نشریه علمی آفاق اطلاعات

بررسی روش های پنهان نگاری اطلاعات در تصاویر دیجیتال به همراه ارائه روشی نوین در حوزه مکان

امیر اسمعیلی[1]

۵
سال دوم
بهار ۱۴۰۴
مقاله پژوهشی
تاریخ دریافت:
۱۴۰۴/۰۶/۰۳
تاریخ پذیرش:
۱۴۰۴/۰۶/۲۵
صص: ۱۶۵-۱۴۹

چکیده

یکی از مباحث حائز اهمیت در امنیت اطلاعات، بحث اختفاء داده محرمانه است. اهمیت این موضوع هنگامی بیشتر می‌شود که قصد ارسال و دریافت یک پیام محرمانه را در فضای ناامنی مثل اینترنت داشته باشیم. پنهان نگاری هنر و علم جاسازی داده‌های محرمانه در داخل یک رسانه پوششی مانند متن، تصویر، صوت و یا ویدئو به‌منظور ارسال و دریافت آن پیام در فضای مجازی است. این تکنیک همواره با محدودیت‌هایی مانند ظرفیت جاسازی، امنیت و مقاومت داده ها، پیچیدگی محاسبات و همچنین مشکلات پیاده‌سازی همراه بوده است. این مقاله در ابتدا به معرفی روش‌های مختلف پنهان نگاری داده در رسانه‌های مختلف پرداخته سپس نقاط قوت و ضعف آن‌ها را بیان می‌کند و درنهایت به طرح یک ایده جدید پنهان نگاری در تصویر با امتیاز ظرفیت و کیفیت بالا و همچنین پروسه جاسازی و بازیابی آسان می پرازد. تکنیکی که در این روش از آن بهره برده می‌شود، استفاده از اطلاعات کانال قرمز پیکسل، جهت تصمیم‌گیری و در ادامه استفاده از فضای مناسب کانال‌های سبز و آبی آن پیکسل جهت جاسازی داده‌های محرمانه است. در این روش، از تصاویر بیت مپ رنگی با عمق ۲۴ بیت استفاده‌شده و بررسی نتایج به‌دست‌آمده نشان می‌دهد که روش پیشنهادی، به میزان قابل قبولی نتایج روش های مشابه قبلی را بهبود داده است.

کلید واژه‌ها: نهان‌نگاری داده، حوزه مکان، روش جایگزینی بیت کم‌ارزش (LSB).

---

۱ . کارشناس ارشد مخابرات سیستم.

مقدمه

با پیشرفت علم و فناوری و گسترش روزافزون استفاده از فضای مجازی، نیاز به محرمانگی و امنیت اطلاعات هر چه بیشتر احساس می‌شود. یک سیستم پنهان نگاری، پیام را در رسانه ی پوشش دهنده[1]به نحوی پنهان می‌کند که فردی که شنود می‌کند اصلاً به وجود پیام مظنون نمی‌شود. در چنین سیستمی، برای پنهان کردن اطلاعات، باید بیت های افزونه‌ی رسانه ی پوشش دهنده شناسایی شوند (بیت هایی که بدون صدمه زدن به تمامیت رسانه میتوانند تغییر داده شوند). این فرایند از طریق جایگزین کردن بیت های افزونه با داده های پیام محرمانه، یک رسانه ی پنهان کننده[2]ایجاد می کند.

هدف پنهان نگاری مدرن این است که حضور پیام پنهان‌شده را غیر قابل کشف کند، اما در حالت کلی سیستمهای پنهان نگاری به خاطر ماهیتی که دارند، در رسانه پوشش دهنده ردپاهایی را برجا میگذارند که قابل کشف است، بطوریکه حتی اگر محتوای پیام کشف نشود، وجود آن مشخص می‌شود. دلیل این امر، تغییر در خصوصیات آماری رسانه ی پنهان کننده است. فرایند پیدا کردن این تغییرات، تحلیل پنهان نگاری[3]نامیده می‌شود.[۱]

اولین تعریف و روش غیر رسمی پنهان نگاری، توسط سایمون ارایه شده است. در این تعریف که به داستان زندان معروف است،باب و آلیس دو زندانی هستند که در حضور نگهبان زندان قصد ارتباط محرمانه با یکدیگر را دارند. ارتباط باید به گونه ای باشد که نگهبانی که ناظر ارتباط بوده و پیام ها را بررسی می‌کند به پیام محرمانه پنهان‌شده در پیام ظاهری پی نبرد.[۲]

