

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 ریاتیک، 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 تغییر یافته 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. MSE و PSNR روش پیشنهادی در مقایسه با روش LSB ساده، به ترتیب دارای نرخ رشد ۰٫۱۳ درصدی و نرخ کاهش ۰٫۱۹ درصدی هستند.

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

۱- مقدمه

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 ته‌نقش‌نگاری^۲، نهان‌نگاری^۳ و رمزنگاری^۴ هستند. به‌منظور حفظ حق مالکیت

امروزه، با استفاده 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].

¹ Data Hiding

² watermarking

³ steganography

⁴ cryptography

تبدیل کسینوسی^۱ (DCT)، فوریه^۲ یا ویولت^۳ باشند [۴]. در این مقاله علاوه بر ارائه روشی در حوزه 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^۴ (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، نهان‌سازی 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 تغییر یافته 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 بخش ۲ به کارهای انجام‌شده در زمینه نهان‌نگاری و در بخش ۳ به معرفی نهان‌نگاری و در بخش ۴ روش LSB ساده پرداخته شده است. در بخش ۵ دسته‌بندی پیکسل‌ها براساس بیت دوم و سوم و در بخش ۶ روش پیشنهادی و در بخش‌های ۷ و ۸ به ترتیب آزمایش‌ها و نتایج آن‌ها و نتیجه‌گیری آورده شده است، و در بخش آخر منابع ذکر شده است.

۲- کارهای مرتبط

سایمونز^۵ و همکارانش در سال ۱۹۸۳ یک سامانه پایه نهان‌نگاری ارائه دادند. در این سامانه دو زندانی با نام‌های

در نشر یک محصول از ته‌نقش‌نگاری استفاده می‌شود. رمزنگاری برای نهان‌سازی 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 نهان و grafia به معنای نوشتن مشتق شده 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، می‌تواند به‌صورت ساده یا تصادفی انتخاب شوند. روش‌های نهان‌نگاری در حوزه تبدیل، با مخفی‌سازی بیت‌های پیام در ضرایب تبدیل تصویر پوشانه انجام می‌شوند. این تبدیل‌ها می‌تواند

¹ Discrete Cosine Transform

² Discrete Fourier Transform

³ Discrete Wavelet Transform

⁴ Least significant bit

⁵ Simmons

تفاضل مقدار پیکسل^۸ (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 بازه 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 به دست 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 DCT، LSB 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 در نهایت الگوریتم‌های کوانتیزاسیون^۹ و کدگذاری طول اجرا^{۱۰} 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 تغییر یافته^{۱۱} بیشتر از تعداد پیکسل‌های بدون تغییر، معکوس می‌شوند. مشکل این روش لحاظ کردن تنها یک دسته است. در حالی که 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 بر اساس مقادیر بیت‌های دوم و سوم و چهارم انجام می‌شوند.

آیس و باب قصد طرح‌ریزی یک نقشه فرار را دارند. برای طرح نقشه فرار، آیس قصد ارسال پیامی برای باب را دارد. ارتباط آیس و باب توسط ویلی زندانبان بررسی می‌شود. آیس 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 حوزه 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]. به منظور افزایش امنیت روش LSB، روش PI^۱ ارائه شده است [۷]. در این روش، پیام در کانل‌های 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^۲ (OPAP) است [۸]. OPAP اختلاف بین پیکسل‌های تصویر اصلی و نهان‌نگاری شده را محاسبه و بیت‌های مخفی شده را به منظور بهبود شفافیت تغییر می‌دهد [۹]. OPAP، مقادیر PSNR^۳ بالایی برای تصاویر استاندارد Baboon و Lena تولید کرده است [۱۰]. یکی دیگر از روش‌های نهان‌نگاری، نهان‌نگاری ادراکی تصویر^۴ 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 برابر حمله‌های آماری مانند حملات هیستوگرامی است. برای توسعه این روش، یک روش نگاشت محرمانه پوشانه توسط چانگدر^۵ و روی^۶ به‌عنوان کمینه مشترک توالی^۷ (LCS) ارائه شده است [۱۲]. این روش، در برابر حمله‌های Brute-Force بسیار مقاوم است. همچنین در این روش، ظرفیت مخفی‌سازی افزایش یافته است.

