دانشگاه صنعتی اصفهان
دانشکده برق و کامپیوتر

پنهان نگاری پرظرفیت وفقی با کاهش تغییرات هیستوگرام

پایان نامه کارشناسی ارشد مهندسی کامپیوتر- معماری کامپیوتر

وجیهه ثابتی

استاد راهنما
دکتر شادرخ سماوی

آبان ۱۳۸٦

تشکر و قدردانی

حمد و سپاس خدایی را که اول است و پیش از او اولی نبوده و آخر است بی آنکه بعد از او آخری باشد. حمد و سپاس خدایی را که بندگانش را با پوشاندن لباس علم و تقوی بر دیگران برتری داد. خدایی که دیده های بینندگان از دیدنش قاصر و اندیشه های وصف کنندگان از وصفش عاجز و ناتوان است.

خداوند سبحان را شکر می گویم که به من توفیق داد تا این دوره را به پایان برسانم. بعد از سپاس از خداوند متعال، از اولین اساتید زندگیم، پدر و مادر عزیزم و تشکر و قدردانی می کنم که در تمام مراحل زندگی پشتیبان و یاور من بوده اند.

از استاد بزرگوارم جناب آقای دکتر شادرخ سماوی تشکر و قدردانی می نمایم که در طول این پایان نامه و دوره کارشناسی ارشد راهنمایی دلسوز برای من بوده اند. همچنین از جناب آقای دکتر محمدعلی منتظری به خاطر انجام مشاوره پایان نامه و جناب آقای دکتر مهدی برنجکوب و جناب آقای دکتر رسول امیر فتاحی به خاطر تقبل امر داوری این پایان نامه سپاسگزارم.

از دوست بسیار عزیزم خانم صدیقه اکرمی و تمام دوستانی که در تمام طول دوره مرا یاری کردند، صمیمانه سپاسگزارم. از آقای مهندس مجتبی مهدوی و اعضای دیگر گروه پنهان‌نگاری دانشگاه صنعتی اصفهان که در طول انجام این پایان نامه به من کمک کرده اند، نیز تشکر و قدردانی می‌کنم.

وجیهه ثابتی

۱۴ آبان ۱۳۸۶

تقدیم به

پدر و مادر عزیز و مهربانم

آنان که را ستی قامتم در شکستگی قامتشان تجلی یافت.

در برابر وجود گرامیشان زانوی ادب بر زمین می نهم و با دلی مملو از عشق و محبت بر دست پر مهرشان بوسه می زنم.

فهرست مطالب

فصل سوم: پنهان شکنی

فصل چهارم: معرفی روش پنهان‌نگاری پر ظرفیت با حداقل سازی تغییرات هیستوگرام تصویر

فصل پنجم: پنهان شکنی روش پنهان‌نگاری برمبنای اختلاف مقادیر پیکسل ها

فصل ششم: نتیجه گیری و پیشنهادات

چکیده

از زمانی که انسان‌ها قادر به ارتباط با یکدیگر شدند، یک خواسته مهم امکان برقراری ارتباط سری بوده است. این خواسته به دلیل اهمیت و ارزش اطلاعات مبادله شده در یک ارتباط است. فراگیری فزاینده و رشد سریع استفاده از اینترنت به عنوان کانال انتقال اطلاعات، امروزه نیاز به امنیت ارتباطات را بیشتر از گذشته مطرح می‌کند. اگر چه استفاده از روش‌های رمزنگاری می‌تواند در برقراری یک ارتباط محرمانه کارامد باشد، اما آشکار بودن وجود ارتباط ایجاد شده با استفاده از این روش‌ها، ممکن است که در بعضی کاربردهای خاص مشکل ساز باشد. در کنار سیستم‌های رمزنگاری نیاز به سیستم‌هایی حس می‌شود که وجود ارتباط را مخفی نگه دارد. هدف روش‌های پنهان نگاری برقراری چنین ارتباطاتی است. پنهان‌نگاری، هنر و علم پنهان کردن ارتباطات است. پنهان-شکنی، روش‌هایی برای کشف وجود یک پیام مخفی در یک ارتباط و در واقع اثبات استفاده از روش‌های پنهان‌نگاری در ارتباط است. در این پایان نامه، روش پنهان‌نگاری جدید تحت عنوان AH-LSB-M پیشنهاد شده است که تکامل یافته روش LSB-M می باشد. روش جدید، ظرفیت جاسازی و امنیت بیشتری نسبت به روش سنتی دارد. استفاده از ایده وفقی و کاهش تغییرات هیستوگرام باعث شده است که روش جدید در برابر حملات مبتنی بر هیستوگرام مقاوم‌تر باشد. بعلاوه، در این پایان نامه حمله‌ای برای دو روش پنهان‌نگاری بر مبنای اختلاف مقادیر پیکسل‌ها (PVD) ارائه شده است.

