

بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيمِ



دانشکده ریاضی و رایانه

بخش علوم رایانه

پایان نامه تحصیلی برای دریافت درجه کارشناسی ارشد

رشته علوم رایانه گرایش سیستم‌های هوشمند

بهینه‌سازی نمان نگاری تصویر با استفاده از منحنی‌های فضا پرکن و الگوریتم رقابت
استعماری گسسته

مؤلف :

فاطمه زریسفی کرمانی

استاد راهنما :

دکتر فرامزر 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 :

دور ۱ :

دور ۲ :

معاونت پژوهشی و تحصیلات تکمیلی دانشکده :

حق چاپ محفوظ و مخصوص به دانشگاه شهید باهنر کرمان است.

تقدیر و شکر:

به مصداق «من لم یسکر المخلوق لم یسکر الخالق» بسی شایسته است از اساتید فریخته و فرزانه

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

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

معلمای مقامت ز عرش برتر باد همیشه توست 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.

بتمم بدرقه راه کن ای طائر قدس

که دراز است ره منزل و من نوسفرم

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، پنهان کردن 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 پنهان‌نگاری^۳ بعنوان یکی از شاخه‌های آن با پنهان کردن داده محرمانه درون رسانه‌های دیجیتال حامل برای حل این مشکلات مورد استفاده قرار می‌گیرد. پنهان‌نگاری تصویر، که داده محرمانه را درون پیکسل‌های 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 پنهان‌نگاری هستند، در این پایان نامه روشی پیشنهاد می‌شود که با ترکیب پنهان‌نگاری و رمزنگاری هر دو معیار را بهبود می‌بخشد. در این فرآیند، داده محرمانه ابتدا با روش رمزنگاری جانشینی تک‌حرفی^۴ رمزنگاری می‌شود 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: پنهان‌نگاری، رمزنگاری جانشینی، انطباق زوج پیکسل، رقابت استعماری گسسته.

^۱ Cryptography

^۲ Information Hiding

^۳ Steganography

^۴ Mono-alphabetic Substitution Cipher

^۵ Discrete Imperialist Competitive Algorithm (DICA)

^۶ Mean Square Error (MSE)

^۷ Peak Signal to Noise Ratio (PSNR)

فهرست مطالب

صفحه	عنوان
۱.....	فصل اول: کلیات
۲.....	۱-۱- مقدمه
۲.....	۲-۱- بیان مسئله
۷.....	۳-۱- پیشینه تحقیق
۸.....	۴-۱- اهداف تحقیق
۹.....	۵-۱- مروری بر فصل های پایان نامه
۱۱.....	۱-۲- مقدمه
۱۰.....	فصل دوم: رمزنگاری
۱۲.....	۲-۲- رمزنگاری
۱۳.....	۳-۲- روشهای سنتی رمزنگاری
۱۳.....	۳-۲-۱- رمزهای جانشینی
۱۳.....	۳-۲-۲- رمزهای جایگشتی
۱۴.....	۴-۲- روش های مدرن رمزنگاری
۱۵.....	۴-۲-۱- رمزنگاری با کلید متقارن
۱۵.....	۴-۲-۱-۱- الگوریتم DES
۱۶.....	۴-۲-۲- رمزنگاری با کلید نامتقارن
۱۷.....	۴-۲-۱-۲- الگوریتم RSA
۱۸.....	فصل سوم: نهان نگاری

