پنهان نگاری و تحلیل پنهان نگاری

فهرست

مقدمه

از زمانی که انسانها قادر به ارتباط با یکدیگر شدند امکان برقراری ارتباط مخفیانه یک خواسته مهم افراد بوده است. گسترش روزافزون اینترنت و رشد سریع استفاده از آن، انسانها را به سوی جهان دیجیتال و ارتباط از طریق داده های رقومی سوق داده است. در این میان امنیت ارتباطات یک نیاز مهم است و هر روزه نیاز به آن بیشتر احساس می شود. بهطور کلی دو شیوه ارتباط پنهانی وجود دارد. در روش اول که رمزنگاری است اطلاعات به طریقی رمز میشود که برای شخص ثالث قابل فهم نیست اما فرستنده و گیرنده با استفاده از کلید مشترک میتوانند اطلاعات مورد نظر را رمزگشایی کنند. پنهاننگاری شیوه دوم ارتباط محرمانه است. در پنهاننگاری علاوه بر مخفی ماندن اطلاعات، وجود ارتباط محرمانه باید مخفی بماند. در واقع پنهان نگاری هنر و علم پنهان کردن ارتباطات است و هدف آن، مخفی کردن وجود هرگونه ارتباط بین فرستنده و گیرنده است. اغلب اوقات تصور میشود که با کد کردن پیام مورد مبادله، ارتباط امن است اما در عمل بعضی اوقات تنها رمز کردن کافی نیست و به همین دلیل روش هایی برای پنهان کردن داده به جای کد کردن آن ارائه شده است.

پنهان نگاری از لحاظ لغوی به معنی «نوشته استتارشده» است و در واقع پنهان کردن ارتباط به وسیله قرار دادن پیام در یک رسانه پوششی [1] است به گونه ای که کمترین تغییر قابل کشف را در آن ایجاد نماید و نتوان موجودیت پیام پنهان در رسانه را حتی به صورت احتمالی آشکار ساخت.

---

[1] Cover writing

اگرچه رمزنگاری [1] واحراز هویت [2] نیز مفاهیمی مشابه پنهان نگاری دارند، اما تفاوت‌هایی بین آنها وجود دارد. در رمزنگاری دسترسی به محتوای پیام برای فرد غیر مجاز ناممکن می گردد لیکن در پنهان نگاری موجودیت پیام انکار می‌شود. هدف رمزنگاری حفظ محرمانگی وتمامیت پیام است که با رمز کردن آن حاصل می شود. پنهان نگاری هم همین اهداف را با پنهان نمودن پیام دنبال می کند. بعلاوه در پنهان نگاری انتخاب جا و ترتیب پنهان نمودن پیام نیز با بهره گیری از نوعی رمز در چینش بیت های پیام لابه لای بیت های میزبان صورت می پذیرد. همچنین می توان پیام را قبل از جا سازی داخل میزبان با استفاده از الگوریتم های رمزنگاری به صورت رمز در آورد و سپس عمل پنهان سازی را انجام داد. بطوریکه می توان گفت با استفاده از پنهان نگاری در حقیقت سه لایه حفاظتی بسیار محکم در دسترسی به پیام ایجاد خواهد شد : اول اینکه وجود ارتباط نامحسوس است و این هدف اصلی در پنهان نگاری است و بنابراین گذشتن از اولین مانع کار چندان ساده ای نخواهد بود. در صورتیکه وجود اطلاعات دریک میزبان مورد سوءظن واقع شود مرحله دوم پیدا کردن الگوریتم پنهان نگاری است و باید جا و ترتیب پنهان شدن اطلاعات مشخص شود. لیکن در این مرحله نیز چون از یک کلید بنام stego_key برای جاسازی پیام استفاده شده است دانستن این کلید ضروری است و بنابراین گذشتن از این مرحله نیز با دشواری همراه خواهد بود و چنانچه دو مرحله قبلی با موفقیت پشت سر گذاشته شوند، اکنون به متن رمز شده دسترسی پیدا شده است که در این مرحله مسائل مربوط به رمزنگاری مطرح می گردند.

