی اطلاعات در داخل یک فایل دیگر روش‌های فراوانی وجود دارد .معروف‌ترین این روش ها،روش LSB می‌باشد که اطلاعات را درون بیت‌های کم ارزش رنگ‌های تصویر قرار می‌دهد. استگانوگرافی علاوه بر حمل اطلاعات مخفی کاربردهای دیگری نیز دارد. یکی از کاربردهای عمومی آن می‌تواند این باشد که برای مثال صاحب حقوقی یک عکس، یک سری پیام درون تصویر جاسازی کند. هر گاه

ISSN: 2745-3673
http://www.Rcsj.ir

چنین تصویری دزدیده شود و در یک وب سایت قرار داده شود، مالک قانونی آن می‌تواند این پیام محرمانه و سری را برای اثبات مالکیت به دادگاه عرضه کند .به این نوع استگانوگرافی اصطلاحاً نشانه گذاری یا watermarking گفته می‌شود.

۵- تقابل امنیت، ظرفیت و مقاومت

به صورت کلی در سیستم‌های اختفاء اطلاعات سه عنصر اصلی ظرفیت، امنیت و مقاومت دخیل هستند. در روش‌های پنهان نگاری عناصر ظرفیت و امنیت اهمیت اصلی را دارند. در دنیای امروز، جوهر نامرئی و کاغذ که در گذشته برای برقراری ارتباط پنهانی به کار برده می‌شد به وسیله رسانه‌های عملی‌تر مثل تصویر -ویدئو- فایل‌های صوتی جایگزین شده‌اند. به دلیل اینکه این رسانه‌های دیجیتال دارای افزونگی اطلاعاتی زیادی هستند می‌توانند به عنوان یک پوشش مناسب برای پنهان کردن پیام استفاده شوند. تصاویر مهم‌ترین رسانه مورد استفاده به خصوص در اینترنت هستند و درک تصویری انسان از تغییرات در تصاویر محدود است. تصاویر نوعی رسانه پوششی مناسب در پنهان نگاری محسوب می‌شوند و الگوریتم‌های پنهان نگاری متعددی برای ساختارهای مختلف تصاویر ارائه شده‌است. هیچ یک از این الگوریتم‌ها تاکنون امنیت را به طور کامل تأمین نکرده‌اند. به طور کلی روش‌های پنهان نگاری در تصویر از الگوریتم جاسازی و الگوریتم استخراج بیت‌ها تشکیل شده‌اند. به تصویر مورد استفاده برای پنهان نگاری پوشانه و به تصویری که در اثر قرار دادن پیام به وسیله الگوریتم جاسازی به دست می‌آید تصویر میزبان یا گنجانه می‌گوییم. الگوریتم‌های پنهان نگاری به صورت عمومی از افزونگی در فضای مکانی یا افزونگی در فضای تبدیل استفاده می‌کنند. در هر کدام از این فضاها به شیوه‌های گوناگونی می‌توان داده‌ها را پنهان کرد که یکی از ساده‌ترین روشها، استفاده از بیت‌های کم ارزش فضای مورد نظر است. در پنهان نگاری نیز همانند رمز نگاری فرض بر آن است که الگوریتم‌های بکار رفته در پنهان نگاری برای همه آشکار است. امنیت در این روشها بر پایه پنهان بودن کلید تعریف می‌گردد به طوری که نتوان بدون داشتن کلید هیچ اطلاعی از وجود پیام پنهان کسب کرد(۲).

۵-۱- تعریف پنهان شکنی

پنهان شکنی هنر کشف حضور اطلاعات پنهان است. روش‌های پنهان نگاری در صورتی امن هستند که تصویر میزبان یا گنجانه دارای نشانه‌های قابل کشف نباشد. به بیان دیگر، خواص آماری تصویر میزبان یا گنجانه باید همانند خواص آماری پوشانه باشد. توانایی کشف پیام در تصویر به طول پیام پنهان بستگی دارد .واضح است که هرچه مقدار اطلاعاتی که در یک تصویر قرار می‌دهیم کمتر باشد امکان کمتری هست که نشانه‌های قابل کشف به وجود آید. انتخاب فرمت تصویر نیز تأثیر زیادی بر سیستم پنهان نگاری دارد. فرمت‌های فشرده نشده‌ای مثل BMP ، فضای زیادی برای پنهان نگاری فراهم می‌کنند ولی استفاده از آنها به دلیل حجم اطلاعات زائد بالای آنها شک برانگیز است.

