

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

امیر اسمعیلی^۱

۳

سال دوم

بهار و تابستان ۱۴۰۴

مقاله پژوهشی

تاریخ دریافت:

۱۴۰۴/۰۵/۰۱

تاریخ پذیرش:

۱۴۰۴/۰۵/۲۹

صص: ۱۶۶-۱۴۹

چکیده

یکی از مباحث حائز اهمیت در امنیت اطلاعات، بحث اختفاء داده محرمانه است. اهمیت این موضوع هنگامی بیشتر می شود که قصد ارسال و دریافت یک پیام محرمانه را در فضای نامنی مثل اینترنت داشته باشیم. پنهان نگاری هنر و علم جاسازی داده های محرمانه در داخل یک رسانه پوششی مانند متن، تصویر، صوت و یا ویدئو به منظور ارسال و دریافت آن پیام در فضای مجازی است. این تکنیک همواره با محدودیت هایی مانند ظرفیت جاسازی، امنیت و مقاومت داده ها، پیچیدگی محاسبات و همچنین مشکلات پیاده سازی همراه بوده است. این مقاله در ابتدا به معرفی روش های مختلف پنهان نگاری داده در رسانه های مختلف پرداخته سپس نقاط قوت و ضعف آن ها را بیان می کند و در نهایت به طرح یک ایده جدید پنهان نگاری در تصویر با امتیاز ظرفیت و کیفیت بالا و همچنین پروسه جاسازی و بازیابی آسان می پردازد. تکنیکی که در این روش از آن بهره برده می شود، استفاده از اطلاعات کانال قرمز پیکسل، جهت تصمیم گیری و در ادامه استفاده از فضای مناسب کانال های سبز و آبی آن پیکسل جهت جاسازی داده های محرمانه است. در این روش، از تصاویر بیت مپ رنگی با عمق ۲۴ بیت استفاده شده و بررسی نتایج به دست آمده نشان می دهد که روش پیشنهادی، به میزان قابل قبولی نتایج روش های مشابه قبلی را بهبود داده است.

کلید واژه ها: پنهان نگاری داده، حوزه مکان، روش جایگزینی بیت کم ارزش (LSB).

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 رسانه‌ی پوشش دهنده^۱ به نحوی پنهان می‌کند که فردی که شنود می‌کند اصلاً به وجود پیام مظنون نمی‌شود. در چنین سیستمی، برای پنهان کردن اطلاعات، باید بیت‌های افزونه‌ی رسانه‌ی پوشش دهنده شناسایی شوند (بیت‌هایی که بدون صدمه زدن به تمامیت رسانه می‌توانند تغییر داده شوند). این فرایند از طریق جایگزین کردن بیت‌های افزونه با داده‌های پیام محرمانه، یک رسانه‌ی پنهان کننده^۲ ایجاد می‌کند.

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 رسانه‌ی پنهان کننده است. فرایند پیدا کردن این تغییرات، تحلیل پنهان نگاری^۳ 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 گونه‌ای باشد که نگهبانی که ناظر ارتباط بوده و پیام‌ها را بررسی می‌کند به پیام محرمانه پنهان‌شده در پیام ظاهری پی نبرد. [۲]

لغت استگانوگرافی^۴ (پنهان نگاری) از لغتی یونانی به معنی نوشته پوشیده شده ایجاد شده است. سابقه استفاده از این تکنیک به هزاران سال پیش باز می‌گردد. یکی از اولین موارد استفاده از این تکنیک در اعصار گذشته مربوط به صده پنجم قبل از میلاد است که در آن هیستیاکوس 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 نوشته شده بر روی آن ها به روش خاصی پنهان نگاری شده اند این متون در کشورهای ترکیه و آلمان یافت شده اند.[۳]

از دیگر نمونه های تاریخی پنهان نگاری می توان به پنهان کردن پیام هایی در مورد زمان حرکت ناوهای آمریکایی در یادداشت های مربوط به خرید و فروش عروسک، استفاده از جوهرهای نامرئی در روم باستان و یادداشت پیام زیر تمبر نامه ها اشاره کرد.[۲]

