ارائه روشی کارا برای پنهان نگاری بدون اتلاف و با ظرفیت جاسازی بالای تصاویر محرمانه

عارف رضائی[۱] مهسا ضامنی[۲] لیلی فرزین‌وش[۳]

۱- دانش‌آموخته کارشناسی ارشد- دانشکده مهندسی برق و کامپیوتر - دانشگاه تبریز - تبریز - ایران
aref.rezaei96@ms.tabrizu.ac.ir

۲- دانش‌آموخته کارشناسی ارشد- دانشکده مهندسی برق و کامپیوتر - دانشگاه تبریز - تبریز - ایران
mhs.zameni95@ms.tabrizu.ac.ir

۳- استادیار- دانشکده مهندسی برق و کامپیوتر - دانشگاه تبریز - تبریز - ایران
l.farzinvash@tabrizu.ac.ir

چکیده: در این مقاله، مسئله پنهان نگاری تصاویر محرمانه بررسی شده است. الگوریتم‌های موجود به دلیل عدم توجه به ساختار و خصوصیات داده‌های تصویری کارایی پایینی دارند. همچنین این الگوریتم‌ها معمولا تصاویر محرمانه را با اتلاف جاسازی می‌کنند. با توجه به مشکلات روش‌های موجود، الگوریتمی کارا به نام Lossless and High Capacity Image Steganography (LHCIS) **ارائه کرده‌ایم که تصویر محرمانه را بدون اتلاف در تصویر پوشانه جاسازی می‌نماید. الگوریتم پیشنهادی شامل فشرده سازی تصویر محرمانه و جاسازی تصویر فشرده شده در تصویر پوشانه توسط الگوریتم** LSB **است. فشرده سازی در دو مرحله انجام می‌شود. در مرحله اول، تصویر تفاضل متناظر با تصویر محرمانه ساخته می‌شود. این تصویر نشان دهنده میزان تغییرات در پیکسل‌های مجاور در تصویر محرمانه بوده و از تفاضل پیکسل‌های متوالی آن حاصل می‌شود. در مرحله بعدی، تصویر تفاضل به دست آمده کد می‌شود تا حجم آن کاهش یابد. با توجه به اینکه مقادیر پیکسل‌های تصویر تفاضل کوچک هستند، میزان فشرده سازی قابل توجه خواهد بود. براساس نتایج شبیه سازی، الگوریتم** LHCIS **ظرفیت جاسازی را ۴۰٪ و مقدار** PSNR **تصاویر میزبان - که از جاسازی تصویر محرمانه در تصویر پوشانه حاصل می‌شود - را ۲/۱۶ واحد نسبت به روش‌های پیشین افزایش داده است.**

واژه های کلیدی: پنهان نگاری، تصویر محرمانه، تصویر پوشانه، تصویر میزبان، فشرده سازی، بدون اتلاف، ظرفیت جاسازی

نوع مقاله: پژوهشی

DOI: 10.29252/jiaeee.18.3.1026

تاریخ ارسال مقاله: ۱۳۹۸/۸/۲۵
تاریخ پذیرش مشروط مقاله: ۱۳۹۹/۰۴/۰۳
تاریخ پذیرش مقاله: ۱۳۹۹/۱۱/۱۲
نام نویسنده‌ی مسئول: دکتر لیلی فرزین‌وش
نشانی نویسنده‌ی مسئول: ایران - تبریز - بلوار ۲۹ بهمن - خیابان امام خمینی - دانشگاه تبریز - دانشکده مهندسی برق و کامپیوتر

۱- مقدمه

با گسترش روز افزون اینترنت، تامین امنیت داده‌ها و تصاویر محرمانه[۱] در این بستر مورد توجه قرار گرفته است. پنهان نگاری[۲] یک روش شناخته شده برای محافظت از داده‌های محرمانه است [۱]. در این مقاله الگوریتمی کارآمد به نام Lossless and High Capacity Image Steganography (LHCIS) برای پنهان نگاری تصاویر محرمانه ارائه شده است. مفهوم پنهان نگاری و الگوریتم پیشنهادی در بخش ۱-۱ توضیح داده شده‌اند. در ادامه روش‌های پنهان نگاری موجود در بخش ۱-۲ بررسی و تحلیل شده‌اند. همچنین نحوه سازمان-دهی مقاله در بخش ۱-۳ بیان شده است.

۱-۱- پنهان نگاری تصاویر

با توسعه اینترنت و گسترش روز افزون بسترهای ارتباطی، تعداد کاربران فضای مجازی افزایش چشم‌گیری داشته است. یکی از نیازهای اصلی کاربران، تامین امنیت داده‌های ارسال شده در بستر اینترنت و محافظت از آنها در مقابل حملات مختلف مانند شنود و تغییر محتوا است. برای محافظت از داده‌های محرمانه روش‌های مختلفی ارائه شده است که رایج‌ترین آنها رمزنگاری[۳] [۲] و پنهان نگاری [۱,۳] هستند. ایده کلی الگوریتم‌های رمزنگاری، کد کردن و نامفهوم کردن داده محرمانه با استفاده از یک کلید است. ایراد اساسی رمزنگاری این است که همه کاربران از جمله حمله کنندگان از وجود داده رمز شده مطلع هستند. بنابراین حمله کنندگان سعی می‌کنند با استفاده از روش‌های رمز شکنی مختلف، داده و کلید محرمانه را استخراج کنند [۴].

روش دیگری که برای تامین امنیت داده‌های محرمانه استفاده می-شود پنهان نگاری است. در این روش، داده محرمانه درون یک داده چند رسانه‌ای مانند تصویر جاسازی می‌شود. با استفاده از این تکنیک، حمله کننده حتی از وجود داده محرمانه نیز آگاه نخواهد شد. اصطلاحاً به تصویر انتخاب شده برای جاسازی داده تصویر پوشانه[۴]، و به تصویر حامل داده محرمانه تصویر میزبان[۵] گفته می‌شود [۱]. علت استفاده از داده تصویری به عنوان میزبان آن است که قابلیت جاسازی در آنها وجود دارد. این خاصیت به دلیل ساختار و خصوصیات داده‌های تصویری است. به عنوان مثال جای‌گذاری کم ارزش‌ترین بیت[۶] (LSB) پیکسل‌ها با بیت‌های داده محرمانه تاثیر زیادی در کیفیت تصویر ندارد [۵,۶]. همچنین با توجه به اینکه بیشتر داده‌های موجود در اینترنت تصویر و ویدیو هستند، فضای کافی برای پنهان کردن داده‌های محرمانه در اختیار کاربران قرار دارد.

در الگوریتم‌های پنهان نگاری ارائه شده در [۱۵-۷] داده محرمانه از نوع تصویر در نظر گرفته شده است. بر اساس کیفیت تصویر محرمانه استخراج شده، الگوریتم‌های موجود به سه دسته تقسیم می‌شوند. دسته اول شامل روش‌هایی است که در آنها تصویر محرمانه فشرده می‌شود تا حجم داده جاسازی شده در تصویر میزبان کاهش و در نتیجه کیفیت آن افزایش یابد [۷,۸]. دسته دیگری از الگوریتم‌ها با ارائه راهکارهایی بین PSNR[۷] تصویر میزبان و تصویر محرمانه استخراج شده (نسبت به تصویر محرمانه اصلی) توازن ایجاد کرده‌اند [۱۱-۹]. برای مثال در [۹] که از شبکه عصبی عمیق برای پنهان نگاری استفاده کرده، تابع هدف به صورت کمینه کردن مجموع وزن‌دار تغییرات در تصاویر محرمانه و پوشانه تعریف شده است. روش‌های ارائه شده در دسته سوم [۱۵-۱۲] تصویر محرمانه را بدون اتلاف[۸] جاسازی کرده‌اند. در نتیجه، تصویر محرمانه مستخرج از تصویر میزبان دقیقا معادل تصویر محرمانه اصلی خواهد بود. ایده کلی الگوریتم‌های ارائه شده در [۱۲,۱۳] نگاشت بهینه بیت‌های تصویر محرمانه به بیت‌های LSB تصویر محرمانه، به‌منظور کمینه کردن میزان تغییرات تصویر میزبان نسبت به تصویر پوشانه است. در [۱۴] برای افزایش ظرفیت جاسازی[۹] تصویر پوشانه، از چند بیت کم ارزش - و نه فقط بیت LSB - برای ذخیره نمودن بیت‌های تصویر محرمانه استفاده شده است.

در این مقاله، الگوریتم LHCIS برای پنهان نگاری تصویر محرمانه در تصویر پوشانه ارائه شده است. در اینجا با توجه به ساختار و خصوصیات تصاویر، روش کارایی برای فشرده سازی تصاویر محرمانه ارائه شده است. فشرده سازی در دو مرحله انجام می‌شود. در مرحله اول یک تصویر تفاضل از روی تصویر محرمانه ساخته می‌شود. هر پیکسل این تصویر برابر تفاضل پیکسل متناظر آن در تصویر محرمانه از پیکسل مجاورش است. در مرحله دوم، تصویر حاصل از مرحله نخست کد می‌شود. با توجه به اینکه پیکسل‌های مجاور در تصاویر اختلاف کمی دارند، تصویر موردنظر شامل اعداد کوچکی خواهد بود. بنابراین تعداد بیت مورد نیاز برای نمایش مقدار هر پیکسل کمتر از هشت بیت - که معادل اندازه پیکسل غیر فشرده است - خواهد بود. در روش پیشنهادی، تصویر بلوک بندی شده و پیکسل‌های هر بلوک با تعداد مشخصی بیت نمایش داده می‌شوند. تعداد بیت‌های مورد نیاز با توجه به ماکزیمم مقدار پیکسل‌های بلوک مشخص می‌شود. خروجی مرحله دوم با استفاده از الگوریتم LSB در تصویر پوشانه جاسازی خواهد شد.

