Downloaded from adst.ir at 14:14 +0330 on Monday February 26th 2018

مجله علمی پژوهشی «علوم و فناوری‌های پدافند نوین»
سال نهم، شماره ۱، بهار ۱۳۹۷؛ ص ۵۰-۳۹

طراحی الگوریتم نهان‌نگاری تطبیقی مبتنی بر آنتروپی و ELSB2

محمدعلی شمع‌علیزاد بایی[۱*]، زین‌العابدین نوروزی[۲]، محمد سبزی نژاد[۳]، محمدرضا کرمی[۴]
۱- دانشجوی دکتری، ۲- استادیار دانشگاه امام حسین (ع) ۳- استادیار، دانشگاه خوارزمی ۴- دانشیار، دانشگاه صنعتی نوشیروانی بابل
(دریافت: ۹۵/۱۱/۲۹، پذیرش: ۹۶/۰۲/۰۶)

چکیده

امنیت، مقاومت و ظرفیت، مهم‌ترین معیارهای ارزیابی در نهان‌نگاری هستند. هدف از امنیت، کاهش احتمال تشخیص وجود پیام در تصویر و هدف از مقاومت، پایداری پیام جاسازی شده در مقابل حذف و تخریب، بر اثر انواع حملات عمد یا غیر عمد، مثل نویز و فیلترینگ است. در این مقاله یک الگوریتم نهان‌نگاری تطبیقی کارآمد در حوزه مکان طراحی می‌شود که قابل استفاده در حوزه فرکانس نیز است. در این الگوریتم، زبری (تغییرات پیکسل‌ها) پنجره‌های ناهم‌پوشان ۳×۳ از تصویر، با استفاده از آنتروپی گراف وزن‌دار متناظر محاسبه می‌شود. آستانه زبری هر پنجره طبق طول پیام و بافت سراسر تصویر محاسبه می‌شود. مخفی سازی پیام در دومین بیت کم‌ارزش ۴ پیکسل از پنجره‌های زبر تصویر با در نظر گرفتن روند تصادفی و عمل xor و با چگالی معین، انجام می‌شود. شبیه‌سازی روی ۵۰۰۰ تصویر طبیعی، علاوه بر بهبود مقاومت، نشان از حدود ۲٪ بهبود امنیت (کاهش احتمال تشخیص)، توسط یکی از الگوریتم‌های معروف نهان‌کاوی، SRM، در مقایسه با چند روش مدرن دیگر دارد.

کلیدواژه‌ها: نهان‌نگاری تطبیقی، آنتروپی تصویر، زبری، امنیت، مقاومت، عملگر Xor.

Designing an Image Steganography Algorithm Based on Entropy and ELSB2

M. A. Shamalizadeh Baei*, Z. Norozi, M. Sabzinezhad, M. R. Karami
Imam Hossein University
(Received: 17/02/2017; Accepted: 26/04/2017)

Abstract

Security, robustness, and capacity are the most important evaluation criteria in steganography. The aim of security is reducing the probability of message detection in an image and the aim of robustness is stabilizing the embedded message against removal and distortion due to intentional and unintentional attacks, such as noise and filtering. In this paper, an efficient adaptive image steganographic algorithm is designed in spatial domain which is also usable in frequency domain. In this algorithm, roughness (pixel changes) of each non-overlapping 3×3 window in the image is calculated using entropy of corresponding weighted graph. Each window threshold roughness is calculated based on length of message and overall image texture. Hiding message is done with specified density in LSB2 of 4 pixels of rough windows of an image by considering xor operator and randomization. Simulation on 5000 natural images and applying a modern steganalytic algorithm, SRM, shows that in comparison with other popular novel method, the proposed method has increased the security (Reducing the probability of message detection) about 2% in addition to robustness improvement.

Keywords: Adaptive Steganography, Entropy of Image, Roughness, Security, Robustness, Xor Operator

*Corresponding Author E-mail: ma.shamalizade@gmail.com

Archive of SID
www.SID.ir

Downloaded from adst.ir at 14:14 +0330 on Monday February 26th 2018

۱. مقدمه

نهان‌نگاری[1] دانش و هنر تبادل اطلاعات پنهان شده در یک رسانه مانند تصویر، صوت یا ویدئو است و هدف از آن پنهان کردن ارتباط، با اختفای پیام در یک رسانه است، به گونه‌ای که کمترین تغییر قابل کشف را در آن رسانه ایجاد نماید و نتوان وجود پیام پنهان در آن را به راحتی تشخیص داد. همچنین، دانش نهان‌کاوی[2] عبارت است از علم و هنر کشف وجود ارتباط پنهان و هدف از آن تشخیص و تمیز دادن رسانه حاوی اطلاعات پنهان (نهانه‌تصویری[3]) از رسانه اصلی یا تمیز (پوشانه‌تصویری[4]) است. لازم به ذکر است که منظور از رسانه در این مقاله، تصویر خاکستری[5] یا سیاه و سفید است و روش‌های نهان‌نگاری مورد بحث ما نیز در حالت سناریوی ناظر غیر فعال است که به طور وسیعی مشغول نظارت بر کانال‌های ارتباطی هستند. به طور کلی، مناطق شلوغ از لبه و نویز یا مناطق پر نوسان تصویر که" زبر[6]" نامیده می‌شود، خصوصیات آماری پیچیده‌تری از مناطق صاف و هموارتر دارند و به شدت به محتوای تصویر وابسته هستند. علاوه بر این، مشاهده تغییرات در چنین مناطقی از مناطق هموار و صاف‌تر، مشکل است. به همین دلیل روش‌های نهان‌نگاری تطبیقی به متن پوشانه تصویری توجه ویژه‌ای دارند. این روش‌ها زبرترین مناطق تصویر به مفهوم فوق را شناسایی کرده و به مخفی سازی پیام در آن مناطق می‌پردازند. یکی از معیارهای مهم دیگری که در نهان‌نگاری تصویر دارای اهمیت فراوانی است، موضوع تخریب سریع و آسان پیام جاسازی شده در پوشانه‌های تصویری در حوزه مکان، براثر حملات عمد یا غیر عمدی مانند فیلترینگ یا اعوجاج‌های دیگر است. پایداری پیام جاسازی شده در مقابل چنین حملاتی را مقاومت[7] می‌گویند. مسئله مهم دیگری که در نهان‌نگاری تطبیقی وجود دارد، اختلاف پیکسل‌های انتخابی در پوشانه در قبل از جاسازی (هنگام اختفاء) و بعد از جاسازی (هنگام استخراج) از نهانه است. بنابراین، طراحی یک الگوریتم نهان‌نگاری کارآمد (امن‌تر و مقاوم‌تر) برای اختفای پیام، که پیکسل‌های انتخابی متناظر در پوشانه و نهانه یکسان باشد، دارای اهمیت فراوانی است [۱ و ۲].

از اولین روش‌های نهان‌نگاری تطبیقی می‌توان روش نهان‌نگاری تفاضل مقادیر پیکسل‌ها (PVD[8]) را نام برد که پیام را در اختلاف بین پیکسل‌های مجاور، یعنی لبه، جاسازی می‌کند [۳]. دسته دیگر، روش‌هایی هستند که صرفاً لبه‌های تصویر را با استفاده از روش‌های معمول در پردازش تصویر، مانند سوبل[9] و کنی[10] شناسایی می‌کنند. محدودیت اصلی این روش‌ها نیز در تفاوت پیکسل‌های لبه در پوشانه و نهانه، یعنی قبل و بعد از جاسازی پیام است. دسته سوم از آن‌ها، روش‌های نهان‌نگاری تطبیقی مبتنی بر کم‌ارزش‌ترین بیت است (LSB[11]) که محدودیت اصلی آن‌ها جاسازی ناخواسته بعضی بیت‌های پیام محرمانه، در مناطق صاف و هموار پوشانه‌های تصویری و شناسایی سریع آن‌ها توسط بسیاری از الگوریتم‌های نهان‌کاوی است.

یکی از ویژگی‌های مشترک بیشتر روش‌های نهان‌نگاری که در بالا نام برده شد، در انتخاب پیکسل یا جفت پیکسل‌ها برای جاسازی پیام است که بعضاً توسط یک مولد شبه تصادفی تعیین می‌شود و بعضی به صورت جستجوی ترتیبی به جاسازی و اختفای پیام در تصویر می‌پردازند. هر یک از این روش‌های انتخاب مکان جاسازی، به‌تنهایی مناسب نیستند، به دلیل اینکه روش‌هایی که صرفاً از تصادف استفاده می‌کنند بعضاً به جاسازی در نواحی صاف تصویر می‌پردازند و دسته دوم روش‌ها، یعنی روش‌های تطبیقی محض هم به دلیل توجه بیش از حد به امر تطبیق و جستجو، از امتیاز تصادف برای افزایش امنیت محروم می‌مانند[۴]. همچنین بسیاری از این الگوریتم‌ها، رابطه بین محتوی تصویر و طول پیام محرمانه را نادیده می‌گیرند. با این حال، بر اساس تجزیه و تحلیل گسترده‌ای، چنین طرح‌های جاسازی از لحاظ امنیتی یا کیفیت بصری تصاویر نهانه، خوب عمل نمی‌کنند. بنابراین یک الگوریتم نهان‌نگاری امن و کارآمد، ترجیحاً با در نظر گرفتن هم‌زمان تصادفی و تطبیقی، قابل دستیابی است. بنابراین، تصمیم در مورد چگونگی انتخاب مناطق جاسازی نیز یکی از مسائل کلیدی طرح پیشنهادی در این مقاله است.

