

بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيمِ

عنوان

مطالعه و ارزیابی روش‌های استگنوگرافی تطبیقی تصاویر

صفحه	فهرست مطالب	عنوان
۷	چکیده
فصل اول: کلیات تحقیق		
۹	۱-۱- مقدمه
۱۰	۲-۱- بیان مسئله
۱۱	۳-۱- اهمیت و ضرورت انجام تحقیق
۱۱	۴-۱- اهداف مشخص تحقیق
۱۱	۴-۱- فرضیه‌های تحقیق
فصل دوم: مطالعه پایه‌ای تحقیق		
۱۳	۱-۲- مقدمه
۱۴	۲-۲- معیارهای یک سیستم پنهان‌سازی اطلاعات
۱۵	۳-۲- ساختار سیستم‌های پنهان‌سازی اطلاعات
۱۶	۴-۲- پنهان‌نگاری
۱۷	۵-۲- تاریخچه پنهان‌نگاری
۱۸	۶-۲- تعاریف اولیه پنهان‌نگاری
۲۰	۷-۲- کلمات و اصطلاحات
۲۰	۸-۲- شاخص‌های مطرح در پنهان‌نگاری
۲۰	۹-۲- شکل‌های مختلف پنهان‌نگاری
۲۲	۱۰-۲- طبقه‌بندی روش‌های پنهان‌نگاری براساس حوزه جاسازی
۲۳	۱-۱۰-۲- تکنیک‌های حوزه مکان
۲۳	۲-۱۰-۲- تکنیک‌های حوزه تبدیل
۲۴	۱۱-۲- تشریح تکنیک‌های پنهان‌نگاری
۲۴	۱۲-۲- تکنیک‌های پنهان‌نگاری تصویر
۲۵	۱-۱۲-۲- فضای دامنه
۲۵	۲-۱۲-۲- پوشش و فیلتر
۲۵	۳-۱۲-۲- دامنه انتقال

۲۵تکنیک اعوجاج ۴-۱۲-۲
۲۶استفاده از سیستم فازی در پنهان‌نگاری ۱۳-۲
۲۷جمع‌بندی ۱۴-۲

فصل سوم: روش‌های انجام شده برای پنهان‌نگاری

۲۹مقدمه ۱-۳
۳۰روش‌های پنهان‌نگاری تصاویر ۲-۳
۳۰پنهان‌نگاری تصویر با استفاده از انتقال دامنه فازی و طبقه‌بندی پیکسل ۱-۲-۳
۳۱ویژگی کاوی و سیستم استنتاج عصبی - فازی برای پنهان‌نگاری LSB تطبیق ۲-۲-۳
۳۱یک روش جاسازی پنهان‌نگاری مبتنی بر شناسایی لبه و کدنویسی XOR ۳-۲-۳
۳۱پنهان‌نگاری تطبیقی تصویر با استفاده از تکنیک درون‌یابی و فشرده‌سازی AMBTC ۴-۲-۳
۳۱پنهان‌نگاری مکانی با حفظ خصوصیات آماری تصویر ۵-۲-۳
۳۲روش پنهان‌نگاری مقاوم در برابر حمله‌ی RS مبتنی بر الگوریتم ژنتیک ۶-۲-۳
۳۲پوشش بین پنهان‌نگاری و منطق فازی برای جاسازی اطلاعات بالا و امنیت بیشتر ۷-۲-۳
۳۳بحث و بررسی ۳-۳
۳۴جمع‌بندی ۴-۳

فصل چهارم: نتیجه‌گیری و پیشنهادات

۳۵نتیجه‌گیری و پیشنهادات ۱-۴
۳۶	مراجع

فهرست اشکال

- شکل ۱-۲- ساختار کلی گنجاننده اطلاعات ۱۵
- شکل ۲-۲- ساختار کلی استخراج کننده اطلاعات با استفاده از رسانه اصلی ۱۶
- شکل ۳-۲- چارچوب پنهان‌نگاری کلید امن ۱۹
- شکل ۴-۲- انواع قالب های مورد استفاده در پنهان‌نگاری ۲۱
- شکل ۵-۲- طبقه‌بندی روش‌های پنهان‌نگاری براساس حوزه جاسازی ۲۲

فهرست جداول

- جدول ۱-۲- برخی اصطلاحات سیستم‌های امنیتی..... ۲۱
- جدول ۲-۲- مقایسه تکنیک‌های مطرح در حوزه مکان و فرکانس..... ۲۳