فصل اول

مقدمه

۱-۱. معرفی

ارتباطات بخش مهمی از زندگی انسان ها را تشکیل می دهد. صوت، تصویر و کلمات محتوای ارتباطات را شامل می شوند. ارسال نامه از طریق پیک، از اولین روش های ارتباط انسان ها بوده است. با گذشت زمان و پیشرفت علم، پست، تلگراف و تلفن روش های پیشرفته تری بودند که انسان ها برای برقراری ارتباط استفاده می کردند و امروزه نیز استفاده از آنها رایج است. اما با رشد تکنولوژی، استفاده از شبکه جهانی اینترنت به عنوان یک راه ارتباطی ساده و سریع گسترش بسیاری در جهان یافته است. فراگیری فزاینده و رشد سریع استفاده از اینترنت انسان‌ها را به سوی جهان دیجیتال و ارتباط از طریق داده‌های دیجیتال سوق داده است. بدین ترتیب میلیون ها پیام در قالب متن، صوت، ویدئو و تصویر دیجیتال در هر لحظه بین نقاط مختلف جهان مبادله می شود.

اما از زمانی که افراد قادر به ارتباط با یکدیگر شدند، یک خواسته مهم امکان برقراری ارتباط پنهانی بوده است. این خواسته به دلیل ارزش اطلاعات مبادله شده در یک ارتباط است. این اطلاعات پنهانی می تواند از اطلاعات برگزاری یک جشن تولد غافلگیر کننده تا اطلاعات فروپاشی یک دولت را شامل شود. استفاده از اینترنت به عنوان کانال انتقال این اطلاعات، نیاز به امنیت ارتباطات را بیشتر مطرح می کند. به صورت کلی، دو روش عمومی برای پنهان کردن تبادل اطلاعات وجود دارد [۱].

در روش اول، ارتباط به گونه ای انجام می شود که برای طرف های مورد نظر، قابل فهم و برای افراد استراق سمع کننده، غیر قابل فهم باشد. برقراری این روش ارتباطی با استفاده از سیستم های رمزنگاری امکان پذیر است. در ارتباط رمز شده، داده مورد مبادله با استفاده از یک کلید به گونه ای تغییر داده می شود که فقط افراد آگاه از کلید قادر به استخراج و فهم داده اصلی باشند. اما عیب عمده این سیستم ها، آشکار بودن وجود یک ارتباط رمز شده و محرمانه بین طرفین ارتباط است. به عبارت دیگر، اگر چه استفاده از روش های رمزنگاری می تواند در برقراری یک ارتباط محرمانه کارامد باشد، ولی آگاهی دشمن از تبادل اطلاعات حتی به صورت رمز شده در بعضی کاربردها می‌تواند عامل بروز مشکلات دیگری گردد. این موضوع به خصوص در ارتباطات سیاسی و نظامی اهمیت پیدا می کند [۲].

بنابراین در کنار سیستم های رمزنگاری، نیاز به سیستم هایی حس می شود که عملاً وجود ارتباط رمز شده را مخفی نگه دارد. در واقع در دسته دوم روش های یک ارتباط امن، ارتباط به صورتی برقرار می شود که هیچ شخص اضافه ای متوجه وجود آن ارتباط نشود و بدین ترتیب حتی دشمن نمی تواند استراق سمع کند. هدف روش های پنهان نگاری، برقراری چنین ارتباط هایی است.

نیاز به برقراری ارتباطات امن، علمی با عنوان مخفی سازی اطلاعات به وجود آورده است که رمز نگاری و پنهان نگاری دو شاخه مختلف از این علم هستند. این علم شاخه های دیگری نیز دارد. به عنوان نمونه، ته نقش نگاری[1] یکی دیگر از روش های مخفی سازی اطلاعات است. روند رو به گسترش تولید و ارائه محصولات فرهنگی مانند فیلم، موسیقی، کتاب و ... و استفاده از شبکه اینترنت جهت تبادل این محصولات، نیاز به داشتن سیستمی امن جهت تبادل این محصولات و جلوگیری از کپی غیر مجاز و شناسایی محصول اصلی از غیر اصلی را بیش از پیش الزامی جلوه می دهد. روش های ته نقش نگاری برای برآورده کردن این اهداف به وجود آمده اند [۳]. اگر چه بخشی از اهداف روش های مختلف مخفی سازی اطلاعات یکسان است، اما تفاوت هایی در اهداف و چگونگی کار آنها وجود دارد. حوزه کاری اصلی در این پایان نامه، روش های پنهان نگاری در تصویر به عنوان روشهایی برای برقراری ارتباط امن است.

لغت استگانوگرافی[2] که ریشه یونانی دارد، به "نوشتار مخفی" اطلاق می شود. در زبان فارسی با عنوان پنهان نگاری از این علم یاد می شود. در واقع، پنهان نگاری هنر و علم پنهان کردن ارتباطات است. یک سیستم پنهان نگاری، اطلاعات محرمانه را به گونه ای ارسال می کند که وجود آن مخفی بماند. روش پنهان نگاری کامپیوتری، روشی از پنهان نگاری است که امنیت اطلاعات را در رسانه دیجیتال فراهم می سازد و هدف آن درج و ارسال پیام محرمانه از طریق رسانه دیجیتال است، بگونه ای که هیچ ظنی مبنی بر ارسال اطلاعات برانگیخته نشود [۴].