۱. تفاوت بین رمزنگاری و پنهان نگاری

به طور کلی دو نوع ارتباط پنهانی وجود دارد: رمزنگاری^۱ 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 می توانند 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 به خودی خود تحریک شده و در جهت شکستن رمز پیام بر می آید اما در پنهان نگاری نهایت تلاش بر این امر واقع می شود 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 افزوده ایم.[۴]

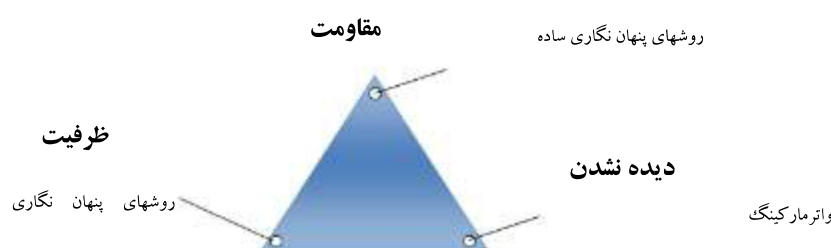
مواردی که در طراحی یک روش پنهان نگاری دارای اهمیت هستند عبارتند از:

الف) شفافیت^۲: از آنجا که 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^۱: مقاومت یک سیستم پنهان نگاری بدین معناست که پیام پنهان شده در مقابل اعمال تغییرات ناخواسته و غیرعمدی که نویز در مسیر انتقال به وجود می آورد و یا تغییرات عمودی که توسط حمله کننده فعال به منظور تغییر پیام و یا از بین بردن آن انجام می گیرد، مقاومت لازم را داشته باشد.

ج) ظرفیت^۲: 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 دسته بندی کلی روش های پنهان نگاری در تصویر را در دو حوزه مکان و فرکانس قرارداد. لذا در این قسمت به تعدادی از کارهای انجام شده و روش های متداول این حوزه ها اشاره می شود.

۳. روش های پنهان نگاری در حوزه مکان

تکنیک های این حوزه بر اساس جایگذاری بیت کم ارزش ۳ پیکسل های تصویر میزبان، با بیت های پیام محرمانه استوار است. نکته مهم در این روش استفاده از تصاویر با جزئیات زیاد است چراکه کوچک ترین تغییرات در یک زمینه یکنواخت سریعاً قابل تشخیص است. در مقاله [۶] نویسندگان روشی را بر مبنای تطبیق ماتریس برای پنهان نگاری در تصویر ارائه داده اند. در این

1. Resistance

2. Capacity

3. Least Significant Bits (LSB)

روش اطلاعات پیام در قالب یک ماتریس ۸ ستونه نوشته می شوند. سپس ۸ پیکسل از تصویر را انتخاب کرده و بیت های سطر اول ماتریس پیام را تک به تک با بیت کم ارزش هر پیکسل عوض می کند. این کار تا جاگذاری تمام بیت های پیام ادامه می یابد. امتیاز این روش این است که کمترین تاثیر را در تغییرات محسوس تصویر، نسبت به جاگذاری تعداد بیشتری از بیت های پیکسل در روش های دیگر، بر جای گذاشته و سیستم بینایی انسان به هیچ عنوان قادر به تشخیص تغییرات نمی باشد.

در مقالات [۷]، [۸] و [۹] نیز به گونه ای دیگر به ارایه روشهایی در این حوزه پرداخته شده است. در [۱۰] پیشنهاد شده است پیام محرمانه ابتدا رمزگذاری شده و سپس بیت های پیام، به شیوه ذکر شده با بیت کم ارزش 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 می گذارد 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	0001110 <u>1</u>	11011100)
(10100110	1100010 <u>1</u>	00001100)
(11010010	1010110 <u>0</u>	01100011)

جاسازی در بیت کم ارزش [۲]

