بسم الله الرحمن الرحيم

دانشکده ریاضی و رایانه

بخش علوم رایانه

پایان نامه تحصیلی برای دریافت درجه کارشناسی ارشد

رشته علوم رایانه گرایش سیستم‌های هوشمند

بهینه سازی نهان نگاری تصویر با استفاده از منحنی‌های فضا پرکن و الگوریتم رقابت استعماری گسسته

مؤلف :

فاطمه زریسفی کرمانی

استاد راهنما :

دکتر فرامرز صادقی

استاد مشاور :

دکتر مرجان کوچکی رفسنجانی

شهریورماه

۱۳۹۲

این پایان نامه به عنوان یکی از شرایط درجه کارشناسی ارشد به

بخش ریاضی و رایانه

دانشکده علوم رایانه

دانشگاه شهید باهنر کرمان

تسلیم شده است و هیچگونه مدرکی به عنوان فراغت از تحصیل دوره مزبور شناخته نمی شود.

دانشجو :

استاد راهنما :

استاد مشاور :

داور ۱ :

داور۲ :

معاونت پژوهشی و تحصیلات تکمیلی دانشکده :

تقدیر و تشکر:

به مصداق «من لم یشکر المخلوق لم یشکر الخالق» بسی شایسته است از اساتید فرهیخته و فرزانه

جناب آقای دکتر فرامرز صادقی و سرکار خانم دکتر مرجان کوچکی رفسنجانی

که با کرامتی چون خورشید، سرزمین دل را روشنی بخشیدند و گلشن سرای علم و دانش را با راهنمایی های کار ساز و سازنده بارور ساختند و جناب آقای دکتر محمد مسعود جاویدی و جناب آقای دکتر حمید خسروی که قبول زحمت کرده و مطالعه و داوری این پایان نامه را پذیرفتند؛ تقدیر و تشکر نمایم.

معلا مقامت ز عرش برتر باد همیشه توسن اندیشه ات مظفر باد

به نکته های دلاویز و گفته های بلند صحیفه های سخن از تو علم پرور باد

همچنین از پدر و مادر عزیز، دلسوز و مهربانم که آرامش روحی و آسایش فکری فراهم نمودند تا با حمایت های همه جانبه در محیطی مطلوب، مراتب تحصیلی را به نحو احسن به اتمام برسانم؛ سپاسگزاری نمایم.

همتم بدرقه راه کن ای طائر قدس

که دراز است ره منزل و من نو سفرم

چکیده:

امروزه با گسترش شبکه‌های کامپیوتری و افزایش تقاضاها برای انتقال داده بر روی آن‌ها، موضوع امنیت ارتباطات بیش از گذشته مورد توجه قرار گرفته است. در این راستا، علاوه بر رمزنگاری[۱]، پنهان‌کردن اطلاعات[۲] نیز بعنوان یک رشته تحقیقاتی مهم برای حل مشکلاتی در امنیت شبکه و ارتباطات ایمن از طریق کانال‌های عمومی و خصوصی پدیدار شده و نهان‌نگاری[۳] بعنوان یکی از شاخه‌های آن با پنهان‌کردن داده محرمانه درون رسانه‌های دیجیتال حامل برای حل این مشکلات مورد استفاده قرار می‌گیرد. نهان‌نگاری تصویر، که داده محرمانه را درون پیکسل-های یک عکس دیجیتال جاسازی می‌کند بیشتر از سایرین مورد استفاده قرار گرفته است.

از آنجا که امنیت و کیفیت دو معیار مهم در ارزیابی روش‌های نهان‌نگاری هستند، در این پایان نامه روشی پیشنهاد می‌شود که با ترکیب نهان‌نگاری و رمزنگاری هر دو معیار را بهبود می-بخشد. در این فرآیند، داده محرمانه ابتدا با روش رمزنگاری جانشینی تک‌حرفی[۴] رمزنگاری می-شود و سپس با استفاده از روش انطباق زوج پیکسل که براساس الگوریتم رقابت استعماری گسسته[۵] بهینه شده، در تصویر میزبان جاسازی می‌شود. در نهایت با محاسبه میانگین مربع خطا (MSE[۶]) و حدبالای سیگنال نسبت به نویز (PSNR[۷]) که دو معیار اندازه‌گیری کیفیت بصری تصاویر محسوب می‌شوند کارایی روش پیشنهادی در مقایسه با سایر روش‌ها نشان داده می‌شود.