بنابراین، در این مقاله، یک روش نهان‌نگاری تطبیقی کارآمد، بر اساس آنتروپی تصویر و یک روند شبه تصادفی و جاسازی پیام ترکیبی، معروف به کدگذاری xor (xor coding[12]) و الگوریتم توسعه یافته مبتنی بر دومین بیت کم‌ارزش (ELSB2[13]) طراحی می‌شود. این روش که با استفاده از نگاشت هر پنجره ۳×۳ از تصویر در یک گراف و محاسبه آنتروپی پنجره تصویر مورد نظر با کمک آنتروپی گراف متناظر تعریف می‌شود، با دقت بیشتری در مقایسه با روش‌های پیشین به شناسایی پنجره‌های زبر تصویر می‌پردازد. یکی از امتیازات اصلی الگوریتم پیشنهادی این است که

[1] Steganography
[2] Steganalysis
[3] Stego Image
[4] Cover Image
[5] Gray Scale
[6] roughness
[7] Robustness
[8] Pixel Value Difference
[9] Sobel
[10] Canny
[11] Least Significant Bit
[12] Xor Coding
[13] Extended LSB2

Archive of SID

www.SID.ir

Downloaded from adst.ir at 14:14 +0330 on Monday February 26th 2018

میزان زبری پنجره‌های متناظر در پوشانه و نهانه یکی است. امتیاز مهم دیگر روش پیشنهادی این است که با انتخاب یک آستانه مناسب به انتشار و مخفی سازی بیت‌های پیام در سراسر تصویر می‌پردازد. در این روش جاسازی ترکیبی، عمل xor تضمین کننده یکی از شرایط امنیت در جاسازی، یعنی تقارن در افزایش یا کاهش شدت روشنایی پیکسل‌ها است. با استفاده از این عمل سه بیت پیام در چهار پیکسل از پیکسل‌های هر پنجره زبر (پنجره‌ای از پوشانه تصویری که شرایط لازم جاسازی را داشته باشد)، جاسازی می‌شود. به علاوه استفاده از عمل xor باعث می‌شود، پیام محرمانه در پوشانه با کمترین میزان تغییرات پیکسلی، یعنی ۰/۲۵ پنهان شود. الگوریتم ELSB2 نیز بدون افزایش تخریب پوشانه، بیت‌های پیام را در دومین بیت کم‌ارزش پیکسل‌ها جاسازی می‌کند.

ادامه این مقاله، در بخش ۲ مروری بر تحقیقات مرتبط خواهم داشت. بخش ۳ به پیش‌زمینه مورد نیاز در طراحی الگوریتم پیشنهادی، مانند نگاشت یک تصویر در گراف و تعریف جدید آنتروپی تصویر با استفاده از گراف متناظر هر پنجره ۳×۳ از تصویر پرداخته می‌شود. الگوریتم پیشنهادی در بخش ۴ ارائه خواهد شد و در بخش ۵ نتایج تجربی الگوریتم پیشنهادی و درنهایت در بخش ۶ نتیجه‌گیری و پیشنهاد تحقیقات آینده انجام می‌گیرد.

۲. تحقیقات مرتبط

شاید اولین روش نهان‌نگاری تطبیقی طراحی شده بر اساس میزان حساسیت کمتر سیستم بینایی انسان، روش تفاضل مقدار پیکسل‌ها (PVD[1]) است، که در آن تلاش می‌شود مخفی سازی پیام در مناطق لبه تصویر صورت گیرد. این روش که توسط ویو و تیسای [۳] ارائه شده، تفاوت‌ها را تنها در یک جهت عمودی یا افقی تصویر در نظر می‌گیرد که شناسایی تمام لبه‌ها را تضمین نمی‌کند. روش تفاضل مقدار پیکسل‌های بهبود یافته (IPVD[2]) برای رفع چالش ایجاد شده در روش PVD توسط ژانگ و وانگ [۵] 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 بر اساس تفاضل بیشتر آن‌ها انتخاب نمی‌کند. در نتیجه باعث ناهمگونی دیگری در هستوگرام نهانه می‌شود. الگوریتم تطبیق لبه مبتنی بر کم‌ارزش‌ترین بیت (AE-LSB[3]) توسط چنگ- هسینگ یانگ و همکارانش[۶] ارائه شد. این روش نیز با تنظیم نحوه جاسازی به صورت 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 باعث یک ناهمگونی در هستوگرام نهانه می‌شود. ناگفته نماند که AE-LSB به دلیل اینکه از میانگین نرخ تغییرات کمتری برخوردار است، دارای ظرفیت جاسازی بالاتری است. اما در مقابل حمله RS[4] دارای ضعف است [۷].

جی‌ملیکی‌نن [۸] الگوریتم نهان‌نگاری تطبیقی اصلاح شده[5] (LSBMR) را ارائه کرد. این الگوریتم برخلاف روش‌های پیشین که به طور مستقل با تک‌تک پیکسل‌های تصویر سروکار دارند، با یک مولد شبه تصادفی، یک زوج پیکسل را به عنوان واحد جاسازی انتخاب می‌کند، که در آن کم‌ارزش‌ترین بیت اولین پیکسل، یک بیت پیام و رابطه دو پیکسل بیت دیگر پیام را حمل می‌کند. این الگوریتم نرخ تغییر پیکسل‌ها را از bpp ۰/۵ به bpp ۰/۳۷۵ کاهش داده است.

لیو و همکارانش[۹] نیز یک الگوریتم تطبیقی بازبینی شده مبتنی بر لبه[6] (EAMR) را طراحی کردند. این رویش لبه‌ها را با محاسبه اختلاف بین پیکسل‌های متوالی جستجو می‌کند و برای جاسازی پیام، لبه‌های افقی و عمودی را با تقسیم تصویر به پنجره‌های ۳×۳ استفاده می‌کند. با این حال، این فرایند می‌تواند ارتباط بین پیکسل‌های عمودی و افقی را از بین ببرد، ولی به دلیل ضعف در انتخاب آستانه، لبه‌های زیادی را از دست می‌دهد و بعضاً در مناطق صاف و هموار، به جاسازی پیام می‌پردازد. بنابراین با توجه به اینکه این روش تأکید زیاد بر تطبیق با لبه دارد، در مقابل بعضی از الگوریتم‌های نهان‌کاوی اختصاصی و عمومی امروزی دارای ضعف است.

الجمال و همکارش [۱۰]، به منظور افزایش مقاومت، یک روش جاسازی پیام ارائه کردند که در آن بعضی از بیت‌های پیام در LSB2 پیکسل‌های پوشانه تصویری جاسازی می‌شود. شمع علی زاده و نوروزی [۱۱] این رویش را توسعه دادند و الگوریتم طراحی شده را LSB2 توسعه یافته (ELSB2[7]) نامیدند، به گونه‌ای که با استفاده از آن، بدون تخریب اضافی در تصویر، کلیه بیت‌های پیام را در دومین بیت کم‌ارزش پیکسل‌ها جاسازی نمودند.

هوانگ و همکاران[۱۲] الگوریتم نهان‌نگاری تطبیقی اصلاح شده مبتنی بر لبه توسعه یافته[8] (I-EAMR) را پیشنهاد داده، که توسعه‌ای از الگوریتم نهان‌نگاری تطبیقی اصلاح شده مبتنی بر

[1] Pixel Value Difference
[2] Improvement PVD
[3] Adaptive Edge LSB
[4] Regular Singular
[5] LSB Matching Revisited
[6] Edge Adaptive LSBMR
[7] Extended
[8] Improved Algorithm of Edge Adaptive Image Steganography Based on LSB Matching Revisited

Archive of SID

www.SID.ir

Downloaded from adst.ir at 14:14 +0330 on Monday February 26th 2018

لبه[1] (EAMR) است. در این روش، برخلاف روش EAMR که در آن زوج پیکسل‌های متوالی به صورت ترتیبی انتخاب می‌شدند، پوشانه به پنجره‌های ناهم‌پوشان ۳×۳ تقسیم شده و زوج پیکسل‌های مجاور به طور تصادفی در هر پنجره بر طبق جهت‌های مختلف انتخاب شده و جاسازی پیام طبق روش LSBMR، در لبه‌های تصویر صورت می‌گیرد، اما مسئله تعیین آستانه همچنان وجود دارد.