---

[1] Watermarking

[2] Steganography

یکی از اجزای اصلی سیستم پنهان نگاری، رسانه دیجیتال یا پوشش انتخاب شده برای مخفی کردن اطلاعات محرمانه است. در سیستم های کنونی رسانه های مختلفی مانند متن، صدا، تصویر، ویدئو، وسایل حافظه، پروتکل های شبکه استفاده می شود و برای هر یک از آن ها کارهای مختلفی انجام شده است. در کارهای انجام شده در این پایان نامه، تصویر به عنوان شئ پوشش استفاده شده است. پنهان نگاری در تصاویر، از محدودیت های بینایی چشم استفاده می کند. به همین دلیل متن، متن کد شده یک تصویر و کلاً هر چیزی که بتوان آن را به بیت تبدیل کرد را می توان در یک تصویر جاسازی کرد. پنهان نگاری در تصویر در سال های اخیر به دلیل بوجود آمدن کامپیوتر های قدرتمند که تصاویر را با سرعت زیاد بررسی می کنند پیشرفت زیادی کرده است. همچنین نرم افزارهایی که این کار را انجام می دهند نیز از اینترنت قابل دریافت هستند.

هدف پنهان نگاری پیشرفته این است که وجود پیام مخفی را غیرقابل کشف نگه دارد، اما سیستم های پنهان نگاری به خاطر طبیعت تهاجمی خود، اثرات قابل کشفی در شئ پوشش باقی می گذارند. تغییر شئ پوشش باعث تغییر ویژگی های آماری آن می شود. به این ترتیب، حتی اگر محتوای مخفی شده قابل خواندن نباشد، اما وجود آن می تواند اثبات شود. استفاده از این تغییرات برای کشف وجود یک پیام مخفی در یک ارتباط و اثبات استفاده از پنهان نگاری در ارتباط، هدف پنهان شکنی[1] است. پنهان شکنی، در واقع روش هایی برای حمله و شکست الگوریتم های پنهان نگاری است [۵].

۱-۲. نوآوری های این پایان نامه

کارهای انجام شده در این پایان نامه را می توان به دو بخش ارائه روشی جدید در پنهان نگاری و ارائه یک روش پنهان شکنی تقسیم بندی کرد. روش جدید پنهان نگاری ارائه شده، روشی بر مبنای روش LSB-M است. روش LSB-M یکی از روش های مبنایی در پنهان نگاری است. در این روش برای جاسازی یک بیت داده متفاوت با LSB پیکسل، مقدار پیکسل به صورت تصادفی کاهش یا افزایش داده می شود. داده جاسازی شده به این روش، از LSB پیکسل قابل استخراج است. اما ظرفیت جاسازی در این روش، تنها یک بیت در هر پیکسل است. بعلاوه تا به حال روش هایی برای حمله به این روش ارائه شده است. تاکنون دو روش [۶] و [۷] برای بهبود دو فاکتور امنیت و ظرفیت در روش LSB-M ارائه شده اند. امنیت در روش وفقی [۷] و ظرفیت در روش افزایش ظرفیت [۶] نسبت به امنیت و ظرفیت روش LSB-M افزایش داده شده است.

روش جدیدی که در این پایان نامه ارائه شده است، هر دو فاکتور امنیت و ظرفیت را در روش LSB-M بهبود داده است. در واقع روش پیشنهادی در این پایان نامه، ترکیبی از دو ایده وفقی و افزایش ظرفیت است. به عبارت دیگر،

---

[1] Steganalysis

روش افزایش ظرفیت [۶] را با استفاده از ایده وفقی [۷] به گونه‌ای اصلاح می‌کنیم که تغییرات هیستوگرام را نسبت به روش پرظرفیت کاهش دهد و از طرف دیگر، ظرفیت جاسازی را نسبت به روش LSB-M وفقی افزایش دهد. بدین ترتیب این ادعا وجود دارد که روش جدید، امنیت و ظرفیت بیشتری نسبت به روش LSB-M دارد. نتایج ارائه شده در پایان نامه، صحت این ادعا را نشان می دهد.

کار دوم انجام شده در این پایان نامه در زمینه پنهان شکنی است. در این کار، حمله ای برای دو روش پنهان نگاری بر مبنای اختلاف مقادیر پیکسل ها[1] (PVD) پیشنهاد شده است. در [۸]، روشی برای جاسازی بر مبنای تفاوت مقدار پیکسل ها ارائه شده است که از آن با عنوان روش PVD ساده نام می بریم. در این روش تصویر به بلاک هایی مجزا از دو پیکسل متوالی تقسیم بندی می شود. جاسازی اطلاعات در مقدار تفاوت پیکسل های درون بلاک انجام می شود. ظرفیت جاسازی هر بلاک به مقدار تفاوت در آن بلاک بستگی دارد. در بلاک های یکنواخت (با مقدار تفاوت کوچک) جاسازی کمتر و در بلاک های لبه (با مقدار تفاوت زیاد) جاسازی بیشتری انجام می شود. بعلاوه در [۹]، روش دیگری بر مبنای روش PVD ارائه شده است که در آن برای جاسازی در بلاک‌های یکنواخت از روش LSB-F و برای جاسازی در بلاک های لبه از روش PVD ساده استفاده می شود.

