





دانشگاه کردستان
دانشکده فنی و مهندسی
گروه مهندسی کامپیوتر و فناوری اطلاعات

عنوان:

نهان نگاری امن پر ظرفیت تصاویر دیجیتال

پژوهشگر:

ام کلثوم شهبازی

استاد راهنما:

دکتر بهرام ظهیر اعظمی

استاد مشاور:

دکتر فردین اخلاقیان طاب

پایان نامه کارشناسی ارشد رشته مهندسی کامپیوتر گرایش هوش مصنوعی.

مهر ماه ۱۳۹۰



دانشگاه کردستان
دانشکده فنی و مهندسی
گروه مهندسی کامپیوتر و فناوری اطلاعات

عنوان:

نهان نگاری امن پر ظرفیت تصاویر دیجیتال

پژوهشگر:

ام کلثوم شهرباری

استاد راهنما:

دکتر بهرام ظهیر اعظمی

استاد مشاور:

دکتر فردین اخلاقیان طاب

پایان نامه کارشناسی ارشد رشته مهندسی کامپیوتر گرایش هوش مصنوعی.

مهر ماه ۱۳۹۰



دانشگاه کردستان
دانشکده فنی و مهندسی
گروه مهندسی کامپیوتر و فناوری اطلاعات

پایان نامه کارشناسی ارشد رشته مهندسی کامپیوتر گرایش هوش مصنوعی

عنوان:

نهان نگاری امن پر ظرفیت تصاویر دیجیتال

پژوهشگر:

ام کلثوم شهرباری

در تاریخ / / ۱۳ توسط کمیته تخصصی و هیات داوران زیر مورد بررسی قرار گرفت و با نمره و درجه به تصویب رسید.

<u>امضاء</u>	<u>مرتبہ علمی</u>	<u>نام و نام خانوادگی</u>	<u>هیات داوران</u>
	استاد یار	دکتر بهرام ظهیر اعظمی	۱- استاد راهنما
	استاد یار	دکتر فردین اخلاقیان طاب	۲- استاد مشاور
	استاد یار	دکتر آرش احمدی	۳- استاد داور خارجی
	استاد یار	دکتر محمد فتحی	۴- استاد داور داخلی

مهر و امضاء معاون آموزشی و تحصیلات تکمیلی

مهر و امضاء گروه

دانشکده

*** تعهد نامه ***

اینجانب ام‌کلثوم شهریاری دانشجوی کارشناسی ارشد رشته مهندسی کامپیوتر گرایش هوش مصنوعی دانشگاه کردستان، دانشکده فنی و مهندسی گروه مهندسی کامپیوتر و فناوری اطلاعات تعهد می‌نمایم که محتوای این پایان‌نامه نتیجه تلاش و تحقیقات خود بوده و از جایی کپی برداری نشده و به پایان رسانیدن آن نتیجه تلاش و مطالعات مستمر اینجانب و راهنمایی و مشاوره اساتید بوده است.

با تقدیم احترام

ام‌کلثوم شهریاری

۱۳۹۰ / ۰۷ / ۱۰

تقدیم به

پدر و مادر بزرگوارم که همیشه پشتیبان من بوده‌اند

و همه راهروان ره علم

سپاس‌گزاری

در ابتدا، بر خود لازم می‌دانم که از زحمات بی‌دریغ و راهنمایی‌های ارزشمند و پشتیبانی‌های استاد گرامی جناب آقای دکتر ظهیراعظمی در راستای انجام این پروژه کمال تشکر و قدردانی را داشته باشم.

همچنین مراتب قدردانی خود را از استاد ارجمند جناب آقای دکتر اخلاقیان، که در انجام این پروژه از راهنمایی‌های سودمند ایشان بهره‌مند شده‌ام، اعلام می‌دارم.

در ادامه جا دارد تا سپاس ویژه‌ای از سرکار خانم دکتر هدیه ساجدی که از هیچ کمکی در راستای انجام این پروژه دریغ ننموده‌اند، داشته باشم.

و در پایان سپاس بی‌پایان خود را نثار پدر و مادر بزرگوaram که در تمام طول تحصیلات، همواره پشتیبان من بوده‌اند، می‌نمایم.