لغت استگانوگرافی[4](پنهان نگاری) از لغتی یونانی به معنی نوشته پوشیده شده ایجادشده است. سابقه استفاده از این تکنیک به هزاران سال پیش باز می گردد. یکی از اولین موارد استفاده از این تکنیک در اعصار گذشته مربوط به صده پنجم قبل از میلاد است که در آن هیستایاکوس فرمانروای روم برای انتقال پیامی سری، سر یکی از سربازان خود را تراشید، متنی را بر روی آن خالکوبی کرد و پس از رویش مجدد موهای سرباز او را برای انتقال پیام راهی نمود. از دیگر موارد یافت شده از اعصار گذشته دست‌نوشته‌هایی به زبان عربی و مربوط به حدود ۱۲۰۰ سال

1.Cover Media
2.Stego Medium
3.Steganalysis
4.Steganography

پیش است که متن نوشته‌شده بر روی آن‌ها به روش خاصی نهان‌نگاری شده‌اند این متون در کشورهای ترکیه و آلمان یافت شده‌اند.[۳]

از دیگر نمونه‌های تاریخی پنهان نگاری می‌توان به پنهان کردن پیام هایی در مورد زمان حرکت ناوهای آمریکایی در یادداشت‌های مربوط به خریدوفروش عروسک، استفاده از جوهرهای نامرئی در روم باستان و یادداشت پیام زیر تمبر نامه‌ها اشاره کرد.[۲]

۱.تفاوت بین رمزنگاری و پنهان نگاری

به طور کلی دو نوع ارتباط پنهانی وجود دارد: رمزنگاری[1]و پنهان نگاری. در رمزنگاری، اطلاعات با روش های مختلفی رمز می شوند تا برای شخص ثالث قابل درک نباشند اما فرستنده و گیرنده با استفاده از کلید مشترک می‌توانند اطلاعات مورد نظر را رمزگشایی کنند. در پنهان نگاری، علاوه بر مخفی ماندن اطلاعات، خود این ارتباط محرمانه نیز باید مخفی بماند. در واقع پنهان نگاری هنر و علم پنهان کردن ارتباطات است و هدف آن مخفی کردن وجود هرگونه ارتباط بین فرستنده و گیرنده است.

تفاوت بین رمزنگاری و پنهان نگاری در این است که در رمزنگاری تلاش می شود دسترسی به محتوای پیام برای فرد غیر مجاز ناممکن گردد ولی در پنهان نگاری سعی بر این است که موجودیت پیام انکار شود لذا در رمزنگاری مخاطب غیر مجاز به‌خودی‌خود تحریک‌شده و در جهت شکستن رمز پیام‌بر می‌آید اما در پنهان نگاری نهایت تلاش بر این امر واقع می‌شود که توجه افراد غیر مجاز را به وجود پیام جلب نکنیم و در صورتی که قبل از پنهان نگاری، پیام را رمز کرده باشیم در واقع یک لایه دیگر به امنیت ارتباط خود افزوده‌ایم.[۴]

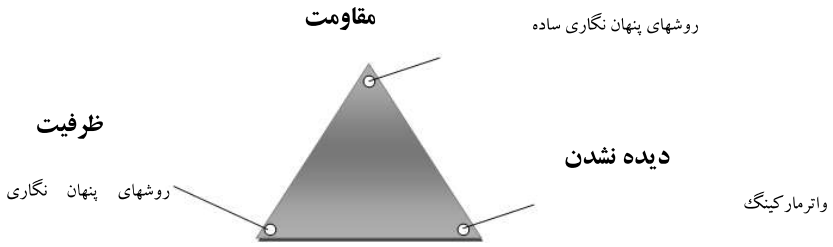
مواردی که در طراحی یک روش پنهان نگاری دارای اهمیت هستند عبارتند از:

الف) شفافیت:[2] ازآنجاکه هدف از پنهان نگاری غیر قابل حس کردن انتقال پیام است لذا ظاهر و باطن میزبان قبل و بعد از جاسازی پیام نباید تفاوت محسوسی داشته باشد و این همان مفهوم شفافیت است.

1. Cryptography
2.Transparency

ب) مقاومت:[1] مقاومت یک سیستم پنهان نگاری بدین معناست که پیام پنهان‌شده در مقابل اعمال تغییرات ناخواسته و غیرعمدی که نویز در مسیر انتقال به وجود می آورد و یا تغییرات عمدی که توسط حمله‌کننده فعال به منظور تغییر پیام و یا از بین بردن آن انجام می‌گیرد، مقاومت لازم را داشته باشد.

ج) ظرفیت:[2] هر چه بتوان پیام بیشتری را در یک میزبان مخفی کرد (با شرط حفظ شفافیت و مقاومت) آن سیستم پنهان نگاری، سیستم بهتری خواهد بود.[۵]



۲.روش های پنهان نگاری در تصویر

روش های مختلفی در طول بیش از یک دهه برای پنهان نگاری در تصاویر دیجیتال ارائه گردیده است. شاید بتوان در یک دسته‌بندی کلی روش های پنهان نگاری در تصویر را در دو حوزه مکان و فرکانس قرارداد. لذا در این قسمت به تعدادی از کارهای انجام‌شده و روش های متداول این حوزه‌ها اشاره می‌شود.