کلید واژه: نهان‌نگاری، رمزنگاری جانشینی، انطباق زوج پیکسل، رقابت استعماری گسسته.

[۱] Cryptography
[۲] Information Hiding
[۳] Steganography
[۴] Mono-alphabetic Substitution Cipher
[۵] Discrite Imperialist Competitive Algorithm (DICA)
[۶] Mean Square Error (MSE)
[۷] Peak Signal to Noise Ratio (PSNR)

فهرست مطالب

عنوان **صفحه**

فهرست شکل‌ها

عنوان **صفحه**

فهرست جداول:

عنوان **صفحه**

فصل ۱:

کلّیات

۱-۱- مقدمه:

تبادل اطلاعات محرمانه بین افراد و سازمان‌ها، همواره یکی از مسائل مهم در ساختار زندگی اجتماعی انسان‌ها و حکومت‌ها می‌باشد که در هر دوره زمانی با توجه به امکانات موجود فرآیندی برای ردوبدل کردن اطلاعات محرمانه پیدا می‌کردند. در حال حاضر، با توجه به پیشرفت تکنولوژی از جمله ذخیره‌سازی اطلاعات به‌شکل عددی[۱]، امکان مخفی کردن اطلاعات در قالب مناسب‌تری فراهم شده است. یکی از این روش‌ها، نهان‌نگاری است. در واقع نهان‌نگاری[۲]، علمی است که برقراری ارتباط داده و اطلاعات محرمانه را از طریق یک حامل چندرسانه‌ای ازجمله فایل‌های عکس، صوت و تصویر دربردارد. این علم تحت این فرضیه رشد و نمو یافته است که اگر ویژگی‌ها و خصوصیاتی مبنی‌بر محرمانگی اطلاعات در ارتباط برقرارشده آشکار و هویدا باشد، متخاصمین را ترغیب به بکارگیری روش‌های مختلف کشف رمز می‌نماید تا بواسطه آن روش‌ها، محتوی اطلاعاتی فاش گردد. بنابراین هدف اصلی در علم نهان‌نگاری، پنهان‌کردن وجود داده محرمانه بجای تغییر شکل آن بوده و هست. فاکتورهای اصلی که نهان‌نگاری را از روش‌های دیگر مثل نشان‌گذاری[۳] و یا رمزنگاری[۴] متمایز می‌کند، تشخیص‌ناپذیری، مقاومت در برابر انواع روش‌های پردازش تصویر و فشرده‌سازی و در نهایت ظرفیت داده پنهان‌شده می‌باشند. بعلاوه امنیت و کیفیت دو فاکتور مهمی هستند که در ارزیابی الگوریتم‌های نهان‌نگاری بیشتر از بقیه مدنظر قرار می‌گیرند.

۱-۲- بیان مسئله:

در قرن ارتباطات، به‌دلیل گسترش روزافزون ارتباطات جهانی و ابداع کانال‌های ارتباطی گوناگون نظیر شبکه اینترنت، ارتباطات ماهواره‌ای و مخابراتی، اطلاعات به‌راحتی در اختیار طیف گسترده‌ای از مردم در سرتاسر دنیا قرار می‌گیرد. تا چندی پیش، ژورنال‌های معتبر بین‌المللی، مقالات و متون علمی، داده‌های محرمانه یا مکاتبات اداری، صرفاً بصورت فیزیکی و کاغذی وجود داشت و هر یک در اختیار طیف محدودی از کاربران قرار می‌گرفت. به‌همان نسبت استفاده غیرقانونی یا سوءاستفاده از آنها یا جعل چنین اسنادی به‌دلیل عدم دسترسی آسان و همچنین نیاز به شگردهای خاص، سخت‌تر و محدودتر بود، اما امروزه ورود فناوری‌های دیجیتال به نظام‌های

---

۱ Digital
۲ Steganography
۳ Watermarking
۴ Cryptography

اداری سراسر دنیا و به زندگی عموم مردم، وجود شبکه جهانی اینترنت و سایر کانال‌های ارتباطی، دسترسی آسان‌تر به اطلاعات را فراهم ساخته‌است.

