
بسم الله الرحمن الرحیم

دانشگاه شاهد

دانشکده فنی و مهندسی

پایان‌نامه دوره کارشناسی ارشد مهندسی فناوری اطلاعات– IT

پنهان نگاری و نهان کاوی تصاویر رنگی با استفاده از اطلاعات فضای رنگ

استاد راهنما:

دکتر مریم حسن زاده

نا م دانشجو

سید محمد علی جوادی

تابستان ۱۳۹۱

تقدیم

به پدر و مادر عزیزم

تشکر و قدردانی

اکنون که به فضل پرورگار، نگارش این پایان نامه به پایان رسیده، بر خود لازم می‌دانم از کسانی که گام هایم را در پیمودن این مسیر استوارتر نموده‌اند، قدردانی نمایم. در این راستا، از استاد راهنمای صبور، توانا و گرانقدارم، سرکار خانم دکتر مریم حسن‌زاده، به خاطر راهنمایی‌ها و زحماتشان، تشکر و سپاسگزاری می‌نمایم و کمال سعاتمندی را برایشان از درگاه خداوند متعال، مسألت دارم.

همچنین بر خود لازم می‌دانم مراتب قدردانی خود را از اساتید ارجمند و گرانقدر، جناب آقای دکتر محمد رحمتی و جناب آقای دکتر علیرضا بهراد، به خاطر قبول زحمت داوری این پایان نامه، ابراز دارم.

چکیده

پنهان‌نگاری شاخه‌ای از علم ارتباطات پوشیده است که عبارت از هنر مخفی کردن اطلاعات در اطلاعات دیگر می باشد. در حالی‌که هدف پنهان‌نگاری، مخفی کردن اطلاعات و جلوگیری از پیدا شدن و جلب توجه آنهاست، هدف نهان‌کاوی تشخیص و تخمین اطلاعات مخفی شده با دانش اندک یا بدون هیچ دانشی درباره الگوریتم پنهان نگاری و پارامترهایشان می باشد. از آنجا که تصاویر رنگی، ظرفیت پنهان نگاری بالایی دارند و استفاده از آن‌ها متداول است و از طرف دیگر تحقیقات کمتری در حوزه‌ی مخفی سازی اطلاعات نسبت به تصاویر خاکستری بر روی آن‌ها صورت گرفته است، ما در این پایان نامه، روش‌های مختلف پنهان‌نگاری و نهان‌کاوی تصاویر رنگی را در فضاهای رنگ مختلف (از جمله RGB، YUV، YIQ، YCbCr، HSV)، به طور جامعی مورد بررسی قرار دادیم و روش‌های جدیدی در این دو حوزه ارائه داده‌ایم.

در حوزه‌ی پنهان‌نگاری، یک روش مقاوم برای پنهان سازی اطلاعات در تصاویر رنگی با استفاده از فضاهای رنگ YUV و YCbCr پیشنهاد کرده‌ایم که در این روش تشخیص پیام سخت تر شده و در مقابل نهان‌کاوها دارای مقاومت بیشتری است. در حوزه‌ی نهان‌کاوی نیز، با استفاده از اطلاعات فضای رنگ RGB روش نهان کاوی‌ای پیشنهاد کردیم که در این روش، ویژگی‌هایی مبتنی بر همبستگی کانال‌های رنگ در نواحی همگن تصاویر طبیعی استخراج شده است که درای دقت خوبی در تشخیص جایگزینی LSB و تطبیق LSB است.

علاوه براین؛ با بررسی سایر فضاهای رنگ (از جمله YUV، YIQ، YCbCr، HSV) روش نهان‌کاوی دیگری پیشنهاد کرده‌ایم که مبتنی بر همبستگیِ مکانیِ پیکسل‌های مجاور در مؤلفه های فضاهای رنگ مختلف است و مستقل از نوع روش پنهان‌نگاری طراحی شده است. این فضاهای رنگ از تجزیه‌ی مؤلفه های رنگ و روشنایی بهره برده که در نتیجه باعث حذف همبستگی بین کانال های R، G و B از فضای رنگ RGB می شود. بنابراین اطلاعات مفیدتری برای نهان‌کاوی در مقایسه با استخراج ویژگی از فضای رنگ RGB فراهم می کنند. نتایج حاصل از روش پیشنهادی مبتنی بر همبستگیِ مکانیِ پیکسل‌های مجاور در مؤلفه های فضاهای رنگ مختلف نشان می دهد که این روش دارای قدرت تشخیص خوبی به منظور نهان کاوی تصاویر رنگی دارد.

