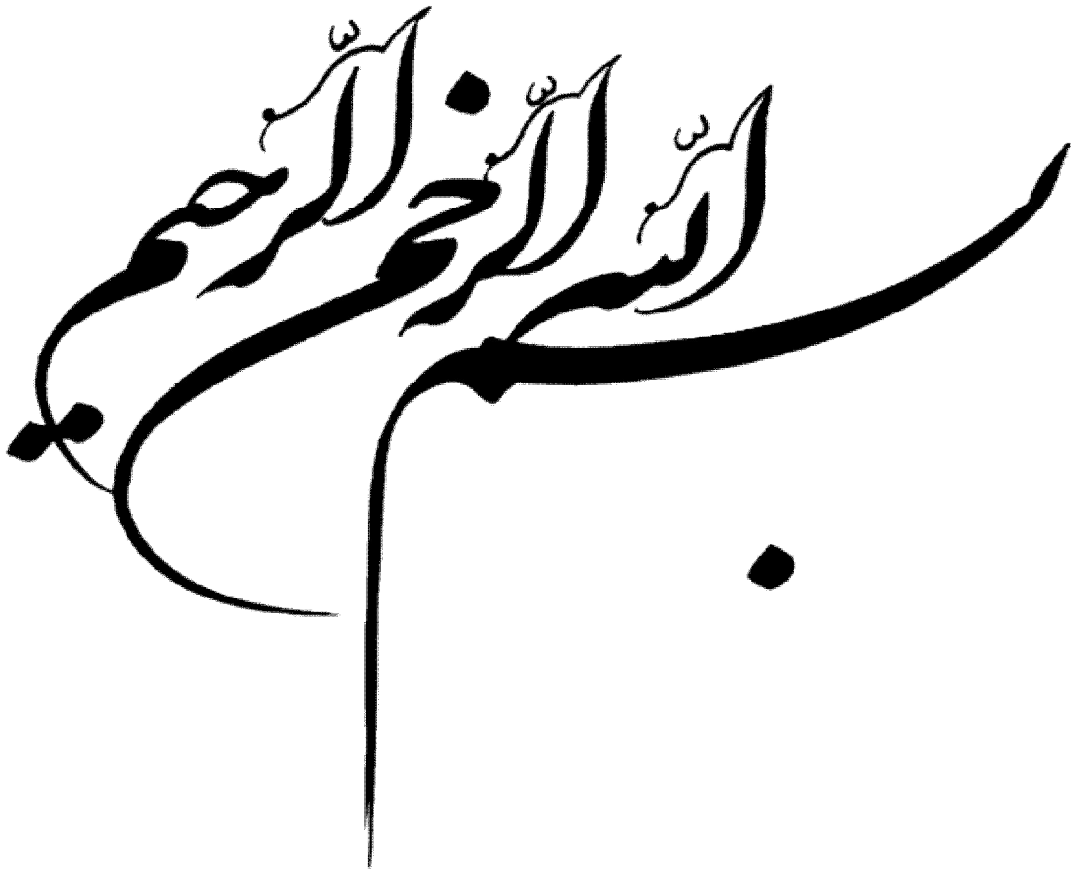

بسم الله الرحمن الرحيم

دانشگاه شاهد

دانشکده فنی و مهندسی

پایان‌نامه دوره کارشناسی ارشد رشته مهندسی فناوری اطلاعات– گرایش IT

پنهان‌نگاری مقاوم در برابر نهان‌کاوی برای تصاویر رنگی

استاد راهنما:

خانم دکتر مریم حسن‌زاده

نام دانشجو

زهرا فرهادی

زمستان ۱۳۹۲

	**اظهار نامه دانشجو**	شماره: تاریخ:

اینجانب زهرا فرهادی دانشجوی کارشناسی ارشد رشته مهندسی فناوری اطلاعات گرایش IT دانشکده فنی و مهندسی دانشگاه شاهد، گواهی می دهم که پایان نامه تدوین شده حاضر با عنوان؛ " پنهان‌نگاری مقاوم در برابر نهان‌کاوی برای تصاویر رنگی " به راهنمایی استاد محترم سرکار خانم دکتر مریم حسن‌زاده، توسط شخص اینجانب انجام و صحت و اصالت مطالب تدوین شده در آن، مورد تأیید است و چنان چه هر زمان، دانشگاه کسب اطلاع کند که گزارش پایان نامه حاضر صحت و اصالت لازم را نداشته، دانشگاه حق دارد، مدرک تحصیلی اینجانب را مسترد و ابطال نماید هم چنین اعلام می دارد در صورت بهره گیری از منابع مختلف شامل؛ گزارش های تحقیقاتی، رساله، پایان نامه، کتاب، مقالات تخصصی و غیره، به منبع مورد استفاده و پدید آورنده آن به طور دقیق ارجاع داده شده و نیز مطالب مندرج در پایان نامه حاضر تاکنون برای دریافت هیچ نوع مدرک یا امتیازی توسط اینجانب و یا سایر افراد به هیچ کجا ارایه نشده است. در تدوین متن پایان نامه حاضر، چارچوب (فرمت) مصوب تدوین پایان‌نامه‌های پژوهشی تحصیلات تکمیلی دانشگاه شاهد به طور کامل مراعات شده و نهایتاً این که، کلیه حقوق مادی ناشی از گزارش پایان نامه حاضر، متعلق به دانشگاه شاهد می باشد.

نام و نام خانوادگی دانشجو(دست نویس):.....

امضاء دانشجو:

تاریخ:

تقدیم

به مهربان فرشتگانی که

لحظات باور بودن، لذت و غرور داشتن، جسارت خواستن، عظمت رویش و تمام تجربه‌های یکتا و زیبانگاری که هم‌اکنون حضور در میان آن‌ها است...

تقدیم به

دامان سبز مادر

و دست‌های خسته پدرم

دو عشق پاک زندگی‌ام

و تقدیم به

خواهران عزیزم که وجودشان شادی‌بخش و صفاشان پایدار من است.