۶-انواع مختلف استگانوگرافی

در پنهان‌نگاری به جای تصویر می‌توان از فایل‌های صوتی و یا تصویری و حتی متنی برای مخفی سازی اطلاعات استفاده کرد. در فایل‌های متنی معمولا از tabها وspaceهای آخر سطرها که در اکثر ویرایشگرها توسط انسان قابل تشخیص نیستند، استفاده می‌شود. اطلاعات مخفی شده نیز لزوما متن نیستند بلکه می‌توانند هر نوع فایلی باشند. مثلا می‌توان یک تصویر را نیز در داخل تصویر دیگر جاسازی کرد. همچنین روش‌های پنهان نگاری، محدود به روش‌های مطرح شده‌ی موجود نیستند بلکه هر شخص می‌تواند از روش دلخواه خود برای پنهان نگاری استفاده کند.

۷- تشریح تکنیک های Steganography

فرمول کلی برای تابع Steganography این چنین است:

شی ای که قراراست اطلاعات در آن نگهداری شود + اطلاعاتی که باید مخفی شوند +الگوریتم مورد نظر = شی مورد نظر که اطلاعات در آن مخفی شده اند.فایلی که برای مخفی کردن اطلاعات به کار می رود، می تواند یک تصویر، فایل صوتی و یا یک فایل ویدئویی باشد. درعین حال دو روش معمول برای Steganographyوجود دارد که عبارتند از.Injection,LSB :

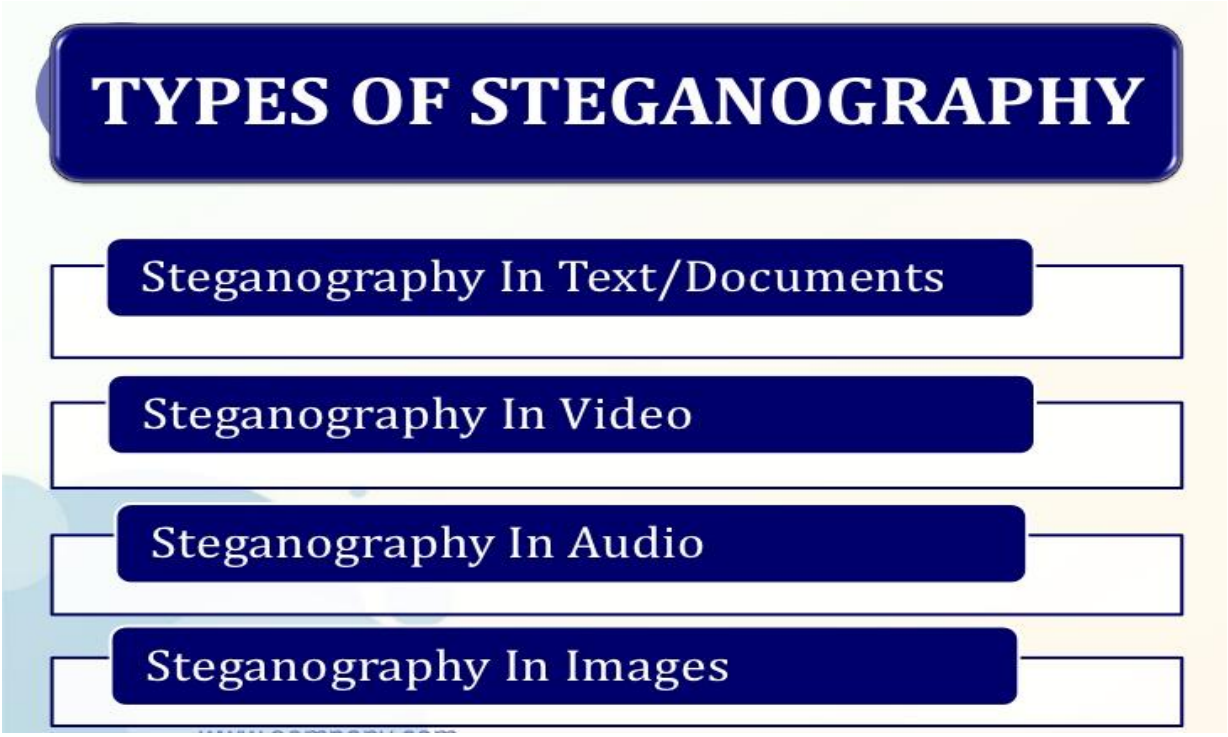
LSB: وقتی فایلی ساخته می شود، معمولاً بعضی از بایت های آن یا قابل استفاده نیستند و یا کم اهمیت هستند. این بایت ها می توانند تغییرداده شوند، بدون اینکه لطمه قابل توجهی به فایل وارد شود. این خاصیت کمک می کند تا بتوان اطلاعاتی را در این بایت ها قرار داد، بدون اینکه کسی متوجه این موضوع گردد.