کلید واژه: پنهان‌نگاری، نهان‌کاوی، فضای رنگ، تصاویر رنگی

فهرست مطالب

عنوان **صفحه**

فهرست جدول‌ها

عنوان **صفحه**

فهرست شکل‌ها

عنوان **صفحه**

مقدمه

به دلیل رشد اینترنت یکی از مهمترین فاکتورهای فناوری اطلاعات و ارتباطات این است که اطلاعات بایستی امنیت[۱] داشته باشند. رمزنگاری[۲] به عنوان یک تکنیکی برای امن کردن ارتباطات مخفی[۳] ایجاد شده و روش‌های مختلفی برای رمزگذاری[۴] و رمزگشایی[۵] به منظور حفاظت از پیام مخفی توسعه داده شده است، متأسفانه گاهی اوقات تنها محافظت از محتوای یک پیام مخفی کافی نیست و ممکن است که نیاز باشد که از وجود پیام مخفی نیز محافظت شود، برای این منظور از پنهان‌نگاری[۶] استفاده می‌کنند[۱].

در رمزنگاری، برای جلوگیری از دسترسی غیر مجاز به محتوای پیام، پیام را طوری تغییر می‌دهند که غیر قابل درک[۷] باشد و فقط برای اشخاص مجاز با استفاده از یک کلید رمز[۸]، اطلاعات به راحتی استخراج می شوند. ولی برای افراد غیر مجاز، دستیابی به اطلاعات رمز شده بدون داشتن کلید و الگوریتم رمزنگاری تقریبا غیرممکن است[۱].

اشکال عمده رمزنگاری این است که اگر شخص ثالثی در حین ارسال اطلاعات پی به وجود اطلاعات محرمانه ببرد، حتی اگر به دلیل رمزنگاری قوی نتواند به این اطلاعات سری دست پیدا کند، می‌تواند از رسیدن پیام به مقصد جلوگیری کند. اگر بتوان اطلاعات را به گونه‌ای فرستاد که شخص ثالث متوجه فرآیند فرستادن اطلاعات سری نشود، این کار باعث افزایش امنیت و محرمانه ماندن پیام خواهد شد. در واقع، پنهان‌نگاری به دنبال تحقق این امر است[۲].

پنهان‌نگاری به علم ارتباطات غیرقابل مشاهده اشاره می‌کند یا به عبارتی دیگر، پنهان‌نگاری اطلاعات هنر مخفی‌کردن اطلاعات در اطلاعات دیگر می‌باشد. برخلاف رمزنگاری، که هدف امنیت اطلاعات است، پنهان‌نگاری به دنبال مخفی‌کردن خود پیام از دید دیگران است[۱].

با وجود استفاده زیاد از عکس‌ها و تصاویر دیجیتال در اینترنت در دنیای امروزی، و به دلیل افزونگی[۹] بالای موجود در این نوع فایل‌ها، تصاویر یکی از بهترین اشیاءِ پوشش برای پنهان نگاری هستند[۱]. تاکنون تحقیقات زیادی در حوزه‌ی پنهان‌نگاری در تصاویر خاکستری[۱۰] انجام شده است که در مقایسه با آن؛ تحقیقات حوزه‌ی تصاویر رنگی[۱۱] بسیار کمتر بوده است.

از آنجا که تصاویر رنگی، ظرفیت پنهان‌نگاری بالایی دارند و متداول هستند، ما در این پایان‌نامه، روش‌های مختلف پنهان‌نگاری و نهان‌کاوی تصاویر رنگی را در فضاهای رنگ[۱۲] مختلف (از جمله RGB، YUV، YIQ، YCbCr، HSV)، به طور جامعی مورد بررسی قرار دادیم. گام اول در پردازش تصاویر رنگی انتخاب فضای رنگ

---

1 - Security
2 - Cryptography
3 - Secrecy of Communication
4 - Encoding
5 - Decoding
6 - Steganography
7 - Imperceptibale
8 - Secret key
9 - Redundancy
10 - Gray Scale Image
11 - Color Image
12 - Color Space

است. از جمله فضاهای رنگ مرتبط با کامپیوتر، فضاهای رنگ RGB، CMY(K)، YUV، YCbCr، YIQ و HSV می‌باشند.

طی مطالعات انجام شده، اکثر روش‌های پنهان‌نگاری اطلاعات، پیام را به طور مستقیم در فضای رنگ RGB تعبیه[۱] می‌کنند که در این زمینه مقالات زیادی با ظرفیت[۲] و مقاومت[۳] مختلف ارائه شده است. در سایر فضاهای رنگ، پنهان‌نگاری به ندرت انجام شده است. در[۳] پنهان‌نگاری در فضای رنگ YUV انجام شده است اما به علت استفاده از تبدیلات فضای رنگ RGB به فضای YUV و برعکس، در هنگام استخراج اطلاعات، پیام تعبیه شده به طور کامل قابل استخراج نیست و به عبارتی BER[۴] دارد. شاید یکی از دلایل اصلی که در سایر فضاهای رنگ؛ پنهان نگاری به ندرت انجام می‌شود به دلیل وجود خطای BER در هنگام استخراج اطلاعات باشد.