تشکر و قدردانی

سپاس بیکران پروردگار یکتا را که هستی‌مان بخشید و به طریق علم و دانش رهنمون‌مان شد و به همنشینی رهروان علم و دانش مفتخرمان نمود و خوشه‌چینی از علم و معرفت را روزی‌مان ساخت.

از استاد راهنمای گرانقدر سرکار خانم دکتر مریم‌زاده که علاوه بر آموزش علم، منش زندگی و مدیریت را به من آموختند و نام و یادشان در ذهن ما خواهد بود کمال تشکر را دارم و برای ایشان آرزوی سلامتی و سعادت و توفیق روز افزون از خداوند متعال خواستارم.

از اساتید محترم جناب آقای دکتر بهراد و جناب آقای دکتر مه‌آبادی که زحمت داوری این پایان‌نامه را متقبل شدند و همچنین جناب آقای دکتر نیک‌بهادلی که با حضور به عنوان نماینده تحصیلات تکمیلی کمال تشکر را دارم.

از جناب آقای مهندس حمید عادل‌جواد که تجربیات خود را در اختیارم قرار دادند، تشکر می‌کنم و برای ایشان آرزوی موفقیت می‌کنم.

از پژوهشگاه دانش‌های بنیادی برای مساعدت در تسریع اجرای برنامه‌ها نیز سپاسگزارم.

چکیده

در این پژوهش، روش‌هایی برای پنهان‌نگاری مقاوم تصاویر رنگی در برابر نهان‌کاوی پیشنهاد شده است که سعی در برقراری تعادل بین سه عامل ظرفیت، نامحسوس بودن و مقاومت را دارند. ابتدا یک روش مقاوم برای پنهان‌نگاری اطلاعات در تصاویر رنگی با استفاده از فضاهای رنگ YUV و YCbCr پیشنهاد شده است. در این روش به دلیل استفاده از ضرایب تبدیلات، مقاومت در برابر حملات نهان‌کاوی افزایش یافته است و استفاده از دو کانال به منظور تعبیه اطلاعات باعث افزایش ظرفیت شده است. در روش پیشنهادی دوم و سوم به ترتیب از اطلاعات فضای رنگ RGB و YUV به منظور تعبیه اطلاعات استفاده شده است. در این روش‌ها به منظور کاهش تخریب تصویر گنجانه و افزایش مقاومت در برابر نهان‌کاوی، ترتیب بیت‌های پیام توسط تئوری آشوب به هم ریخته می‌شود؛ پس از تعبیه پیام به هم ریخته، مسأله به صورت یک مسأله بهینه‌سازی چندهدفه تبدیل می‌شود که اهداف آن‌ها (مقاومت و نامحسوس بودن در مورد فضای رنگ RGB و مقاومت، نامحسوس بودن و کاهش خطا در مورد فضای رنگ YUV) از ملزومات سیستم پنهان‌نگاری هستند. بهینه‌سازی اهداف در فضای رنگ RGB بر اساس روش جمع وزنی اهداف و در فضای رنگ YUV بر اساس الگوریتم NSGA-II انجام می‌شود. برای ارزیابی مقاومت در روش پیشنهادی دوم و سوم نیز، روشی مبتنی بر استخراج ویژگی در فضای رنگ YIQ اقتباس شده است. نتایج نشان می‌دهد که فضای جستجو به دلیل استفاده از تئوری آشوب بزرگ است و بهبود جزئی اهداف به دلیل بزرگ بودن فضای جستجو تحقق یافته است. عملکرد الگوریتم NSGA-II نیز به منظور بهینه‌سازی چندهدفه بر اساس ارزیابی معیارهای کارایی مطلوب است.

کلید واژه: پنهان‌نگاری، نهان‌کاوی، تئوری آشوب، الگوریتم ژنتیک، الگوریتم NSGA-II

فهرست مطالب

عنوان **صفحه**

فهرست جدول‌ها ..... ه
فهرست شکل‌ها ..... و
فهرست الگوریتم‌ها ..... ح

فصل ۱- مقدمه ۱
۱-۱- پیشگفتار ۱
۱-۲- تاریخچه پنهان‌نگاری اطلاعات ۲
۱-۳- شیوه‌های نوین و بررسی نقاط ضعف و قوت روش‌ها ۳
۱-۴- هدف از انجام پژوهش ۴
۱-۵- پایان‌نامه در یک نگاه و نوآوری پژوهش ۵
۱-۶- ساختار پایان‌نامه ۵

فصل ۲- پنهان‌نگاری و نهان‌کاوی ۶
۲-۱- مقدمه ۶
۲-۲- پنهان‌نگاری ۶
۲-۲-۱- مدل اصلی پنهان‌نگاری ۷
۲-۲-۲- مسائل طراحی سیستم پنهان‌نگاری ۹
۲-۲-۳- ویژگی‌های سامانه پنهان‌سازی اطلاعات ۱۱
۲-۲-۴- ترکیب پنهان‌نگاری با روش‌های دیگر ۱۲
۲-۲-۵- کاربردهای پنهان‌نگاری ۱۳
۲-۳- آب‌نشانی و تفاوت آن با پنهان‌نگاری ۱۳
۲-۴- مقایسه بین پنهان‌نگاری، آب‌نشانی و رمزنگاری ۱۴
۲-۵- نهان‌کاوی ۱۵
۲-۵-۱- معیارهایی برای نهان‌کاوی، ماتریس اغتشاش و منحنی ROC ۱۶
۲-۵-۲- طبقه‌بندی الگوریتم‌های نهان‌کاوی ۱۸
۲-۵-۳- چالش‌های نهان‌کاوی ۱۹
۲-۵-۴- انواع حملات در نهان‌کاوی ۱۹
۲-۵-۴-۱- حملات مربوط به تجزیه و تحلیل رمز ۲۰
۲-۵-۴-۲- حملات مرتبط با نهان‌کاو ۲۰
۲-۶- جمع‌بندی ۲۱

فصل ۳- مروری بر روش‌های پنهان‌نگاری و بررسی انواع روش‌های پنهان‌نگاری در تصاویر رنگی..... ۲۲
۳-۱- مقدمه ۲۲