ارائه دهندگان هر دو روش ادعا می‌کنند که چون جاسازی داده به صورت مستقیم در فضای پیکسلی تصویر انجام نمی‌شود، این روش‌ها در برابر حملاتی که به دنبال تغییرات در فضای پیکسلی تصویر و هیستوگرام حاصل از آن هستند، مقاوم است. اما علی‌رغم ادعای ارائه دهندگان مبنی بر شکست ناپذیری در برابر حملات موجود، در این پایان نامه روشی ارائه شده است که توانسته است هر دو روش بر مبنای PVD را کشف کند.

۱-۳. دستاوردهای پژوهشی

دستاوردهای پژوهشی این پایان نامه را می توان در دو گروه تقسیم بندی کرد:

- مقالات کاملاً مرتبط با پایان نامه

1. Sabeti V., Samavi S., Mahdavi M. and Shirani S., "*Steganalysis of pixel-value differencing steganographic method*", IEEE Pacific Rim Conference on Communications, Computers and Signal Processing, Canada, August 2007.

۲. مهدوی، م. ، سماوی، ش. و ثابتی و. ، "پنهان نگاری پرظرفیت با حداقل سازی تغییرات هیستوگرام "، چهارمین کنفرانس انجمن رمز ایران، مهر ۱۳۸۶

- مقالات در ارتباط با پایان نامه

۱. مهدوی م.، سماوی ش. و ثابتی و.، "ارائه مدل ریاضی روش های پنهان نگاری LSB-F و LSB-M "، چهارمین کنفرانس انجمن رمز ایران، مهر ۱۳۸۶

[1] Pixel_value difference (PVD)

۲. مهدوی م.، سماوی ش. و ثابتی و.، "پنهان نگاری در حوزه تبدیل تصاویر BMP با استفاده از بلاک بندی شبه تصادفی "، چهارمین کنفرانس انجمن رمز ایران، مهر ۱۳۸۶
۳. مهدوی م.، تولا الف.، ثابتی و. و سماوی، ش.، "پنهان شکنی روش پنهان نگاری تطبیقی بر پایه تبدیل موجک"، دوازدهمین کنفرانس برق ایران، اردیبهشت ۱۳۸۶

۱-٤. ساختار ارائه پایان نامه

مطالب ارائه شده در فصول بعدی این پایان نامه به شرح زیر است:

در فصل دوم، ابتدا مفاهیم ابتدایی علم پنهان نگاری مورد بررسی قرار می گیرد. مفاهیم ابتدایی مورد بررسی عبارتند از: اصطلاحات و مدل کلی سیستم های پنهان نگاری، تاریخچه پنهان نگاری، تفاوت پنهان نگاری با دیگر روش های پنهان سازی اطلاعات و فاکتورهای مهم در روش های مختلف پنهان نگاری. با توجه به این که کارهای انجام شده در این پایان نامه در رابطه با پنهان نگاری در تصویر می باشد، در ادامه فصل دوم مقدماتی از تصویر در کامپیوتر بررسی می شود. فرمت فایل JPEG به دلیل اهمیت در روش های پنهان نگاری، در این بخش معرفی می شود. سپس تکنیک های پنهان نگاری در تصویر در دو گروه روش های جاسازی در دامنه مکانی و دامنه تبدیل مورد بررسی قرار می گیرد.

در فصل سوم، تمرکز اصلی بر روی پنهان شکنی است. در این فصل روش های پنهان شکنی بررسی می شود. در ابتدا تکنیک های پنهان شکنی خاص مانند χ^2، RS، حمله مرکز ثقل، حمله بلوکی شدن و حمله برمبنای سازگاری JPEG به صورت جزئی معرفی شده است. هدف این حملات، شکستن روش های پنهان نگاری مشخصی است. اما در قسمت بعدی این فصل، روش هایی بررسی می شود که روش های جامع نامیده می شوند و شکستن روش پنهان نگاری خاصی را هدف نمی گیرند. در این قسمت، دو روش معرفی می شود.

در فصل چهارم، روش پنهان نگاری جدیدی با عنوان روش افزایش ظرفیت با حداقل سازی تغییرات هیستوگرام تصویر ارائه می شود. پس از معرفی اجمالی روش های افزایش ظرفیت و LSB-M وفقی، الگوریتم روش پیشنهادی بررسی می شود. در انتهای فصل نیز نتایج پیاده سازی این روش و تست های انجام شده آورده شده است. نتایج ارائه شده شامل مقایسه هیستوگرام، مرکز جرم تبدیل فوریه هیستوگرام، پارامترهای PSNR و Error و نتایج حمله χ^2 برای چند تصویر تست است.

در فصل پنجم، یک روش پنهان شکنی برای روش پنهان نگاری بر مبنای اختلاف مقادیر پیکسل ها ارائه می شود. در این فصل، ابتدا دو روش PVD ساده و PVD تعمیم یافته به صورت کامل تشریح می شود. سپس رفتار آماری روش

های PVD بررسی می شود و با استفاده از آن روش حمله نهایی ارائه می شود. در انتها نیز نتایج پیاده سازی حمله پیشنهادی برای چند تصویر تست بررسی می شود.

در فصل ششم در یک جمع بندی، ابتدا نتایج حاصله از تحقیقات انجام گرفته در این پایان نامه بررسی می شود و سپس موضوعاتی بیان می شود که می تواند مبنای تحقیقات آینده قرار گیرد.