۱۹.....	۱-۳-۱- مقدمه
۱۹.....	۲-۳-۲- نمان نگاری
۲۱.....	۳-۳-۳- نمان نگاری عكس
۲۱.....	۱-۳-۳- تعريف عكس ديگييال
۲۲.....	۲-۳-۳- تكنيك هاي نمان نگاری عكس
۲۳.....	۴-۳-۴- نمان نگاری در حوزه مكان
۲۳.....	۱-۴-۳- بيت هاي كم ارزش و عكس هاي مبتي بر بيت
۲۴.....	۲-۴-۳- بيت هاي كم ارزش و عكس هاي مبتي بر جعبه رنگ
۲۵.....	۳-۴-۳- مروري بر كارهاي انجام شده در حوزه مكان
۲۵.....	۱-۳-۴-۳- روش هاي نمان نگاری برگشت ناپذير
۲۷.....	۲-۳-۴-۳- روش هاي نمان نگاری برگشت پذير
۲۸.....	۵-۳-۵- نمان نگاری در حوزه فرکانس
۲۸.....	۱-۵-۳- فشرده سازی JPEG
۳۰.....	۲-۵-۳- مروري بر كارهاي انجام شده در حوزه فرکانس
۳۲.....	فصل چهارم: بهينه سازی
۳۳.....	۱-۴-۱- مقدمه
۳۴.....	۲-۱-۴- بهينه سازی چند هدفه
۳۵.....	۱-۲-۱-۴- روش وزندهی
۳۷.....	۲-۴-۲- الگوریتم رقابت استعماری
۳۸.....	۱-۲-۴- شكل دهی امپراطوری های اولیه
۴۰.....	۲-۲-۴- سیاست جذب

۴۱.....	۳-۲-۴- انقلاب
۴۲.....	۴-۲-۴- جابه جایی موقعیت مستعمره و استعمارگر
۴۳.....	۵-۲-۴- قدرت کل امپراطوری
۴۳.....	۶-۲-۴- رقابت استعماری
۴۵.....	۷-۲-۴- سقوط امپراطوری های ضعیف
۴۶.....	۸-۲-۴- همگرایی الگوریتم
۴۸.....	۳-۴- الگوریتم رقابت استعماری گسسته
۴۹.....	۴-۴- الگوریتم ICA گسسته پیشنهادی
۵۱.....	فصل پنجم: پیشنیازهای تحقیق
۵۲.....	۱-۵- مقدمه
۵۲.....	۲-۵- روش انطباق LSB
۵۶.....	۳-۵- روش جانشینی LSB براساس منحنی های فضا پرکن
۵۸.....	۴-۵- منحنی های فضا پرکن
۵۸.....	۱-۴-۵- Raster-SFC
۵۹.....	۲-۴-۵- Hilbert-SFC
۵۹.....	۳-۴-۵- Moore-SFC
۶۰.....	۴-۴-۵- ZigZag-SFC
۶۱.....	۵-۴-۵- (Peano-SFC) Z-SFC
۶۲.....	فصل ششم: روش نهان نگاری پیشنهادی
۶۳.....	۱-۶- مقدمه

۶۴.....	۲-۶- یافتن بهترین لیست تنظیم با استفاده از الگوریتم رقابت استعماری گسسته پیشنهادی
۶۶.....	۱-۲-۶- چگونگی تشکیل امپراطوری های اولیه
۶۹.....	۲-۲-۶- حرکت مستعمره ها به سمت استعمارگر (سیاست جذب)
۷۰.....	۳-۲-۶- انقلاب مستعمره ها
۷۱.....	۴-۲-۶- جابه جایی مستعمره و استعمارگر
۷۱.....	۵-۲-۶- محاسبه قدرت کل هر امپراطوری
۷۲.....	۶-۲-۶- رقابت استعماری
۷۳.....	۷-۲-۶- سقوط امپراطوری
۷۳.....	۸-۲-۶- همگرایی الگوریتم
۷۴.....	فصل هفتم: پیاده سازی و ارزیابی نتایج
۷۵.....	۱-۷- مقدمه
۷۵.....	۲-۷- پیاده سازی
۷۷.....	۱-۲-۷- مرحله جاسازی
۷۹.....	۱-۱-۲-۷- پیاده سازی الگوریتم رقابت استعماری گسسته پیشنهادی (DICA)
۸۱.....	۲-۲-۷- مرحله استخراج
۸۳.....	۳-۷- نتایج
۹۱.....	فصل هشتم: نتیجه گیری و پیشنهادات
۹۲.....	۱-۸- نتیجه گیری
۹۳.....	۲-۸- تخمین میزان پیچیدگی روش پیشنهادی
۹۴.....	۳-۸- پیشنهاد برای کارهای آینده