۳-۲- مروری بر روش‌های پنهان‌نگاری ۲۲
۳-۳- روش‌های پنهان‌نگاری متداول ۲۳
۳-۳-۱- پنهان‌نگاری در حوزه مکان ۲۳
۳-۳-۱-۱- پنهان‌نگاری مبتنی بر کم‌ارزش‌ترین بیت‌ها ۲۳
۳-۳-۱-۲- پنهان‌نگاری مبتنی بر اضافه کردن نویز ۳۰
۳-۳-۱-۳- پنهان‌نگاری داده در اختلاف مقادیر پیکسل‌ها ۳۱
۳-۳-۲- روش‌های پنهان‌نگاری در حوزه تبدیل ۳۳
۳-۳-۲-۱- روش‌های پنهان‌نگاری JPEG ۳۴
۳-۴- روش‌های پنهان‌نگاری در تصاویر رنگی ۳۸
۳-۴-۱- سیستم بینایی انسان ۳۸
۳-۴-۲- مبانی رنگ ۳۹
۳-۴-۳- مدل‌های رنگ ۴۰
۳-۴-۳-۱- مدل رنگ RGB ۴۰
۳-۴-۳-۲- مدل‌های رنگ CMY و CMYK ۴۱
۳-۴-۳-۳- مدل‌های رنگ HSI، YIQ، YCbCr و YUV ۴۱
۳-۴-۴- تبدیل مدل رنگ RGB به مدل‌های رنگ دیگر و برعکس ۴۲
۳-۴-۵- روش پنهان‌نگاری Triple-A ۴۵
۳-۴-۶- روش پیکسل نماینده برای پنهان‌نگاری تصاویر RGB ۴۶
۳-۴-۷- پنهان‌نگاری بیت‌های متغیر مبتنی بر شدت روشنایی تصاویر RGB ۴۸
۳-۴-۸- پنهان‌نگاری تصویر رنگی با استفاده از اختلاف کانال و توزیع پیام مخفی ۴۹
۳-۴-۹- پنهان‌نگاری در فضای رنگ YUV ۵۲
۳-۴-۱۰- پنهان‌نگاری مقاوم اطلاعات در تصاویر رنگی با استفاده از اطلاعات فضاهای رنگ مختلف ۵۳
۳-۴-۱۱- روش پنهان‌نگاری با ظرفیت بالا برای تصاویر خاکستری و رنگی ۵۳
۳-۵- جمع‌بندی ۵۵

فصل ۴- مفاهیم بهینه‌سازی و به‌کارگیری الگوریتم ژنتیک در پنهان‌نگاری ۵۶

۴-۱- مقدمه ۵۶
۴-۲- مفاهیم کلی بهینه‌سازی چندهدفه ۵۷
۴-۳- بهینه‌سازی چندهدفه با استفاده از الگوریتم‌های تکاملی ۵۹
۴-۳-۱- الگوریتم ژنتیک با مرتب‌سازی نامغلوب (NSGA-II) ۶۱
۴-۳-۱-۱- روش مرتب‌سازی سریع نامغلوب (fast non-dominated sorting) ۶۴
۴-۳-۱-۲- حفظ تنوع ۶۶
۴-۳-۱-۳- حلقه اصلی الگوریتم NSGA-II ۶۷
۴-۴- روش‌های پنهان‌نگاری بر اساس الگوریتم ژنتیک ۶۸
۴-۴-۱- پنهان‌نگاری امن تصاویر JPEG با استفاده از الگوریتم ژنتیک ۷۰
۴-۴-۲- روش پنهان‌نگاری نامحسوس بر اساس الگوریتم ژنتیک ۷۱
۴-۴-۳- پنهان‌نگاری بیت کم‌ارزش تطبیقی بهبودیافته بر اساس آشوب و الگوریتم ژنتیک ۷۲

۴-۴-۴- پنهان‌نگاری به کمک الگوریتم ژنتیک و تشخیص گوشه ۷۵
۴-۵- جمع‌بندی ۷۷

فصل ۵- روش‌های پنهان‌نگاری پیشنهادی ۷۸
۵-۱- مقدمه ۷۸
۵-۲- روش پنهان‌نگاری پیشنهادی اول با استفاده از فضای رنگ YUV و YCbCr ۷۸
۵-۳- روش پیشنهادی دوم بر مبنای الگوریتم ژنتیک و تئوری آشوب در فضای رنگ RGB ۸۱
۵-۳-۱- تئوری آشوب و چگونگی عملکرد آن برای به هم ریختن ترتیب بیت‌های پیام ۸۲
۵-۳-۲- چگونگی بررسی اهداف (مقاومت و PSNR) در روش پیشنهادی دوم ۸۴
۵-۳-۳- بهینه‌سازی اهداف بر اساس رویکرد جمع وزنی ۸۶
۵-۳-۴- به کارگیری الگوریتم ژنتیک در روش پیشنهادی دوم ۸۶
۵-۴- روش پیشنهادی سوم بر مبنای الگوریتم ژنتیک با مرتب‌سازی نامغلوب (NSGA-II) و تئوری آشوب ۸۹
۵-۴-۱- چگونگی بررسی اهداف (مقاومت، PSNR و خطا) در روش پیشنهادی سوم ۹۰
۵-۴-۲- به کارگیری الگوریتم ژنتیک با مرتب‌سازی نامغلوب (NSGA-II) در روش پیشنهادی سوم ۹۰
۵-۵- جمع‌بندی ۹۳

فصل ۶- نتایج روش‌های پیشنهادی ۹۴
۶-۱- مقدمه ۹۴
۶-۲- نتایج روش پنهان‌نگاری پیشنهادی به منظور صفر کردن BER در دو فضای رنگ YUV و YCbCr ۹۴
۶-۲-۱- نتایج صفر شدن BER ۹۴
۶-۲-۲- نتایج نهان‌کاوی ۹۵
۶-۲-۳- ارزیابی کیفیت تصاویر ۱۰۰
۶-۳- نتایج روش پنهان‌نگاری بر مبنای الگوریتم ژنتیک و تئوری آشوب در تصاویر RGB ۱۰۱
۶-۳-۱- نتایج بهبود اهداف به صورت مجزا ۱۰۱
۶-۳-۲- نتایج بهبود جمع وزنی اهداف ۱۰۳
۶-۴- نتایج روش پنهان‌نگاری بر مبنای الگوریتم NSGA-II وتئوری آشوب در تصاویر YUV ۱۰۴
۶-۴-۱- ارزیابی معیارهای کارایی ۱۰۵
۶-۵- جمع‌بندی ۱۱۰