از طرف دیگر به عمل اضافه کردن نشانه ای در عکس، ویدئو یا صدا برای نشان دادن هویت آن اثر نیز پنهان نگاری یا احراز هویت می گویند. البته پنهان نگاری واحراز هویت کمی با یکدیگر تفاوت دارند، وقتی نشانه تجاری یا مشخصه‌ای در یک

---

[1] Cryptography
[2] Fingerprinting

اثر مانند عکس، ویدئو یا صدا به شکل مخفیانه ذخیره می شود به آن پنهان نگاری می گویند، اما مخفی کردن شماره سریال یا یک مشخصه از یک چیز در چیز مشابه دیگر را احراز هویت می نامند. هر دوی این روش ها برای جلوگیری از دزدی آثار بکار می روند، از دومی برای پیدا کردن ناقضین کپی رایت و از اولی برای اثبات آن استفاده می‌شود.

از سوی دیگر در برابر پنهاننگاری، دانش تحلیل پنهان نگاری [1]، هنر کشف وجود ارتباط پنهان، قرار دارد که هدف آن تمیز دادن بین رسانه های حاوی اطلاعات از رسانه عادی است. همانگونه که پنهان نگاری از اهمیت بسیاری برخوردار است داشتن دانش تحلیل پنهان نگاری نیز بسیار مهم وضروری است چرا که علی رغم امتیازهای مثبتی که پنهان نگاری دارد امکان سوء استفاده از آن برای مقاصد خرابکارانه نیز وجود دارد.

[1] Steganalysis

فصل ۱

سیر تاریخی پنهان نگاری اطلاعات

تاریخچه ارتباطات به صورت مخفیانه، قدمتی برابر با خود ارتباطات دارد. نخستین باری که از اصطلاح نوشتن مخفیانه[۱] استفاده شده است در افسانه ایلیاد هومر می‌باشد.

اما اولین نوشته ها در زمینه روش های انتقال اطلاعات به صورت مخفیانه توسط هردوت[۲] یک مورخ یونانی در قرن ۵ قبل از میلاد به ثبت رسیده است. او در کتاب خود[۳] داستانی از هیستیائوس[۴] حاکم یونان نقل می کند. هنگامی که این پادشاه توسط داریوش، پادشاه ایران در شوش زندانی شده بود می بایست پیغامی مخفیانه به پسرش آرستیوگوراس[۵] در میلتوس[۶] بفرستد. بدین منظور موی سر غلامش را تراشید و پیغامی

---

[1] Secret writing
[2] Herodotus
[3] The histories
[4] Histiaeus
[5] Aristogoras
[6] Miletus

را روی فرق سرش خال کوبی کرد. وقتی موهای غلام به اندازه کافی رشد کرد او را عازم مقصد کرد.

داستان دیگری که از یونان باستان رسیده است مربوط به همین پادشاه است . وسیله نوشتن در آن زمان لوح هایی بوده که روی آن را با موم می پوشاندند. یکی از حکام برای اطلاع دادن به پادشاه، مبنی بر اینکه به زودی کشورش مورد تاخت و تاز قرار خواهد گرفت موم روی لوح را پاک کرد و متنش را بر روی لوح چوبی حک نمود. سپس دوباره آن را با موم پوشاند و بدین ترتیب بدون اینکه در بازرسی ها کسی متوجه پیغام شود، پیغام به مقصد رسید.

جوهرهای نامرئی یکی از عمومی ترین ابزارها برای پنهان نگاری هستند و استفاده از آنها از زمان های بسیار دور در بسیاری از نقاط دنیا مرسوم بوده است. در روم باستان از جوهر هایی مانند آبلیمو ، شیر، اوره و .. برای نوشتن بین خطوط استفاده می کردند. وقتی متن ها را حرارت می دادند متن آن تیره و نمایان می شد. از جوهرهای نامرئی در جنگ جهانی اول و دوم هم استفاده می شد. بعدها با پیشرفت علم شیمی جوهرهای جدیدی ارائه شد که متن نوشته شده با آنها تحت نور فرا بنفش مرئی می شود.

