دانشگاه جامع علمی کاربردی مخابرات خراسان رضوی

پایان نامه دوره کارشناسی ناپیوسته (ICT)

بررسی روشهای پنهان نگاری اطلاعات در تصاویر

نگارش : مجید سرحدی

استاد راهنما :جناب آقای دکتر محمد عبدالهی

تاریخ دفاعیه : اسفند ماه ۱۳۹۳

فهرست مطالب

با تشکر از خداوند متعال که این فرصت را به بنده داد تا این تحقیق را به پایان برسانم
و با تشکر از آقای دکتر عبدالهی به دلیل راهنمائی های مداوم در انجام این پایان نامه
و با تشکر از همسر و فرزند عزیزم

چکیده پایان نامه

در حال حاضر متن ، تصویر ، صدا و ویدئو را می‌توان به صورت دیجیتال ذخیره‌سازی و اجراء نمود . روشهای ذخیره‌سازی متنوعی برای هر یک از این فرمتها معرفی گردیده است و یا در حال تعریف است، از طرفی رشد سریع اینترنت و استفاده از داده‌های دیجیتال باعث گردیده که ارتباطات نیز از طریق داده‌های دیجیتال روز به روز در حال افزایش باشد. از این‌رو ارسال و ذخیره رسانه‌های الکترونیکی افزایش یافته است؛ چرا که نسخه برداری از داده‌ها بدون هیچ افت کیفیت و با هزینه‌ای بسیار اندک امکان‌پذیر شده است. بدین ترتیب بهره‌گیری از آثار دیجیتال بدون رعایت حق نشر، دست‌کاری اسناد و استفاده از اسناد جعلی ابعاد تازه‌تری یافته است.

اما ارسال و دریافت اطلاعات محرمانه در محیطی عمومی مانند اینترنت باعث پیدایش علومی مانند رمزنگاری و پنهان‌نگاری اطلاعات در داده های دیجیتال گردیده که باعث ایجاد امنیت در اطلاعات در دنیای مجازی گردیده است. پنهان نگاری دیجیتالی عبارت است از توانایی حمل اطلاعات همراه با رسانه مورد نظر جهت پنهان داشتن اطلاعات اصلی. در دنیای دیجیتال امروزه، پنهان نگاری تصویر که در آن یک سیگنال حامل داده به صورت نامرئی و مقاوم در برابر حملات در تصویر تعبیه می شود، به عنوان یک راهکار برای حل مسئله حفاظت از حق تالیف محصولات تصویری ، اهراز هویت و یا انتقال اطلاعات محرمانه معرفی شده است. برای این منظور تاکنون جهت پنهان نگاری، روشهای متعددی به کار گرفته شده است که از آن جمله می توان به استفاده از مدلهای بینایی جهت یافتن میزان بیشینه انرژی پنهان نگاره برای تعبیه در تصویر و استفاده از حوزه‌های مقاوم در برابر حملات، اشاره نمود. در همین راستا در این پایان‌نامه سعی بر این است که با استگانوگرافی (پنهان‌نگاری) و روشهای پیاده سازی آن اشاره گردد.

۱ فصل‌اول

معرفی موضوع تحقیق

۱.۱ مقدمه

پنهان نگاری [۱]

استگانوگرافی در یونانی به معنای پوشیده شده یا نوشتن مخفیانه است. پنهان نگاری خود شاخهای از علم مخفی سازی اطلاعات می‌باشد. مخفی‌سازی اطلاعات خود شامل چندین شاخه از جمله رمزنگاری وته نقش نگاری میباشد. پنهان‌نگاری یعنی مخفی کردن یک پیام به نوعی که هیچ نشانه ای از وجود پیام موجود نباشد. تفاوت این با رمزنگاری [۲] در این است که در رمزنگاری ما فقط می‌خواهیم خود پیام توسط افراد غیرمرتبط قابل خوانده شدن نباشد و اهمیت نمی‌دهیم که آیا آنها می دانند اصلاً پیامی وجود دارد. هدف پنهان نگاری این است که پیغامی را در یک‌پیغام دیگر بی خطر به روشی ذخیره کند که دشمن پی به‌وجود پیغام اولی در پیغام دوم