هدف اصلی ما در این پایان‌نامه استفاده از اطلاعات فضاهای رنگ مختلف به منظور پنهان‌نگاری و نهان‌کاوی می‌باشد. ایده‌ی اصلی به منظور پنهان‌نگاری این است که تصویر پوشش از فضای رنگ RGB به فضای رنگ مورد نظر تبدیل شود و در یک کانال از آن فضای رنگ با استفاده از الگوریتم LSB[۵] تعبیه انجام شود و پس از تعبیه؛ تصویر مجدد به فضای رنگ RGB تبدیل شود. استفاده از تبدیلات فضای رنگ باعث امنیت بیشتر روش پیشنهادی در مقابل روش‌های نهان‌کاوی می‌شود و همچنین می توان از ضرایب تبدیلات به عنوان کلید رمز استفاده کرد. اما تنها مشکلی که در استفاده از فضاهای رنگ غیر از RGB وجود دارد؛ خطای BER است که ما در این پایان‌نامه، با این که از تبدیلات فضای رنگ استفاده می‌کنیم ولی BER نداریم ، به عبارتی BER را با تغییر در ضرایب کانال‌های دیگر به صفر رساندیم.

در زمینه‌ی نهان‌کاوی؛ اکثر روش‌های نهان‌کاوی‌ای که در فصل سوم مورد بررسی قرار دادیم، ویژگی هایشان را از فضای رنگ RGB استخراج می‌کردند و پردازش های مستقلی به منظور استخراج ویژگی در کانال‌های R، G و B انجام داده و از همبستگی‌ای[۶] که بین کانال‌های رنگ در فضای RGB وجود دارد استفاده نکرده اند؛ این درحالی است که اغلب الگوریتم‌های پنهان‌نگاری‌ای که در فصل سوم مورد بررسی قرار دادیم از همبستگی میان کانال‌های R، G و B برای کاهش تغییرات مقدار رنگ در تصاویر استفاده می‌کنند. معمولاً آن ها پیام را به طور مستقل در سه کانال تعبیه نمی‌کنند، بلکه همزمان (در همه کانال ها) تعبیه می‌کنند، و به ندرت از اطلاعات سایر فضاهای رنگ استفاده شده است.

ما در این پایان نامه دو روش نهان‌کاوی پیشنهاد کردیم که روش نهان‌کاوی اول؛ توسعه ای بر "روش نهان کاوی مبتنی بر همبستگی کانال‌های رنگ و همبستگی پیکسل‌های مجاور[۴] " است که ویژگی‌ها در فضای رنگ RGB استخراج می‌شود. در روش نهان‌کاوی پیشنهادی دوم؛ ویژگی ها را از سایر فضاهای رنگ (از جمله فضاهای رنگ YUV، YIQ، YCbCr، HSV) به‌جای فضای رنگ RGB استخراج می‌کنیم. پایه روش پیشنهادی دوم؛ مبتنی بر همبستگیِ مکانیِ[۷] پیکسل‌های مجاور در مؤلفه‌های فضاهای رنگ مختلف است و مستقل از نوع روش پنهان‌نگاری طراحی شده است. این فضاهای رنگ از تجزیه‌ی مؤلفه‌های رنگ[۸]و روشنایی[۹] بهره برده که در نتیجه باعث حذف همبستگی بین کانال های R، G و B از فضای رنگ RGB می شود. همچنین

---

[1] - Embedding
[2] - Capacity
[3] - Robustness
[4] - Bit Error Rater
[5] - Least Significant Bit
[6] - Correlation
[7] – Spatial Correlation
[8] - Chrominance Component
[9] - Luminance Component

این فضاهای رنگ، اثرات یک روش پنهان‌نگاری را یکپارچه می‌کنند، بنابراین اطلاعات مفیدتری برای نهان‌کاوی در مقایسه با استخراج ویژگی از فضای رنگ RGB فراهم می‌کنند. نتایج حاصل از روش پیشنهادی نشان می‌دهد که این روش دارای قدرت تشخیص خوبی به منظور نهان‌کاوی تصاویر رنگی دارد. ادامه این پایان‌نامه به شرح ذیل می باشد.

در فصل اول این پایان‌نامه مروری بر مفاهیم و تعاریف مرتبط پنهان‌نگاری و نهان‌کاوی و طبقه بندی روش‌های پنهان نگاری و نهان‌کاوی در تصویر داریم. در فصل دوم، ابتدا مروری بر مفاهیم و تعاریف مرتبط با فضاهای رنگ داریم و سپس روش‌های پنهان‌نگاری و نهان‌کاوی تصاویر رنگی مختلف در فضاهای رنگ مختلف را به طور مفصل مورد بررسی قرار دادیم. در فصل سوم روش‌های پیشنهادی به منظور پنهان‌نگاری و نهان‌کاوی در تصاویر رنگی را شرح دادیم. در فصل چهارم نتایج حاصل از پنهان‌نگاری در فضاهای رنگ مختلف و سپس نتایج حاصل از روش پنهان‌نگاری و نهان‌کاوی پیشنهادی را ذکر کردیم. در فصل پنجم نتیجه‌گیری کلی و پیشنهاداتی برای کارهای آینده را خواهیم داشت.