یکی از قدیمی‌ترین محققان در پنهان‌نگاری، یوهانس تریتمیوس [1] آلمانی (۱۵۲۶-۱۴۶۲) بود. کتاب او به نام استگانوگرافیا [2] یک مجموعه سه جلدی است که سیستم‌های جادویی و رمزی را توصیف می کند و شامل یک سیستم پیچیدهٔ رمزنگاری نیز است.

البته شایان ذکر است که استگانوگرافیکا در زمان تریتمیوس منتشر نشد، زیرا او از فاش شدن اسرارش وحشت داشت. این کتاب در سال ۱۶۰۶ منتشر شد و جالب

---

[1] Johannes Trithemius
[2] Steganographia

اینجاست که استفاده از واژه پنهان نگاری(استگانوگرافی [1])، ۱۵۰ سال بعد از انتشار کتاب استگانوگرافیکا رایج شد.

در سال های اخیر ریدز [2] از آزمایشگاه AT&T کدهای رمز شده ای از جلد سوم استگانوگرافیکا استخراج کرده است که نشان می دهد تریتمیوس بیشتر روی رمزنگاری کار میکرده است. روش‌های او بسیار جالب و خواندنی است. به عنوان مثال یکی از روش هایی که او برای پنهان نمودن پیام در متن استفاده می کرده این است که پیام را به صورت الگویی از حروف درکلمات مخفی نموده است و بدین طریق پیام را در عبارات نیایش ملائک جاسازی کرده است.

یک اختراع هوشمندانه دیگر در این کتاب، روش رمزنگاری آوماریا [3]است. که در آن از یک سری جدول استفاده می شود و درجداول مذکور برای هر حرف یک کلمه در نظر گرفته می شود. هنگام کد کردن پیام حرف مربوط به پیام با کلمه متناظر با آن جایگزین می شود و اگر از جدول به درستی استفاده شود آنگاه پیام به صورت یک دعای معمولی مشاهده می‌شود.

اما اولین کتاب واقعی در زمینه پنهان کردن اطلاعات را گسپری اسکاتی [4] در سال ۱۶۶۵ در ۴۰۰ صفحه با نام استگانوگرانیکا [5] نوشت. بیشترمطالب این کتاب از ایده‌های تریتمیوس گرفته شده است.

پنهان نگاری در قرن های ۱۵ و ۱۶ توسعه یافت. بدلیل اینکه اکثر نویسندگان این کتاب ها از ایجاد تفرقه بین احزاب و فرقه ها می ترسیدند نام خود را در کتاب‌هایشان مخفی می کردند.

---

[1] Steganography
[2] Jim Reeds
[3] Ave Maria
[4] Gasperi Sehotti
[5] Steganographica

از دیگر نوشته هایی که در این زمینه وجود دارد رساله ویلکینز[1] است. اودر رساله خود روش هایی را برای جاسازی پیام در رسانه های مختلف مثل موزیک ومتن را شرح داده است . همچنین اولین ایده ها مربوط به رمز گشایی با استفاده از تناوب کلمات توسط او پیشنهاد شده است .

در اوایل قرن ۲۰در زمان جنگ بور[2]، رابرت پاول [3] برای ثبت مکان توپخانه دشمن به جای اینکه نقشه را به روش معمولی بکشد آن را به شکل یک پروانه می کشید تا اگر دستگیر شد کسی چیزی از آن نفهمد.

در جنگ جهانی دوم توجه زیادی به پنهان نگاری شد و تجربیات زیادی در این مورد کسب شد. در اوایل جنگ از جوهر های نامرئی استفاده می شد، ولی بعد ها از حروف و پیغام های معمولی برای مخفی کردن پیغام اصلی استفاده کردند. این پیغام ها درباره اتفاقات بسیار ساده و پیش پا افتاده بودند که توجه هیچ کس را جلب ن می کرد، بنابراین بدون اینکه کسی مشکوک بشود آن ها را انتقال می دادند. برای مثال متن زیر 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 بعد از رمز گشایی این متن با کلید صحیح ، پیغام زیر از کلمات آن استخراج شد :

Pershing sails from NY June 1.

---

[1] Bishop John Wilkins
[2] Boer
[3] Robert Baden-Powell

از طرح بندی متن ها نیز در مخفی کردن اطلاعات استفاده می شد. بوسیله تنظیم کردن مکان خط ها و کلمه ها متن را نشانه گذاری و قابل شناسایی می کردند. از وسایلی مانند سوزن نیز برای مشخص کردن لغات مورد نظر استفاده می شد.

