مروری بر نهان‌نگاری تصویر مبتنی بر مخفی‌سازی در کم‌ارزش‌ترین بیت و دسته‌بندی پیکسل و ارائه روشی جدید در این حوزه

منصور فاتح*[۱]، سمیرا رجب‌لو[۲] و الهه علی‌پور[۳]

[۱] منصور فاتح، استادیار، گروه هوش مصنوعی و رباتیک، دانشکده مهندسی کامپیوتر و فناوری اطلاعات، دانشگاه صنعتی شاهرود، شاهرود، ایران

mansoor_fateh@shahroodut.ac.ir

[۲]سمیرا رجب‌لو، دانشجوی کارشناسی ارشد، دانشکده مهندسی کامپیوتر و فناوری اطلاعات، دانشگاه صنعتی شاهرود، شاهرود، ایران

rajabloo88@yahoo.com

[۳]الهه علی‌پور، دانشجوی کارشناسی ارشد، دانشکده مهندسی کامپیوتر و فناوری اطلاعات، دانشگاه صنعتی شاهرود، شاهرود، ایران

elahealipour@shahroodut.ac.ir

چکیده

در این مقاله، ابتدا مروری جامع بر نهان‌نگاری تصویر مبتنی بر مخفی‌سازی در کم‌ارزش‌ترین بیت و دسته‌بندی پیکسل انجام و سپس، روشی برای نهان‌نگاری اطلاعات در تصویر ارائه شده است. این روش مبتنی بر مخفی‌سازی پیام در کم‌ارزش‌ترین بیت (LSB) تصویر است. هدف ما در این مقاله، به‌کمینه‌رساندن تغییرات در تصویر پوشانه است. در روش پیشنهادی، ابتدا پیکسل‌های تصویر برای مخفی‌سازی پیام انتخاب و سپس مکمل پیام در بیت‌های کم‌ارزش پیکسل‌های انتخابی مخفی می‌شوند. در این مقاله، برای حل برخی از مشکلات روش LSB و به‌حداقل رساندن تغییرات، پیکسل‌ها بر اساس مقادیر بیت‌های دوم، سوم و چهارم آن‌ها دسته‌بندی می‌شوند. در هر دسته، نسبت پیکسل‌های تغییریافته به پیکسل‌های بدون تغییر محاسبه می‌شود. اگر این نسبت بزرگ‌تر از یک بود، بیت‌های کم‌ارزش آن دسته معکوس می‌شوند و تغییرات به کمینه می‌رسند. برای ارزیابی کیفیت تصویر نهانه از دو معیار میانگین مربعات خطا و نسبت سیگنال به نوفه استفاده می‌شود. PSNR و MSE روش پیشنهادی در مقایسه با روش LSB ساده، به‌ترتیب دارای نرخ رشد۰,۱۳ درصدی و نرخ کاهش ۰,۱۹ درصدی هستند.

واژگان کلیدی: نهان‌نگاری، دسته‌بندی پیکسل‌ها، روش کم‌ارزش‌ترین بیت، محرمانگی

۱- مقدمه

امروزه، با استفادهٔ روزافزون از اینترنت، انتقال اطلاعات سریع‌تر و آسان‌تر شده است. این انتقال آسان، موجب ارسال هر چه بیشتر رسانه‌های دیجیتال در فضای مجازی شده است. حفظ محرمانگی در انتقال برخی از اطلاعات بسیار حائز اهمیت است. با افزایش ارسال اطلاعات در فضای مجازی، تقاضای حفظ محرمانگی در این فضا افزایش می‌یابد. تشخیص پزشکی، اطلاعات مالی و نظامی بخشی از اطلاعات محرمانه در فضای مجازی هستند[۱].

همواره، تهدیدهایی برای محرمانگی این اطلاعات وجود دارد که منجر به ایجاد سازوکارهایی برای حفاظت محتوای داده‌ها می‌شود. مخفی‌سازی اطلاعات[۱]، یک نیاز بالقوه در حفظ اطلاعات و ایجاد یک ارتباط امن است. انواع روش‌های مخفی‌سازی اطلاعات شامل ته‌نقش نگاری[۲]، نهان‌نگاری[۳] و رمزنگاری[۴] هستند. به‌منظور حفظ حق مالکیت

[1] Data Hiding
[2] watermarking
[3] steganography
[4] cryptography

در نشر یک محصول از تهنقش نگاری استفاده می‌شود. رمزنگاری برای پنهان‌سازی محتوای داده‌ها استفاده می‌شود[۱]. در رمزنگاری، فرستنده و گیرنده قابل شناسایی هستند و هدف تنها مخفی‌سازی محتوای پیام است.

در نهان‌نگاری از یک کلید و یک بستر به نام پوشانه برای مخفی‌سازی اطلاعات استفاده می‌شود. هدف از نهان‌نگاری، مخفی‌سازی فرستنده، گیرنده و محتوای پیام و اطلاعات تنها توسط گیرنده قابل رؤیت است [۱]. کلمه نهان‌نگاری از کلمات یونانی stego به معنای پنهان و grafia به معنای نوشتن مشتق‌شده است که به‌عنوان نوشتن محرمانه تعریف می‌شود [۲]. نهان‌نگاری یک روش برای انتقال اطلاعات در یک پوشانه و از طریق کانال‌های ارتباط عمومی است. در این روش، مهاجم نمی‌تواند اطلاعات محرمانه در پوشانه را شناسایی کند [۳]. در ارسال مخفی اطلاعات، سه پارامتر ظرفیت، مقاومت و شفافیت از اهمیت ویژه‌ای برخوردارند. افزایش این پارامترها، موجب افزایش محرمانگی خواهد شد؛ اما افزایش این سه پارامتر با هم دشوار است. با افزایش شفافیت و ظرفیت، مقاومت کاهش می‌یابد و با افزایش مقاومت در برابر حملات، شفافیت و ظرفیت کمتر مورد توجه قرار می‌گیرد؛ پس هدف مخفی‌سازی پیام باید مشخص باشد. در تهنقش‌نگاری بیش‌تر مقاومت در اولویت قرار دارد و هدف بیش‌تر روش‌های نهان‌نگاری، ایجاد ظرفیت بالا و شفافیت مناسب در نهانه است که در غالب موارد موجب کاهش مقاومت در برابر حملات می‌شود. در نهان‌نگاری، اولویت با افزایش شفافیت است و افزایش ظرفیت اولویت بعدی روش‌های نهان‌نگاری است. در نهان‌نگاری، پوشانه می‌تواند تصویر، صوت، ویدئو، متن، پروتکل یا غیره باشد [۴]. تصویر، به‌دلیل ظرفیت بالا، تنوع مناسب و استفاده وسیع کاربران از آن، کاربرد زیادی به‌عنوان پوشانه دارد. مخفی‌سازی در تصویر را نهان‌نگاری تصویر گویند. نهان‌نگاری در تصویر باید به‌گونه‌ای باشد که ویژگی‌های تصویر دچار تغییرات قابل ملاحظه‌ای نشوند.