۳. روش های پنهان نگاری در حوزه مکان

تکنیک های این حوزه بر اساس جایگذاری بیت کم‌ارزش[3]پیکسل‌های تصویر میزبان، با بیت های پیام محرمانه استوار است. نکته مهم در این روش استفاده از تصاویر با جزئیات زیاد است چراکه کوچک‌ترین تغییرات در یک زمینه یکنواخت سریعاً قابل تشخیص است. در مقاله [۶] نویسندگان روشی را بر مبنای تطبیق ماتریس برای پنهان نگاری در تصویر ارایه داده اند. در این

۱.Resistance

2.Capacity

3.Least Significant Bits (LSB)

روش اطلاعات پیام در قالب یک ماتریس ۸ ستونه نوشته می‌شوند. سپس ۸ پیکسل از تصویر را انتخاب کرده و بیت های سطر اول ماتریس پیام را تک‌به‌تک با بیت کم‌ارزش هر پیکسل عوض می‌کند. این کار تا جاگذاری تمام بیت های پیام ادامه می‌یابد. امتیاز این روش این است که کمترین تاثیر را در تغییرات محسوس تصویر، نسبت به جاگذاری تعداد بیشتری از بیت های پیکسل درروش های دیگر، بر جای گذاشته و سیستم بینایی انسان به هیچ عنوان قادر به تشخیص تغییرات نمی‌باشد.

در مقالات [۷]، [۸] و [۹] نیز به گونه ای دیگر به ارایه روشهایی در این حوزه پرداخته‌شده است. در [۱۰] پیشنهادشده است پیام محرمانه ابتدا رمزگذاری شده و سپس بیت های پیام، به شیوه ذکرشده با بیت کم‌ارزش تصویر جاگذاری شوند. مقاله [۱۱] پیشنهاد جاسازی پیام در تصاویر رنگی بر پایه RGB را ارائه کرده و بیت های پیام را در رنگی که کمترین شدت را داشته و تغییر آن کمترین تاثیر را در تصویر می‌گذارد جاسازی می کند.

مثالی از پنهان کردن عدد ۲۰۰ در داخل سه پیکسل فرضی در شکل زیر آورده شده است:

```
(00101101   00011100   11011100)
(10100110   11000100   00001100)
(11010010   10101101   01100011)
```

جاسازی عدد ۲۰۰ (معادل ۱۱۰۰۱۰۰۰) در سه پیکسل فرضی فوق

```
(00101101   00011101   11011100)
(10100110   11000101   00001100)
(11010010   10101100   01100011)
```

جاسازی در بیت کم ارزش [۲]

۴.تشریح روش ارائه‌شده توسط گاتاب

این الگوریتم که توسط گاتاب و همکارانش ارائه‌شده و مبنای تحقیق حاضر قرار گرفته است، بیت های پیام محرمانه را در حوزه مکان، در تصاویر رنگی RGB جاسازی می کند. روشی که وی ارائه نموده است بر پایه استفاده از داده های اصلی یکی از کانال های پیکسل (قرمز، سبز یا آبی) جهت تصمیم‌گیری استوار است؛ به این صورت که در هر مرحله از پروسه جاسازی، دو بیت کم‌ارزش کانال قرمز موردبررسی قرار گرفته و در مورد جاسازی داده محرمانه در بیت های کم‌ارزش دو کانال دیگر (سبز و آبی) تصمیم‌گیری می‌شود. در این روش در صورت مثبت بودن شاخص جاسازی، در هر کانال تنها دو بیت از پیام محرمانه به‌جای دو بیت کم‌ارزش آن کانال قرار می‌گیرد، یعنی حداکثر چهار بیت را می‌توان در یک پیکسل (البته در صورتی که هر دو بیت کم‌ارزش کانال قرمز، یک باشند) جاسازی کرد.

پروسه تصمیم‌گیری جهت جاسازی داده محرمانه در این روش، به این صورت است که دو بیت کم‌ارزش کانال قرمز بررسی می‌شود؛ اگر هر دو بیت اشاره‌شده، مقدار صفر داشته باشند، هیچ داده ای در کانال های دوم و سوم جاسازی نخواهد شد و باید به سراغ پیکسل بعدی برویم. اگر دو بیت کم‌ارزش کانال قرمز به صورت ۰۱ باشند، در این صورت دو بیت از داده محرمانه در کانال آبی جاسازی خواهد شد ولی در کانال سبز داده ای جاسازی نمی شود. یا اگر دو بیت مذکور به صورت ۱۰ باشند، در این صورت برعکس حالت قبل عمل خواهیم کرد؛ و نهایتاً اگر دو بیت کم‌ارزش کانال قرمز به صورت ۱۱ باشند، آنگاه هم در کانال سبز و هم در کانال آبی آن پیکسل دو بیت از پیام محرمانه را جاسازی می کنیم که در این صورت، مجموعاً چهار بیت را در یک پیکسل مخفی کرده ایم.[۱۱]