با پیشرفت فناوری، امکان مخفی کردن اطلاعات با حجم زیاد افزایش یافت. آلمانی ها میکرودات ها[1] را که عکس های بسیار کوچکی در اندازه یک نقطه بودند و اطلاعات مختلفی مانند عکس و متن را در خود جای می دادند، اختراع کردند.

اندازه بسیار کوچک این عکس ها امکان نوشتن یک متن ساده با آن ها را فراهم می کند و اینگونه بر روی خطوط یک کلمه می توان اطلاعات زیادی را جاسازی کرد.

در آن زمان بازار فرستادن متن ها به این روش ها آنچنان گرم شده بود که محدودیت های زیادی برای ارسال متن و حتی عکس اعمال می شد. محدودیت هایی که امروز بسیار بی معنی می باشند. در آمریکا پست شطرنج، نقشه های بافندگی، تکه های روزنامه و حتی نقاشی کودکان ممنوع بود. حتی فرستادن گل در انگلستان و آمریکا ممنوع شد.

اما در قرن بیستم بود که حقیقتا پنهان نگاری شکوفا شد. در زمان کامپیوترها پنهان نگاری پیشرفت حیرت انگیزی داشت. روش های قدیمی مخفی کردن در عکس با ورود کامپیوتر های پر قدرت نیرو گرفتند. و روز به روز بر تعداد مقالات و محققینی که در این زمینه فعالیت میکردند افزوده شد.

---

[1] Microdot

در سال های اخیر، با توجه به پیشرفت قابل توجه ارتباطات دیجیتال نظیر اینترنت نگاه دوباره‌ای به پنهان‌نگاری در رسانه‌های دیجیتال شده است. این شاخه از علم، کاربردهای متعددی نظیر حق رونوشت، امنیت تجارت الکترونیکی، سرویس‌های بلادرنگ، ارتباطات پنهانی، محفوظ نگه‌داشتن اطلاعات خاص نظیر اطلاعات بیمار در تصاویر پزشکی و ... پیدا کرده است.

فصل ۲

روش‌های پنهان نگاری اطلاعات

به طور کلی روش‌های پنهان نگاری در سه دسته زیر قرار می گیرند :

- پنهان نگاری صنعتی[۱]

در این نوع از پنهان نگاری، از علوم مهندسی، فیزیک و... برای پنهان کردن اطلاعات بهره می‌برند. مثال‌هایی از این نوع پنهان نگاری همان استفاده از جوهرهای نامرئی و یا میکرودات‌ها هستند.

- پنهان نگاری زبانی[۲]

در این شیوه، برای پنهان کردن اطلاعات، از طریق نوشتن استفاده می کنند که خود به دو دسته Semagrams و Open code تقسیم می‌شود. در Semagrams برای پنهان کردن پیام از علائم بصری و سمبل‌ها استفاده

[1] Technical steganography
[2] Linguistic steganography

می‌شود. مثلا سایز حرف خاصی را تغییر می‌دهند. در حالیکه در Open code الگویی را به طریقی در متن جاسازی می کنند که توسط اکثر خوانندگان قابل کشف نیست.

- پنهان نگاری رقومی[1]

پنهان نگاری رقومی در واقع علم جاسازی اطلاعات در یک رسانه دیجیتال مثل فایل صدا، تصویر، متن و ... است.

امروزه با توجه به رشد وسیع ارتباطات دیجیتال و سهولت در رد و بدل کردن اطلاعات از طریق شبکه های رایانه ای، نظیر اینترنت، پنهان نگاری رقومی کاربرد مناسبی پیدا کرده است و استفاده از آن روز به روز بیشتر می‌شود.

پنهان نگاری در رسانه های مختلف

در یک سیستم پنهاننگاری رقومی "رسانه پوششی" هر نوع فایل دیجیتالی از قبیل تصویر، صوت، فیلم و ... می تواند باشد. «رسانه استگو[2]»، خروجی فرآیند پنهان نگاری است که پیام ارسالی را در بردارد. اما از نظر ظاهری مشابه رسانه پوششی است. در ادامه در مورد پنهان نگاری در سه رسانه پر استفاده یعنی متن، صدا و تصویر توضیحاتی ارائه می گردد.