فصل ۷- نتیجه‌گیری و موضوعاتی برای تحقیق بیشتر ۱۱۲
۷-۱- مقدمه ۱۱۲
۷-۲- موضوعاتی برای تحقیق بیشتر ۱۱۳

ضمیمه أ - نتایج استخراج ویژگی‌ها برای بررسی مقاومت در تصاویر RGB ۱۱۴

ضمیمه ب - نتایج استخراج ویژگی‌ها برای بررسی مقاومت در تصاویر YUV ۱۱۵

فهرست مراجع..... ۱۱۶
واژه نامه فارسی به انگلیسی ۱۲۱
واژه نامه انگلیسی به فارسی ۱۲۵

فهرست جدول‌ها

عنوان **صفحه**

جدول ۲- ۱- مقایسه پنهان‌نگاری، آب‌نشانی و رمزنگاری ۱۵

جدول ۳- ۱- تخصیص اعداد تصادفی توسط s۱ ۴۶
جدول ۳- ۲- تخصیص اعداد تصادفی توسط s۲ ۴۶
جدول ۳- ۳- ارتباط بین بیت‌های نماینده و میزان داده‌های مخفی ۴۷
جدول ۳- ۴- معیار انتخاب کانال نماینده ۴۷

جدول ۶- ۱- نتایج صفر شدن خطا برای فضای رنگ YUV ۹۵
جدول ۶- ۲- نتایج صفر شدن خطا برای فضای رنگ YCbCr ۹۵
جدول ۶- ۳- نتایج ارزیابی PSNR برای روش پیشنهادی (در دو فضای رنگ YUV و YCbCr) و روش RGB ۱۰۰
جدول ۶- ۴- نتایج بهبود اهداف به صورت مجزا برای نرخ تعبیه ۰.۲ ۱۰۱
جدول ۶- ۵- نتایج بهبود اهداف به صورت مجزا برای نرخ تعبیه ۱ ۱۰۲
جدول ۶- ۶- نتایج بهبود اهداف به صورت مجزا برای نرخ تعبیه ۲ ۱۰۲
جدول ۶- ۷- پارامترهای الگوریتم ژنتیک در روش پیشنهادی دوم ۱۰۳
جدول ۶- ۸- پارامترهای الگوریتم ژنتیک در روش پیشنهادی سوم ۱۰۵
جدول ۶- ۹- مقایسه درصد جواب‌های نامغلوب قبل از اعمال الگوریتم ژنتیک و بعد از اعمال الگوریتم ژنتیک برای سه نرخ تعبیه ۱۰۶
جدول ۶- ۱۰- مقایسه درصد جواب‌های نامغلوب بین دو الگوریتم NSGA-II و NRGA ۱۰۸
جدول ۶- ۱۱- مقایسه معیار MID بین دو الگوریتم NSGA-II و NRGA ۱۰۹

فهرست شکل‌ها

عنوان **صفحه**

شکل ۱- ۱- پنهان کردن کدهای مورس ۳

شکل ۲- ۱- سیستم‌های امنیتی و اجزای مختلف آن ۶
شکل ۲- ۲- فرمت فایل‌های متداول برای پنهان‌نگاری ۷
شکل ۲- ۳- مدل پنهان‌نگاری و نهان‌کاوی ۸
شکل ۲- ۴- مسائل طراحی سیستم پنهان‌نگاری ۹
شکل ۲- ۵- ماتریس اغتشاش ۱۷
شکل ۲- ۶- منحنی ROC ۱۷

شکل ۳- ۱- نمودار RS یک تصویر گرفته شده توسط دوربین دیجیتال ۲۶
شکل ۳- ۲- پیمایش عرضی در روش PVD ۳۱
شکل ۳- ۳- پیمایش عرضی، طولی، زیگزاگ و پادزیگزاگ ۳۳
شکل ۳- ۴- الگوریتم فشرده‌سازی تصویر JPEG ۳۵
شکل ۳- ۵- مقادیر کوانتیزه شده استفاده شده در طرح فشرده سازی JPEG (اجزای شدت روشنایی) ۳۵
شکل ۳- ۶- روند کلی پنهان‌نگاری در تصاویر JPEG ۳۶
شکل ۳- ۷- تشریح B- Block و H- Block در YASS ۳۷
شکل ۳- ۸- یک مقطع افقی از چشم انسان ۳۹
شکل ۳- ۹- مکعب رنگی RGB ۴۱

شکل ۴- ۱- دیاگرام یک تابع یا فرآیند بهینه شده ۵۶
شکل ۴- ۲- تنوع در جمعیت وجود دارد ۵۸
شکل ۴- ۳- تنوع در جمعیت وجود ندارد ۵۹
شکل ۴- ۴- اجزای کلیدی EA ۶۰
شکل ۴- ۵- جبهه‌های نامغلوب بر اساس الگوریتم NSGA ۶۲
شکل ۴- ۶- مکانیزم کلی عملکرد الگوریتم NSGA-II ۶۴
شکل ۴- ۷- محاسبه فاصله ازدحام ۶۶
شکل ۴- ۸- یک کروموزوم با ۶۴ ژن ۷۲
شکل ۴- ۹- فرآیند تعبیه اطلاعات ۷۳
شکل ۴- ۱۰- فرآیند استفاده از GA برای یافتن بهترین جفت ورودی برای نگاشت لوجیستیک ۷۴
شکل ۴- ۱۱- الگوریتم استخراج ۷۵
شکل ۴- ۱۲- الگوریتم تعبیه اطلاعات ۷۶