فصل ۱– مفاهیم و تعاریف مرتبط با پنهان نگاری و نهان کاوی

در این فصل در ابتدا تاریخچه‌ای از پنهان‌نگاری و توضیح مختصری در مورد رمزنگاری و آب نشانی[1] داده می‌شود و در ادامه به مدل کلاسیک پنهان نگاری و مفاهیم و تعاریف مرتبط با آن و تفاوت پنهان نگاری با آب نشانی و رمزنگاری پرداخته می‌شود و معیارهای ارزیابی پنهان‌نگاری مورد بررسی قرار داده می شود و در ادامه مروری بر نهان‌کاوی و مفاهیم و تعاریف مرتبط با آن و انواع مختلف آن و همچنین معیارهای ارزیابی نهان کاوی مورد بررسی قرار داده می شود.

۱–۱– تاریخچه

واژه Steganography از واژه "stego" به معنی پوشیده و واژه"graphy" به معنی نویسی است. اولین استفاده‌ی پنهان‌نگاری توسط هردوتس یک مورخ یونانی به ثبت رسیده و ماجرای آن به یونان باستان باز می گردد. وقتی حاکم یونان هیستیائوس[2] به دستِ داریوش در شوش در قرن پنجم پیش از میلاد زندانی شده بود می‌بایست پیغامی مخفیانه به بردار خوانده اش در ملیتوس[3] بفرستد. برای همین‌منظور موی سر غلامش را تراشید و پیغامی را روی سرش خال‌کوبی کرد. وقتی موهای غلام به اندازه کافی رشد کرد او را عازم مقصد کرد[۲].

مورد دیگری از پنهان نگاری که از یونان باستان رسیده مربوط به همین پادشاه است. وسیله‌ی نوشتن در آن زمان لوح‌هایی بوده که روی آن با موم پوشانیده شده بود. یکی از حکام برای اطلاع دادن به وی مبنی بر این که کشورش مورد تاخت و تاز قرار خواهد گرفت و برای این‌که این پیغام پیدا نشود مومِ روی لوح ها را پاک کرد و متن مورد نظر را بر روی لوحِ چوبی حک کرد سپس دوباره موم بر روی آن زد و لوح مانند لوح های استفاده نشده تبدیل شد. سپس بدون این که در بازرسی ها برای متن و لوح مشکلی پیش آید به مقصد رسید[۲].

جوهرهای نامرئی یکی از عمومی‌ترین ابزارها برای پنهان‌نگاری هستند. در روم باستان از جوهرهایی مانند آبلیمو برای نوشتن بین خطوط استفاده می‌کردند. وقتی متن ها را حرارت می‌دادند متن آن تیره و نمایان می‌شد. جوهرهای نامرئی در جنگ جهانی دوم نیز مورد استفاده قرار می‌گرفتند[۲].

یکی از پیشگامان پنهان‌نگاری و رمزنگاری، ژوهان تریثمیوث[4] (۱۴۶۲ تا ۱۵۲۶ آلمانی بود. اولین کار وی بر روی پنهان‌نگاری، استگانوگرافیا[5] نام داشت که درباره سیستم‌های جادو و پیشگویی توضیحاتی داده بود، همچنین در آن کتاب درباره سیستم‌های پیچیده رمزنگاری هم مطالبی یافت می‌شد. این کتاب در زمان وی منتشر نشد، زیرا او از فاش شدن اسرارش می‌ترسید[۲].

اولین کتاب واقعی در این زمینه را گاسپاری اسچوتی[6] در سال ۱۶۶۵ در ۴۰۰ صفحه با نام استگانوگرافیا نوشت. اما اکثر ایده‌هایش مربوط به تریثمیوث بود، او آغازگر این راه بود[۲].

---

[1] - watermarking
[2] – Histiaeus
[3] - Melitoos
[4] - Johannes Trithemius
[5] – Steganographia
[6] - Gaspari Schotti

پنهان‌نگاری در قرن‌های ۱۵ و ۱۶ توسعه یافت، به دلیل این که اکثر نویسندگان این کتاب‌ها از ایجاد تفرقه بین احزاب و فرقه‌ها می‌ترسیدند نام خود را مانند داستان‌ها در میان کتاب مخفی می‌کردند. یکی از رساله‌هایی که در این زمینه نوشته شده توسط ویلکینز[1] بوده است. او روش‌هایی را از کد کردن پیغام ها در موزیک تا جوهرهای نامرئی پیشنهاد داد. همچنین او اولین طرح ها را در رمزگشایی با استفاده از تناوب کلمات ساخت[۲].

