مجله علمی- پژوهشی "پدافند الکترونیکی و سایبری"
سال پنجم، شماره ۲، تابستان ۱۳۹۶، ص ۱۰۷-۹۵

نهان‌نگاری تطبیقی تصویر مبتنی بر آنتروپی در گراف با کارایی و امنیت بهبودیافته

محمدعلی شمع علیزاده بایی [۱*]، زین‌العابدین نوروزی [۲]، محمد سبزی‌نژاد [۳]، محمدرضا کرمی [۴]

۱- دانشجوی دکتری، ۲- استادیار، دانشگاه امام حسین (ع)، ۳- استادیار، دانشگاه خوارزمی، ۴- دانشیار، دانشگاه صنعتی نوشیروانی بابل
(دریافت: ۹۵/۰۶/۲۸، پذیرش: ۹۵/۱۰/۱۴)

چکیده

نهان‌نگاری تطبیقی در حوزه‌های مکان و فرکانس کاربرد وسیعی دارد. از آن‌جایی‌که تشخیص وجود پیام مخفی‌شده در لبه‌های تیز واقع در نواحی پر اعوجاج و شلوغ یا زبر دشوار است، مخفی‌سازی پیام در این نقاط بهینه است. در این مقاله یک روش نهان‌نگاری تطبیقی در حوزه مکان طراحی شده است که قابل استفاده در حوزه فرکانس است. در این الگوریتم زبری پنجره‌های ناهم‌پوشان ۳×۳ از تصویر، با استفاده از آنتروپی گراف وزن‌دار متناظرش، محاسبه می‌شود. هم‌چنین پیکسل‌های لبه پنجره‌های زبر به شیوه جدیدی استخراج می‌شود. اهمیت دیگر روش این است که این الگوریتم، با توجه به طول پیام، آن‌ها را با چگالی مناسبی در سراسر تصویر مخفی می‌کند. پیاده‌سازی الگوریتم پیشنهادی روی ۵۰۰۰ تصویر طبیعی و به‌کارگیری یک الگوریتم نهان‌کاوی مدرن، نشان می‌دهد که الگوریتم پیشنهادی در مقایسه با الگوریتم‌های تطبیقی نوین دیگر، بیش از ۱٪ از سطح امنیت بالاتری برخوردار است.

واژه‌های کلیدی: نهان‌نگاری تطبیقی، آنتروپی در گراف، پنجره‌های زبر، امنیت.

۱- مقدمه

علم و هنر مخفی‌سازی اطلاعات در یک رسانه دیجیتال (تصویر، صوت، فیلم، متن) را نهان‌نگاری می‌نامند و هدف از آن پنهان‌کردن هرگونه ارتباط بین فرستنده و گیرنده یک پیام است. فرآیند جاسازی پیام در یک تصویر را پنهان‌سازی[۱] پیام می‌گویند. به تصویر مورد استفاده برای پنهان‌سازی پیام، پوشانه[۲] و به تصویری که در اثر جاسازی پیام به‌وسیله یک الگوریتم نهان‌نگاری به‌دست می‌آید، تصویر میزبان یا نهانه[۳] می‌گویند [۱]. برخی از نویسندگان به‌جای واژه نهان‌نگاری از کلمه پنهان‌نگاری نیز استفاده می‌کنند. برخلاف نهان‌نگاری، علم نهان‌کاوی[۴] نیز به‌منظور تشخیص این‌که آیا پیام محرمانه‌ای در یک رسانه دیجیتال جاسازی‌شده یا خیر، طراحی گردید. در اندازه‌گیری امنیت، علم تحلیل نهان‌نگاری یا نهان‌کاوی، به‌منظور ارزیابی کارایی الگوریتم‌های نهان‌نگاری از دیدگاه امنیت، به‌کارگیری می‌شود. روش‌های نهان‌کاوی با استفاده از عملیات پردازش تصویر، ویژگی‌های آماری ساختار تصویر نهانه مانند آماره درجه اول (هیستوگرام) یا آماره درجه دوم (ارتباط بین پیکسل‌ها) را تحلیل می‌کنند [۲].

روش‌های نهان‌نگاری تطبیقی به متن پوشانه توجه ویژه‌ای دارند. به‌دلیل اهمیت لبه‌ها و مکان‌های نویزی تصویر از لحاظ حفظ و ارتقای امنیت، روش‌های نهان‌نگاری تطبیقی مبتنی بر لبه شکل‌گرفته‌اند. چراکه تشخیص وجود پیام جاسازی‌شده در چنین نقاطی آسان نیست. مسئله دیگری که در نهان‌نگاری مبتنی بر لبه وجود دارد، اختلاف پیکسل‌های لبه تصویر در قبل و بعد از نهان‌نگاری، یعنی در پوشانه و نهانه است. از آن‌جایی‌که تحقیقات در نهان‌نگاری تطبیقی سابقه زیادی ندارد، تلاش برای رفع محدودیت‌های فوق نیازمند تحقیقات بیش‌تری است.

از اولین روش‌های نهان‌نگاری تطبیقی می‌توان روش نهان‌نگاری PVD[۵] را نام برد که مبتنی بر لبه شکل گرفته است و پیام را در اختلاف بین پیکسل‌های مجاور جاسازی می‌کند [۳]. دسته دیگری از روش‌های نهان‌نگاری مبتنی بر لبه، روش‌هایی هستند که لبه را با استفاده از روش‌های معمول در پردازش تصویر، مانند سوبل[۶] و کنی[۷] شناسایی می‌کنند. محدودیت این روش‌ها نیز در تفاوت پیکسل‌های لبه در پوشانه و نهانه، قبل و بعد از جاسازی پیام است. دسته سوم از آن‌ها، روش‌های نهان‌نگاری تطبیقی مبتنی بر LSB، مانند LSBMR[۸]، EAMR[۹] و I-EAMR[۱۰] هستند که محدودیت اصلی آن‌ها جاسازی ناخواسته در مناطق صاف تصویر و

* رایانامه نویسنده مسئول: ma.shamalizade@gmail.com

1- Message hiding
2- Cover
3- Stego
4- Steganalysis
5- Pixel Value Difference
6- Sobel
7- Canny
8- LSB Matching Revisited
9- Edge Adaptive LSB Matching Revisited
10- Inproved EAMR

تشخیص توسط بعضی از الگوریتم‌های نهان‌کاوی است.

در این مقاله، یک روش نهان‌نگاری تطبیقی کارآمد براساس تشخیص نواحی شلوغ از لبه و نویز (نواحی زبر[1]) در پوشانه تصویری ارائه می‌شود که در آن از مفهوم آنتروپی در گراف استفاده می‌شود. این روش، که با استفاده از نگاشت تصویر در گراف تعریف می‌شود در مقایسه با روش‌های قبلی، با دقت بیش‌تری به شناسایی نواحی زبر و شلوغ از لبه و نویز در تصویر می‌پردازد. لذا، از امنیت خوبی برخوردار است. امتیاز مهم دیگر روش پیشنهادی این است که با انتخاب یک آستانه مناسب به انتشار و جاسازی بیت‌های پیام در سراسر تصویر می‌پردازد که این کار باعث تقویت امنیت پیام جاسازی‌شده در تصویر می‌شود. مسئله مهم دیگر در نهان‌نگاری تطبیقی این است که الگوریتم باید به‌گونه‌ای طراحی شود تا مکان لبه‌های پوشانه و نهانه یک تصویر داده‌شده، یکسان گردد. الگوریتم پیشنهادی از این امتیاز نیز برخوردار است.

در ادامه این مقاله، در بخش ۲ روش‌های نهان‌نگاری مرتبط بررسی می‌شود. بخش ۳ به پیش زمینه مورد نیاز در طراحی الگوریتم پیشنهادی، مانند نگاشت یک تصویر در گراف و آنتروپی در گراف پرداخته می‌شود. الگوریتم پیشنهادی در بخش ۴ بیان می‌شود. در بخش ۵ نتایج تجربی الگوریتم طراحی‌شده و درنهایت در بخش ۶ نتیجه‌گیری می‌شود.

۲- تحقیقات مرتبط

رؤیت‌ناپذیری[2] یک شرط اساسی در نهان‌نگاری است که توانایی این روش‌ها را در بهبود کیفیت بینایی تصاویر نهانه تولیدشده منعکس می‌کند. به‌خوبی می‌دانیم که سیستم بینایی انسان در نواحی زبر و تیز تصویر در مقایسه با نواحی صاف و نرم، از حساسیت کم‌تری برخوردار است. از طرفی برجستگی‌های لبه و نویز به‌دلیل تفاوتی که با پیکسل‌های مجاور دارند، به‌راحتی توسط روش‌های نهان‌کاوی قابل شناسایی نیستند. اولین روش نهان‌نگاری طراحی‌شده براساس این واقعیت، روش PVD[3] است که تلاش می‌کند جاسازی را در لبه‌ها انجام دهد. این روش که در ۲۰۰۳ توسط ویو[4] و تیسای[5] ارائه شد [۳]، تفاوت‌ها را تنها در یک جهت عمودی یا افقی تصویر درنظر می‌گیرد که شناسایی تمام لبه‌ها را تضمین نمی‌کند. روش IPVD[6] [۴] برای رفع چالش ایجادشده در PVD در سال ۲۰۰۴ توسط ژانگ[7] و وانگ[8] مطرح شد. این روش با تنظیم نحوه جاسازی به نحو مطلوب‌تر، ناهمگونی مورد نظر در روش PVD را برطرف کرد. اما دارای یک ایراد اساسی است و آن این است که زوج پیکسل‌ها را براساس تفاضل بیش‌ترشان انتخاب نمی‌کند. درنتیجه باعث ناهمگونی دیگری در هیستوگرام نهانه می‌شود. روش AE-LSB[9] در ۲۰۰۸ توسط چنگ- هسینگ یانگ[10] و همکارانش ارائه شد [۵]. این روش نیز با تنظیم نحوه جاسازی به‌صورت مطلوب‌تر ناهمگونی مورد نظر در روش PVD را برطرف کرد. ولی مشابه IPVD جاسازی پیام را در یک مکان تصادفی از تصویر به پایان می‌رساند که این هم باعث یک ناهمگونی در هیستوگرام نهانه می‌شود. ناگفته نماند که AE-LSB به‌دلیل این‌که از میانگین نرخ تغییرات کم‌تری برخوردار است، دارای ظرفیت جاسازی بالاتری است اما در مقابل حمله‌ای معروف به حمله RS[11] دارای ضعف است [۶].