یک ویژگی مهم روش ارائه شده آن است که تصویر محرمانه را بدون اتلاف کد می‌کند. بنابراین کیفیت تصویر در فرآیند پنهان نگاری افت پیدا نمی‌کند. همچنین متوسط میزان فشرده سازی روش پیشنهادی ۴۰٪ است. با توجه به میزان کاهش حجم تصویر محرمانه، تغییرات تصویر پوشانه پس از جاسازی به میزان قابل توجهی کاهش خواهد یافت. مراجع [۱۱-۷] نیز از تکنیک فشرده سازی استفاده نموده‌اند ولی در آنها کیفیت تصویر محرمانه شدیدا کاهش یافته است. در مقابل، الگوریتم‌های ارائه شده در [۱۵-۱۲] که روش‌های بدون اتلاف هستند، از تکنیک فشرده‌سازی استفاده ننموده‌اند. در [۱۴,۱۵] برای افزایش ظرفیت جاسازی تصویر پوشانه از چند بیت کم ارزش پیکسل‌ها استفاده شده است. این کار باعث می‌شود که PSNR تصویر میزبان به نحو قابل ملاحظه‌ای کاهش یابد. همچنین، مراجع [۱۲,۱۳] بیت‌های تصویر محرمانه را به نحوی به بیت‌های LSB تصویر پوشانه

نگاشت کرده‌اند که مقدار تغییرات تصویر پوشانه کمینه شود. با توجه به اینکه این روش‌ها تصویر محرمانه را فشرده نمی‌کنند، ظرفیت جاسازی کمتری در مقایسه با الگوریتم پیشنهادی دارند.

۱-۲- کارهای مرتبط

روش‌های پنهان نگاری از نظر نحوه جاسازی به دو دسته دامنه فضایی[10] و دامنه فرکانسی[11] تقسیم می‌شوند. در الگوریتم‌های دامنه فضایی، داده محرمانه به صورت مستقیم در تصویر پوشانه جاسازی می‌شود [۱۸-۱۴,۱۶-۱۰,۱۲-۶]. یکی از متداول‌ترین الگوریتم‌های این حوزه، روش LSB است که در آن داده محرمانه به صورت مستقیم در کم ارزش‌ترین بیت پیکسل‌های تصویر پوشانه جاسازی می‌شود [۵]. الگوریتم‌های بسیاری از روش LSB برای جاسازی داده محرمانه استفاده کرده‌اند [۱۷-۱۴,۱۶-۱۰,۱۲-۶]. مرجع [۱۶] داده محرمانه را در تصاویر رنگی جاسازی می‌کند. ابتدا داده محرمانه به منظور افزایش امنیت رمز می‌شود. سپس تصویر پوشانه به سه کانال رنگی مدل RGB[12] (قرمز، سبز، آبی) تفکیک می‌شود. برای جاسازی یک بیت از داده محرمانه، مقدار آن با بیت LSB یک پیکسل از کانال قرمز XOR شده و براساس نتیجه به دست آمده، داده محرمانه در بیت LSB کانال آبی یا سبز پیکسل متناظر جایگزین می‌شود.

در [۱۷] نیز داده محرمانه برای افزایش امنیت رمز می‌شود. در این روش تصویر پوشانه براساس مدل رنگی HVS[13] به سه کانال رنگ، اشباع، و ارزش تفکیک شده و داده محرمانه با استفاده از روش LSB در کانال اشباع ذخیره می‌شود. برای جاسازی داده محرمانه، ابتدا کانال اشباع تصویر بلوک بندی می‌شود. سپس داده محرمانه در بیت LSB پیکسل‌های بلوک‌ها جاسازی می‌شود. ترتیب انتخاب بلوک‌ها و همچنین نحوه پیمایش پیکسل‌ها در هر بلوک با استفاده از یک کلید محرمانه مشخص می‌شود. الگوریتم PVD [۱۹] روشی شناخته شده در حوزه روش‌های دامنه فضایی است که براساس میزان اختلاف مقدار پیکسل‌های متوالی در تصویر پوشانه عمل می‌کند. در این روش تصویر پوشانه به بلوک‌هایی با اندازه دو پیکسل تقسیم می‌شود. تعداد بیت‌های ذخیره شده در هر بلوک متناسب با اختلاف مقدار پیکسل‌های آن خواهد بود. الگوریتم‌های ارائه شده در [۲۰,۲۱] با توسعه روش PVD مقدار PSNR و ظرفیت جاسازی تصویر میزبان را افزایش داده‌اند.

مراجع [۱۴-۱۰,۱۲-۷] داده محرمانه را از نوع تصویر در نظر گرفته و الگوریتمی مبتنی بر روش دامنه فضایی برای جاسازی تصویر محرمانه ارائه داده‌اند. در الگوریتم ارائه شده در [۷] برای فشرده کردن تصویر محرمانه ابتدا تبدیل کسینوسی گسسته[14] روی آن اعمال شده و سپس تصویر تبدیل شده کوانتیزه[15] می‌شود. خروجی به دست آمده با استفاده از روش LSB در تصویر پوشانه جاسازی می‌شود. در [۸] برای فشردگی بیشتر تصویر محرمانه، ابتدا فیلتر منظم[16] و سپس تبدیل کسینوسی گسسته بر روی آن اعمال می‌شود. ایراد عمده الگوریتم‌های ارائه شده در [۷,۸] آن است که تصویر محرمانه را با اتلاف[17] فشرده می‌کنند. در نتیجه کیفیت تصویر محرمانه بازیابی شده در مقایسه با تصویر محرمانه اصلی کاهش خواهد یافت.

الگوریتم‌های پیشنهادی در [۱۱-۹] بین کیفیت تصاویر محرمانه بازیابی شده و میزبان توازن ایجاد کرده‌اند. مرجع [۹] از یادگیری عمیق[18] برای پنهان نگاری تصاویر محرمانه بهره جسته است. در اینجا دو شبکه عصبی عمیق برای جاسازی و استخراج تصویر محرمانه ارائه شده است. همچنین برای جاسازی تصویر محرمانه، از تمام بیت‌های پیکسل‌های تصویر پوشانه - و نه فقط بیت LSB آنها - استفاده می‌شود. در [۱۰]، تصویر محرمانه قبل از جاسازی فشرده می‌شود. برای جاسازی تصویر محرمانه، بسته به اندازه آن از ترکیبی از چهار بیت کم ارزش پیکسل‌های تصویر پوشانه استفاده می‌شود. همچنین روش‌های مختلف پیمایش پیکسل‌های تصویر پوشانه بررسی شده تا پیمایشی که PSNR تصویر میزبان را بیشینه می‌کند به‌دست آید.

روش‌های ارائه شده در [۱۴-۱۲] تصویر محرمانه را بدون اتلاف جاسازی می‌کنند. مرجع [۱۲] تعداد تغییرات در بیت‌های LSB تصویر میزبان را کاهش داده است. در اینجا تصویر محرمانه پردازش شده تا تعداد بیت‌های صفر تصویر محرمانه افزایش یابد. برای این منظور، پیکسل‌هایی که فراوانی بیشتری دارند به سطوح خاکستری که تعداد بیت یک کمتری دارند، نگاشت می‌شوند. همچنین تصویر پوشانه پردازش می‌شود تا با کمترین تغییر در کیفیت تصویر، تعداد بیت‌های LSB که مقدار صفر دارند افزایش یابد. در ادامه، تصویر پوشانه با استفاده از روش LSB جاسازی می‌شود. در روش ارائه شده در [۱۳]، ابتدا هر دو تصویر پوشانه و محرمانه به بلوک‌هایی با اندازه یکسان تقسیم‌بندی می‌شوند. هر بلوک از تصویر محرمانه در یک بلوک از تصویر پوشانه جاسازی می‌شود. هدف الگوریتم پیشنهادی یافتن نگاشت بهینه بین بلوک‌های تصاویر محرمانه و پوشانه است به نحوی که مقدار PSNR تصویر میزبان بیشینه شود. برای این کار از الگوریتم کلونی زنبور عسل استفاده شده است. در [۱۴] تصویر پوشانه بلوک بندی شده و بلوک‌ها بسته به شدت تغییرات مقادیر پیکسل‌هایشان به چند دسته تقسیم می‌شوند. در بلوک‌های متعلق به هر دسته، تعداد مشخصی بیت از تصویر محرمانه در بیت‌های کم‌ارزش‌تر پیکسل‌های آنها جاسازی می‌شوند. دسته بندی بلوک‌ها براساس یک مقدار حد آستانه انجام می‌شود. مقدار حد آستانه به نحوی تنظیم می‌شود که تصویر محرمانه بدون اتلاف جاسازی شود.

از مزیت‌های روش دامنه فضایی می‌توان به ظرفیت بالای جاسازی و عدم پیچیدگی محاسباتی اشاره کرد. این ویژگی‌ها باعث شده است که این روش در مقایسه با روش دامنه فرکانسی کاربرد بیشتری داشته باشد. ضعف عمده این روش آسیب پذیری آن در مقابل حملات تحلیل پنهان نگاری است. این مسئله در مراجع مختلف از جمله [۲۴-۲۲] مورد بررسی قرار گرفته است. همچنین برای مقاوم سازی الگوریتم‌های دامنه فرکانسی در مقابل حملات، تکنیک‌های مختلفی ارائه شده است که از آن جمله می‌توان به [۲۷-۲۵] اشاره کرد.

