دانشگاه ملایر

دانشکده فنی و مهندسی

پایان نامه کارشناسی رشته مهندسی کامپیوتر گرایش نرم افزار

با عنوان: پنهان نگاری بر بستر تصویر

دانشجو:

علی ساریخانی

استاد راهنما:

دکتر سارا احمدی

پاییز ۱۴۰۱

چکیده

امنیت اطلاعات حوزه مهمی در عرصه دنیای دیجیتال به شمار می‌رود و نیاز روز افزون به آن شاهد این ادعا است. پنهان نگاری[1] یکی از سطوح امنیتی است که به هنگام تبادل اطلاعات خصوصا روی شبکه‌های ناامن مورد استفاده قرار می‌گیرد. هدف از پنهان نگاری مخفی کردن وجود ارتباط است، بدین مفهوم که اطلاعات درون یک رسانه دیجیتال پنهان می‌شود به طوری که گمانی مبنی بر وجود اطلاعات درون این رسانه برانگیخته نشود. تصویر یکی از مهم‌ترین رسانه‌ها در زمینه پنهان نگاری محسوب می‌شود. پنهان نگاری تصویر در دو حوزه مکانی و حوزه تبدیل یافته انجام می‌شود. هدف این پایان نامه پیاده سازی یک روش پنهان نگاری در حوزه تبدیل است.

واژه های کلیدی: پنهان نگاری، تصویر، ارتباط امن

1. Steganography

فهرست مطالب

عنوان شماره صفحه

فهرست نمودار ها و شکل ها

عنوان شماره صفحه

۱. مقدمه ای بر پنهان نگاری

داده ها به با ارزش ترین دارایی جهان تبدیل شده اند و استفاده از آن، چه مثبت یا منفی، می تواند تأثیر قابل توجهی بر افراد، مشاغل، سازمان ها و دولت ها بگذارد.

با رشد تکنولوژی و نیز توسعه انواع بسترهای ارتباطی، امروزه چالش اساسی در حوزه ارتباطات دیگر برقراری ارتباط محسوب نمی‌شود بلکه آن‌چه که باید در مرکز توجه قرار بگیرد امنیت این ارتباطات است. محیط اینترنت و سایر زیرساخت‌های ارتباطی که در عصر کنونی به طور گسترده‌ای جهت تبادل اطلاعات استفاده می‌شود، عموما از امنیت کافی برخوردار نیستند. از سوی دیگر هم‌پای پیشرفت تکنولوژی داده ها، انواع حملات نیز برای دسترسی به اطلاعات مورد تبادل در دنیای دیجیتال توسعه یافته است که هدف اکثر این حملات نقض محرمانگی اطلاعات و یا خدشه دار کردن اطلاعات می‌باشد که در بسیاری از عرصه‌ها این حملات می‌توانند آسیب‌های جدی وارد نمایند.

در ارتباطات امروزی می توان داده ها را به سبک دیجیتالی بدون از دست دادن کیفیت، هزینه کم و تحویل تقریبا لحظه ای تبادل نمود. اما امنیت این ارتباط را نمی توان تضمین کرد. داده های مهم و محرمانه را می توان در هنگام جا به جایی دزدید. تقاضا برای احراز هویت داده ها و ابزارهای موثر برای کنترل یکپارچگی آنها به طور پیوسته در حال افزایش است. چنین تقاضایی به دلیل آسان بودنِ دستکاری داده های دیجیتال است که باید آنها را به روش های مختلف ایمن سازی کرد و ارتباط امنی را به وجود آورد. تکنیک‌های کریپتوگرافی(رمزنگاری) و استگانوگرافی(پنهان نگاری) می‌توانند این مشکل را حل کنند و وجود اطلاعاتِ مخفی را که قرار است در این ارتباطات منتقل‌شوند، پنهان کنند. در واقع استگانوگرافی هنر انتقال ایمنِ داده از فرستنده به گیرنده است.

۱-۱- پنهان نگاری و رمز نگاری

رمزنگاری یک تکنیک آشکار و امن برای معکوس کردن داده ها به یک کد درهم است که می تواند از طریق یک شبکه خصوصی یا عمومی توزیع و رمزگشایی شود. دراصل، رمزنگاری دانش تغییر دادن متن پیام یا اطلاعات به کمک کلید رمز و با استفاده از یک الگوریتم رمز است. به صورتیکه

تنها شخصی که از کلید و الگوریتم آگاه است می‌تواند اطلاعات اصلی را از اطلاعات رمزگذاری، استخراج کند و شخصی که از یکی یا هر دوی آن‌ها آگاهی ندارد نمی‌تواند به اطلاعات دسترسی پیدا کند. در رمزنگاری، وجود اطلاعات یا فرستادن پیام به هیچ وجه پنهان نیست.

پنهان نگاری نشان دهنده تکنیکی است که برای انتقال داده های مخفی با نوشتن پیام پشت یک حامل چند رسانه ای مناسب، استفاده می شود. وجود پیام به جز فرستنده و گیرنده در نظر گرفته شده، برای شخص سومی مشخص نمی شود. استگانوگرافی به طور متعارف شامل ارتباطِ مخفی نقطه به نقطه است.

رمزنگاری و پنهان نگاری دو تکنیک مورد استفاده جهت تامین امنیت اطلاعات در دنیای دیجیتال برشمرده میشوند. در عرصه دیجیتال، رمزنگاری روشی برای پنهان کردن اطلاعات به وسیله درهم سازی است به طوری که اطلاعات برای افراد غیرمجاز ناخوانا می‌شود، اما این روش به طور کامل امنیت را تضمین نمی‌کند چرا که حمله کننده می‌تواند حدس بزند که پیام محرمانه‌ای در این میان وجود دارد و ارتباطی برقرار شده است.

پنهان نگاری علم و هنر پنهان سازی وجود ارتباط است، بدین صورت که با پنهان کردن اطلاعات در یک رسانه دیجیتال وجود ارتباط از دید شخص سوم پنهان بماند. این تغیرات به گونه‌ای است که کمترین تغییر قابل کشف را در رسانه پوششی ایجاد می نماید و که نتوان موجودیت پیام پنهان در رسانه را حتی به صورت احتمالی آشکار ساخت. پنهان نگاری به عنوان یک لایه امنیتی برای ارتباطات با دیدگاهی متفاوت از اکثر سطوح امنیتی و با توجه به ماهیت شبکه‌های کنونی یک عنصر ضروری در برقراری ارتباط امن محسوب می‌شود. از کاربردهای مهم پنهان نگاری می‌توان ارتباطات و ذخیره سازی داده‌های محرمانه، جلوگیری از ایجاد تغییر در داده، سیستم کنترل دسترسی برای توزیع محتوای دیجیتال و سیستم‌های پایگاه داده رسانه‌ای را نام برد.

در استگانوگرافی مدرن، داده ها ابتدا به روشی رمزگذاری یا مبهم می شوند و سپس با استفاده از یک الگوریتم خاص در داده هایی در بخشی از یک فرمت فایل وارد می شوند.

۱-۲- طرح مساله

پنهان نگاری در رسانه‌های مختلفی مانند تصویر، صوت و ویدئو قابل انجام است. در میان رسانه‌های مطرح

شده تصویر به علت ظرفیت بالا، تنوع حجم و قالب و نیز فراگیر بودن بیشتر مورد توجه قرار گرفته است. دو حوزه متداول برای جاسازی داده در تصاویر وجود دارد: حوزه مکان[۲] و حوزه تبدیل یافته[۳]. الگوریتم‌های پنهان نگاری در حوزه مکان، پیام را به طور مستقیم در شدت نور پیکسل‌های تصویر جاسازی می‌کنند. روش‌های مکانی عموما ظرفیت بالایی برای جاسازی دارند اما مقاومت پایینی در برابر حملات از خود نشان می‌دهند.

در الگوریتم‌های حوزه تبدیل، تصاویر ابتدا به حوزه تبدیل منتقل شده و سپس پیام در ضرایب تبدیل جاسازی می شود. از جمله مزایای روش‌های حوزه تبدیل میتوان به نرخ فشرده سازی بالا ، نرخ خطای بیتی پایین و قابلیت تجمیع اطلاعات اشاره کرد. از سوی دیگر روش‌های حوزه تبدیل مقاومت بیشتری در برابر حملات را دارا هستند چرا که نسبت به روش‌های دامنه مکانی روش‌های پیچیده‌تری محسوب شده و نیز تغییرات به وجود آمده را در تمام دامنه سیگنال پخش می‌کنند.