نهان‌نگاری تصویر، بیش‌تر در دو حوزه مکان و تبدیل صورت می‌پذیرد. روش‌های نهان‌نگاری در حوزه مکان برخی از بیت‌های موجود در پیکسل‌های تصویر پوشانه را تغییر می‌دهند. پیکسل‌ها جهت مخفی‌سازی پیام، می‌توانند به‌صورت ساده یا تصادفی انتخاب شوند. روش‌های نهان‌نگاری در حوزهٔ تبدیل، با مخفی‌سازی بیت‌های پیام در ضرایب تبدیل تصویر پوشانه انجام می‌شوند. این تبدیل‌ها می‌توانند تبدیل کسینوسی[1] (DCT)، فوریه[2] یا ویولت[3] باشند [۴].

در این مقاله علاوه‌بر ارائهٔ روشی در حوزهٔ مکان، آن را با برخی از روش‌های موجود در این حوزه مقایسه می‌کنیم. یکی از روش‌های نهان‌نگاری تصویر در حوزه مکان، مخفی‌سازی بیت‌های پیام در کم‌ارزش‌ترین بیت[4] (LSB) تصویر پوشانه است. روش مبتنی بر LSB یکی از چالش‌برانگیزترین روش‌ها است. در این روش، با جایگزینی تعداد کمی از بیت‌های LSB، تفاوت بین تصویر پوشانه و تصویر نهانه، به‌سختی قابل تشخیص است [۴]. تغییرات بیش از اندازه در تصویر پوشانه، یکی از معایب این روش است. در برخی موارد، پنهان‌سازی مکمل پیام در پوشانه تغییرات کمتری ایجاد می‌کند. این روش LSB معکوس نامیده می‌شود. روش LSB معکوس همیشه کارآمد نیست و گاهی موجب افزایش تغییرات نیز می‌شود. در این مقاله، برای حل مشکلات ناشی از دو روش مذکور، از ترکیب آن‌ها برای به کمینه رساندن تغییرات استفاده شده است. بدین منظور پیکسل‌های تصویر پوشانه به چند دسته تقسیم می‌شوند. این دسته‌بندی براساس مقادیر بیت‌های دوم، سوم و چهارم انجام می‌گیرد؛ سپس پیام، در بیت‌های کم‌ارزش پیکسل‌های انتخابی مخفی می‌شوند. در هر دسته، نسبت پیکسل‌های تغییریافته به پیکسل‌های بدون تغییر محاسبه می‌شود. اگر این نسبت بزرگ‌تر از یک بود، بیت‌های کم‌ارزش آن دسته معکوس می‌شوند. با این معکوس‌سازی، تغییرات به کمینه می‌رسند.

این مقاله از ۸ بخش تشکیل شده است. در بخش۲ به کارهای انجام‌شده در زمینه نهان‌نگاری و در بخش۳ به معرفی نهان‌نگاری و در بخش۴ روش LSB ساده پرداخته شده است. در بخش۵ دسته‌بندی پیکسل‌ها براساس بیت دوم و سوم و در بخش۶ روش پیشنهادی و در بخش‌های ۷ و ۸ به‌ترتیب آزمایش‌ها و نتایج آن‌ها و نتیجه‌گیری آورده شده است، و در بخش آخر منابع ذکر شده است.

۲- کارهای مرتبط

سایمونز[5] و همکارانش در سال ۱۹۸۳ یک سامانهٔ پایهٔ نهان‌نگاری ارائه دادند. در این سامانه دو زندانی با نام‌های

[1] Discrete Cosine Transform
[2] Discrete Fourier Transform
[3] Discrete Wavelet Transform
[4] Least significant bit
[5] Simmons

آلیس و باب قصد طرح‌ریزی یک نقشه فرار را دارند. برای طرح نقشه فرار، آلیس قصد ارسال پیامی برای باب را دارد. ارتباط آلیس و باب توسط ویلی زندانبان بررسی می‌شود. آلیس باید پیام خود را در قالب یک پیام پنهان‌شده در پیام عادی، برای باب ارسال کند تا سوءظن ویلی برانگیخته نشود و باب هم قادر به فهم کامل پیام باشد [۵]. یکی از روش‌های نهان‌نگاری در حوزهٔ مکان LSB است. نهان‌نگاری مبتنی بر LSB یکی از ساده‌ترین روش‌های نهان‌نگاری است. در این روش، پیام محرمانه در بیت‌های کم‌ارزش پیکسل تصویر پوشانه مخفی می‌شوند [۶]. به‌منظور افزایش امنیت روش LSB، روش PI[1] ارائه شده است [۷]. در این روش، پیام در کانال‌های رنگی تصاویر ۲۴ بیتی مخفی می‌شوند. در روش PI کانال منتخب، گزینش می‌شود و برای نرخ مخفی‌سازی کمتر از ۳ بیت، خرابی‌های بصری کمی تولید می‌شود. این روش، در برابر حمله‌های بصری و هیستوگرامی مقاوم است.