به‌دلیل گسترش نظام‌های اداری"فاقد کاغذ"، بسیاری از اسناد و اطلاعات در قالب داده‌های دیجیتال تهیه و عرضه می‌شوند. این داده‌ها می‌توانند در قالب‌های گوناگون نظیر متن، کتب الکترونیک، تصویر ساکن، تصویر متحرک، فایل صوتی، نرم‌افزارها، بازی‌های کامپیوتری و انواع دیگر باشند. ماهیت دیجیتالی داده ایجاب می‌کند که به اشتراک‌گذاری، ذخیره و انتشار اطلاعات سریع‌تر و آسان‌تر از قبل صورت گیرد، اما همین امر دسترسی‌ها و تحریف‌های غیرمجاز به داده‌ها و اطلاعات شخصی، بازرگانی و تجاری را افزایش می‌دهد.

در واقع اینترنت بعنوان یک کانال باز محسوب می‌شود که اصلاح[۱]، قطع[۲]، تحریف[۳] و اشکال دیگری از تحریف و اعوجاج می‌تواند در آن رخ دهد[۱]. بدین صورت که حمله‌کننده[٤]-های بدخواه[٥] درصورتی که هیچ مکانیزم امنیتی در جریان فرآیند انتقال داده درنظر گرفته نشده-باشد، به‌سادگی به آنها دسترسی پیدا خواهندکرد[۲]، بدین‌ترتیب مفهوم امنیت نقش اساسی را در ارتباطات چندرسانه‌ای[٦] و دیجیتال بیش از پیش ایفا می‌کند[۳]. به همین منظور رویکردها و مکانیزم‌های متنوعی برای بهبود امنیت ارتباطات ارائه‌شده که می‌توان آنها را به دو دسته زیر تقسیم‌بندی کرد:

۱) رمزنگاری :

هنر و علم نوشتن اطلاعات محرمانه به طریقی که هیچکس به‌جز گیرنده موردنظر نتواند آن-را بازیابی کند[٤].

۲) پنهان‌کردن اطلاعات[۷]:

شامل رویه‌های نشان‌گذاری و نهان‌نگاری، داده محرمانه را در رسانه‌های دیجیتال ازقبیل متن، عکس، صدا و تصویر بعنوان رسانه میزبان[۸] پنهان می‌کند بطوریکه وجود داده محرمانه غیرقابل تشخیص و مشاهده می‌باشد[٥،٦].

---

۱ Modification
۲ Interception
۳ Falsification
٤ Attacker
٥ Malicious
٦ Multimedia
۷ Hiding information
۸ Host media

نشان‌گذاری ، هنر و علم تغییر و اصلاح جزئی و نامحسوس بخشی از داده به منظور جاسازی اطلاعاتی درباره آن است. همانگونه که از تعریف برمی‌آید، نشان‌گذاری بایستی این دو ویژگی مهم را دارا باشد که اولاً تغییرات رسانه میزبان بایستی جزئی و نامحسوس باشد و ثانیاً داده محرمانه بایستی متناسب با محتوی رسانه میزبان باشد[۷].

نهان‌نگاری ، هنر و علم جاسازی داده محرمانه در هر رسانه دیجیتال به روشی غیرقابل تشخیص است، بطوریکه تناسب موضوع و محتوی بین داده محرمانه و رسانه میزبان الزامی نیست[۸].

همانگونه که بیان شد، هر دو علم رمزنگاری و پنهان‌کردن اطلاعات جهت حفاظت از اطلاعات و تأمین امنیت در ارتباطات دیجیتال مطرح شده‌اند اما، اهداف و مقاصد گوناگونی را دنبال می‌کنند که در جدول۱-۱ مورد مقایسه قرارگرفته‌اند[۹].