در جنگ جهانی دوم توجه زیادی به پنهان‌نگاری شد و تجربیات زیادی در این مورد کسب شد. در اوایل جنگ از جوهرهای نامرئی استفاده می‌شد ولی بعداً از حروف و پیغام‌های معمولی برای مخفی‌کردن پیغام اصلی استفاده کردند. این پیغام‌ها درباره‌ی اتفاقات بسیار ساده و پیش پا افتاده بودند که توجه هیچ کس را جلب نکند، بنابراین بدون این‌که کسی مشکوک شود؛ آن متن‌ها را انتقال می‌دادند. از طرح بندی متن‌ها نیز در مخفی‌کردن اطلاعات استفاده می‌شد. به وسیله‌ی تنظیم کردن مکان خط‌ها و کلمه‌ها؛ متن را آب نشانی و قابل شناسایی می کردند. از وسایلی مانند سوزن نیز برای مشخص کردن لغات مورد نظر نیز استفاده می‌شد[۲].

همان طور که به خاطر پیشرفت تکنولوژی مخفی‌کردن اطلاعات بدون نمایان شدن با حجم زیادی انجام می گرفت علم پیدا کردن متون مخفی نیز در حال پیشرفت بود. از دیگر موارد پنهان‌نگاری اختراع میکرودات[2] بوسیله آلمانی‌ها است، میکرودات‌ها عکس‌های بسیار کوچکی بودند که اطلاعات مختلفی مانند عکس و متن را در خود جای می‌دادند، این عکس‌ها در اندازه یک نقطه بودند بنابراین می توان با آن‌ها یک متن ساده نوشت[۲].

در حقیقت فضای فرستادن متن‌ها به این روش‌ها آنچنان بود که محدودیت‌های زیادی برای ارسال متن و حتی عکس اعمال می‌شد، محدودیت‌هایی که امروز بسیار بی‌معنی می‌باشند. در آمریکا پُست کردن شطرنج، نقشه‌های بافندگی، تکه‌های روزنامه و حتی نقاشی کودکان ممنوع بود. حتی فرستادن گل در انگلستان و آمریکا ممنوع شد[۲].

اما در قرن بیستم بود که حقیقتاً پنهان‌نگاری شکوفا شد. در عصر کامپیوترها پنهان‌نگاری پیشرفت حیرت انگیزی داشت. روش‌های قدیمی مخفی‌کردن با ورود کامپیوترهای پر قدرت؛ نیرو گرفتند[۲].

۱-۲- پنهان نگاری

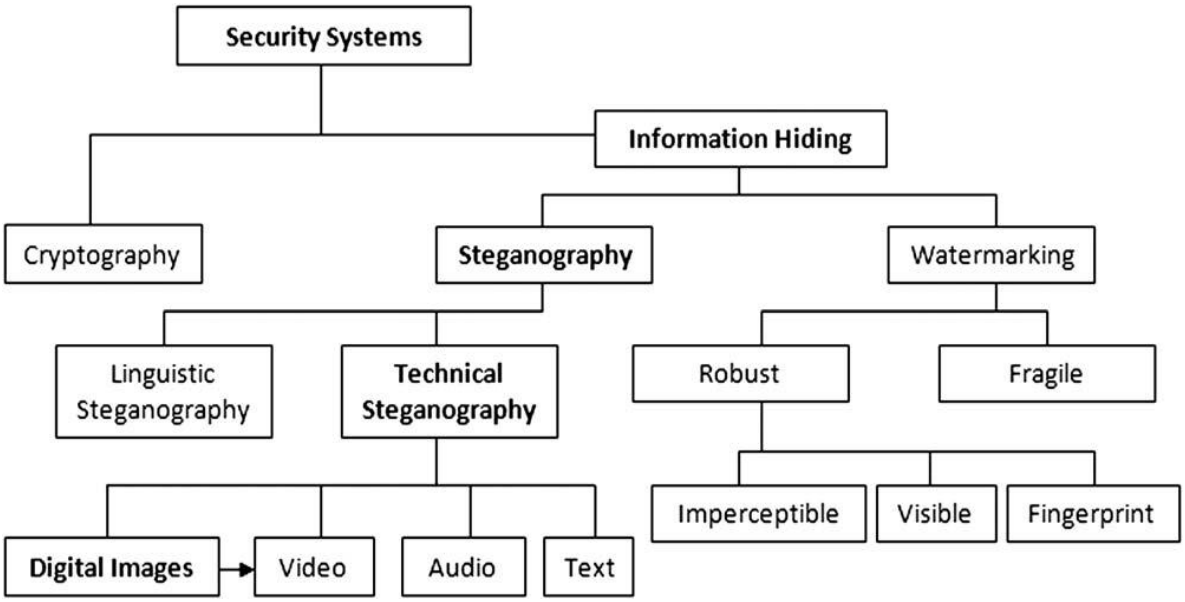
همان‌طور که در شکل ۱-۱ [۵] نشان داده شده‌است، برای امنیت اطلاعات می‌توان از دو روش رمزنگاری[3] و پنهان‌سازی اطلاعات[4] استفاده کرد، که در رمز نگاری بر روی حفاظت از محتوای پیام مخفی تاکید می شود ولی در پنهان‌سازی اطلاعات بر روی حفاظت از وجود پیام مخفی تاکید می‌شود. در ادامه توضیحات تکمیلی آورده شده است.