در روش دامنه فرکانسی، یکی از تبدیلات رایج ریاضی مانند تبدیل فوریه[19] [۲۸]، تبدیل کسینوسی گسسته [۲۹]، تبدیل موجک گسسته[20] [۳۰,۳۱]، و تبدیل موجک عدد صحیح[21] [۳۲]، بر روی تصویر پوشانه اعمال می‌شود. سپس داده محرمانه در مولفه‌های فرکانس بالا جاسازی می‌شود. در ادامه با اعمال تبدیل معکوس، تصویر پوشانه به دست می‌آید. روش پیشنهاد شده در [۳۳] از تبدیل موجک تطبیقی[22] برای جاسازی داده محرمانه استفاده کرده است. در این مقاله از الگوریتم ژنتیک برای مشخص نمودن مقادیر پارامترهای تبدیل استفاده شده است. همچنین داده محرمانه در مولفه‌هایی جاسازی می‌شود که معادل پیکسل‌های لبه تصویر پوشانه در دامنه فضایی هستند. این کار کیفیت تصویر میزبان را افزایش می‌دهد.

پنهان نگاری تصاویر محرمانه با استفاده از روش دامنه فرکانسی در [۱۱,۱۵] بررسی شده است. مرجع [۱۱] از تبدیل موجک و نگاشت آرنولد برای پنهان نگاری بهره جسته است. مکان‌های پیکسل‌های تصویر محرمانه با اعمال نگاشت آرنولد به صورت شبه تصادفی تغییر داده می‌شوند. در ادامه تصاویر محرمانه تبدیل شده و پوشانه با استفاده از تبدیل موجک مبتنی بر گراف به حوزه دامنه فرکانسی انتقال داده می‌شوند. تصویر میزبان با اعمال معکوس تبدیل موجک بر روی مجموع وزن‌دار خروجی‌های تصاویر تبدیل شده به‌دست می‌آید. پارامتر وزن بین مقادیر PSNR تصویر میزبان و تصویر محرمانه استخراج شده (نسبت به تصویر محرمانه اصلی) توازن ایجاد می‌کند. در [۱۵] از تبدیل موجک مترقی[23] برای جاسازی تصاویر محرمانه استفاده شده است. در این روش ابتدا تبدیل موجک مترقی دو بعدی بر تصویر پوشانه اعمال شده تا ماتریس‌های ضرایب متناظر با آن به‌دست آید. سپس با استفاده از یک تابع آشوب[24]، ضرایب هر ماتریس درهم ریخته شده و بیت‌های تصویر محرمانه در آنها جاسازی می‌شوند.

مقالات بررسی شده در این بخش در جدول (۱) جمع بندی شده‌اند.

۱-۳- سازمان‌دهی مقاله

ادامه مقاله به صورت زیر سازمان‌دهی شده است. الگوریتم پیشنهادی در بخش ۲ ارائه شده است. در ادامه کارایی الگوریتم ارائه شده در بخش ۳ تحلیل و بررسی شده است. در نهایت مقاله در بخش ۴ جمع بندی شده است.

۲- الگوریتم LHCIS

در این بخش الگوریتم LHCIS برای جاسازی و همچنین استخراج تصویر محرمانه شرح داده شده است. در الگوریتم جاسازی ارائه شده، ابتدا تصویر محرمانه با استفاده از روش ارائه شده در بخش ۲-۱ کد می‌شود. سپس تصویر کد شده با استفاده از الگوریتم LSB در تصویر پوشانه جاسازی می‌شود. برای استخراج تصویر محرمانه، ابتدا تصویر کد شده با اعمال LSB به‌دست می‌آید. در ادامه با استفاده از روش کدگشایی ارائه شده در بخش ۲-۲، تصویر محرمانه بازیابی می‌شود. برای توضیح بیشتر روش کدگذاری پیشنهادی، در بخش ۲-۳ این الگوریتم بر روی یک تصویر محرمانه با ابعاد ۸×۸ اعمال شده است.

۲-۱- جاسازی تصویر محرمانه

الگوریتم جاسازی تصویر محرمانه شامل فشرده کردن تصویر و جاسازی آن در تصویر پوشانه با استفاده از روش LSB است. فشرده سازی با توجه به ساختار داده تصویری انجام می‌شود. در تصاویر، مقادیر پیکسل‌های مجاور تفاوت چندانی با هم ندارند. بنابراین مقادیر به دست آمده از تفاضل پیکسل‌های مجاور اعداد کوچکی خواهند بود که برای ذخیره نمودن آنها تعداد بیت کمی لازم است. با توجه به این خصوصیت، در روش فشرده سازی پیشنهادی، کدگذاری بر روی مقادیر تفاضل پیکسل‌های مجاور انجام می‌شود. فشرده کردن تصویر محرمانه حجم آن را به نحو قابل ملاحظه‌ای کاهش می‌دهد. در نتیجه، تصویر میزبان نسبت به تصویر پوشانه تغییرات کمی خواهد داشت. مزیت دیگر روش ارائه شده آن است که تصویر محرمانه را بدون اتلاف فشرده می‌کند. بنابراین، بر خلاف الگوریتم‌های ارائه شده در [۱۱-۷]، کیفیت تصویر محرمانه استخراج شده کاهش نخواهد یافت.

در ادامه روش ارائه شده برای فشرده سازی تصویر محرمانه S با ابعاد $m\times n$ به تفضیل توضیح داده شده است.

مرحله اول (ساخت تصویر تفاضل): ابتدا تصویر تفاضل D از روی تصویر محرمانه S ساخته می‌شود. هر پیکسل این تصویر با محاسبه قدر مطلق تفاضل پیکسل متناظر آن در تصویر S از پیکسل مجاورش به دست می‌آید. همچنین برای بازیابی تصویر S، باید علامت مقدار تفاضل پیکسل‌های مجاور نیز ذخیره شود. ماتریس G برای این منظور تعریف شده است. نحوه تشکیل تصویر D و ماتریس G در ادامه بیان شده است

فاز اول (تشکیل تصویر *D*): هر پیکسل d_{ij} به صورت قدر مطلق تفاضل پیکسل s_{ij} از پیکسل مجاور آن تعریف می‌شود:

$$d_{ij}=\begin{cases} abs(s_{i,j-1}-s_{ij}) & 1\le j\le n \\ s_{ij} & j=1 \end{cases} \qquad (۱)$$

که در نماد abs نشان دهنده تابع قدر مطلق است.

فاز دوم (تشکیل ماتریس *G*): ماتریس G بیان‌گر علامت متناظر با پیکسل‌های تصویر D است. هر درایه g_{ij} این ماتریس یک مقدار یک بیتی است که به صورت زیر مقداردهی می‌شود:

$$g_{ij}=\begin{cases} 0 & 1< j\le n, s_{ij}\le s_{i,j-1} \\ 1 & 1< j\le n, s_{ij}> s_{i,j-1} \\ 0 & j=1 \end{cases} \qquad (۲)$$

مرحله دوم (کد کردن تصویر تفاضل): در این مرحله تصویر D کد می‌شود. در روش کدگذاری پیشنهادی، به این نکته توجه شده است که حذف صفرهای سمت چپ پیکسل‌های تصویر D باعث از

جدول (۱): مشخصات الگوریتم‌های پنهان نگاری ارائه شده

مرجع	روش جاسازی	نوع تصویر پوشانه	نوع داده محرمانه	بدون اتلاف	سال ارائه
[۵,۱۹-۲۱, ۲۵,۲۷]	فضایی	هر دو	متن	✓	۲۰۰۴, ۲۰۰۳ ۲۰۱۷, ۲۰۲۰ ۲۰۱۴, ۲۰۰۴
[۶,۱۸]	فضایی	خاکستری	متن	✓	۲۰۲۱, ۱۳۸۸
[۷,۸]	فضایی	هر دو	تصویر	-	۲۰۱۷, ۱۳۹۷
[۹]	فضایی	رنگی	تصویر	-	۲۰۱۹
[۱۰]	فضایی	هر دو	تصویر	-	۲۰۱۴
[۱۱]	فرکانسی	خاکستری	تصویر	-	۲۰۱۸
[۱۲,۱۳]	فضایی	هر دو	تصویر	✓	۲۰۱۹, ۲۰۱۸
[۱۴]	فضایی	خاکستری	تصویر	✓	۲۰۱۵
[۱۵]	فرکانسی	خاکستری	تصویر	✓	۲۰۱۷
[۱۶,۱۷]	فضایی	رنگی	متن	✓	۲۰۱۷, ۲۰۱۸
[۲۸,۳۱]	فرکانسی	رنگی	متن	✓	۲۰۱۶, ۲۰۱۸
[۲۹,۳۰]	فرکانسی	هر دو	متن	✓	۲۰۱۸, ۲۰۲۰
[۳۲,۳۳]	فرکانسی	خاکستری	متن	✓	۲۰۲۰, ۲۰۱۷
LHCIS	فضایی	هر دو	تصویر	✓	

دست رفتن اطلاعات نمی‌شود. به عنوان مثال در پیکسل 00001011 فقط چهار بیت سمت راست با ارزش و حاوی اطلاعات است. بنابراین می‌توان این پیکسل را به صورت 1011 کد کرد. با توجه به اینکه پیکسل‌های تصویر D اعداد کوچکی هستند، حجم پیکسل‌های کد شده بسیار کم بوده و تصویر به میزان قابل توجهی فشرده خواهد شد.