جدول۱-۱: مقایسه روش‌های رمزنگاری، نشان‌گذاری و نهان‌نگاری [۹].

معیار / روش	نهان نگاری	نشان گذاری	رمزنگاری
حامل[۱]	هر نوع رسانه دیجیتال	بیشتر فایل‌های عکس و صوت	معمولاً براساس فایلهای متنی است اما برای فایلهای عکس توسعه یافته است.
داده محرمانه		نشانه	متن آشکار[۲]
کلید	اختیاری		ضروری
فایل‌های ورودی	حداقل دو فایل		یک فایل
بازیابی و کشف[۳]	کور(بدون نیاز به حضور رسانه میزبان اصلی)	وجود رسانه میزبان اصلی برای بازیابی ضروررری است	کور(بدون نیاز به حضورمتن اصلی)
تصدیق/ سندیت[۴]	بازیابی کل داده		بازیابی کل داده
هدف	ارتباطات امن	نگه‌داری و حفاظت حق چاپ	حفاظت داده
نتیجه	فایل نهان‌نگاری شده	فایل نشان‌گذاری شده	متن رمزی[۵]
پارامترهای ارزیابی	کیفیت و یا ظرفیت	میزان تخریب پذیری[۶]	میزان تخریب پذیری
نوع حملات	تجزیه و تحلیل فایل نهان نگاری شده[۷]	الگوریتم‌های پردازش تصویر	تجزیه و تحلیل متن رمزی

[۱] Carrier
[۲] Plain text
[۳] Detection
[۴] Autenthication
[۵] Cipher text
[۶] Robustness
[۷] Steganalysis

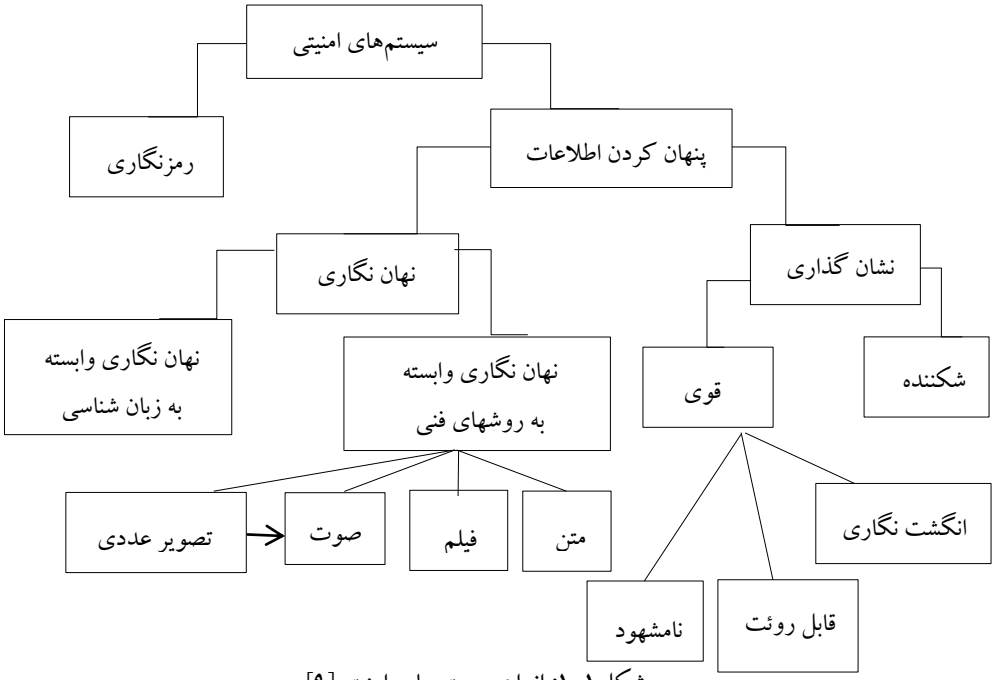
قابلیت دیده شدن[1]	هرگز	گاهی اوقات (بسته به نوع روش بکاررفته برای نشان‌گذاری)	همیشه
شکست‌می‌خورد	تشخیص داده شود	حذف یا جایگزین شود	رمزگشایی شود
میزان شباهت با رسانه میزبان	غیر ضروری است. داده محرمانه مهم‌تر از رسانه میزبان است	معمولاً متناسب با رسانه میزبان انتخاب می‌شود. رسانه میزبان مهم‌تر از داده محرمانه است.	
قابلیت انعطاف	در انتخاب رسانه میزبان آزادی عمل دارد.	در انتخاب رسانه میزبان با محدودیت رو به روست.	
تاریخچه	به غیر از روش‌های ارائه شده برای نسخه دیجیتال، در کل روشی قدیمی و باستانی است.	روش جدید	روش جدید