۱-۲-۱- رمز نگاری

به رمزکردن محتوای یک پیام رمزنگاری گفته می‌شود. رمزنگاری بر روی حفاظت از محتوای یک پیام مخفی تاکید دارد. رمزنگاری دارای دو فرآیند رمزگذاری و رمزگشایی است. فرستنده‌ی پیام ، پیام را با یک کلید رمزگذاری[5] و الگوریتم رمزگذاری، رمزگذاری می‌کند و برای آن‌که رمزگشایی امکان پذیر گردد، فرستنده‌ی پیام

[1] - Bishop John Wilkins
[2] - Microdot
[3] - Cryptography
[4] - Information Hiding
[5] - Encoding key

حتماً بایستی برای گیرنده؛ کلید رمزگشایی[1] را بفرستد. کلید نبایستی در اختیار موجودیت دیگری غیر از گیرنده قرار بگیرد[۵].



شکل ۱-۱: سیستم های امنیتی و پنهان سازی اطلاعات[۵]

۱-۲-۲- پنهان سازی اطلاعات

روش‌های پنهان‌سازی اطلاعات بر روی حفاظت از وجود یک پیام مخفی تاکید دارند و به دو دسته پنهان نگاری و آب نشانی تقسیم می‌شوند[۵].

۱-۲-۲-۱- پنهان نگاری

پنهان‌نگاری به علم ارتباطات غیرقابل مشاهده اشاره می‌کند یا به عبارتی دیگر، پنهان‌نگاری اطلاعات هنر مخفی‌کردن اطلاعات در اطلاعات دیگر می‌باشد. برخلاف رمزنگاری، که هدف امنیت اطلاعات است، پنهان‌نگاری به دنبال مخفی‌کردن خودِ پیام از دید دیگران است. در ادامه توضیحات کامل در مورد پنهان نگاری ارائه می شود.

۱-۲-۲-۲- آب نشانی و کاربرد های آن

آب‌نشانی به معنای پنهان‌کردن داده‌ها در تصاویر است به نحوی که با چشم قابل تشخیص نباشد و فقط افراد مجاز قادر به استخراج این داده‌ها باشند. برخی از کاربردهای آب‌نشانی در زیر ذکر شده است[۶].

۱- حفاظتِ حقِ مالکیت[2]، نظیرِ حفاظت حقِ مالکیتِ محصولات چندرسانه ای، دستاوردهای علمی، کتب الکترونیکی، اقلام نرم افزاری.
۲- ردیابی کاربران مجاز و غیرمجاز در محیط‌های گوناگون[3]، نظیرِ ردیابی کاربران از طریق کنترل شماره سریال‌های آب‌نشان شده محصولات دیجیتالی مختلف.
۳- کنترل و اثباتِ اعتبار[1]، نظیر کنترل اصالت محتوا .

[1] - Decoding key
[2] - Copyright protection
[3] - Tracking / Product Serialization

۴- تحت نظر گرفتن[۲]، نظیرِ کنترل و انتشار برنامه‌های رادیویی و تلویزیون ، کنترل پخش تبلیغات بازرگانی در شبکه‌های مختلف.

۱-۳- مدل کلاسیک پنهان نگاری

شکل جدید پنهان‌نگاری معمولاً به صورت مساله زندانی[۳] مطرح می‌شود، که در آن آلیس[۴] و باب[۵] زندانی هستند و برای طرح نقشه فرار، آلیس می‌خواهد پیامی را برای باب ارسال کند. ارتباط آلیس و باب از طریق ارسال و دریافت نامه‌هایی با محتوای مجاز انجام می‌گیرد، که توسط وندی[۶] زندانبان کنترل می‌شود. بدیهی است چنانچه وندی ارسال پیامی غیرمجاز را تشخیص دهد به سرپرست زندان اطلاع خواهد داد و این موجب قطع ارتباط آلیس و باب خواهد شد. بنابراین آلیس باید پیام خود را در قالب یک پیام عادی همراه با پیام پنهان‌شده در آن، برای باب ارسال کند، به طوری که سوءِ ظن وندی برانگیخته نشود و باب هم قادر به فهم کامل پیام آلیس باشد. برای این منظور، آلیس پیام سری M را در یک شیءِ پوشش[۷] تعبیه[۸] می‌کند و شیءِ گنجانه‌ی[۹] S را به وجود می‌آورد و آن را از طریق یک کانال عمومی برای باب ارسال می‌کند[۷].

تعاریف زیر در حوزه پنهان‌نگاری متداول اند.