وستفلد [۱۳]، روش F_5 را معرفی کرد که در آن برای جاسازی n بیت، 2^n-1 پیکسل مصرف می‌شود. این روش برای $n=2$ دارای نرخ جاسازی ۰/۶۷ bpp و نرخ تغییر ۰/۲۵ bpp است که نرخ‌های مناسبی هستند.

هات الدیمور و احمد الانی [۱۴] با تقسیم تصویر به پنجره‌های ۳×۳ ناهم‌پوشان و محاسبه میانگین تفاضلات ستون‌های چپ و راست هر پنجره، و تکرار آن برای سطرهای بالا و پایین و همین‌طور قطرهای اصلی و فرعی، حداکثر مقدار آن‌ها را e نامیده و با در نظر گرفتن یک آستانه تجربی T پنجره‌های که $e > T$ 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 پیکسل‌ها ۰/۲۵ bpp است، فقط چهار پیکسل از هر پنجره ۳×۳ در شناسایی پیکسل‌های لبه نقش دارند و بقیه پیکسل‌ها را در نظر نمی‌گیرند به همین دلیل از دقت پایین‌تری برخوردار است.

۳. پیش‌زمینه

پیکسل‌های نواحی زبر و شلوغ از لبه و نویز به علت ازدیاد تغییر فرکانس، انتخاب مناسب‌تری برای مخفی سازی پیام در نهان نگاری هستند. چرا که احتمال تشخیص تغییرات ناشی از مخفی سازی پیام در این مناطق، با استفاده از الگوریتم‌های نهان‌کاوی، کمتر از مناطق صاف و هموار تصویر است.

معیارهای مختلفی برای شناسایی مناطق زبر نسبت به نواحی صاف تصویر وجود دارد. یکی از این معیارها، آنتروپی است. آنتروپی، کاربرد زیادی در زمینه‌های مختلف پردازش تصویر، به ویژه نهان‌نگاری و نهان‌کاوی دارد. آنتروپی شانون در حالت کلی مفاهمی نظیر میانگین اطلاعات موجود و عدم قطعیت را برآورد می‌کند. می‌دانید که آنتروپی وابسته به تعریف یک متغیر تصادفی روی پیشامدها است. یکی از تعاریفی که برای آنتروپی تصویر $I=[I_{ij}]^{w\times h}$ وجود دارد و بر اساس تعریف کلی آنتروپی شانون است، به صورت $H(I)=-\sum_{i=0}^{255}\frac{f_I(i)}{N}\log\frac{f_I(i)}{N}$ است در این تعریف $N=w\times h$ و $f_I(i)$ فرکانس شدت روشنایی $i=0,1,2,\dots,255$ است [۱۵]. همان‌طور که می‌دانید، این تعریف تصاویر صاف و همواری را که از تغییرات کمتری برخوردارند، با آنتروپی کمتر و تصاویر ناهموار با تغییرات بیشتر را با آنتروپی بیشتر شناسایی می‌کند. در ضمن، به دلیل استفاده این تعریف از فرکانس شدت روشنایی پیکسل‌ها، برای ارزیابی ناهمواری یک تصویر کامل مناسب است. تعریف دیگری نیز برای آنتروپی تصویر بیان شده است[۱۶]، که به جای استفاده از فرکانس، از شدت روشنایی تک‌تک پیکسل‌های آن استفاده می‌کند. این تعریف به دلیل اینکه به صورت محلی نیز تعریف می‌شود، کاربرد زیادی در زمینه‌های مرتبط با پردازش تصویر، به ویژه در نهان‌کاوی دارد. در ادامه بخش، این تعریف را بازگو کرده و در حالت محلی نیز برای پنجره‌های ۳×۳ از تصویر بیان می‌شود. سپس با استفاده از آنتروپی گراف متناظر با هر پنجره ۳×۳ از تصویر، تعریف کارآمد دیگری برای آن به‌دست می‌آید که با مقایسه این دو تعریف نشان داده می‌شود که تعریف مبتنی بر گراف، معیار دقیق‌تری برای تشخیص پنجره‌های زبر و ناهموار از پنجره‌های صاف و هموار، در نهان‌نگاری تصویر است.

۳-۱. آنتروپی تصویر بر اساس شدت روشنایی

در نظریه اطلاع و پردازش تصویر محتویات اطلاعاتی یک تصویر خاکستری $I=[I_{ij}]$ با ابعاد $w\times h$ با استفاده از آنتروپی آن به صورت زیر ارزیابی می‌شود:

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

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

که در آن، I_{ij} شدت روشنایی پیکسل (i,j)، q_{ij} توزیع احتمال I_{ij} و H آنتروپی تصویر I است [۱۶]. این تعریف آنتروپی، نشان دهنده میزان تفرق و پراکندگی شدت روشنایی پیکسل‌های تصویر است. مطابق این تعریف، با توجه به اینکه بیشینه (۱) زمانی اتفاق می‌افتد که $q_{xy}=q_{x'y'}$، بنابراین، برخلاف روش مبتنی بر تعریف شانون، این نشان می‌دهد، تصاویری که شدت روشنایی یکنواختی 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 زیر ماتریس از تصویر با واریانس و انحراف معیار داده‌های ماتریس، رابطه عکس دارد. این یعنی با افزایش واریانس و انحراف معیار، آنتروپی کاهش و در نتیجه داده‌های چنین ماتریسی از یکنواختی و صافی دور می‌شود. بنابراین معمولاً

[1] Edge Adaptive Image Steganography Based on LSB Matching Revisited

Archive of SID

www.SID.ir

Downloaded from adst.ir at 14:14 +0330 on Monday February 26th 2018

آنتروپی یک پنجره از تصویر با تقسیم فرمول فوق بر انحراف معیار داده‌های ماتریس به صورت زیر به‌دست می‌آید [۱۶]:

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

در این صورت رابطه مقادیر عددی آنتروپی محاسبه شده و نوسان و تغییرات پیکسل‌ها برعکس می‌شود. یعنی مقدار عددی بزرگ‌تر آنتروپی نشان دهنده نوسانات و اعوجاج کمتر و مقادیر عددی کمتر، گواه تغییرات و اعوجاج بیشتر در تصویر خواهد بود. این مطلب نشان می‌دهد که آنتروپی می‌تواند ملاک و معیار مناسبی برای شناسایی تصاویر زبر و پر نوسان از تصاویر صاف و هموار باشد. بنابراین برای به‌کارگیری آنتروپی در گراف سعی می‌شود به یک آنتروپی محلی در تصویر برسیم که نواحی زبر تصویر را دقیقاً شناسایی کند.

۳-۲. گراف و آنتروپی

هر گراف از زوج $G = (E, V)$ تشکیل شده است 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 [۱۷ و ۱۸]. در این تعریف، اگر ترتیب مهم باشد گراف مورد نظر را جهت‌دار و در غیر این صورت، بدون جهت می‌گویند.

در نظریه گراف آنتروپی هر گراف $G = (E, V)$ با رئوس $X = \{v_1, v_2, \dots, v_n\}$ به صورت زیر قابل تعریف است [۱۹ و ۲۰].

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

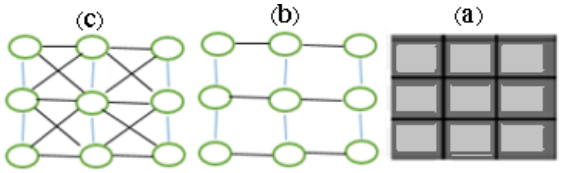
که در آن، G یک گراف ثابت دلخواه، τ معیاری برای استخراج کلاس‌های معادل X_i و مقدار $\frac{|X_i|}{|X|}$ می‌تواند به عنوان احتمالی برای کلاس X_i تعبیر شود. همچنین با در نظر گرفتن گراف G برای رأس دلخواه $v_i \in V$ تعریف می‌شود: $p(v_i) = \frac{f(v_i)}{\sum_j f(v_j)}$ که در آن f نشان دهنده یک تابع اطلاعاتی از وضعیت ساختاری در گراف G است و با توجه به اینکه $\sum_{i=1}^{n} p(v_i) = 1$ می‌توان $p(v_i)$ را به عنوان احتمال رأسی v_i تعبیر شود که در این صورت یک آنتروپی وابسته به تابع اطلاعاتی f، بیان کننده یک ویژگی مانند وزن یال‌ها، برای گراف G به صورت زیر قابل تعریف خواهد بود[۱۹ و ۲۰]:

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

معیارهای آنتروپی فوق، برای توصیف یک گراف با تعیین محتوای اطلاعاتی آن، در حالت کلی بیان شدند که هر یک معیاری بر اساس ویژگی‌های محلی هستند.