شکل ۴- ۱۳- الگوریتم استخراج اطلاعات ۷۶

شکل ۵- ۱- حساسیت به شروط اولیه در سیستم آشوب ۸۳
شکل ۵- ۲- فرآیند الگوریتم ژنتیک برای بدست آوردن $(x.,\mu)$ بهینه ۸۸
شکل ۵- ۳- فرآیند تعبیه اطلاعات در روش پیشنهادی دوم ۸۹
شکل ۵- ۴- فلوچارت الگوریتم پیشنهادی روش سوم ۹۲
شکل ۵- ۵- فلوچارت الگوریتم NSGA-II در روش پیشنهادی سوم ۹۳

شکل ۶- ۱- نتایج نهان‌کاوی SP در مورد روش پیشنهادی در فضای رنگ YUV و روش RGB ۹۶
شکل ۶- ۲- نتایج نهان‌کاوی WS در مورد روش پیشنهادی در فضای رنگ YUV و روش RGB ۹۶
شکل ۶- ۳- نمودار PrecisionRate روش نهان‌کاوی SP برای تشخیص روش پیشنهادی در فضای رنگ YUV و روش RGB ۹۷
شکل ۶- ۴- نمودار PrecisionRate روش نهان‌کاوی WS برای تشخیص روش پیشنهادی در فضای رنگ YUV و روش RGB ۹۷
شکل ۶- ۵- نتایج نهان‌کاوی SP در مورد روش پیشنهادی در فضای رنگ YCbCr و روش RGB ۹۸
شکل ۶- ۶- نتایج نهان‌کاوی WS در مورد روش پیشنهادی در فضای رنگ YCbCr و روش RGB ۹۸
شکل ۶- ۷- نمودار PrecisionRate روش نهان‌کاوی SP برای تشخیص روش پیشنهادی در فضای رنگ YCbCr و روش RGB ۹۹
شکل ۶- ۸- نمودار PrecisionRate روش نهان‌کاوی WS برای تشخیص روش پیشنهادی در فضای رنگ YCbCr و روش RGB ۹۹
شکل ۶- ۹- نتیجه بهبود جمع وزنی اهداف برای نرخ تعبیه ۱ در تصویر اول ۱۰۴
شکل ۶- ۱۰- نمودار پیاده‌سازی روش پیشنهادی سوم قبل از اعمال GA در الگوریتم NSGA-II ۱۰۷
شکل ۶- ۱۱- نمودار پیاده‌سازی روش پیشنهادی سوم بعد از اعمال GA در الگوریتم NSGA-II ۱۰۷

فهرست الگوریتم‌ها

عنوان **صفحه**

الگوریتم ۴- ۱- شبه کد الگوریتم NSGA ۶۱
الگوریتم ۴- ۲- شبه کد الگوریتم NSGA-II ۶۳
الگوریتم ۴- ۳- شبه کد روش مرتب‌سازی سریع نامغلوب ۶۵
الگوریتم ۴- ۴- شبه کد محاسبه فاصله ازدحام ۶۶
الگوریتم ۴- ۵- فرآیند نخبه‌گرایی برای یک نسل خاص ۶۸

الگوریتم ۵- ۱- شبه کد الگوریتم تعبیه روش پیشنهادی اول ۸۰

فصل ۱- مقدمه

۱-۱- پیشگفتار

جوامع مختلف همواره به دنبال راه‌های جدید و کارآمد برای برقراری ارتباط هستند. با وجود ارتباطات الکترونیکی، نیازهای جدید و مسائل مختلفی بوجود می‌آیند. در هنگام برقراری ارتباطات، ترجیح می‌دهیم که تنها گیرنده مورد نظر توانایی کشف[۱] محتویات پیام را داشته باشد [۱]. بنابراین امنیت[۲] یکی از فاکتورهای مهم، در فناوری اطلاعات و ارتباطات است [۲].

یک راه حل، رمز کردن[۳] اطلاعات برای پنهان کردن محتویات پیام است [۱] و رمزنگاری[۴] به عنوان روشی برای تأمین امنیت ارتباطات است. متأسفانه گاهی اوقات تنها حفاظت از محتوای پیام کافی نیست و ممکن است لازم باشد که از وجود پیام مخفی نیز حفاظت شود [۲]. بنابراین گاهی اوقات ترجیح می‌دهیم که کل فرآیند ارتباطات از دید هر ناظری، پنهان شود. پنهان‌سازی اطلاعات[۵] به معنای جایگزینی برای رمزنگاری نیست، بلکه به منظور افزایش محرمانه بودن[۶] اطلاعات است. می‌توان تصور کرد که پنهان‌سازی اطلاعات به عنوان ابزار دیگری برای انتقال اطلاعات و فراهم کردن محرمانگی[۷] است [۱].

بنابراین هنگامی که اطلاعات حساس در یک کانال عمومی به اشتراک گذاشته می‌شود، محرمانگی ضروری است و باید فراهم شود. رمزنگاری و پنهان‌نگاری[۸] دو ابزار مهم برای فراهم کردن محرمانگی و حفاظت از اطلاعات حساس هستند. در رمزنگاری اطلاعات به گونه‌ای پنهان می‌شوند که تنها گیرنده مورد نظر توانایی بازیابی اطلاعات را دارد؛ در صورتی که در پنهان‌نگاری، اطلاعات حساس در اسناد (پوشش/ حامل[۹]) مختلف به روش غیر قابل کشف پنهان می‌شوند [۳].

محرمانگی نیز تنها انگیزه برای پنهان‌سازی اطلاعات نیست. با تعبیه یک داده در داده دیگر، دو موجودیت[۱۰] تبدیل به یک موجودیت می‌شوند و بدین ترتیب نیاز به حفظ ارتباط بین اجزای مجزا یا خطر احتمال جدایی آن‌ها از بین می‌رود [۱].