منابع ۹۵

واژه نامه فارسی به انگلیسی ۱۰۱

واژه نامه انگلیسی به فارسی ۱۰۵

فهرست شکل‌ها

عنوان	صفحه
شکل ۱-۱: انواع سیستم‌های امنیتی [۹]	۶
شکل ۱-۲: رمزنگاری جایگشت	۱۴
شکل ۲-۲: مدل رمزنگاری با کلید متقارن [۱۵]	۱۵
شکل ۳-۲: الگوریتم رمزنگاری و رمزگشایی DES [۲۲]	۱۶
شکل ۴-۲: مثالی از الگوریتم RSA [۱۵]	۱۷
شکل ۱-۳: نمودار مسئله زندانی‌ها [۳۰]	۲۰
شکل ۲-۳: مدل تعریف شده برای یک تصویر [۳۳]	۲۱
شکل ۳-۳: دسته بندی‌های نهان‌نگاری عکس [۳۵]	۲۲
شکل ۴-۳: صفحات بیتی عکس خاکستری ۸ بیتی	۲۴
شکل ۵-۳: بخشی از یک عکس ۸ بیتی	۲۴
شکل ۶-۳: پیکسل‌های اصلاح شده	۲۴
شکل ۷-۳: الگوی زیگزاگ [۳۳]	۲۹
شکل ۱-۴: تابع پیشینه‌سازی [۷۴]	۳۴
شکل ۲-۴: مفهوم غالب بودن [۷۶]	۳۵
شکل ۳-۴: شمای کلی الگوریتم رقابت استعماری [۸۱]	۳۷
شکل ۴-۴: اجزاء تشکیل دهنده یک کشور [۸۱]	۳۹
شکل ۵-۴: تشکیل امپراطوری‌های اولیه [۸۱]	۴۰
شکل ۶-۴: شمای کلی حرکت مستعمرات به سمت امپراطوری‌ها [۸۱]	۴۱
شکل ۷-۴: انقلاب (تغییر ناگهانی در ویژگی‌های سیاسی اجتماعی یک کشور) [۸۱]	۴۲
شکل ۸-۴: تغییر موقعیت مستعمره و استعمارگر [۸۱]	۴۳
شکل ۹-۴: امپراطوری بعد از تغییر موقعیت‌ها [۸۱]	۴۳

- شکل ۴-۱۰: شمای کلی رقابت استعماری [۸۱]..... ۴۴
- شکل ۴-۱۱: سقوط امپراطوری ضعیف تر [۸۱]..... ۴۶
- شکل ۴-۱۲: فلوچارت الگوریتم رقابت استعماری..... ۴۷
- شکل ۴-۱۳: عملگر ترکیب دونقطه ای..... ۴۹
- شکل ۴-۱۴: عمل جهش درژن پنجم..... ۵۰
- شکل ۵-۱: عکس پوششی H و پیام محرمانه S..... ۵۳
- شکل ۵-۲: روش انطباق LSB زوج پیکسل..... ۵۴
- شکل ۵-۳: (الف) Raster-SFC با پیمایش سطری. (ب) Raster-SFC با پیمایش ستونی..... ۵۸
- شکل ۵-۴: (الف) Hilbert-SFC مرتبه ۱. (ب) Hilbert-SFC مرتبه ۲..... ۵۹
- شکل ۵-۵: Hilbert-SFC مرتبه ۳..... ۵۹
- شکل ۵-۶: (الف) Moore-SFC مرتبه ۱. (ب) Moore-SFC مرتبه ۲..... ۶۰
- شکل ۵-۷: Moore-SFC مرتبه ۳..... ۶۰
- شکل ۵-۸: (الف) ZigZag^۱-SFC. (ب) ZigZag^۲-SFC..... ۶۰
- شکل ۵-۹: (الف) Z-SFC مرتبه ۱. (ب) Z-SFC مرتبه ۲..... ۶۱
- شکل ۵-۱۰: Z-SFC مرتبه ۳..... ۶۱
- شکل ۶-۱: نمودار جریان روش پیشنهادی..... ۶۴
- شکل ۶-۲: نمودار جریان الگوریتم رقابت استعماری گسسته (DICA) پیشنهادی..... ۶۶
- شکل ۶-۳: مثالی از ماتریس نمره M و یک لیست تنظیم متناظر با آن..... ۶۶
- شکل ۶-۴: لیست تنظیم J_۱..... ۶۷
- شکل ۶-۵: لیست تنظیم J_۲..... ۶۷
- شکل ۶-۶: سیاست جذب..... ۷۰
- شکل ۶-۷: رویه اعتبارسنجی..... ۷۰
- شکل ۶-۸: پدیده انقلاب روی ویژگی های ۱ و ۵..... ۷۱
- شکل ۶-۹: شمای کلی رقابت استعماری..... ۷۲
- شکل ۷-۱: تصاویر میزبان انتخاب شده..... ۷۶