۵.روش های پنهان نگاری در حوزه فرکانس

به جرات می توان گفت روش های ارائه‌شده حوزه فرکانس بسیار مقاوم‌تر از حوزه تصویر است. بسیاری از نرم افزارهای قوی موجود در زمینه پنهان نگاری از روش های تعریف‌شده در این حوزه بهره می‌برند. روش های حوزه فرکانس، پیام را به گونه ای در تصویر پوششی جاسازی می کنند که آن را در مقابل حملات مختلفی مانند فشرده‌سازی، دست‌کاری و برخی دیگر از انواع

پردازش تصویر مقاوم کند. لذا د ر مقایسه با روش جاگذاری بیت کم‌ارزش در کل از مقاومت بیشتری برخوردار می گردد.[۱۲]

روش های این حوزه بیشتر بر پایه تبدیلات حوزه فرکانس مانند تبدیل فوریه گسسته[1] تبدیل کسینوسی گسسته[2]و تبدیل موجک گسسته[3]استوارند. در مورد تبدیل کسینوسیپس از اعمال تبدیلدر بلاک های ۸ × ۸ تصویر میزبان و انجام عمل کوانتیزاسیون، داده های پیام محرمانه با بیت های کم‌ارزش ماتریس مذکور جایگشت می‌شوند؛ مثلا در [۱۳] روشی که ارایه شده، بر مبنای تبدیل کسینوسی گسسته است. به این منظور برای دستیابی به نتایج بهتر و مقاومت بیشتر، تصویر میزبان را به بلوک های ۲ × ۲ تقسیم کرده و تبدیل فوریه گسسته را روی هر یک از اعضاء انجام می‌دهند. سپس بیت های کم‌ارزش ضرایب فوریه را با بیت داده محرمانه عوض می‌کنند و نهایتا عکس تبدیل رامی گیرند. در [۱۴] از تبدیل موجک گسسته برای تصاویر رنگی استفاده‌شده است. به این صورت که داده های محرمانه، در یک تصویر رنگی شناخته‌شده و در دسترس عموم، با استفاده از یک استراتژی که بر مبنای کوانتیزاسیون استوار است، جاسازی می شوند.

۶. مقایسه نقاط قوت و ضعف روش ها

روش جاگذاری بیت کم‌ارزش، اگرچه مقدار اطلاعات زیادی را پنهان می‌کند اما مقاومت کمی در برابر حملات آماری و دست‌کاری یا پردازش تصویر به‌ویژه فشرده‌سازی با تلف از خود نشان می دهد. تکنیک های نویدبخشی مانند تبدیل کسینوسی و تبدیل موجک و همچنین پنهان نگاری تطبیقی در مقابل حملات رنگ نمی بازند، مخصوصاً اینکه حجم پیام جاسازی‌شده کم باشد. در مقابل دارای ظرفیت کمتری نسبت بهروش‌های حوزه مکان‌دارند. جاسازی پیام با تبدیل موجک گسسته نتایج بهتری نسبت به تبدیل کسینوسی نشان داده اند، مخصوصاً در مورد بقاء پیام بعد از فشرده‌سازی.

می‌توان ادعا کرد یک روش خوب پنهان نگاری در تصاویر روشی است که با در نظر گرفتن امنیت و شفافیت، بیشترین مقدار داده را در تصویر میزبان جاسازی کند.

1 .Discrete Fourier Transform (DFT)
2 .Discrete Cosine Transform (DCT)
3 .Discrete Wavelet Transform (DWT)

روش جاگذاری بیت کم‌ارزش (LSB) یکی از ساده ترین روش ها به لحاظ پیاده‌سازی و اجراست که بیت های پیام محرمانه را بانظم خاصی در کم‌ارزش ترین بیت یا بیت های هر پیکسل تصویر میزبان جاگذاری (جاسازی) می‌کند. پایداری هر چه بیشتر این روش می تواند با دقت در بهینه کردن جاسازی (با انتخاب صحیح پیکسل‌های هدف در تصویر) حاصل شود.

تصاویر می‌توانند به عنوان یکی از منابع بزرگ حمل‌کننده اطلاعات محرمانه با ظرفیت بالا باشند، لذا استفاده از تصاویر خاکستری (۸ بیتی) جهت پنهان نگاری ما را از نیل به این هدف (افزایش ظرفیت بارگذاری) باز می دارد. در مقابل تصاویر رنگی ۲۴ بیتی RGB می‌توانند به خاطر فضای بیشتری که کانال های رنگ در اختیار ما قرار می‌دهند، جهت افزایش ظرفیت بارگیری کمک شایانی به ما نمایند.