فصل دوم
پنهان نگاری

۲-۱. مفاهیم پنهان نگاری

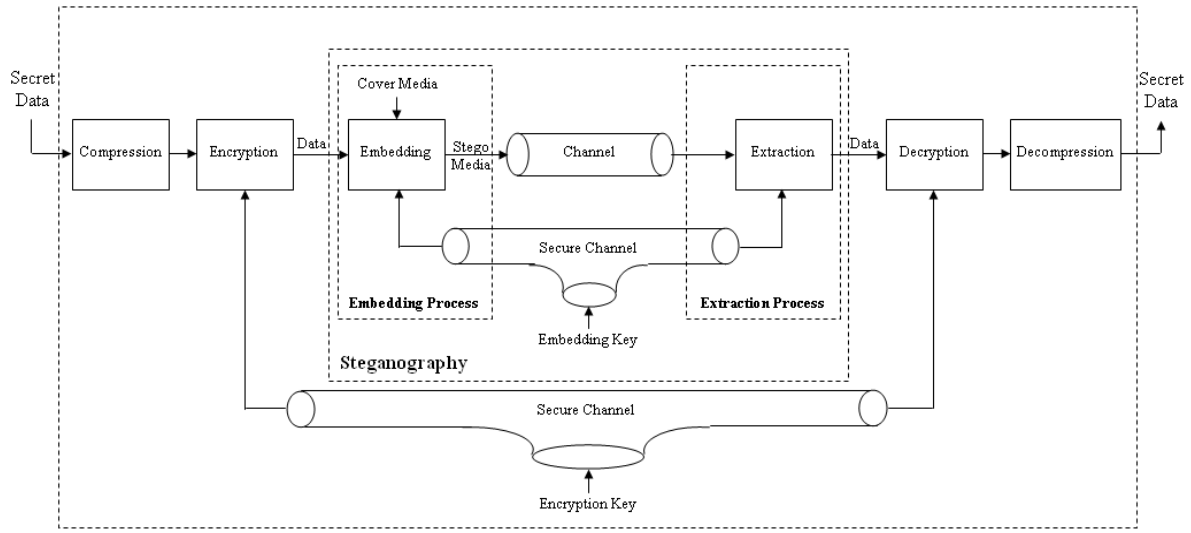
متن، تصویر، صوت و ویدئو را می‌توان به صورت داده‌های دیجیتال بیان کرد. فراگیری فزاینده و رشد سریع استفاده از اینترنت انسان‌ها را به سوی جهان دیجیتال و ارتباط از طریق داده‌های دیجیتال سوق داده است. امنیت ارتباطات یک نیاز مهم است که هر روزه نیاز به آن بیشتر حس می‌شود. علم پنهان‌نگاری یکی از روش‌هایی است که برای برآورده کردن این نیاز پیشنهاد شده‌است.

لغت معادل علم پنهان‌نگاری در زبان انگلیسی، Steganography است که از لغت یونانی ″stegano″ به معنای پوشیده شده و ″graphy″ به معنای نوشته تشکیل شده است. بنابراین پنهان‌نگاری از جنبه لغوی به معنای ″نوشته پوشیده شده″ می‌باشد. هدف پنهان‌نگاری این است که وجود ارتباط برای دشمن (شخص یا سیستمی که قصد شنود دارد) غیر قابل کشف گردد. در واقع، پنهان‌نگاری هنر و علم پنهان کردن ارتباطات است. یک سیستم پنهان‌نگاری، اطلاعات محرمانه را به گونه‌ای ارسال می‌کند که وجود آن مخفی بماند. روش پنهان‌نگاری کامپیوتری، روشی از پنهان‌نگاری است که امنیت اطلاعات را در رسانه دیجیتال فراهم می‌سازد و هدف آن درج و ارسال پیام محرمانه از طریق رسانه دیجیتال است، بگونه‌ای که هیچ ظنی مبنی بر ارسال اطلاعات برانگیخته نشود. پیام محرمانه می‌تواند به صورت یک تصویر یا متن و یا سیگنال و یا هر چیزی باشدکه بتواند به صورت یک رشته بیتی از صفر و یک بیان شود[۴].

علم پنهان‌نگاری از جنبه‌های مختلف قابل بررسی است. اما قبل از بحث تخصصی در این زمینه، نیاز است که بعضی از مفاهیم ابتدایی مورد بررسی قرار گیرد. سیستم‌های پنهان‌نگاری همگی از یک مدل کلی پیروی می‌کنند. در ادامه، این مدل به همراه اصطلاحات معمول در زمینه پنهان‌نگاری معرفی می‌شوند. سپس با توجه به سابقه طولانی پنهان‌نگاری، تاریخچه پنهان‌نگاری در دو دوره کلاسیک و پیشرفته بررسی می‌شود. برای آشنایی بیشتر و درک بهتر ویژگی‌های پنهان‌نگاری، تفاوت‌های مهم آن با دیگر روش‌های پنهان‌سازی اطلاعات در ادامه بررسی می‌شود و سپس ویژگی‌های مهم در روش‌های مختلف پنهان‌نگاری و میزان اهمیت هر کدام از آنها بررسی خواهد شد.

