



دانشگاه جامع علمی کاربردی مخابرات خراسان رضوی

پایان نامه دوره کارشناسی ناپيوسته (ICT)

## بررسی روشهای پنهان نگاری اطلاعات در تصاویر

نگارش : مجید سرحدی

استاد راهنما : جناب آقای دکتر محمد عبدالمهدی

تاریخ دفاعیه : اسفند ماه ۱۳۹۳

## فهرست مطالب

۵	چکیده پایان نامه
	۱ فصل اول معرفی موضوع تحقیق
۶	۱.۱ مقدمه
۷	۲.۱ اهمیت و ضرورت تحقیق
۱۳	۳.۱ سوالات تحقیق
۱۴	۴.۱ تعریف واژه ها و اصطلاحات فنی و تخصصی
۱۴	۵.۱ فن آوری تعریف شده در تحقیق
۱۵	۶.۱ خلاصه فصل
	۲ فصل دوم روشهای پنهان سازی اطلاعات
۱۵	۱.۲ مقدمه
۱۶	۲.۲ مختصر اشاره به فن آوری های قبلی
۱۶	۱.۲.۲ تصویر دیجیتال چیست؟

۱۹	۲.۲.۲ بررسی حساسیت چشم انسان
۲۲	۳.۲.۲ روشهای پنهان نگاری اطلاعات
۲۳	۱.۳.۲.۲ روش تزریق
۲۴	۲.۳.۲.۲ روش LSB
۲۴	۳.۲ خلاصه فصل
	۳ فصل سوم روشها و الگوریتم های پیشنهادی
۲۵	۱.۳ مقدمه
۲۶	۲.۳ شرایط احراز میزان
۲۷	۳.۳ بررسی نحوه پنهان نگاری در روشهای موجود
۲۷	۱.۳.۳ پنهان نگاری در فرمت PNG
۲۹	۲.۳.۳ پنهان نگاری در فرمت BMP
۲۹	۳.۳.۳ پنهان نگاری در فرمت JPEG
۳۱	۴.۳ روشهای افزایش امنیت و مقاومت در پنهان نگاری
۳۳	۵.۳ روش پیشنهادی در تحقیق
۳۴	۶.۳ خلاصه فصل
	۴ فصل چهارم نتایج حاصل از تحقیق
۳۵	۱.۴ مقدمه
۳۵	۲.۴ نتیجه های بدست آمده
۳۶	۱.۲.۴ روش متداول
۳۷	۲.۲.۴ روش پیشنهادی
۳۷	۳.۴ پیاده سازی روش پیشنهادی
۳۸	۱.۳.۴ تابع mpg تابع اصلی
۳۸	۲.۳.۴ تابع filesize تابع مشخص کننده اندازه تصویر
۳۸	۳.۳.۴ تابع typepic تابع مشخص کننده نوع تصویر
۳۸	۴.۳.۴ تابع free تابع صفر کننده بتهای کم ارزش
۳۸	۵.۳.۴ تابع CDMOP تابع ساخت ماتریس سطری از تصویر

۳۹	۶.۳.۴ تابع CDMOT تابع ساخت ماتریس سطری از فایل متن
۳۹	۷.۳.۴ تابع Emmbdدر تابع جاسازی کننده
۳۹	۸.۳.۴ تابع HAL تابع شکننده
۳۹	۹.۳.۴ تابع Extractor تابع بازسازی کننده
۴۰	۱۰.۳.۴ تابع join تابع متصل کننده
۴۰	۱۱.۳.۴ تابع ShowError تابع نمایش دهنده پیغام خطا
۴۰	۴.۴ نمونه کار انجام شده
۴۱	۵.۴ خلاصه فصل
۴۲	مراجع
۴۳	پیوست ها
۵۱	چکیده انگلیسی

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 راهنمایی هلی مدوم 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 علومى مانند رمزنگاری و پنهان‌نگاری اطلاعات در داده‌های دیجیتال گردیده که باعث ایجاد امنیت در اطلاعات در دنیای مجازی گردیده است. پنهان‌نگاری دیجیتالی عبارت است از توانایی حمل اطلاعات همراه با رسانه مورد نظر جهت پنهان داشتن اطلاعات اصلی. در دنیای دیجیتال امروزه، پنهان‌نگاری تصویر که در آن یک سیگنال حامل داده به صورت نامرئی و مقاوم در برابر حملات در تصویر تعبیه می‌شود، 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 پنهان‌نگاری، روشهای متعددی به کار گرفته شده است که از آن جمله می‌توان به استفاده از مدل‌های بینایی جهت یافتن میزان بیشینه انرژی پنهان‌نگاره 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 پیاده‌سازی آن اشاره گردد.