با توجه به متغیر بودن طول پیکسل‌های کد شده، مقدار طول آنها نیز باید در تصویر پوشانه جاسازی شود. سربار ناشی از ذخیره کردن طول پیکسل‌ها قابل توجه بوده و نرخ فشرده سازی را کاهش می‌دهد. برای حل این مشکل، تصویر D بلوک بندی شده و هر بلوک به صورت جداگانه کد می‌شود. بنابراین، برای هر بلوک فقط یک مقدار به عنوان طول ذخیره خواهد شد. مقدار طول متناظر با بلوک‌ها در ماتریس BL ذخیره می‌شود. همچنین تصویر خروجی مرحله کدگذاری، تصویر O نامیده می‌شود. در ادامه نحوه ساخت ماتریس BL و تصویر O توضیح داده می‌شود.

فاز اول (تشکیل ماتریس BL): برای این منظور، ابتدا تعداد بیت‌های مورد نیاز برای ذخیره نمودن پیکسل d_{ij} محاسبه می‌شود:

$$l_{ij} = ceil\left(\lg_2 d_{ij}\right) \qquad (۳)$$

که در آن l_{ij} نشان دهنده مینیمم تعداد بیت‌های لازم برای نمایش d_{ij} است. مقدار l_{ij} در واقع برابر طول رشته به دست آمده حاصل از حذف بیت‌های صفر سمت چپ پیکسل d_{ij} است. برای مثال اگر مقدار d_{ij} برابر 00001011 باشد، متغیر l_{ij} برابر چهار خواهد بود. همچنین تابع $ceil$ برای محاسبه مقدار سقف به کار رفته است.

همان‌طور که اشاره شد، برای کاهش سربار ناشی از ذخیره کردن طول پیکسل‌ها، تصویر D بلوک بندی شده و یک مقدار به عنوان طول هر بلوک در نظر گرفته می‌شود. مقدار ذخیره شده برای بلوک B_{pq} با bl_{pq} نشان داده شده و به صورت زیر محاسبه می‌گردد:

$$bl_{pq} = \max_{d_{ij} \in B_{pq}} l_{ij} \qquad (۴)$$

در این مقاله ابعاد بلوک‌ها ۴×۴ در نظر گرفته شده‌است. با توجه به اینکه پیکسل‌های تصویر O حداکثر هشت بیتی هستند، می‌توان مقدار طول بلوک‌ها را در چهار بیت ذخیره کرد.

فاز دوم (تشکیل تصویر O): در انتها تصویر کد شده O با ابعاد $m \times n$ ساخته می‌شود. این کار با استفاده از تصویر D و ماتریس BL انجام می‌شود. مقدار هر پیکسل $o_{ij} \in B_{pq}$ با استخراج bl_{pq} بیت کم ارزش پیکسل d_{ij} محاسبه می‌شود. برای مثال فرض کنید مقدار d_{ij} برابر 00001011 باشد. همچنین $d_{ij} \in B_{pq}$ بوده و مقدار bl_{pq} برابر پنج باشد. در این صورت مقدار پیکسل o_{ij} برابر 01011 خواهد بود.

جاسازی تصویر محرمانه: برای جاسازی تصویر محرمانه، ابتدا ماتریس‌های G و BL با استفاده از روش LSB در تصویر پوشانه جاسازی می‌شوند. در ادامه بلوک‌های تصویر کد شده O به صورت ردیفی با استفاده از روش LSB جاسازی می‌شوند.

ماتریس BL شامل داده‌های چهار بیتی و با ابعاد $m/۴ \times n/۴$ است. بنابراین اندازه این ماتریس برابر $mn/۴$ خواهد بود. ماتریس G شامل $m \times n$ درایه یک بیتی است. همچنین، هر بلوک B_{pq} شامل $۴\times۴\times bl_{pq}$ بیت است. بنابراین، تعداد کل بیت‌های ذخیره شده در تصویر میزبان به صورت زیر محاسبه می‌شود:

$$No.of\ bits = \frac{5}{4}mn + \sum_{p=1}^{m/4}\sum_{q=1}^{n/4} 16 bl_{pq} \qquad (۵)$$

فلوچارت جاسازی تصویر محرمانه در شکل (۱) نمایش داده شده است.

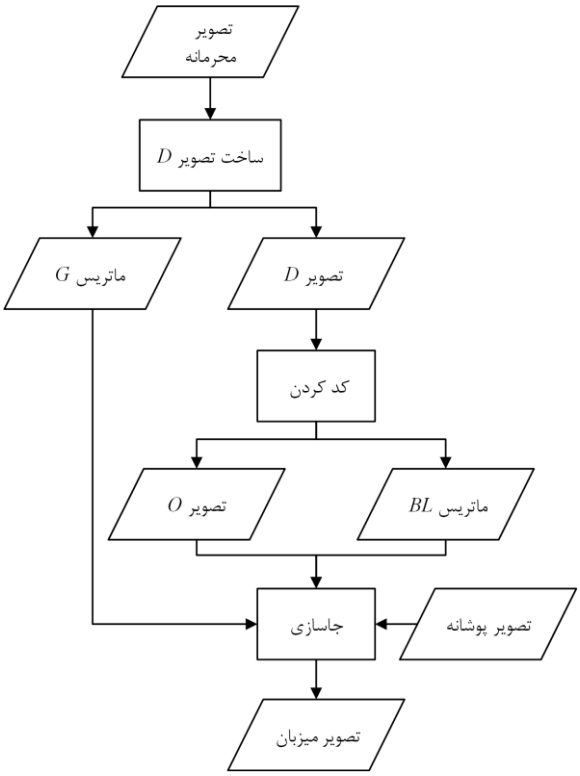
۲-۲- استخراج تصویر محرمانه

برای استخراج تصویر محرمانه، ابتدا ماتریس‌های G و BL، و تصویر کد شده O با استفاده از الگوریتم LSB از تصویر میزبان استخراج می‌شود. سپس مراحل الگوریتم فشرده سازی به صورت وارون اعمال می‌شوند تا تصویر محرمانه حاصل شود. مراحل کار در ادامه توضیح داده شده‌است.

بازیابی داده‌های جاسازی شده: برای بازیابی تصویر کد شده O، ابتدا ماتریس BL از تصویر میزبان استخراج می‌شود. در ادامه این تصویر با استفاده از مقادیر متغیرهای bl بازسازی می‌شود. با توجه به اینکه بلوک‌های تصویر O به صورت ردیفی جاسازی شده‌اند، محدوده ذخیره سازی پیکسل $o_{ij} \in B_{pq}$ به صورت زیر به‌دست می‌آید:

$$b_{ij} = \frac{5}{4}mn + \sum_{r=1}^{p-1}\sum_{s=1}^{n/4} 16\,bl_{rs} + \sum_{s=1}^{q-1} 16\,bl_{ps} + ((i \div 4)\,4 + j)\,bl_{pq} \quad (۶)$$

$$e_{ij} = b_{ij} + bl_{pq} \quad (۷)$$



شکل (۱): فلوچارت جاسازی تصویر محرمانه

که در آن b_{ij} شماره بایتی از تصویر میزبان است که اولین بیت o_{ij} در آن جاسازی شده است. همچنین آخرین بیت o_{ij} در بایت e_{ij} تصویر میزبان جاسازی شده است.

مرحله اول (کدگشایی تصویر تفاضل): در این مرحله تصویر D با استفاده از تصویر کد شده O بازسازی می‌شود. برای بازسازی پیکسل $d_{ij} \in B_{pq}$، به تعداد $8\text{-}bl_{pq}$ بیت صفر به سمت چپ بیت o_{ij} افزوده می‌شود. برای مثال فرض کنید مقدار o_{ij} برابر 01011 باشد. همچنین $d_{ij} \in B_{pq}$ بوده و مقدار bl_{pq} برابر پنج باشد. در این صورت، مقدار پیکسل o_{ij} برابر 00001011 خواهد بود.

مرحله دوم (بازیابی تصویر محرمانه): در ادامه تصویر محرمانه S از روی تصویر D بازیابی می‌شود. هر پیکسل این تصویر با توجه به مقادیر پیکسل‌های متناظر در تصویر D و ماتریس G به دست می‌آید:

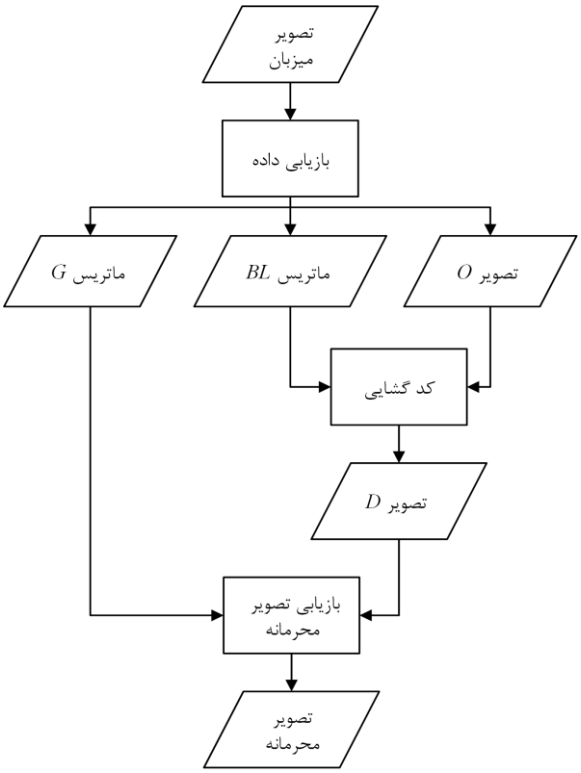
$$s_{ij} = \begin{cases} s_{i,j-1} - d_{ij} & 1 < j \le n, g_{ij} = 0 \\ s_{i,j-1} + d_{ij} & 1 < j \le n, g_{ij} = 1 \\ d_{ij} & j = 1 \end{cases} \quad (۸)$$

لازم به ذکر است که برای حصول تصویر محرمانه، ستون‌های آن باید به ترتیب - از اولین تا n امین ستون - بازیابی شوند.