---

۱ Decipher
۲ Security
۳ Encryption
۴ Crytography
۵ Information hiding
۶ Secrecy
۷ Privacy
۸ Steganography
۹ Carrier
۱۰ Entity

سیستم رمزنگاری اطلاعات، از الگوریتم رمزنگاری برای انتقال اطلاعات در متون رمز[۱] شده استفاده می‌کند و تنها کاربر مجاز توانایی رمزگشایی داده‌ها از این متون را دارد. با این وجود، متون رمز شده بی‌معنی به نظر می‌رسند و ممکن است باعث ایجاد شک شوند. اشکال سیستم رمزنگاری این است که شخص ثالث می‌تواند اطلاعات را بازیابی کند یا در هنگام مواجه شدن با مشکل در هنگام بازیابی، آن‌ها را نابود کند [۴].

پنهان کردن اطلاعات مخفی در رسانه‌های پوشش[۲] مانند متن، تصویر، صدا، ویدیو و غیره روشی برای حل این مسأله است. مزیت پنهان‌سازی اطلاعات این است که رسانه گنجانه[۳] (که اطلاعات مخفی در آن تعبیه شده است) مانند داده معمولی به نظر می‌رسد و کسی متوجه وجود اطلاعات مخفی در آن نمی‌شود. بنابراین اطلاعات مخفی به صورت امن منتقل می‌شود [۴].

۱-۲- تاریخچه پنهان‌نگاری اطلاعات

کلمه پنهان‌نگاری از کلمات یونانی"Covered Writing" به معنای نوشته پوشیده شده استخراج شده است و در طول هزاران سال به شکل‌های مختلف مورد استفاده قرار گرفته است. با توسعه اینترنت و پیشرفت‌های مختلف، پنهان‌نگاری به شکل دیجیتالی درآمده است [۵].

پنهان‌سازی اطلاعات علم جدیدی نمی‌باشد. برخی از اولین نمونه‌های مستند را می‌توان در تاریخ هردوتس[۴]، پدر تاریخ در ارتباط با داستان‌های مختلف یونان باستان یافت [۱]. هیستائوس[۵] می‌بایست با پسرخوانده‌اش در یونان ارتباط برقرار می‌کرد. بدین منظور او موی سریکی از مورد اعتمادترین غلامانش را تراشید و پیام را روی پوست سر او خالکوبی کرد و هنگامی که موی سر او به اندازه کافی رشد کرد، او را با پیام مخفی اعزام نمود [۲].

همچنین در یونان باستان، متن را روی قرص‌های چوبی پوشیده شده با موم می‌نوشتند. برای پنهان کردن پیام، موم را می‌تراشیدند و پیام را روی چوب می‌نوشتند و سپس دوباره آن را با موم می‌پوشاندند[۶].

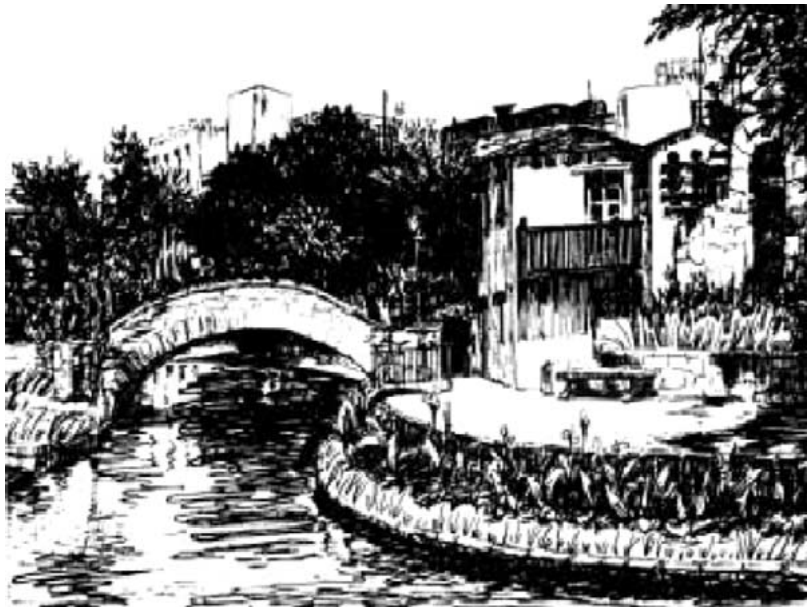
فرم متداول دیگر نوشتن نامحسوس، استفاده از جوهرهای نامرئی بود. چنین جوهرهائی با موفقیت زیاد در جنگ جهانی دوم استفاده می‌شدند [۶].

همچنین در سال ۱۹۴۵، کد مورس[۶] در یک نقاشی مطابق شکل ۱-۱ پنهان شده بود. اطلاعات مخفی در علف‌های کنار رودخانه کدگذاری شده‌اند. علف‌های بلند نشان‌دهنده خطوط و علف‌های کوتاه نشان‌دهنده نقاط هستند و پیام رمزگشایی شده به این صورت است [۵].

---

[۱] Cipher texts
[۲] Cover media
[۳] Stego media
[۴] Herodotus
[۵] Histaeus
[۶] Morse

"Compliments of CPSA MA to our chief Col Harold R. Shaw on his visit to San Antonio May ۱۱ th ۱۹۴۵"



شکل ۱- ۱- پنهان کردن کدهای مورس [۵]

۱-۳- شیوه‌های نوین و بررسی نقاط ضعف و قوت روش‌ها

بیشتر روش‌های پنهان‌نگاری در تصاویر رنگی از فضای رنگ RGB به منظور تعبیه اطلاعات استفاده می‌کنند و تاکنون تحقیقات زیادی در این زمینه انجام شده است. پنهان‌نگاری در فضای رنگ RGB به دلیل اینکه نیاز به تبدیل فضا ندارد، از پیچیدگی محاسباتی کمی برخوردار است و کیفیت تصاویر نیز در این روش نسبت به روش‌های پنهان‌نگاری در فضاهای رنگ غیر از RGB بالاتر است. همچنین مقدار خطا در تصاویر RGB صفر است و اطلاعات به صورت کامل قابل بازیابی هستند. اما مشکل پنهان‌نگاری در تصاویر RGB مقاومت[۱] کم آن‌ها در برابر حملات نهان‌کاوی[۲] است.