چکیده

گسترش چشم‌گیر داده‌های چند رسانه‌ای در دنیای الکترونیک ما، الزام به وجود رهیافت جدیدی برای برقراری ارتباط، به نام نهان‌نگاری دیجیتال دارد. از طرف دیگر تصاویر به دلیل داشتن افزونگی بالا و درک دیداری محدود انسان به تغییرات ایجاد شده در آن‌ها، و نیز گسترش استفاده در اینترنت، سیگنال‌های پوشش مناسبی به‌شمار می‌روند. در نقطه مقابل نهان‌نگاری، روش‌های تحلیل نهان‌نگاری وجود دارند که سعی در پی‌بردن به وجود ارتباط سری دارند. یک سیستم نهان‌نگاری بایستی داده پیام را به صورت غیرقابل مشاهده و غیر قابل شناسایی در سیگنال پوشش جایگذاری نماید. در این پایان‌نامه درصد ارائه روش‌های نهان‌نگاری ای هستیم که این دو مهم را برآورده سازند. در پایان‌نامه حاضر، سه روش نهان‌نگاری ارائه شده است. روش اول، داده پیام را در ضرایب کانتورلت تصویر جایگذاری می‌نماید. روش ارائه شده از دو جهت مورد توجه است: اول آن‌که تبدیل کانتورلت تحلیل دقیق‌تری از تصویر به‌دست می‌دهد و تغییر در یک ضریب، تاثیر کم‌تری در ضرایب دیگر دارد. دوم آن‌که روش‌های تحلیل نهان‌نگاری موجود، محدود به دامنه DCT و موجک هستند و در شناسایی تصاویر نهان‌نگاری شده در حوزه کانتورلت با مشکل مواجه می‌شوند. روش پیشنهادی دوم، پیام را در دامنه موجک تصویر به نحوی جایگذاری می‌کند که کم‌ترین تغییرات متوجه تصویر پوشش شود و نیز روش‌های تحلیل نهان‌نگاری مختلف نیز قادر به تشخیص وجود پیام سری نشوند.

ایده روش سوم از متد تجزیه به وسیله ترکیب در ووکودر CELP گرفته شده است و آن را "نهان-نگاری به وسیله نهان‌کاوی" نامیده‌ایم. در این روش ابتدا پیام مخفی توسط روشی نوین مبتنی بر تبدیل موجک صحیح، در تصویر پوشش جایگذاری می‌شود و به واحد تحلیل نهان‌نگاری داده می‌شود تا امنیت آن توسط نهان‌کاوهای مختلف مورد ارزیابی قرار گیرد. خروجی واحد تحلیل فیدبکی برای واحد نهان‌نگاری محسوب می‌شود. کنترل این حلقه را الگوریتم ژنتیک به عهده می‌گیرد. نتایج به-دست آمده از این روش، حاکی از تولید تصاویر نهان‌نگاری شده‌ای با PSNR بالاتر از 70 dB و مقاوم در برابر روش‌های تحلیل آماری است، و نیز روش‌های تحلیل نهان‌نگاری فراگیری مانند نهان‌کاو ۲۷۴ بعدی و WBS نتوانسته‌اند با دقتی بیشتر از ۶۰ درصد، وجود پیام را تشخیص دهند.

کلمات کلیدی: الگوریتم ژنتیک، تبدیل کانتورلت، تبدیل موجک صحیح، تحلیل نهان‌نگاری، نهان-نگاری دیجیتال

فهرست مطالب

فصل اول

- ۱-۱ مقدمه..... ۱
- ۲-۱ تفاوت رمزنگاری و نهان‌نگاری..... ۲
- ۳-۱ تاریخچه نهان‌نگاری..... ۳
- ۴-۱ نهان‌نگاری در قالب مساله زندانی‌ها..... ۴
- ۵-۱ تحلیل نهان‌نگاری..... ۵
- ۶-۱ پارامترهای سیستم پنهان‌سازی اطلاعات..... ۶
- ۷-۱ چشم‌انداز..... ۸