تبدیل کسینوسی گسسته یکی از مهم‌ترین و پرکاربردترین تبدیلات است. مزیت اصلی تبدیل کسینوسی گسسته نسبت به روش‌های دامنه مکانی این است که با استفاده از این تبدیل می‌توان داده را در نواحی از تصویر پنهان ساخت که کمتر در معرض فشرده‌سازی، برش و پردازش قرار دارند. حوزه DCT امکان تفکیک تصویر به گروه‌های فرکانسی مجزا شامل فرکانس بالا، پایین و متوسط را فراهم می‌کند و بدین ترتیب می توان مناسب‌ترین مکان‌ها برای جاسازی را انتخاب کرد. امروزه تصاویری که در فضای اینترنت مورد استفاده قرار می‌گیرند بیشتر از نوع تصاویر فشرده مانند تصاویر JPEG هستند. در نتیجه استفاده از تکنیکی برای پنهان نگاری که قابلیت پیاده سازی بر روی این نوع تصاویر را داشته باشد، بسیار حائز اهمیت است. از این رو پنهان نگاری مبتنی بر DCT به دلیل دارا بودن این قابلیت نسبت به سایر تبدیلات بیشتر مورد تمرکز حوزه پنهان نگاری تصاویر است.

۱-۳- الگوریتم کلی پنهان نگاری

برای پیاده سازی سیستم استگانوگرافی، دو مرحله مورد نیاز است: یکی برای مخفی کردن داده ها(Encoder) و دیگری برای استخراج موفقیت آمیز(Decoder) . موضوع اصلی در الگوریتم جاسازی، پنهان کردن پیام مخفی در رسانه پوشش(Cover File) بدون جلب توجه است که از طریق کانال ارتباطی(Communication Channel) ارسال می شود. الگوریتم استخراج فرآیند ساده‌تری دارد

3. Spatial Domain
4. Transformation Domain

و با معکوس کردن مراحل الگوریتم تعبیه می‌توان به آن دست یافت، در صورتی که گیرنده از موقعیت هایی که اطلاعات در آن مخفی شده باشد، اطلاع داشته باشد. اما در این حین باید یک ظرف برای پوشش در نظر گرفت؛ در ۵ قرن قبل از میلاد از سر تراشیده ی انسان کمک میگرفتند و اطلاعات محرمانه را بر روی پوست سر حکاکی می کردند به گونه ای که بعد از حکاکی منتظر رویش مو می شدند و بعد از آن داده یا همان انسان را ارسال می کردند.

امروزه با تغییر نوع ارتباطات می توان هر نوع داده ای را در فضایی امن دیجیتالی توسط متن، تصویر، صوت و ...که هر کدام یک محتوای دیجیتالی اند، جا به جا نمود.

برای آزمایش یک روش استگانوگرافیک سه پارامتر اولیه در نظر گرفته می شود؛ ظرفیت پنهان مناسب، نامحسوس بودن و استحکام در برابر حملات آماری. دستیابی به همه این پارامترها به طور همزمان یک کار دشوار است. برای مثال، اگر سعی کنیم ظرفیت بار را افزایش دهیم، کیفیت بصری یا عوامل امنیتی ممکن است به طور مشابه برای پارامترهای دیگر کاهش یابد. فرآیند جاسازی باید به گونه ای باشد که تغییرات بسیار کمی در شی ایجاد شود. اطلاعات مربوط برای جاسازی ممکن است از طریق یک کلید استگو مخفی(Key) ارائه شود.

تصاویر به علت داشتن ظرفیت مناسب، مقاومت نسبی در برابر حملات آماری و اندازه کوچک آنها به عنوان شی پوشش ترجیح داده می شود و حامل خوبی برای انتقال پیام های مخفی از طریق اینترنت هستند. در واقع پیام در یک تصویر پوششی جاسازی می شود که تصویر تولید شده پس از پنهان نگاری به تصویر نهانه یا تصویر استگو معروف است.

۱-۴- اصول پنهان نگاری

عواملی مختلفی وجود دارد که قدرت و ضعف روش‌های پنهان نگاری را مشخص می‌کنند. بسته به نوع کاربرد این عوامل درجه اهمیت متفاوتی را دارا هستند. چند مورد از این عوامل که در صدر قرار دارند در زیر اشاره می‌شود.

- ظرفیت مخفی سازی: اندازه اطلاعاتی که می‌تواند مخفی شود نسبت به اندازه شی پوشانه را ظرفیت مخفی سازی می‌گویند. ظرفیت مخفی سازی بزرگ امکان استفاده از رسانه پوشانه کوچکتر برای پیامی با اندازه ثابت ایجاد می‌کند که در نتیجه پهنای باند مورد نیاز برای ارسال گنجانه کاهش

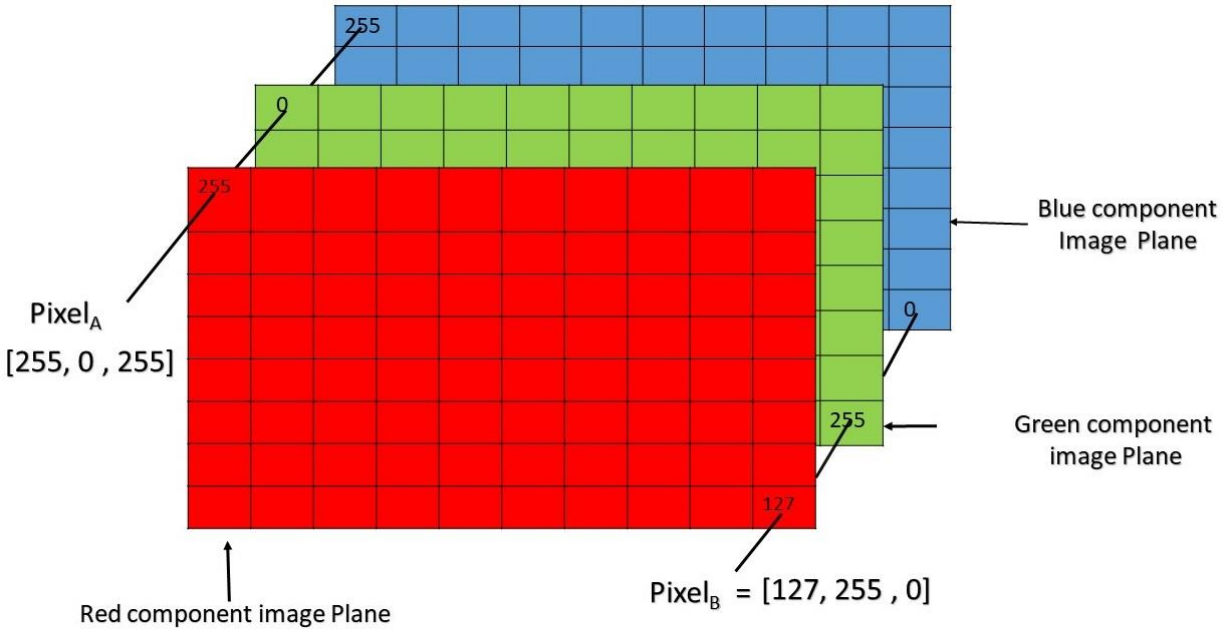
می‌یابد.

- شفافیت ادراکی: عمل پنهان سازی داده در رسانه پوشانه به ایجاد نویز یا انحراف در تصویر نیاز دارد. نکته بسیار مهم در عملیات پنهان نگاری این است که جاسازی بدون کاهش قابل ملاحظه یا از دست رفتن کیفیت تصویر پوشانه انجام شود. در ارتباطات سری، گاهی اگر دشمن یا فرد متخاصم متوجه وجود داده در تصویر گنجانه شده و انحرافی را تشخیص دهد، حتی اگر قادر به استخراج پیام نباشد باز هم روش پنهان نگاری با شکست مواجه شده است. شفافیت ادراکی و ظرفیت مخفی سازی دو عامل در تقابل با یکدیگر هستند.
- مقاومت: مقصود از مقاومت در اینجا درست باقی ماندن داده جاسازی تحت شرایط خاص مانند فیلتر کردن خطی و غیر خطی، اضافه کردن نویز تصادفی، چرخش یا تغییر اندازه، فشرده سازی با اتلاف و تبدیل از دیجیتال به آنالوگ و از آنالوگ به دیجیتال است.
- پایداری در برابر مداخله: به مشکل بودن تغییر یا جعل داده مخفی شده در تصویر گنجانه برای فرد متخاصم گفته می‌شود. معمولا کاربردهایی که نیاز به مقاومت بالا دارند درجه زیادی از مداخله را نیز می‌طلبند.