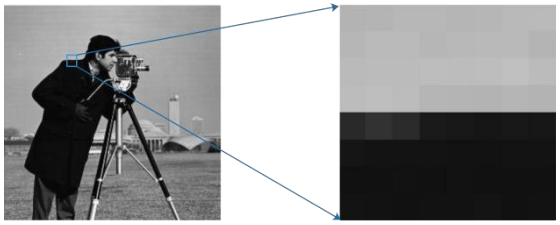
فلوچارت استخراج تصویر محرمانه در شکل (۲) آورده شده است.

۲-۳- مثالی از نحوه کدگذاری تصاویر محرمانه

در این بخش روش کدگذاری پیشنهادی بر روی یک قطعه ۸×۸ از تصویر محرمانه Cameraman اعمال شده است. بلوک انتخاب شده در شکل (۳) مشخص شده است.



شکل (۲): فلوچارت استخراج تصویر محرمانه



(الف)

177	179	180	183	183	181	182	185	186
186	182	186	186	182	184	185	185	180
186	186	187	187	189	188	189	192	187
184	188	190	188	181	180	179	181	179
29	41	50	43	26	24	22	24	23
19	21	19	19	19	18	18	19	19
19	17	17	18	17	18	17	17	17
19	19	18	17	18	18	20	17	18

(ب)

شکل (۳): قطعه انتخاب شده از تصویر Cameraman: (الف) موقعیت بلوک در تصویر، (ب) مقادیر عددی متناظر با پیکسل‌های بلوک. ستون تکی سمت چپ نشان دهنده ستون سمت چپ بلوک انتخاب شده در تصویر است

در مرحله اول، ابتدا تصویر D متناظر با قطعه نمایش داده شده در شکل (۳) با استفاده از (۱) ساخته می‌شود. این تصویر در شکل (۴) نشان داده شده است.

-2	-1	-3	0	2	-1	-3	-1
4	-4	0	4	-2	-1	0	5
0	-1	0	-2	1	-1	-3	5
-4	-2	2	7	1	1	-2	2
-12	-9	7	17	2	2	-2	1
-2	2	0	0	1	0	-1	0
2	0	-1	1	-1	1	0	0
0	1	1	-1	0	-2	3	-1

شکل (۴): تصویر D متناظر با شکل (۳)

در فاز دوم از مرحله اول، ماتریس G متناظر با تصویر D نمایش داده شده در شکل (۴) تشکیل می‌شود. این ماتریس در شکل (۵) آورده شده است.

1	1	1	0	0	1	1	1
0	1	0	0	1	1	0	0
0	1	0	1	0	1	1	0
1	1	0	0	0	0	1	0
1	1	0	0	0	0	1	0
1	0	0	0	0	0	1	0
0	0	1	0	1	0	0	0
0	0	0	1	0	1	0	1

شکل (۵): ماتریس G متناظر با تصویر D ارائه شده در شکل (۴)

در ادامه در فاز اول از مرحله دوم، ماتریس BL ساخته می‌شود. برای این منظور، ابتدا تصویر به بلوک‌های ۴×۴ تقسیم می‌شود. با تعیین bl هر بلوک، ماتریس BL به‌دست می‌آید. به عنوان مثال در بلوک سمت چپ در پایین، بزرگ‌ترین پیکسل برابر 10001 است. بنابراین bl متناظر با این بلوک معادل پنج خواهد بود. مراحل کار در شکل (۶) نمایش داده شده است.

10	1	11	0	10	1	11	1
100	100	0	100	10	1	0	101
0	1	0	10	1	1	11	101
100	10	10	111	1	1	10	10
1100	1001	111	10001	10	10	10	1
10	10	0	0	1	0	1	0
10	0	1	1	1	1	0	0
0	1	1	1	0	10	11	1

(الف)

3	3
5	2

(ب)

0011	0011
0101	0010

(ج)

شکل (۶): ماتریس BL متناظر با تصویر D در شکل (۴): (الف) نمایش باینری تصویر D، (ب) ماتریس BL، (ج) نمایش باینری ماتریس BL

در نهایت در فاز دوم تصویر O ساخته می‌شود. تصویر O به دست آمده در شکل (۷) نمایش داده شده است. همان‌طور که در این شکل دیده می‌شود، تعداد بیت‌های هر پیکسل برابر با مقدار bl بلوک متناظر با آن است. برای مثال تعداد بیت‌های پیکسل (۲،۳) برابر سه است که این مقدار معادل درایه (۱،۱) ماتریس BL در شکل (۶)(ب) است.

010	001	011	000	010	001	011	001
100	100	000	100	010	001	000	101
000	001	000	010	001	001	011	101
100	010	010	111	001	001	010	010
01100	01001	00111	10001	10	10	10	01
00010	00010	00000	00000	01	00	01	00
00010	00000	00001	00001	01	01	00	00
00000	00001	00001	00001	00	10	11	01

شکل (۷): تصویر O متناظر با تصویر D نمایش داده شده در شکل (۴)

۳- نتایج شبیه‌سازی

در این بخش کارایی الگوریتم LHCIS در جاسازی تصاویر محرمانه ارزیابی شده است. برای این منظور، روش پیشنهادی با الگوریتم L_IWSIM [۱۲] و روش‌های ارائه شده در [۱۰،۱۳] مقایسه شده است. در [۱۰،۱۳] به ترتیب از الگوریتم‌های ژنتیک و کلونی زنبور عسل برای جاسازی تصویر محرمانه استفاده شده است. بر این اساس، این الگوریتم‌ها در ادامه GA[۲۵] و ABC[۲۶] نامیده شده‌اند. برای پیاده سازی الگوریتم‌ها، از نرم افزار Matlab 2015a استفاده شده است. کارایی الگوریتم‌های مورد مطالعه از نظر کیفی و کمی مورد بررسی قرار گرفته است. برای بررسی کیفی الگوریتم‌ها، نمودار هیستوگرم چند تصویر پوشانه و میزبان در بخش ۳-۱ با هم مقایسه شده‌اند. در مطالعه کمی الگوریتم‌ها، از معیارهای PSNR و SSIM[۲۷] استفاده شده است. این معیارها به ترتیب در بخش‌های ۳-۲ و ۳-۳ بررسی شده‌اند.

تصاویر پوشانه و محرمانه از پایگاه داده استاندارد SIPI که در اکثر مقالات مورد استفاده قرار می‌گیرد، انتخاب شده‌اند. این تصاویر در شکل (۸) نمایش داده شده‌اند. تصاویر Lena، House، Splash، Baboon، Airplane، Sailboat، و Peppers، به عنوان تصویر پوشانه، و تصاویر Cameraman، Clock، و Walter Cronkite به عنوان تصویر محرمانه مورد استفاده قرار گرفته‌اند. اندازه تصاویر پوشانه و محرمانه به ترتیب برابر ۵۱۲×۵۱۲ و ۲۵۶×۲۵۶پیکسل است. همچنین تصاویر پوشانه رنگی و تصاویر محرمانه خاکستری هستند.

۳-۱- نمودار هیستوگرام

یکی از روش‌های رایج نمایش پراکندگی پیکسل‌های تصویر، استفاده از نمودار هیستوگرام است. در محور افقی نمودار هیستوگرام بازه عددی قابل قبول برای پیکسل‌های تصویر قرار می‌گیرد که برابر [۰-۲۵۵] است. محور عمودی نیز نشان‌دهنده فراوانی پیکسل‌ها است. یکی از معیارهای ارزیابی الگوریتم‌های پنهان نگاری، شباهت بین هیستوگرام-

های تصاویر پوشانه و میزبان است. بیشتر بودن میزان شباهت این نمودارها نشان دهنده کارایی بهتر الگوریتم پنهان نگاری ارائه شده است. شکل (۹) هیستوگرام‌های تصویر Lena قبل و بعد از جاسازی تصاویر محرمانه مختلف را نمایش می‌دهد. همان‌طور که در اینجا مشاهده می‌شود، هیستوگرام‌های تصویر Lena قبل و پس از جاسازی تصاویر محرمانه تغییر قابل توجهی که با چشم انسان قابل شناسایی باشد، نداشته‌اند. دلیل این مسئله آن است که در الگوریتم پیشنهادی تصویر محرمانه به خوبی فشرده شده است. در نتیجه میزان تغییرات در تصویر میزبان نسبت به تصویر پوشانه کمینه خواهد بود.