فصل دوم

- ۱-۲ مقدمه..... ۹
- ۲-۲ دسته‌بندی کلی روش‌های نهان‌نگاری..... ۹
- ۱-۲-۲ روش‌های حوزه مکان..... ۱۰
- ۲-۲-۲ روش‌های حوزه تبدیل..... ۱۳
- ۱-۲-۲-۲ تبدیلات..... ۱۵
- ۱-۲-۲-۲-۱ تبدیل فوریه گسسته..... ۱۵
- ۲-۲-۲-۲-۱ تبدیل کسینوسی گسسته..... ۱۵
- ۳-۲-۲-۲-۱ تبدیل موجک گسسته..... ۱۵
- ۴-۲-۲-۲-۱ تبدیل کانتورلت..... ۱۸
- ۲-۲-۲-۲ روش‌های موجود در دامنه DCT..... ۲۱
- ۳-۲-۲-۲ روش‌های موجود در دامنه موجک..... ۲۵
- ۴-۲-۲-۲ روش‌های موجود در دامنه کانتورلت..... ۲۷

فصل سوم

۲۸	۱-۳ مقدمه
۲۹	۲-۳ تحلیل نهان‌نگاری در پنهان‌سازی اطلاعات به صورت LSB
۲۹	۱-۲-۳ روش Chi-Square
۳۲	۲-۲-۳ روش Chi-Square تعمیم یافته
۳۲	۳-۲-۳ حمله با استفاده از بافت‌نگار تصویر
۳۳	۱-۳-۲-۳ حمله Harmsen
۳۴	۲-۳-۲-۳ حمله Ker
۳۵	۴-۲-۳ حمله RS
۳۷	۳-۳ تحلیل نهان‌نگاری در نهان‌نگاری اطلاعات در دامنه موجک
۳۸	۱-۳-۳ WBS
۳۸	۲-۳-۳ روش Liu
۳۹	۴-۳ FBS
۳۹	۵-۳ روش نهان‌کاوی با بردار ویژگی ۲۷۴ بعدی
۳۹	۶-۳ روش نهان‌کاوی با بردار ویژگی ۳۲۴ بعدی
۴۰	۷-۳ روش نهان‌کاوی YASS
۴۱	۸-۳ جمع‌بندی

فصل چهارم

۴۲	۱-۴ مقدمه
۴۲	۲-۴ روش پیشنهادی اول
۴۲	۱-۲-۴ شرح الگوریتم
۴۴	۲-۲-۴ فرایند جایگذاری پیام
۴۵	۳-۲-۴ فرایند استخراج پیام
۴۶	۳-۴ روش پیشنهادی دوم

۴۶	۱-۳-۴ شرح الگوریتم
۴۷	۲-۳-۴ فرایند جایگذاری پیام
۴۹	۳-۳-۴ فرایند استخراج پیام
۴۹	۴-۴ روش پیشنهادی سوم
۴۹	۱-۴-۴ شرح الگوریتم
۵۲	۲-۴-۴ تعریف کروموزوم
۵۴	۳-۴-۴ فرایند جایگذاری پیام
۵۵	۴-۴-۴ فرایند استخراج پیام
۵۵	۵-۴ تبدیل موجک صحیح
۵۷	۶-۴ مروری بر الگوریتم‌های ژنتیک

فصل پنجم

۶۰	۱-۵ مقدمه
۶۰	۲-۵ آزمایش‌های مربوط به الگوریتم پیشنهادی اول
۶۰	۱-۲-۵ شفافیت
۶۴	۲-۲-۵ مقاومت در برابر روش‌های نهان‌کاوی
۶۵	۳-۲-۵ ظرفیت نهان‌نگاری
۶۶	۴-۲-۵ زمان اجرای الگوریتم
۶۶	۳-۵ آزمایش‌های مربوط به الگوریتم پیشنهادی دوم
۶۶	۱-۳-۵ شفافیت
۶۹	۲-۳-۵ مقاومت در برابر روش‌های نهان‌کاوی
۷۰	۳-۳-۵ ظرفیت نهان‌نگاری
۷۰	۴-۳-۵ زمان اجرای الگوریتم
۷۰	۴-۵ آزمایش‌های مربوط به الگوریتم پیشنهادی سوم