یکی دیگر از روش‌های توسعه‌یافته الگوریتم LSB، فرآیند تنظیم پیکسل بهینه[2] (OPAP) است [۸]. OPAP اختلاف بین پیکسل‌های تصویر اصلی و نهان‌نگاری‌شده را محاسبه و بیت‌های مخفی‌شده را به‌منظور بهبود شفافیت تغییر می‌دهد [۹]. OPAP، مقادیر PSNR[3] بالایی برای تصاویر استاندارد Baboon و Lena تولید کرده است [۱۰]. یکی دیگر از روش‌های نهان‌نگاری، نهان‌نگاری ادراکی تصویر[4] است. این روش مبتنی بر کلید امن است. در این روش، به جای مخفی‌سازی مستقیم اطلاعات محرمانه، از درک تصویر استفاده می‌شود. در روش نهان‌نگاری ادراکی تصویر، از یک ماتریس نگاشت برای مخفی‌سازی اطلاعات استفاده می‌شود. این روش در برابر حمله Brute-Force مقاوم است [۱۱]. یکی دیگر از موفقیت‌های این روش، امنیت بالا در برابرحمله‌های آماری مانند حملات هیستوگرامی است. برای توسعهٔ این روش، یک روش نگاشت محرمانه پوشانه توسط چانگدر[5] و روی[6] به‌عنوان کمینه مشترک توالی[7] (LCS) ارائه شده است [۱۲]. این روش، در برابر حمله‌های Brute-Force بسیار مقاوم است. همچنین در این روش، ظرفیت مخفی‌سازی افزایش یافته است.

تفاضل مقدار پیکسل[8] (PVD)، روشی دیگر برای نهان‌نگاری اطلاعات است [۱۳]. در این روش، تصویر پوشانه به بلاک‌هایی فاقد هم‌پوشانی تقسیم می‌شود. اختلاف مقادیر دو پیکسل در هر بلاک محاسبه و همه مقادیر اختلاف به تعدادی بازه دسته‌بندی و سپس مقادیر اختلاف، با یک مقدار جدید جایگزین می‌شوند تا تعدادی از بیت‌های پیام محرمانه، جاسازی شوند. تعداد بیت‌های قابل جاسازی در یک جفت پیکسل، با توجه به عرض بازهٔ اختلاف تعیین می‌شوند. برای بهبود ظرفیت و شفافیت تصویر پوشانه، می‌توان از ترکیب روش LSB و PVD استفاده کرد [۱۴]. در این روش، ابتدا مقدار اختلاف دو پیکسل متوالی با به‌کارگیری روش PVD به‌دست می‌آید. در مناطق هموار اختلاف دو پیکسل متوالی اندک و در لبه‌ها این اختلاف قابل توجه است. نهان‌نگاری در مناطق هموار، با روش LSB و در لبه‌ها با روش PVD انجام می‌شود.

یکی دیگر از روش‌های توسعه‌یافته الگوریتم LSB، روشی ترکیبی از روش‌های LSB، DCT و روش‌های فشرده‌سازی است [۱۵]. در این روش، ابتدا الگوریتم LSB برای جاسازی بیت‌های پیام در تصویر پوشانه استفاده می‌شود؛ سپس تصویر حاصل با استفاده از DCT به حوزه فرکانس منتقل می‌شود و درنهایت الگوریتم‌های کوانتیزاسیون[9] و کدگذاری طول اجرا[10] برای فشرده‌سازی تصویر پوشانه استفاده می‌شوند تا امنیت بالا رود.

در روشی دیگر از نهان‌نگاری مبتنی بر LSB، دسته‌بندی پیکسل‌ها برای به کمینه رساندن تغییرات آن‌ها انجام می‌شود [۱۶]. این دسته‌بندی بر اساس مقادیر بیت‌های دوم و سوم پیکسل‌ها است. در این روش پس از اعمال LSB معکوس، تعداد تغییرات در هر دسته، محاسبه می‌شود. در ادامه، دسته‌ای با تعداد پیکسل‌های تغییریافتهٔ بیشتر از تعداد پیکسل‌های بدون تغییر، معکوس می‌شوند. مشکل این روش لحاظ‌کردن تنها یک دسته است. درحالی‌که برای به کمینه رساندن تغییرات می‌توان برای همه دسته‌ها این کار را انجام داد. در روش پیشنهادی این مقاله، همه دسته‌ها لحاظ می‌شوند و برای بهبود بیشتر، تعداد دسته‌ها افزایش می‌یابند. بدین منظور، دسته‌بندی براساس مقادیر بیت‌های دوم و سوم و چهارم انجام می‌شوند.

[1] Pixel Indicator
[2] Optimal Pixel Adjustment Procedure
[3] Peak Signal-to-Noise Ratio
[4] Image Realization Steganography
[5] Changder
[6] Roy
[7] Longest Common Subsequence

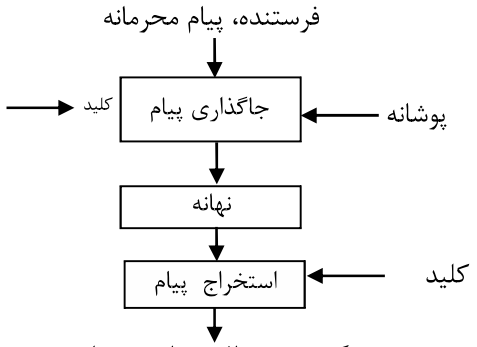
[8] pixel-value differencing
[9] quantization
[10] runlength coding algorithm

۳- نهان‌نگاری

نهان‌نگاری برای نخستین بار توسط حاکم یونانی اسیرشده به دست داریوش در قرن پنجم انجام شد. این حاکم یونانی با حکاکی پیام بر روی سر غلام خود، نهان‌نگاری را شکل داد. بعد از آن، نهان‌نگاری در لوح‌های پوشیده از موم، نامرئی‌نویسی با جوهرهای آبلیمو در زمان روم باستان مورد استفاده قرار گرفت. همچنین نهان‌نگاری در جنگ جهانی دوم در مکتوبات غیرمحرمانه استفاده شد [۱۷]. هدف از نهان‌نگاری، مخفی‌سازی ماهیت پیام محرمانه از افراد غیرمجاز است و مهاجم نمی‌تواند انتقال اطلاعات محرمانه در پس‌زمینه یک ارتباط عمومی را شناسایی کند[۳]. در رمزنگاری فرستنده، گیرنده و پیام رمزشده مشخص است؛ اما در نهان‌نگاری پنهان ماندن فرستنده، گیرنده و پیام محرمانه از ارکان اصلی محسوب می‌شوند.