چن[12] و همکارانش در سال ۲۰۱۰ یک روش ترکیبی تشخیص لبه برای پنهان‌سازی پیام معرفی کردند [۷]. در این روش، یک تصویر لبه توسط اجرای روش‌های تشخیص لبه فازی و کنی ایجاد می‌شود. مشکل اصلی این روش، تغییرات ناخواسته‌ای است که در تصویر نتیجه ایجاد می‌شود.

لیو[13] و همکارانش نیز در سال ۲۰۱۰ یک الگوریتم تطبیقی بازبینی‌شده از LSBMR [۸] معروف به EAMR را مطابق لبه طراحی کردند [۹]. این روش لبه‌های عمودی و افقی را به روشی سازگار شناسایی می‌کند. این روش نواحی لبه را با محاسبه اختلاف بین پیکسل‌های متوالی جستجو می‌کند. انتخاب نواحی به‌طول پیام محرمانه بستگی دارد و توسط یک مقدار آستانه شناخته می‌شود. این روش از لبه‌های افقی و عمودی با تقسیم تصویر به پنجره‌های ۳×۳ و سپس دوران پنجره‌ها با یک زاویه تصادفی استفاده می‌کند. با این حال، این فرایند نیز می‌تواند ارتباط بین پیکسل‌های عمودی و افقی را از بین ببرد، ولی با این وجود، به‌دلیل ضعف در انتخاب آستانه، لبه‌های زیادی را از دست می‌دهد و بعضاً در مناطق صاف و هموار جاسازی می‌کند. در سال ۲۰۱۴، هوانگ[14] و همکاران الگوریتم I-EAMR را پیشنهاد دادند [۱۰] که توسعه‌ای از الگوریتم EAMR است. در این روش، برخلاف روش EAMR که در آن زوج پیکسل‌های متوالی به‌صورت ترتیبی انتخاب می‌شدند، پوشانه به پنجره‌های ناهمپوشان ۳×۳ تقسیم شده و زوج پیکسل‌های مجاور به‌طور تصادفی در هر پنجره

1- High texture
2- Imperceptibility
3- Pixel Value Difference
4- Wu
5- Tsai
6- Improvement PVD
7- Zhang
8- Wang
9- Adaptive Edge LSB
10- Cheng-Hsing Yang
11- Regular Singular
12- Chen
13- Lou
14- Huang

۳×۳، برطبق جهت‌های مختلف انتخاب شده و جاسازی پیام طبق روش LSBR، در لبه‌های تصویر صورت می‌گیرد، اما مسئله تعیین آستانه هم‌چنان وجود دارد.

جاسازی ماتریسی اولین بار توسط کراندال[1] در سال ۱۹۹۸ [۱۱] به‌منظور افزایش کارایی نهان‌نگاری از طریق کاهش اختلاف بین تصاویر پوشانه و نهانه معرفی شد که از عمل xor برای پنهان‌کردن بیت‌های پیام در پیکسل‌های تصویر استفاده می‌کند. سپس وستفلد[2] در سال ۲۰۰۱ روش F_5 را معرفی کرد که در آن برای جاسازی n بیت، $2^n - 1$ پیکسل مصرف می‌شود [۱۲]. این روش برای $n = 2$ دارای نرخ جاسازی ۰/۶۷ bpp و نرخ تغییر bpp ۰/۲۵ است که نرخ‌های مناسبی هستند. هیات الدیمور[3] و احمد الانی در سال ۲۰۱۶ [۱۳] با تقسیم تصویر به پنجره‌های ۳×۳ ناهم‌پوشان و محاسبه میانگین تفاضلات ستون‌های چپ و راست هر قالب و تکرار آن برای سطرهای بالا و پایین و همین‌طور قطرهای اصلی و فرعی، حداکثر مقدار آن‌ها را e نامیده و با درنظر گرفتن یک آستانه تجربی Th پنجره‌های که $e > Th$ باشد را پنجره‌های لبه نامیدند. آن‌ها در این روش، پس از تشخیص پنجره‌های لبه، در چهار پیکسل از آن‌ها با استفاده از عمل xor، سه بیت پیام را جاسازی می‌کنند. در این روش با وجود این‌که نرخ تغییر پیکسل ها bpp ۰/۲۵ است، فقط چهار پیکسل از هر پنجره ۳×۳ در شناسایی پیکسل‌های لبه نقش دارند و بقیه پیکسل‌ها که اکثریت دارند، به‌کار گرفته نمی‌شوند.

۳- پیش زمینه

پیچیدگی یک تصویر می‌تواند توسط میزان صافی[4] و یکنواختی آن به‌طور کمی ارزیابی شود. به‌طورکلی، یکنواختی و صافی یک پنجره از تصویر به چگونگی توزیع شدت روشنایی پیکسل‌های آن بستگی دارد. توزیع یکنواخت‌تر، صافی بیش‌تر تصویر را نشان می‌دهد و در مقابل پنجره‌هایی با صافی کم‌تر به معنی وجود نوسان بیش‌تر شدت روشنایی در آن‌ها است که اصطلاحاً در این مقاله پنجره‌های زبر[5] نامیده می‌شوند. در این مقاله برای ارزیابی کمی زبری هر پنجره ۳×۳ از تصویر، استفاده از آنتروپی محلی در گراف متناظر تصویر، در دستور کار قرار داده می‌شود. بنابراین، در این بخش نخست روش معمول محاسبه آنتروپی در پردازش تصویر یادآوری می‌شود. سپس با استفاده از مفاهیم نظریه گراف و آنتروپی در گراف، روش نوینی برای محاسبه آنتروپی محلی تصویر طرحی شده و نتایج تجربی آن‌ها مقایسه می‌شود. در ادامه این بخش روشی برای استخراج پیکسل‌های لبه پنجره‌های زبر تصویر طراحی می‌شود که اهمیت آن در این است که لبه‌های شناسایی‌شده در پنجره متناظر یک پوشانه و نهانه مربوطه یکسان است.

۳-۱- آنتروپی تصویر

با توجه به مفاهیم مطرح‌شده در نظریه اطلاعات و پردازش تصویر محتویات اطلاعاتی یک سیگنال با استفاده از آنتروپی قابل ارزیابی است [۱۴]. اگر $I = [I_{ij}]$ یک تصویر خاکستری $M \times N$ باشد، آنتروپی تصویر I به‌صورت زیر قابل محاسبه است:

$$H = -\sum_{i=1}^{M}\sum_{j=1}^{N} q_{ij}\,\mathrm{Log}\,q_{ij} \qquad (۱)$$

$$q_{ij} = \frac{I_{ij}}{\sum_{i=1}^{M}\sum_{j=1}^{N} I_{ij}} \qquad (۲)$$

که در آن، I_{ij} شدت روشنایی پیکسل(i,j)، q_{ij} توزیع احتمال I_{ij} و H آنتروپی تصویر I است [۱۴]. آنتروپی تصویر نشان‌دهنده میزان تفرق و پراکندگی شدت روشنایی پیکسل‌های آن است. با توجه به این‌که ماکزیمم رابطه (۱) زمانی اتفاق می‌افتد که $q_{xy} = q_{x'y'}$، لذا می‌توان نتیجه گرفت تصاویری که شدت روشنایی یکنواخت‌تری دارند آنتروپی بیش‌تر و در مقابل تصاویری که تغییرات شدت روشنایی آن‌ها زیاد و شدیدتر باشد، دارای آنتروپی کم‌تری هستند. از طرفی، از مطلب فوق می‌توان نتیجه گرفت که آنتروپی یک زیرماتریس از تصویر با واریانس و انحراف معیار داده‌های ماتریس رابطه عکس دارد. این یعنی با افزایش واریانس و انحراف معیار، آنتروپی کاهش و درنتیجه داده‌های چنین ماتریسی از یکنواختی و صافی دور می‌شود. بنابراین معمولاً آنتروپی یک پنجره از تصویر با تقسیم فرمول فوق بر انحراف معیار داده‌های ماتریس به‌صورت زیر به دست می‌آید [۱۴]:

$$H_w = -\frac{\sum_{i=1}^{M}\sum_{j=1}^{N} q_{ij}\,\mathrm{Log}\,q_{ij}}{\sigma_w} \qquad (۳)$$

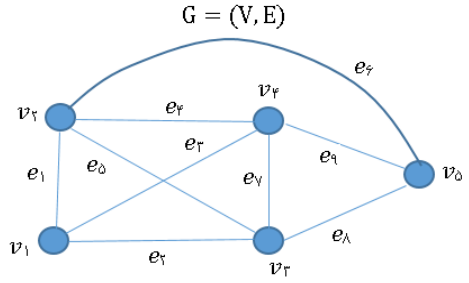
که در این صورت، رابطه مقادیر عددی آنتروپی محاسبه شده و نوسانات و تغییرات پیکسل‌ها برعکس می‌شود. یعنی مقدار عددی بزرگ‌تر آنتروپی نشان‌دهنده نوسانات و اعوجاج کم‌تر و مقادیر عددی کم‌تر، گواه تغییرات و اعوجاج بیش‌تردر تصویر خواهد بود. این بحث نشان می‌دهد که آنتروپی می‌تواند ملاک و معیار مناسبی برای شناسایی تصاویر زبر و پرنوسان از تصاویر صاف و هموار است. بنابراین برای به‌کارگیری آنتروپی در نهان‌نگاری سعی کرده به آنتروپی محلی رسیده و چالش‌ها و موانع موجود را شناسایی و برطرف کنیم. لذا در بخش بعد، ابتدا نحوه نگاشت یک پنجره از تصویر در یک گراف را بیان کرده سپس با استفاده از آنتروپی گراف، معیار دقیق‌تری جهت شناسایی

1- Crandall
2- Westfeld
3- Hayat-Aldamour
4- Flatness
5- High Texture

پنجره‌های زبر تصویر، برای جاسازی پیام در نهان‌نگاری، طراحی می‌شود.

