

یک متد اصلاح شده پنهان نگاری تصاویر بر اساس تکنیک LSB

و متد خط بریل در کانال های رنگ آبی و سبز

حمید نوروززاده^۱، محمد اکبرپور^۲، فرهنگ پدیداران مقدم^۳

۱ موسسه آموزش عالی اشراق بجنورد h.nrzd65@gmail.com

۲ استادیار موسسه آموزش عالی اشراق بجنورد

۳ استادیار موسسه آموزش عالی اشراق بجنورد

چکیده

با رشد شدید انتقال داده های چند رسانه ای و ارتباطات مخفی، برای تکنیک های پنهان سازی اطلاعات نقش های خیلی مهمی در نظر گرفته شده است. از طرف دیگر استگنوگرافی یکی از مهمترین تکنیک های پنهان سازی اطلاعات است، با استفاده از پنهان نگاری، اطلاعات در حامل هایی از قبیل فایل های عکس و صدا و ویدئو و فایل های متنی مخفی میشوند. در این مقاله یک متد پنهان نگاری بهینه بر اساس دامنه مکانی پیشنهاد شده است. این متد پیشنهادی پیام را با استفاده از ۶ بیت باینری، با استفاده از متد خط بریل (LSBraille) بجای استفاده از فرمت اسکی نمایش می دهد. بر اساس مطالعات انجام شده، تقریباً ۶۵ درصد مخروپهای چشم انسان به نور قرمز، ۳۳ درصد به نور سبز، و فقط ۲ درصد به نور آبی حساس اند، برای همین در این متد، پیام رمز تنها در پیکسل های آبی و سبز مخفی می شوند. یک عکس ۲۴ بیتی که از ۳ کانال رنگی (قرمز و سبز و آبی) تشکیل شده است، هر ۳ بیت پیام را در یک پیکسل مخفی می کند، از این ۳ بیت پیام، ۲ بیت آن در لایه آبی پنهان می شود و یک بیت در لایه سبز همان پیکسل مخفی میشود، در کانال آبی، پیام تنها در یکی از LSB-1 یا LSB-2 یا LSB-3 مخفی می شود. از نتایج بدست آمده پیداست که یک ظرفیت مخفی سازی ماکزیمم خیلی بالا (MHC) و کیفیت بصری بالاتر که توسط PSNR نشان داده می شود بدست می آید.

واژه های کلیدی

پنهان نگاری، PSNR، کانال های رنگی، LSBraille

۱. مقدمه

با توجه به گسترش فناوری در دنیای امروز و امکان انجام اکثر عملیات از راه دور، با استفاده از شبکه های جهانی و محلی، همچنین عدم لزوم تمرکز همه داده ها در یک محل و نیاز به دستیابی به برخی از اطلاعات راه دور و هم چنین حفظ امنیت اطلاعات در زمان ارسال و دریافت، اهمیت مسئله نگهداری اطلاعات از دسترسی های غیر مجاز را بیش از پیش آشکار می سازد [1]. از طرفی فراگیری فزاینده و رشد سریع استفاده از اینترنت انسان ها را به سوی جهان

دیجیتال و ارتباط از طریق داده های دیجیتال سوق داده است. هر جا سخن از ارتباط به میان آید، مساله امنیت کانال ارتباطی نیز مطرح می گردد. در واقع، در یک کانال ارتباطی، استگنوگرافی یا همان پنهان نگاری روشی از ارسال اطلاعات محرمانه است به نحوی که وجود خود کانال در این ارتباط مخفی بماند. روش پنهان نگاری کامپیوتری، روشی از پنهان نگاری است که امنیت اطلاعات را در رسانه دیجیتال فراهم می سازد و هدف آن درج و ارسال پیام محرمانه از طریق رسانه دیجیتال است بگونه ای که هیچ ظنی مبنی بر ارسال اطلاعات برانگیخته نشود. پیام محرمانه می تواند به صورت یک تصویر یا متن و یا سیگنال کنترل و خلاصه هر چیزی که بتوان بصورت یک رشته بیتی از صفر و یک بیان شود، باشد. قابل توجه است، امکان دارد، پیام محرمانه قبل از پنهان نگاری تحت مراحل فشرده سازی و یا رمزنگاری نیز قرار گیرد. پنهان نگاری دارای سه پارامتر ظرفیت اطلاعات وارد شونده، کیفیت ادراکی و مقاومت است. بدون شک پیشینه سازی توأم همه ای این پارامترها امکان پذیر نیست و تنها بسته به کاربرد می باید مصالحه ای بین این پارامترها ایجاد کرد. روش های پنهان نگاری کامپیوتری، اساساً باید به گونه ای باشد که به هیچ وجه تصویر پنهان نگاری قابل کشف از تصویر اصلی نباشد. این چنین روش هایی از پنهان نگاری می توانند برای اهداف مختلفی مورد استفاده قرار گیرند. در کاربردهای اطلاعاتی، تصویر دیجیتال به عنوان سیگنال حامل بوده و پیام محرمانه می تواند به صورت نامه های بسیار محرمانه نقشه های نظامی و تصاویر مخصوصی باشد در این کاربردها تاکید اصلی بر این است که ناظر سوم به هیچ وجه متوجه وجود اطلاعات در تصویر نشده و نتواند تداخلی در کانال ارتباطی ایجاد کند یا موفق به کشف پیام شود [2].

۲. پژوهش های مرتبط

در [3]، نویسندگان یک متد را پیشنهاد می کنند که پیام محرمانه را درون تصویر کاور با استفاده از بازنمایی کاراکترهای پیام محرمانه به کمک متد بریل (متد خواندن و نوشتن نابینایان) مخفی می کند که می تواند بیشتر از یک چهارم فضای مورد نیاز برای جاسازی را