- شکل ۲-۷: روند استخراج داده محرمانه ۸۲
- شکل ۳-۷: نتایج جاسازی داده محرمانه در تصویر Lena ۸۵
- شکل ۴-۷: نتایج جاسازی داده محرمانه در تصویر Baboon ۸۵
- شکل ۵-۷: نتایج جاسازی داده محرمانه در تصویر Jet ۸۶
- شکل ۶-۷: نتایج جاسازی داده محرمانه در تصویر Gandhi ۸۶
- شکل ۷-۷: نتایج جاسازی داده محرمانه در تصویر Lena ۸۸
- شکل ۸-۷: نتایج جاسازی داده محرمانه در تصویر Baboon ۸۸
- شکل ۹-۷: نتایج جاسازی داده محرمانه در تصویر Jet ۸۹
- شکل ۱۰-۷: نتایج جاسازی داده محرمانه در تصویر Gandhi ۸۹

فهرست جداول:

صفحه	عنوان
۴	جدول ۱-۱: مقایسه روشهای رمزنگاری، نشانگذاری و نهمان نگاری [۹].
۱۱	جدول ۱-۲: فهرست افراد اخلاکگر و انگیزه آنها [۱۵].
۱۴	جدول ۲-۲: مقایسه روش های پایه رمزنگاری [۱۸].
۳۰	جدول ۱-۳: جدول نرمال سازی استاندارد [۳۳].
۷۸	جدول ۱-۷: کدهای دودویی هر الگوی پیمایشی.
۸۱	جدول ۲-۷: پارامترهای الگوریتم رقابت استعماری گسسته پیشنهادی.
۸۴	جدول ۳-۷: نتایج پیاده سازی کلاس اول (بلاک ۴×۴).
۸۷	جدول ۴-۷: نتایج پیاده سازی کلاس دوم (بلاک ۸×۸).

فصل ١:

كليات

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 به شکل 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 از جمله فایل‌های عکس، صوت و تصویر دربردارد. این علم تحت این فرضیه رشد و نمو یافته است که اگر ویژگی‌ها و خصوصیات مبنی بر محرمانگی اطلاعات در ارتباط برقرار شده آشکار و هویدا باشد، متخصصین را ترغیب به بکارگیری روش‌های مختلف کشف رمز می‌نماید تا بواسطه آن روش‌ها، محتوی اطلاعاتی فاش گردد. بنابراین هدف اصلی در علم نهان‌نگاری، پنهان کردن 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، به دلیل گسترش روزافزون ارتباطات جهانی و ابداع کانال‌های ارتباطی گوناگون نظیر شبکه اینترنت، ارتباطات ماهواره‌ای و مخابراتی، اطلاعات به راحتی 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. به همان نسبت استفاده غیرقانونی یا سوءاستفاده از آنها یا جعل چنین اسنادی به دلیل 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.