از روش‌های نهان‌نگاری می‌توان به نهان‌نگاری صنعتی، زبانی و دیجیتال اشاره کرد. در نهان‌نگاری صنعتی از علوم مهندسی، فیزیک و غیره جهت پنهان‌کردن اطلاعات استفاده می‌شود. در نهان‌نگاری زبانی، مخفی‌سازی اطلاعات از طریق نوشتن صورت می‌پذیرد. همچنین نهان‌نگاری دیجیتال، علم مخفی‌سازی پیام در یک رسانه دیجیتال مانند صوت، تصویر، ویدئو و متن است.

امروزه به‌دلیل تنوع زیاد تصویر، تصویر به‌عنوان بستری ایمن جهت مخفی‌سازی پیام استفاده می‌شود و به آن پوشانه می‌گویند. به تصویر تولیدشده بعد از درج داده‌های محرمانه، نهانه می‌گویند. در روش‌های نهان‌نگاری، اغلب از یک کلید جهت به‌هم‌ریختگی پیام استفاده می‌شود تا درصورت شناسایی وجود پیام محرمانه، محتوای پیام به‌طور صریح آشکار نشود. شمای کلی نهان‌نگاری با کلید به‌صورت شکل (۱) است:



(شکل-۱): شمای کلی نهان‌نگاری با کلید

روش‌های حوزهٔ مکان، از روش‌های نهان‌نگاری در تصویر هستند. در این روش‌ها، برخی بیت‌های موجود در پیکسل‌های تصویر، جهت پنهان‌سازی داده‌ها به‌طورمستقیم تغییر می‌کنند. در این روش‌ها، از اطلاعات RGB یا شدت روشنایی پیکسل‌های تصویر جهت پنهان‌سازی اطلاعات استفاده می‌شود. یکی از روش‌های نهان‌نگاری تصویر در حوزهٔ مکان روش LSB است که در بخش بعدی به شرح آن پرداخته شده است.

۴- روش LSB

نهان‌نگاری مبتنی بر LSB یکی از ساده‌ترین روش‌های نهان‌نگاری است. در این روش، پیام محرمانه در بیت‌های کم‌ارزش پیکسل‌های موردنظر مخفی می‌شوند. تغییرات ایجادشده در این روش، قابل ردیابی توسط چشم نیست [۶]؛ اما این روش اغلب بر روی هیستوگرام تصویر، تأثیرگذار است و توسط الگوریتم‌های نهان‌کاوی قابل ردیابی است. یک مثال ساده از روش LSB در ادامه آمده است:

پیام موردنظر جهت مخفی‌سازی: ۱۰۱

پیکسل‌های تصویر پوشانه جهت مخفی‌سازی:

۰۱۰۱۱۰۱۰ ۱۱۱۰۱۰۰۱ ۱۰۱۰۱۱۱۰

با استفاده از روش LSB (مخفی‌سازی بیت‌های پیام در بیت‌های کم‌ارزش پیکسل‌ها) پیکسل‌های نهانه به‌صورت زیر هستند:

۰۱۰۱۱۰۱۱ ۱۱۱۰۱۰۰۰ ۱۰۱۰۱۱۱۱

همان‌طور که مشاهده می‌شود، تمامی پیکسل‌ها دچار تغییر شده‌اند. یک روش برای به کمینه رساندن تعداد تغییرات در LSB، دسته‌بندی پیکسل‌ها براساس بیت‌های دوم و سوم کم‌ارزش آن‌ها است [۱۶]. این روش در بخش بعدی شرح داده شده است.

۵- دسته‌بندی پیکسل‌ها براساس بیت دوم و سوم کم‌ارزش آن‌ها

پیکسل‌ها را می‌توان براساس بیت دوم و سوم کم‌ارزش آن‌ها دسته‌بندی و تغییرات را پس از مخفی‌سازی پیام در بیت‌های کم‌ارزش پیکسل‌ها، محاسبه کرد [۱۶]. در این روش، پیکسل‌ها در چهار دسته قرار می‌گیرند. این دسته‌ها براساس مقادیر بیت دوم و سوم کم‌ارزش هر پیکسل یعنی ۰۰، ۰۱، ۱۰ و ۱۱ ایجاد شده‌اند. در این روش، ابتدا با روش LSB

بیت‌های پیغام در کم‌ارزش‌ترین بیت هر پیکسل جاسازی می‌شود؛ سپس به‌منظور کاهش تغییرات، LSB نخستین دستهٔ با بیش از ۵۰٪ تغییرات، معکوس می‌شود. چارت این روش در شکل (۲) آمده است. یکی از عیب‌های این روش، اولویت‌دهی به دسته‌ها است. دسته‌ها براساس اولویت بررسی می‌شوند و LSB نخستین دسته با شرط بالا، معکوس می‌شود.