ISSN: 2745-3673
http://www.Rcsj.ir

روش LSB بر روی فایل های تصویری که دارای رزولوشن وتعداد رنگ های بالایی است و بر روی فایل های صوتی که دارای تعداد زیادی صدای مختلف است، به خوبی کارمی کند. ضمناً این روش حجم فایل را افزایش نمی دهد.

Injection: روشی ساده است که برمبنای آن، اطلاعاتی که قراراست مخفی شوند را در یک فایل تزریق می کنند. مهمترین مسأله در این روش، افزایش حجم فایل است(۳).

۸-Steganographyدر فرمت های مختلف:



۸-۱- Steganographyدر تصاویر

وقتی از یک تصویر برای مخفی نمودن یک متن(نوشته)استفاده می شود، معمولاً ازروش LSBاستفاده می شود. ضمناً اگر در درون یک تصویر اطلاعاتی درج شده باشد وسپس این تصویربه فرمت دیگری تبدیل شود، به احتمال بسیار زیاد، بخش اعظمی ازاطلاعات مخفی شده از بین می رود وبخش باقی مانده نیزشاید با سختی فراوان قابل بازیابی باشد.

۸-۲- Steganographyدرصوت

برای این منظور نیز از روشی مشابه روش LSB استفاده می کنند. البته مشکل استفاده از بیت های کم ارزش در یک فایل صوتی، این است که تغییرات در این بیت ها نیز برای گوش انسان قابل تشخیص است. در حقیقت Spread Spectrum روش دیگری برای مخفی نمودن اطلاعات در یک فایل صوتی است. دراین روش، یک نویز به طور تصادفی در سراسر فایل پخش می شود و اطلاعات در کنار این نویزها قرارداده می شوند .Echo data hiding نیز روش دیگری برای مخفی نمودن اطلاعات در یک فایل صوتی است. این روش از اکو)پژواک) در فایل استفاده می کند تا بتواند اطلاعات را مخفی نماید. دراین وضعیت با اضافه کردن صداهای اضافی به بخش های اکو، می توان اطلاعات را در این قسمت ها مخفی نمود.

۸-۳- Steganographyدر ویدئو

برای این کار ، معمولاً از روش DCTاستفاده می شود. این تکنیک شبیه تکنیک LSB است. یک فایل ویدئویی از تعدادی تصاویر پشت سرهم تشکیل شده است که این تصاویر به نام فریم شناخته می شوند. بنابراین کافی است که اطلاعات خود را درهر فریم یک فایل ویدئویی ، به روش LSB مخفی نماییم.