---

[1] Digital Steganography
[2] Stego

- پنهان نگاری در متن

یکی از مشکلاتی که برای نویسندگان وجود دارد توزیع غیر قانونی نوشته ها بوسیله ابزار های پیشرفته مانند پست الکترونیکی است. بدین معنی که بدون پرداخت هزینه به نویسنده، نوشته وی را به دیگران می دهند. لذا برای مقابله با آن روش‌هایی ابداع شد. مانند ساختن کلمه‌ای که از نظر خواننده دیده نمی‌شود ولی مشخصه آن متن است. یا کد کردن متن یا تغییر آن به روشی که قابل کپی برداری با دستگاه‌های فتوکپی نباشد. روش دیگر استفاده از کلمات حاشیه‌ای است که مخفی می‌باشد ولی کارگزارهای پست الکترونیکی[1] را می توان نسبت به آن حساس کرد تا از پخش آن جلوگیری کنند.

- پنهان نگاری در صوت

از آنجا که محدوده سیستم شنوایی انسان محدود است امکان جاسازی اطلاعات در صدا نیز وجود دارد. سیستم شنوایی انسان می تواند قدرتی بین یک تا یک میلیون و فرکانسی بیشتر از یک تا یک هزار را درک کند. همچنین نسبت به پارازیت‌هایی که اضافه می‌شود بسیار حساس است. هرگونه مزاحمتی در یک فایل صوتی قابل درک است، حتی اگر به کمی یک قسمت از ده میلیون باشد. به هر حال با اینکه سیستم شنوایی انسان حساسیت زیادی دارد ولی دربرابر بعضی تغییرات حساسیت خود را از دست می‌دهد. مثلاً صداهای بلند صداهای آرام را در خود جای می دهند.

[1] Mail Server

در هنگام پنهان نگاری در صوت دو نکته مهم را بایستی مورد توجه قرار داد:

- باید از ضعف سیستم شنوایی انسان سو استفاده کرد.
- توجه خاصی به حساسیت فوق العاده آن داشت.

- پنهان نگاری در تصاویر

از آنجا که تصاویر مهمترین رسانه مورد استفاده به خصوص در اینترنت هستند و درک تصویری انسان از تغییرات در تصاویر محدود است. تصاویر به عنوان یکی از بهترین رسانه های پوششی در پنهان نگاری معرفی شدند و بدین ترتیب الگوریتم های پنهان نگاری متعددی برای ساختارهای مختلف تصاویر نظیر تصاویر خام یا BMP (۲۴ بیتی رنگی یا ۸ بیتی سیاه و سفید)، تصاویر پالت (۱۶ رنگ، ۲۵۶ رنگ، ...) تصاویر فشرده شده نظیرJPEG، JPEG2000 و ... در حوزه مکانی[1] و حوزه تبدیل[2] ارائه شده است.

استفاده از ساختار JPEG برای انتقال تصویر به خصوص در محیط اینترنت بسیار مرسوم‌تر از بقیه ساختارها است. لذا روش های متعددی برای پنهان نگاری در تصاویرJPEG معرفی شده است. در مورد تصاویر Gif بایست اشاره نمود که علی رغم کاربرد وسیع این تصاویر در سطح اینترنت و علاقه کاربران به استفاده از آن، استفاده از آن ها برای کاربرد پنهان‌نگاری محدودیت‌هایی دارد. در حقیقت محدودیت تعداد رنگ‌های

---

[1] Spatial
[2] Transform

موجود در یک تصویر پالت (مانند GIF) و سایز کوچک این تصاویر استفاده امن از الگوریتم‌های پنهان‌نگاری را دچار اشکال می کند.

برای استفاده بهتر از ظرفیت تصویر و بعلاوه دلایل امنیتی، اعمال دو ماژول فشرده سازی[1] و رمز نگاری[2] روی داده مورد نظر قبل از انجام تابع جاسازی و متعاقبا استفاده از الگوریتمهای رمزگشایی[3] و بازگشایی[4] روی پیام استخراج شده الزامی است.