[1] **Steganography**
[2] **Encryption**

نبرد . به همین دلیل است که در رمزشکنی زمانی حمله را موفق میدانیم که بتوان به تمام یا بخشی از محتوای پیام پی برد ولی در پنهان‌شکنی زمانی حمله کننده موفق به اجرای حمله میشود که بتواند به وجود ارتباط یا پیام مخفی پی برده و یا به صورتی احتمالی آنرا آشکار نماید. در ته نقش نگاری[1]، هدف عموماً حفاظت از یک رسانه در مقابل انتشار غیر مجاز است این کار عمدتاً به صورت درج یک ته نقش معمولاً کوتاه در رسانه صورت میگیرد و بنابراین دشمن زمانی موفق به اجرای حمله میگردد که بتواند ته نقش را از رسانه حذف کند به طریقی که رسانه آسیب جدی نبیند.

۲.۱ اهمیت و ضرورت تحقیق

هنر پنهان نگاری سال ها است که مورد توجه انسان قرار گرفته است. اهمیت آن در این است که خیلی اوقات لو رفتن وجود یک پیام حتی به صورت رمز شده خطرناک است. مثلاً این سناریو را فرض کنید، یک نفر به جرم جاسوسی بازداشت می‌شود و همراه وی کلی مدارک رمز شده پیدا می‌گردد. وجود این اسناد رمز شده نشان دهنده این است که این فرد رابطه ای با جاسوسی دارد و یک آدم معمولی نیست که ضن پلیس را در همان لحظه اول برانگیخته و در پی اصل محتوای پنهان شده در مدارک خواهند گشت و با استفاده از روش های مختلف امکان دارد به اصل موضوع پیام رمز شده نیز دست پیدا کنند.

حالا با تغییر شرایط فرض کنید که این همین فرد به جرم جاسوسی دستگیر شده است و همراه وی فقط یک سری مجله و چند تا سی دی آهنگ پیدا می کنند. اگر پنهان نگاری در اسناد به

[1] watermarking

انـدازه کـافی خـوب باشـد، پلـیس در لحظـه اول ممکـن نیسـت متوجـه وجـود محتـوای مخفـی شـده در مدارک همراه فرد بشود. لذا از این لحاظ ضن افراد کمتر برانگیخته می‌شود.

یکـی از قـدیمی تـرین نشـانه هـای اسـتفاده از پنهـان نگـاری بـه حـدود دو هـزار و پانصـد سـال پـیش بـر مـی‌گـردد. هیسـتیئس[1]، یکـی از حاکمـانی کـه قـدرتش را مـدیون داریـوش کبیـر بـود دسـتور داد موهـای سـر یکـی از مـورد اعتمـاد تـرین کـارگرانش را بتراشـند و پیغـامی روی کـف سـر او بنویسـند. وقتـی دوبـاره موهـا بلنـد شـد پیغـام مخفـی شـده بـود و ایـن فـرد آمـاده بـرای سـفر بـه سـمت گیرنـده پیـام .ایـن پنهـان نگاری نقشه های نظامی ایرانیان را به یونانیان لو داد و باعث شورش شد.

یکـی از کـاربرد هـای اسـتگانوگرافی رد و بـدل کـردن پیغـام در جنـگ هاسـت. نـازی هـا بـرای تبـادل پیامهایشـان از انـواع روشـهای اسـتگانوگرافی اسـتفاده مـی کردنـد. یکـی از ایـن روش هـا ارسـال پیـام های رمزی بود. به طور مثال یک جاسوس نازی پیغام زیر را فرستاد:

[1] Histiaeus

Apparently neutral's protest is thoroughly discounted and ignored. Isman hard hit. Blockade issue affects pretext for embargo on by-products, ejecting suets and vegetable oils.