ISSN: 2745-3673
http://www.Rcsj.ir

۴-۸- تشریح تکنیک LSB بر روی یک فایل تصویری

هر فایل تصویری صرفاً یک فایل دودویی است که حاوی رنگ یا شدت نور هر پیکسل برحسب عددی دودویی است.تصاویر معمولاً از فرمت ۸ بیتی یا ۲۴ بیتی استفاده می کنند. در فرمت ۸ بیتی، تنها قادر به استفاده از ۲۵۶ رنگ برای هرپیکسل هستیم (از این ۸ بیت، هر بیت می تواند یکی از مقادیر ۰ یا ۱ را برگزیند که در مجموع ۲ به توان ۸، یعنی ۲۵۶ رنگ مختلف داریم). درفرمت ۲۴ بیتی نیز هرپیکسل از۲ به توان ۲۴ بیت رنگ می تواند استفاده کند. در این فرمت، هرپیکسل از۳ بایت ۸ بیتی استفاده می کند. هر بایت نشان دهنده شدت روشنایی یکی از سه رنگ اصلی آبی، قرمز و سبز است.به عنوان نمونه،رنگ ها در فرمت html بر اساس فرمت ۲۴ بیتی است، که هر رنگ، کدی بر مبنای ۱۶ دارد که از ۶ کاراکتر تشکیل شده است.دو کاراکتر اول، مربوط به رنگ قرمز، دو کاراکتر دوم مربوط به رنگ آبی و دو کاراکتر سوم، مربوط به رنگ سبز است . برای نمونه برای ساختن رنگ نارنجی، باید مقادیر شدت روشنایی رنگ های قرمز، سبز و آبی ، به ترتیب ٪۱۰۰ و٪۵۰ و۰ باشد که در html با #FF7FOO قابل تعریف است(۴).

همچنین اندازه یک تصویر، به تعداد پیکسل ها در تصویر بستگی دارد. برای نمونه، برای تصویری با رزولوشن ۴۸۰× ۶۴۰ که از فرمت ۸ بیتی استفاده می کند، اندازه تصویر باید حدود ۴۸۰*۶۴۰ Byte=307KB*باشد. به عنوان مثالی دیگر، تصویری با رزولوشن ۱۰۲۴*۷۶۸ که ازفرمت ۲۴ بیتی استفاده می کند، اندازه تصویر باید حدود ۳*۷۶۸*۱۰۲۴ Byte=2.36MBباشد. البته این اعداد درصورتی صادق هستند که هیچ فشردگی بر روی فایل اعمال نشده باشد.لازم به ذکراست، فرمت های تصویری GIF و BMP، ۸ بیتی بوده و از روش Lossless(روشی در گرافیک برای فشرده سازی تصاویراست که درآن تمام اطلاعات تصویرحفظ می شود و فقط از تعداد محدودی ازاطلاعات استفاده می شود و در برنامه های خاصی، اطلاعات حفظ شده قابل بازیابی است بنابراین از کیفیت تصویر نیز کاسته نمی شود) استفاده می کنند.

درمقابل، فرمت JPEGازروش (دراین روش بخشی ازاطلاعات تصویر برای همیشه ازبین می رود)استفاده می کند.

درSteganography از فرمت های GIF و BMPبه دلیل ویژگی هایی که دارند، استفاده می شوند.

ساده ترین راه برای پیاده سازی Steganography استفاده ازبیت های کم ارزش هرپیکسل یا همان روش(Least significant bit insertion) است.

برای این منظور اطلاعات را به دو صورت دودویی درآورده و در بیت های کم ارزش پیکسل های تصویر قرار می دهیم . البته ما خواهان این هستیم که تصویر مورد نظر نیز زیاد تغییری نداشته باشد. بنابراین اگر از فرمت ۲۴ بیتی برای این کار استفاده کنیم، چشم انسان قادر به شناسایی این تغییر در تصویر نیست.

سبز آبی قرمز

۱۱۰۰۱۰۰۱ ۰۰۰۰۱۱۰۱ ۱۰۰۱۰۱۰۱ پیکسل ۱

۱۱۰۰۱۰۱۰ ۰۰۰۰۱۱۱۱ ۱۰۰۱۰۱۱۰ پیکسل ۲

۱۱۰۰۱۰۱۱ ۰۰۰۱۰۰۰۰ ۱۰۰۱۱۱۱۱ پیکسل ۳

حال فرض کنید که می خواهیم ۹ بیت اطلاعات ۱۰۱۱۰۱۱۰۱را در این پیکسل ها مخفی نماییم (فرض میشود که این ۹ بیت اطلاعات رمزنگاری شده، یک پیام باشند). حال اگر ازروش LSB استفاده شود و این ۹ بیت در بیت های کم ارزش بایت های این سه پیکسل قرارداده شوند، جدول زیر را خواهیم داشت.