پیچیدگی محاسباتی: جاسازی و استخراج داده چه اندازه پیچیدگی محاسباتی در بردارد.

۱-۵- تصویر (Image):

نمایشی از واقعیت که در صحفه مانیتور خود می بینید، داده های شبیه سازی شده از یک شی سه بعدی است که دریافت و تبدیل به ماتریسی از اعداد شده اند. این داده‌ها از یک تصویر دیجیتال، شامل کانال هایی از سه رنگ قرمز، سبز و آبی(RGB) است که می‌تواند به حالت های مختلفی در یک فایل ذخیره شود. در واقع میتوان از سه رنگ اصلی کد گذاری شده هرمقدار را برداشته و مخلوط کرد سپس در آرایه ای از اعداد که هردرایه آن پیکسل نام دارد، ذخیره کرد.



شکل۱-۱ پیکسل های تجزیه شده یک تصویر رنگی

تصاویر سیاه وسفید، پیکسل های ۰ و ۱ را به خود اختصاص داده اند. برای تصاویر خاکستری(Gray Scale)، پیکسل ها مقادیری در بازه ۰ تا ۲۵۵ ذخیره می کنند.

فرمت های متنوعی برای تصاویر ارائه شده اند که هر کدام دارای خصوصیات منحصر به فردی است و با توجه به نیاز خاصی طراحی شده اند. این فرمت ها به چگونگی ذخیره مقادیر هر پیکسل اشاره دارد.

فرمت های غیر فشرده: فرمت هایی هستند که تمامی اطلاعات تصویر را در خود نگهداری می کنند و دارای حجم زیادی هستند. این گونه از تصاویر به علت داشتن حجم و اطلاعات زائد زیاد از بهترین فرمت ها برای پنهان نگاری در تصویر به شمار می آیند. اما برای انتقال در اینترنت، حجم بالای آنها عامل شک برانگیزی برای ناظر شبکه به حساب می آیند. از جمله فرمت های غیر فشرده میتوان به BMP و TIF اشاره کرد.

اما فشرده سازی مستقیماً با فضای حافظه مورد نیاز مرتبط است. یعنی هرچه نسبت فشرده سازی بهتر باشد، فضای کش کمتر است، که در زمان و هزینه تبادل کمک کننده است. تکنیک های

فشرده سازی به دنبال الگوهای تکراری در داده ها می گردند و سپس آن الگوها را با الگوهای کوتاه تر جایگزین می کنند. مانند استفاده از یک مخفف برای یک کلمه یا عبارت طولانی تر است.

فرض کنید جای یک کتابدار تمام شده است و به فضای بیشتری برای کتاب نیاز دارد. اگر او برخی از کتاب ها را با نسخه های دیجیتال جایگزین کند، فشرده سازی بدون تلفات است. اگر او برخی از کتاب‌ها را بسوزاند، فشرده‌سازی با اتلاف است. سوزاندن کتاب هایی که هیچ کس هرگز نمی خواند. چگونه تصمیم بگیریم چه چیزی را نگه داریم؟ در مورد فشرده‌سازی تصویر، شما با درک اینکه کدام بخش‌های تصویر برای درک انسان مهم هستند و کدام‌ها مهم نیستند، شروع می‌کنید. سپس راهی برای حفظ ویژگی های مهم پیدا می کنید و بقیه را سطل زباله می کنید.

فرمت های فشرده با اتلاف: اینگونه فرمت ها اطلاعات غیر ضروریِ تصویر که بینایی انسان قادر به تشخیص آنها نیست را حذف و حجم تصویر را کاهش میدهند بدون اینکه در کیفیت تصویر تغییری ایجاد شود. این فرمت ها میتواند بستر مناسبی برای انتقال در اینترنت باشد اما ظرفیت زیادی برای پنهان سازی اطلاعات ندارند به طوریکه تغییر در کم ارزش ترین بیت یک پیکسل از تصویر قابل کشف است. از رایج ترین این فرمت میتوان به JPEG اشاره کرد که برای فشرده سازی از تکنیک تبدیل کسینوسی استفاده میکند.

فرمت های فشرده بدون اتلاف: این فرمت ها نسبت به فشرده با اتلاف، دارای حجم بیشتری اند چون اطلاعاتِ زائدِ حذف شده در این فشرده سازی قابل بازگشت هستند مثل PNG. تکنیک مورد استفاده در این نوع فرمت ها، RLE یا رمزگذاریِ طولِ اجرا نام دارد که توالی‌هایی که در آن مقدار داده یکسانی در بسیاری از عناصر داده رخ می‌دهد، به‌عنوان یک مقدار داده و تعداد واحد ذخیره می شوند.

- JPEG

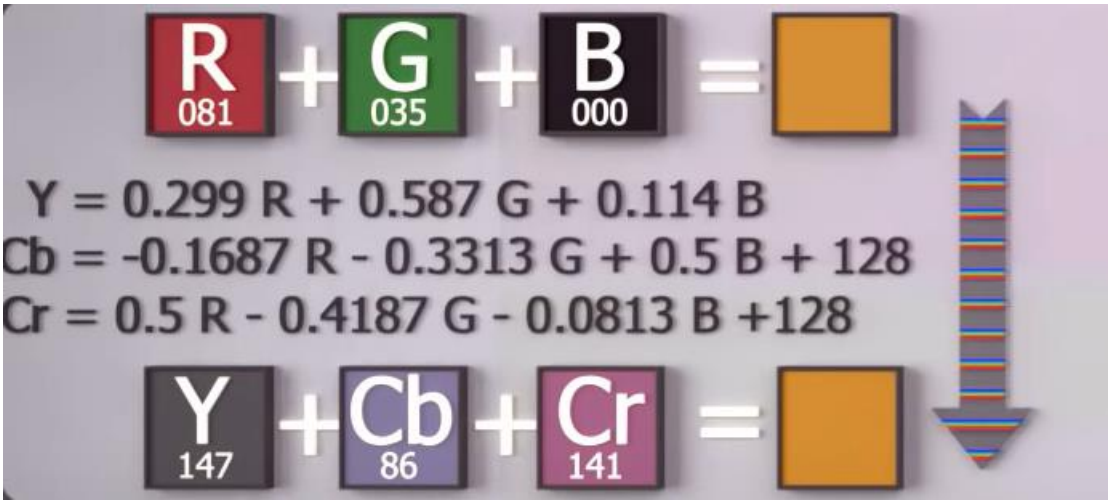
سوال اینجاست که چگونه می توان فضای ذخیره تصاویر را به یک دهم اندازه فایل فشرده نشده خود فشرده کرد که وضوح و کیفیت تصویر یکسان بماند.

در JPEG، فشرده سازی با اتلاف بر دو اصل بصری استوار است:

۱. تغییر در روشنایی مهمتر از تغییر رنگ است: شبکیه چشم انسان دارای حدود ۱۲۰ میلیون سلول میله ای حساس به روشنایی است، اما تنها حدود ۶ میلیون سلول مخروطی حساس به رنگ است.

۲. تغییرات فرکانس پایین مهمتر از تغییرات فرکانس بالا هستند. چشم انسان در قضاوت تغییرات نور با فرکانس پایین، مانند لبه‌های اجسام، خوب است. در قضاوت تغییرات نور با فرکانس بالا، مانند جزئیات ظریف در یک الگوی شلوغ یا بافت، دقت کمتری دارد.