(شکل-۲): چارت روش دسته‌بندی پیکسل‌ها براساس بیت دوم و سوم کم‌ارزش آنها

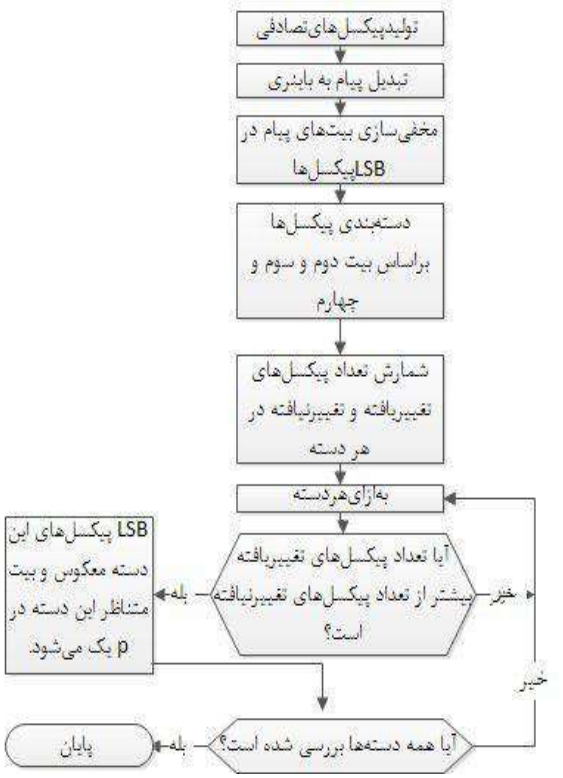
بنابراین سایر دسته‌ها بررسی نمی‌شوند. در این روش، ممکن است که دسته‌های بررسی‌نشده میزان تغییرات بیشتری نسبت به نخستین دسته انتخابی داشته باشد و بتوان با اعمال LSB معکوس، کاهش بیشتری در تعداد تغییرات ایجاد کرد. برای بهبود این روش، باید تمام دسته‌ها را بررسی کرد و LSB دسته‌ای با بیشترین تغییر را معکوس کرد. این بهبود تا کنون در هیچ مقاله‌ای ارائه نشده است. در این مقاله، جهت بهبود روش مرجع [۱۶]، دسته‌بندی پیکسل‌ها براساس بیت دوم، سوم و چهارم و بدون لحاظ‌کردن اولویت، ارائه شده است که نتایج به‌مراتب بهتری از روش مرجع [۱۶] و بهبودیافتهٔ آن را حاصل کرده است.

۶- روش پیشنهادی

در این مقاله، روشی مبتنی بر LSB معکوس و دسته‌بندی پیکسل‌ها به هشت دسته ارائه شده است. این روش دارای دو مرحلهٔ مخفی‌سازی و استخراج پیام است که در ادامه به آنها پرداخته شده است.

۶-۱- مرحلهٔ مخفی‌سازی پیام

در مرحلهٔ مخفی‌سازی، ابتدا پیام به‌صورت دودویی نوشته و تبدیل به رشته‌ای از اعداد صفر و یک می‌شود. در گام بعدی، پیکسل‌های تصویر پوشانه با توجه به کلید انتخاب می‌شوند؛ سپس بیت‌های پیام در کم‌ارزش‌ترین بیت پیکسل‌های تصویر پوشانه مخفی می‌شوند. در ادامه، این پیکسل‌ها، براساس بیت دوم، سوم و چهارم به هشت دستهٔ ۰۰۰، ۰۰۱، ۰۱۰، ۰۱۱، ۱۰۰، ۱۰۱، ۱۱۰ و ۱۱۱ تقسیم می‌شوند. سپس بیت‌های پیام در کم‌ارزش‌ترین بیت پیکسل‌های تصویر پوشانه مخفی می‌شوند. درر ادامه، این پیکسل‌ها، براساس بیت دوم، سوم و چهارم به هشت دستهٔ ۰۰۰، ۰۰۱، ۰۱۰، ۰۱۱، ۱۰۰، ۱۰۱، ۱۱۰ و ۱۱۱ تقسیم می‌شوند. در گام بعدی پس از مخفی‌سازی پیام، در هر دسته نسبت LSB های تغییر کرده به تغییر نکرده محاسبه می‌شود. اگر این نسبت بیشتر از یک بود، LSB های آن دسته معکوس می‌شود. در روش پیشنهادی، یک آرایهٔ p هشت بیتی جهت علامت‌گذاری دسته‌هایی با LSB معکوس لحاظ شده است. در این آرایه، بیت متناظر با دسته‌ای با LSB معکوس یک می‌شود و در غیر این صورت صفر باقی می‌ماند. چارت مخفی‌سازی پیام در شکل (۳) آمده است.



(شکل-۳): چارت مخفی‌سازی پیام

علاوه‌بر پیام، آرایهٔ p نیز همراه پیام ارسال می‌شود. بعد از اعمال تغییرات در آرایهٔ p، آن را همراه با پیام در پوشانه مخفی می‌کنیم. در مخفی‌سازی ابتدا بیت‌های آرایه p (۸بیت) و سپس بیت‌های پیام محرمانه مخفی می‌شوند. با استفاده از این روش، تعداد تغییرات نسبت به روش مرجع [۱۶] ، بهبودیافته آن و LSB ساده کمتر شده و نتایج قابل قبولی ارائه می‌دهد که نتایج در بخش آزمایش‌ها ذکر شده است.

۶-۲- مرحلهٔ استخراج پیام

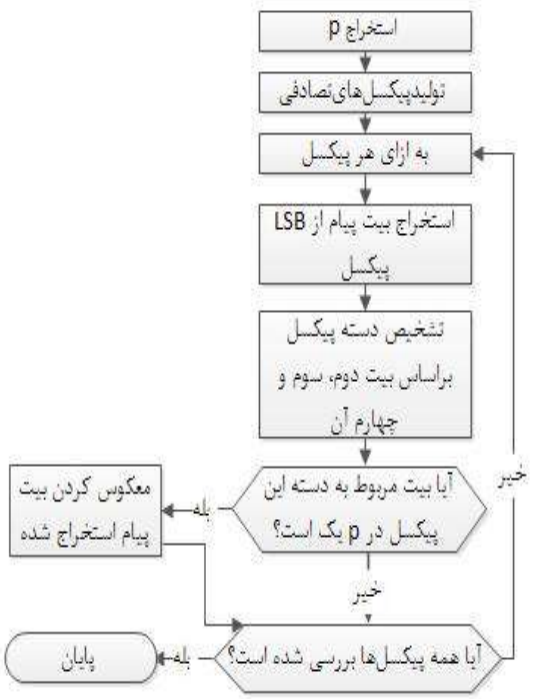
گیرنده با دراختیارداشتن نهانه و کلید می‌تواند پیام را استخراج کند. گیرنده با دریافت نهانه به‌خوبی نسبت به آرایه‌ی p آگاهی دارد و به تغییرات اعمال‌شده در بیت‌های کم‌ارزش پیکسل‌های تصادفی تولیدشده پی خواهد برد. هشت بیت ابتدایی پیام استخراج‌شده شامل بیت‌های آرایه p و سایر بیت‌ها، پیام محرمانه است. گیرنده با استخراج p، دسته‌هایی با LSB معکوس را تشخیص می‌دهد؛ سپس با توجه به کلید پیکسل‌های حاوی بیت‌های پیام، مشخص می‌شوند. براساس دستهٔ هر پیکسل و مقدار p برای این دسته، پیام اصلی استخراج می‌شود. درصورتی‌که بیت متناظر در p برابر با یک باشد، پیام اصلی برابر با معکوس LSB آن پیکسل است و در غیر این‌صورت پیام اصلی برابر با LSB آن پیکسل است. چارت استخراج پیام در شکل (۴) آمده است.