سبز آبی قرمز

۱۱۰۰۱۰۰۱ ۰۰۰۰۱۱۰۰ ۱۰۰۱۰۱۰۱ پیکسل ۱

۱۱۰۰۱۰۱۱ ۰۰۰۰۱۱۱۰ ۱۰۰۱۰۱۱۱ پیکسل ۲

۱۱۰۰۱۰۱۱ ۰۰۰۱۰۰۰۰ ۱۰۰۱۱۱۱۱ پیکسل ۳

ملاحظه می شود که فقط ۴ بیت تغییر داده شده اند و این لطمه زیادی به تصویر وارد نمی کند، به طوری که چشم اصلاً قادر به تشخیص این تغییرات نیست. به عنوان مثال، تغییربیت رنگ آبی از ۱۱۱۱۱۱۱۱ به ۱۱۱۱۱۱۱۰ اصلاًبرای چشم قابل تشخیص نیست. ناگفته نماند تصاویر سیاه وسفید نیز برای Steganography بسیار مناسب هستند.حال شاید خواهان مخفی کردن یک متن در یک تصویر باشیم. در این وضعیت هر کاراکتر، یک بایت(۸ بیت)فضا اشغال می کند. از آنجا که این بیت ها را باید درون پیکسل های تصویری قرار دهیم، می بایست این هشت بیت را به بسته های ۱ بیتی تقسیم نماییم و هر بیت را در بیت های سطح پایین یکی ازسه رنگ اصلی پیکسل ها، قرار دهیم با این شیوه، کلمات تمامی زبان هایی را که با ساختار ASCIIیا UTF-8 سازگارند، می توان درون تصاویر جاسازی نمود(۵).

ISSN: 2745-3673
http://www.Rcsj.ir

۹-پیاده سازی تکنیکLSB

برای این کار معمولاً از فرمت BMF 24 بیتی استفاده می شود. در واقع در این روش معمولاً از دو بیت کم ارزش هر یک از بایت های پیکسل استفاده می شود .این کار به این دلیل است که در یک تصویر، تعداد زیادی کاراکتر را بتوان جا داد همچنین متنی را که قرار است در تصویر مخفی شود، به کد ASCII تبدیل می کنند. سپس هر کاراکتر را به بسته های ۲ بیتی تقسیم می کنند، یعنی هر کاراکتر از ۴ بسته ۲ بیتی تشکیل می شود. سپس این بسته های ۲ بیتی را در دو بیت کم ارزش هر یک از بایت های یک پیکسل، پخش می کنند.

یعنی برای هر کاراکتر، ما احتیاج به ۴ بایت از اطلاعات تصویر داریم، که ۳ بایت آن از یک پیکسل بدست می آید و بایت چهارم هم از پیکسل دیگر گرفته می شود. برای راحتی کار، معمولاً بسته های ۲ بیتی را در اولین پیکسل جا سازی می کنند و به همین ترتیب پیش می روند تا تمام متن در تصویر جاسازی گردد.

۱۰- استخراج اطلاعات پنهان شده

برای استخراج متون مخفی شده در تصویر عملیات زیر را به ترتیب انجام می دهیم:

استخراج بیت های استفاده شده

ادغام بیت ها و تبدیل آنها به بایت

تبدیل بایت ها به کاراکتر

مشاهده کامل متن جا سازی شده

بر پایه مباحث پیشین، همانند مخفی کردن یک متن در یک تصویر، می توان هر نوع فایلی را نیز در یک فایل تصویر یا فایل صدا مخفی کرد. البته به شرطی که تصویر یا صدای مورد نظر، گنجایش لازم برای مخفی کردن فایل را داشته باشد.

۱۱-معایب استگانوگرافی:

استگانوگرافی به اعتقاد بسیاری از نویسندگان و متخصصان علوم کامپیوتر، استگانوگرافی کاربرد های بد و غیرقانونی نیز وجود دارد . بر اساس آمار وب سایت www.techsec.com بیش از ۳۰۰ نوع برنامه استگانوگرافی در اینترنت وجود دارند که به صورت رایگان و بی نام قابل دانلود شدن هستند. بدین ترتیب هر کس که تنها اطلاعات کمی درمورد کامپیوتر داشته باشد می تواند یکی از این برنامه ها را دانلود کرده و از آنها برای فرستادن پیام های مخفی استفاده کند. حال این فرد می تواند یک فرد عضو یک گروه جنایتکار و تبهکار باشد. و یا یکی دیگر ازاستفاده های بد استگانوگرافی را می توان هرزه نگاری برخی افراد و پنهان کردن آنها در داخل عکس های معمولی و قرار دادن آن عکس ها در داخل وب سایت ها برشمرد که در این صورت حتی ما از وجود آنها در بین فایل هایمان نیز بی اطلاع خواهیم بود(۶).