۳-۲- گراف و آنتروپی

یک گراف از زوج $G=(E,V)$ تشکیل می‌شود که در آن، $V=\{v_1,v_2,\dots,v_n\}$ به مجموعه رئوس گراف و E، که زیرمجموعه‌ای از تمام دو عضوی‌ها در V است، به مجموعه یال‌های گراف G معروف است [۱۶-۱۵]. در این تعریف، اگر ترتیب مهم باشد گراف مورد نظر را جهت‌دار و در غیر این صورت، بدون جهت می‌گویند. هم‌چنین اگر به هر راس گراف عددی نسبت دهیم گراف را وزن‌دار گویند. شکل(۱) نمونه‌ای از یک گراف وزن‌دار را نشان می‌دهد.



شکل (۱): نمونه‌ای از یک گراف بدون جهت وزن‌دار

راشیوسکی[1] [۱۷]، تراکو[2] [۱۸]، موشوویتز[3] [۲۲-۱۹]، اولین محققان در زمینه آنتروپی گراف بودند. پس از تحقیقات پایه‌ای این افراد، کرنر[4] یک تعریف متفاوت از آنتروپی گراف تحت عنوان آنتروپی کرنر [۲۳] ارائه داد که به کدینگ و نظریه اطلاعات نزدیک است. هدف این مقاله، رسیدن به فرمول محاسبه آنتروپی گراف متناظر تصویر در نهان‌نگاری تطبیقی است. به‌طورکلی، مطرح‌کردن آنتروپی در نظریه گراف، یکی از روش‌های عمده و اصلی برای اندازه‌گیری پیچیدگی ساختارهای ریاضی در شاخه‌های مختلف علوم است. این روش‌ها خود به دو دسته کلی آنتروپی قطعی[5] و احتمالی[6] تقسیم می‌شوند. معیارهای احتمالی که موضوع بحث ما است با توجه به ویژگی‌های ساختاری گراف طراحی می‌شوند. مقادیر عددی این معیارها توسط یک تابع آنتروپی با یک توزیع احتمال به‌دست می‌آیند. انواع معیار محاسبه پیچیدگی احتمالی، در روش تعیین توزیع احتمال متفاوت هستند. اولین معیار پیچیدگی گراف که در بیش‌تر منابع به چشم می‌خورد، براساس یک معیار داخلی، مطابق خاصیت تشابه در گراف است [۲۴]. این معیار پیچیدگی با "میزان اطلاعات" طبق آنتروپی احتمالی متناهی شانون، متناظر با گراف برابر گرفته می‌شود. در حالت کلی، چنین معیارهای کلاسیکی برای گراف G به‌صورت زیر تعریف می‌شود:

$$H(G,\tau)=-\sum_i \frac{|X_i|}{|X|}\ \mathrm{Log}\left(\frac{|X_i|}{|X|}\right) \qquad (۴)$$

که در آن، G یک گراف ثابت دلخواه، τ معیاری برای استخراج کلاس‌های معادل X_i و مقدار $\frac{|X_i|}{|X|}$ می‌تواند به‌عنوان احتمالی برای کلاس X_i تعبیر شود. هم‌چنین با درنظر گرفتن گراف G برای رأس دلخواه $v_i \in V$ می‌توانیم تعریف کنیم: $p(v_i)=\frac{f(v_i)}{\sum_j f(v_j)}$ که در آن، f نشان‌دهنده یک تابع اطلاعاتی از وضعیت ساختاری در گراف G است و با توجه به این‌که $\sum_{i=1}^{n} p(v_i)=1$ می‌توانیم $P(v_i)$ را به‌عنوان احتمال رأسی v_i تعبیر کنیم که در این صورت یک آنتروپی وابسته به تابع اطلاعاتی f برای گراف G به‌صورت زیر قابل تعریف خواهد بود:

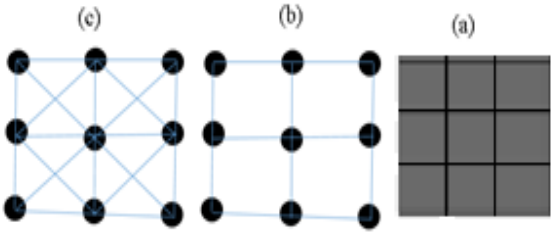
$$H_f=-\sum_{j=1}^{n}\frac{f(v_j)}{\sum_{i=1}^{n} f(v_i)}\ \mathrm{Log}\left(\frac{f(v_j)}{\sum_{i=1}^{n} f(v_i)}\right) \qquad (۵)$$

معیارهای آنتروپی فوق، برای توصیف یک گراف با تعیین محتوای اطلاعاتی‌شان، در حالت کلی بیان شدند. که هریک معیاری براساس ویژگی‌های محلی و زیربنایی هستند.

۳-۳- طراحی معیار شناسایی پنجره زبر با استفاده از آنتروپی گراف

به‌منظور به‌کارگیری مفاهیم نظریه گراف در نهان‌نگاری تصویر، ابتدا تصویر باید در یک گراف نگاشته شود. این نگاشت، هر پیکسل تصویر را به یک رأس گراف به‌صورت یک رابطه یک‌به‌یک می‌نگارد. متناظر هر پیکسل در تصویر، یک رأس در گراف داریم. هم‌چنین، رابطه مجاورت پیکسل‌ها در تصویر نیز به‌طور مشابه به‌صورت ۴- همسایگی یا ۸- همسایگی در گراف نگاشته می‌شود. در شکل (۲)، (a) یک پنجره ۳×۳ متشکل از پیکسل‌های یک تصویر، (b) گراف متناظر با ۴- همسایگی و (c) گراف متناظر با ۸- همسایگی آن پنجره از تصویر است. در این تناظر یک‌به‌یک بین یک پنجره از تصویر و یک گراف بدون جهت، متناظر پیکسل‌های p_i و p_j در تصویر، رئوس v_i و v_j در گراف را داریم. برای دو رأس v_i و v_j در گراف، یک یال (i,j) را داریم که رابط دو رأس است. اگر به هر یال این گراف یک عدد مانند $|v_i-v_j|$ اختصاص داده شود، گراف وزن‌دار خواهد شد.

1- Rashevsky
2- Trucco
3- Mowshowitz
4- Körner
5- Deterministic
6- Probability



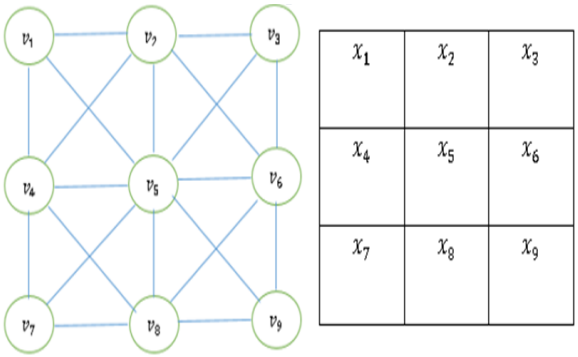
شکل (۲): (a) یک پنجره ۴×۴ از یک تصویر (b) گراف متناظر با ۴-همسایگی (C) گراف متناظر ۸-همسایگی

لذا در راستای هدفمان در این مقاله فرض می‌کنیم d یک متریک در مجموعه اعداد حقیقی نامنفی باشد و D یک زیر گراف k راسی از گراف G با رئوس $V=\{v_1,v_2,\dots,v_n\}$ باشد، با نشان‌دادن آنتروپی این زیرگراف نسبت به رأس v_i با $H_D(v_i)$ (آنتروپی محلی D نسبت به رأس v_i) می‌توان تعریف کرد:

$$H_D(v_i)=-\sum_{j=1}^{k}\frac{d(v_i,v_j)}{d(v_i)}\,Log\left(\frac{d(v_i,v_j)}{d(v_i)}\right) \qquad (۶)$$

که در آن، $d(v_i,v_j)$ می‌تواند کوتاه‌ترین فاصله رئوس v_i و v_j بوده و $d(v_i)=\sum_j d(v_i,v_j)$ باشد. واضح است که در این تعریف با قراردادن $i,j=1,\dots,k$ ، $p(v_j)=\frac{d(v_i,v_j)}{d(v_i)}$ داریم: $p(v_j)\geq 0$ و $\sum_j p(v_j)=1$ که نشان از صحت تعریف آنتروپی دارد. برای فهم شهودی موضوع می‌توان این روابط را با شکل (۲) تطبیق داد. در این شکل متناظر پیکسل x_i راس v_i را داشته و گراف متناظر با درنظر گرفتن ۸- همسایگی تعیین شد.

همان‌طوری‌که قبلاً اشاره شد، بررسی مطلوبیت ناحیه مورد نظر از تصویر از لحاظ زبری شرط اصلی جاسازی پیام در نهان‌نگاری تطبیقی است. برای به‌دست‌آوردن معیار تعیین زبری به‌طور بهینه فرض می‌کنیم $I=[I_{ij}]$ یک تصویر و G گراف متناظر باشد. یک پنجره ۳×۳ از تصویر I و گراف ۸- همسایگی متناظر آن را مطابق شکل (۳) در نظر می‌گیریم.



شکل (۳): یک پنجره ۳×۳ از تصویر و گراف ۸- همسایگی متناظر آن

طبق روابط تعریف‌شده در (۶) به یک معیار عددی مشخص برای یک پنجره محلی از تصویر می‌رسیم. برای این‌کار دو حالت درنظر می‌گیریم.