در مقابل تحقیقات کمتری در مورد پنهان‌نگاری در فضاهای رنگ غیر از RGB انجام شده است. برای مثال روش‌های پنهان‌نگاری در [۴۲،۴۳و۴۶] از تعبیه اطلاعات در فضاهای رنگ غیر از RGB بهره می‌برند. پنهان‌نگاری در فضاهای رنگ غیر از RGB به دلیل استفاده از ضرایب تبدیلات دارای مقاومت بیشتری در برابر حملات نهان‌کاوی است. اما مشکل اصلی این روش، وجود خطا در هنگام بازیابی اطلاعات است و به همین منظور امکان بازیابی کامل اطلاعات در این روش‌ها وجود ندارد. مشکل عدم بازیابی کامل اطلاعات هم‌چنان در روش‌های [۴۲و۴۳] وجود دارد. اما در [۴۶] یک روش تصحیح خطا در هنگام کدینگ پیشنهاد شده است که خطا در هنگام بازیابی اطلاعات را در دو فضای رنگ YUV و YCbCr به صفر می‌رساند. در تمام روش‌های مذکور در پنهان‌نگاری فضای رنگ غیر از RGB، از یک

---

[۱] Robustness

[۲] Steganalysis

کانال به منظور تعبیه استفاده شده است و به همین دلیل ظرفیت[۱] تعبیه اطلاعات در این روش‌ها کم است. همچنین کیفیت تصاویر در پنهان‌نگاری فضاهای رنگ غیر از RGB به دلیل استفاده از ضرایب تبدیلات در مقایسه با روش‌های پنهان‌نگاری در فضای رنگ RGB کمتر است.

الگوریتم ژنتیک (GA)[۲]، روشی مؤثر برای بهینه‌سازی در بسیاری از مسائل پنهان‌سازی اطلاعات است و برای بهینه‌سازی نیازهایی که اساساً با هم متضاد هستند مانند (نامحسوس بودن[۳]، امنیت و مقاومت) استفاده می‌شود [۵۶]. در [۸] روش پنهان‌نگاری بر اساس تئوری آشوب[۴] و الگوریتم ژنتیک ارائه شده است که در آن، تخریب تصویر گنجانه از طریق پیدا کردن بهترین نگاشت بین پیام مخفی و تصویر پوشش به حداقل می‌رسد. در این روش ترتیب بیت‌های پیام توسط تئوری آشوب به هم ریخته می‌شود که پارامترهای آن قبلاً به‌وسیله الگوریتم ژنتیک تنظیم شده است. در [۶۶] نیز، روشی مشابه روش [۸] پیشنهاد شده است که از تئوری آشوب و الگوریتم ژنتیک برای افزایش کیفیت و امنیت استفاده می‌شود. در این روش با توجه به اینکه سیستم بینایی انسان به تغییرات در مناطق گوشه نسبت به مناطق غیر گوشه حساسیت کمتری دارد، ابتدا نواحی گوشه شناسایی می‌شود و سپس بیت‌های به هم ریخته پیام به نسبت متفاوت (تعبیه بیشتر در نواحی گوشه) در مناطق گوشه و غیر گوشه تعبیه می‌شوند.

با توجه به اینکه سیستم آشوب به شرایط اولیه بسیار حساس است و تغییری اندک در شرایط اولیه باعث ایجاد نتایج بسیار متفاوت می‌شود، فضای جستجو در تئوری آشوب بزرگ است و امکان جستجوی محلی وجود ندارد. به همین دلیل بهبود مورد نظر در روش‌های مذکور به کمک تئوری آشوب کمتر از حد انتظار است.

در روش‌های مذکور به کمک الگوریتم ژنتیک و تئوری آشوب، تصاویر خاکستری به عنوان تصویر پوشش مورد استفاده قرار می‌گیرند و تنها معیار ماکزیمم نسبت سیگنال به نویز (PSNR)[۵] به عنوان برازش در نظر گرفته شده است.

۱-۴- هدف از انجام پژوهش

هدف از انجام پژوهش استفاده از فضاهای رنگ غیر از RGB (YUV و YCbCr) به منظور تعبیه اطلاعات برای افزایش مقاومت در برابر حملات نهان‌کاوی و افزایش ظرفیت تعبیه با بهره‌گیری از تعبیه اطلاعات در بیش از یک کانال است. همچنین بازیابی کامل و بدون خطای اطلاعات از جمله اهداف پنهان‌نگاری در فضاهای رنگ YUV و YCbCr است.

هدف دیگر این پژوهش، استفاده از ترکیب الگوریتم ژنتیک و تئوری آشوب در فضای رنگ RGB و YUV به منظور افزایش امنیت و کیفیت تصویر گنجانه با در نظر گرفتن مسأله به صورت یک مسأله

---

[۱] Capacity

[۲] Genetic Algorithm

[۳] Imperceptibility

[۴] Chaos

[۵] Peak-signal-to-noise ratio

بهینه‌سازی چندهدفی است. اهداف مورد نظر از ملزومات سیستم پنهان‌نگاری مانند (کیفیت، نامحسوس بودن و کاهش خطا در مورد تصاویر YUV) هستند که بهینه‌سازی همزمان آن‌ها به کمک روش‌های چندهدفی مانند روش جمع وزنی اهداف و روش الگوریتم ژنتیک با مرتب‌سازی نامغلوب (NSGA-II)[1] انجام می‌شود.

ارزیابی مقاومت بر اساس استخراج و تحلیل رفتار ویژگی‌ها از فضای رنگ YIQ مبتنی بر روش [۴۶]، از جمله اهداف دیگر این پژوهش می‌باشد.

۱-۵- پایان‌نامه در یک نگاه و نوآوری پژوهش

در این پایان‌نامه با بهره‌گیری از فضاهای رنگ غیر از RGB مانند YUV و YCbCr روشی مقاوم[2] برای پنهان‌نگاری تصاویر رنگی پیشنهاد شده است که مقاومت آن در برابر نهان‌کاوی در مقایسه با فضای رنگ RGB بیشتر است و اطلاعات نیز بدون خطا قابل استخراج هستند.