این الگوریتم فشرده سازی هر یک از این ایده ها را به نوبه خود اعمال میکند. از پنج مرحله کلیدی تشکیل شده؛ مرحله اول تبدیل فضای رنگی(color space conversion) است، فرایندی که برای هر پیکسل سه مقدار قرمز، سبز و آبی را میگیرد و سه مقدار جدید به شکل زیر محاسبه میکند



شکل۱-۲

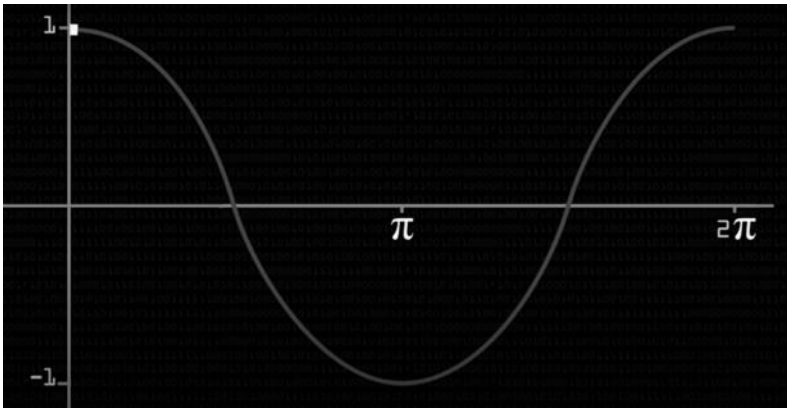
مرحله بعد که نمونه برداری برجسته(Downsampling Chrominance) نام دارد، مقدار قابل توجهی از داده ها را حذف میکند، به این صورت که تصاویر را به بلوک های دو در دو تقسیم میکند و درخشندگی آبی(Cb) و درخشندگی قرمز(Cr) هر پیکسل را گرفته، مقدار متوسط هر بلوک را حساب کرده و معادل یک پیکسل قرار می دهد و سعی بر حفظ اندازه کانال روشنایی(Y) دارد. این عمل اطلاعاتی را حذف میکند که چشمان ما درک ضعیفی از آنها دارد.

در دو مرحله بعد، تبدیل کسینوس گسسته(Transformation Cosine Discrete) و کوانتیزاسیون(Quantization)، مناطقی از تصویر که دارای فرکانس بالایی دارد را حذف میکنند.

- Discrete Cosine Transformation

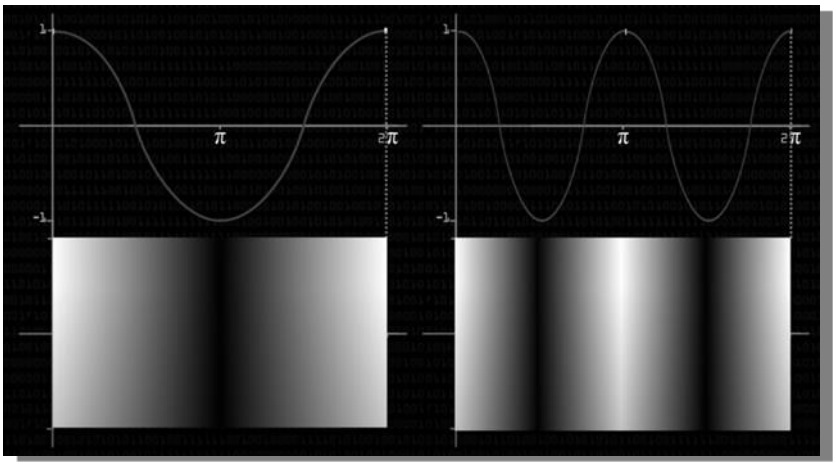
قبل از صحبت درباره اینکه تصاویر چگونه با استفاده از تبدیل کسینوس گسسته فشرده سازی می شوند ، بهتر است با یک مثال از اینکه تبدیل کسینوس گسسته چیست و چگونه کار می کند شروع می کنیم.

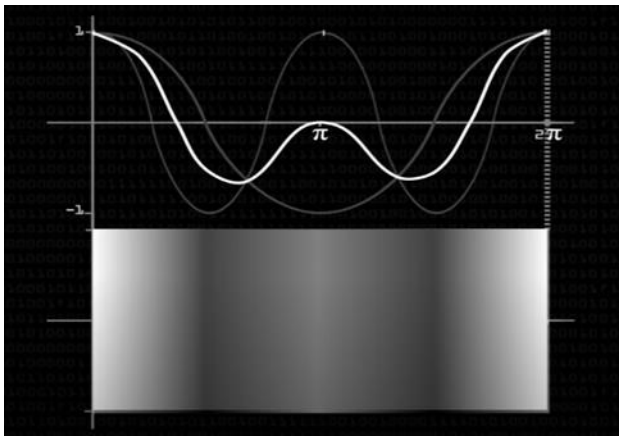
تابع کسینوس تابعی است که بین ۱ و -۱ قرار می گیرد. موج کسینوسی که در شکل ۳-۱ میبینیم، موج کسینوس فرکانس استاندارد ما است:



شکل۱-۳ تابع کسیونس

روشی که تبدیل کسینوس گسسته کار می کند به این صورت است که داده هایی را میگیریم، در این مورد داده های تصویری، و سپس آن را با مجموع تعداد زیادی از این امواج با فرکانس های مختلف نشان می دهیم که هر موج یک جز کوچک از خروجی را نشان می دهد:



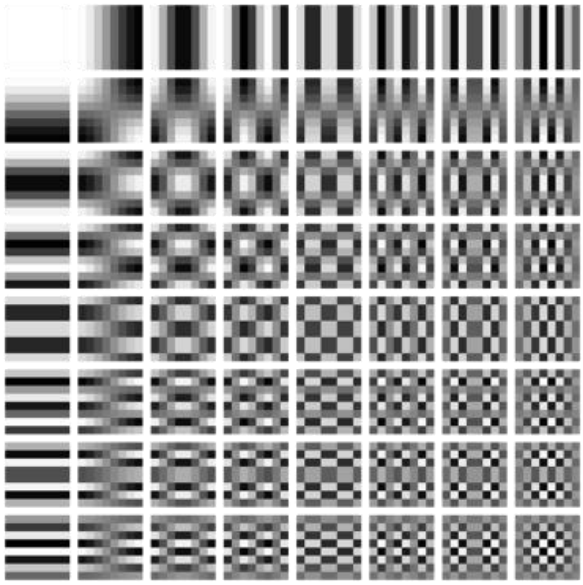


شکل ۱-۴ تابع کسینوس

روشی که ریاضیات کار می کند ، به این صورت است که اگر سیگنالی به طول ۸ داشته باشیم، در می یابیم که میتوانیم آن را با استفاده از ۸ موج کسینوس با فرکانس های مختلف نمایش دهیم که همین امر در مورد یک تصویر نیز صادق است. کاری که JPEG انجام می دهد این است که هر تصویر را به بلوک های ۸ در ۸ تقسیم می کند(۶۴ پیکسل با اعداد بین ۰ تا ۲۵۵). مقدار هر پیکسل را با کم کردن از ۱۲۸ تغییر می دهد و سپس تصویر را با استفاده از تصویر پایه که از ۶۴ تابع کسینوس تشکیل شده، بازسازی میکند:

$$DCT(i,j)$$
$$= \frac{1}{\sqrt{2N}} C(i)C(j) \sum_{x=0}^{N-1} \sum_{y=0}^{N-1} pixel(x,y) \cos[\frac{(2x+1)i\pi}{2N}] \cos[\frac{(2x+1)i\pi}{2N}]$$