۳-۲- معیار PSNR

معیار PSNR یک شاخص مهم برای ارزیابی کمی الگوریتم‌های پنهان نگاری است. این معیار نشان دهنده نسبت ماکزیمم توان سیگنال‌های یک تصویر مفروض نسبت به ماکزیمم توان نویز اضافه شده به آن است. بیشتر بودن میزان PSNR تصویر دارای نویز نشان دهنده شباهت زیاد آن به تصویر اصلی است. در الگوریتم‌های پنهان نگاری، نویز تولید شده در تصویر میزبان ناشی از جاسازی داده یا تصویر محرمانه در آن است. بیشتر بودن مقدار PSNR تصویر میزبان به معنای آن است که جاسازی داده یا تصویر محرمانه اعوجاج کمتری در تصویر میزبان ایجاد کرده است. بنابراین، تصویر میزبان اختلاف کمتری با تصویر پوشانه خواهد داشت. مقدار PSNR تصویر میزبان با استفاده از (۹) به‌دست می‌آید:

$$PSNR = 10\log_{10}\left(\frac{MAX_I^2}{MSE}\right) \qquad (۹)$$

در اینجا MAX_I نشان دهنده مقدار بیشینه پیکسل‌های تصویر میزبان - یعنی مقدار ۲۵۵ - است. معیار MSE[۲۸] یا خطای میانگین مربعات برابر مجذور میزات اختلاف پیکسل‌های تصاویر پوشانه و میزبان است و به صورت زیر بیان می‌شود:

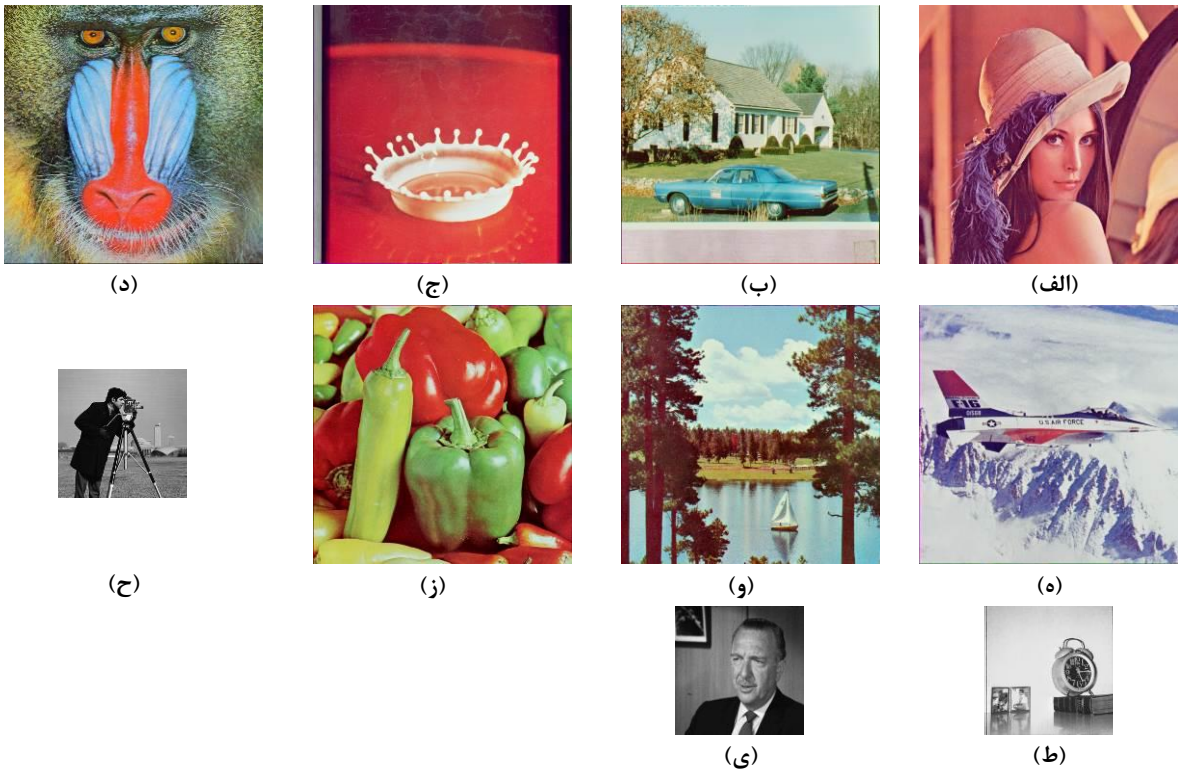
$$MSE = \frac{1}{mn}\sum_{i=1}^{n}\sum_{j=1}^{m}\left(t_{ij} - c_{ij}\right)^2 \qquad (۱۰)$$

با توجه به اینکه از تصاویر محرمانه مورد استفاده در ابعاد ۵۱۲×۵۱۲ پیکسل هستند، مقدار پارامترهای m و n برابر ۵۱۲ است. همچنین نمادهای t_{ij} و c_{ij} به ترتیب نشان دهنده پیکسل (i,j) از تصاویر میزبان و پوشانه هستند. با توجه به (۹)، معیارهای PSNR و MSE رابطه عکس با یکدیگر دارند. یعنی کاهش MSE و در نتیجه افزایش PSNR نشان از عملکرد خوب الگوریتم‌ها دارد.

مقادیر PSNR به دست آمده توسط الگوریتم‌های بررسی شده در جدول (۲) نشان شده است. همان‌طور که دیده می‌شود، الگوریتم پیشنهادی معیار PSNR را به میزان قابل توجهی بهبود داده است. میزان بهبود PSNR روش پیشنهادی نسبت به الگوریتم‌های GA، L_IWSIM، و ABC، به ترتیب برابر ۲/۱۹، ۲/۲۰، و ۲/۱۰ است. بنابراین میزان نویز ایجاد شده در تصویر میزبان توسط الگوریتم پیشنهادی در مقایسه با سایر الگوریتم‌ها کمتر است. همچنین مقدار متوسط افزایش PSNR برای تصاویر محرمانه Cameraman، Clock، و Walter Cronkite، به ترتیب برابر ۱/۶۷، ۲/۱۵، ۲/۶۶ است. تغییرات در افزایش PSNR به دلیل تفاوت تصاویر محرمانه از نظر میزان مسطح بودن نواحی مختلف آنها است. در تصویر Cameraman میزان تغییرات در پیکسل‌های مجاور نواحی مختلف قابل توجه است. در Clock برخی نواحی مسطح هستند و تغییرات در آنها کم است. مقدار نواحی مسطح و بدون تغییر در Walter Cronkite بیشتر است. با افزایش قابلیت فشردگی تصویر محرمانه، PSNR به دست آمده توسط الگوریتم پیشنهادی نیز افزایش می‌یابد.

جدول (۲): مقادیر PSNR الگوریتم‌های بررسی شده

تصویر محرمانه	تصویر پوشانه	GA	L_IWSIM	ABC	روش پیشنهادی
Cameraman	Lena	۵۲/۹۲	۵۲/۸۷	۵۳/۰۱	۵۴/۵۸
	House	۵۲/۹۲	۵۲/۹۲	۵۳/۰۲	۵۴/۶۳
	Splash	۵۲/۹۳	۵۲/۹۷	۵۳/۰۴	۵۴/۶۴
	Baboon	۵۲/۹۲	۵۲/۸۹	۵۳/۰۰	۵۴/۶۳
	Airplane	۵۲/۹۲	۵۲/۹۲	۵۳/۰۱	۵۴/۶۵
	Sailboat	۵۲/۹۲	۵۲/۹۲	۵۳/۰۱	۵۴/۶۴
	Peppers	۵۲/۹۲	۵۲/۹۶	۵۳/۰۳	۵۴/۶۴
	میانگین	۵۲/۹۲	۵۲/۹۲	۵۳/۰۲	**۵۴/۶۳**
Clock	Lena	۵۲/۹۳	۵۲/۸۷	۵۳/۰۲	۵۵/۰۱
	House	۵۲/۹۲	۵۲/۹۳	۵۳/۰۱	۵۳/۱۱
	Splash	۵۲/۹۴	۵۲/۹۸	۵۳/۰۳	۵۵/۱۲
	Baboon	۵۲/۹۳	۵۲/۹۰	۵۳/۰۱	۵۵/۰۸
	Airplane	۵۲/۹۲	۵۲/۹۲	۵۳/۰۰	۵۵/۱۲
	Sailboat	۵۲/۹۲	۵۲/۹۲	۵۳/۰۰	۵۵/۱۲
	Peppers	۵۲/۹۴	۵۲/۹۷	۵۳/۰۱	۵۵/۱۳
	میانگین	۵۲/۹۳	۵۲/۹۳	۵۳/۰۱	**۵۵/۱۱**
Walter Cronkite	Lena	۵۲/۹۳	۵۲/۸۷	۵۳/۰۰	۵۵/۵۸
	House	۵۲/۹۲	۵۲/۹۱	۵۳/۰۳	۵۵/۶۲
	Splash	۵۲/۹۴	۵۲/۹۸	۵۳/۰۴	۵۵/۶۳
	Baboon	۵۲/۹۲	۵۲/۹۰	۵۲/۹۹	۵۵/۶۱
	Airplane	۵۲/۹۲	۵۲/۹۲	۵۳/۰۱	۵۵/۶۳
	Sailboat	۵۲/۹۲	۵۲/۹۲	۵۳/۰۲	۵۵/۶۳
	Peppers	۵۲/۹۳	۵۲/۹۵	۵۳/۰۴	۵۵/۶۴
	میانگین	۵۲/۹۳	۵۲/۹۲	۵۳/۰۲	**۵۵/۶۲**