۷- آزمایش‌ها و نتایج

در این بخش، جهت بررسی کارایی روش پیشنهادی، از سه تصویر cameraman، coins و football به‌عنوان پیام محرمانه استفاده شده است. پیام محرمانه در شش تصویر Lena، peppers، Baboon، Autumn، Kids و Office به‌عنوان پوشانه نهان‌نگاری می‌شود. به‌عنوان نمونه، تصویر cameraman در تصویر Lena نهان‌نگاری شده است. تصویر Lena قبل و بعد از نهان‌نگاری و همچنین پیام استخراج شده از آن در شکل (۵) آمده است.

جهت ارزیابی تصویر نهانه، از دو معیار ارزیابی کیفیت تصویر، میانگین مربعات خطا[1] (MSE) و نسبت سیگنال به نوفه (PSNR) استفاده شده است. MSE بیان‌کننده اختلاف پیکسل به پیکسل تصویر پوشانه و نهانه است. طریقهٔ محاسبهٔ MSE در رابطهٔ (۱) نشان داده شده است.

$$MSE = \frac{1}{M*N}\sum_{i=1}^{M}\sum_{j=1}^{N}[C(i,j) - S(i,j)]^2 \qquad (۱)$$



(شکل-۴): چارت استخراج پیام

[1] Mean Square Error

(شکل-۵): نتایج روش پیشنهادی

$C(i,j)$ تصویر پوشانه، $S(i,j)$ تصویر نهانه، M و N ابعاد تصویر پوشانه و نهانه است.

MSE کوچک‌تر به معنی تفاوت کمتر تصاویر نهانه و پوشانه است. کم‌شدن تفاوت تصویر نهانه و پوشانه، به معنی حفظ هر چه بیشتر کیفیت تصویر پوشانه و افزایش شفافیت و امنیت است. معیار دیگر PSNR به معنی نسبت سیگنال به نوفه است. نحوهٔ محاسبهٔ این پارامتر در روابط (۲) و (۳) آمده است.

$$PSNR = 10 * \log \frac{p^2}{MSE} \quad (۲)$$

$$p = \max(C(i,j), S(i,j)) \quad (۳)$$

PSNR بزرگ‌تر، به معنی حفظ هرچه بیشتر کیفیت تصویر و ارائهٔ روش نهان‌نگاری بهتر است. عملکرد روش پیشنهادی، در جدول (۱) با روش مرجع [۱۶]، بهبودیافته آن و LSB ساده مقایسه شده است.

با توجه به نتایج به دست آمده در جدول (۱)، روش پیشنهادی عملکرد بهتری از روش مرجع [۱۶] دارد و درنتیجه منجر به محرمانگی بیشتری می‌شود. در روش مرجع [۱۶] بر طبق یک اولویت، تنها بیت کم‌ارزش یک دسته از پیکسل‌ها معکوس می‌شوند. درواقع، از میان چند دسته از پیکسل‌ها، با بیت کم‌ارزش تغییریافتهٔ بیشتر از تغییرنیافته، تنها بیت کم‌ارزش یک دسته معکوس می‌شوند. این حالت ممکن است که برای چند دسته از پیکسل‌ها رخ دهد. در این صورت، با معکوس‌کردن بیت کم‌ارزش تمام این دسته از پیکسل‌ها، میزان تغییرات تصویر پوشانه خیلی کمتر خواهد شد. در روش پیشنهادی، علاوه‌بر لحاظ‌کردن معکوس تمام دسته‌ها، تعداد دسته‌ها به هشت دسته افزایش یافته است. با افزایش تعداد دسته‌ها، بیت کم‌ارزش پیکسل‌های بیشتری را می‌توان معکوس کرد و تغییرات در تصویر پوشانه را کاهش داد. روش مرجع [۱۶] گاهی از LSB ساده هم ضعیف‌تر است. نمونه‌ای از نتایج در جدول (۱) نشان داده شده است. در روش مرجع [۱۶]، ابتدا معکوس LSB ذخیره و سپس طبق اولویت، تنها یک دسته معکوس می‌شود. در این روش، گاهی تغییرات بیشتری نسبت به روش LSB ساده ایجاد می‌شود. اما عملکرد روش پیشنهادی، در همه موارد از روش LSB ساده و روش مرجع [۱۶] بهتر است.

۸- نتیجه‌گیری

در این مقاله روشی مبتنی بر **LSB** معکوس جهت نهان‌گاری در حوزه مکان ارائه شده است. در این روش، برای به کمینه‌رساندن تغییرات پیکسل‌های تصویر پوشانه از دسته‌بندی پیکسل‌ها استفاده شده است.

در روش مرجع [۱۶]، دسته‌بندی پیکسل‌ها براساس بیت دوم و سوم کم‌ارزش پیکسل‌ها انجام شده بود که مشکلاتی داشت. با رفع مشکلات و بهبود روش مذکور، روشی مبتنی بر دسته‌بندی پیکسل‌ها براساس بیت دوم، سوم و چهارم، بیت‌های کم‌ارزش پیکسل‌ها، در این مقاله، ارائه شد که میزان تغییرات را به حداقل رساند.