۲-۱-۱. اصطلاحات و مدل کلی

در شکل ۲-۱، شمای کلی یک ارتباط سری با استفاده از پنهان‌نگاری نشان داده شده است [۱۰]. هدف اصلی در این ارتباط تبادل یک پیام سری است. این پیام علیرغم شکل ظاهری خود، شامل متن، تصویر، صوت و ویدئو، می‌تواند به صورت یک رشته بیتی بیان شود. استفاده از دو ماژول فشرده‌سازی[۱] و رمزگذاری[۲] قبل از اعمال روش پنهان‌نگاری الزامی است. فشرده کردن باعث حذف افزونگی‌های موجود در داده و کاهش حجم نهایی و در نتیجه جلوگیری از اتلاف ظرفیت تصویر می‌شود. بعلاوه برای افزایش امنیت ارتباط، یک الگوریتم رمزنگاری برای پنهان کردن مفهوم پیام، روی داده فشرده شده اعمال می‌شود. بدین ترتیب ورودی روش پنهان‌نگاری یک داده فشرده شده و رمز شده است که همانند یک رشته بیت شبه تصادفی است. از این ویژگی در آنالیز روش‌های پنهان‌نگاری و پنهان‌شکنی بسیار استفاده می‌شود.



شکل ۲-۱: شمای کلی یک ارتباط سری با استفاده از پنهان‌نگاری

[1] Compression
[2] Encryption

به طور کلی روش‌های پنهان‌نگاری از دو فرآیند جاسازی[۱] و استخراج[۲] تشکیل شده‌اند. در فرآیند جاسازی، داده فشرده شده و رمزشده با استفاده از یک الگوریتم جاسازی در یک رسانه پوشانه[۳] پنهان می‌شود. در نتیجه این مرحله، رسانه گنجانه[۴] تولید می‌شود که باید برای گیرنده موردنظر ارسال شود. برای افزایش امنیت معمولاً از یک کلید جاسازی در این مرحله استفاده می‌شود. این کلید اغلب برای پراکنده کردن داده در رسانه پوشانه کاربرد دارد. بعلاوه ممکن است از این کلید برای انتخاب تصادفی پارامترهای الگوریتم جاسازی استفاده کرد. به طور خلاصه، فرآیند جاسازی می‌تواند به صورت رابطه زیر نمایش داده شود [۱۱]:

رسانه پوشانه + پیام جاسازی شده + (کلید جاسازی) ⟵ رسانه گنجانه

گیرنده بعد از دریافت رسانه گنجانه، فرآیند استخراج را انجام می‌دهد. در این مرحله گیرنده با استفاده از یک الگوریتم استخراج، داده مخفی شده را از رسانه گنجانه خارج می‌کند. در صورتی که فرستنده در مرحله جاسازی از کلید استفاده کرده باشد، در مرحله استخراج نیز گیرنده به آن نیاز دارد، پس گیرنده باید به روشی امن از این کلید مطلع شود. فرآیند استخراج به صورت خلاصه می‌تواند به صورت رابطه زیر نمایش داده شود:

رسانه گنجانه + (کلید جاسازی) ⟵ پیام مخفی شده

با توجه به استفاده از مراحل فشرده سازی و رمزنگاری قبل از الگوریتم پنهان‌نگاری، گیرنده برای خارج کردن پیام اصلی، باید الگوریتم‌های رمزگشایی[۵] و سپس بازگشایی[۶] را نیز روی پیام استخراج شده اعمال کند [۱۲]. در صورتی که الگوریتم رمز استفاده شده نیز به کلید رمز نیاز داشته باشد، گیرنده و فرستنده باید از طریق یک ارتباط امن، روی مقدار این کلید نیز توافق کنند.

مدل سیستم‌های پنهان‌نگاری موجود اغلب به عنوان "مسئله زندانی" بیان می‌شود، که در آن Alice و Bob دو زندانی هستند که می‌خواهند برای طراحی یک نقشه فرار با هم ارتباط برقرار کنند. اما، همه ارتباطات آن‌ها توسط نگهبان، Wendy، بررسی می‌شود. در صورتی که نگهبان به ارتباط مخفی آن‌ها شک کند، آن‌ها را در سلول انفرادی زندانی خواهد کرد. در مدل کلی پنهان‌نگاری، که در شکل ۲-۲ نشان داده شده است، Alice می‌خواهد یک پیام مخفی m به Bob بفرستد. برای انجام این کار، او m را داخل یک شئ پوشانه جاسازی کرده و یک شئ گنجانه می‌سازد. سپس شئ گنجانه را از طریق یک کانال عمومی می‌فرستد.

به طور معمول فرض می‌شودکه الگوریتم مورد استفاده دو زندانی سری نیست و تنها کلید استفاده شده بوسیله الگوریتم به عنوان رمز بین دو طرف حفظ می‌شود. به عنوان مثال، کلید رمز می تواند یک عدد باشد که به عنوان