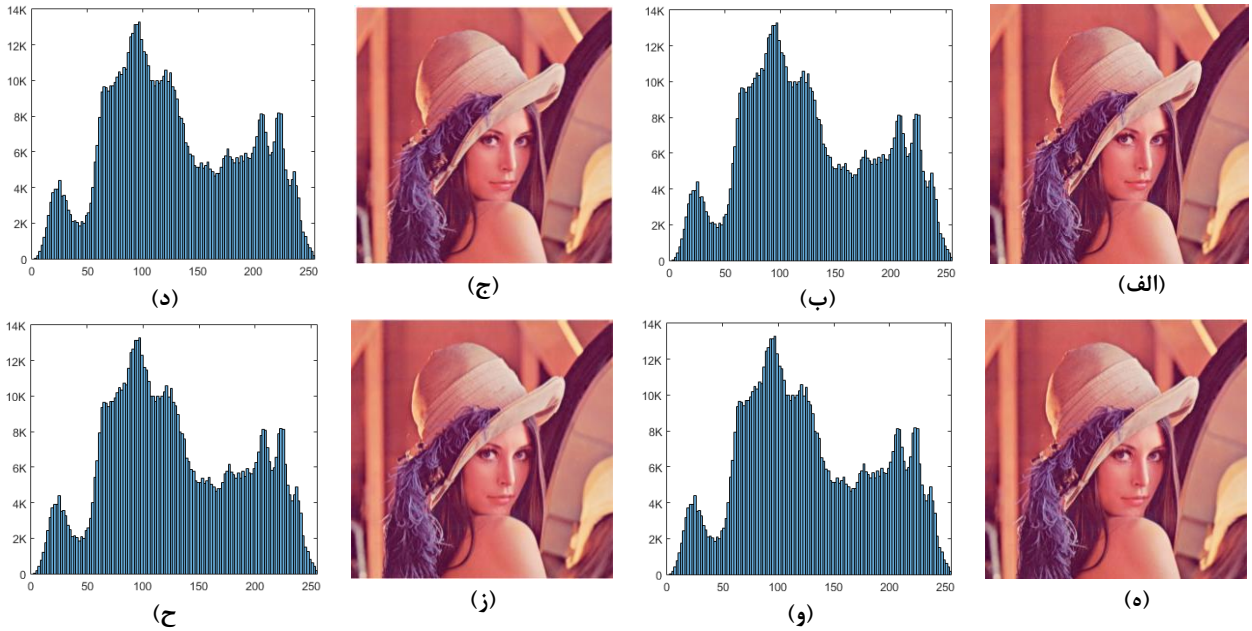


(الف) (ب) (ج) (د)

(ه) (و) (ز) (ح)

(ط) (ی)

شکل (۸): تصاویر انتخاب شده از مجموعه SIPI: (الف) Lena، (ب) House، (ج) Splash، (د) Baboon، (ه) Airplane، (و) Sailboat، (ز) Peppers، (ح) Cameraman، (ط) Clock، (ی) Walter Cronkite



(الف) (ب) (ج) (د)

(ه) (و) (ز) (ح)

شکل (۹): هیستوگرام تصویر میزبان Lena با جاسازی تصاویر محرمانه مختلف: (الف) تصویر پوشانه، (ب) هیستوگرام (الف)، (ج) تصویر محرمانه Cameraman، (د) هیستوگرام (ج)، (ه) تصویر محرمانه Clock، (و): هیستوگرام (ه)، (ز) تصویر محرمانه Walter Cronkite، (ح) هیستوگرام (ز)

	Peppers	۰/۹۹۹۹	۰/۹۹۹۹	۰/۹۹۹۹	۰/۹۹۹۹
	میانگین	۰/۹۹۹۵	۰/۹۹۹۵	۰/۹۹۹۵	**۰/۹۹۹۷**

۳-۳- معیار SSIM

معیار SSIM یا شباهت ساختاری یک شاخص شناخته شده برای سنجش نویز بر کیفیت تصاویر است. این معیار میزان شباهت ساختاری یک تصویر دارای نویز با همان تصویر در حالت بدون نویز را بیان می‌کند. بیشتر بودن مقدار SSIM به دست آمده نشان دهنده میزان شباهت بیشتر بین تصاویر بدون نویز و دارای نویز و کارایی بالاتر الگوریتم است. در حوزه روش‌های پنهان نگاری، نویز توسط داده یا تصویر محرمانه ایجاد می‌شود. بنابراین تصاویر میزبان و پوشانه نیز معادل تصاویر نویز دار و بدون نویز خواهند بود. مقدار شباهت ساختاری دو تصویر میزبان (T) و پوشانه (C) با استفاده از (۱۱) محاسبه می‌شود:

$$SSIM(C,T)=\frac{(2\mu_C\mu_T+C_1)(2\sigma_{CT}+C_2)}{(\mu_C^2+\mu_T^2+C_1)(\sigma_C^2+\sigma_T^2+C_2)} \qquad (۱۱)$$

جدول (۳) مقادیر SSIM حاصل از اعمال الگوریتم‌های پنهان نگاری مختلف را گزارش داده است. بر اساس نتایج این جدول، مقدار SSIM به دست آمده توسط الگوریتم پیشنهادی ۰/۰۰۰۱ نسبت به سایر روش‌ها بهبود یافته است. با توجه به نتایج به دست آمده در این بخش، الگوریتم پیشنهادی بیشترین کارایی را در مقایسه با سایر روش‌ها دارد.

جدول (۳): مقادیر SSIM الگوریتم‌های بررسی شده

تصویر محرمانه	تصویر پوشانه	GA	L_IWSIM	ABC	روش پیشنهادی
Cameraman	Lena	۰/۹۹۹۹	۰/۹۹۹۹	۰/۹۹۹۹	۰/۹۹۹۹
	House	۰/۹۹۹۳	۰/۹۹۹۴	۰/۹۹۹۴	۰/۹۹۹۵
	Splash	۰/۹۹۹۷	۰/۹۹۹۷	۰/۹۹۹۷	۰/۹۹۹۸
	Baboon	۰/۹۹۹۸	۰/۹۹۹۸	۰/۹۹۹۸	۰/۹۹۹۹
	Airplane	۰/۹۹۷۹	۰/۹۹۸۰	۰/۹۹۸۰	۰/۹۹۸۴
	Sailboat	۰/۹۹۹۶	۰/۹۹۹۷	۰/۹۹۹۷	۰/۹۹۹۷
	Peppers	۰/۹۹۹۹	۰/۹۹۹۹	۰/۹۹۹۹	۰/۹۹۹۹
	میانگین	۰/۹۹۹۴	۰/۹۹۹۵	۰/۹۹۹۵	**۰/۹۹۹۶**
Clock	Lena	۰/۹۹۹۹	۰/۹۹۹۹	۰/۹۹۹۹	۰/۹۹۹۹
	House	۰/۹۹۹۴	۰/۹۹۹۴	۰/۹۹۹۴	۰/۹۹۹۶
	Splash	۰/۹۹۹۷	۰/۹۹۹۷	۰/۹۹۹۷	۰/۹۹۹۸
	Baboon	۰/۹۹۹۸	۰/۹۹۹۸	۰/۹۹۹۸	۰/۹۹۹۹
	Airplane	۰/۹۹۷۹	۰/۹۹۸۱	۰/۹۹۸۱	۰/۹۹۸۵
	Sailboat	۰/۹۹۹۷	۰/۹۹۹۷	۰/۹۹۹۷	۰/۹۹۹۸
	Peppers	۰/۹۹۹۹	۰/۹۹۹۹	۰/۹۹۹۹	۰/۹۹۹۹
	میانگین	۰/۹۹۹۵	۰/۹۹۹۵	۰/۹۹۹۵	**۰/۹۹۹۶**
Walter Cronkite	Lena	۰/۹۹۹۹	۰/۹۹۹۹	۰/۹۹۹۹	۰/۹۹۹۹
	House	۰/۹۹۹۴	۰/۹۹۹۴	۰/۹۹۹۴	۰/۹۹۹۶
	Splash	۰/۹۹۹۷	۰/۹۹۹۷	۰/۹۹۹۷	۰/۹۹۹۸
	Baboon	۰/۹۹۹۸	۰/۹۹۹۸	۰/۹۹۹۸	۰/۹۹۹۹
	Airplane	۰/۹۹۷۹	۰/۹۹۸۱	۰/۹۹۸۱	۰/۹۹۸۷
	Sailboat	۰/۹۹۹۶	۰/۹۹۹۷	۰/۹۹۹۷	۰/۹۹۹۸

۴- نتیجه‌گیری

در این مقاله، الگوریتم LHCIS برای پنهان نگاری تصاویر محرمانه ارائه شده است. در الگوریتم پیشنهادی، تصویر محرمانه در دو مرحله، شامل تشکیل و کد کردن تصویر تفاضل، فشرده می‌شود. هر پیکسل تصویر تفاضل از تفریق دو پیکسل از تصویر محرمانه، شامل پیکسل متناظر و پیکسل مجاور آن، به دست می‌آید. برای کد کردن تصویر تفاضل، تصویر بلوک بندی شده و پیکسل‌های هر بلوک به صورت مستقل کد می‌شوند. در نهایت تصویر کد شده با استفاده از روش LSB در تصویر پوشانه جاسازی می‌شود. ویژگی مهم الگوریتم LHCIS، توجه به ساختار تصویر محرمانه برای فشرده سازی حداکثری آن است. یک مزیت دیگر الگوریتم پیشنهادی آن است که تصویر محرمانه را بدون اتلاف جاسازی می‌کند. در نتیجه تصویر بازیابی شده دقیقا معادل تصویر اصلی خواهد بود. با توجه به نتایج به دست آمده از الگوریتم ارائه شده، نتیجه گیری می‌شود که این روش معیارهای PSNR و SSIM را بهبود داده و تصویر محرمانه را با ایجاد کمترین اعواجاج در تصویر میزبان جاسازی کرده است.