حال اگر حرف دوم همه کلمات را کنار یکدیگر قرار دهید جمله زیر بدست می آید که منظور پیام اصلی جاسوس نازی بوده است: Pershing sails from NY June I

یک نمونه معروف دیگر استفاده از پنهان نگاری بر می گردد به جنگ جهانی دوم. خانم ولوالی دیسکینسون [1] به جاسوسی علیه آمریکا متهم شد. او در کار خرید و فروش عروسک بود و نامه هایی به آمریکای جنوبی می فرستاد. نامه های او به ظاهر سفارشاتی راجع به تعداد و مدل عروسک های مورد نیاز او بودند اما متنی که در نامه های مخفی شده بود در اصل موقعیت و وضعیت ناوهای نظامی آمریکا بود. این خانم در نهایت با تحقیقات FBI لو رفت.

مارگارت تاچر وزیر بریتانیا که از نشت اطلاعات و اسناد محرمانه توسط کابینه‌اش به بیرون اطلاع پیدا کرده بود و از این موضوع بسیار ناراحت بود با استفاده از ترفندی مشخصات هر وزیر را با استفاده از فاصله انداختن بین کلمات در اسناد تحویلی به هر یک به نحوی ثبت کرد و به این ترتیب وزیر خائن را پیدا کرد.

نمونه های ساده ای از پنهان نگاری را چنانچه متولد دهه ۵۰ تا ۷۰ باشید در نوشتن روی کاغذ با آب لیمو حتماً به یاد خواهید داشت شما این نوشته را درحالت عادی نخواهید دید و متوجه آن نخواهید شد تا زمانی که این کاغذ در نزدیکی حرارت قرار گیرد و نوشته های آن تغییر رنگ داده و مرئی گردد.

ولی در حال حاضر با پیشرفت سریع کامپیوتر ها هنر پنهان نگاری شکل تازه‌ای به خودش گرفته است. با وجود بیش از صدها نرم افزار (طبق آمار منتشر شده از سایت گوگل بیش از سیصد

[1] Velva lee Dickinson

نـرم‌افـزار پنهـان نگـاری و کـاملاً رایگـان بـر روی اینترنـت قـرار دارد) مختلـف بـرای پنهـان نگـاری ایـن کـار خیلی ساده تر و گسترده تر شده است.

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.

مـی‌شـود اطلاعـات مـورد نظـر را در یـک عکـس یـا یـک فایـل صـوتی دیگـر مخفـی کـرد (بـا تغییـر کـم اهمیـت تـرین بیـت، اطلاعـات بـه صـورت نـویز مخفـی مـی شـوند) یعنـی هـر عکسـی کـه شـما در اینترنـت مـی بینیـد، از آواتـار دوسـتان‌تـان در فـیس بـوک گرفتـه تـا هـر عکسـی در هـر سـایتی مـی‌توانـد حـاوی اطلاعات مخفی شده باشد.

بـا ذکـر نمونـه‌ای بهتـر اسـت موضـوع را شـفاف تـر کنـیم کـه بـا چشـم خودتـان نحـوه بـه کـار گیـری پنهـان نگـاری را ببینیـد، عکـس سـمت راسـت، تصـویر گربـه‌ای اسـت کـه در اصـل از تصـویر درخـت سـمت چـپ استخراج شده است.


چند وقت پیش سر و صدای زیادی در این رابطه شده بود که تروریست ها از پنهان نگاری استفاده می‌کنند و پیغام های خودشان را در عکس کالا های مختلف که روی Ebay به فروش گذاشته می‌شود پنهان می کنند. گیرنده هم فقط کافی است در Ebay آن جنس را پیدا کرده و عکس را با نرم افزار مخصوصش بخواند. به چشم بقیه هم هیچ چیز مهمی نیست.

در حال حاظر در اینترنت موتور های جستجو مخصوصی وجود دارند که هر عکسی را که پیدا می‌کنند بررسی و تحلیل برای وجود چنین پیغام هایی در درون آن را انجام می‌دهد.