در حالت اول، با تعریف $f(v_i)=v_i$ و $\sum_j f(v_j)=\sum_j v_j$ بنابر رابطه (۵) برای زیرگراف D از G خواهیم داشت:

$$H_1(D)=-\sum_i\frac{v_i}{\sum_j v_j}\,Log\left(\frac{v_i}{\sum_j v_j}\right) \qquad (۷)$$

یعنی آنتروپی زیرگراف D برحسب مقدار رئوس زیرگراف محاسبه می‌شود (شدت روشنایی پیکسل‌های تصویر) که می‌تواند یکی از ویژگی‌های ساختاری در هر گراف باشد. واضح است که این رابطه همان فرمول معمول برای محاسبه آنتروپی در پردازش تصویر و نظریه اطلاعات، یعنی رابطه (۱) است که تأثیر شدت روشنایی هر پیکسل در پیکسل‌های همسایه برای محاسبه آنتروپی مورد توجه قرار نمی‌گیرد.

در حالت دوم، با توجه به این‌که هر پیکسل از لحاظ آنتروپی به معنی پیش‌بینی‌ناپذیری و درنتیجه عدم قطعیت و پیچیدگی در همه هشت همسایه خودش تأثیرگذار است. بنابر رابطه (۶) برای زیرگراف D از G، برای هر رأس v_j با قراردادن $d(v_i,v_j)=|v_i-v_j|$ به‌عنوان وزنی برای یال متناظر در این گراف و $d(v_j)=\sum_{(v_i,v_j)}|v_i-v_j|$ ، $i\neq j$ خواهیم داشت:

$$H_2(D)=-\sum_{(v_i,v_j)}\frac{|v_i-v_j|}{\sum_{(v_i,v_j)}|v_i-v_j|}\,Log\left(\frac{|v_i-v_j|}{\sum_{(v_i,v_j)}|v_i-v_j|}\right) \qquad (۸)$$

به‌این‌ترتیب، برای هر رأس گراف و درنتیجه هر پیکسل، با توجه به همه هشت همسایه‌اش به محاسبه آنتروپی اقدام می‌کنیم. این بدین معنی است که در واقع متناظر هر پنجره ۳×۳ در تصویر، یک گراف وزن‌دار موجود است که در آن وزن یال (i,j) برابر $|v_i-v_j|$ است که آنتروپی متناظر آن رأس در پنجره مورد نظر (D) مطابق رابطه (۸) قابل محاسبه است. درنتیجه تاکنون دو معیار رابطه‌های (۸-۷) برای محاسبه آنتروپی یک پنجره از تصویر ارائه شد که برای مقایسه آن‌ها اقدام می‌کنیم. در ادامه، به‌صورت عملی هم ملاحظه خواهیم کرد که معیار جدید یعنی فرمول (۸) نتایج بهتری از فرمول (۷)، یعنی فرمول معمول محاسبه آنتروپی در پردازش تصویر و نظریه اطلاعات، خواهد داشت. اما برای تکمیل‌تر کردن دو فرمول (۸-۷) دو تصویر زیر را در نظر می‌گیریم:

$$D_1=\begin{bmatrix}1&2&3\\4&5&6\\7&8&9\end{bmatrix},D_2=\begin{bmatrix}10&20&30\\40&50&60\\70&80&90\end{bmatrix}$$

با به‌کارگیری روابط (۸-۷) روی دو زیرگراف، در حالت اول $H_1(D_1)=H_1(D_2)=$ ۲/۲۷۶۵۹ و در حالت دوم ۴/۲۹۱۰۵ $=H_2(D_1)=H_2(D_2)$ به‌دست خواهد آمد که با توجه به برابری

آن‌ها در هر مورد یک محدودیت خواهیم داشت. به‌دلیل این‌که در D_2 دامنه تغییرات دنباله اعداد به‌کاررفته ۱۰ برابر شد، ولی آنتروپی محاسبه‌شده یکسان به‌دست آمده است. لذا برای رفع محدودیت گفته‌شده و نظر به این‌که آنتروپی در تصویر با واریانس و انحراف معیار شدت روشنایی پیکسل‌ها رابطه عکس دارد، با محاسبه انحراف معیارها به‌صورت: $\sigma_v = \mathrm{Stdev}(v_1, v_2, \dots, v_9)$ و $\sigma_v^* = \mathrm{Stdev}(\{|v_i - v_j|, \forall i \neq j\})$، هر دو فرمول را بر انحراف معیارشان تقسیم می‌کنیم. یعنی:

$$H_1^*(D) = \frac{H_1(D)}{\sigma_v} \quad (۹)$$

$$H_2^*(D) = \frac{H_2(D)}{\sigma_v^*} \quad (۱۰)$$

جدول (۱): محاسبه آنتروپی چند زیرگراف متناظر یک تصویر در دو حالت

ردیف	داده	H_1^*	H_2^*
۱	۱,۲,۳,۴	۱/۴۳۰۲۵	۲/۹۹۶۲۶
۲	۳۱ , ۳۲ , ۳۳ , ۳۴	۱/۵۴۸۵۳	۲/۹۹۶۲۶
۳	۸۰ , ۸۱ , ۸۲ , ۸۳	۱/۵۴۹۰۹	۲/۹۹۶۲۶
۴	۱۰,۲۰,۳۰,۴۰	۰/۱۴۳۰۲	۰/۲۹۹۶۳
۵	۵۰,۶۰,۷۰,۸۰	۰/۱۵۳۲۵	۰/۲۹۹۶۳
۶	۴۰, ۵ , ۶ , ۷	۰/۰۸۱۱۶	۰/۱۰۱۲۵
۷	۵۰ , ۱۵ , ۱۶ , ۱۷	۰/۱۰۴۳۰	۰/۱۰۱۲۵
۸	۱,۲,...,۹	۱/۱۷۹۸۵	۳/۶۳۸۸۱
۹	۱۱,۱۲,...,۱۹	۱/۱۴۹۶۲	۳/۶۳۸۸۱
۱۰	۱۰۱,۱۰۲, ... ,۱۰۹	۱/۱۵۷۳۳	۳/۶۳۸۸۱

حال برای نتیجه‌گیری بهتر و مقایسه‌ی آن‌ها، چند زیرگراف محلی متناظر یک تصویر را درنظر گرفته و نتایج را در جدول (۱) نشان می‌دهیم.

با توجه به داده‌های ثبت‌شده در جدول(۱) می‌توان نتیجه گرفت که:

۱) در ردیف‌های ۱، ۲ و ۳ مقادیر H_1^* متفاوت ولی مقادیر H_2^* ثابت است. درحالی‌که تغییرات داده ثابت است.

۲) در ردیف‌های ۴ و ۵ مقادیر H_1^* متفاوت ولی مقادیر H_2^* ثابت است درحالی‌که تغییرات داده ثابت است.

۳) در ردیف‌های ۶ و۷ مقادیر H_1^* متفاوت است ولی مقادیر H_2^* ثابت است. درحالی‌که تغییرات داده ثابت است.

۴) در ردیف‌های ۸، ۹ و ۱۰ هم نتیجه مشابهی برای یک پنجره ۳×۳ داریم. به‌این‌ترتیب که مقادیر H_1^* هر ردیف با ردیف دیگر متفاوت است، ولی مقادیر H_2^* برای هر سه ردیف یکسان است. لذا، این نتایج قابل اعتمادتربودن فرمول پیشنهادی این مقاله، یعنی (۱۰) در مقایسه با فرمول (۹) را نشان می‌دهد که قبل از این برای تعیین زبری محلی در تصویر به‌کار گرفته می‌شد.

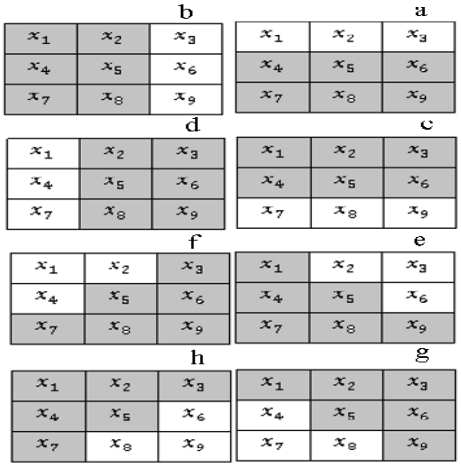
۳-۴- تعیین آستانه زبری

با توجه به مباحث گذشته، اگر در یک تصویر کامل $M \times N$ از گوشه چپ بالا تمامی پنجره‌های ناهمپوشان را استخراج کرده، گراف ۸- همسایگی هر یک را درنظر گرفته مطابق فرمول (۱۰) آنتروپی هریک را محاسبه کنیم، پنجره‌هایی که دارای آنتروپی متناظر صفر باشند پنجره‌های صاف و یکنواخت تصویر هستند که در نهان‌نگاری، قابل استفاده نیستند. با درنظر گرفتن گراف متناظر هر پنجره، مطابق شکل (۲)، به محاسبه آنتروپی محلی آن طبق فرمول (۱۰) می‌پردازیم. در این محاسبه، مقادیر صفر را که نشان‌دهنده پنجره‌های صاف هستند، حذف کرده و بقیه را تا k رقم اعشار گرد نموده و در آرایه‌ای چون $h_2^*[i], i = 1,2,\dots,l$ ذخیره می‌کنیم. سپس، آرایه را به‌صورت صعودی مرتب می‌کنیم. نکته قابل توجه این است که پنجره‌های زبرتر دارای آنتروپی محلی کم‌تری هستند که هنگام جاسازی پیام باید در اولویت قرار گیرند. لذا برای جاسازی پیام M با طول $|M|$ لازم است آستانه‌ای $T_1 > 0$ را طوری به‌دست آورد که تعداد پنجره‌های زبر شمارش‌شده به ازای آن مقدار T_1 یعنی N_w، ظرفیت لازم برای جاسازی آن پیام را داشته باشد. لذا T_1 را طوری تعیین می‌کنیم که $N_w \times K \geq |M|$ باشد که K تعداد بیت‌های پیامی است که بسته به روش جاسازی پیام، می‌توان در یک پنجره زبر جاسازی کرد. بنابراین، پنجره‌هایی با آنتروپی موجود دربازه $[0, T_1]$ قالب یا پنجره زبر نامیده می‌شوند و برای جاسازی بیت‌های پیام درنظر گرفته می‌شوند. اما تعیین T_1 به طول پیام و تعداد بیت‌های پیامی که در هر پنجره زبر می‌توان جاسازی کرد، بستگی دارد. یعنی این روش T_1 را طوری پیدا می‌کند که بیت‌های پیام بتوانند در سراسر تصویر پخش شوند و به‌عبارتی از کل ظرفیت تصویر برای جاسازی پیام استفاده می‌شود.