۳-۳. شناسایی پنجره زبر با استفاده از آنتروپی گراف

به منظور به‌کارگیری مفاهم نظریه گراف در نهان‌نگاری تصویر، ابتدا تصویر باید در یک گراف نگاشته شود. این نگاشت، هر پیکسل تصویر را به یک رأس گراف به صورت یک رابطه یک‌بهک می‌نگارد. متناظر هر پیکسل در تصویر، یک رأس در گراف دارید. همچنین، رابطه مجاورت پیکسل‌ها در تصویر نیز به طور مشابه به صورت ۴- همسایگی یا ۸- همسایگی در گراف نگاشته می‌شود. شکل (۱) را ببینید که در آن (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 یک‌بهک 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 دارید. برای دو رأس v_i و v_j در گراف، یک یال (i, j) را دارید که رابط دو رأس است [۱۸]. اگر به هر یال این گراف یک عدد مانند $|v_i - v_j|$ اختصاص داده شود، گراف وزن‌دار خواهد شد.



شکل ۱. (a) یک پنجره ۳×۳ از یک تصویر (b) گراف متناظر با ۴- همسایگی (b) گراف متناظر۸- همسایگی [۱۸]

فرض کنید d یک متر در مجموعه اعداد حقیقی نامنفی باشد و D یک زیرگراف k رأسی از گراف G با رئوس $V = \{v_1, v_2, \dots, v_n\}$ باشد، با نشان دادن آنتروپی این زیرگراف نسبت به رأس v_i با $H_D(v_i)$ (آنتروپی محلی D نسبت به رأس v_i) می‌توان تعریف کرد:

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

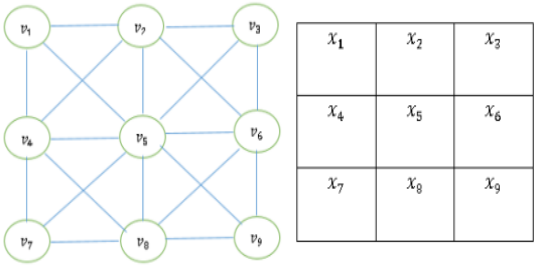
که در آن رئوس v_i و v_j مجاور و $d(v_i, v_j)$ می‌تواند فاصله رئوس v_i و v_j بوده و $d(v_i) = \sum_j d(v_i, v_j)$ باشد. واضح است که در این تعریف با قرار دادن $p(v_j) = \frac{d(v_i, v_j)}{d(v_i)}; i, j = 1, \dots, k$ دارید: $p(v_j) \geq 0$ و $\sum_j p(v_j) = 1$ که نشان از صحت تعریف آنتروپی دارد. برای فهم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

همان‌طوری که قبلاً اشاره شد، بررسی مطلوبیت ناحیه مورد نظر از تصویر، از لحاظ زبری، شرط اصلی جاسازی پیام در نهان‌نگاری تطبیقی است. برای به‌دست آوردن این معیار فرض می‌شود $I = [I_{ij}]$ یک تصویر و G گراف متناظر باشد. یک پنجره ۳ × ۳ از تصویر I و گراف ۸- همسایگی متناظر آن را مطابق شکل (۲) در نظر بگیرید.

Archive of SID

www.SID.ir

Downloaded from adst.ir at 14:14 +0330 on Monday February 26th 2018



شکل ۲. یک پنجره ۳ × ۳ از تصویر و گراف ۸- همسایگی متناظر آن

طبق روابط تعریف شده در رابطه (۶) به یک معیار عددی مشخص برای یک پنجره محلی از تصویر می‌رسید. برای این کار دو حالت در نظر گرفته می‌شود.

الف: با تعریف $f(v_i) = v_i$ و $\sum_j f(v_j) = \sum_j v_j$ و بنابر رابطه (۵) برای زیر گراف D از G خواهید 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 زیر گراف D بر حسب 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 اطلاع، یعنی رابطه (۱) است که تأثیر شدت روشنایی همه پیکسل‌های همسایه در محاسبه آنتروپی مورد توجه قرار نمی‌گیرد.

ب: با توجه به اینکه هر پیکسل از لحاظ آنتروپی به معنی پیش‌بینی ناپذیری و در نتیجه عدم قطعیت و پیچیدگی، در همه هشت همسایه خودش تأثیرگذار است. بنابر رابطه (۶) برای هر دو راس مجاور v_i و v_j که $i \neq j$ تعریف می‌شود:

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

به این ترتیب، برای هر رأس گراف و در نتیجه هر پیکسل، با توجه به همه هشت همسایه‌اش به محاسبه آنتروپی اقدام می‌شود. 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 فرمول (۸) قابل محاسبه است. در نتیجه تاکنون دو معیار (۷ و ۸) برای محاسبه آنتروپی یک پنجره از تصویر ارائه شد که آن‌ها با هم مقایسه خواهد شد. در ادامه، خواهید دید که معیار جدید، یعنی فرمول (۸) نتایج بهتری از فرمول (۷)، یعنی فرمول آنتروپی تصویر مرسوم در نظریه اطلاع و پردازش تصویر خواهد داشت. با محاسبه انحراف معیارها به صورت: $\sigma_v = Stdev(v_1, v_2, \dots, v_9)$ و $\sigma_v^* = Stdev(\{|v_i - v_j|, \forall i \neq j\})$، هر دو فرمول را بر انحراف معیارشان تقسیم می‌شود. یعنی:

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

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

حال برای نتیجه‌گیری بهتر و مقایسه آن‌ها، ماتریس داده چند پنجره از یک تصویر فرضی را در نظر گرفته می‌شود و نتایج محاسبه آنتروپی آن‌ها را طبق فرمول‌های (۹) و (۱۰) در ستون‌های سوم و چهارم جدول (۱) نشان داده می‌شود.

با توجه به داده‌های موجود در هر ردیف جدول (۱)، که در آن هر دسته داده، تشکیل یک پنجره از تصویر مانند $\begin{bmatrix} 11 & 12 \\ 13 & 14 \end{bmatrix}$ را می‌دهند، ملاحظه می‌شود که در هر یک از زوج ردیف‌های ۱ و ۲، ۳ و ۴ همچنین ۵ و ۶، مقادیر H_1^* متفاوت ولی مقادیر H_2^* یکسان است. این در حالی است که تغییرات داده‌ها در هر یک از این زوج ردیف‌های متوالی، ثابت است و در هر زوج ردیف متناظر، داده‌های ماتریسی ردیف دوم از افزایش عدد ثابتی به داده‌های ردیف اول به‌دست آمده است و بنابراین، انتظار به‌دست آمدن یک مقدار به عنوان معیار زبری چنین پنجره‌هایی را دارید. این موضوع نشان دهنده دقت بالاتر H_2^* در مقایسه با H_1^* است و به ویژه در طراحی الگوریتم نهان‌نگاری تصویر، که لازم است پنجره‌های زبر در نهانه و پوشانه یکسان باشد، استفاده از معیار دقیقی چون H_2^* ابزار مهمی برای رسیدن به یک الگوریتم کارآمد است.

جدول ۱. محاسبه آنتروپی چند زیرگراف متناظر یک تصویر در دو حالت

ردیف	داده‌ها	H_1^*	H_2^*
۱	۱,۲ ,۳ ,۴	۱/۴۳۰۲۵	۲/۹۹۶۲۶
۲	۳۱ , ۳۲ , ۳۳ , ۳۴	۱/۵۴۸۵۳	۲/۹۹۶۲۶
۳	۱۰,۲۰,۳۰,۴۰	۰/۱۴۳۰۲	۰/۲۹۹۶۳
۴	۴۰,۵۰,۶۰,۷۰	۰/۱۵۳۲۵	۰/۲۹۹۶۳
۵	۱۱,۱۲,...,۱۹	۱/۱۴۹۶۲	۱/۵۱۳۸۸
۶	۱۲۱,۱۲۲,...,۱۲۹	۱/۱۵۷۳۸	۱/۵۱۳۸۸

۳-۴. شناسایی پیکسل‌های مناسب جاسازی و تعیین آستانه زبری

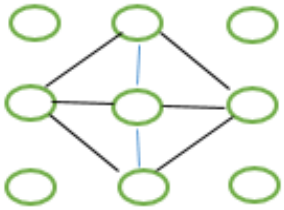
برای این کار پنجره‌های ناهمپوشان ۳×۳ از یک تصویر را مانند شکل (۲-a) در نظر گرفته می‌شود. برای انتخاب پیکسل‌های مناسب جاسازی، آنتروپی گراف متناظر آن را ($H_2^*[i]$ که v_i رأس میانی هر پنجره است) بدون در نظر گرفتن چهار پیکسل گوشه‌ای، مطابق شکل (۳) و فرمول (۱۰) محاسبه می‌شود. علت شرکت ندادن چهار پیکسل گوشه‌ای هر پنجره، در محاسبات این است که می‌خواهیم پیکسل‌های انتخابی در پوشانه، برای جاسازی

Archive of SID

www.SID.ir

Downloaded from adst.ir at 14:14 +0330 on Monday February 26th 2018

و پیکسل‌های انتخابی در نهانه، برای استخراج پیام جاسازی شده، یکسان شود.