۷۰ شفافیت ۱-۴-۵
۷۳ مقاومت در برابر روش‌های نهان‌کاوی ۲-۴-۵
۷۴ حمله RS ۱-۲-۴-۵
۷۵ حمله Harmsen ۲-۲-۴-۵
۷۵ نهان‌کاو WBS ۳-۲-۴-۵
۷۶ بافت‌نگار تصویر ۳-۴-۵
۷۷ ظرفیت نهان‌نگاری ۴-۴-۵
۷۷ زمان اجرای الگوریتم ۵-۴-۵

فصل ششم

۷۸ مقدمه ۱-۶
۷۹ پیشنهادهایی برای فعالیت‌های آتی ۲-۶
۸۱ منابع
۸۵ واژگان انگلیسی به فارسی
۸۸ واژگان فارسی به انگلیسی

فهرست جداول

- جدول ۴-۱: نحوه تغییر ضریب کانتورلت برای جایگذاری یک بیت پیام ۴۵
- جدول ۴-۲: الگوی استخراج بیت‌های پیام ۴۶
- جدول ۴-۳: نحوه محاسبه پارامترهای a, b ۴۹
- جدول ۴-۴: نحوه تغییر ضرایب ۴۹
- جدول ۴-۵: پارامترهای مورد استفاده در الگوریتم ژنتیک ۵۳
- جدول ۵-۱: میانگین PSNR برای ۲۵۰ تصویر از پایگاه داده ۶۲
- جدول ۵-۲: درصد دقت شناسایی روش‌های نهان‌کاوی بر روی تصاویر نهان‌نگاری شده با روش پیشنهادی اول ۶۴
- جدول ۵-۳: درصد دقت نهان‌کاوهای مختلف روی تصاویری که با استفاده از روش‌های نهان‌نگاری مختلف به‌وجود آمده‌اند. ۶۵
- جدول ۵-۴: متوسط ظرفیت نهان‌نگاری روش‌های مختلف ۶۶
- جدول ۵-۵: میانگین PSNR برای تصاویر پایگاه داده نهان‌نگاری شده با روش مبتنی بر موجک پیشنهاد شده ۶۷
- جدول ۵-۶: درصد دقت شناسایی روش‌های نهان‌کاوی بر روی تصاویر نهان‌نگاری شده با روش پیشنهادی دوم ۷۰
- جدول ۵-۷: میانگین PSNR برای تصاویر پایگاه داده نهان‌نگاری شده با روش پیشنهادی سوم ۷۱
- جدول ۵-۸: نتایج حمله RS به روش پیشنهادی سوم. روابط (۵-۱) با دقت بسیار خوبی برای تصاویر نهان‌نگاری شده در قیاس با تصاویر اصلی برقرار است. ۷۴
- جدول ۵-۹: درصد دقت شناسایی روش‌های نهان‌کاوی بر روی تصاویر نهان‌نگاری شده با روش پیشنهادی سوم ۷۶