(جدول ۱): مقایسه روش پیشنهادی با سایر روش‌ها

تصویر پوشانه	پیام محرمانه	LSB ساده		روش [۱۶]		بهبودیافته [۱۶]		روش پیشنهادی	
		MSE	PSNR	MSE	PSNR	MSE	PSNR	MSE	PSNR
Lena ۵۱۲×۵۱۲	cameraman ۶۴×۶۴	۰,۰۶۲۷	۶۰,۱۵۵۹	۰,۰۶۲۰	۶۰,۲۰۶۱	۰,۰۶۱۹	۶۰,۲۱۴۴	۰,۰۶۱۷	۶۰,۲۳۰۷
Lena ۵۱۲×۵۱۲	coins ۶۴×۷۹	۰,۰۷۶۶	۵۹,۲۸۹۶	۰,۰۷۶۷	۵۹,۲۸۰۸	۰,۰۷۶۴	۵۹,۳۰۰۰	۰,۰۷۶۱	۵۹,۳۱۶۸

Lena ۵۱۲×۵۱۲	football ۶۴×۸۰	۰,۰۷۸۵	۵۹,۱۸۲۰	۰,۰۷۷۶	۵۹,۲۳۱۶	۰,۰۷۷۶	۵۹,۲۳۱۶	۰,۰۷۷۴	۵۹,۲۴۱۷
Peppers ۳۸۴×۵۱۲	cameraman ۶۴×۶۴	۰,۰۸۳۱	۵۸,۹۳۳۸	۰,۰۸۳۱	۵۸,۹۳۴۸	۰,۰۸۲۵	۵۸,۹۶۴۲	۰,۰۸۲۴	۵۸,۹۷۰۶
Peppers ۳۸۴×۵۱۲	coins ۶۴×۷۹	۰,۱۰۲۶	۵۸,۰۱۸۷	۰,۱۰۲۷	۵۸,۰۱۵۹	۰,۱۰۲۲	۵۸,۰۳۴۲	۰,۱۰۱۹	۵۸,۰۴۸۳
Peppers ۳۸۴×۵۱۲	football ۶۴×۸۰	۰,۱۰۴۲	۵۷,۹۵۱۶	۰,۱۰۳۹	۵۷,۹۶۶۵	۰,۱۰۳۴	۵۷,۹۸۷۴	۰,۱۰۳۲	۵۷,۹۹۵۱
Baboon ۵۱۲×۵۱۲	cameraman ۶۴×۶۴	۰,۰۶۲۵	۶۰,۱۷۰۹	۰,۰۶۲۲	۶۰,۱۹۴۳	۰,۰۶۱۹	۶۰,۲۱۴۹	۰,۰۶۱۷	۶۰,۲۳۰۷
Baboon ۵۱۲×۵۱۲	coins ۶۴×۷۹	۰,۰۷۷۰	۵۹,۲۶۸۳	۰,۰۷۶۹	۵۹,۲۷۰۷	۰,۰۷۶۵	۵۹,۲۹۵۹	۰,۰۷۶۲	۵۹,۳۱۰۵
Baboon ۵۱۲×۵۱۲	football ۶۴×۸۰	۰,۰۷۷۹	۵۹,۲۱۳۹	۰,۰۷۷۸	۵۹,۲۲۲۵	۰,۰۷۷۴	۵۹,۲۴۴۲	۰,۰۷۷۲	۵۹,۲۵۲۰
Autumn ۳۴۵×۲۰۶	cameraman ۶۴×۶۴	۰,۲۲۹۹	۵۴,۵۱۴۹	۰,۲۲۸۸	۵۴,۵۳۵۴	۰,۲۲۷۷	۵۴,۵۵۶۸	۰,۲۲۷۷	۵۴,۵۵۷۶
Autumn ۳۴۵×۲۰۶	coins ۶۴×۷۹	۰,۲۸۵۴	۵۳,۵۷۶۱	۰,۲۸۰۵	۵۳,۶۵۲۲	۰,۲۷۹۵	۵۳,۶۶۶۳	۰,۲۷۹۱	۵۳,۶۷۲۵
Autumn ۳۴۵×۲۰۶	football ۶۴×۸۰	۰,۲۸۶۲	۵۳,۵۶۴۴	۰,۲۸۸۵	۵۳,۵۲۸۹	۰,۲۸۴۲	۵۳,۵۹۵۰	۰,۲۸۴۱	۵۳,۵۹۵۷
Kids ۳۱۸×۴۰۰	cameraman ۶۴×۶۴	۰,۱۲۷۸	۵۷,۰۶۴۲	۰,۱۲۵۳	۵۷,۱۵۲۲	۰,۱۲۵۳	۵۷,۱۵۲۲	۰,۱۲۴۰	۵۷,۱۹۵۴
Kids ۳۱۸×۴۰۰	coins ۶۴×۷۹	۰,۱۵۶۵	۵۶,۱۸۶۵	۰,۱۵۶۵	۵۶,۱۸۶۹	۰,۱۵۶۰	۵۶,۱۹۹۸	۰,۱۵۵۵	۵۶,۲۱۲۳
Kids ۳۱۸×۴۰۰	football ۶۴×۸۰	۰,۱۶۰۳	۵۶,۰۸۰۹	۰,۱۶۱۴	۵۶,۰۵۱۶	۰,۱۵۸۵	۵۶,۱۳۱۶	۰,۱۵۷۷	۵۶,۱۵۱۹
Office ۹۰۳×۶۰۰	cameraman ۶۴×۶۴	۰,۰۳۰۱	۶۳,۳۴۶۵	۰,۰۳۰۰	۶۳,۳۶۲۵	۰,۰۲۹۹	۶۳,۳۷۲۷	۰,۰۲۹۹	۶۳,۳۷۲۷
Office ۹۰۳×۶۰۰	coins ۶۴×۷۹	۰,۰۳۷۲	۶۲,۴۲۷۳	۰,۰۳۷۰	۶۲,۴۴۵۷	۰,۰۳۶۸	۶۲,۴۷۰۴	۰,۰۳۶۷	۶۲,۴۸۲۴
Office ۹۰۳×۶۰۰	football ۶۴×۸۰	۰,۰۳۷۶	۶۲,۳۷۶۳	۰,۰۳۷۸	۶۲,۳۵۲۱	۰,۰۳۷۶	۶۲,۳۷۷۴	۰,۰۳۷۳	۶۲,۴۰۹۷

روش پیشنهادی، نسبت به LSB ساده و روش دسته‌بندی پیکسل‌ها براساس بیت دوم و سوم کم‌ارزش بسیار کارآمد است. کارایی این روش با دو معیار ارزیابی کیفیت MSE و PSNR سنجیده شده است. روش ارائه‌شده در این مقاله دارای MSE **کمتر** و PSNR بالاتری نسبت به روش‌های LSB ساده و دسته‌بندی پیکسل‌ها براساس بیت دوم و سوم کم‌ارزش است.