هرچند، رمزنگاری داده روشی ساده وسریع است اما از آنجا که یک فرم غیرقابل تشخیص و نامفهوم از داده محرمانه ایجاد می‌کند، برای حمله‌کننده‌ها جلب توجه کرده و آنها را به بکاربردن روش‌هایی جهت کشف رمز یا حتی خراب‌کردن متن رمزی، درصورتیکه بازیابی اصل داده زمان-بر یا دشوار باشد، ترغیب می‌کند، در اینصورت گیرنده نمی‌تواند به اصل داده محرمانه دسترسی پیدا کند. در حالیکه در رویکردهای مربوط به پنهان‌کردن اطلاعات، به‌علت مخفی کردن پیام، انگیزه حمله‌کننده برای کشف و دستکاری پیام کاهش می‌یابد. البته بایستی به این نکته توجه داشت که نمی‌توان رویه‌های پنهان‌کردن اطلاعات به ویژه نهان‌نگاری را بعنوان جایگزینی برای روش‌های متنوع رمزنگاری درنظر گرفت بلکه بهتر است آنها را بعنوان مکمل‌های مناسبی برای روش‌های رمزنگاری پنداشته و هردو علم را برای حفاظت بهتر پیام با یکدیگر ترکیب کرد[۱۰]. دراین صورت، اگر نهان‌نگاری تشخیص داده شده و پیام استخراج شود هنوز بایستی از روش‌های مختلف رمزگشایی برای دستیابی به اصل پیام استفاده کرد.

همانگونه که گفته شد، سیستم‌های امنیتی را می‌توان بصورت نشان داده شده در شکل۱-۱ تقسیم‌بندی کرد. آنچه از این شکل برمی‌آید این است که هر نوع فایل دیجیتالی، اعم از متن، عکس، صوت و تصویر، می‌توانند برای نهان‌نگاری مورد استفاده قرار گیرند اما معمولاً قالب‌هایی که درجه افزونگی[2] بالاتری داشته باشند برای این منظور مناسب‌ترند. افزونگی می‌تواند بعنوان بیت‌هایی از یک شیء تعریف شوند که دقت بیش از حد نیاز را برای استفاده و نمایش آن فراهم

[1] Visibility
[2] Redundancy

می‌کنند[۱۰]. در واقع بیت‌های افزونه، آن دسته از بیت‌هایی هستند که می‌توانند بدون ایجاد تغییرات آشکار، دستکاری و اصلاح شوند[۳].



شکل۱-۱: انواع سیستم‌های امنیتی[۹].

از آنجا که فایل‌های عکس و فیلم دارای درجه افزونگی بالاتری نسبت به سایر قالب‌های دیجیتال هستند بنابراین بیشتر الگوریتم‌های مربوط به پنهان کردن اطلاعات و به‌ویژه نهان‌نگاری با توجه به این فایل‌ها طراحی شده‌اند. این در حالیست که برخی از محققین سایر قالب‌ها را نیز برای این منظور مورد استفاده قرار می‌دهند.

در این پایان نامه بر روی نهان‌نگاری عکس[۱] تمرکز کرده، روش‌ها و الگوریتم‌های ارائه شده در این حوزه را مورد بحث وبررسی قرار داده و در نهایت سعی می‌شود با استفاده از الگوریتم رقابت استعماری[۲] روشی برای بهبود خروجی تولید شده با الگوریتم‌های موجود در این حوزه ارائه شود.

[۱] Image steganography
[۲] Imperialist Competition Algorithm (ICA)