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

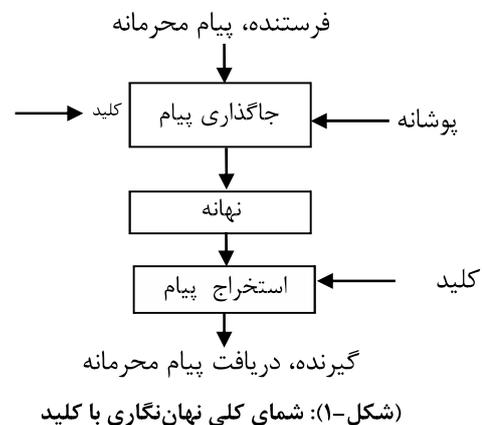
¹⁰ runlength coding algorithm

۳- نهان نگاری

نهان نگاری برای نخستین بار توسط حاکم یونانی اسیر شده به دست داریوش در قرن پنجم انجام شد. این حاکم یونانی با حکاکمی پیام بر روی سر غلام خود، نهان نگاری را شکل داد. بعد از آن، نهان نگاری در لوح‌های پوشیده از موم، نامرئی نویسی با جوهرهای آبلیمو در زمان روم باستان مورد استفاده قرار گرفت. همچنین نهان نگاری در جنگ جهانی دوم در مکتوبات غیرمحرمانه استفاده شد [۱۷]. هدف از نهان نگاری، مخفی سازی ماهیت پیام محرمانه از افراد غیرمجاز است و مهاجم نمی تواند انتقال اطلاعات محرمانه در پس زمینه یک ارتباط عمومی را شناسایی کند [۳]. در رمزنگاری فرستنده، گیرنده و پیام رمز شده مشخص است؛ اما در نهان نگاری پنهان ماندن فرستنده، گیرنده و پیام محرمانه از ارکان اصلی محسوب می شوند.

از روش های نهان نگاری می توان به نهان نگاری صنعتی، زبانی و دیجیتال اشاره کرد. در نهان نگاری صنعتی از علوم مهندسی، فیزیک و غیره جهت پنهان کردن اطلاعات استفاده می شود. در نهان نگاری زبانی، مخفی سازی اطلاعات از طریق نوشتن صورت می پذیرد. همچنین نهان نگاری دیجیتال، علم مخفی سازی پیام در یک رسانه دیجیتال مانند صوت، تصویر، ویدئو و متن است.

امروزه به دلیل تنوع زیاد تصویر، تصویر به عنوان بستری ایمن جهت مخفی سازی پیام استفاده می شود و به آن پوشانه می گویند. به تصویر تولید شده بعد از درج داده های محرمانه، نهان می گویند. در روش های نهان نگاری، اغلب از یک کلید جهت به هم ریختگی پیام استفاده می شود تا در صورت شناسایی وجود پیام محرمانه، محتوای پیام به طور صریح آشکار نشود. شمای کلی نهان نگاری با کلید به صورت شکل (۱) است:



روش های حوزه مکان، از روش های نهان نگاری در تصویر هستند. در این روش ها، برخی بیت های موجود در پیکسل های تصویر، جهت پنهان سازی داده ها به طور مستقیم تغییر می کنند. در این روش ها، از اطلاعات RGB یا شدت روشنایی پیکسل های تصویر جهت پنهان سازی اطلاعات استفاده می شود. یکی از روش های نهان نگاری تصویر در حوزه مکان روش LSB است که در بخش بعدی به شرح آن پرداخته شده است.

۴- روش LSB

نهان نگاری مبتنی بر LSB یکی از ساده ترین روش های نهان نگاری است. در این روش، پیام محرمانه در بیت های کم ارزش پیکسل های مورد نظر مخفی می شوند. تغییرات ایجاد شده در این روش، قابل ردیابی توسط چشم نیست [۶]؛ اما این روش اغلب بر روی هیستوگرام تصویر، تأثیر گذار است و توسط الگوریتم های نهان کاوی قابل ردیابی است. یک مثال ساده از روش LSB در ادامه آمده است:

پیام مورد نظر جهت مخفی سازی: ۱۰۱

پیکسل های تصویر پوشانه جهت مخفی سازی:

۰۱۰۱۱۰۱۰ ۱۱۱۰۱۰۰۱ ۱۰۱۰۱۱۱۰

با استفاده از روش LSB (مخفی سازی بیت های پیام در بیت های کم ارزش پیکسل ها) پیکسل های نهان به صورت زیر هستند:

۰۱۰۱۱۰۱۱ ۱۱۱۰۱۰۰۰ ۱۰۱۰۱۱۱۱

همان طور که مشاهده می شود، تمامی پیکسل ها دچار تغییر شده اند. یک روش برای به کمینه رساندن تعداد تغییرات در LSB، دسته بندی پیکسل ها بر اساس بیت های دوم و سوم کم ارزش آن ها است [۱۶]. این روش در بخش بعدی شرح داده شده است.