***

با توجه به موارد فوق اساس کلر روش های موجود در پنهان نگاری را می توان به دو دسته کلی زیر تقسیم کرد :

- روش هایی که بر پایه نقص در سیستم بینایی انسان استواراست.
- روش هایی که بر پایه نقص در سیستم شنوایی انسان استوار است.

با وجود همه تفاوت های بیان شده درالگوریتم ها، نکته مشترک همه آنها داشتن امنیت بالا است. امنیت یک سیستم پنهان نگاری به این مفهوم است که طی فرآیند جاسازی اطلاعات علاوه بر اینکه کیفیت بصری تصویر بایستی کاملاً حفظ شود حفظ مشخصات آماری هم اهمیت ویژه ای دارد.

به عبارت دیگر در این حالت حتی اگر دشمن نسبت به ارتباط پنهانی بین گیرنده و فرستنده مشکوک شود نتواند تصمیم خاصی بگیرد. در راستای رسیدن به این هدف، برخی از پارامترها را بایستی محدود کرد. به عنوان مثال ظرفیت در این حالت برابر ماکزیمم مقدار اطلاعاتی است که می توان در یک رسانه پوششی پنهان کرد بدون

[1] Compression
[2] Encryption
[3] Decryption
[4] Decompression

اینکه به امنیت سیستم خدشه ای وارد شود و اینکه بتوان پیغام را با اطمینان بالایی از تصویر استگوی حاصل بازیابی نمود.

مواردی که در طراحی یک روش پنهان نگاری دارای اهمیت هستند :

۱. شفافیت[1] : شفافیت سیستم بیان می دارد که موضوع میزبان قبل وبعد از جاسازی در پیام نباید تفاوت محسوسی داشته باشد، چرا که هدف غیر قابل حس کردن انتقال پیام است و در حقیقت امنیت یک سیستم پنهان سازی در همین مسأله شفافیت نهفته است و هر چقدر که شباهت موضوع میزبان پیام در هر دو حالت عاری وحاوی پیام بیشتر باشد امنیت این سیستم در سطح بالاتری قرار دارد.

۲. مقاومت[2] : مقاومت یک سیستم پنهان سازی به معنای این است که پیام پنهان شده درمقابل اعمال تغیرات ناخواسته و غیر عمدی که وجود نویز در طول مسیر انتقال بوجود می آورد و یا اعمال تغییرات عمدی که توسط حمله کننده فعال به منظور تغییر پیام یا از بین بردن آن انجام می گیرد مقاومت لازم راداشته باشد.

۳. ظرفیت[3] : در یک سیستم پنهان سازی هر چقدر بتوان پیام بیشتری را در یک میزبان مخفی نمود این سیستم مناسب تر خواهد بود. حجم داده‌ای که می توان در یک میزبان ذخیره کرد دقیقا بستگی به ماهیت میزبان دارد و این که تاچه حدی می توان داده در آن پنهان کرد بدون اینکه در شفافیت آن تأثیری جدی بگذارد. سه ویژگی فوق بطور بسیار تنگاتنگ در ارتباط با یکدیگر هستند بدین معنی که با ثابت فرض

---

[1] Transparency
[2] Resistance
[3] Capacity

کدن ویژگی اول و افزایش ویژگی دوم، ویژگی سوم حتما کاهش خواهد یافت.

ثابت= مقاومت*ظرفیت

فصل ۳

تحلیل پنهان نگاری اطلاعات

در حالیکه هدف پنهان نگاری مخفی کردن اطلاعات و جلوگیری از پیدا شدن و جلب توجه آنهاست، تحلیل پنهان نگاری علمی است که برای اثبات وجود یک پیغام در یک رسانه ی پنهان‌نگار، تخریب، استخراج و یا تغییر پیغام به کار می رود و در راستای رسیدن به این اهداف بسته به اینکه چه نوع اطلاعاتی در مورد الگوریتم جاسازی دارد می‌توان حملات مختلفی را طراحی نمود.