در الگوی پیشنهادی، ما از تصاویر رنگی ۲۴ بیتی جهت پنهان‌سازی داده، استفاده کرده ایم. به این صورت که ابتدا پیام متنی یا تصویری مورد نظر به رشته بیت باینری تبدیل‌شده و سپس با استفاده از روش جاگذاری بیت کم‌ارزش در حوزه مکان در داخل تصویر پوشش جاسازی می شوند.

نکته مهمی که در این روش از آن بهره برده شده است، استفاده از کانال قرمز به عنوان کانال تصمیم گیر است. ازآنجاکه حساسیت چشم انسان به تغییرات رنگی در مورد رنگ قرمز ۶۵ درصد، رنگ سبز ۳۳ درصد و رنگ آبی تنها ۲ درصد است، جاسازی در بیت های کم‌ارزش کانال قرمز می‌تواند مشهودتر از دست‌کاری دو کانال سبز و مخصوصاً آبی باشد. لذا با توجه به حساسیت بالای سیستم بینایی انسان به تغییرات رنگ قرمز، انتخاب کانال قرمز به عنوان کانال تصمیم‌ساز که عملاً هیچ تغییری در بیت های این کانال داده نمی شود، کاملاً منطقی و درست به نظر می‌رسد.

طبعاً این روش نیز همانند سایر روش های پنهان نگاری دارای دو الگوریتم جاسازی (برای فرستنده) و بازیابی پیام (برای گیرنده) خواهد بود که از این قرارند.

۷. مراحل جاسازی

ورودی: پیام محرمانه و تصویر پوششی

خروجی: تصویر پنهان نگاری شده (تصویر استگو)

تبدیل پیام محرمانه به رشته بیت باینری

محاسبه طول پیام

ذخیره کردن عدد مربوط به طول پیام در ۱۰ پیکسل اول تصویر. (که این عدد در دو بیت کم‌ارزش کانال قرمز ده پیکسل ذخیره خواهد شد)

با استفاده از دو بیت کم‌ارزش کانال قرمز (برای پیکسل‌های یازدهم به بعد) تصمیم‌گیری در مورد اینکه آیا در پیکسل مربوطه قسمتی از پیام جاسازی خواهد شد یا خیر، انجام می‌گیرد. نحوه این تصمیم‌گیری در جدول ۰-۱ آمده است.

جدول ۰-۱: نحوه تصمیم‌گیری از روی‌داده‌های کانال قرمز

ذخیره پیام در کانال آبی	ذخیره پیام در کانال سبز	دو بیت LSB کانال قرمز
×	×	۰۰
✓	×	۰۱
×	✓	۱۰
✓	✓	۱۱
✓	✓	

۱- پس‌ازاینکه مشخص شد کدام‌یک از کانال های سبز یا آبی و یا هر دو برای جاسازی پیام انتخاب‌شده‌اند، کانال مربوطه را به قسمت باارزش و کم‌ارزش تقسیم می‌کنیم. به‌عنوان‌مثال کانالی که برای جاسازی داده انتخاب‌شده، در جدول زیر نمایش داده‌شده است که به دو قسمت پرارزش (MSB) و کم‌ارزش (LSB) تقسیم‌شده است.

جدول ۰-۲: تقسیم کانال به دو منطقه کم‌ارزش و باارزش

۸	۷	۶	۵	۴	۳	۲	۱
منطقه باارزش‌تر				منطقه کم‌ارزش‌تر			

۲- در این مرحله قسمت باارزش‌تر کانال مربوطه جهت تعیین تعداد بیت پیام که می‌بایست در قسمت کم‌ارزش‌تر کانال جاسازی شوند، استفاده می‌شود. به این صورت که تعداد صفرهای موجود در قسمت باارزش تررا محاسبه و یادداشت می کنیم.

۳- تصمیم‌گیری در مورد تعداد بیت جاسازی به این صورت خواهد بود که:

✓ اگر تعداد صفرهای قسمت MSB برابر با صفر یا ۴ باشد، فقط یک بیت از پیام در بخش LSB کانال مذکور جاسازی می شود.

✓ اگر تعداد صفرهای قسمت MSB برابر با ۲ باشد، در این صورت ۲ بیت از پیام در بخش LSB کانال مذکور جاسازی می شود.

✓ اگر تعداد صفرهای قسمت MSB برابر با ۱ یا ۳ باشد، در این صورت ۳ بیت از پیام در بخش LSB کانال مذکور جاسازی می شود.

نحوه تصمیم‌گیری در مورد تعداد بیت های قابل جاسازی در کانال مورد نظر در جدول ذیل آمده است.

