اشتراک ویژه در رمزنگاری بصری مدل (2,n) تصاویر رنگی (RGB) با استفاده از جا به جایی پیکسلی

مسعود اسحاقی[۱]، علی شهزادی[۲]

۱- دانشجوی کارشناسی ارشد برق مخابرات سیستم، دانشگاه سمنان، masoud_EN@semnan.ac.ir

۲- استادیار گروه مخابرات، دانشگاه سمنان، shahzadi@semnan.ac.ir

چکیده

با رشد سریع برنامه های کاربردی اینترنتی و کاربران شبکه، پردازش تصاویر دیجیتال از طریق اینترنت بسیار آسیب پذیر شده است. هدف از رمزنگاری بصری تصاویر رنگی (RGB) مبتنی بر جا به جایی تصادفی پیکسل ها مانند هر شیوه رمزنگاری تصویری دیگر، رمزنگاری و رمزگشایی سریع بدون محاسبات پیچیده است. یکی از چند تکنیک رایج در رمزنگاری بصری مدل (2,n) است که n اشتراک یکسان ایجاد می کند و هر ۲ اشتراک دلخواه می تواند برای بازیابی تصویر اصلی ترکیب شود. اشکال سیستم موجود این است که کاربر مهاجم می تواند تصویر اصلی را بازیابی کند اگر بتواند فقط دو اشتراک را بدست آورد. سیستم پیشنهادی برای ارتقای امنیت بکارگیری اشتراک ویژه است که بازیابی تصویر اصلی را زمانی امکان پذیر میسازد که اگر و تنها اگر یکی از دو اشتراک در دسترس، اشتراک ویژه باشد. رمزگشایی با هر دو اشتراک دلخواه از n-۱ اشتراک (نبود اشتراک ویژه) چیزی از تصویر اصلی را نشان نمی دهد. برای ارزیابی سیستم پیشنهادی از تصاویر رایج در سایر مقاله های مرتبط و از معیارهای آنتروپی و همبستگی استفاده شده و در انتها نمونه کار قرار داده شده است.

واژه های کلیدی: اشتراک ویژه، تصاویر رنگی (RGB)، رمزنگاری بصری مدل (2,n)، جا به جایی تصادفی پیکسلی

۱- مقدمه

رمزنگاری بصری یکی از شاخه های جالب توجه در دنیای کامپیوتر و ارتباطات میباشد. از آنجا که برخی از تصاویر ممکن است ماهیتی رمزگونه و امنیتی داشته باشند (مانند تصاویر و نقشه های نظامی، تصاویر افراد و...) توجه به این شاخه بیشتر پدیدار میگردد. موضوع مورد بحث در این زمینه حفاظت از تصاویر در مقابل دسترسی های غیرمجاز و عدم نمایش آنها به افراد نامطمئن است. [1] یکی از بهترین روش‌هایی که در زمینه رمزنگاری بصری ارائه شده است متعلق به مونی نائور و آدی شامیر می‌باشد که در سال ۱۹۹۴ و با دیدگاه رمزنگاری صفحات اشتراک رمز گسترش داده شد. [۲] در روش آن‌ها که برای اشتراک (2,n) تصاویر سیاه و سفید ارائه شده است، یک تصویر به n اشتراک رمز شکسته می‌شود به نحوی که این اشتراک ها به تنهایی هیچ اطلاعاتی از تصویر اصلی را نمایان نمیسازند. تنها در شرایطی تصویر اصلی قابل بازیابی است که 2 اشتراک وجود داشته باشد. در روش آنها هر کدام از اشتراک‌های رمز روی صفحات شفاف بصورت توزیعی از پیکسل‌ها چاپ می‌شود و برای رمزگشایی لازم است صفحات اشتراک را روی هم قرار بدهیم. زمانی که تمام اشتراک‌ها را روی هم قرار بدهیم تصویر اصلی ظاهر خواهد شد. امروزه این عملیات به صورت دیجیتال و توسط رایانه ها انجام میشود. با افزایش رسانه های دیجیتال، نیاز به روش هایی برای حفظ این چنین اطلاعاتی ضروری به نظر می رسد.

در سال ۲۰۱۳ پاندی[۱] طرح رمزنگاری بصری را با استفاده از اشتراک های تصادفی فشرده ارائه کرده است. [۳] در این روش، طرح رمزنگاری بصری قادر است تعداد منحصر به فردی از اشتراک ها با ابعاد متراکم شده را به دست آورد.

در سال ۲۰۱۴ هایوکسان تسو[۲] با پیشنهاد روش نوآورانه طرح به اشتراک گذاری تصاویر پزشکی رمزنگاری شده با استفاده از شبکه های تصادفی را ارائه داد. [۴] در این روش، شبکه های تصادفی برای ساخت دو اشتراک استفاده می شود. در این روش نمیتوان با یک اشتراک از تصاویر پزشکی بیمار به اطلاعات خاصی پی برد.

در سال ۲۰۱۵ فرزین[۳] و سلیمان[۴] طرح اشتراک ویژه در رمزنگاری بصری (2,n) با استفاده از شبکه های تصادفی را برای

۱- Pandey
۲- Hao-KuanTso
۳- Farzin Ahammed
۴- Sulaiman