۳-۵- شناسایی پیکسل‌های لبه در پنجره‌های زبر

تاکنون ملاحظه شد که نواحی مختلف تصویر را می‌توان به دو بخش " زبر" و "صاف و یکنواخت" تقسیم کرد. نواحی زبر در واقع نواحی دارای نویز و لبه بیشتر هستند که دارای نوسانات و تغییرات بیش‌تری هستند. این موضوع می‌تواند در هر پنجره از تصویر،

ازجمله پنجره‌های ۳×۳، ملاک عمل قرار گیرد. در بخش قبل، معیاری برای شناسایی پنجره‌های "زبر" ارائه شد (وجود آنتروپی در بازه $0 < h_2^* \le T_1$ که آستانه T_1 با توجه به طول پیام تعیین می‌شود) اما برای جاسازی امن‌تر در پیکسل‌ها، شناسایی پیکسل‌های برجسته‌تر همواره مورد توجه محققان بوده است. هر پنجره زبر با پیکسل‌های $B = \{x_1, x_2, \dots, x_9\}$ را می‌توان به دو دسته پیکسل‌های لبه، زیرمجموعه B_1 و پیکسل‌های غیرلبه، زیرمجموعه B_2، تقسیم کرد. خواص پیکسل‌های دسته اول عبارتند از: ۱) از نظر تعداد در اقلیت هستند. ۲) قدر مطلق تفاضل این دسته از پیکسل‌ها با پیکسل‌های هم‌نوع ناچیز و با پیکسل‌های غیرهم‌نوع قابل توجه‌تر است. ۳) این پیکسل‌ها حداقل با یکی از پیکسل‌های همسایه، غیرهم‌نوع هستند. اما ویژگی‌های پیکسل‌های دسته دوم، یعنی پیکسل‌های صاف و یکنواخت، عبارتند از: ۱) مهم‌ترین ویژگی و وجه تمایز آن‌ها این است که این پیکسل‌ها از لحاظ تعداد در هر تصویر و یا در هرپنجره در اکثریت هستند. ۲) قدر مطلق تفاضل این دسته از پیکسل‌ها با پیکسل‌های هم‌نوع خود ناچیز و با پیکسل‌های غیرهم‌نوع نسبتاً زیاد است. ۳) این پیکسل‌ها نیز ممکن است با همه پیکسل‌های همسایه خود مشابه باشند. یعنی اگر پیکسلی با همه پیکسل‌های همسایه هم‌نوع باشد، جزو پیکسل‌های صاف است. بنابراین، هر پیکسل در هر پنجره زبر را می‌توان متعلق به یکی از دسته‌های فوق دانست. پیکسل‌های لبه، مطابق شکل (۴)، دارای یکی از هشت جهت نشان داده شده هستند.



شکل (۴): نمایش جهت‌های مختلف لبه در یک پنجره ۳×۳ از تصویر

برای شناسایی پیکسل‌های لبه در هر پنجره زبر، کافی است پیکسل‌های غیرلبه یعنی مجموعه B_2 را شناسایی کنیم. جهت این‌کار برای این پیکسل‌ها عدد تشابه، $|B_2|$، را به‌صورت زیر تعریف می‌کنیم:

$$|B_2| = |\{ x \mid \exists\, y \in B_2 \,;\, |x - y| \le T_2\}| \qquad (۱۱)$$

که در آن، T_2 یک آستانه از پیش تعریف شده است. اگر $|B_2| \ge ۶$ آن‌گاه B_1 شامل ۰، ۱، ۲ یا ۳ پیکسل لبه است. بنابراین، با توجه به مکان پیکسل‌های لبه، متناظر تصویر اصلی I، تصویر لبه L و تصویر نهانه I' را تشکیل می‌دهیم. ناگفته نماند که استفاده از مجموعه B_2 برای شناسایی پیکسل‌های لبه، تضمین‌کننده لبه‌های یکسان در پوشانه و نهانه تصویری است که با تغییر پوشانه به‌دست می‌آید. درحالی‌که بسیاری از الگوریتم‌های نهان‌نگاری، به‌خصوص آن‌هایی که مبتنی بر لبه‌یابی معمولی باشند، دارای این ویژگی نیستند. شکل (۵) تصویر سبد میوه و نواحی زبر و لبه استخراج‌شده از آن‌را توسط الگوریتم پیشنهادی، با انتخاب آستانه زبری $T_1 = 1$ و آستانه شناسایی لبه $T_2 = 5$ نشان می‌دهد.

شکل (۵): (a) تصویر میوه و (b) استخراج لبه آن توسط الگوریتم پیشنهادی

۴- روش نهان‌نگاری تطبیقی پیشنهادی

همان‌طوری‌که قبلاً اشاره شد، سیستم بینایی انسان نسبت به تغییرات در نواحی لبه‌دار و نویزدار، معروف به نواحی زبر، در مقایسه با نواحی نرم و صاف حساسیت کم‌تری دارد. بنابراین، منطقی است که پیام را در نواحی زبر پنهان کنیم. تصویر لبه تولیدشده توسط روش‌های تشخیص لبه معمولی معمولاً نسبت به تغییرات در تصاویر خاکستری، حتی تغییرات کوچک، حساس می‌باشند. این ویژگی، کاربرد روش‌های تشخیص لبه معمولی را در پنهان‌سازی پیام محدود می‌سازد، چرا که پنهان‌سازی پیام، تغییراتی بر تصویر اصلی اعمال خواهد کرد. بنابراین، جاسازی در پیکسل‌های شناسایی‌شده توسط روش‌های تشخیص لبه معمولی، همانند سوبل[1] یا کنی[2]، شناسایی دقیق لبه را برای تصاویر پوشانه و نهانه در قبل و بعد از نهان‌نگاری تضمین نمی‌کند. در این مقاله الگوریتم نهان‌نگاری تطبیقی نوینی با استفاده از معیار طراحی‌شده با کمک آنتروپی در گراف، جهت کشف و شناسایی

1- Sobel
2- Canny

پنجره‌های زبر و پیکسل‌های لبه در آن‌ها، با ویژگی‌های زیر پیشنهاد می‌شود. در این روش کلیه پیکسل‌های هرپنجره در همه جهت‌های افقی و عمودی در محاسبه معیار زبری دخالت دارند. این موضوع تضمین‌کننده دقت روش است. دوم آن‌که میزان زبری ناحیه، برای بالابردن رؤیت‌ناپذیری و سطح امنیت روش، با اندازه دلخواه و بر طبق طول پیام قابل تعیین است. سوم آن‌که این روش با دقت بالایی که دارد، نواحی صاف را به‌طور دقیق شناسایی می‌کند. لذا، به هیچ وجه اجازه جاسازی پیام در آن‌ها را نمی‌دهد.

۴-۱- الگوریتم پیشنهادی

ورودی‌ها: تصویر پوششی I با ابعاد $H \times W$ و پیام محرمانه M.
خروجی: تصویر نهانه I' با ابعاد $H \times W$ و آستانه استخراج پیام از آن یعنی T_1'.

گام ۱) تقسیم پوشانه تصویری به پنجره‌های نا هم‌پوشان

در این گام تصویر را به‌صورت پنجره‌های ناهم‌پوشان ۳×۳ تقسیم کرده و مطابق شکل (۲) برای هر پنجره یک گراف ۸- همسایگی برای محاسبه آنتروپی، یعنی معیار زبری درنظر می‌گیریم.

گام ۲) محاسبه آنتروپی هر پنجره یا قالب

با درنظر گرفتن گراف متناظر هر پنجره، مطابق شکل (۲)، به محاسبه آنتروپی محلی آن طبق فرمول (۱۰) می‌پردازیم. در این محاسبه، مقادیر صفر را که نشان‌دهنده پنجره‌های صاف هستند، حذف کرده و بقیه را تا k رقم اعشار گرد نموده و در ارائه $h^*[i], i = 1,2, \dots, l$ ذخیره کرده و سپس، ارائه را به‌صورت صعودی مرتب می‌کنیم. نکته قابل توجه این است که پنجره‌های شامل پنجره‌های زبرتر دارای آنتروپی محلی کوچک‌تری هستند.

گام ۳) محاسبه آستانه زبری پنجره‌ها

با توجه به این‌که آرایه $h^*[i]$ شامل آنتروپی کلیه پیکسل پنجره‌های ناصاف تصویر مورد نظر با ترتیب صعودی است و مقادیر کم‌تر در آن نشان‌دهنده پیکسل پنجره‌های زبرتر است، با توجه به طول پیام M، آستانه زبری $0 < T_1 \le h^*[l]$ را طوری انتخاب می‌کنیم که $N_w \times K \ge |M|$ باشد و K تعداد بیت‌های پیامی است که بسته به روش جاسازی پیام، می‌توان در هر پنجره زبر جاسازی کرد (در این‌جا $K = 3$ است). پس از محاسبه T_1 گام‌های ۴ و ۵ را تا پایان جاسازی کلیه بیت‌های پیام M تکرار می‌کنیم.

گام۴) شناسایی پیکسل‌های لبه در هر پنجره زبر

برای شناسایی پیکسل‌های لبه، جهت جاسازی پیام، در هر پنجره زبر B، کافی است پیکسل‌های غیرلبه یعنی مجموعه B_2 را در هر پنجره زبر شناسایی کنیم. جهت این‌کار برای این پیکسل‌ها عدد تشابه یعنی $|B_2|$ را با درنظر گرفتن آستانه از پیش تعیین‌شده و دلخواه T_2 از رابطه زیر به‌دست می‌آوریم:

$$|B_2| = |\{ x \mid \exists\, y \in B_2 ; |x - y| \le T_2\}| \qquad (۱۲)$$

اگر $|B_2| = 6$ آن‌گاه B_1 شامل سه پیکسل لبه، مطابق یکی از جهت‌های نشان داده شده در شکل (۳) است. بنابراین، با توجه به مکان سه پیکسل لبه، دو بیت پیام m_1 و m_2 را در LSB آن سه پیکسل، با استفاده از عمل xor و روش F5 (گام ۵) جاسازی می‌کنیم.