- شیءِ پوشش: به شئ ای اشاره دارد که به عنوان حامل برای تعبیه‌ی پیام ها در داخل آن، به کار می رود. شئ های گوناگونی از قبیل صوت، تصویر، ویدئو و حتی صفحات وب را می‌توان برای این منظور مورد استفاده قرار داد.
- شیءِ گنجانه : به شئ ای اشاره دارد که پیام سری در آن تعبیه شده است.
- پیام تعبیه شده[۱۰] : اطلاعاتی که باید به صورت پنهانی منتقل شوند را مشخص می‌کند.
- الگوریتم تعبیه کننده : الگوریتم یا تابعی که پیام را در شیءِ پوشش قرار می‌دهد.
- استخراج[۱۱] پیام تعبیه شده : الگوریتم یا تابعی که پیام سری را از شیءِ گنجانه بازیابی می‌کند.

در پنهان‌نگاری معمولاً سه عامل مورد بررسی قرار می‌گیرد و سعی می‌شود که با توجه به کاربرد و پیش فرض‌ها و دیگر شرایط موجود، هریک از این عوامل در حد مورد نیاز رعایت شوند. این عوامل عبارتند از؛ ظرفیت، نامحسوس بودن و مقاومت[۷].

۱- ظرفیت[۱۲] : ظرفیت مخفی‌سازی، حجم اطلاعاتی است که با توجه به نوع شیءِ پوشش می‌توان تعبیه کرد. هر چه این ظرفیت بالاتر باشد، امکان استفاده از یک شیءِ پوشش کوچکتر را برای یک پیام با حجم ثابت به وجود می‌آورد و بنابراین پهنای باند[۱۳] لازم برای انتقال شئ گنجانه را کاهش می‌دهد. این

---

[1] - Tamper proofing
[2] - Monitoring
[3] - Prisone's problem
[4] - Alice
[5] - Bob
[6] - Wendy
[7] - Cover object
[8] - Embedding
[9] - Stego Object
[10] - Embeded Message
[11] - Extraction
[12] - Capacity
[13] - Bandwidth

عامل، مشخص کننده‌ی ظرفیت پنهان‌سازی روش پیاده‌سازی شده است، به این صورت که همیشه سعی می‌شود در یک الگوریتم پنهان‌نگاری، تا جای ممکن ظرفیت را برای پنهان‌کردن داده‌ها در شیءِ پوشش افزایش داد. البته باید توجه داشت که این افزایش باید به گونه‌ای متعادل انجام گیرد. به طورکلی، روش های مختلف پنهان‌نگاری سعی می‌کنند که ظرفیت پنهان‌نگاری را تا جای ممکن، با حفظ دیگر عوامل افزایش دهند.

۲- نامحسوس بودن[۱]: مشخص‌کننده‌ی توانایی الگوریتم پنهان‌نگاری در پنهان‌کردن داده ها در شیءِ پوشش است، به طوری که باعث جلب توجه نشود. به عبارت دیگر، باید به گونه‌ای عمل پنهان‌سازی انجام گیرد که کیفیت اولیه شیءِ پوشش، تا حد ممکن حفظ شود و این حفظ کیفیت اولیه شیءِ پوشش باعث می شود که داده‌های مخفی شده کمتر مشخص شوند. به همین دلیل نامحسوس بودن و کیفیت تقریباً بیانگر یک مفهوم هستند. البته روش‌های دیگری نیز برای ایجاد امنیت به طور مستقل وجود دارند، مانند رمزنگاری داده‌ها، که به دلیل این که رمزنگاری به صورت مستقل از کیفیت شیءِ پوشش عمل می‌کند، می‌توان آن را صرفا روشی برای امنیت بیشتر در صورت شکست خوردن روش پنهان‌نگاری در نظر گرفت.

به عبارتی نامحسوس بودن بیان می‌کند که محتوای شیءِ پوشش قبل و بعد از تعبیه پیام سری در آن نباید تفاوت محسوسی داشته باشد، زیرا هدف غیر قابل تشخیص‌کردن انتقال پیام محرمانه است و در حقیقت، امنیت یک سیستمِ پنهان‌سازی اطلاعات در همین مسأله‌ی شفافیت نهفته شده است. هر قدر که شباهت شیءِ پوشش، در هر دو حالت اولیه و پس از پنهان‌سازی پیام، با یکدیگر بیشتر باشد، امنیت این سیستم در سطح بالاتری قرار دارد. در ضمن، برای کاربردهایی که به شفافیت ادراکی[۲] بالایی نیاز نیست، می توان با اجازه دادن به کاهش کیفیت بیشتر شیءِ گنجانه، ظرفیت، مقاوم بودن یا هر دو را افزایش داد.