# معرفی موضوع تحقیق

## ۱.۱ مقدمه

### پنهان نگاری<sup>۱</sup>

استگانوگرافی در یونانی به معنای پوشیده شده یا نوشتن مخفیانه است. پنهان نگاری خود شاخه‌ای از علم مخفی سازی اطلاعات می‌باشد. مخفی سازی اطلاعات خود شامل چندین شاخه از جمله رمزنگاری و ته نقش نگاری می‌باشد. پنهان نگاری یعنی مخفی کردن یک پیام به نوعی که هیچ نشانه‌ای از وجود پیام موجود نباشد. تفاوت این با رمزنگاری<sup>۲</sup> در این است که در رمزنگاری ما فقط می‌خواهیم خود پیام توسط افراد غیرمرتبط قابل خوانده شدن نباشد و اهمیت نمی‌دهیم که آیا آنها می‌دانند اصلاً پیلمی وجود دارد. هدف پنهان نگاری این است که پیغامی را در یک پیغام دیگر بی خطر به روشی ذخیره کند که دشمن پی به وجود پیغام اولی در پیغام دوم

<sup>۱</sup> Steganography

<sup>۲</sup> 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 ته‌نقش‌نگاری<sup>۱</sup>، هدف عموماً حفاظت از یک رسانه در مقابل انتشار غیر مجاز است این کار عمدتاً به صورت درج یک ته‌نقش معمولاً کوتاه در رسانه صورت می‌گیرد و بنابراین دشمن زمانی موفق به اجرای حمله می‌گردد که بتواند ته‌نقش را از رسانه حذف کند به طریقی که رسانه آسیب جدی نبیند.

## ۲.۱ اهمیت و ضرورت تحقیق

هنر پنهان‌نگاری سال‌ها 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 نشان‌دهنده این است که این فرد رابطه‌ای با جاسوسی دارد و یک آدم معمولی نیست که ضمن پلیس را در همان لحظه اول برانگیخته و در پی اصل محتوای پنهان شده در مدارک خواهند گشت و با استفاده از روش‌های 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 تاسی دی‌آهنگ پیدا می‌کنند. اگر پنهان‌نگاری در اسناد به

---

<sup>1</sup> watermarking

اندازه کافی خوب باشد، پلیس در لحظه اول ممکن نیست متوجه وجود محتوای مخفی شده در مدارک همراه فرد بشود. لذا از این لحاظ ضمن افراد کمتر برانگیخته می‌شود.



یکی از قدیمی ترین نشانه های استفاده از پنهان نگاری به حدود دو هزار و پانصد سال پیش بر می‌گردد. هیستیئس<sup>1</sup>، یکی از حاکمانی که قدرتش را مدیون داریوش کبیر بود دستور داد موهای سر یکی از مورد اعتماد ترین کارگزارانش را بتراشند و پیغامی روی کف سر او بنویسند. وقتی دوباره موها بلند شد پیغام مخفی شده بود و این فرد آماده برای سفر به سمت گیرنده پیام. این پنهان نگاری نقشه های نظامی ایرانیان را به یونانیان لو داد و باعث شورش شد.

یکی از کاربرد های استگانوگرافی رد و بدل کردن پیغام در جنگ هاست. نازی ها برای تبادل پیامهایشان از انواع روشهای استگانوگرافی استفاده می کردند. یکی از این روش ها ارسال پیام های رمزی بود. به طور مثال یک جاسوس نازی پیغام زیر را فرستاد:

<sup>1</sup> 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<sup>1</sup> 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 سفارشات را جمع به تعداد و مدل عروسک های مورد نیاز او بودند اما متنی که در نامه های مخفی شده بود در اصل موقعیت و وضعیت نلوهای نظمی آمریکا بود. این خانم در نهایت با تحقیقات FBI لو رفت.

مارگارت تاچر وزیر بریتانیا که از نشئت اطلاعات و اسناد محرمانه توسط کابینه اش 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 در حالت 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 کامپیوترها هنر پنهان نگاری شکل تازه ای به خودش گرفته است. با وجود بیش از صدها نرم افزار (طبق آمار منتشر شده از سایت گوگل بیش از سیصد

---

<sup>1</sup> Velva lee Dickinson

نرم‌افزار پنهان‌نگاری و کاملاً رایگان بر روی اینترنت قرار دارد) مختلف برای پنهان‌نگاری این کار 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.