گام ۵) جاسازی دو بیت پیام m_1 و m_2 در LSB سه پیکسل لبه از یک پنجره زبر

در این مرحله، دو بیت پیام m_1 و m_2 در LSB سه پیکسل لبه از یک پنجره زبر، که آن‌ها را p_1، p_2 و p_3 می‌نامیم، مطابق فرایند زیر جاسازی می‌شود:

۱) دو عمل xor مقابل $k_1 = p_1 \oplus p_2$ و $k_2 = p_2 \oplus p_3$ اجرا می‌شود.

۲) برای جاسازی دو بیت پیام m_1 و m_2 دو بیت محاسبه‌شده k_1 و k_2 با بیت‌های پیام m_1 و m_2 مقایسه می‌شوند. نتایج این مقایسه‌ها می‌تواند یکی از چهار حالت در جدول (۲) باشد.

جدول (۲): شرایط جاسازی

تغییرات	شرط	شرط
بدون تغییر	$m_2 = k_2$	$m_1 = k_1$
تغییر $\mathbf{p_3}$	$m_2 \neq k_2$	$m_1 = k_1$
تغییر $\mathbf{p_1}$	$m_2 = k_2$	$m_1 \neq k_1$
تغییر $\mathbf{p_2}$	$m_2 \neq k_2$	$m_1 \neq k_1$

پس از جاسازی در هر پنجره از تصویر I'، آنتروپی آن پنجره جدید را محاسبه کرده با آنتروپی پنجره زبر اولیه در پوشانه I مقایسه و عدد بیش‌تر را در متغیر T_1' ذخیره می‌کنیم.

گام۶) آستانه شناسایی پنجره‌های زبر در نهانه یعنی T_1' و آستانه شناسایی پیکسل‌های غیرلبه در پنجره‌های نهانه یعنی T_2 و طول پیام جاسازی‌شده $|M|$ را در مکان خاصی از نهانه جاسازی کرده یا از طریق کانال امن به مقصد ارسال می‌کنیم (شکل ۶).

۴- ۲- الگوریتم استخراج پیام

فرآیند استخراج پیام جاسازی‌شده در تصویر نهانه آسان‌تر از فرآیند جاسازی آن در پوشانه هست. شکل (۷) نشان‌دهنده نمودار عملیاتی این فرآیند می‌باشد که با بازیابی مقدار آستانه آغاز می‌گردد.

پنجره‌های زبر تصویر نهانه با استفاده از آستانه زبری، T_1'، بازیابی می‌شوند. سپس، در هر پنجره زبر نهانه با استفاده از آستانه تشخیص پیکسل‌های غیرلبه، T_2، پیکسل‌های لبه را شناسایی می‌کنیم. در ادامه، LSB پیکسل‌های لبه در هرپنجره نهانه را q_1، q_2 و q_3 نامیده و عملیات xor به‌صورت $m_1 = q_1 \oplus q_2$ و $m_2 = q_2 \oplus q_3$ جهت بازیابی دو بیت پیام m_1 و m_2 جاسازی‌شده در هر پنجره زبر به کار می‌رود.

۵- نتایج تجربی و بحث

سه آزمون استاندارد برای ارزیابی روش‌های نهان‌نگاری وجود دارد که یکی از آن‌ها نرخ[1] یا ظرفیت جاسازی[2] (بارجاسازی[3]) است، دومی نرخ تغییر[4] (پیکسل‌ها) یا کارایی جاسازی[5] است و سومی سطح امنیت (آشکارناپذیری) روش نهان‌نگاری می‌باشد. در این بخش، ابتدا تعاریف موارد یادشده را یادآوری کرده سپس نتایج تجربی الگوریتم پیشنهادی خود و چند روش تطبیقی جدید دیگر را با استفاده از متلب R2016b و ۵۰۰۰ تصویر طبیعی در مقیاس خاکستری با ابعاد ۵۱۲×۵۱۲ از پایگاه BOWS2 ارائه می‌دهیم.

جدول (۳): نرخ تغییر و ظرفیت جاسازی پیام مهم‌ترین روش‌های نهان‌نگاری

نام روش	ظرفیت جاسازی	نرخ تغییر	توضیحات
LSB	٪۱۲/۵	bpp ۰/۵	جاسازی یک بیت در یک پیکسل
LSBMR	٪۱۲/۵	bpp ۰/۳۷۵	جاسازی دو بیت در دو پیکسل
EAMR	٪۱۲/۵	bpp ۰/۳۷۵	جاسازی دو بیت در دو پیکسل
F_5	٪۸/۳	bpp ۰/۲۵	جاسازی دو بیت در سه پیکسل
Edge xor Coding	٪۹/۳	bpp ۰/۲۵	جاسازی سه بیت در چهار پیکسل

ظرفیت جاسازی یک معیار مهم برای ارزیابی کارایی روش‌های نهان‌نگاری است که فرمول محاسبه آن عبارت است از:

$$E = \frac{k}{WH}(bpp) \qquad (۱۳)$$

که در آن، k حداکثر تعداد بیت‌های پیام محرمانه است که می‌توان در پوشانه تصویری جاسازی کرد و w و H طول و عرض تصویر می‌باشند. برخی از روش‌های جاسازی پیام، ظرفیت جاسازی ثابتی دارند. به‌عنوان‌مثال ظرفیت جاسازی روش LSB با جاسازی یک بیت در هر پیکسل دارای ظرفیت جاسازی ٪۱۲/۵ است. منظور از نرخ تغییر یک روش جاسازی احتمال تغییر یک پیکسل از پوشانه تصویری به ازای جاسازی یک بیت پیام است. جدول (۳) ظرفیت جاسازی و نرخ تغییر چند روش جاسازی پیام را نشان می‌دهد.

در حالت کلی به‌جزء روش LSB بقیه روش‌ها برای بالابردن امنیت، با دقت در متن پوشانه‌های مختلف و بسته به تصویر، ظرفیت جاسازی متفاوتی دارند. به همین دلیل، مقادیری که در ستون جاسازی ملاحظه می‌شود بدون توجه به متن پوشانه می‌باشد. اما اگر نهان‌نگاری تطبیقی به همراه این روش‌ها اعمال شود، بسته به دقت روش و تصویر این مقادیر متفاوت خواهند بود. بنابراین، برای مقایسه‌ها از میانگین استفاده می‌شود. روش پیشنهادی در این مقاله به‌دلیل این‌که تصویر را به پنجره‌های ناهم‌پوشان ۳×۳ تقسیم می‌کند و برای ارتقای امنیت روش در هر پنجره زبر سه پیکسل لبه را برای جاسازی پیام برمی‌گزیند، لذا از روش جاسازی پیام F_5 استفاده می‌کند.

۵-۱- ارزیابی تخریب ناشی از جاسازی[6]

کیفیت تصویر نهانه با استفاده از نرخ سیگنال به نویز حداکثر (PSNR) برای ارزیابی تفاوت بین تصاویر پوشانه و نهانه مطابق فرمول (۱۶) محاسبه می‌شود.

$$\mathrm{PSNR} = 10\log10\left[\frac{255^2}{\mathrm{MSE}}\right](\mathrm{db}) \qquad (۱۴)$$

MSE میانگین مجموع مربعات خطای بین تصاویر پوشانه و نهانه می‌باشد که به‌صورت زیر است:

$$\mathrm{MSE} = \frac{1}{\mathrm{WH}}\sum_{i=1}^{W}\sum_{j=1}^{H}(C_{ij} - S_{ij})^2 \qquad (۱۵)$$

معیار کیفیت PSNR تخریب ایجادشده در هر تصویر نهانه را بدون درنظر گرفتن سیستم بینایی انسان، HVS، اندازه‌گیری می‌کند. wPSNR مقیاس کیفی دیگری است که در معادله (۱۸) آمده است. این مقیاس از یک پارامتر اضافی به‌نام تابع قابلیت دید نویز[7] (NVF) استفاده می‌کند. البته، wPSNR برای نواحی یکنواخت

1- Rate of Embedding
2- Embedding Capacity
3- Embedding Payload
4- Rate of change
5- Embedding Efficiency

6- Embedding distortion
7- Noise Visibility Function

مانند PSNR است ولی برای نواحی لبه مقادیر بیش‌تری را نشان می‌دهد. در واقع، wPSNR معیار اندازه‌گیری کیفی دقیق‌تری است.

$$\text{wPSNR} = 10\log_{10}\left(\frac{\max(x)^2}{||\text{NVF}(C_S)||^2}\right) \text{ (db)} \qquad (۱۶)$$

$$\text{NVF}(I,j) = \frac{1}{1+\sigma^2_{L_{(i,j)}}} \qquad (۱۷)$$

جدول (۴) کیفیت تصاویر نهانه را با استفاده از الگوریتم پیشنهادی در حوزه مکان با نرخ جاسازی ۵٪ تا ۳۰٪ نشان می‌دهد. ملاحظه می‌شود که روش پیشنهادی به‌همراه روش Edge xor Coding، به‌دلیل استفاده از کدگذاری xor، بهترین کیفیت نهانه را در مقایسه با EAMR به‌دست آورده است.

هم‌چنین با توجه به انتخاب دقیق‌تر پیکسل‌های لبه برای جاسازی پیام، مقادیر wPSNR درروش پیشنهادی تقریباً در همه موارد بهتر از دو روش دیگر است. دلیل این موضوع هم این است که روش پیشنهادی با دقت بالاتری پیکسل‌های لبه در پنجره‌های زبر را برای جاسازی پیام استفاده می‌کند.