فهرست اشکال

- شکل ۱-۱: پنهان‌نگاری در قالب مساله زندانی‌ها..... ۵
- شکل ۲-۱: پارامترهای سیستم پنهان سازی اطلاعات..... ۷
- شکل ۱-۲: ساختار کلی یک سیستم پنهان‌نگاری..... ۱۰
- شکل ۲-۲: پنهان‌نگاری به روش LSB..... ۱۱
- شکل ۳-۲: تجزیه تصویر به صفحه بیت‌های مربوطه..... ۱۲
- شکل ۴-۲: پنهان‌نگاری در حوزه تبدیل..... ۱۴
- شکل ۵-۲: بلاک دیاگرام تحلیل فیلتر..... ۱۷
- شکل ۶-۲: فیلتربانک سه سطحی..... ۱۸
- شکل ۷-۲: سه مرحله تبدیل موجک بر روی تصویر..... ۱۸
- شکل ۸-۲: تفاوت کانتورلت و موجک در نمایش یک منحنی..... ۱۹
- شکل ۹-۲: ساختار لاپلاسین هرمی الف. تجزیه یک سطحی ب: بازسازی بر اساس لاپلاسین هرمی..... ۲۰
- شکل ۱۰-۲: فیلتربانک‌های جهت‌دار..... ۲۰
- شکل ۱۱-۲: با ترکیب ساختار هرمی لاپلاسین و فیلتربانک‌های جهت‌دار به ساختار کانتورلت خواهیم رسید..... ۲۱
- شکل ۱۲-۲: تبدیل موجک دو بعدی..... ۲۶
- شکل ۱-۳: بافت‌نگار ضرایب DCT الف: پیش از جایگذاری پیام ب: پس از جایگذاری پیام به روش Jsteg..... ۳۰
- شکل ۲-۳: احتمال وجود پیام سری باروش Chi-Square در یک تصویر پنهان‌نگاری شده به روش Jsteg..... ۳۲
- شکل ۳-۳: مدل پنهان‌نگاری به صورت نويز جمع‌شونده..... ۳۳
- شکل ۴-۳: نمودار RS برای تصویر گرفته‌شده با دوربین دیجیتال و $M = [0 \ 1 \ 1 \ 0]$ ۳۷
- شکل ۵-۳: بلاک دیاگرام تولید ویژگی‌ها در روش پنهان‌کاوی با بردار ویژگی ۳۲۴ بعدی..... ۴۰
- شکل ۱-۴: تجزیه تصویر Lena با تبدیل کانتورلت یک سطحی در هشت جهت..... ۴۳
- شکل ۴-۲: بلاک دیاگرام پنهان‌نگاری پیام مخفی در ضرایب کانتورلت تصویر الف: فرایند جایگذاری پیام. ب: فرایند استخراج پیام..... ۴۴
- شکل ۳-۴: بلاک 3×3 و ضریب منتخب برای جایگذاری پیام..... ۴۵
- شکل ۴-۴: تجزیه تصویر Lena با استفاده از تبدیل موجک گسسته دو بعدی..... ۴۷
- شکل ۵-۴: بلاک دیاگرام روش پیشنهادی مبتنی بر موجک الف: فرایند جایگذاری پیام ب: فرایند استخراج پیام..... ۴۸
- شکل ۶-۴: اعمال تبدیل موجک به بلاک‌های تصویر و انتخاب زیرباند جزئیات برای فرایند جایگذاری پیام..... ۴۸
- شکل ۷-۴: بلاک دیاگرام روش پیشنهادی سوم..... ۵۰
- شکل ۸-۴: نمونه‌ای از کروموزوم تعریف شده برای الگوریتم ژنتیک..... ۵۳
- شکل ۹-۴: ضرایب منتخب برای جایگذاری پیام..... ۵۴
- شکل ۱۰-۴: روال کلی یک الگوریتم ژنتیک..... ۵۹
- شکل ۱-۵: کیفیت تصویر Lena بعد از جایگذاری پیام با طول مختلف. الف: تصویر اصلی Lena ب: جایگذاری ۱۰۰۰ بیت پیام ج: جایگذاری ۲۰۰۰ بیت پیام د: جایگذاری ۴۰۰۰ بیت پیام ه: جایگذاری ۸۰۰۰ بیت پیام..... ۶۱
- شکل ۲-۵: مقایسه PSNR روش پیشنهادی با روش‌های Wavelet-based و ContSteg..... ۶۲