به دلیل 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^۴-های بدخواه^۵ در صورتی که هیچ مکانیزم امنیتی در جریان فرآیند انتقال داده در نظر گرفته نشده-باشد، به سادگی به آنها دسترسی پیدا خواهند کرد[۲]، بدین ترتیب مفهوم امنیت نقش اساسی را در ارتباطات چندرسانه‌ای^۶ و دیجیتال بیش از پیش ایفا می‌کند[۳]. به همین منظور رویکردها و مکانیزم‌های متنوعی برای بهبود امنیت ارتباطات ارائه شده که می‌توان آنها را به دو دسته زیر تقسیم‌بندی کرد:

(۱) رمزنگاری:

هنر و علم نوشتن اطلاعات محرمانه به طریقی که هیچکس به جز گیرنده موردنظر نتواند آن-را بازیابی کند[۴].

(۲) پنهان کردن اطلاعات^۷:

شامل رویه‌های نشان‌گذاری و پنهان‌نگاری، داده محرمانه را در رسانه‌های دیجیتال از قبیل متن، عکس، صدا و تصویر بعنوان رسانه میزبان^۸ پنهان می‌کند بطوریکه وجود داده محرمانه غیرقابل تشخیص و مشاهده می‌باشد[۵،۶].

^۱ Modification

^۲ Interception

^۳ Falsification

^۴ Attacker

^۵ Malicious

^۶ Multimedia

^۷ Hiding information

^۸ Host media

نشان گذاری ، هنر و علم تغییر و اصلاح جزئی و نامحسوس بخشی از داده به منظور جاسازی اطلاعاتی درباره آن است. همانگونه که از تعریف برمی آید، نشان گذاری 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].

نهان نگاری ، هنر و علم جاسازی داده محرمانه در هر رسانه دیجیتال به روشی غیر قابل 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 پنهان کردن اطلاعات جهت حفاظت از اطلاعات و تأمین امنیت در ارتباطات دیجیتال مطرح شده اند اما، اهداف و مقاصد گوناگونی را دنبال می کنند که در جدول ۱-۱ مورد مقایسه قرار گرفته اند [۹].

جدول ۱-۱: مقایسه روش های رمزنگاری، نشان گذاری و نهان نگاری [۹].

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

^۱ Carrier

^۲ Plain text

^۳ Detection

^۴ Authentication

^۵ Cipher text

^۶ Robustness

^۷ Steganalysis

قابلیت دیده شدن ^۱	هرگز	گاهی اوقات (بسته به نوع روش بکاررفته برای نشان گذاری)	همیشه
شکست می خورد	تشخیص داده شود	حذف یا جایگزین شود	رمز گشایی شود
میزان شباهت با رسانه میزبان	غیر ضروری است. داده محرمانه مهم تر از رسانه میزبان است	معمولاً متناسب با رسانه میزبان انتخاب می شود. رسانه میزبان مهم تر 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 روش های ارائه شده برای نسخه دیجیتال، در کل روشی قدیمی و باستانی است.	روش جدید	روش جدید