همچنین از ترکیب الگوریتم ژنتیک و تئوری آشوب برای افزایش کیفیت تصویر گنجانه و کاهش تخریب آن بهره گرفته شده است. در نظر گرفتن مسأله پنهان‌نگاری به صورت یک مسأله بهینه‌سازی چندهدفه[3] که اهداف آن از ملزومات سیستم پنهان‌نگاری هستند و بهینه‌سازی اهداف بر اساس روش‌های چندهدفی مانند روش جمع وزنی اهداف و الگوریتم NSGA-II از جمله نوآوری این پژوهش می‌باشد.

تحلیل رفتار ویژگی‌ها در فضای رنگ YIQ برای ارزیابی مقاومت روش‌های پیشنهادی دوم و سوم و سنجش مقاومت بر اساس رفتار آن‌ها از جمله نوآوری دیگر این پژوهش می‌باشد.

۱-۶- ساختار پایان‌نامه

ساختار پایان‌نامه به صورت زیر است:

در فصل اول، مقدمه شامل تاریخچه پنهان‌نگاری اطلاعات، شیوه‌های نوین و بررسی نقاط ضعف و قوت روش‌ها، هدف از انجام پژوهش و نوآوری پژوهش تشریح شد. در فصل دوم مفاهیم پنهان‌نگاری و نهان‌کاوی مورد بررسی قرار می‌گیرد. فصل سوم شامل مروری بر روش‌های پنهان‌نگاری و بررسی انواع روش‌های پنهان‌نگاری در تصاویر رنگی است. مفاهیم بهینه‌سازی و به کارگیری الگوریتم ژنتیک در پنهان‌نگاری در فصل چهارم مورد بحث قرار می‌گیرد. روش‌های پنهان‌نگاری پیشنهادی به تفضیل در فصل پنجم تشریح می‌شوند. نتایج روش‌های پیشنهادی و نتیجه‌گیری نیز به ترتیب در فصل ششم و هفتم مورد بررسی قرار می‌گیرند.

[1] Non-dominated sorting genetic algorithm

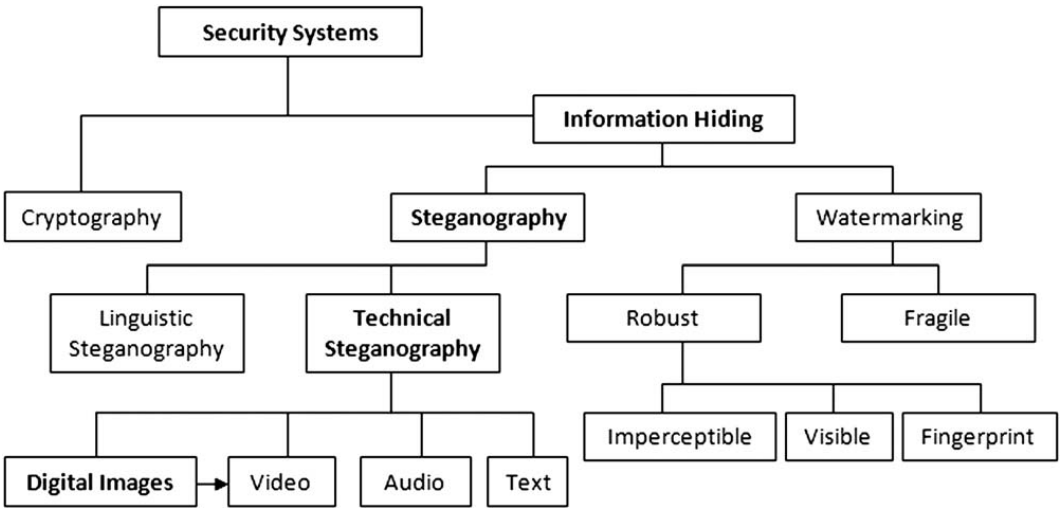
[2] Robust

[3] Multiobjective optimization

فصل ۲- پنهان‌نگاری و نهان‌کاوی

۲-۱- مقدمه

سیستم‌های امنیتی به دو دسته پنهان‌سازی اطلاعات و رمزنگاری تقسیم می‌شوند و پنهان‌سازی اطلاعات نیز شامل پنهان‌نگاری و آب‌نشانی[۱] است. پنهان‌نگاری و آب‌نشانی مفاهیم بسیار نزدیک به یکدیگر هستند و تفکیک حوزه آن‌ها از یکدیگر پیچیده می‌باشد [۵]، اما به صورت کلی دارای اهداف متفاوتی هستند. رمزنگاری نیز برای حفاظت از محتوا استفاده می‌شود و وجود پیام را پنهان نمی‌کند. شکل ۲-۱ ساختار کلی سیستم‌های امنیتی و فرآیند تفکیک سه مفهوم پنهان‌نگاری، آب‌نشانی و رمزنگاری و حوزه فعالیت هر یک را نشان می‌دهد.



شکل ۲- ۱- سیستم‌های امنیتی و اجزای مختلف آن [۵]

بر اساس شکل ۲-۱، پنهان‌نگاری به دو دسته پنهان‌نگاری تکنیکی و پنهان‌نگاری زبان‌شناختی تقسیم می‌شود و پنهان‌نگاری تکنیکی نیز به کمک تصاویر دیجیتالی، فایل‌های ویدیویی، فایل‌های صوتی و متون انجام می‌گیرد. آب‌نشانی نیز به دو دسته مقاوم و شکننده[۲] تقسیم می‌شود. با توجه به موضوع پژوهش، در ادامه پنهان‌نگاری اطلاعات و مباحث مربوط به آن تشریح می‌شوند. همچنین مفهوم آب‌نشانی و کاربردهای آن به صورت مختصر بیان می‌شوند.

۲-۲- پنهان‌نگاری

پنهان‌نگاری روشی مؤثر برای حفاظت از اطلاعات محرمانه است و نقش مهمی در به اشتراک‌گذاری اطلاعات محرمانه بازی می‌کند. این کار به وسیله پنهان کردن داده‌ها در رسانه‌های مختلف به روشی که

[۱] Watermarking

[۲] Fragile