$$C(x) = \frac{1}{\sqrt{2}} if\ x = 0\ , else\ 1\ if\ x > 0$$



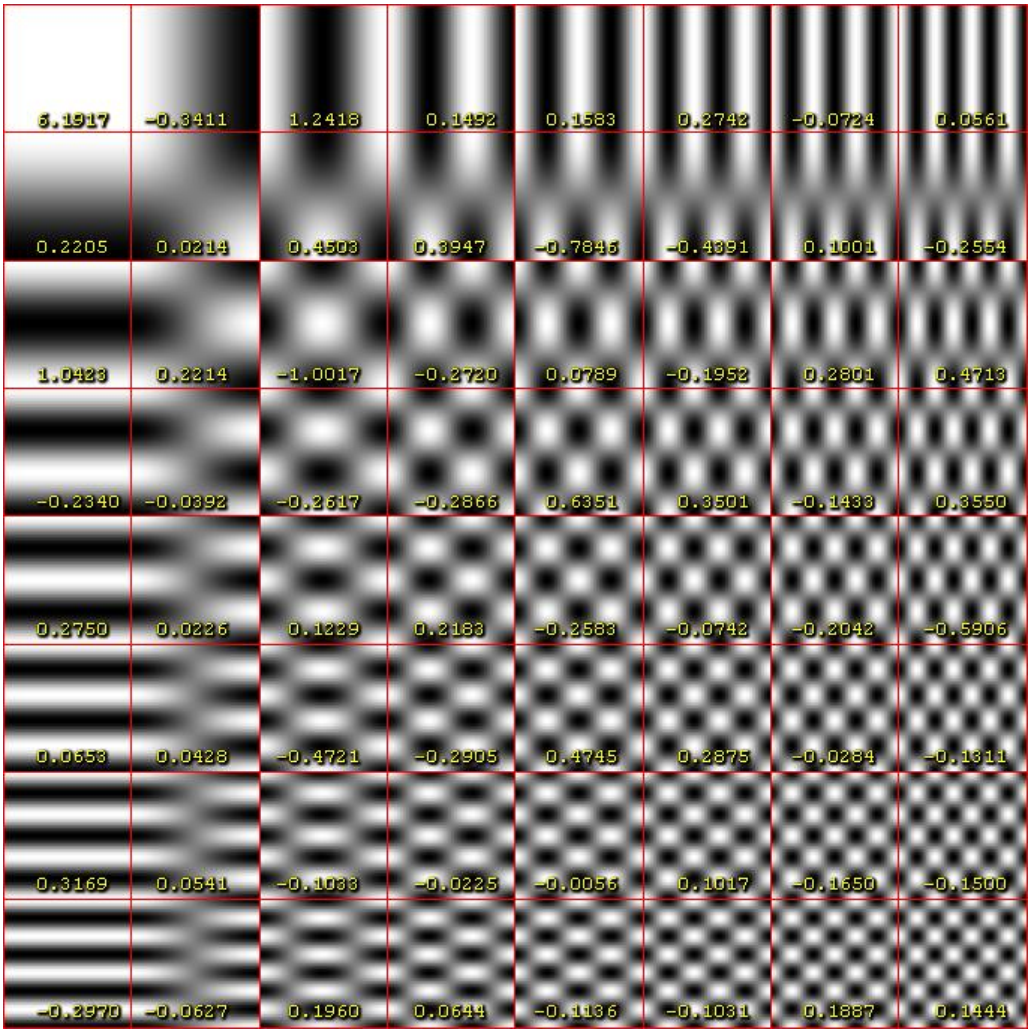
شکل ۱-۵ ۶۴ تابع کسینوس که میتوان آن را با هر تصویر ۸ در ۸ ترکیب کرد

به عنوان مثال این تصویر ۸×۸ مقیاس خاکستری از حرف بزرگ A را در نظر بگیرید

شکل ۱-۶

$$X(k) = \sum_{n=0}^{N-1} \cos\left[\frac{\pi}{N}\left(n+\frac{1}{2}\right)k\right] \quad for\ k = 0,1,\dots N-1$$

که بعد از تبدیل کسینوس گسسته، ضرایب این امواج را محاسبه، و در یک ماتریس این ضرایب DCT را ذخیره می شوند که نشان دهنده میزان استفاده از هر تصویر پایه است.



شکل ۱-۷ *ضرایب* DCT

بعد از آن اعداد مربوط به استفاده از هر تصویر پایه را به جدول کوانتیزاسیون تقسیم و به نزدیکترین عدد صحیح گرد میکند. هر چه یک عدد در یکی از جداول کوانتیزاسیون بزرگتر باشد، اطلاعات بیشتری از آن قسمت محدوده فرکانس حذف می شود.

مرحله آخر طول اجرا و کد گذاری هافمن(Run Length and Huffman Encoding) می باشد که در آن همه مقادیر برای هر بلوک را طبق الگوریتم های مربوطه فهرست میکند. در نهایت با معکوس کردن تمام مراحل تصویر فشرده شده ذخیره می شود.

۲.الگوریتم های پنهان نگاری تصویر

دسته بندی و تکنیک های متفاوتی برای پنهان سازی اطلاعات در تصاویر ارائه شده که تمامی این روش ها در دو حوزه مکان(فضایی) و حوزه تبدیل(فرکانس) قرار می گیرند.

در حوزه مکانی، پنهان نگاری در مختصات تصویر اعمال می شود و هیچگونه تبدیلی بر روی سیگنال تصویر پوششی در هنگام جاسازی پیام اعمال نمی شود. قدرت اصلی این روش ساده بودن، ظرفیت بیشتر و محاسبات کم آنهاست که باعث میشود پنهان نگاری به سرعت مورد استفاده قرار بگیرد یکی از دلایل اینکه نهان نگاریِ حوزه مکان را با چالش مواجه می سازد توانایی بسیار پایین آن برای مقابله با تغییرات در تصویر می باشد. در واقع اکثریت روشهای نهان نگاری در حوزه مکان نسبت به کوچکترین تغییرات در تصویر حساس بوده و اطلاعات نهان نگاری شده در آن ها مخدوش می گردد. در عین حال در صورتی که از تعداد بیتهای زیادی برای نهان نگاری استفاده شود تغییرات موجود در تصویر می توانند حتی با چشم انسان نیز قابل شناسایی باشند.

۲-۱- روش های حوزه مکان

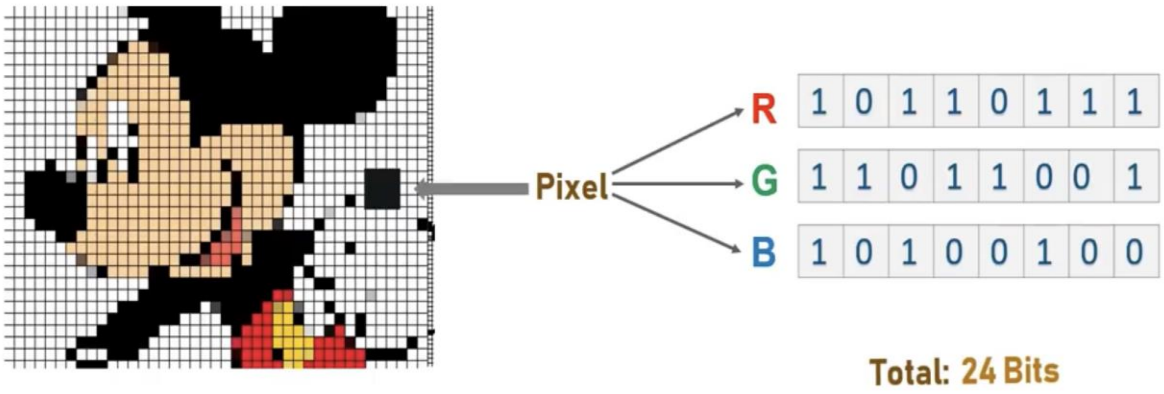
- LSB

معمول ترین روش پنهان نگاری روش LSB (Least Significant Bit) است. در این روش هر نوع اطلاعاتی را در بیت های کم ارزش تصویر نهانه مخفی سازی می کند. همچنین میتوان میزان شفافیت و ظرفیت پنهان نگاری را با تغییر تعداد بیت های به کار گرفته شده برای مخفی سازی تغییر داد و شاید بتوان این را یکی از مهم ترین مزایا LSB دانست. الگوریتم کلی آن به صورت زیر است:

ابتدا هر کاراکتر از پیام به معادل دودویی تبدیل می شود:

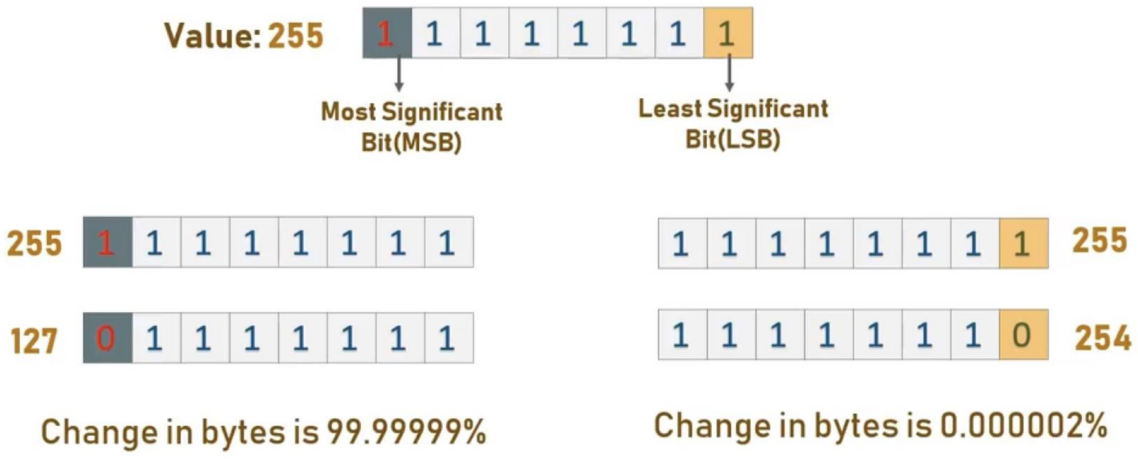
شکل۲-۱

یک پیکسل از تصویر نهانه هم انتخاب شده و معادل باینری رنگ های آن محاسبه می شود



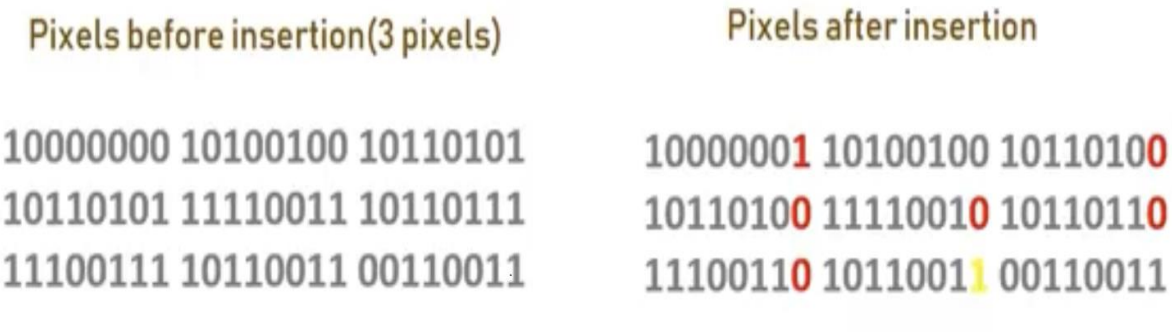
شکل۲-۲

سپس با توجه حجم پیام، آخرین بیت های هر پیکسل برای مخفی کردن انتخاب میشود که باید این نکته هم در نظر گرفت که هر چه تعداد بیشتری بیت از تصویر برای جایگذاری پیام انتخاب گردد ، تغییرات بیشتری در عکس ایجاد میکند اما باعث افزایش ظرفیت نگهداری می شود.



شکل۲-۳

حالا با ترکیب پیکسل های تصویر پوشش و معادل باینری هر کاراکتر از پیام، معدل عددی تازه ساخته می شود



شکل ۲-۴

همانطور که ملاحظه شد افزایش سطح LSB یا افزایش تعداد بیت های به کار گرفته شده، ظرفیت پنهان نگاری را افزایش و شفافیت کاهش می یابد.

در این روش پیدا کردن و از بین بردن داده های مخفی شده بسیار آسان است به همین دلیل این روش معمولا به تنهایی به کار گرفته نمی شود و معمولا از ترکیب آن با سایر روش ها استفاده می شود.[1]

- Pixel Value

در این روش میتوان هر کاراکتر از پیام را در سه رنگ(R,G,B) مخفی کرد؛ موارد زیر الگوریتم این روش را توضیح میدهد:

ابتدامعادل اسکی(عددی) کاراکتری را که باید مخفی شود، محاسبه می شود. به عنوان مثال کد اسکی کاراکتر W برابر ۱۱۹ است.

عدد به دست آمده در مرحله قبل به قسمت های یکان، دهگان و صدگان تقسیم می شود که برای ۱۱۹ داریم ۹ ، ۱ و ۱

رقم یکان معادل عددی هر یک از اجزا پیکسل صفر می شود. مثلا برای (R = 125) و (G = 243) و (B = 254) داریم (R = 120) و (G = 240) و (B = 250).

کد اسکی تقسیم شده را به ترتیب با اعداد تغییر پیدا کرده مرحله قبل جمع کرده به این صورت که صدگان را با قرمز، دهگان را با سبز و یکان را با آبی.

سپس اعداد به دست آمده، به عنوان مقادیر جدید در پیکسل نوشته می شوند و برای تمام کاراکترها این مراحل تکرار می شوند.[2]

- PVD

در روش Pixel Values Differencing (PVD)، دو پیکسل کنار هم از تصویر پوشش را انتخاب کرده و تفاضل عددی دو پیکسل را برای ارزیابی اینکه چه تعداد بیت می توانند در آنها تعبیه شوند محاسبه می شود. این روش به طور مستقیم بر شدت رنگ پیکسلها اثر نمی گذارد بلکه در مناطق لبه(محل تغییرات شدید رنگ) استفاده می شود تا کیفیت افزایش یابد. این روش برای هر دو تصاویر رنگی و سیاه سفید استفاده می شود.

الگوریتم روش PVD:

ابتدا تصویر پوشش به بلوک های دو پیکسلی تقسیم می شود(پیکسل ها دنبال هم اند).

مقدار اختلاف دو پیکسل در هر بلوک محاسبه می شود.و بعد از اینکه مشخص شد این اختلاف در چه بازه ای قرار گرفته، بر اساس آن تعداد بیت هایی که قابل جاسازی هست تعیین می شود.

حال طبق فرمول های خاص این روش، اختلاف جدیدی برای دو پیکسل مجاور محسابه و در نهایت مقدار جدید هر پیکسل تعیین می شود.[3]

- EBE

در این روش از لبه‌های تصویر پوشش برای جاسازی پیام‌ها استفاده می شود. برای لبه یابی از مجموعه عملیات ریاضی استفاده می شود که به کمک آنها می توان نقاطی از تصویر که روشنایی بطور شدید تغییر می کند را شناسایی کرد. پیکسل‌های متعلق به هر لبه انتخابی به عنوان پیکسل‌های نویزدار برای جاسازی در نظر گرفته می‌شوند و میتوان در این شلوغی، پیام را مخفی نمود. بنابراین، لبه‌ها گزینه بهتری برای پنهان کردن داده‌های مخفی نسبت به هر منطقه دیگری از تصویر اند برای اینکه هیچ تغییری در لبه‌ها قبل و بعد از جاسازی باقی نماند، LSB های تصویر پوشش ماسک می‌شوند

شکل ۲-۵

a) تصویر پوشش b) لبه های تصویرِ پوشش بعد از ماسک

c) تصویر استگو d) تفاوت بین تصویر لبه یاب شده و تصویر استگو

انتخاب لبه ها برای جاسازی به حجم پیام و تصویر بستگی دارد. با افزایش اندازه محموله، از آستانه ضعیفی برای انتخاب لبه ها استفاده می شود تا بتوان لبه های بیشتری را برای تطبیق با حجم افزایش یافته انتخاب کرد. برای یک محموله مشخص، تیزترین لبه های ممکن برای جاسازی پیام انتخاب می شوند؛ تیزتر به معنای تغییر شدیدتر در ویژگی های بصری و آماری در تصویر است که تشخیص داده های پنهان را سخت تر می کند.[4].

۲-۲- روش های حوزه تبدیل

- J-STEG

در اصل روش JSTEG بر پایه روش LSB (استفاده از کم اهمیت ترین بیت ها برای مخفی سازه داده) است. در این الگوریتم، داده به جای قرارگیری در مقادیر واقعی پیکسل‌های تصویر، در ضرایب DCT که صفر یا یک نیستند پنهان می‌شوند.

- OUTGUESS

در این الگوریتم، یک تصویر jpeg به عنوان ورودی به بلوک های ۸ در ۸ تقسیم و هر بلوک به استفاده از تبدیل کسینوس گسسته به حوزه فرکانس تبدیل می شود. بیت‌های پیام را در امتداد یک پیاده‌روی تصادفی در ضرایب LSB تعبیه می‌کند در حالی که از ۰ و ۱ عبور می کند.[5] قبل از جاسازی، کاربر محتوای پیام را رمز گذاری و همچنین تابع تولید کننده اعداد تصادفی را مقدار دهی اولیه میکند.