لزوم تحلیل پنهان نگاری

به دلیل رشد وسیع ارتباطات دیجیتال و سهولت در رد و بدل نمودن اطلاعات و پرونده‌ها از طریق شبکه‌های کامپیوتری نظیر اینترنت و همچنین حجم بسیار زیاد اطلاعات رد و بدل شده، پنهان‌نگاری کاربرد مناسبی پیدا کرده است و استفاده از آن روزبه‌روز بیشتر می‌شود. از طرفی برای جلوگیری یا اطلاع از ارتباطات باندهای تروریستی یا افراد بزهکار و یا خروج اطلاعات محرمانه از شرکت ها یا

سازمان‌ها یا به منظور ارزیابی امنیتی سیستم‌های پنهان‌نگاری که توسط نیروهای نظامی یا امنیتی استفاده می‌شوند، به تحلیل پنهان‌نگاری نیاز است. هر چقدر پهنای باند اینترنت برای انتقال پرونده‌های بزرگ نظیر پرونده‌های ویدئویی، بیشتر می‌شود، انتقال اطلاعات غیرعادی و مشکوک نیز ساده‌تر شده و غیرقابل آشکارتر می‌شود. در طی سال‌های اخیر تلاش‌هایی برای طراحی الگوریتم‌های تحلیل انجام شده است.

بررسی‌ها نشان می‌دهد که در کل دنیا بودجه های کلانی به تحقیق و پژوهش در این حوزه اختصاص می‌دهند. برای مثال آماری که از سال ۲۰۰۶ وجود دارد این است که کارلز بونسلت[1] پروفسور دانشکده‌ی مهندسی الکترونیک و کامپیوتر دانشگاه دلاویر[2] یک بودجه‌ی ۱۶۷۰۰۰ دلاری از NSF[3] برای تحلیل پنهان‌نگاری گرفته است.

اهداف تحلیل پنهان نگاری

به‌طورکلی اهداف تحلیل پنهان‌نگاری و یا حالت‌هایی که تحلیل انجام می‌گیرد به ترتیب زیر است :

۱. اثبات وجود و یا عدم وجود پیغام پنهانی در یک رسانه‌ی مشکوک
این حالت مهمترین هدف تحلیل پنهان‌نگاری است و اکثر الگوریتم‌های ارائه شده نیز در این مقوله هستند.

۲. تخریب پیغام
این حالت مربوط به بازرسی فعال می‌شود. در یک کانال ارتباطی مشکوک تمام رسانه‌های رد و بدل شده را طوری تغییر می‌دهند که

---

[1] Carles Boncelet
[2] Delaware
[3] National Science Foundation

مطمئن باشند هیچ پیغامی رد و بدل نمی‌شود. البته در این زمینه نیز نکته‌هایی وجود دارد که در بعضی مقالات مطرح شده است. مهمترین نکته این است که تغییر رسانه با هدف تخریب، کمترین تأثیر را روی کیفیت رسانه بگذارد.

۳. استخراج پیغام

اگر فرستنده و گیرنده از الگوریتم‌های ساده ی پنهان‌نگاری استفاده کنند که نیازی به کلید رمز یا عمومی ندارد و یا این که کلید لو رفته باشد و الگوریتم توسط دشمن شناسایی شده باشد، دشمن می‌تواند پیغام را استخراج نماید. البته این حالت در پنهان‌نگاری به سختی اتفاق می‌افتد.

۴. تغییر پیغام

پس از استخراج پیغام، ممکن است دشمن به قصد فریب، پیغام را تغییر دهد و آنرا در تصویر قرار داده و برای گیرنده ارسال کند.

۵. استخراج کلید عمومی و کلید رمز

در بسیاری از الگوریتم های پنهان‌نگاری، کلید عمومی در بخشی از رسانه ی پنهان‌نگار به صورت ترتیبی قرار می‌گیرد که می‌توان الگوریتم‌های تحلیل خاصی به این منظور طراحی نمود.

۶. یافتن الگوریتم پنهان‌نگاری

یک نوع تحلیل می‌تواند این باشد که پیغام به نوعی به دست دشمن رسیده است و دشمن می‌خواهد الگوریتم پنهان‌نگاری را به دست آورد تا برای رسانه‌های پنهان‌نگار بعدی بتواند پیغام پنهانی را استخراج کند.