می‌شود اطلاعات مورد نظر را در یک عکس یا یک فایل صوتی دیگر مخفی کرد (با تغییر کم اهمیت‌ترین بیت، اطلاعات به صورت نویز مخفی می‌شوند) یعنی هر عکسی که شما در اینترنت می‌بینید، از آواتار دوستان‌تان در فیس‌بوک گرفته تا هر عکسی در هر سایتی می‌تواند حاوی اطلاعات مخفی شده باشد.

با ذکر نمونه‌ای بهتر است موضوع را شفاف‌تر کنیم که با چشم خودتان نحوه به کارگیری پنهان‌نگاری را ببینید، عکس سمت راست، تصویر گربه‌ای است که در اصل از تصویر درخت سمت چپ استخراج شده است.



چند وقت پیش سر و صدای زیادی در این رابطه شده بود که تروریست‌ها از پنهان‌نگاری استفاده می‌کنند و پیغام‌های خودشان را در عکس کلاهای مختلف که روی Ebay به فروش گذاشته می‌شود پنهان می‌کنند. گیرنده هم فقط کافی است در Ebay آن جنس را پیدا کرده و عکس را با نرم افزار مخصوص بخواند. به چشم بقیه هم هیچ چیز مهمی نیست.

در حال حاضر در اینترنت موتورهای جستجو مخصوصی وجود دارند که هر عکسی را که پیدا می‌کنند بررسی و تحلیل برای وجود چنین پیغام‌هایی در درون آن را انجام می‌دهد.

این اطلاعات می‌تواند در فایل‌های صوتی هم پنهان شده باشد. با تغییر بیت‌های کم‌ارزش<sup>1</sup> اطلاعات به فایل صوتی اضافه می‌شود. این تغییرات باعث به وجود آمدن نویز<sup>2</sup> روی فایل می‌شود. اما اگر اطلاعات مخفی شده زیاد نباشد این نویز ابدأ قابل تشخیص برای انسان نیست و فقط نرم‌افزارهای فوق‌العاده پیچیده قادر به پیدا کردن آنها خواهند بود. همچنین این اطلاعات در ویدئو و اسناد نیز قابل جاسازی هستند. پنهان‌نگاری در ویدئو مانند پنهان‌نگاری 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 پنهان‌نگاری انجام می‌شود، در این روش از فاصله‌های سفید انتهایی خطوط و یا حاشیه اسناد که اطلاعاتی ندارد متون یا اطلاعات مخفی را می‌توان جاسازی کرد. که برای این موضوع نیز از الگوریتم‌های متفاوتی استفاده می‌شود.

می‌توان اطلاعات را اول توسط الگوریتم‌های دیگر رمزنگاری کرد و سپس آنها را پنهان‌نگاری کرد. در این صورت حتی اگر پیغام پیدا شود، قابل خواندن نخواهد بود.

---

<sup>1</sup> Least Significant Bit

<sup>2</sup> Noise

یکی از روش های دیگر پنهان نگاری که نسبتاً جدید تر و کشف آن پیچیده تر است پنهان نگاری شبکه 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 بسته های 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 می کنید 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 خلصی 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 شود می بینید که روشهای پنهان نگاری بسیار زیاد است و می توان از هر چیزی برای پنهان نگاری استفاده کرد حال الگوریتم یا روش پنهان نگاری متفاوتی که نیز در هر روش نیز استفاده می شود را به آن بیافزاییم، به نظر میرسد که پی بردن به پیام ارسالی تقریباً غیر ممکن است.

در حقیقت پنهان 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.

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 که 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 در کشور لزوم استفاده از قانون حق تکثیر و حفظ حقوق مربوط به مالکیت محصولات نرم‌افزاری و تولیدات الکترونیکی اعم از موسیقی، آثار هنری، 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؟

## ۴.۱ 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 واژه‌ی که جهت رمزنگاری اطلاعات در مبداء و رمزگشائی 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.

## ۵.۱ 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 بی‌خبرند و حتی نمی‌دانند 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 فناوری نوین استفاده کنیم.

## ۶.۱ 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 فصل دوم

# 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 ویدئویی انجام می شود ولی در این تحقیق ما بر روی نحوه پنهان نگاری اطلاعات دیجیتالی بر روی یک تصویر به عنوان میزبان متمرکز میگردیم.