- شکل ۳-۵: نمونه‌ای از تصاویر پایگاه داده و تصویر نهان‌نگاری شده و PSNR متناظر بعد از جایگذاری ۴۰۰۰ بیت پیام ۶۴
- شکل ۴-۵: تصویر نهان‌نگاری شده Lena با روش مبتنی بر موجک پیشنهادی و با پیام‌های با اندازه‌های مختلف الف: ۱۰۰۰ بیت ب: ۲۰۰۰ بیت ج: ۴۰۰۰ بیت د: ۸۰۰۰ بیت ۶۷
- شکل ۵-۵: نمونه‌ای از تصاویر پایگاه داده و تصویر نهان‌نگاری شده حاصل از جایگذاری ۴۰۰۰ بیت پیام به روش پیشنهادی دوم ۶۹
- شکل ۶-۵: تصویر نهان‌نگاری شده Lena با روش پیشنهادی سوم و با پیام‌های با اندازه‌های مختلف الف: ۱۰۰۰ بیت ب: ۲۰۰۰ بیت ج: ۴۰۰۰ بیت د: ۸۰۰۰ بیت ۷۱
- شکل ۷-۵: نمونه‌ای از تصاویر پایگاه داده و تصویر نهان‌نگاری شده حاصل از جایگذاری ۴۰۰۰ بیت پیام به روش پیشنهادی سوم ۷۳
- شکل ۸-۵: توزیع اندازه مشخصه حمله Harmsen به ۲۵۰ تصویر پوشش و تصاویر نهان‌نگاری شده متناظر آن‌ها که با الگوریتم ۳ نهان‌نگاری شده‌اند ۷۵
- شکل ۹-۵: نمایش بافت‌نگار تصویر Lena الف: بافت‌نگار تصویر اصلی ب: بافت‌نگار تصویر نهان‌نگاری شده با جایگذاری پیام‌های با اندازه مختلف ۷۷

CoM	Center of Mass
DCT	Discrete Cosine Transform
DWT	Discrete Wavelet Transform
GA	Genetic Algorithm
HCF	Histogram Characteristic Function
HE	Histogram Error
HVS	Human Visual System
JPEG	Joint Photographic Expert Group
LSB	Least Significant Bit
MAE	Mean Absolute Error
MB	Model Based
PQ	Perturbed Quantization
PSNR	Peak Signal to Noise Ratio
SS	Spread Spectrum
SVM	Support Vector Machine
TIFF	Tag Image File Format
WBS	Wavelet Based Steganalysis
YASS	Yet Another Steganographic Scheme

فصل اول. مقدمه

۱-۱ مقدمه

با گسترش اینترنت و رشد سریع و روزافزون داده‌های دیجیتال، نیاز به یک بستر ارتباطی امن، که در آن داده‌ها به طریقی امن مبادله شوند، بیش از پیش احساس می‌شود. در جهت برقراری یک ارتباط امن می‌توان داده‌ها را به طریقی انتقال داد که برای شنونده غیر مجاز قابل فهم نباشد. طریق دیگر مخفی نمودن ارتباط است. روش اول به رمزنگاری^۱ موسوم است و روش دوم نهان‌نگاری^۲ نامیده می‌شود [۱].

نهان‌نگاری دیجیتال عبارت است از مخفی کردن نامحسوس اطلاعات پیام در داخل یک سیگنال میزبان، مانند صوت، تصویر، ویدیو یا متن، به نحوی که تخریب آشکاری در سیگنال میزبان ایجاد نشود و سیگنال نهان‌نگاره حاصل از سیگنال میزبان قابل تشخیص و تمایز نباشد [۲] و با اطلاع کامل از روش نهان‌نگاری و کلیدهای مورد استفاده، بتوان اطلاعات مخفی را از سیگنال نهان‌نگاری شده بازیابی کرد.

سیگنال تصویر، به دو دلیل، سیگنال پوشش مناسبی در نهان‌نگاری محسوب می‌شود. دلیل اول کاربرد وسیع تصاویر در ارتباطات روزمره است. مثلاً تصاویر در اینترنت به گستردگی مورد استفاده قرار می‌گیرند. دلیل دوم، وجود همبستگی^۳ زیاد در تصاویر است. این همبستگی به معنی وجود افزونگی در تصویر است، که می‌توان از این افزونگی، برای مخفی کردن پیام استفاده کرد.

¹Cryptography

²Steganography

³Correlation

به طور کلی سیستم‌های پنهان‌سازی اطلاعات به دو دسته کلی پنهان‌نگاری و نشانه‌گذاری^۴ تقسیم می‌شوند. در پنهان‌نگاری هدف انتقال نامحسوس پیغام است و تاکید بر روی مخفی نگه‌داشتن وجود تبادل اطلاعات است و رسانه میزبان اهمیت چندانی ندارد. در حالی که نشانه‌گذاری برای اهدافی چون حق کپی و اصالت مالکیت به کار می‌رود و آن‌چه شایان اهمیت است، رسانه میزبان است.