۴. تشریح روش ارائه شده توسط گاتاب

این الگوریتم که توسط گاتاب و همکارانش ارائه شده 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 تصمیم گیری استوار است؛ به این صورت که در هر مرحله از پروسه جاسازی، دو بیت کم ارزش کانال قرمز مورد بررسی قرار گرفته و در مورد جاسازی داده محرمانه در بیت های کم ارزش دو کانال دیگر (سبز و آبی) تصمیم گیری می شود. در این روش در صورت مثبت بودن شاخص جاسازی، در هر کانال تنها دو بیت از پیام محرمانه به جای دو بیت کم ارزش آن کانال قرار می گیرد، یعنی حداکثر چهار بیت را می توان در یک پیکسل (البته در صورتی که هر دو بیت کم ارزش کانال قرمز، یک باشند) جاسازی کرد.

پروسه تصمیم گیری جهت جاسازی داده محرمانه در این روش، به این صورت است که دو بیت کم ارزش کانال قرمز بررسی می شود؛ اگر هر دو بیت اشاره شده، 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 کم ارزش 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 کم ارزش 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 ارائه شده حوزه فرکانس بسیار مقاوم تر از حوزه تصویر است. بسیاری از نرم افزارهای قوی موجود در زمینه پنهان نگاری از روش های تعریف شده در این حوزه بهره می برند. روش های حوزه فرکانس، پیام را به گونه ای در تصویر پوششی جاسازی می کنند که آن را در مقابل حملات مختلفی مانند فشرده سازی، دست کاری و برخی دیگر از انواع

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

روش های این حوزه بیشتر بر پایه تبدیلات حوزه فرکانس مانند تبدیل فوریه گسسته^۱، تبدیل کسینوسی گسسته^۲ و تبدیل موجک گسسته^۳ استوارند. در مورد تبدیل کسینوسی از اعمال تبدیلهای 8×8 تصویر میزبان و انجام عمل کوانتیزاسیون، داده های پیام محرمانه با بیت های کم ارزش ماتریس مذکور جایگشت می شوند؛ مثلاً در [۱۳] روشی که ارائه شده، بر مبنای تبدیل کسینوسی گسسته است. به این منظور برای دستیابی به نتایج بهتر و مقاومت بیشتر، تصویر میزبان را به بلوک های 2×2 تقسیم کرده و تبدیل فوریه گسسته را روی هر یک از اعضا انجام می دهند. سپس بیت های کم ارزش ضرایب فوریه را با بیت داده محرمانه عوض می کنند و نهایتاً عکس تبدیل را می گیرند. در [۱۴] از تبدیل موجک گسسته برای تصاویر رنگی استفاده شده است. به این صورت که داده های محرمانه، در یک تصویر رنگی شناخته شده 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 کم ارزش، اگرچه مقدار اطلاعات زیادی را پنهان می کند اما مقاومت کمی در برابر حملات آماری و دست کاری یا پردازش تصویر به ویژه فشردن سازی 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 جاسازی شده کم باشد. در مقابل دارای ظرفیت کمتری نسبت به روش های حوزه مکان دارند. جاسازی پیام با تبدیل موجک گسسته نتایج بهتری نسبت به تبدیل کسینوسی نشان داده اند، مخصوصاً در مورد بقاء پیام بعد از فشردن سازی.

می توان 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 ساده‌ترین روش‌ها به لحاظ پیاده‌سازی و اجراست که بیت‌های پیام محرمانه را بانظم خاصی در کم‌ارزش‌ترین بیت یا بیت‌های هر پیکسل تصویر میزبان جاگذاری (جاسازی) می‌کند. پایداری هر چه بیشتر این روش می‌تواند با دقت در بهینه‌کردن 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 پنهان‌نگاری ما را از نیل به این هدف (افزایش ظرفیت بارگذاری) باز می‌دارد. در مقابل تصاویر رنگی ۲۴ بیتی RGB می‌توانند به خاطر فضای بیشتری که کانال‌های رنگ در اختیار ما قرار می‌دهند، جهت افزایش ظرفیت بارگیری کمک‌شایانی 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 تبدیل شده و سپس با استفاده از روش جاگذاری بیت کم‌ارزش در حوزه مکان در داخل تصویر پوشش جاسازی می‌شوند.