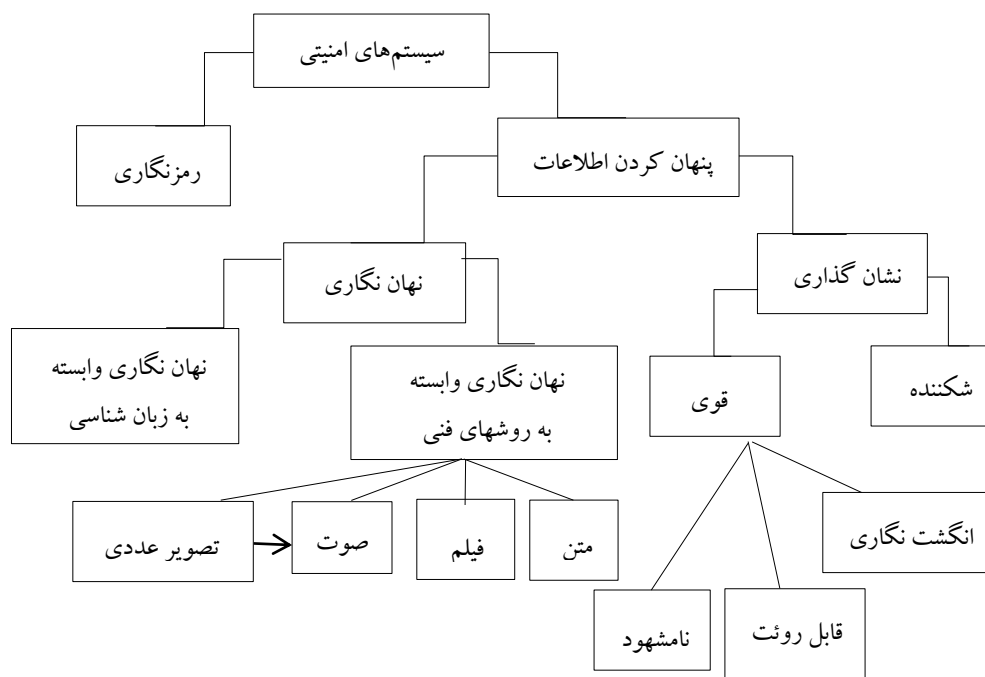
هرچند، رمزنگاری داده روشی ساده و سریع است اما از آنجا که یک فرم غیر قابل تشخیص و نامفهوم از داده محرمانه ایجاد می کند، برای حمله کننده ها جلب توجه کرده و آنها را به بکاربردن روش هایی جهت کشف رمز یا حتی خراب کردن متن رمزی، در صورتیکه بازیابی اصل داده زمان-بر یا دشوار باشد، ترغیب می کند، در این صورت گیرنده نمی تواند به اصل داده محرمانه دسترسی پیدا کند. در حالیکه در رویکردهای مربوط به پنهان کردن اطلاعات، به علت مخفی کردن پیام، انگیزه حمله کننده برای کشف و دستکاری پیام کاهش می یابد. البته بایستی به این نکته توجه داشت که نمی توان رویه های پنهان کردن اطلاعات به ویژه پنهان نگاری را بعنوان جایگزینی برای روش های متنوع رمزنگاری در نظر گرفت بلکه بهتر است آنها را بعنوان مکمل های مناسبی برای روش های رمزنگاری پنداشته و هر دو علم را برای حفاظت بهتر پیام با یکدیگر ترکیب کرد [۱۰]. در این صورت، اگر پنهان نگاری تشخیص داده شده و پیام استخراج شود هنوز بایستی از روش های مختلف رمز گشایی برای دستیابی به اصل پیام استفاده کرد.

همانگونه که گفته شد، سیستم های امنیتی را می توان بصورت نشان داده شده در شکل ۱-۱ تقسیم بندی کرد. آنچه از این شکل برمی آید این است که هر نوع فایل دیجیتالی، اعم از متن، عکس، صوت و تصویر، می توانند برای پنهان نگاری مورد استفاده قرار گیرند اما معمولاً قالب هایی که درجه افزونگی^۲ بالاتری داشته باشند برای این منظور مناسب ترند. افزونگی می تواند بعنوان بیت هایی از یک شیء تعریف شوند که دقت بیش از حد نیاز را برای استفاده و نمایش آن فراهم

^۱ Visibility

^۲ Redundancy

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



شکل ۱-۱: 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 نشان‌نگاری 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 پایان‌نامه بر روی نشان‌نگاری عکس^۱ تمرکز کرده، روش‌ها و الگوریتم‌های ارائه شده در این حوزه را مورد بحث و بررسی 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)