در بررسی سیستم‌های محرمانه از دیدگاه تئوری اطلاعات^۵، شانون سه دسته از ارتباطات مخفی را به صورت زیر بیان نمود [۳]:

۱. سیستم‌های اختفا^۶: شامل روش‌هایی است که وجود پیام از دید دشمن مخفی است مانند جوهر نامرئی، مخفی کردن یک پیام در یک متن و غیره
۲. سیستم‌های پوشیدگی^۷.
۳. سیستم‌های رمزنگاری.

شانون پنهان‌نگاری را از زیرشاخه‌های سیستم‌های اختفا به حساب می‌آورد.

در رمزنگاری تلاش می‌شود اطلاعات سری از دید افراد غیرمجاز مخفی نگه‌داشته شود، در حالی که پنهان‌نگاری وجود اطلاعات را پنهان می‌سازد و هدف مخفی کردن وجود ارتباط است.

۱-۲ تفاوت رمزنگاری و پنهان‌نگاری

در رمزنگاری هدف مخفی نمودن محتوای پیام است. بدین صورت که پیام رمز شده در یک کانال ارتباطی آزاد به سوی گیرنده مجاز فرستاده می‌شود و بدین طریق محتوای پیام از دسترسی افراد غیر مجاز مصون می‌ماند. اما چون معمولاً داده‌های مهم رمز می‌شوند، داده‌های رمز شده توجه بیشتری را به خود جلب می‌کنند و بیشتر مورد حمله مهاجمین قرار می‌گیرند. روش‌های پنهان‌نگاری برای غلبه بر محدودیت الگوریتم‌های رمزنگاری و با هدف مخفی کردن ارتباط به وجود آمده‌اند. امنیت رمزنگاری به معنای محرمانگی پیام است اما امنیت پنهان‌نگاری به پنهان بودن حضور پیام در سیگنال پوشش وابسته است. شکست در یک سیستم پنهان‌نگاری به معنای پی‌بردن به وجود پیام مخفی در یک رسانه است و نیازی به استخراج آن نیست.

⁴Watermarking

⁵Information theory

⁶Concealment System

⁷Privacy Systems

در رمزنگاری مهاجم حتی اگر به وجود اطلاعات مخفی در سیگنال پی ببرد، نباید بتواند بدون استفاده از کلید رمز به اطلاعات مخفی دسترسی یابد. در رمزنگاری، فرض می‌شود که جزئیات الگوریتم رمزنگاری برای مهاجم شناخته شده است (اصل Kerckhoff [۳]).

Cachin مدلی برای امنیت نهان‌نگاری بر اساس مفاهیم تئوری اطلاعات ارائه داده است و امنیت نهان‌نگاری را همانند امنیت رمزنگاری تعریف می‌کند: یک الگوریتم جایگذاری اطلاعات کاملاً امن است اگر یک حمله نتواند به صورت آماری میان رسانه حاوی پیام و رسانه بدون پیام تفاوت قائل شود [۴].

۳-۱ تاریخچه نهان‌نگاری

نهان‌نگاری معادل واژه Steganography است که در اصل واژه‌ای یونانی بوده و از ترکیب دو کلمه Steganos به معنای پوشش و Grpahy به معنی نوشتن تشکیل شده است [۵].

نهان‌نگاری به عنوان یک هنر از قدیمی‌ترین فنونی است که انسان به آن مشغولیت یافته است. سابقه اولین طرح‌های پنهان کردن اطلاعات از دید دشمن، به حدود ۴۰۰۰ سال پیش بازمی‌گردد [۶]. اما نهان‌نگاری به عنوان یک علم بسیار جوان است و از سه دهه گذشته مورد توجه محققین حوزه ارتباطات واقع شده است و تحقیقات زیادی در این زمینه صورت می‌گیرد.