۱۲-Watermarkingچیست؟

با پیشرفت آی تی و استفاده هر چه بیشتر از محصولات چند رسانه ای حفظ حقوق صاحبان این محصولات از اهمیت بیشتری برخوردار شده است. یکی از روش هایی که می توان به وسیله آن حقوق صاحب اثر را حفظ کرد اضافه کردن اطلاعات اثر به صورت مخفی در محصول چند رسانه ای است. دو مساله اساسی در واترمارکینگ سختی)جداناپذیری واترمارک از تصویر) و مشاهده ناپذیری واتر مارک است. یک بده بستان بین سختی و غیر قابل مشاهده بودن وجود دارد بطوری که هر چه سختی روش واتر مارکینگ بیشتر باشد مشاهده پذیری آن بیشتر و بالعکس. چکیده : پنهان‌نگاری هنر و علم جاسازی اطلاعات در یک رسانه حامل است که با توجه به پیشرفت قابل توجه ارتباطات دیجیتال استفاده از آن رو به افزایش می‌باشد. در پنهان‌نگاری هدف اصلی، امنیت به معنای عدم توانایی در اثبات وجود پیغام است در حالیکه در واترمارکینگ با توجه به کاربردهای مختلف، بیشتر مقاومت در مورد تغییرات اهمیت دارد(۷).

هر یک از حوزه‌های پنهان‌نگاری و واترمارکینگ کاربردهای متنوع و خاص خود را دارند. امروزه واترمارکینگ قابل مشاهده و پنهان در شاخه‌های مختلف کاربردی شده و یک نیاز جدی به حساب می‌آید. نرم‌افزار نهان‌ساز با هدف واترمارکینگ و پنهان‌نگاری در تصویر، طراحی و پیاده‌سازی شده است و از الگوریتم‌های متنوع با هدف دستیابی به امنیت، مقاومت و ظرفیت‌های مورد نظر بهره گرفته شده تا کاربردهای مختلفی از واترمارکینگ و پنهان‌نگاری پوشش داده شود .واترمارکینگ (فیزیکی) که در زبان فارسی به چاپ سفید ترجمه شده‌است، طرحی است که علاوه بر طرح زمینه، به صورتی غیر محسوس بر روی اسناد کاغذی چاپ می‌شود و با کمک رنگ روشن‌تر و یا از راه در معرض نور قرار گرفتن قابل رؤیت می‌باشد. واترمارکینگ دیجیتال رابطهٔ نزدیکی با نهان‌نگاری و پنهان‌سازی داده دارد. ولی با این حال، بسته به کاربردهایی که دارد، تفاوت‌هایی نیز مشاهده می‌شود. لذا در عین حال که می‌توان از مفاهیم مشابه در نهان‌نگاری برای ارزیابی الگوریتم‌های واترمارکینگ بهره گرفت، نباید از تفاوت‌هایی که در عمل بین آن‌ها وجود دارد، غافل بود. تعریف واتر مارکینگ : واتر +

ISSN: 2745-3673
http://www.Rcsj.ir

مارکینگ به معنی نشانه گذاری یا نقش بر آب می باشد که از ترکیب دو واژه به معنی نشانه گذاشتن و آب می باشد water . و mark اگر توجه کرده باشید اگر یک چوبی را در دست خود بگیرید و بر روی آب نقشی حک کنید می بینید بعد از مدتی محو می شود ولی این نوشته وجود داشته است.خوب کاربرد آن چیست؟ بیشترین کاربرد واترمارکینگ در حک کردن اسم ها و امضاها بر روی عکس ها می باشد به طوری که مشخص نخواهد بود.این امر باعث می شود تا دیگر عکسی تقلب در آن صورت نگیرد و می توانید ادعا کنید که این عکس برای شماست.کسی این نوشته را نمی بیند و لی شما می توانید با یک الگوریتمی آن را استخراج کنید.خوب این نرم افزار همین کار را بر روی عکس انجام می دهد و نوشته هایی را به صورت هاید بر روی عکس می نویسد.امیدوارم از این برنامه نهایت استفاده را در سکیوریتی عکس ها ببرید. تصویری از واتر مارکینگ هدف از واترمارکینگ چیست ؟ هدف از واتر مارکینگ کردن پنهان نگاری اطلاعات در ساختار دیجیتال است . در پنهان نگاری هدف اصلی، امنیت به معنای عدم توانایی در اثبات وجود پیغام است در حالی که در واترمارکینگ با توجه به کاربردهای مختلف ، بیشتر مقاوت در مورد تغییرات اهمیت دارد(۸).