در راستای رسیدن به اهداف یاد شده تحلیلگر دو نوع بازرسی(فعال و غیرفعال) می تواند انجام دهد:

- بازرسی فعال[1]

در این نوع بازرسی، ناظر پیغام‌ها را با اندکی دست‌کاری تغییر می‌دهد تا امیدوار باشد که هیچ ارتباط پنهانی برقرار نمی‌شود. چون روش های پنهان‌نگاری بیشتر روی امنیت و ظرفیت تکیه دارد، معمولاً شکننده و غیرمقاوم هستند لذا پنهان‌نگاری در برابر ناظر فعال، کار مشکلی است و در این حالت باید از تکنیک‌های واترمارک مقاوم بهره گرفت.

- بازرسی غیرفعال[2]

در بازرسی غیرفعال، تحلیلگر تمام پیغام‌هایی را که بین فرستنده و گیرنده رد و بدل می‌شود بررسی می کند و هیچ پیغامی را تغییر نمی‌دهد. لازم به ذکر است که در ارتباط فرستنده و گیرنده، رسانه استگو قابل تشخیص نیست و این تحلیلگر است که باید با هنر خود آن را پیدا کند.

شیوه حملات تحلیل

تحلیل را با دو شیوه‌ی حملات مشاهده‌ای[3] و آماری[4] می‌توان انجام داد. اگر چه پنهان‌نگاری سعی می کند اطلاعات را طوری پنهان نماید که قابل مشاهده و ادراک نباشد ولی اعوجاج هایی روی مشخصات آماری سیگنال پوششی ایجاد می کند. هنر روش های تحلیل، شناسایی این ویژگی‌ها و دسته‌بندی آن ها، برای جداسازی تصاویر پنهان‌نگار و غیرپنهان‌نگار است.

---

[1] Active warden
[2] Passive warden
[3] Visual Attacks
[4] Statistical Attacks

روش‌های تحلیل آماری خود به دو گروه روش های عمومی و الگوریتم‌هایی که برای یک روش خاص پنهان‌نگاری طراحی می‌شوند، تقسیم می‌گردند. در روش های عمومی، تحلیل برای همهٔ روش های پنهان‌نگاری یا برای دسته‌ای از روش های پنهان‌نگاری انجام می‌شود. اگر چه روش های عمومی کاربردی‌تر و جذاب‌تر هستند برای یک الگوریتم خاص نسبت به گروه دوم، پاسخ‌های ضعیف‌تری تولید می‌کنند.

البته بایستی اشاره کرد که با توجه به ساختارهای تصویری، دسته بندی‌های مختلفی برای تحلیل پنهان نگاری می توان ارائه نمود. به عنوان مثال تحلیل پنهان نگاری در حوزه مکانی و در حوزه تبدیل و یا تحلیل پنهان نگاری برای تصاویر غیر فشرده و تصاویر فشرده. تحلیل پنهان‌نگاری برای تصاویر رنگی، سیاه و سفید و باینری.

پنهان نگاری در امور تجاری بسیار پرکاربرد است و در کشورهایی که متعهد به اجرای قانون حق تکثیر هستند خدمات خوبی برای صاحبان تولیدات الکترونیکی روی شبکه اینترنت ارائه نموده است . در کشور ما در حال حاضر متاسفانه به دلیل عدم رعایت قانون ذکر شده شاید اهمیت کاربردی این علم زیاد مورد توجه نباشد لیکن با پیشرفت صنعت IT در آینده ای نه چندان دور توجه بیشتر به آن گریز ناپذیر خواهد بود. همچنین به لحاظ ارتباط این علم با مسائل امنیتی در برقراری ارتباطات پوشیده توجه ارگان ها و نهادهای ذیربط و ذینفع را می طلبد و غفلت از آن زیان های جبران ناپذیری را متصور می سازد. متاسفانه در این میان گروه های خرابکار و گروه های تروریستی نیز که معمولاً از امکانات مالی خوبی بر خوردار هستند از این فناوری چشم پوشی نمی کنند، لذا توجه به تحلیل پنهان‌نگاری بسیار ضروری است.