چکیده

هدف پنهان‌نگاری، برقراری ارتباط امن به صورت کاملاً غیر آشکار می‌باشد. در واقع یک سیستم پنهان‌نگاری باید به گونه‌ای اطلاعات محرمانه را در یک حامل رسانه‌ای مانند (صوت، تصویر، ویدئو و غیره) پنهان کند که هیچ تغییر محسوسی در رسانه ایجاد نشده و شنود کننده غیر مجاز کانال (حمله کننده) نتواند به وجود اطلاعات سری پی ببرد. با این حال، تشخیص وجود پیام محرمانه در حامل با استفاده از الگوریتم‌های آشکارسازی امکان پذیر است. لازم به ذکر است، اگر الگوریتمی بتواند با نرخ موفقیتی بیش از حدس تصادفی فقط حضور پیام را مشخص نماید سیستم پنهان‌نگاری شکسته شده است. پنهان‌نگاری اطلاعات، روشی است که می‌توان اطلاعات مورد نظر را در قالب یک عامل پوشاننده و با بیشترین میزان دقت به امنیت، بین نقاط مورد نظر جابجا نمود، به گونه‌ای که حتی اگر در طی مسیر، اطلاعات از طریق افراد غیرمجاز مورد دسترسی قرار گرفت امکان دستیابی به داده‌های پنهان شده وجود نداشته باشند. در پنهان‌نگاری هدف اصلی، امنیت به معنای عدم توانایی در اثبات وجود پیغام است. بسیاری از روش‌های موجود از روش‌های رایج برای پنهان‌نگاری تصویر استفاده می‌کنند، که حملات برای شکستن پیام مخفی در این مورد مطرح می‌شود. روش‌های متعددی برای پنهان‌نگاری ارائه شده است، استفاده از روش لبه‌یابی می‌تواند به افزایش ظرفیت مخفی‌سازی و امنیت داده برای پنهان کردن اطلاعات کمک کند؛ در این سمینار ابتدا به بحث مربوط به پنهان‌نگاری پرداخته و سپس روش‌های ارائه شده برای پنهان‌نگاری تطبیقی را مورد مطالعه قرار می‌دهیم.

واژه‌های کلیدی: پنهان‌نگاری، لبه‌یابی، جاسازی، تصویر، تطبیقی.

فصل اول

کلیات تحقیق

از دیرباز با برقراری ارتباطات، انسان‌ها در پی یافتن راهی برای برقراری ارتباط محرمانه بوده‌اند. امروزه گسترش روزافزون اینترنت و ابزار دیجیتال، انسان‌ها را به سوی برقراری ارتباط از طریق داده‌های باینری در کانال ناامن اینترنت سوق داده است. از این روی امنیت ارتباطات یک نیاز مهم و اساسی محسوب می‌شود. از جمله راه‌های تامین امنیت رمزنگاری و پنهان‌نگاری است. در رمزنگاری اطلاعات به صورتی رمز می‌شوند که برای سایر افراد قابل فهم نباشد، اما فرستنده و گیرنده با استفاده از یک کلید مشترک می‌توانند اطلاعات موردنظر را رمزگشایی کنند. در پنهان‌نگاری علاوه بر مخفی ماندن اطلاعات، وجود ارتباط محرمانه نیز باید مخفی بماند. در پنهان‌نگاری دانش تحلیل پنهان‌نگاری که هدف آن تمیز دادن بین رسانه‌های حاوی اطلاعات از رسانه‌های عادی است، بسیار مهم است. همانطور که پنهان‌نگاری از اهمیت بالایی برخوردار است، داشتن دانش تحلیل آن نیز بسیار مهم است چرا که علی‌رغم امتیازهای مثبتی که پنهان‌نگاری دارد، امکان سوء استفاده از آن برای مقاصد خرابکارانه نیز وجود دارد. لذا داشتن شناخت کافی از پنهان‌نگاری و دانش تحلیل آن بسیار مهم است. روش‌های متعددی برای پنهان‌نگاری در تصویر ارائه شده‌اند که این روش‌ها بیت‌های اطلاعات را در حوزه مکان و یا حوزه تبدیل تصویر پوشا جاسازی می‌کنند. در این گزارش علم پنهان‌سازی اطلاعات در تصاویر دیجیتالی مورد بررسی قرار گرفت. این علم با چالش‌های مختلف مانند افزایش کیفیت تصویر خروجی و افزایش ظرفیت ذخیره‌سازی و از همه مهمتر، کاهش آنورمالی‌های آماری تصویر خروجی به منظور کاهش احتمال پنهان شکنی مواجه می‌باشد. انواع روش‌های پنهان‌نگاری برای تصویر و رسانه‌های دیگر توسط محققان این حیطه ارائه شده که هر یک ویژگی‌های مثبت و منفی خاص خود را دارند. امروزه از روش‌های بسیار پیشرفته و در حوزه‌های مختلف استفاده می‌شود که حوزه‌ی تصاویر دیجیتال یکی از آن حوزه‌ها می‌باشد. با توجه به اینکه امروزه روش‌های زیادی برای ارسال امن اطلاعات در بستر فضای مجازی وجود دارد استفاده از روش‌های پنهان‌نگاری می‌تواند کمک شایانی جهت ارسال و دریافت داده‌ها نمایند به علاوه اینکه این تکنیک می‌تواند به گونه‌ای ارسال شود که فقط افراد فرستنده و گیرنده قابلیت استخراج اطلاعات را داشته باشند. و از طرفی قابلیت تغییر اصل داده به راحتی امکان پذیر نباشد.