شکل ۳. گراف در نظر گرفته شده برای تعیین پیکسل‌های مناسب جاسازی

در این محاسبه، مقادیر صفر را که نشان‌دهنده پنجره‌های صاف هستند، حذف کرده و بقیه را تا k رقم اعشار گرد نموده، در آرایه $H_2^*[\mathrm{i}];\ \mathrm{i}=1,2,\dots,\mathrm{l}$ ذخیره می‌شود. نکته قابل توجه این است که با توجه به مبحث قبل، پنجره‌های زبرتر دارای آنتروپی محلی کمتری هستند که هنگام جاسازی پیام باید در اولویت قرار گیرند. بنابراین، برای جاسازی پیام M با طول $|M|$ لازم است آستانه‌ای $T>0$ را طوری به‌دست آورد که تعداد پنجره‌های زبر شمارش شده در سراسر تصویر، به ازای آن مقدار T یعنی N_w، ظرفیت جاسازی پیامی با طول $|M|$ را داشته باشد. این یعنی T را طوری تعیین می‌شود 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. به عبارت دیگر:

$$T = H_2^*[p] = arg.\min\{_{H_2^*[i]}|\{H_2^*[i]; H_2^*[i] \leq H_2^*[p]\}| \geq \frac{|M|}{K}\} \quad (۱۱)$$

بنابراین، پنجره‌هایی با آنتروپی موجود در بازه $[0,T]$ پنجره زبر نامیده می‌شوند و برای جاسازی بیت‌های پیام مناسب هستند.

اما تعیین T به طول پیام و تعداد بیت‌های پیامی که در هر پنجره زبر می‌توان جاسازی کرد، بستگی دارد، یعنی T را طوری پیدا می‌شود که بیت‌های پیام بتوانند در سراسر تصویر پخش شوند. در نتیجه از کل ظرفیت تصویر برای جاسازی پیام استفاده می‌شود.

۴. طراحی روش نهان‌نگاری تطبیقی و مقاوم

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 شود. از طرفی جاسازی در پیکسل‌های شناسایی شده توسط روش‌های تشخیص لبه معمولی، مانند سوبل[1] یا کنی[2]، شناسایی لبه‌ها را برای تصاویر پوشانه و نهانه در قبل و بعد از نهان‌نگاری تضمین نمی‌کنند. در این مقاله الگوریتم نهان‌نگاری تطبیقی نوینی با استفاده از آنتروپی گراف، پیشنهاد می‌شود. در این روش کلیه پیکسل‌های هر پنجره در همه جهت‌های ۸-همسایگی پیکسل‌ها، برای محاسبه معیار زبری دخالت دارند. این موضوع تضمین کننده دقت روش است. دوم آنکه میزان زبری ناحیه، برای بالا بردن رؤیت ناپذیری 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 به طور دقیق شناسایی می‌کند. بنابراین، به هیچ وجه اجازه جاسازی پیام در آن‌ها را نمی‌دهد. امتیاز مهم دیگر این روش این است که پنجره‌های زبر در پوشانه و نهانه‌های تصویری یکسان است. این الگوریتم به دلیل بهره بردن از xor coding امنیت مناسب و به خاطر جاسازی در بیت دوم کم‌ارزش از مقاومت بالاتری نیز برخوردار است و با این وجود کیفیت تصاویر نهانه به‌دست آمده معادل جاسازی در اولین بیت کم‌ارزش است. در این الگوریتم علاوه بر شناسایی تطبیقی پیکسل‌ها برای تقویت امنیت از روند تصادفی هم استفاده می‌شود.

۴-۱. الگوریتم پیشنهادی

ورودی‌ها: تصویر پوششی C با ابعاد $h \times w$ و پیام محرمانه M.

خروجی‌ها: تصویر نهانه S با ابعاد $h \times w$ و آستانه استخراج پیام از آن یعنی T.

گام ۱. تقسیم پوشانه تصویری به پنجره‌های ناهم‌پوشان و دوران آن: در این گام تصویر را به صورت پنجره‌های ناهم‌پوشان ۳×۳ تقسیم کرده، هر پنجره را با کلید محرمانه key1 به یکی اندازه‌های تصادفی $\{0, 90, 180, 270\}$ بر حسب درجه دوران دهید. با این چرخش تصادفی، دو مزیت به‌دست می‌آید. اول اینکه می‌تواند از دست‌یابی آشکارساز به واحدهای درست جاسازی بدون عمل دوران، طبق کلید key1، جلوگیری کند، دوم اینکه به این ترتیب در هر پنجره زبر، رشته پیکسل‌ها به طور تصادفی برای جاسازی انتخاب می‌شوند.

گام ۲. محاسبه آنتروپی هر پنجره: با در نظر گرفتن گراف متناظر برای هر پنجره مطابق گام اول، به محاسبه آنتروپی محلی آن طبق فرمول (۱۰) پرداخته می‌شود. در این محاسبه، مقادیر صفر را که نشان دهنده پنجره‌های صاف هستند، حذف کرده و بقیه را تا k رقم اعشار گرد نموده، در ارائه $H_2^*[\mathrm{i}];\ \mathrm{i}=1,2,\dots,\mathrm{l}$ ذخیره می‌شود.

گام ۳. محاسبه آستانه زبری پنجره‌های تصویر: با توجه به اینکه آرایه $H_2^*[i]$ شامل آنتروپی کلیه پنجره‌های ناصاف تصویر

[1] Sobel

[2] Canny

www.SID.ir

Downloaded from adst.ir at 14:14 +0330 on Monday February 26th 2018

مورد نظر است. مقادیر کمتر در آن نشان دهنده پنجره‌های زبرتر است، با توجه به طول پیام M ،آستانه زبری $0 < T \leq H_2^*[p]$ را طوری انتخاب می‌شود که $N_w \times k \geq |M|$ باشد و k تعداد بیت‌های پیامی است که بسته به روش جاسازی پیام، می‌توان در هر پنجره زبر جاسازی کرد (در اینجا $k = 4$ است). به عبارت دیگر:

$T = H_2^*[p] = arg.\min\{_{H_2^*[i]} |\{H_2^*[i]; H_2^*[i] \leq H_2^*[p]\}| \geq \frac{|M|}{K}\}$ یعنی آستانه را متناسب با طول پیام طوری انتخاب می‌شود که تا حد امکان پیام در سراسر تصویر پخش و مخفی سازی شود. پس از محاسبه T، گام اصلی ۴ را تا پایان جاسازی کلیه بیت‌های پیام M تکرار می‌شود.

گام ۴. از گوشه چپ بالای تصویر، گراف متناظر هر پنجره ناهم‌پوشان را مطابق شکل (۳) در نظر گرفته آنتروپی آن را، H_2^*، نامیده می‌شود. چنانچه $H_2^* \leq T$ باشد، چهار پیکسل گوشه‌ای پنجره مورد نظر مناسب جاسازی پیام است و $LSB2$ آن‌ها را به ترتیب p_1, p_2, p_3 و p_4 نامیده می‌شود. سه بیت پیام m_1, m_2, m_3 را نیز در نظر گرفته می‌شود. سپس k_1, k_2 و k_3 به صورت زیر تعریف می‌شود:

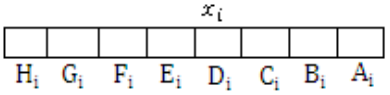
$$k_1 = p_1 \oplus p_2$$
$$k_2 = p_3 \oplus p_4$$
$$k_3 = p_1 \oplus p_3$$

و مطابق جدول (۲) مقایسه‌ای زیر، p_i های$(new\mathrm{p}_i)$ جدید را محاسبه می‌شود.

جدول ۲. شرایط جاسازی xor coding

شرط			عمل
$m_1 = k_1$	$m_2 = k_2$	$m_3 = k_3$	بدون تغییر
$m_1 \neq k_1$	$m_2 = k_2$	$m_3 = k_3$	$\sim p_2$
$m_1 = k_1$	$m_2 \neq k_2$	$m_3 = k_3$	$\sim p_4$
$m_1 = k_1$	$m_2 = k_2$	$m_3 \neq k_3$	$\sim p_3$, $\sim p_4$
$m_1 \neq k_1$	$m_2 \neq k_2$	$m_3 = k_3$	$\sim p_2$, $\sim p_4$
$m_1 = k_1$	$m_2 \neq k_2$	$m_3 \neq k_3$	$\sim p_3$
$m_1 \neq k_1$	$m_2 = k_2$	$m_3 \neq k_3$	$\sim p_1$
$m_1 \neq k_1$	$m_2 \neq k_2$	$m_3 \neq k_3$	$\sim p_1$, $\sim p_4$

اکنون $new\mathrm{p}_i = \mathrm{p}_i$ قرار دهید و هر یک از آن‌ها را مطابق الگوریتم ELSB2 در دومین بیت کم‌ارزش LSB2 پیکسل‌های مناسب جاسازی پوشانه، x_i، جاسازی می‌شود (افزایش مقاومت).