- SHEILD

در این روش پس از اعمال DCT و کوانتیزه (رقمی) کردن مقادیر، تعدادی از ضرایب فرکانس بالا به صفر تبدیل می‌شوند. از این ضرایب صرف نظر شده و از میان ضرایب غیر صفر برای جاسازی انتخاب می‌شود. بسته به این که ضرایب چه مقداری دارند تعداد بیت برای جاسازی درون هر ضریب تعیین می‌شود. انتخاب تعداد بیت برای هر ضریب بر اساس جدول زیر صورت می‌پذیرد:

جدول ۲-۱

تعداد بیت‌ها	مقادیر DCT کوانتیزه شده
۱	۲-۸
۲	۹-۱۶
۳	۱۷-۳۱
۴	۳۲-۶۴
۵	>۶۵

استگانالیز هنر کشف پیام پنهان است

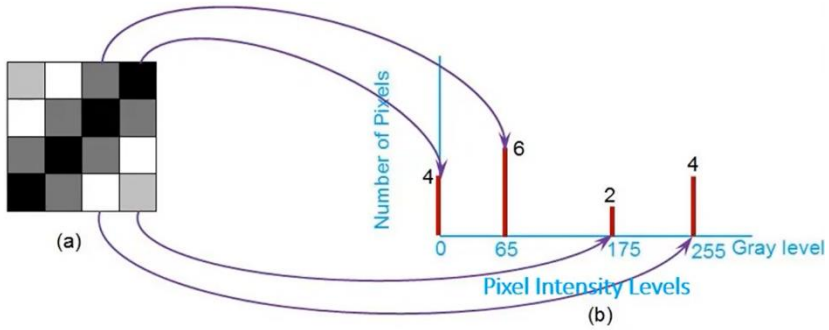
در طرف دیگر داستان، مهاجمان سعی می‌کنند از روش‌های استگانالیز برای کشف وجود پیام مخفی در تصویر استگو و استخراج آن استفاده کنند. دو تجزیه بصری و آماری برای کشف وجود پیام مخفی استفاده می شوند.یک نوع استگانالیز وجود یا عدم وجود پیام را تشخیص می دهد و نوع دیگر اندازه پیام و مکانی که پیام پنهان شده.لذا معیار هایی را برسی میکنیم که قدرت یک سیستم پنهان نگاری را تخمین میزنند. به عنوان مثال پیک سیگنال به نویز (PSNR) و شاخص تشابه ساختاری (SSIM) دو ابزار اندازه گیری هستند که به طور گسترده در ارزیابی کیفیت تصویر استفاده و معتبر در نظر گرفته می شوند. به خصوص در تصویر استگانو از این دو برای اندازه گیری کیفیت نامحسوس بودن استفاده می شود.

۲-۳- معیارهای تست سنجش:

- Histogram

از روش های رایج استگانالیز، مطالعه تغییراتی است که در هیستوگرام تصویر قبل و بعد از جاسازی پیام مخفی رخ می دهد.

هیستوگرام یک نمودار میله ای دو بعدی است که در بحث تصاویر، شدت روشنایی را اندازه گیری میکند. به بیانی ساده تر، تعداد دفعات تکرار از هر رنگ را شمارش میکند و نمایش میدهد. شکل زیر هیستوگرامِ بخش کوچکی از یک تصویرخاکستری است:



شکل ۲-۶

یک روش استگانوگرافی باید تفاوت بین هیستوگرام تصویر پوشش اصلی و تصویر استگو را به حداقل برساند. این کار با ثابت نگه داشتن فرکانس هر مقدار رنگ در تصویر از طریق انجام تغییرات مخالف در مقادیر دیگر رنگ ها انجام می شود.[6]

- Mean Square Error (MSE)

میانگین خطای مربع(MSE) تفاوت بین دو تصویر داده شده را اندازه می گیرد. عمدتا برای تجزیه و تحلیل کیفیت تصویر ما استفاده می شود. باید تا حد امکان عدد به دست آمده به صفر نزدیک باشد که اگر صفر باشد به این معنی است که تصویر استگو و اصلی شبیه به هم هستند.

$$\mathrm{MSE} = \frac{1}{\mathrm{M} * \mathrm{N}} \sum_{\mathrm{X}=1}^{\mathrm{M}} \sum_{\mathrm{Y}=1}^{\mathrm{N}} (\mathrm{f}(\mathrm{x},\mathrm{y}) - \mathrm{f}'(\mathrm{x},\mathrm{y}))^2$$

در فرمول بالا M و N ابعاد تصویر، $f(x,y)$ تصویر اصلی و $f'(x,y)$ تصویر استگو است.

- Structural Similarity Index Measure (SSIM)

شاخص تشابه ساختاری یک معیار ادراکی است که افت کیفیت تصویر ناشی از پردازش مانند فشرده سازی داده یا تلفات در انتقال داده را اندازه گیری می کند. این معیار به دو تصویر از یک تصویرِ یکسان نیاز دارد؛ یک تصویر مرجع و یک تصویر پردازش شده. که مقداری بین -۱ و +۱ را به خود اختصاص می دهد. مقدار ۱+ نشان می دهد که دو تصویر داده شده بسیار شبیه یا یکسان هستند در حالی که مقدار -۱ نشان می دهد که دو تصویر داده شده بسیار متفاوت هستند.

مقایسه بین دو تصویر بر اساس ویژگی های زیر صورت میگیرد:

درخشندگی، که با میانگین گیری روی تمام مقادیر پیکسل اندازه گیری می شود.

کنتراست، که با گرفتن انحراف استاندارد از تمام مقادیر پیکسل اندازه گیری می شود.

و در نهایت سیگنال ورودی را به انحراف استاندارد آن تقسیم می کنیم تا نتیجه دارای انحراف استاندارد واحد باشد که امکان مقایسه قوی تری را با استفاده از توابع مقایسه ای، فراهم می کند.

- Peak Signal to Noise Ratio (PSNR)

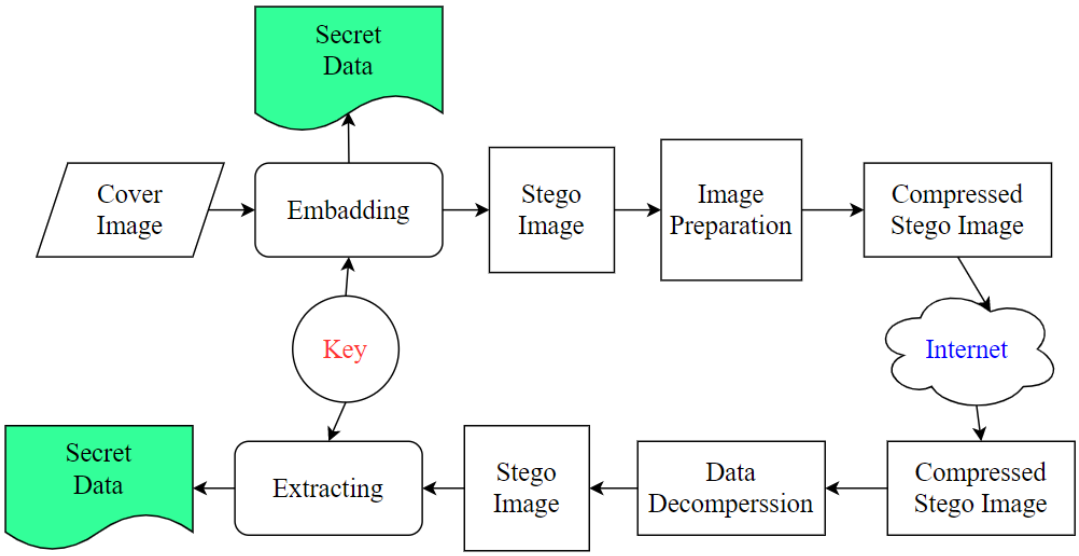
یکی از پارامترهای کلیدی نامحسوس بودن است که نسبت بین قدرت سیگنال به نویز است. هر چه PSNR بالاتر باشد، کیفیت تصویر خوب است و بستگی به MSE تصویر داده شده دارد. زمانی که تفاوت کمتری بین دو تصویر وجود دارد، PSNR بالاست و کیفیت تصویر نیز بالا می‌رود.

$$\text{PSNR} = 10\log 10\ (\frac{MAX^2}{MSE})$$

در فرمول بالا MAX حداکثر مقدار پیکسل ممکن تصویر است. هنگامی که پیکسل ها با استفاده از ۸ بیت در هر نمونه نمایش داده می شوند، این عدد ۲۵۵ است.