جدول ۰-۳: نحوه تصمیم‌گیری در مورد تعداد بیت های قابل جاسازی

تعداد صفرهای قسمت پرارزش کانال	**تعداد بیت های قابل جاسازی در قسمت کم‌ارزش کانال**
۰ یا ۴	۱ بیت
۲	۲ بیت
۱ یا ۳	۳ بیت

۴- تمامی مراحل فوق تا اتمام جاسازی تمامی رشته بیت پیام ادامه یافته و نهایتا با صفر شدن شمارنده برنامه که با طول پیام تنظیم‌شده است اجرای برنامه متوقف می‌گردد.

۸. مراحل بازیابی

۱- با استفاده از کانال های قرمز ۱۰ پیکسل اول تصویر استگو (دو بیت از قسمت کم‌ارزش هر بایت) طول پیام محرمانه را استخراج می‌کنیم.

۲- این عدد (طول پیام) را در یک متغیر ذخیره می‌کنیم.

۳- با استفاده از دو بیت کم‌ارزش کانال قرمز هر پیکسل، تصمیم‌گیری در مورد اینکه آیا در کانال های سبز و آبی آن پیکسل داده ای مخفی‌شده است یا نه صورت می‌گیرد (البته این کار از پیکسل یازده به بعد انجام خواهد گرفت).

۴- پس‌ازاینکه مشخص شد در کانال سبز یا آبی داده ای جاسازی‌شده است با استفاده از تقسیم کانال مربوطه به دو قسمت کم‌ارزش و پرارزش و شمارش تعداد صفرهای قسمت باارزش کانال مذکور می‌توان طبق جدول شماره به تعداد بیت های جاسازی‌شده در قسمت LSB کانال پی برد.

۵- تصمیم‌گیری در مورد تعداد بیت های جاسازی‌شده که باید بازیابی شوند به صورت زیر می‌باشد:

✓ اگر تعداد صفرها ۰ یا ۴ باشد نتیجه می‌گیریم فقط یک بیت در LSB آن کانال جاسازی‌شده و لذا فقط یک بیت را بازخوانی می‌کنیم و در امتداد رشته بیت قرار می‌دهیم.

✓ اگر تعداد صفرها ۲ باشد، ۲ بیت از LSB کانال برداشته و در ادامه رشته بیت استخراج‌شده می‌نویسیم.

✓ اگر تعداد صفرها ۱ و یا ۳ باشد، تعداد ۳ بیت از LSB کانال استخراج کرده و یادداشت می‌کنیم.

۶- پس از رسیدن به عدد طول پیام، رشته بیت استخراج‌شده، توسط سیستم به بلوک های ۸ تایی تقسیم‌شده و می‌توان کاراکترهای دریافت شده نمایش داد.

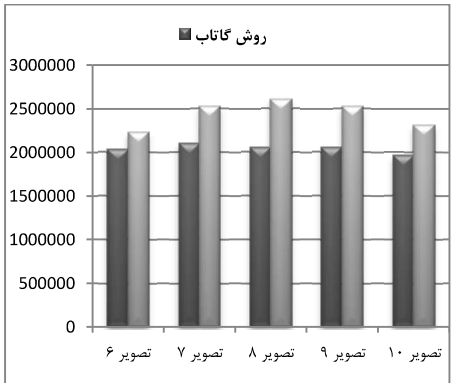
۹.بررسی و مقایسه نتایج به دست آمده

در ادامه نتایج آزمایشات حاصل از روش پیشنهادی در دو مبحث ظرفیت و کیفیت با نتایج روش گاتاب مورد مقایسه قرار گرفته است.

۹-۱. ظرفیت بارگیری

جدول زیر ظرفیت‌های بارگیری را برای روش ارائه‌شده توسط گاتاب و روش پیشنهادی را برای ۱۰ تصویر بیت مپ مختلف، با عمق رنگ ۲۴ بیت، در سایز ۱۰۲۴ در ۱۰۲۴ نمایش می‌دهد. داده های جدول نشان می دهد که ظرفیت به دست آمده برای الگوریتم پیشنهادی در همه موارد بزرگ‌تر از ظرفیت بارگیری به روش گاتاب است.

شماره تصویر	روش گاتاب	روش پیشنهادی
تصویر ۱	۲۰۰۷۲۵۲	۲۴۵۲۱۰۱
تصویر ۲	۲۰۷۰۵۴۰	۲۳۰۲۴۰۸
تصویر ۳	۲۰۷۰۲۵۴	۲۴۹۷۱۱۷
تصویر ۴	۲۰۹۳۶۹۲	۲۴۵۳۷۹۳
تصویر ۵	۲۰۵۳۵۱۶	۲۳۰۴۷۷۹
تصویر ۶	۲۰۳۷۵۵۰	۲۲۲۷۸۴۶
تصویر ۷	۲۱۰۰۳۳۰	۲۵۲۱۹۴۹
تصویر ۸	۲۰۵۷۵۴۸	۲۶۰۸۸۴۰
تصویر ۹	۲۰۵۸۳۳۰	۲۵۲۰۹۰۱
تصویر ۱۰	۱۹۶۰۶۷۶	۲۳۰۶۵۶۸



نمودارهای مقایسه‌ای فوق نیز که از روی اطلاعات جدول رسم شده است، به این واقعیت اشاره دارد که درروش پیشنهادی ظرفیت بارگیری داده محرمانه به صورت چشمگیری افزایش‌یافته است.