برای جاسازی بیت $newp_i$ در دومین بیت کم‌ارزش یعنی روی B_i (LSB2)، الگوریتم ELSB2 در زیر به نحوی عمل می‌کند که حداکثر تغییر در پیکسل x_i به اندازه یک واحد باشد (یعنی به اندازه LSB1).

```
if (B_i = new p_i) Then     do nothing
Else If (new p_i = 0 and B_i = 1)
{
 If (A_i = 0)
{ B_i = 0; A_i = 1; }
   Else If (A_i = 1 )      {
   If (C_i = 0)
{C_i = 1; B_i = A_i = 0 ;}
    Else If (D_i = 0)
{D_i = 1; C_i = B_i = A_i = 0 ;}
    Else If (E_i = 0)
{E_i = 1; D_i = C_i = B_i = A_i = 0 ;}
 Else If (F_i = 0)

 {F_i = 1; E_i = D_i = C_i = B_i = A_i = 0 ;}
 Else If (G_i = 0) {G_i = 1; F_i = E_i = D_i = C_i = B_i = A_i = 0 ;}
 Else If (H_i = 0)
{H_i = 1 ; G_i = F_i = E_i = D_i = C_i = B_i = A_i = 0 ;}
                    }
}
Else If (new p_i = 1 and B_i = 0)
    {
If (A_i = 1)   then
  { B_i = 1; A_i = 0; }
Else If (A_i = 0)    {
      If (C_i = 1)
{C_i = 0;     B_i = A_i = 1 ;}
       Else If (D_i = 1)
{D_i = 0; C_i = B_i = A_i = 1 ;}
       Else If (E_i = 1)
{E_i = 0; D_i = C_i = B_i = A_i = 1 ;}
 Else If (F_i = 1){F_i = 0; E_i = D_i =   C_i = B_i = A_i = 1 ;}
 Else If (G_i = 1){G_i = 0; F_i = E_i = D_i = C_i = B_i = A_i = 1 ;}

 Else If (H_i = 1){H_i = 0 ; G_i = F_i = E_i = D_i = C_i = B_i = A_i =
1 ;}
                    }
}
```

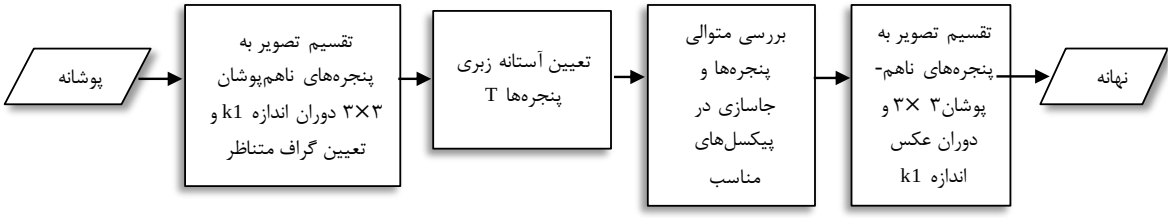
گام ۵: پس از جاسازی پیام، تصویر حاصله را مجدد به پنجره‌های ناهم‌پوشان ۳ × ۳ تقسیم کرده و هر یک از آن‌ها را با یک درجه تصادفی $\{0, 90, 180, 270\}$ بر اساس کلید key1 و در جهت عکس دوران داده می‌شود.

گام ۶: آستانه شناسایی پنجره‌های زبر یعنی T و طول پیام جاسازی شده یعنی $|M|$ را در مکان خاصی از نهانه جاسازی کرده یا از طریق کانال امن به مقصد ارسال می‌شود (شکل ۴).

Archive of SID

www.SID.ir

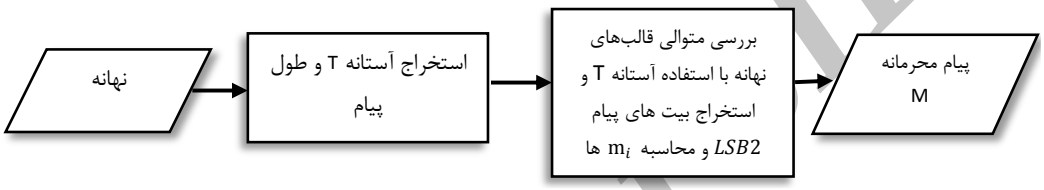
Downloaded from adst.ir at 14:14 +0330 on Monday February 26th 2018



شکل ۴. فرایند جاسازی پیام در یک تصویر پوشانه

۴- ۲. الگوریتم استخراج پیام

شکل (۵) نشان دهنده نمودار عملیاتی فرایند استخراج برای یک نهانه تصویری است که با بازیابی مقدار آستانه آغاز می‌گردد. پنجره‌های زبر تصویر نهانه با استفاده از آستانه زبری T، بازیابی می‌شوند. در ادامه، ۴ پیکسل گوشه‌ای هر پنجره زبر که آنتروپی



شکل ۵. فرایند استخراج داده از یک تصویر نهانه

۵. نتایج و بحث

با سه آزمون استاندارد، به ارزیابی الگوریتم پیشنهادی پرداخته می‌شود که یکی از آن‌ها نرخ[1] یا ظرفیت جاسازی[2] است، دومی نرخ تغییر[3] (پیکسل‌ها) یا کارایی جاسازی[4] است و سومی سطح امنیت (احتمال آشکارپذیری یا احتمال تشخیص) روش نهان‌نگاری می‌باشد. ظرفیت جاسازی یک معیار مهم برای ارزیابی کارایی روش‌های نهان‌نگاری است [۱۴]:

$$E = \frac{k}{WH}(bpp) \qquad (۱۲)$$

در این فرمول k حداکثر تعداد بیت‌های پیام 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. به عنوان مثال 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.

همان‌طوری که جدول (۳) نشان می‌دهد. روش پیشنهادی با وجود جاسازی در LSB2 و ارتقای مقاومت دارای نرخ تغییر bpp ۰/۲۵ است که کمتر از نرخ تغییر روش EAMR است. از طرفی گراف متناظر آن مطابق شکل (۳) محاسبه می‌شود، انتخاب شده و LSB2 آن‌ها را به ترتیب q_1، q_2، q_3 و q_4 نامیده می‌شود و عملیات xor به صورت زیر است:

$$m_1 = q_1 \oplus q_2$$
$$m_2 = q_2 \oplus q_3$$
$$m_3 = q_1 \oplus q_3$$

جهت بازیابی سه بیت پیام m_1، m_2 و m_3 به‌کار می‌رود.

این روش بعد از LSB1 دارای بیشترین نرخ جاسازی یعنی ۹/۳% است.

جدول ۳. نرخ تغییر و ظرفیت جاسازی پیام مهم‌ترین روش‌های نهان‌نگاری

نام روش	ظرفیت جاسازی	نرخ تغییر	توضیحات جاسازی
LSB	۱۲/۵%	۰/۵bpp	یک بیت در LSB1 یک پیکسل
LSBMR	۱۲/۵%	۰/۳۷۵bpp	دو بیت در LSB1 دو پیکسل
EAMR	۱۲/۵%	۰/۳۷۵bpp	دو بیت در LSB1 دو پیکسل
F_5	۸/۳%	۰/۲۵bpp	دو بیت در LSB1 سه پیکسل
Edge xor Coding	۹/۳%	۰/۲۵bpp	سه بیت در LSB1 چهار پیکسل
پیشنهادی	۹/۳%	۰/۲۵bpp	سه بیت در LSB2 چهار پیکسل

۵-۱. ارزیابی تخریب جاسازی[5]

کیفیت تصویر نهانه با استفاده از نرخ سیگنال به نویز حداکثر (PSNR) برای ارزیابی تفاوت بین تصاویر پوشانه و نهانه مطابق فرمول (۱۳) محاسبه می‌شود [۱۴].

$$\mathrm{PSNR} = 10\log10\left[\frac{255^2}{\mathrm{MSE}}\right](\mathrm{db}) \qquad (۱۳)$$

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

$$\mathrm{MSE} = \frac{1}{\mathrm{WH}}\sum_{i=1}^{W}\sum_{j=1}^{H}(C_{ij} - S_{ij})^2 \qquad (۱۴)$$

[1] Rate of Embedding
[2] Embedding Capacity
[3] Rate of Change
[4] Embedding Efficiency
[5] Embedding Distortion