۳. طرح پیشنهادی

در طرح پیشنهادی به دنبال یافتن راه‌های مختلف برای بازآرایی داده‌های مخفی هستیم تا هرگونه تغییر در تصویر استگو به حداقل برسد. مرحله اول این طرح رمزگذاری پیام ورودی از طریق استفاده از روش رمزنگاری RSA می باشد. سپس یک تصویر ورودی را به حوزه تبدیل برده و جاسازی را در بیت کم ارزش ضرایب حاصل از تبدیل انجام می دهیم.[7]



شکل ۱-۳

- RSA Encryption Algorithm

تکنیک های رمزنگاری برای اطمینان از انتقال ایمن داده ها و تضمین حریم خصوصی کاربر استفاده می شود. با استفاده از رمزگذاری، اطلاعات از متن ساده به کد مخفی تبدیل می

شوند و تنها کاربر مورد نظر که دارای کلید است می تواند به اطلاعات دسترسی داشته باشد. کاربر RSA، یک کلید عمومی را بر اساس دو عدد اول بزرگ را همراه با یک مقدار تصادفی ساخته و به صورت عمومی منتشر می‌کند. هر کسی می‌تواند از این کلید عمومی برای رمزگذاری یک پیام استفاده کند، اما تنها کسی که آن دو عدد اولی که کلید بر اساس آن‌ها ساخته شده را می‌داند، قادر به رمزگشایی پیام است. تاکنون هیچ روشی برای شکست دادن این سیستم (در صورت استفاده کلید به اندازه کافی بزرگ) منتشر نشده‌است.

مراحل زیر برای ساخت کلید طی می‌شود:

۱. دو عدد اولِ بزرگ $p\ ,\ q$ را تصادفی انتخاب میکنیم به طوری که $p \neq q$.
۲. عدد n را محاسبه کنید به طوری که $n = pq$
۳. تابع $\varphi(n)$ هم محاسه میشود : $\varphi(n) = lcm\ (p-1\ ,q-1)$
۴. عدد e را به عنوان توان کلید عمومی طوری انتخاب کنید که $1 < e < \varphi(n)$ و نسبت به $\varphi(n)$ اول باشد؛ معمول‌ترین مقدار انتخاب شده برای e ، حدود عدد 2^{16} یک که برابر با ۶۵۵۳۶ است می‌باشد. کوچک‌ترین و سریع‌ترین مقدار ممکن برای e ، عدد ۳ است اما چنین مقدار کمی نشان داده‌است که در بعضی ساختارها امنیت کم تری را ایجاد می‌کند.
۵. عدد d که $d \equiv e^{-1}(mod\ \varphi(n))$ را محاسبه کنید.

فرض کنید باب میخواهد اطلاعاتی را به آلیس بفرستد. اگر آنها تصمیم بگیرند که از RSA استفاده کنند، باب باید کلید عمومی آلیس را برای رمزگذاری پیام بداند و آلیس باید از کلید خصوصی ای که در اختیار دارد استفاده کند تا پیام را رمزگشایی نماید. بنابراین آلیس کلید عمومی (n, e) خود را توسط یک مسیر مطمعن به باب منتقل میکند. کلید خصوصی آلیس (n, d) هرگز منتقل نمی شود.

رمزنگاری پیام:

حالا که باب کلید عمومی آلیس را دریافت کرد، قصد دارد پیام m را توسط این الگوریتم به آلیس بفرستد. پیام باب باید در قالب یک عدد طوری طراحی شود که این فرایند برگشت پذیر باشد. همچنین اگر پیام بیش از حد بزرگ بود آن را در قالب بسته های جداگانه تقسیم میکند. سپس محاسبه عدد c

$$c = m^e\ mod\ n$$

رمزگشایی پیام:

آلیس c را دریافت میکند و با استفاده از کلید خصوصی خود، پیام را بازیابی میکند[8]

$$m = c^d \, mod \, n$$

۴.پیاده سازی

الگوریتم پنهان نگاری :

در طول فرآیند، چندین مرحله کلیدی دنبال می شود. آنها عبارتند از:

- پیام مخفی به کمک RSA کدگذاری می شود
- فشرده سازی تصویر با استفاده از DCT
- استفاده از LSB برای جاسازی پیام کدگذاری شده در تصویر پوشش
- بازگشت تصویر به حوزه مکان و بازسازی نهایی تصویر
-

الگوریتم استخراج :

- بردن تصویر به حوزه تبدیل
- استخراج ضرایب تبدیل
- استخراج پیام رمز گذاری شده با LSB
- رمزگشایی پیام رمزگذاری شده با استفاده از RSA

نتایج حاصل از آزمایش ها

۵.نتیجه گیری

تاکنون روش‌های متعددی برای پنهان‌نگاری در تصاویر پیشنهاد شده است. برای هر الگوریتم پنهان نگاری می توان سه پارامتر مهم تعریف کرد:

۱- حوزه جاسازی ۲- بستر جاسازی ۳- روش جاسازی

دو حوزه متداول برای جاسازی داده در تصاویر وجود دارد: حوزه مکان و حوزه تبدیل یافته. الگوریتم های پنهان نگاری در حوزه مکان، پیام را به طور مستقیم در شدت نور پیکسل های تصویر جاسازی می‌کنند، اما در الگوریتم‌های حوزه تبدیل، تصاویر ابتدا به حوزه تبدیل موردنظر (مثلا DCT، DWT و...) منتقل می‌شوند و سپس پیام در ضرایب تبدیل جاسازی می‌شود. روش استفاده از حوزه تبدیل برای پنهان نگاری به منظور بهبود ویژگی‌های خاص تصویر برای جاسازی اطلاعات استفاده می‌شود. از جمله مزایای این روش نرخ فشرده سازی بالا ، نرخ خطای بیتی پایین و قابلیت تجمیع اطلاعات خوب است.

پارامتر دوم مشخص می‌کند که الگوریتم پنهان نگاری در حوزه مورد نظر خود، از چه بستری برای جاسازی داده استفاده می‌کند. برای مثال در حوزه مکان، جاسازی ممکن است مستقیما در مقدار یک پیکسل انجام شود و یا اینکه یک رابطه میان چند پیکسل تعریف شود و داده مورد نظر در مقدار این رابطه جاسازی شود.

در هر الگوریتم پنهان نگای، پس از تعیین حوزه و بستر جاسازی باید روش جاسازی داده انتخاب شود. در این گام بستر انتخاب شده، به منظور جاسازی طوری تغییر می‌کند که بعداً و توسط الگوریتم استخراج، بتوان داده جاسازی شده را از آن استخراج نمود. با توجه به استفاده وسیع از تصاویر JPEG در محیط اینترنت، امروزه الگوریتم‌های پنهان نگاری در حوزه DCT یکی از حوزه‌های تحقیقاتی فعال است. مزیت اصلی تبدیل DCT نسبت به روش‌های دامنه مکانی این است که با استفاده از این تبدیل می‌توان داده را در نواحی از تصویر پنهان ساخت که کمتر در معرض فشرده‌سازی، برش و پردازش قرار دارند

در این پایان نامه ترکیب RSA و DCT به‌عنوان روشی برای ایمن‌سازی و فشرده‌سازی پیام‌ها، حتی پنهان کردن پیام‌ها در یک تصویر جلد، با هدف تولید یک تصویر استگو با کیفیت بالا پیشنهاد می شد. از طریق مقایسه پارامترهای تصاویر برای الگوریتم ها، تحقیق به این نتیجه رسیدیم که کدگذاری RSA گامی مهم برای شروع فرایند پنهان نگاری است و جاسازی در بیت کم ارزش به حفظ کیفیت تصویر کمک کرده است گرچه ظرفیت جاسازی اندکی کاهش می باید.

مراجع

[1] W. Bender, D. Gruhl, N. Morimoto, and A. Lu, Techniques for data hiding, IBM System Journal, vol. 35, no. 3, pp. 313-336, 1996

[2] V.Nagaraja, V. Vijayalakshmib and G. Zayarazc "Color Image Steganography based on Pixel Value Modification Method Using Modulus Function", 2013 International Conference on Electronic Engineering and Computer Science 2013

[3] Wu, Tsai , " A steganographic method for images by pixel-value differencing " ,Volume 24, Issues 9- 10, June 2003, pages 1613-16

[4] Saiful Islam, Mangat R Modi & Phalguni Gupta " Edge-based image steganography "

[5] Provos, N. and Honeyman, P. Detecting Steganographic Content on the Internet. CITI Technical Report 01-11, 2001

[6] Image Steganography Method Preserves the Histogram Shape of Image EURASIP Journal on Information Security volume 2014

[7] Osama F. AbdelWahab, Aziza I. Husseinc,Hamdy M.Kelash.(2021).Eficient combination of rsa cryptography,lossy and lossless compression] [steganography

[8].https://fa.wikipedia.org/wiki/%D8%A2%D8%B1%D8%A7%D8%B3%E2%80%8C%D8%A7%DB%8C