
بسم الله الرحمن الرحيم
بسم الله الرحمن الرحيم
بسم الله الرحمن الرحيم

دانشگاه کردستان

دانشکده فنی و مهندسی

گروه مهندسی کامپیوتر و فناوری اطلاعات

عنوان:

نهان‌نگاری امن پرظرفیت تصاویر دیجیتال

پژوهشگر:

ام‌کلثوم شهریاری

استاد راهنما:

دکتر بهرام ظهیراعظمی

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:

نهان‌نگاری امن پرظرفیت تصاویر دیجیتال

پژوهشگر:

ام‌کلثوم شهریاری

استاد راهنما:

دکتر بهرام ظهیراعظمی

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:

نهان‌نگاری امن پرظرفیت تصاویر دیجیتال

پژوهشگر:
ام‌کلثوم شهریاری

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

هیات داوران	نام و نام خانوادگی	مرتبه علمی	امضاء
۱ـ استاد راهنما	دکتر بهرام ظهیراعظمی	استادیار	
۲ـ استاد مشاور	دکتر فردین اخلاقیان طاب	استادیار	
۳ـ استاد داور خارجی	دکتر آرش احمدی	استادیار	
۴ـ استاد داور داخلی	دکتر محمد فتحی	استاد یار	

مهر و امضاء گروه
دانشکده

مهر و امضاء معاون آموزشی و تحصیلات تکمیلی

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 می نماییم که محتوای این پایان نامه 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

۱۰/ ۰۷ / ۱۳۹۰

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 بزرگوارم 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 پایان-نامه درصدد ارائه روش‌های نهان‌نگاری‌ای 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 آن‌را "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

فصل دوم

فصل سوم

فصل چهارم

فصل پنجم

فصل ششم

فهرست جداول

فهرست اشکال

فهرست اختصارات

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.

---

[1] Cryptography

[2] Steganography

[3] Correlation

به طور کلی سیستم‌های پنهان‌سازی اطلاعات به دو دسته کلی نهان‌نگاری و نشانه‌گذاری[۴] تقسیم می‌شوند. در نهان‌نگاری هدف انتقال نامحسوس پیغام است و تاکید بر روی مخفی نگه‌داشتن وجود تبادل اطلاعات است و رسانه میزبان اهمیت چندانی ندارد. در حالی‌که نشانه‌گذاری برای اهدافی چون حق کپی و اصالت مالکیت به‌کار 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 نهان‌نگاری را از زیرشاخه‌های سیستم‌های اختفا به حساب می‌آورد.

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

۱-۲ تفاوت رمزنگاری و نهان‌نگاری

در رمزنگاری هدف مخفی نمودن محتوای پیام است. بدین صورت که پیام رمزشده 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 معمولا داده‌های مهم رمز می‌شوند، داده‌های رمز شده توجه بیشتری را به خود جلب می‌کنند و بیشتر مورد حمله مهاجمین قرار می‌گیرند. روش‌های نهان‌نگاری برای غلبه بر محدودیت الگوریتم‌های رمزنگاری و با هدف مخفی کردن ارتباط به‌وجود آمده‌اند. امنیت رمزنگاری به معنای محرمانگی پیام است اما امنیت نهان‌نگاری به پنهان بودن حضور پیام در سیگنال پوشش وابسته است. شکست در یک سیستم نهان‌نگاری به معنای پی‌بردن به وجود پیام مخفی در یک رسانه است و نیازی به استخراج آن نیست.

[4] Watermarking

[5] Information theory

[6] Concealment System

[7] Privacy 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 کاملا امن است اگر یک حمله نتواند به صورت آماری میان رسانه حاوی پیام و رسانه بدون پیام تفاوت قائل شود [۴].

۱-۳ 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. هنگامی‌که 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

[8] Trithemius

[9] Schotti

[10] Wilkins

[11] Trinity

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 تقریبا همه کارهای انجام شده در این زمینه مربوط بهدو 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 می-توانند 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 مسأله یک مهاجم است و می‌تواند فعال و یا غیرفعالباشد. 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.

[12] Simmons