Archive of SID

www.SID.ir

Downloaded from adst.ir at 14:14 +0330 on Monday February 26th 2018

معیار کیفیت PSNR تخریب ایجاد شده در هر تصویر نهانه را بدون در نظر گرفتن سیستم بینایی انسان، HVS، اندازه‌گیری می‌کند. wPSNR مقیاس کیفی دیگری است که در معادله (۱۵) آمده است. این مقیاس از یک پارامتر اضافی به نام تابع قابلیت دید نویز (NVF) استفاده می‌کند. البته، wPSNR برای نواحی یکنواخت مانند PSNR است ولی برای نواحی لبه مقادیر بیشتری را نشان می‌دهد. در واقع، wPSN معیار اندازه‌گیری کیفی دقیق‌تری است [۱۴].

$$\mathrm{wPSNR} = 10\log_{10}\left(\frac{\max(x)^2}{||\mathrm{NVF}(C_S)||^2}\right)\ (\mathrm{db}) \qquad (۱۵)$$

$$\mathrm{NVF}(I,j) = \frac{1}{1+\sigma^2_{L_{(i,J)}}} \qquad (۱۶)$$

جدول (۴) کیفیت تصاویر نهانه را با استفاده از الگوریتم پیشنهادی در حوزه مکان، با نرخ جاسازی ۵ تا ۳۰ درصد نشان می‌دهد. ملاحظه می‌شود که در روش پیشنهادی بهترین کیفیت نهانه را در مقایسه با EAMR به‌دست آمده است. انتخاب دقیق‌تر پیکسل‌های مناسب جاسازی پیام، باعث بهبود wPSNR روش پیشنهادی نسبت به دو روش دیگر می‌گردد.

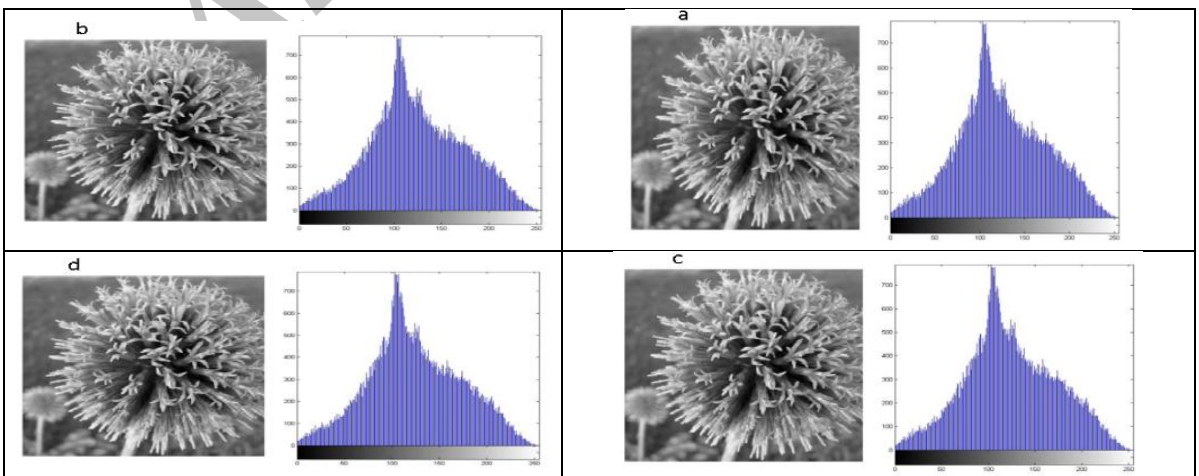
۵-۲. ارزیابی امنیت

برای ارزیابی امنیت پیام جاسازی شده توسط الگوریتم‌های نهان‌نگاری از حملات مختلفی استفاده می‌شود. یکی از این حملات، حمله بصری (بینایی) است که در آن سعی می‌شود وجود پیام محرمانه در یک تصویر از طریق دقت در تصویر یا هستوگرام آن، با چشم غیر مسلح یا رایانه، حدس زده شود. سپس با به‌کارگیری روش‌های خلاقانه یا روش‌های نهان‌کاوی دیگر وجود پیام در تصویر به اثبات برسد.

شکل (۷) تصویر پوشانه a و نهانه‌های (d-b) ناشی از پیاده‌سازی الگوریتم پیشنهادی برای تصویر گل با ابعاد ۵۱۲×۵۱۲ و با نرخ‌های جاسازی ۱۰، ۲۰ و ۳۰ درصد را نشان می‌دهد که تفاوت‌های بینایی بین تصاویر پوشانه و نهانه با چشم و حتی با مقایسه هستوگرام‌های آن‌ها قابل تشخیص نیست.

جدول ۴. کیفیت تصاویر نهانه را با استفاده از الگوریتم پیشنهادی در حوزه مکان، با نرخ جاسازی ۵ تا ۳۰ درصد

نرخ جاسازی (٪)	روش	میانگین MSE	میانگین PSNR	میانگین wPSNR
۵	EAMR	۰/۰۱۵۶	۶۶/۱۹۹۶	۶۴/۲۵۱۹
	F_5	۰/۰۱۶۵	۶۵/۹۵۶۰	۶۱/۳۱۴۴
	Edge xor Coding	۰/۰۱۵۵	۶۶/۲۲۷۵	۶۶/۳۱۲۴
	روش پیشنهادی	۰/۰۱۵۱	**۶۶/۳۴۱۰**	**۶۷/۱۳۰۰**
۱۰	EAMR	۰/۰۲۰۱	۶۵/۰۹۸۸	۶۳/۲۵۱۹
	F_5	۰/۰۲۱۳	۶۴/۸۴۷۰	۵۹/۴۲۱۸
	Edge xor Coding	۰/۰۱۹۹	۶۵/۱۴۲۳	۶۵/۲۴۱۵
	روش پیشنهادی	۰/۰۲۱۴	**۶۵/۸۲۶۷**	**۶۶/۱۸۰۹**
۱۵	EAMR	۰/۰۲۵۹	۶۳/۹۹۷۸	۶۹/۱۹۷۸
	F_5	۰/۰۲۴۵	۶۴/۲۳۹۱	۵۸/۰۱۲۴
	Edge xor Coding	۰/۰۲۵۸	۶۴/۰۱۴۶	۶۴/۸۵۴۶
	روش پیشنهادی	۰/۰۲۶۲	**۶۴/۹۴۷۸**	**۶۵/۸۹۱۴**
۲۰	EAMR	۰/۰۳۰۹	۶۳/۲۳۱۲	۶۱/۱۳۲۰
	F_5	۰/۰۲۸۸	۶۳/۵۳۶۹	۵۷/۳۲۱۵
	Edge xor Coding	۰/۰۲۹۱	۶۳/۴۹۱۹	۶۳/۱۴۱۹
	روش پیشنهادی	۰/۰۲۷۷	**۶۳/۷۰۶۰**	**۶۵/۹۹۰۰**
۳۰	EAMR	۰/۰۳۸۸	۶۲/۲۴۲۵	۶۰/۱۳۴۱
	F_5	۰/۰۳۷۷	۶۲/۳۶۷۴	۵۶/۴۴۱۹
	Edge xor Coding	۰/۰۳۱۲	۶۳/۱۸۹۳	۶۳/۰۱۲۰
	روش پیشنهادی	۰/۰۳۰۴	**۶۳/۳۰۲۱**	**۶۴/۴۵۲۷**



شکل ۷. a. تصویر اصلی و هستوگرام آن، و b، c و d تصاویر نهانه و هستوگرام‌های آن‌ها با نرخ‌های جاسازی ۱۰، ۲۰ و ۳۰ درصد

Archive of SID

www.SID.ir

Downloaded from adst.ir at 14:14 +0330 on Monday February 26th 2018

روش دیگر ارزیابی امنیتی الگوریتم‌های نهان‌نگاری، 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 نهانه‌های موجود توسط یک استخراج کننده ویژگی، استخراج شده سپس ویژگی‌های استخراج شده در مرحله آموزش، به یک طبقه‌بندی کننده، آموزش داده می‌شود. سرانجام توسط یک طبقه‌بندی کننده آموزش دیده، در مرحله آزمون به تفکیک پوشانه از نهانه اقدام می‌شود.