۱۳- فرق watermarking وfingerprinting

watermarkingو fingerprinting کمی با یکدیگر تفاوت دارند ، وقتی نشانه تجاری یا مشخصه ای در یک اثر مانند عکس ، ویدئو یا صدا به شکل مخفیانه ذخیره می شود به آن watermarkingمی گویند ؛ اما مخفی کردن شماره سریال یا یک مشخصه از یک چیز در چیز مشابه دیگر را fingerprinting می نامند . هر دوی این روش ها برای جلوگیری از دزدی آثار بکار می روند ، از دومی برای پیدا کردن ناقضین copyright و از اولی برای اثبات آن استفاده می شود . اما این دو روش بخشی از مطلب کلی تری به نام Steganographyهستند(۹و۱۰).

۱-۱۳-Steganalysisچیست ؟

درحالی که هدف steganography مخفی کردن اطلاعات و جلوگیری از پیدا شدن و جلب توجه آنهاست ، steganalysis(پنهان شکنی) علمی است که برای پیدا کردن چنین مطالب مخفی شده ای به کار می رود . استگانالایزیز (Steganalysis)می توان گفت استگانالازیز شبیه یک کاراگاه است و استگانوگرافی شبیه یک مجرم .یکی سعی می کند دیگری را بیابد.(البته این بدین مفهوم نیست که استگانوگرافی بد است بلکه این مثال برای درک بهتر مطلب آورده شده است) استگانالازیز سعی می کند تا اطلاعات پنهان شده را پیدا کند اما اغلب متون مخفی که با استفاده از نرم افزارهای استگانوگرافی مخفی شده اند علامت خاصی از خود نشان نمی دهند یعنی مثلا اگر به شما چندین عکس داده شود تا یک متن مخفی را ازدرون آنها پیدا کنید بایستی ابتدا تشخیص دهید که کدام عکس شامل این متن مخفی است چراکه هیچ علامت خاصی وجود ندارد تا شما آن را تشخیص دهید حتی اگر عکس اولیه و اورجینال نیز وجود داشته باشد براحتی قابل تشخیص نیست چراکه نه از لحاظ ظاهری و نه از لحاظ حجم این دو عکس تفاوت چندانی با یکدیگر ندارند. نسل های مختلفی از نرم افزار های استگانوگرافی وجود دارد که استگانالازیز یکی از انواع ان است.به طور کلی روش‌های پنهان نگاری در صورتی امن هستند که تصویر میزبان یا گنجانه دارای نشانه‌های قابل کشف نباشد. به بیان دیگر، خواص آماری تصویر میزبان یا گنجانه باید همانند خواص آماری پوشانه باشد. توانایی کشف پیام در تصویر به طول پیام پنهان بستگی دارد .واضح است که هرچه مقدار اطلاعاتی که در یک تصویر قرار می‌دهیم کمتر باشد امکان کمتری هست که نشانه‌های قابل کشف به وجود آید. انتخاب فرمت تصویر نیز تأثیر زیادی بر سیستم پنهان نگاری دارد. فرمت‌های فشرده نشده‌ای مثلBMP ، فضای زیادی برای پنهان نگاری فراهم می‌کنند ولی استفاده از آنها به دلیل حجم اطلاعات زائد بالای آنها شک برانگیز است.(۱۱)

