
بسم الله الرحمن الرحيم

سمینار

عنوان

روش‌های پنهان‌نگاری تصاویر

نگارنده

فهرست مطالب

عنوان | **صفحه**

فصل سوم: روش‌های انجام شده برای پنهان نگاری

فصل چهارم: نتیجه‌گیری و پیشنهادات

فهرست اشکال

فهرست جداول

چکیده

هدف پنهان‌نگاری، برقراری ارتباط امن به صورت کاملا 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 موردنظر 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. در این سمینار ابتدا به بحث مربوط به پنهان‌نگاری پرداخته و سپس روش‌های ارائه شده برای پنهان‌نگاری تصاویر را مورد مطالعه قرار می‌دهیم.

واژه‌های کلیدی: پنهان‌نگاری، حملات، جاسازی، تصویر، پیکسل.

فصل اول

مقدمه

۱-۱- مقدمه

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 علی رغم 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 شده اند 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 ذخیره سازی 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 روش های بسیار پیشرفته و در حوزه‌های مختلف استفاده می‌شود که حوزه‌ی تصاویر دیجیتال یکی از آن حوزه‌ها می‌باشد. باتوجه 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 داده ها نمایند به علاوه اینکه این تکنیک می‌تواند به گونه‌ای ارسال شود که فقط افراد فرستنده وگیرنده قابلیت استخراج اطلاعات را داشته باشند و از طرفی قابلیت تغییر اصل داده به راحتی امکان پذیر نباشد. یک روش ایده آل در پنهان‌نگاری، روشی است که در عین حال که دارای ظرفیت جاسازی بالایی باشد. کیفیت تصویری مطلوبی نیز برای تصویر stego (تصویر حاصل از جاسازی بیت‌های محرمانه در تصویر پوشش) ایجاد کند و در برابر حملات مختلف پنهان‌شکنی

نیز مقاوم باشد[1]. معمولا بین نرخ جاسازی و کیفیت تصویر stego موازنه‌ای برقرار است. به این صورت که با افزایش ظرفیت جاسازی، کیفیت تصویر stego کاهش پیدا می‌کند و برعکس. در نتیجه مطلوب است قبل از مرحله جاسازی، حجم داده‌های محرمانه را تا حد امکان با استفاده از روش‌های مختلف فشرده‌سازی کاهش داد. برخلاف روش‌های غیر تطبیقی در پنهان‌نگاری [2] که تعداد بیت قابل جاسازی در هر پیکسل ثابت است، در روش‌های تطبیقی [3] ظرفیت جاسازی پیکسل‌ها در نواحی مختلف تصویر متفاوت است. روش‌های تطبیقی با بهره‌گیری از ضعف سیستم بینایی انسان، سعی در جاسازی تعداد بیت بیشتری از اطلاعات محرمانه را در پیکسل‌های لبه‌ای تصویر دارند، زیرا چشمان انسان نسبت به تغییرات ایجاد شده در این نواحی، حساسیت کمتری دارد و می‌توان بدون ایجاد تغییرات قابل رویت در تصویر، تعداد بیت بیشتری از داده‌های محرمانه را در نواحی لبه‌ای تصویر مخفی کرد[4].