۵-۲- ارزیابی امنیت

موضوع امنیت یک هدف اصلی در نهان‌نگاری است. برای ارزیابی امنیتی الگوریتم‌های نهان‌نگاری از حملات مختلف استفاده می‌شود. یکی از این حملات، حمله بصری (بینایی) می‌باشد که در آن سعی می‌شود وجود پیام محرمانه در یک تصویر از طریق دقت در تصویر یا هیستوگرام آن، با چشم غیرمسلح یا رایانه، حدس زده می‌شود. سپس با به‌کارگیری روش‌های خلاقانه یا روش‌های نهان‌کاوی دیگر وجود پیام در تصویر اثبات می‌شود.

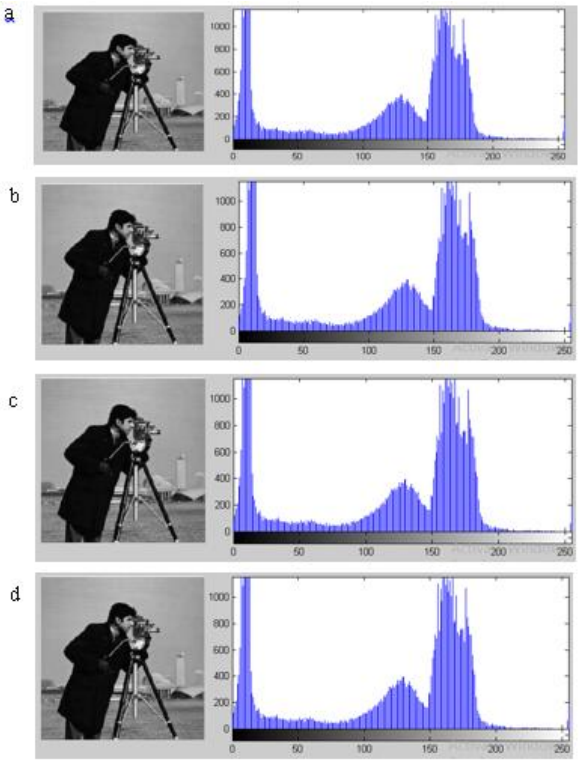
شکل (۸) تصویر پوشانه (a) و نهانه‌های (b-d) منتج از الگوریتم پیشنهادی برای تصویر مرد عکاس با ابعاد ۵۱۲×۵۱۲ و با نرخ‌های جاسازی ۱۰٪، ۲۰٪ و ۳۰٪ را نشان می‌دهد که تفاوت‌های بینایی بین تصاویر پوشانه و نهانه با چشم و حتی با مقایسه هیستوگرام‌های آن‌ها قابل‌تشخیص نیست. روش دیگر ارزیابی امنیتی الگوریتم‌های نهان‌نگاری با استفاده از الگوریتم‌های نهان‌کاوی است. این الگوریتم‌ها خود به دو دسته معین[1] یا اختصاصی و کور[2] یا جامع تقسیم می‌شوند. دسته اول مختص الگوریتم‌های نهان‌نگاری معین طراحی می‌شوند ولی دسته دوم که معمولاً مبتنی بر آماره‌های مراتب بالاتر و استخراج انواع ویژگی‌های آماری هستند، برای تشخیص جاسازی اکثر روش‌های نهان‌نگاری در حوزه مربوطه (مکان یا فرکانس) با الگوریتم نامشخص به‌کار می‌روند. اجرای هر الگوریتم نهان‌کاوی شامل دو مرحله آموزش[3] و آزمون[4] می‌باشد. به این ترتیب که ابتدا بردارهای ویژگی پوشانه‌ها و نهان‌های موجود توسط یک استخراج‌کننده ویژگی، استخراج شده سپس ویژگی‌های استخراج شده در مرحله آموزش، به یک طبقه‌بندی‌کننده، آموزش داده می‌شود. سرانجام توسط یک طبقه‌بندی‌کننده آموزش‌دیده، در مرحله آزمون به تفکیک پوشانه از نهانه اقدام می‌شود.

جدول (۴): مقایسه روش پیشنهادی با دو روش دیگر نهان‌نگاری ازلحاظ ارزیابی کیفی تصاویر نهانه به‌دست‌آمده از ۵۰۰۰ تصویر پوشانه

نرخ جاسازی(٪)	روش	میانگین MSE	میانگین PSNR	میانگین wPSNR	میانگین نرخ تغییر
۵	EAMR	۰/۰۳۷۵	۶۴/۴۱	۶۳/۱۱	۰/۰۳۷۱
	Edge xor Coding	۰/۰۲۹۶	۶۶/۲۱	۶۷/۱۳	۰/۰۲۵۲
	روش پیشنهادی	۰/۰۲۷۲	۶۳/۱۲	۶۹/۷۷	۰/۰۲۵۵
۱۰	EAMR	۰/۰۵۳۱	۶۲/۳۵	۶۰/۳۳	۰/۰۳۷۶
	Edge xor Coding	۰/۰۴۹۵	۶۱/۹۱	۶۵/۷۸	۰/۰۲۴۴
	روش پیشنهادی	۰/۰۴۷۹	۶۱/۵۵	۶۷/۳۱	۰/۰۲۳۵
۱۵	EAMR	۰/۰۹۸۵	۵۸/۱۷	۵۹/۷۵	۰/۰۳۶۸
	Edge xor Coding	۰/۰۸۵۵	۵۹/۱۳	۶۱/۳۲	۰/۰۲۵۶
	روش پیشنهادی	۰/۰۸۴۸	۵۹/۷۸	۶۳/۲۴	۰/۰۲۵۷
۲۰	EAMR	۰/۱۱۴۲	۵۵/۴۵	۵۷/۴۴	۰/۰۳۸۰
	Edge xor Coding	۰/۱۱۱۹	۵۷/۱۸	۶۰/۵۶	۰/۰۲۶۶
	روش پیشنهادی	۰/۱۱۰۸	۵۷/۳۴	۶۳/۴۹	۰/۰۲۶۷
۳۰	EAMR	۰/۱۲۹۵	۵۰/۶۶	۵۳/۲۸	۰/۰۳۸۸
	Edge xor Coding	۰/۱۲۵۵	۵۲/۶۲	۵۵/۸۴	۰/۰۲۸۱
	روش پیشنهادی	۰/۱۲۳۱	۵۳/۱۱	۵۶/۶۴	۰/۰۲۸۰

1- Targeted
2- Blind or Universal

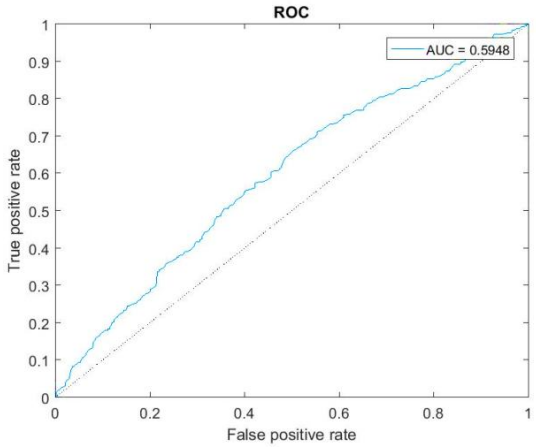
3- Training
4- Test



شکل (۸): (a) تصویر اصلی و هیستوگرام آن، و (b، c و d) تصاویر نهانه و هیستوگرام‌های آن‌ها با نرخ‌های جاسازی ۱۰٪، ۲۰٪ و ۳۰٪

برای ارزیابی الگوریتم نهان‌نگاری پیشنهادی از نرم‌افزار نهان‌کاوی SRM[1] و طبقه‌بندی‌کننده Ensemble Classifier استفاده می‌کنیم که در [۲۶] در دسترس همگان است. چهار رخداد متفاوتی که در هنگام طبقه‌بندی پوشانه و نهانه رخ می‌دهند به یکدیگر وابسته بوده و بر هم تأثیر متقابل دارند. برای فهم بهتر و مقایسه ارزیابی همه‌جانبه عملکرد حمله نهان‌کاوی‌مان از یک منحنی مشخصه عملکرد گیرنده[2] معروف به منحنی ROC،که نشان‌دهنده تغییرات نرخ تشخیص مثبت نادرست f_p در مقابل نرخ تشخیص مثبت درست t_p است، استفاده می‌شود [۲-۱]. به‌عنوان نمونه نتیجه یکی از آزمون‌ها با یک منحنی ROC مطابق شکل (۹) به نمایش گذاشته شده است. بقیه نتایج برای ۵۰۰۰ تصویر، مطابق نرخ جاسازی، براساس سطح زیرمنحنی هر یک معروف به AUC[3] در جدول (۵) به نمایش درآمده است. مساحت زیرمنحنی ROC یا AUC همان احتمال تشخیص درست[4] (P_{detect}) است [۲۵] که با استفاده از رابطه (۱۸) قابل محاسبه است.

1- Spatial Rich Model
2- Receiver Operating Characteristic Curve
3- Area Under Curve
4- Detection Accuracy



شکل (۹): منحنی ROC ناشی از ارزیابی پیاده‌سازی الگوریتم پیشنهادی برای ۵۰۰۰ تصویر با نرخ جاسازی ۲۰٪ از پایگاه داده BOWS2 با استفاده از روش نهان‌کاوی SRM و طبقه‌بندی‌کننده Ensemble Classifier

$$P_{detect} = 1 - P_{error} \quad (۱۸)$$

$$P_{error} = \frac{1}{2} \times P_{FP} + \frac{1}{2} \times P_{FN} \quad (۱۹)$$

که در آن، P_{FP} و P_{FN} به‌ترتیب برابر احتمال تشخیص مثبت نادرست و احتمال تشخیص منفی نادرست است. مقدار $P_{detect} = 0/5$ نشان می‌دهد که طبقه‌بندی‌کننده در تشخیص نهانه از پوشانه معادل حدس و گمان و تصادف کامل است. به‌عبارتی، نشان‌دهنده امنیت صددرصدی الگوریتم نهان‌نگاری است. در مقابل $P_{detect} = 1$ نیز نشان‌دهنده این است که طبقه‌بندی‌کننده‌دارای دقت صددرصدی است و الگوریتم نهان‌نگاری هیچ‌گونه امنیتی ندارد. احتمال تشخیص درست P_{detect} یا AUC حاصل از ارزیابی الگوریتم پیشنهادی و دو الگوریتم دیگر توسط الگوریتم نهان‌کاوی SRM در جدول (۵) به نمایش درآمده است.