نکته مهمی که در این روش از آن بهره برده شده است، استفاده از کانال قرمز به عنوان کانال تصمیم‌گیر است. از آنجا که 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 بیت‌های 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 بیت‌های این کانال داده نمی‌شود، کاملاً منطقی و درست به نظر می‌رسد.

طبعاً این روش نیز همانند سایر روش‌های پنهان‌نگاری 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 کم ارزش کانال قرمز ده پیکسل ذخیره خواهد شد)
با استفاده از دو بیت کم ارزش کانال قرمز (برای پیکسل های یازدهم به بعد) تصمیم گیری در مورد اینکه آیا در پیکسل مربوطه قسمتی از پیام جاسازی خواهد شد یا خیر، انجام می گیرد. نحوه این تصمیم گیری در جدول ۱-۰ آمده است.

جدول ۱-۰: نحوه تصمیم گیری از روی داده های کانال قرمز

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

۱- پس از اینکه مشخص شد کدام یک از کانال های سبز یا آبی و یا هر دو برای جاسازی پیام انتخاب شده اند، کانال مربوطه را به قسمت با ارزش و کم ارزش تقسیم می کنیم. به عنوان مثال کانالی که برای جاسازی داده انتخاب شده، در جدول زیر نمایش داده شده است که به دو قسمت پر ارزش (MSB) و کم ارزش (LSB) تقسیم شده است.

جدول ۲-۰: 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 باارزش‌تر را محاسبه و یادداشت می‌کنیم.

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 می‌شود.

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

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

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

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

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

۴- تمامی مراحل فوق تا اتمام جاسازی تمامی رشته بیت پیام ادامه یافته و نهایتاً با صفر شدن شمارنده برنامه که با طول پیام تنظیم شده است اجرای برنامه متوقف می گردد.

۸. مراحل بازیابی

- ۱- با استفاده از کانال های قرمز ۱۰ پیکسل اول تصویر استگو (دو بیت از قسمت کم ارزش هر بیت) طول پیام محرمانه را استخراج می کنیم.
- ۲- این عدد (طول پیام) را در یک متغیر ذخیره می کنیم.
- ۳- با استفاده از دو بیت کم ارزش کانال قرمز هر پیکسل، تصمیم گیری در مورد اینکه آیا در کانال های سبز و آبی آن پیکسل داده ای مخفی شده است یا نه صورت می گیرد (البته این کار از پیکسل یازده به بعد انجام خواهد گرفت).
- ۴- پس از اینکه مشخص شد در کانال سبز یا آبی داده ای جاسازی شده است با استفاده از تقسیم کانال مربوطه به دو قسمت کم ارزش و پر ارزش و شمارش تعداد صفرهای قسمت با ارزش کانال مذکور می توان طبق جدول شماره به تعداد بیت های جاسازی شده در قسمت LSB کانال پی برد.
- ۵- تصمیم گیری در مورد تعداد بیت های جاسازی شده که باید بازیابی شوند به صورت زیر می باشد:
- ✓ اگر تعداد صفرها ۰ یا ۴ باشد نتیجه می گیریم فقط یک بیت در LSB آن کانال جاسازی شده و لذا فقط یک بیت را بازخوانی می کنیم و در امتداد رشته بیت قرار می دهیم.
- ✓ اگر تعداد صفرها ۲ باشد، ۲ بیت از LSB کانال برداشته و در ادامه رشته بیت استخراج شده می نویسیم.
- ✓ اگر تعداد صفرها ۱ و یا ۳ باشد، تعداد ۳ بیت از LSB کانال استخراج کرده و یادداشت می کنیم.
- ۶- پس از رسیدن به عدد طول پیام، رشته بیت استخراج شده، توسط سیستم به بلوک های ۸ تایی تقسیم شده و می توان کاراکترهای دریافت شده نمایش داد.