ISSN: 2745-3673
http://www.Rcsj.ir

نتیجه گیری

باتوجه به اینکه امروزه روش های زیادی برای ارسال امن اطلاعات در بستر فضای مجازی وجود دارد استفاده از روش های استگانوگرافی می تواند کمک شایانی جهت ارسال و دریافت داده ها نمایند به علاوه اینکه این این تکنیک می تواند به گونه ای ارسال شود که فقط افراد فرستنده وگیرنده قابلیت استخراج اطلاعات را داشته باشند .واز طرفی قابلیت تغییر اصل داده به راحتی امکان پذیر نباشد . Steganographyعلمی است که از زمان های دور از مفهوم آن برای انتقال اطلاعات سری استفاده می شد و امروزه نیز در سطح گسترده ای از آن استفاده می کنند . اکثر سرویس های اطلاعاتی روش های مشابهی برای انتقال اطلاعات سری خود بکار می گیرند . در این میان گروه های خراب کار و گروه های تروریستی نیز که معمولاً از امکانات مالی خوبی بر خوردار هستند از این تکنولوژی چشم پوشی نمی کنند ، شاید وقتی شما برنامه را در تلویزیون تماشا می کنید صدای مجری یا حتی عکس پشت سر آن حاوی اطلاعاتی برای گروه خاصی باشد که بعد ها وقتی آن اطلاعات از طبقه بندی خارج شد ما هم مفهوم آنها را بفهمیم . استگانوگرافی هرگز تهدیدی عمومی برای بشر به حساب نمی آید و ما اعتقاد نداریم که ممکن است برای مقاصد شوم مورد استفاده قرار بگیرد. اعتقاد بر این است که استگانوگرافی برای مخفی سازی اطلاعات محرمانه و انتقال آنها از محلی به محل دیگر است.مردم باید بر تاثیرات استگانوگرافی تمرکز کرده و بدانند واقعا برای چه از آن استفاده می کنند.

ISSN: 2745-3673
http://www.Rcsj.ir

منابع و مراجع

[1] Zhang Yong, Niu Xia-mu, Wu Di, Zhao Liang, Li Jun-cao, Xu Wei-jun, 2002. A Method of Verifying Relational Databases Ownership with Image Watermark. Multidiscipline Scientific Research Foundation of Harbin Institute of Technology Project, Project Number: HIT.MD-2002.11.

[2] Langelaar, G.C., Lagendijk, R.L. and Setyawan, I., 2000. Watermarking Digital Image and Video Data, In IEEE Signal Processing Magazine, vol. 17, p. 20-43.

[3] Arnold, M., 2000. Audio Watermarking: Features, applications and Algorithms, In Proceedings of the 5th IEEE International Conference on Computer and Multimedia and Expo, vol.2, p. 1013-1016.

[4] Potdar, V.M., Han, S. and Chang, E., 2005. A Survey of Digital Image Watermarking Techniques, In Proceedings of the IEEE 3rd International Conference on Industrial Informatics, p. 709-716.

[5] Agrawal, R. and Kiernan, J., 2002. Watermarking relational databases, In Proceeding of the 28th International conference on Very Large Databases, p. 155-166.

[6] Raju Halder, Shantanu Pal, Agostino Cortesi, 2010. Watermarking Techniques for Relational Databases: Survey, Classification and Comparison, Journal of Universal Computer Science, vol.16, no.21, p. 3164-3190.

[7] Agrawal, R., Haas, P.J. and Kiernan, J.,2003. Watermarking relational data: framework, algorithms and analysis, VLDB Journal, vol.3.

[8] Zhi-hao Zhang, Xiao-ming Jin, Jian-min wang, De-yi li, 2004. Watermarking relational database using image, In Proceedings of International Conference on Machine Learning and Cybernetics, vol. 3, p. 1739-1744.

[9] Jianhua Sun, Zaihui Cao, Zhongyan Hu, 2008. Multiple Watermarking Relational Databases Using Image, In IEEE International Conference on MultiMedia and Information Technology, p. 373-376.

[10] Chaokun Wang, Jianmin Wang, Ming Zhou, Guisheng Chen, Deyi Li, 2008. Atbam: An Arnold transform based method on watermarking relational data, In Proceedings of the 2008 International Conference on Multimedia and Ubiquitous Engineering, p. 263- 270.

[11] Zhongyan Hu, Zaihui Cao, Jianhua Sun, 2009. An Image Based Algorithm for Watermarking Relational Databases, In Proceedings of the 2009 International Conference on Measuring Technology and Mechatronics Automation, p. 425-428.