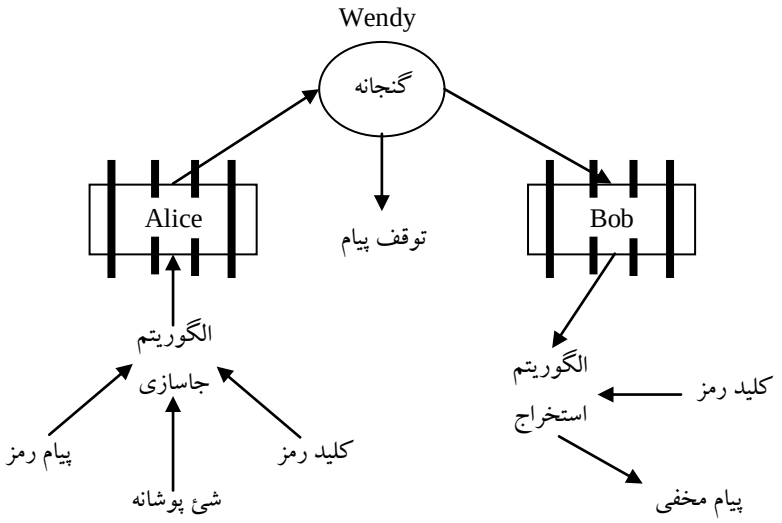
---

[1] Embedding
[2] Extraction
[3] Cover Media
[4] Stego Media
[5] Decryption
[6] Decompression

هسته ابتدایی یک مولد اعداد شبه تصادفی استفاده شود. چنانچه شئ پوشانه تصویر باشد، از دنباله اعداد تولید شده توسط این مولد برای انتخاب مکان پیکسل برای جاگذاری پیام سری در تصویر پوشانه استفاده می‌شود. Wendy با این که از الگوریتم مورد استفاده در جاسازی پیام آگاه است، اما اطلاعی از کلید رمز بین Alice و Bob ندارد.

نگهبان کسی است که برای بررسی همه پیام‌های مبادله شده بین Alice و Bob آزاد است و می‌تواند به حالت فعال یا غیرفعال عمل کند. یک نگهبان غیرفعال، پیام‌ها را بررسی کرده و سعی می‌کند تشخیص دهد که آیا آن شامل یک پیام سری است. در صورتی که وجود پیام سری را تشخیص دهد، می‌تواند پیام را متوقف کند و یا اعمال مناسب دیگری انجام دهد، در غیر این صورت اجازه می‌دهد که پیام بدون انجام هیچ تغییری عبور کند. از طرف دیگر، یک نگهبان فعال می‌تواند حتی در صورتی که اثری از پیام مخفی نبیند، آن پیام را عمداً تغییر دهد تا هر ارتباط پنهانی بین Alice و Bob شکست بخورد. مقدار تغییری که نگهبان اجازه انجام آن را دارد، به مدل و شئ پوشانه مورد استفاده بستگی دارد. برای مثال، برای تصاویر، نگهبان اجازه تغییر تا حدی را دارد که کیفیت تصویر گنجانه مورد انتظار به طور قابل ملاحظه ای تغییر نکند.

Wendy نباید قادر به تفکیک شئ پوشانه و شئ گنجانه باشد. مجموعه روش‌هایی که به Wendy در تشخیص بین شئ پوشانه و شئ گنجانه کمک می‌کند، پنهان شکنی نام دارد. Wendy باید این تشخیص را بدون اطلاع از کلید رمز مشترک و حتی در بعضی مواقع بدون اطلاع از الگوریتم استفاده شده انجام دهد. آنچه در پنهان‌نگاری اهمیت فراوانی دارد، این است که پنهان نمودن نباید مشخصه های اصلی شئ پوشانه را به نحوی تغییر دهد که با بررسی آنها بتوان به وجود اطلاعات در آنها شک کرد. پنهان شکنی ذاتاً یک مسئله سخت است. اینکه تنها تشخیص وجود پیام مخفی کافی است، عاملی است که کار را کمی ساده‌تر می‌کند [۳].



شکل ۲-۲: مدل کلی پنهان نگاری

۲-۱-۲. تاریخچه پنهان‌نگاری

تاریخچه پنهان‌نگاری می‌تواند به دو بخش کلاسیک و پیشرفته تقسیم‌بندی شود [۵]. امنیت سیستم‌های کلاسیک به ناشناخته بودن روش پنهان‌نگاری بستگی دارد. اما در پنهان‌نگاری پیشرفته، گنجانه تنها در صورت شناخته شدن کلید قابل کشف است. در ادامه این دو نوع پنهان‌نگاری بیشتر بررسی می‌شود.

- پنهان‌نگاری کلاسیک

اولین استفاده‌های پنهان‌نگاری توسط هرودوت[1]، مورخ یونانی، به ثبت رسیده و ماجرای آن به یونان باستان باز می‌گردد. وقتی حاکم یونان Histiaeus توسط داریوش در قرن پنجم پیش از میلاد زندانی شده بود، می‌بایست پیغامی مخفیانه به بردار خوانده‌اش در Miletus بفرستد. به همین منظور موی سر غلامش را تراشید و پیغام را روی سرش خال کوبی کرد. وقتی موهای غلام رشد کرد او را عازم مقصد کرد.

داستان دیگری که توسط هرودوت از یونان باستان نقل شده است، مربوط به دمراتوس[2] است. وسیله نوشتن در آن زمان لوح‌هایی بوده است که روی آن با موم پوشانیده شده بود. دمراتوس برای ارسال گزارشی از دربار ایران به Sparta با این مضمون که خشایارشاه قصد حمله به یونان را دارد و برای اینکه این پیغام پیدا نشود، موم روی لوح‌ها را پاک کرد و متنش را بر روی لوح چوبی حک کرد، سپس دوباره موم بر روی آن زد و لوح مانند لوح‌های اولیه شد. سپس بدون اینکه در بازرسی‌ها برای متن و لوح مشکلی پیش آید به مقصد رسید.