این اطلاعات می تواند در فایل های صوتی هم پنهان شده باشد. با تغییر بیت های کم ارزش [1] اطلاعات به فایل صوتی اضافه می شود .این تغییرات باعث به وجود آمدن نویز[2] روی فایل می‌شود. اما اگر اطلاعات مخفی شده زیاد نباشد این نویز ابداً قابل تشخیص برای انسان نیست و فقط نرم‌افزارهای فوق العاده پیچیده قادر به پیدا کردن آنها خواهند بود. همچنین این اطلاعات در ویدئو و اسناد نیز قابل جاسازی هستند. پنهان نگاری در ویدئو مانند پنهان نگاری در تصاویر است چون در اصل یک ویدئو تشکیل شده از چندین عکس که با فاصله زمانی مشخص پشت سرهم پخش میشود ولی در اسناد هم پنهان نگاری انجام می‌شود ، در این روش از فاصله های سفید انتهای خطوط و یا حاشیه اسناد که اطلاعاتی ندارد متون یا اطلاعات مخفی را می‌توان جاسازی کرد. که برای این موضوع نیز از الگوریتم های متفاوتی استفاده می‌شود.

می توان اطلاعات را اول توسط الگوریتم های دیگر رمزنگاری کرد و سپس آنها را پنهان نگاری کرد. در این صورت حتی اگر پیغام پیدا شود، قابل خواندن نخواهد بود.

[1] Least Significant Bit
[2] Noise

یکی از روش های دیگر پنهان نگاری که نسبتآ جدید تر و کشف آن پیچیده تر است پنهان‌نگاری‌شبکه است. در این روش پیام با استفاده از مشخصه های ساده پروتوکول های ارتباطی مخفی می شود. مبحث پیچیده ای است که در اینجا فقط یک مختصر اشاره ای به آن میکنیم. می دانید که اطلاعات در اینترنت به بسته‌های کوچک تقسیم شده و ارسال و دریافت می شوند. حالا فرض کنید ما برنامه ای بنویسیم که هنگام ارسال اطلاعات به یک گیرنده خاص از عمد یک مقدار مشخص بین ارسال هر Packet تاخیر ایجاد کند این تاخیر زمانی می تواند به عنوان یک فاکتور برای پنهان نگاری استفاده شود.

یک مثال دیگر استفاده از پروتوکول VoIP است. وقتی شما با دوست تان در اسکایپ صحبت می‌کنید بعضی از بسته های اطلاعاتی که از کامپیوتر شما به کامپیوتر دوست تان ارسال می شود به خاطر تاخیر زیاد یا ناقص بودن از طرف کامپیوتر دوست تان نادیده گرفته می شوند. حالا می توان یک برنامه نوشت که از عمد بسته هایی ناقص یا با تاخیر بفرستد که حاوی اطلاعات خاصی باشند. در آن طرف هم برنامه ای دیگر به جای اینکه آنها را دور بریزد می خواند و پردازش می کند. به این صورت یک پیغام می تواند به صورت مخفیانه جا به جا شودمی‌بین‌ید که روشهای پنهان نگاری بسیار زیاد است و می‌توان از هر چیزی برای پنهان نگاری استفاده کرد حال الگوریتم یا روش پنهان نگاری متفاوتی که نیز در هر روش نیز اسفاده می‌شود را به آن بیافراییم، به نظر میرسد که پی بردن به پیام ارسالی تقریباً غیر ممکن است.

در حقیقت پنهان نگاری پروسه‌ای است که در طی آن یک داده را در دیگر شکل‌های دیگر داده‌ای مثل فایل‌های عکس یا متن مخفی می کنند .معروف ترین و رایج ترین متد مخفی کردن داده در فایلها بکارگیری تصاویرگرافیکی به عنوان مکانهایی مخفی می باشد.