۵- دسته بندی پیکسل ها بر اساس بیت

دوم و سوم کم ارزش آن ها

پیکسل ها را می توان بر اساس بیت دوم و سوم کم ارزش آن ها دسته بندی و تغییرات را پس از مخفی سازی پیام در بیت های کم ارزش پیکسل ها، محاسبه کرد [۱۶]. در این روش، پیکسل ها در چهار دسته قرار می گیرند. این دسته ها بر اساس مقادیر بیت دوم و سوم کم ارزش هر پیکسل یعنی ۰۰، ۰۱، ۱۰ و ۱۱ ایجاد شده اند. در این روش، ابتدا با روش LSB

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 لحاظ کردن اولویت، ارائه شده است که نتایج به‌مراتب بهتری از روش مرجع [۱۶] و بهبود یافته 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 مرحله مخفی‌سازی و استخراج پیام است که در ادامه به آنها پرداخته شده است.

۶-۱- مرحله مخفی‌سازی پیام

در مرحله 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 دسته ۰۰۰، ۰۰۱، ۰۱۰، ۰۱۱، ۱۰۰، ۱۰۱، ۱۱۰ و ۱۱۱ تقسیم می‌شوند. سپس بیت‌های پیام در کم‌ارزش‌ترین بیت پیکسل‌های تصویر پوشانه مخفی می‌شوند. در ادامه، این پیکسل‌ها، براساس بیت دوم، سوم و چهارم به هشت دسته 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 آرایه 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.

بیت‌های پیام در کم‌ارزش‌ترین بیت هر پیکسل جاسازی می‌شود؛ سپس به‌منظور کاهش تغییرات، LSB نخستین دسته 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 بررسی نشده میزان تغییرات

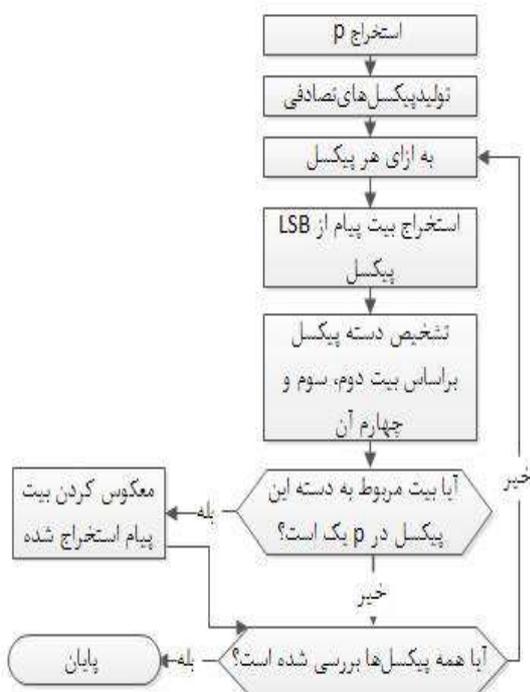
پیکسل است و در غیر این صورت پیام اصلی برابر با LSB آن پیکسل است. چارت استخراج پیام در شکل (۴) آمده است.