جدول (۵): مقایسه احتمال تشخیص صحت P_{detect} یا AUC

نرخ جاسازی (٪)	EAMR	Edge xor Coding	الگوریتم پیشنهادی
۵	۰/۵۴۲۱	۰/۵۳۴۴	۰/۵۲۴۸
۱۰	۰/۵۷۶۱	۰/۵۶۶۲	۰/۵۵۵۵
۱۵	۰/۶۰۳۲	۰/۵۹۴۶	۰/۵۸۵۷
۲۰	۰/۶۳۲۸	۰/۶۱۴۴	۰/۵۹۴۸
۳۰	۰/۶۶۲۹	۰/۶۲۴۴	۰/۶۱۴۳

۶- نتیجه‌گیری

در این مقاله یک روش نهان‌نگاری امن تصویر براساس واقعیت مربوط به حساسیت کم‌تر سیستم بینایی انسان نسبت به تغییرات

در مناطق زبر تصویر طراحی گردید. کار اصلی انجام‌شده در الگوریتم پیشنهادی، معرفی معیاری کارآمد با استفاده از آنتروپی گراف متناظر پنجره‌های ناهم‌پوشان تصویر برای شناسایی مناطق زبرتر تصاویر خاکستری است. سپس، یک راه‌کار ابتکاری جهت شناسایی پیکسل‌های لبه واقع‌شده در پنجره‌های زبر ارائه شد، به‌گونه‌ای که در صورت اجرا روی تصویر نهانه یا پوشانه، پیکسل‌های لبه به‌دست‌آمده یکسان است. مهم‌ترین ویژگی‌های الگوریتم طراحی‌شده عبارت است از: ۱) کلیه پیکسل‌های هر پنجره در همه جهت‌های افقی و عمودی در هر پنجره در این معیار دخالت دارند که این موضوع تضمین‌کننده دقت روش است. ۲) میزان زبری ناحیه، جهت بالابردن رؤیت‌ناپذیری و سطح امنیت روش، با اندازه دلخواه و برطبق طول پیام قابل تعیین است، به‌طوری‌که اگر طول پیام کوتاه‌تر باشد، بیت‌های پیام در نواحی زبرتر تصاویر جاسازی خواهند شد. ۳) این روش با دقت بالایی که دارد به‌هیچ‌وجه اجازه جاسازی پیام در پنجره‌های صاف را نمی‌دهد. الگوریتم برای حوزه مکان طراحی شده است که توازن خوبی بین سه معیار ارزیابی یعنی نرخ جاسازی، رؤیت‌ناپذیری و امنیت برقرار نموده است. در پایان با شبیه‌سازی روی پایگاه داده بزرگی شامل ۵۰۰۰ تصویر طبیعی نتایجی به‌دست آمده است که دلیل بر کارآمدی الگوریتم پیشنهادی است. ازلحاظ کیفی حتی برای نرخ جاسازی ۳۰٪ مقدار wPSNR حدود ۵۶ است که مقدار قابل قبولی است. هم‌چنین در ارزیابی توسط الگوریتم نهان‌کاوی SRM روی همین نرخ جاسازی، مقدار AUC برابر ۰/۶۱۴۳ است که نسبت به روش‌های نوین دیگر، به ۰/۵ نزدیک‌تر است. این الگوریتم، بر روی تصاویر خاکستری در حوزه مکان پیاده‌سازی شده است، اما در مطالعات آینده می‌توان آن را در حوزه تبدیل، با ظرفیت بیش‌تر، هزینه محاسباتی کم‌تر و امنیت و مقاومت بیش‌تر تعمیم داد.

۷- مراجع

[1] I. Cox, M. Miller, J. Bloom, J. Fridrich, and T. Kalker, "Digital Watermarking and Steganography," Second edition, Morgan Kaufmann, Burlington, 2007.

[2] R. Bohem, "Advanced Statistical Steganalysis," Springer-Verlag Berlin Heidelberg, 2010.

[3] D. C. Wu and W. H. Tsai, "A steganographic method for images by pixel value differencing," Pattern Recognition Letters, vol. 24, pp. 1613–1626, 2003.

[4] S. Dumitrescu, X. Wu, and Z. Wang, "Detection of LSB steganography via sample pair analysis," IEEE Trans. Signal Process., vol. 51, no. 7, pp. 1995–2007, 2003.

[5] C. H. Yang, C. Y. Weng, S. J. Wang, and H. M. Sun, "Adaptive data hiding in edge areas of images with spatial LSB domain systems," IEEE Trans. Inf., Forensics Security, vol. 3, no. 3, pp. 488–497, 2008.

[6] L. Bin et al, "A Survey on Image Steganography and Steganalysis," Ubiquitous International Journal of Information Hiding and Multimedia Signal Processing, vol. 2, pp. 2073-4212, 2011.

[7] W.-J. Chen, C.-C. Chang, and T. Le, "High payload steganography mechanism using Hybrid edge detector," Expert Systems with applications, vol. 4, pp. 3292–3301, 2010.

[8] J. Mielikainen, "LSB matching revisited," IEEE Signal Processing Letters, vol. 13, no. 5, pp. 285-287, 2006.

[9] W. Luo, F. Huang, and J. Huang, "Edge adaptive image steganography based on LSB matching revisited," IEEE Trans. Inf., Forensics Secur., vol. 5, no. 2, pp. 201-214, 2010.

[10] F. Huang, Y. Zhong, and J. Huang, "Improved Algorithm of Edge Adaptive Image Steganography Based on LSB Matching Revisited Algorithm," Springer-Verlag Berlin Heidelberg, pp. 19-31, 2014.

[11] R. Crandall, "Some Notes on Steganography," Posted on Steganography Mailing List, http://os.inf.tu-dresden.de/~westfeld/crandall.pdf 297, 1998.

[12] A. Westfeld, "High capacity despite better steganalysis (F5 - a steganographic algorithm)," in Proc. 4th Int. Workshop on Information Hiding, Pittsburgh, PA, USA, pp. 289-302, 2001.

[13] H. Al-Dmour and A. Al-Ani, "A steganography embedding method based on edge identification and XOR coding," Expert Systems With Applications, vol. 46, pp. 293-306, 2016.

[14] G. Guanghua, Y. Zhao, and Z. Zhenfeng, "Integrated image representation based natural scene classification," Expert Systems with Applications, vol. 38, pp. 11273-11279, 2011.

[15] K. Thulasiraman and M. N. S. Swamy, "Graphs Theory and Algorithms. Wiley-Interscience," 1992.

[16] F. Malmberg, "Graph Based Method for Interactive Image Segmentation," Digital Comprehensive Summarise of Uppsala Dissertations from the Faculty of science and Technology 813, pp. 51-59, 2011.

[17] N. Rashevsky, "Life, information theory and topology," Bull. Math. Biophys, vol. 17, pp. 229-235, 1955.

[18] E. Trucco, "A note on the information content of graphs," Bulletin of Mathematical Biology," vol. 18, no. 2, pp. 129-135, 1956.

[19] A. Mowshowitz, "Entropy and the complexity of the graphs I," an index of the relative complexity of a graph, Bulletin of Mathematical Biophysics 30, pp. 175-204, 1968.

[20] A. Mowshowitz, "Entropy and the complexity of graphs II: the information content of digraphs and infinite graphs," Bulletin of Mathematical Biophysics 30, pp. 225-240, 1968.

[21] A. Mowshowitz, "Entropy and the complexity of graphs III: graphs with prescribed information content," Bulletin of Mathematical Biophysics 30, pp. 387-414, 1968.

[22] A. Mowshowitz, "Entropy and the complexity of graphs IV: entropy measures and graphical structure," Bulletin of Mathematical Biophysics, vol. 30, pp. 533-546, 1968.

[23] J. Körner, "Coding of an information source having ambiguous alphabet and the entropy of graphs," in: Transactions of the Sixth Prague Conference on Information Theory, pp. 411-425, 1973.

[24] Z. Chen, M. Dehmer, and Y. Shi, "A Note on Distance-based Graph Entropies," Journal of Entropy, vol. 16, pp. 5416-5427, 2014.

[25] K. Solanki, A. Sarkar, and B. S. Manjunath, "YASS: Yet another Steganographic Scheme That Resists Blind Steganalysis," in Proc. 9th Int. Workshop on Information Hiding, Saint Malo, Brittany, pp. 16-31, 2007.

[26] http://dde.binghamton.edu/download/feature_extractors/

Journal Of Electronical & Cyber Defence
Vol. 5, No. 2, 2017, Serial No. 18

Adaptive Image Steganography Based on Graph Entropy with Improved Efficiency and Security

M. A. ShamalizadehBaei*, Z. Norozi, M. Sabzinezhad, M. R. Karami

*Imam Hossein University

(Received: 18/09/2016, Accepted: 03/01/2017)

ABSTRACT

LBlock is a Lightweight block cipher, with a 64-bit block size and 80-bit key length. Biclique attack is a kind of MITM attack that has recently attracted lots of attention. Biclique cryptanalysis often breaks full version of the cipher on which many other existing attacks do not work. In this paper, firstly, asymmetric biclique is introduced, then by using low data complexity algorithm technique (LDC), a biclique attack on full round Lightweight block cipher LBlock is presented. The computation and data complexity of this attack are and, respectively. The data complexity is considerably less than the existing cryptanalytic result. The computational complexity remains the same as the previous ones.

Keywords: Lightweight, LBlock, Meet in the Middle Attack, BicAdaptive Steganography, Entropy of Graph, High Texture Window, Security

* Corresponding Author Email: ma.shamalizade@gmail.com