جوهرهای نامرئی یکی دیگر از عمومی‌ترین ابزارها برای پنهان‌نگاری در قدیم بوده است. در روم باستان از جوهرهایی مانند آبلیمو برای نوشتن بین خطوط استفاده می‌کردند. وقتی متن‌ها را حرارت می‌دادند پیام آن نمایان می‌شده است. جوهرهای نامرئی توسط جاسوسان در جنگ جهانی اول نیز استفاده شده است.

پنهان‌نگاری در قرن‌های ۱۵ و ۱۶ توسعه یافت. یکی از پیشگامان پنهان‌نگاری و رمزنگاری، Johannes Trithemius یک روحانی آلمانی بود که در سال های ۱۴۶۲ تا ۱۵۲۶ زندگی می‌کرده است. اولین کار وی بر روی پنهان‌نگاری، Steganographia نام داشت که درباره سیستم‌های جادو و پیشگویی توضیحاتی داده بود. بعلاوه در آن کتاب درباره سیستم‌های رمزنگاری هم مطالبی وجود داشت. این کتاب در زمان وی منتشر نشد، زیرا او از فاش شدن اسرارش می‌ترسید. اولین کتاب واقعی در این زمینه را Gaspari Schotti در سال ۱۶۶۵ در ۴۰۰ صفحه با نام Steganographia نوشت، اما اکثر ایده‌هایش مربوط به Trithemius بود.

در جنگ جهانی دوم توجه زیادی به پنهان‌نگاری شد و تجربیات زیادی در این مورد کسب شد. در اوایل جنگ از جوهرهای نامرئی استفاده شد ولی بعداً از حروف و پیغام‌های معمولی برای مخفی کردن پیغام اصلی استفاده کردند.

---

[1] Herodotus

[2] Demeratus

راین پیغام‌ها درباره اتفاقات بسیار ساده و پیش پا افتاده بودند که توجه هیچ کس را جلب نکند، بنابراین بدون اینکه کسی مشکوک بشود آن متن‌ها را انتقال می‌دادند. برای مثال این متن توسط جاسوسان آلمانی در زمان جنگ جهانی دوم فرستاده شده است :

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.

اما با رمز گشایی پیام رسیده، متن زیر از حروف دوم کلمات آن استخراج شد:

Pershing sails from NY June 1.

با پیشرفت در علم عکاسی میکروفیلم‌هایی تولید شد که برای انتقال پیام از طریق کبوترهای حامل استفاده می‌شد. با پیشرفت بیشتر در این زمینه، فیلم و لنزهایی ساخته شد که توانایی کاهش اندازه پیام مخفی به اندازه یک نقطه را داشتند. آلمان‌ها در جنگ جهانی دوم از این تکنیک استفاده کردند که به ریزنقطه[1] معروف است. یکی از مسئولین FBI از این اختراع به عنوان "شاهکار جاسوسی دشمن"[2] تعبیر کرده است. با استفاده از این روش یک عکس از پیام گرفته می‌شود و به یک عکس با قطر ۰,۰۵ اینچ تبدیل می‌شود. این عکس کوچک برای مثال می‌تواند به جای نقطه یکی از 'i' های درون پیام قرار داده شود.

از طرح بندی متن‌ها بوسیله تنظیم کردن مکان خط‌ها و کلمه‌ها نیز برای مخفی کردن اطلاعات استفاده می‌کردند. در حقیقت فضای فرستادن پیام‌ها با استفاده از روش‌های مختلف باعث شد که محدودیت‌های زیادی برای ارسال متن و حتی عکس اعمال شود، محدودیت‌هایی که امروزه بسیار بی‌معنی می‌باشند. طی جنگ جهانی دوم در آمریکا پست شطرنج، نقشه‌های بافندگی، تکه‌های روزنامه و نقاشی کودکان و حتی فرستادن گل در انگلستان و آمریکا ممنوع شد [۲و۱۲و۱۳].

امنیت روش‌هایی که تا به حال معرفی شدند، به ناشناخته ماندن روش تکیه دارد. اگرچه این روش‌ها تا زمان ناشناخته بودن به خوبی کار می‌کنند، اما به محض شناسایی، کشف پیام در آن‌ها ساده است. برای مثال، اگر اولین روش استفاده شده شناخته می‌شد، سربازان باید سر تمام افرادی که عبور می‌کردند را می‌تراشیدند تا پیام پنهان شده را کشف می‌کردند. با آشکار شدن چگونگی کار روش‌ها، سیستم‌های استفاده کننده به راحتی شکست می‌خوردند.

- پنهان‌نگاری پیشرفته

اما در قرن بیستم و با پیشرفت تکنولوژی و ورود کامپیوترها علم پنهان‌نگاری شکوفا شد. روش‌های پنهان‌نگاری دیجیتال جدید ارائه شد و رسانه‌های دیجیتالی مانند صدا، ویدئو و تصاویر به عنوان رسانه پوشانه برای پنهان‌نگاری

---

[1] Microdot

[2] "The enemy's masterpiece of espionage"