۷- آزمایش‌ها و نتایج

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

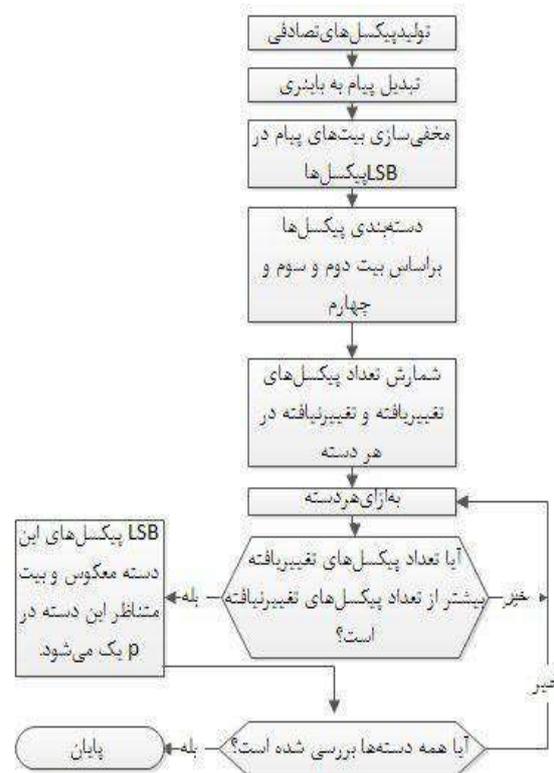
جهت ارزیابی تصویر نهانه، از دو معیار ارزیابی کیفیت تصویر، میانگین مربعات خطا^۱ (MSE) و نسبت سیگنال به نوفه (PSNR) استفاده شده است. MSE بیان‌کننده اختلاف پیکسل به پیکسل تصویر پوشانه و نهانه است. طریقه محاسبه^۱ MSE در رابطه (۱) نشان داده شده است.

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



(شکل-۴): چارت استخراج پیام

^۱ Mean Square Error



(شکل-۳): چارت مخفی‌سازی پیام

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

۶-۲- مرحله استخراج پیام

گیرنده با در اختیار داشتن نهانه و کلید می‌تواند پیام را استخراج کند. گیرنده با دریافت نهانه به خوبی نسبت به آرایه^p آگاهی دارد و به تغییرات اعمال شده در بیت‌های کم‌ارزش پیکسل‌های تصادفی تولید شده پی خواهد برد. هشت بیت ابتدایی پیام استخراج شده 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 دسته هر پیکسل و مقدار^p برای این دسته، پیام اصلی استخراج می‌شود. در صورتی که بیت متناظر در^p برابر با یک باشد، پیام اصلی برابر با معکوس LSB آن

در نتیجه منجر به محرمانگی بیشتری می‌شود. در روش مرجع [۱۶] بر طبق یک اولویت، تنها بیت کم‌ارزش یک دسته از پیکسل‌ها معکوس می‌شوند. در واقع، از میان چند دسته از پیکسل‌ها، با بیت کم‌ارزش تغییر یافته بیشتر از تغییر نیافته، تنها بیت کم‌ارزش یک دسته معکوس می‌شوند. این حالت ممکن است که برای چند دسته از پیکسل‌ها رخ دهد. در این صورت، با معکوس کردن بیت کم‌ارزش تمام این دسته از پیکسل‌ها، میزان تغییرات تصویر پوشانه خیلی کمتر خواهد شد. در روش پیشنهادی، علاوه بر لحاظ کردن 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.



(الف) تصویر پوشانه (ب) پیام محرمانه



(ج) تصویر نهانه (د) پیام استخراج شده

(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. نحوه محاسبه این پارامتر در روابط (۲) و (۳) آمده است.

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

$$p = \max(C(i, j), S(i, j)) \quad (3)$$

PSNR بزرگ‌تر، به معنی حفظ هر چه بیشتر کیفیت تصویر و ارائه روش نهان‌نگاری بهتر است. عملکرد روش پیشنهادی، در جدول (۱) با روش مرجع [۱۶]، بهبود یافته 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

(جدول ۱): مقایسه روش پیشنهادی با سایر روش‌ها

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

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

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 secure 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.

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

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

۱۳۸۷ مدرک 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 هیئت 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

کامپیوتر از دانشگاه سلمان فارسی

کازرون دریافت نمود. هم‌اکنون

ایشان دانشجوی مقطع کارشناسی

ارشد در رشته مهندسی کامپیوتر گرایش هوش مصنوعی در

دانشگاه صنعتی شاهرود می‌باشد. زمینه تحقیقاتی مورد

علاقه وی امنیت در شبکه های خودروپی می‌باشد.



الهه علی‌پور مدرک کارشناسی

خود را در سال ۱۳۹۴ در رشته

مهندسی کامپیوتر گرایش نرم‌افزار

از دانشگاه بیرجند دریافت نمود.

هم‌اکنون 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.

[6] Morkel T, Eloff JH, Olivier MS. An overview of image steganography. *InfSSA 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. In *Information 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. In *Image 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. In *Contemporary 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. In *Intelligent 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