۲-۹. بررسی کیفیت

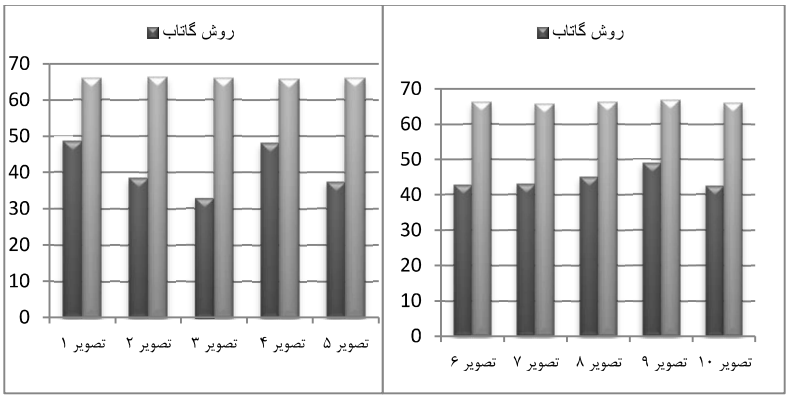
هدف از این بخش بررسی تفاوت‌های بین تصاویر اصلی با تصاویر بارگیری شده است. یکی از معیارهای این مقایسه، به دست آوردن نسبت پیک سیگنال به نویز (PSNR) می‌باشد. نتایج نشان می دهند، مقادیر سیگنال به نویز به دست آمده درروش پیشنهادی، بیشتر از مقادیر روش گاتاب برای تصاویر ورودی یکسان بوده و این به معنی بالاتر بودن کیفیت تصاویر بعد از جاسازی درروش پیشنهادی است؛ به عبارت بهتر، بر روی تصاویر استگوی حاصل از روش پیشنهادی، نسبت به تصاویر اصلی تغییرات کمتری وجود دارد. البته این تغییرات، با توجه به بالا بودن مقادیر PSNR در هر دو روش، به هیچ عنوان با چشم، قابل تشخیص نیستند.

با در نظر گرفتن افزایش چشمگیر ظرفیت بارگیری، اگر حتی در بد بینانه ترین حالت، مقادیر سیگنال به نویز در دو روش، با هم برابر می‌بود، روش ارائه‌شده نسبت به روش گاتاب در مرتبه بالاتری از کیفیت قرار می‌گرفت. همان طور که نتایج آزمایشات نشان می دهند، با افزایش ظرفیت که درنتیجهٔ اعمال روش پیشنهادی بر روی تصاویر مختلف حاصل می‌شود، نه تنها از کیفیت

تصاویر پنهان نگاری شده کاسته نشده، بلکه در تمامی موارد آزمایش‌شده، مقادیر PSNR روش پیشنهادی، به طور قابل ملاحظه‌ای بیشتر از مقادیر PSNR روش گاتاب به دست آمده اند.

جدول زیر مقادیر محاسبه‌شده PSNR را در روش گاتاب و روش پیشنهادی، برای ده تصویر مشترک با اندازه‌های ۲۰۱۴ در ۲۰۱۴ نشان می دهد. در این آزمایش، برای جاسازی پیام محرمانه در هر دو روش، از یک فایل متنی یکسان، با تعداد ۲۴۷۵ کاراکتر (۱۹۸۰۰ بیت) استفاده‌شده است.

شماره تصویر	روش گاتاب	روش پیشنهادی
تصویر ۱	۴۸/۶۲۶۳	۶۵/۹۶۴۸
تصویر ۲	۳۸/۳۳۲۶	۶۶/۱۱۰۸
تصویر ۳	۳۲/۹۰۸۸	۶۶/۰۵۰۱
تصویر ۴	۴۸/۰۲۱۲	۶۵/۵۹۰۸
تصویر ۵	۳۷/۳۲۸۴	۶۶/۰۲۵۴
تصویر ۶	۴۲/۵۷۷۷	۶۶/۰۶۵۶
تصویر ۷	۴۳/۱۰۸۱	۶۵/۵۸۴۰
تصویر ۸	۴۴/۹۴۲۳	۶۶/۰۹۹۸
تصویر ۹	۴۸/۹۰۵۴	۶۶/۵۸۳۲
تصویر ۱۰	۴۲/۴۵۵۵	۶۵/۸۹۴۲



نمودارهای مقایسه‌ای فوق نیز که از روی اطلاعات جدول رسم شده است، به این واقعیت اشاره دارد که در روش پیشنهادی، کیفیت تصاویر بهتر از روش گاتاب است.