مراجع

[1] Kadhim, I. J., Premaratne, P., Vial, P. J., Halloran, B., "Comprehensive Survey of Image Steganography: Techniques, Evaluations, and Trends in Future Research", Neurocomputing, vol. 335, pp. 299-326, 2019.

[2] Chai, X., Zheng, X., Gan, Z., Han, D., Chen, Y., "An Image Encryption Algorithm Based on Chaotic System and Compressive Sensing", Signal Processing, vol. 148, pp. 124-144, 2018.

[3] Hussain, M., Abdul Wahab, A. W., Idris, Y. I. B., Ho, A. T. S., Jung, K-H., "Image Steganography in Spatial Domain: A Survey", Signal Processing: Image Communication, vol. 65, pp. 46-66, 2018.

[۴] نعمتی نیا، محمد صادق، اقلیدس، ترانه، پاینده، علی، "بهبود حمله حدس و تعیین اکتشافی به سامانه های رمز جریانی TIPSY و SNOW1.0"، پردازش علائم و داده‌ها، دوره ۱۲، شماره ۴، صفحه ۴۲-۳۳، ۱۳۹۴.

[5] Chan, C. K., Cheng, L. M., "Hiding Data in Images by Simple LSB Substitution", Pattern Recognition, vol.37, no. 3, pp. 469-474, 2004.

[6] Laishra, D., Tuithung, T., "A Novel Minimal Distortion-Based Edge Adaptive Image Steganography Scheme using Local Complexity", Multimedia Tools and Applications, vol. 80, pp. 831-854, 2021.

[7] Sheidae, A., Farzinvash, L., "A Novel Image Steganography Method based on DCT and LSB", In: IEEE International Conference on Information and Knowledge Technology (IKT), Iran, Tehran, 2017.

[۸] شیدائی، علی، فرزین‌وش، لیلی، **"پنهان سازی تصویر در تصاویر بامعنی به کمک فیلتر منظم و تبدیلات کسینوسی گسسته"**،

چهارمین کنفرانس ملی محاسبات توزیعی و پردازش داده های بزرگ، ایران، تبریز، ۱۳۹۷.

[9] Duan, X., Jia, K., Li, B., Guo, D., Zhang, E., Qin, C., "Reversible Image Steganography Scheme Based on a U-Net Structure", IEEE Access, vol. 7, pp. 9314-9323, 2019.

[10] Kanan, H. R., Nazeri, B., "A Novel Image Steganography Scheme with High Embedding Capacity and Tunable Visual Image Quality Based on a Genetic Algorithm", Expert Systems with Applications, vol. 41, no. 14, pp. 6123-6130, 2014.

[11] Sharma, V. K., Srivastava, D. K., Mathur, P., "Efficient Image Steganography using Graph Signal Processing", IET Image Processing, vol. 12, no. 6, pp. 1065-1071, 2018.

[12] Abdulla, A. A., Sellahewa, H., Jassim, S. A., "Improving Embedding Efficiency for Digital Steganography by Exploiting Similarities Between Secret and Cover Images", Multimedia Tools and Applications, vol. 78, no. 13, pp 17799-17823, 2019.

[13] Banharnsakun, A., "Artificial Bee Colony Approach for Enhancing LSB Based Image Steganography", Multimedia Tools and Applications, vol. 77, no. 20, pp. 27491-27504, 2018.

[14] Sajasi, S., Eftekhari Moghadam, A-M., "An Adaptive Image Steganographic Scheme based on Noise Visibility Function and an Optimal Chaotic Based Encryption Method", Applied Soft Computing, vol. 30, pp. 375-389, 2015.

[15] Kanso, A., Ghebleh, M., "An Algorithm for Encryption of Secret Images into Meaningful Images", Optics and Lasers in Engineering, vol. 90, pp. 196-208, 2017.

[16] Muhammad, K., Ahmad, J., Rehman, N. U., Jan, Z., Sajjad, M., "CISSKA-LSB: Color Image Steganography using Stego Key-Directed Adaptive LSB Substitution Method", Multimedia Tools and Applications, vol. 76, no. 6, pp. 8597-8626, 2017.

[17] Muhammad, K., Sajjad, M., Mehmood, I., Rho, S., Baik, S. W., "Image Steganography using Uncorrelated Color Space and Its Application for Security of Visual Contents in Online Social Networks", Future Generation Computer Systems, vol. 86, pp. 951-960, 2018.

[۱۸] مهدوی، مجتبی، سماوی، شادرخ، خدامی، الهه، **"پنهان نگاری وفقی براساس پیچیدگی نسبی پیکسلها در تصاویر دوسطح"**، نشریه مهندسی برق و الکترونیک ایران، دوره ۶، شماره ۱، صفحه ۳۷-۴۹، ۱۳۸۸.

[19] Wu, D., Tasi, W., "A Steganographic Method for Images by Pixel-Value Differencing", Pattern Recognition Letters, vol. 24, no. 9, pp. 1613-1626, 2003.

[20] Hussain, M., Abdul Wahab, A. W., Ho, A. T. S., Javed, N., Jung, K. H., "A Data Hiding Scheme using Parity-Bit Pixel Value Differencing and Improved Rightmost Digit Replacement", Signal Processing: Image Communication, vol. 50, pp. 44-57, 2017.

[21] Mukherjee, N., Paul, G., Saha, S. K., Burman, D., "A PVD Based High Capacity Steganography Algorithm with Embedding in Non-Sequential Position", Multimedia Tools and Applications, vol. 79, pp. 13449-13479, 2020.

[22] Xia, Z., Wang, X., Sun, X., Liu, Q., Xiong, N., "Steganalysis of LSB Matching using Differences Between Nonadjacent Pixels", Multimedia Tools and Applications, vol. 75, no. 4, pp. 1947-1962, 2016.

[23] Li, L., Zhang, W., Qin, C., Chen, K., Zhou, W., Yu, N., "Adversarial Batch Image Steganography Against CNN-based Pooled Steganalysis", Signal Processing, vol. 181, 2021, DOI: 10.1016/j.sigpro.2020.107920.

[۲۴] ابوالقاسمی، مجتبی، آقایی نیا، حسن، فائز، کریم، "پنهان شکنی تصویر براساس ویژگیهای ماتریس هم‌وقوعی"، نشریه مهندسی برق و الکترونیک ایران، دوره ۷، شماره ۱، صفحه ۱۵-۲۴، ۱۳۸۹.

[25] Qazanfari, K., Safabakhsh, R., "A New Steganography Method Which Preserves Histogram: Generalization of LSB^{++}", Information Sciences, vol. 277, pp. 90-101, 2014.

[26] Chen, B., Luo, W., Zheng, P., Huang, J., "Universal Stego Post-Processing for Enhancing Image Steganography", Journal of Information Security and Applications, vol. 55, 2020, DOI: 10.1016/j.jisa.2020.102664.

[27] Zhang, X., Wang, S., "Vulnerability of Pixel-Value Differencing Steganography to Histogram Analysis and Modification for Enhanced Security", Pattern Recognition Letters, vol. 25, no. 3, pp. 331-339, 2004.

[28] Shaukat, A., Chaurasia, M., Sanyal, G., "A Novel Image Steganographic Technique using Fast Fourier Transform", in: IEEE International Conference on Recent Trends in Information Technology, Chennai, India, 2016.

[29] Zhang, X., Peng, F., Long, M., "Robust Coverless Image Steganography based on DCT and LDA Topic Classification", IEEE Transactions on Multimedia, vol. 20, no. 12, pp. 3223-3238, 2018.

[30] Liu, Q., Xiang, X., Qin, J., Tan, Y., Tan, J., Luo, Y., "Coverless Steganography Based on Image Retrieval of DenseNet Features and DWT Sequence Mapping", Knowledge-Based Systems, vol. 192, 2020, DOI: 10.1016/j.knosys.2019.105375.

[31] Thanki, R., Borra, S., "A Color Image Steganography in Hybrid FRT–DWT Domain", Journal of Information Security and Applications, vol. 40, pp. 92-102, 2018.

[32] Muhuri, P. K., Ashraf, Z., Goel, S., "A Novel Image Steganographic Method based on Integer Wavelet Transformation and Particle Swarm Optimization", Applied Soft Computing, vol. 92, 2020, DOI: 10.1016/j.asoc.2020.106257.

[33] Miri, A., Faez, K., "Adaptive Image Steganography Based on Transform Domain via Genetic Algorithm", Optik, vol. 145, pp. 158-168, 2017.

زیرنویس‌ها

[1] Secret image
[2] Steganography
[3] Cryptography
[4] Cover image
[5] Stego image
[6] Least significant bit
[7] Peak signal to noise ratio
[8] Lossless
[9] Embedding capacity
[10] Spatial domain
[11] Frequency domain
[12] Red, Green, Blue
[13] Hue, Saturation, Lightness
[14] Discrete cosine transform
[15] Quantization

[16] Regularized filter
[17] Lossy
[18] Deep learning
[19] Fourier transform
[20] Discrete wavelet transform
[21] Integer wavelet transform
[22] Adaptive wavelet transform
[23] Lifting wavelet transform
[24] Chaotic map
[25] Genetic algorithm
[26] Artificial bee colony
[27] Structural similarity index
[28] Mean squared error