ولی به جزء موارد اشاره شده از اصول و الگوریتم های پنهان نگاری جهت کاهش حجم فایل و اجتناب از ذخیره افزونه فایلها نیز استفاده می‌گردد که رایج ترین آن استفاده در تصاویر ذخیره شده توسط دوربین‌های دیجیتالی است ک معمولاً از تصاویر ذخیره شده توسط آن جهت دید بصری استفاده می‌گردد. به طور کل موضوعاتی که پنهان سازی اطلاعات دربرگیرنده آنها می‌باشد عبارتند از:

۱- موارد مربوط به حق مالکیت تولیدات نرم افزاری و الکترونیکی شامل نقش زمینه و اثر انگشت که جنبه تجاری از این علم هستند.

۲- استفاده از پنهان سازی در ارسال و دریافت پیام به صورت غیر محسوس.

توجه به پنهان سازی اطلاعات از هر دو منظر فوق دارای اهمیت است چرا که با فراهم شدن زمینه های IT درکشور لزوم استفاده از قانون حق تکثیر و حفظ حقوق مربوط به مالکیت محصولات نرم‌افزاری و تولیدات الکترونیکی اعم از موسیقی ،آثارهنری ،کتابهای الکترونیکی و ... شناخت و استفاده از این علم را ایجاب می‌کند.

۳.۱ سوالات تحقیق

سوالاتی که در این تحقیق به آنها پاسخ داده میشود از این قرار است:

۱- تصویر دیجیتال چیست؟
۲- چگونه میتوان در یک تصویر دیجیتال اطلاعات را مخفی کرد؟
۳- روشهای مخفی سازی اطلاعات چیست؟
۴- چگونه می‌توان این اطلاعات مخفی را از دید عموم مخفی نگاه داشت؟
۵- چطور اطلاعات مخفی شده را برگردانیم؟

٤.١ تعریف واژه ها و اصطلاحات فنی و تخصصی

میزبان: در این تحقیق به فایلی که داده در آن پنهان یا تزریق میشود گفته می‌شود.
پیام :فایل ، داده یا اطلاعاتی قرار است توسط میزبان منتقل گردد.
گنجانه : فایلی که در آن اطلاعات مخفی شده است.
کلید : به کد واژه ی که جهت رمز نگاری اطلاعات در مبداء و رمز گشائی در مقصد مورد استفاده قرار می‌گیرد.
تابع جاسازی کننده (Embedder) : قطعه کدی از برنامه که وظیفه پنهان سازی پیام را داخل میزبان بر عهده دارد.
تابع بازسازی کننده (Extractor) : قطعه کدی از برنامه که وظیفه استخراج پیام را از داخل میزبان یا به عبارتی پنهان شکنی را برعهده دارد.

٥.١ فناوری تعریف شده در تحقیق

استگانوگرافی موضوعی است که به ندرت از طریق هواخواهان امنیتی فناوری اطلاعات مورد توجه قرار گرفته است .اغلب مردم از موضوع استگانوگرافی بی خبرند و حتی نمی دانند استگانوگرافی چیست. در این تحقیق بآن هستیم که علم پنهان نگاری اطلاعات را بشناسیم و از آن در ارسال اطلاعات محرمانه و یا ثبت حق مالکیت نرم افزارها و رسانه های دیجیتال به عنوان یک فن‌آوری نوین استفاده کنیم.

٦.١ خلاصه فصل

آنچه در این فصل بیان شد آشنائی با مفهوم پنهان نگاری به عنوان یک علم که از دیرباز مورد استقبال بوده است و همچنین اشاره به برخی از موارد استفاده از استگانوگرافی در گذشته و کاربردهای استفاده از پنهان نگاری در اثبات حق تألیف و ارسال و دریافت پیام مخفی بود.

۲ فصل‌دوم

روشهای پنهان سازی اطلاعات

۱.۲ مقدمه

همان طور که در فصل قبل اشاره شد پنهان سازی اطلاعات قدمت بسیار زیادی دارد و در دنیای دیجیتال در حال حاضر پنهان سازی اطلاعات بر روی عکس ، متن ، صدا و فیلم ویدوئی انجام می‌شود ولی در این تحقیق ما بر روی نحوه پنهان نگاری اطلاعات دیجیتالی بر روی یک تصویر به عنوان میزبان متمرکز میگردیم.