۱۰. بحث و نتیجه‌گیری

اشاره شد که هدف غایی از پنهان نگاری، مخفی کردن یک پیام محرمانه در یک رسانه پوششی است بطوریکه جلب توجه نکند و فرد ثالث قادر به درک وجود و بازیابی پیام نباشد. در این راستا به تعدادی از روش های موجود در مقالات مختلف اشاره کردیم. بسیاری از این روش ها بر اساس جایگذاری بیت کم‌ارزش چه در حوزه تصویر و چه در حوزه فرکانس استوار بودند. مسئله اصلی در تمام این روش ها محدودیت‌هایی چون ظرفیت جاسازی، امنیت و نیز کیفیت رسانه پوششی پس از پنهان نگاری است. بعد از مطالعه تعدادی از روش های مرسوم پنهان نگاری در حوزه مکان و فرکانس و مقایسه بین آن‌ها، روشی ارائه شد که ظرفیت بارگیری و نیز کیفیت (شفافیت) تصویر را نسبت به روشی که مبنای این کار قرار گرفته بود، به صورت چشمگیری ارتقاء داده است. از طرفی، استفاده از تصاویر شلوغ با جزئیات زیاد و عدم استفاده از تصاویر با زمینهٔ ثابت و دارای الگوی تکراری و نیز مخفی نگه‌داشتن وجود ارتباط بین فرستنده و گیرنده، می‌تواند نگرانی در مورد امنیت ارسال و دریافت را کاهش داده و استفاده از این الگوریتم را با توجه به ظرفیت بالای بارگیری داده محرمانه، کاملاً توجیه‌پذیر سازد. البته استفاده از رمزنگاری

قبل از جاسازی داده ها، به عنوان یکی از لایه های مهم امنیتی، می‌تواند بر کارایی و به خصوص امنیت این روش که در حوزه مکان ارائه‌شده، بیفزاید.

نگاهی دیگربار به نتایج به دست آمده از آزمایشات، نشان می دهد که روش پیشنهادی، هم به لحاظ ظرفیت (با توجه به اینکه درروش پیشنهادی، در مواردی می‌توان تا ۳ بیت در هر پیکسل ذخیره کرد) و هم به لحاظ کیفیت (PSNR)، در مرتبه بالاتری از روش ارائه‌شده توسط گاتاب و برخی دیگر از روش های ارائه‌شده در حوزه مکان قرار می‌گیرد.

منابع:

[1] Shawn D.Dickman, "*An Overview of Steganography*", James Madison University infosecTechreport, 2017.

[2] T. Morkel, J.H.P. Eloff, and M.S. Oliver."*An overview of image steganography.*"۲۰۱۵

[3] I.J. Cox, M.L. Bloom, J.A. Fridrich, and T. Kalkert"*Digital watermarking and steganography*" USA: Morgan Kaufman Publishers, 2018

[4]ShikhaSharda, SumitBudhiraja, *"Image Steganography: A Review",* ۲۰۱۳

[5] Cheddad, A. Condell, J. Curran, K.McKevvit, "*Digital Image Steganography: Survey and analysis of current methods*", March 2010

[6] J. KAUR, M. DUHAN, A. KUMAR, and R. K. YADAV, "*Matrix matching method for secret communication using image steganography*"2012

[7] H. J. Patel and P. K. Dave, "*Least significant bits based steganography technique*, IJECCE, vol. 3, no. 1, pp. 97-۱۰۳, ۲۰۱۲.

[8] S. Tiwari, R. Mahajan, and N. Shrivastava, "*Steganography an approach for data hiding based on encryption and lsb insertion*"2011

[9]. H. Mathkour, G. M. Assassa, A. Al Muharib, and I. Kiady, "*A novel approach for hiding messages in images*, International Conference, pp. 89-۹۳, □□□□ ۲۰۰۹.

[10]. S. MasudKarim, M. Rahman, and M. Hossain, "*A new approach for lsb based image steganography using secret key*, IEEE 2011.

[11]Gutub.A, Ankeer.M,*"Pixel indicator high capacity technique for RGB image basedsteganography,"*IEEE, 2008

[12] Z. K. AL-Ani, A. Zaidan, B. Zaidan, H. Alanazi, et al. "*Overview: Main fundamentals for steganography*", 2010.

[13] D. Bhattacharyya, J. Dutta, P. Das, R. Bandyopadhyay, S. Bandyopadhyay, and T.h. Kim, "*Discrete fourier transformation based image authentication technique*, 8th IEEE International Conference on, pp. ۱۹۶-۲۰۰, □□□□, ۲۰۰۹.

[14] V. Banoci, G. Bugar, and D. Levicky, "*A novel method of image steganography in dwt domain*,"21st InternationalConference, pp. 1-4, IEEE, ۲۰۱۱.