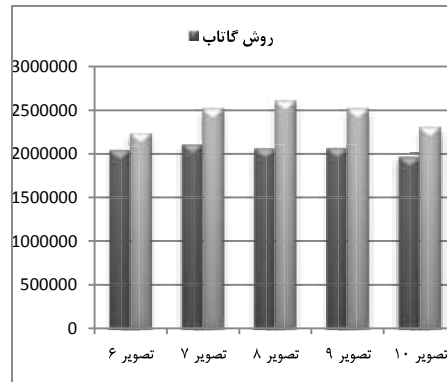
۹. بررسی و مقایسه نتایج به دست آمده

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 ارائه شده 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	۲۶۰۸۱۴۰
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 در روش پیشنهادی ظرفیت بارگیری داده محرمانه به صورت چشمگیری افزایش یافته است.

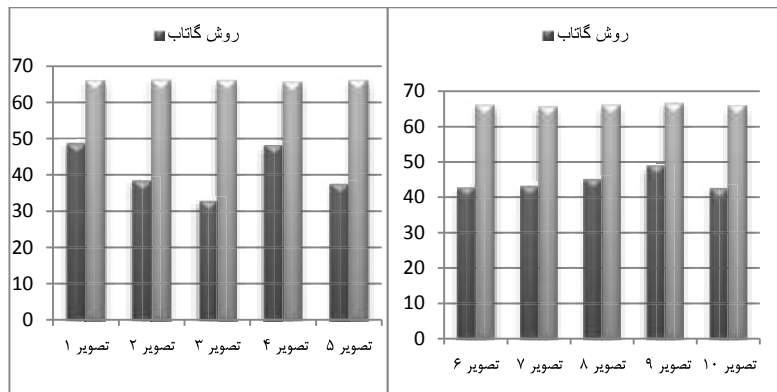
۲-۹. بررسی کیفیت

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 می‌دهند، مقادیر سیگنال به نویز به دست آمده در روش پیشنهادی، بیشتر از مقادیر روش گاتاب برای تصاویر ورودی یکسان بوده و این به معنی بالاتر بودن کیفیت تصاویر بعد از جاسازی در روش پیشنهادی است؛ به عبارت بهتر، بر روی تصاویر استگویی 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 ارائه شده نسبت به روش گاتاب در مرتبه بالاتری از کیفیت قرار می‌گرفت. همان طور که نتایج آزمایشات نشان می‌دهند، با افزایش ظرفیت که در نتیجه اعمال روش پیشنهادی بر روی تصاویر مختلف حاصل می‌شود، نه تنها از کیفیت

تصاویر پنهان نگاری شده کاسته نشده، بلکه در تمامی موارد آزمایش شده، مقادیر PSNR روش پیشنهادی، به طور قابل ملاحظه‌ای بیشتر از مقادیر PSNR روش گاتاب به دست آمده اند. جدول زیر مقادیر محاسبه شده 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) استفاده شده 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 بازبازی 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 کم ارزش 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 زمینه ثابت و دارای الگوی تکراری و نیز مخفی نگه داشتن 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، می تواند بر کارایی و به خصوص امنیت این روش که در حوزه مکان ارائه شده، بیفزاید.

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

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*.”2015
- [3] I.J. Cox, M.L. Bloom, J.A. Fridrich, and T. Kalkert “*Digital watermarking and steganography*” USA: Morgan Kaufman Publishers, 2018
- [4] Shikha Sharda, Sumit Budhiraja, “*Image Steganography: A Review*”, 2013
- [5] Cheddad, A. Condell, J. Curran, K. McKeivitt, “*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. 97-103, 2012.
- [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. 89-93, IEEE 2009.
- [10]. S. Masud Karim, 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 based steganography*, ”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. 196-200, IEEE, 2009.
- [14] V. Banoci, G. Bugar, and D. Levicky, “*A novel method of image steganography in dwt domain*,”21st International Conference, pp. 1-4, IEEE, 2011.