البته روش پیشنهادی، معایبی نیز دارد. یکی از معایب این روش، سربار آرایه p است که موجب ذخیره‌سازی بیت‌های بیشتری خواهد شد. البته در پیام‌های مخفی به‌نسبه بزرگ، این سربار قابل چشم‌پوشی است.

۹- مراجع

[1] Rai P, Gurung S, Ghose MK. Analysis of Image Steganography Techniques: A Survey. International Journal of Computer Applications. 2015 Jan 1;114(1): pp. 11-17.

[2] Anderson RJ, Petitcolas FA. On the limits of steganography. IEEE Journal on selected areas in communications. 1998 May;16(4): pp. 474-81.

[3] Provos N, Honeyman P. Hide and seek: An introduction to steganography. IEEE security & privacy. 2003 May;99(3): pp. 32-44.

[4] Devi KJ. A sesure image steganography using LSB technique and pseudo random encoding technique. National Institute of Technology Rourkela. 2013.

[5] Roy R, Changder S, Sarkar A, Debnath NC. Evaluating image steganography techniques: Future research challenges. International Conference on Computing, Management and Telecommunications (ComManTel 2013) [IEEE]. 2013 Jan: pp. 309-314.

[6] Morkel T, Eloff JH, Olivier MS. An overview of image steganography. InISSA 2005 Jun: pp. 1-11.

[7] Gutub AA. Pixel indicator technique for RGB image steganography. Journal of Emerging Technologies in Web Intelligence. 2010 Feb;2(1): pp. 56-64.

[8] Steganalysis HC, Westfeld A. F5—A Steganographic Algorithm. InInformation Hiding: 4th International Workshop, IH 2001, Pittsburgh, PA, USA, April 25-27, 2001. Proceedings 2001 Nov 7 (Vol. 2137). pp. 289-302.

[9] Chan CK, Cheng LM. Hiding data in images by simple LSB substitution. Pattern recognition. 2004 Mar 31;37(3): pp. 469-74.

[10] Sallee P. Model-based steganography. In International Workshop on Digital Watermarking 2003 Oct 20. pp. 154-167. Springer Berlin Heidelberg.

[11] Samima S, Roy R, Changder S. Secure key based image realization steganography. InImage Information Processing (ICIIP), 2013 IEEE Second International Conference on 2013 Dec 9. pp. 377-382. IEEE.

[12] Roy R, Changder S. Image realization steganography with LCS based mapping. InContemporary Computing (IC3), 2014 Seventh International Conference on 2014 Aug 7. pp. 218-223. IEEE.

[13] Wu DC, Tsai WH. A steganographic method for images by pixel-value differencing. Pattern Recognition Letters. 2003 Jun 30;24(9): pp. 1613-1626.

[14] Wu HC, Wu NI, Tsai CS, Hwang MS. Image steganographic scheme based on pixel-value differencing and LSB replacement methods. IEE Proceedings-Vision, Image and Signal Processing. 2005 Oct 1;152(5): pp. 611-615.

[15] Raja KB, Chowdary CR, Venugopal KR, Patnaik LM. A secure image steganography using LSB, DCT and compression techniques on raw images. InIntelligent Sensing and Information Processing, 2005. ICISIP 2005. Third International Conference on 2005 Dec 14. pp. 170-176. IEEE.

[16] Bhardwaj R, Sharma V. Image Steganography Based on Complemented Message and Inverted Bit LSB Substitution. Procedia Computer Science. 2016 Dec 31;93: pp. 832-838.

[17] Siper A, Farley R, Lombardo C. The rise of steganography. Proceedings of Student/Faculty Research Day, CSIS, Pace University. 2005 May 6.

منصور فاتح در سال ۱۳۹۴ مدرک کارشناسی مهندسی برق و الکترونیک خود را از دانشگاه صنعتی شاهرود و در سال ۱۳۸۷مدرک کارشناسی ارشد مهندسی برق خود را از دانشگاه تربیت مدرس تهران اخذ کرد. پس از آن در سال ۱۳۸۸ به دوره دکترای مهندسی برق و الکترونیک در دانشگاه تربیت مدرس تهران وارد گردید. ایشان از سال ۱۳۹۰ بورسیه دانشگاه صنعتی شاهرود گردید و از سال ۱۳۹۴ به‌عنوان عضو هئیت علمی دانشکده کامپیوتر با این دانشگاه همکاری می‌نماید. زمینه پژوهشی مورد علاقه او پردازش تصویر و ویدئو، بازشناسی الگو و هوش مصنوعی است.

سمیرا رجب‌لو مدرک کارشناسی خود را در سال ۱۳۹۳ در رشته علوم کامپیوتراز دانشگاه سلمان فارسی کازرون دریافت نمود. هم‌اکنون ایشان دانشجوی مقطع کارشناسی ارشد در رشته مهندسی کامپیوتر گرایش هوش‌مصنوعی در دانشگاه صنعتی شاهرود می‌باشد. زمینه تحقیقاتی مورد علاقه وی امنیت در شبکه های خودرویی می‌باشد.

الهه علی‌پور مدرک کـــارشناسی خود را در سال ۱۳۹۴ در رشـــته مهندسی کامپیوتر گرایش نرم‌افزار از دانشگاه بیرجند دریافت نمود. هم اکنون ایشان دانشجوی مقطع کارشناسی ارشد در رشته مهندسی کامپیوتر گرایش هوش-مصنوعی در دانشگاه صنعتی شاهرود می‌باشد. زمینه تحقیقاتی مورد علاقه وی پردازش تصویر می‌باشد.