قدیمی‌ترین مثال نهان‌نگاری به حدود سال‌های ۴۴۰ قبل از میلاد برمی‌گردد. هنگامی که حاکم یونان به دست داریوش زندانی شده بود، به دنبال راهی می‌گشت تا پیام‌های مخفی را به لشکریان خودی برساند. او سر برده‌ها را می‌تراشید، پیام را روی سر آن‌ها خالکوبی می‌کرد و پس از رشد مجدد موها، برده‌ها را عازم مقصد می‌نمود.

در سال ۱۴۹۹ تریتموس^۸ اولین کتاب در زمینه نهان‌نگاری با نام "Steganographia" را نوشت. در این کتاب تکنیک‌هایی مانند نوشتن پیام مخفی در بین سطرهای یک متن به وسیله جوهر نامرئی آورده شده بود. این کتاب در زمان وی منتشر نشد. اولین کتاب در این زمینه را اسکاتی^۹ در سال ۱۶۶۵ با نام "Steganographica" نوشت، اما اکثر ایده‌هایش مربوط به تریتموس بود.

نهان‌نگاری در قرن‌های ۱۵ و ۱۶ توسعه یافت. یکی از رساله‌هایی که در این زمینه نوشته شده توسط ویلکینز^{۱۰} است، که بعداً در کالج ترینتی^{۱۱} به استادی رسید. او روش‌هایی را از کد کردن پیام‌ها

⁸Trithemius

⁹Schotti

¹⁰Wilkins

¹¹Trinity

در موزیک تا جوهرهای نامرئی پیشنهاد داد. همچنین او اولین طرح‌ها را در رمزگشایی با استفاده از تناوب کلمات ساخت [۷].

از نمونه‌های تاریخی جدیدتر استفاده از نهان‌نگاری، می‌توان به استفاده آلمانی‌ها در جنگ جهانی اول از جوهرهای نامرئی اشاره کرد [۶]. در جنگ جهانی دوم از حروف خود متن برای نهان‌نگاری استفاده نمودند. به عنوان مثال جاسوسان آلمانی پیام سری را در حروف یک متن ساده و کم اهمیت پنهان می‌نمودند.

اولین روش‌های نهان‌نگاری دیجیتال در دهه ۸۰ مطرح شدند [۷] و تقریباً همه کارهای انجام شده در این زمینه مربوط به دهه اخیر است.

۱-۴ نهان‌نگاری در قالب مساله زندانی‌ها

در سال ۱۹۸۴ تعریف نهان‌نگاری به شکل کلاسیک توسط سیمونز^{۱۲} تحت عنوان مساله زندانی‌ها بیان شد [۸]. آلیس و باب دو زندانی در دو سلول جداگانه هستند که قبل از زندانی شدن، توافقاتی با یکدیگر به منظور طراحی نقشه فرار انجام داده‌اند و بر روی یک کلید مشترک توافق کرده‌اند. آنها می‌توانند پیغام‌هایی را با یکدیگر مبادله کنند. هر ارتباطی که بین این دو صورت می‌گیرد توسط وندی که زندانبان است کنترل می‌شود. وندی اگر فعالیت شک برانگیزی را مشاهده کند، مانع ارتباط باب و آلیس می‌شود. پس پیغام‌های مبادله شده باید طوری باشند که وندی را مشکوک نسازد. بنابراین باب و آلیس از نهان‌نگاری استفاده کرده و پیام‌های نقشه فرار خود را در اشیاء پوششی مناسبی مانند تصاویر پنهان می‌کنند. شیء حاوی پیغام که به آن نهان‌نگاره می‌گویند از طریق کانال ناامنی که وندی ناظر آن است و به آن دسترسی دارد، بین دو طرف مبادله می‌شود. وندی در این مساله یک مهاجم است و می‌تواند فعال و یا غیرفعال باشد. اگر مهاجم فعال باشد، می‌تواند محتوای پیام مورد مبادله را تغییر دهد و نیز می‌تواند پیامی را جعل کرده و به جای آلیس به باب و یا از باب به آلیس بفرستد. در حالتی که مهاجم غیر فعال است، تنها ضرورت برای برقراری امنیت روش نهان‌نگاری این است که داده جایگذاری شده غیرقابل شناسایی باشد.

¹²Simmons