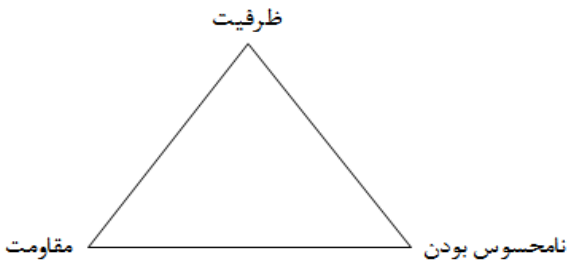
۳- مقاومت[۳] : مقاومت یک سیستم پنهان‌سازی اطلاعات، به معنای این است که پیام پنهان‌شده در مقابل اعمال تغییرات ناخواسته و غیرعمدی که در طول مسیر انتقال به وجود می‌آیند (مانند نویز[۴]) و یا اعمال تغییرات عمدی که توسط حمله کننده‌ی فعال[۵] به منظور تغییر پیام یا از بین بردن آن انجام می‌گیرد، مقاومت لازم را داشته باشد. از جمله حملات معمول می‌توان به فیلتر کردن خطی یا غیرخطی، افزودن نویز، محو یا تیز کردن، تغییر اندازه‌ی[۶] تصویر و فشرده سازی با اتلاف[۷] اشاره کرد. البته مقاومت در مقابل حملات بیشتر برای تکنیک آب‌نشانی تصویرها کاربرد دارد.

به عبارت دیگر، روش‌های پنهان‌نگاری باید تا حد ممکن به گونه ای طراحی و پیاده‌سازی شوند که توانایی ایستادگی و مقاومت را در مقابل روش‌های مختلف نهان‌کاوی[۸]، که به منظور آشکارسازی داده های مخفی شده به کار می‌روند را داشته باشند. برای مثال، هیستوگرام[۹] یا توزیع‌های آماری ، از جمله روش‌های متداول برای نهان‌کاوی هستند.

---

[1] - Imperceptible
[2] - Perceptual Transparency
[3] - Robustness
[4] - Noise
[5] - Active Attacker
[6] - Resize
[7] - Lossy Compression
[8] - Steganalysis
[9] - Histogram

به طورکلی، در طراحی یک سیستم پنهان‌نگاری مناسب، باید سعی شود که با توجه به کاربردها و نیازهای موجود و همچنین تهدید های بالقوه، تعادلی را بین سه عامل یاد شده برقرار کرد. البته باید به این نکته توجه داشت که پارامترهای یاد شده را می‌توان به صورت سه رأس یک مثلث در نظر گرفت که در تقابل با یکدیگر هستند؛ یعنی افزایش هر یک از عوامل، منجر به کاهش عامل دیگر می شود (شکل۱-۲). بنابراین باید سعی کرد تعادل را در بین عوامل نامبرده برقرار کرد.



شکل ۱-۲: مثلث پنهان نگاری و عوامل اصلی[۷].

در روش‌های پنهان‌نگاری مختلف تاکید اصلی بر بررسی دو عامل متقابل ظرفیت و نامحسوس بودن قرار دارد. در روش‌های پنهان‌نگاری‌ای که در فصل دوم بررسی خواهند شد دو عامل ظرفیت پنهان‌سازی داده‌ها و نامحسوس بودن (کیفیت) شیءِ پوشش در روش‌های پنهان‌نگاری مورد بحث خواهند بود. البته هر چه نامحسوس بودن بیشتر باشد باعث خواهد شد تا مقاومت آن روش‌ها در برابر روش‌های نهان کاوی افزایش یابد.

۱-۴- تفاوت پنهان نگاری و آب نشانی

تفاوت اصلی پنهان‌نگاری و آب‌نشانی، در عدم وجود متخاصم فعال است. در کاربردهای آب‌نشانی مانند حفاظت حق مالکیت و تصدیق[۱]، متخاصم فعالی وجود دارد که تلاش می‌کند تا نشانه‌ها[۲] را جعل، نامعتبر یا حذف کند، اما در پنهان‌نگاری داده‌ها چنین متخاصم فعالی وجود ندارد[۷].

یک حمله‌ی[۳] موفق بر روی سیستم پنهان‌نگاری عبارت است از این که ادعا شود که در یک فایل، اطلاعاتی پنهان شده است، در حالی‌که یک حمله‌ی موفق بر روی سیستم آب‌نشانی این است که علامت تشخیص داده شود[۵].

تفاوت دیگر آب‌نشانی و پنهان‌نگاری در آن است که در پنهان‌نگاری تناسب موضوع و محتوا میان پیام و شیءِ پوشش الزامی نیست و به عبارتی محتوای پیام و میزبانِ پیام، می‌تواند کاملاً مستقل از هم باشند، اما در آب‌نشانی محتوای پیام و شیءِ پوشش بایستی مرتبط با هم باشند. به عنوان مثال می‌توان در یک فایل حاوی اطلاعات گذرنامه اشخاص، از مشخصات ظاهری فرد نظیر اثر انگشت، رنگ چشم یا طرح عنبیه بعنوان آب نشان[۴]، ضمیمه به فایل اصلی استفاده کرد. در فایل تولیدات یک مرکز علمی می توان، از اطلاعات کپی رایت آن مرکز، لیست مشتری‌ها ، طرح لوگوی مرکز، تاریخ و نظایر آن به عنوان آب‌نشان استفاده کرد[۶].

---

[1] - Copyright
[2] - Mark
[3] - Attack
[4] -Watermark