برای ارزیابی الگوریتم نهان‌نگاری پیشنهادی، از نرم‌افزار نهان‌کاوی SRM[5] و یک طبقه‌بندی کننده[6] استفاده می‌شود. چهار رویداد متفاوتی که در هنگام طبقه‌بندی پوشانه‌ها و نهانه‌ها رخ می‌دهند، به یکدیگر وابسته بوده و بر هم تأثیر متقابل دارند. برای فهم بهتر و مقایسه ارزیابی همه جانبه عملکرد حمله نهان‌کاوی از یک منحنی مشخصه عملکرد گیرنده[7] معروف به منحنی ROC که نشان دهنده تغییرات نرخ تشخیص مثبت نادرست f_p در مقابل نرخ تشخیص مثبت درست t_p است، استفاده می‌شود [۱ و ۲]. این کار را با استفاده از ۵۰۰۰ تصویر، بر طبق نرخ‌های جاسازی متفاوت، بر اساس سطح زیر منحنی ROC هر یک، معروف به AUC[8] در جدول (۵) به نمایش گذاشته می‌شود. مساحت زیر منحنی ROC یا همان AUC در واقع نشان دهنده احتمال تشخیص مثبت درست[9] (P_{detect}) است [۲۱] که با استفاده از رابطه (۱۸) قابل محاسبه است.

$$p_{detect} = 1 - p_{error} \quad (۱۷)$$

$$p_{error} = \frac{1}{2} \times P_{FP} + \frac{1}{2} \times p_{FN} \quad (۱۸)$$

که در آن، P_{FP} و P_{FN} به ترتیب برابر احتمال تشخیص مثبت نادرست و احتمال تشخیص منفی نادرست است. مقدار p_{detect}=۰/۵ نشان می‌دهد که تشخیص طبقه‌بندی کننده در شناسایی نهانه از پوشانه معادل یک روند تصادفی است. به عبارتی نشان دهنده امنیت کامل الگوریتم نهان‌نگاری است. در مقابل $p_{detect} = 1$ نیز نشان دهنده این است که طبقه‌بندی کننده دارای دقت کامل 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 گذاشته شده است.

جدول ۵. مقایسه احتمال تشخیص صحت p_{detect} یا AUC

الگوریتم پیشنهادی	Edge xor Coding	EAMR	نرخ جاسازی (٪)
۰/۵۲۶۶	۰/۵۳۴۴	۰/۵۴۲۱	۵
۰/۵۵۶۱	۰/۵۶۶۲	۰/۵۷۶۱	۱۰
۰/۵۷۸۸	۰/۵۹۴۶	۰/۶۰۳۲	۱۵
۰/۵۹۴۴	۰/۶۱۴۴	۰/۶۳۲۸	۲۰
۰/۶۰۱۸	۰/۶۲۴۰	۰/۶۶۲۹	۳۰

۶. نتیجه‌گیری

در این مقاله یک روش نهان‌نگاری امن و مقاوم تصویر بر اساس واقعیت مربوط به حساسیت کمتر سیستم بینایی انسان نسبت به تغییرات در مناطق زبر تصویر طراحی شد. در الگوریتم پیشنهادی، با استفاده از آنتروپی گراف متناظر پنجره‌های ناهم‌پوشان ۳×۳ تصویر، معیاری کارآمد برای شناسایی مناطق زبر تصاویر خاکستری ارائه گردید. سپس با استفاده از این معیار و یک روش جاسازی پیام ترکیبی مرکب از xor coding و ELSB2 یک الگوریتم امن و کارآمد طراحی شد که مهم‌ترین ویژگی‌های آن عبارتند از: ۱- پیکسل‌های متناظر انتخاب شده در پوشانه برای جاسازی و در نهانه برای استخراج بیت‌های پیام مخفی سازی شده، کاملاً یکسان است. ۲- کلیه پیکسل‌های هر پنجره در جهت همه پیکسل‌های همسایه (۸- همسایگی) در این معیار دخالت دارند. ۳- این الگوریتم علاوه بر استفاده از تطبیق در انتخاب پیکسل‌های مناسب جاسازی، از یک الگوریتم شبه تصادفی نیز برای افزایش امنیت برخوردار است ۴- آستانه زبری یا آستانه جاسازی برای هر برای هر تصویر مطابق طول پیام M، طوری تعیین می‌شود که پیام در سراسر تصویر پخش شده و مخفی شود. ۵- این روش با دقت بالایی که دارد به هیچ وجه اجازه جاسازی پیام در پنجره‌های صاف را نمی‌دهد. ۶- همان‌طوری که شبیه‌سازی‌ها نشان می‌دهد، جدول (۴)، این الگوریتم با وجود اینکه بیت‌های پیام را در LSB2 پیکسل‌ها جاسازی می‌کند، میزان تخریبی که در پوشانه ایجاد می‌کند، بسیار نزدیک به روش‌هایی است که از LSB1 استفاده می‌کنند. ۷- این الگوریتم برای حوزه مکان طراحی شده است که توازن خوبی بین سه معیار ارزیابی یعنی نرخ جاسازی، رؤیت ناپذیری و امنیت، برقرار نموده است. در پایان با شبیه‌سازی روی پایگاه داده

[1] Targeted
[2] Blind or Universal
[3] Training
[4] Test
[5] Spatial Rich Model
[6] Ensemble Classifier
[7] Receiver Operating Characteristic Curve
[8] Area Under Curve
[9] Detection Accuracy

Archive of SID

www.SID.ir

Downloaded from adst.ir at 14:14 +0330 on Monday February 26th 2018

بزرگی شامل ۵۰۰۰ تصویر طبیعی، نتایجی به‌دست آمده است که دلیل بر کارآمدی الگوریتم پیشنهادی است. از لحاظ کیفی حتی برای نرخ جاسازی ٪۳۰ مقدار wPSNR بیش از ۶۰ است که مقدار قابل قبولی است. همچنین در ارزیابی توسط الگوریتم نهان‌کاوی SRM روی همین نرخ جاسازی، مقدار AUC یعنی احتمال تشخیص حدود ۰/۶۰ 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 تعمیم داد یا با اعمال الگوریتم شبه تصادفی، به نحو مطلوب‌تر، به بهبود این الگوریتم نهان‌نگاری پرداخت.

۷. مراجع

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

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

[3] Wu, D. C.; Tsai, W. H. "A Steganographic Method for Images by Pixel Value Differencing"; Pattern Recognition Letters 2003, 24, 1613–1626.

[4] Filler, T.; Fridrich, J. "Gibbs Construction in Steganography"; IEEE Trans. Inform. Forensics and Security 2010, 5, 705–720.

[5] Zhang, X.; Wang, S. "Vulnerability of Pixel-Value Differencing Steganography to Histogram Analysis and Modification for Enhanced Security"; Pattern Recogn. Lett. 2004, 25, 331–339.

[6] Yang, C-H.; Weng, C-Y.; Wang, S-J.; Sun, H-M. "Adaptive Data Hiding in Edge Areas of Images with Spatial LSB Domain Systems"; IEEE Trans. Inf. Forensics Security 2008, 3, 488–497.

[7] Bin, L.; Junhui, He.; Jiwu, H.; Yun, Q. S. "A Survey on Image Steganography and Steganalysis"; Ubiquitous Int. J. Inform. Hiding and Multimedia Signal Processing 2011, 2, 2073-4212.

[8] Mielikainen, J. "LSB Matching Revisited"; IEEE Signal Processing Letters 2006, 13, 285-287.

[9] Luo, W.; Huang, F.; Huang, J. "Edge Adaptive Image Steganography Based on LSB Matching Revisited"; IEEE Trans. Inf. Forensics Security 2010, 5, 201–214.

[10] Mustafa, A. E.; Elgamal, A. M. F. ElAlmi, M. E.; Ahmed, B. D. "A Proposed Algorithm for Steganography in Digital Image Based on Least Significant Bit"; Research J. Specific Education Faculty of Specific Education, Mansoura University, 2011, 21, 752-767.

[11] Shamalizade, M. A.; Norozi, Z.; Karami, M. R. "A New Algorithm for Embedding Message in Image Steganography"; Int. J. Eng. Res. Technol. 2014, 3, 2278 – 0181.

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

[13] Westfeld, A. "High Capacity despite Better Steganalysis (F5–A Steganographic Algorithm)"; Moskowitz, I. S. (eds.): Information Hiding. 4 the Int. Workshop. Lecture Notes in Computer Science, Springer-Verlag, Berlin Heidelberg New York, 2001, 2137, 289– 302.

[14] Al-Dmour, H.; Al-Ani, A. "A Steganography Embedding Method Based on Edge Identification and XOR Coding"; Elsevier, Science Direct, 2016, 46, 293-306.

[15] Pun, T. "A New Method for Gray-Level Picture Thresholding Using the Entropy of the Histogram"; Signal Processing, 1980, 2, pp. 223-237.

[16] Guanghua, G. U.; Zhao, Yao; Zhenfeng, Zhu. "Integrated Image Representation Based Natural Scene Classification"; Elsevier; Expert Systems with Applications, 2011, 38, 11273–11279.

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

[18] Malmberg, F. "Graph Based Method for Interactive Image Segmentation"; Digital Comprehensive Summaries of Uppsala Dissertations from the Faculty of Science and Technology 2011, 813, 51-59.

[19] Chen, Z.; Dehmer, M.; Shi, Y. "A Note on Distance-Based Graph Entropies"; J. Entropy 2014, 16, 5416-5427.

[20] Dehmer, M.; Mowshowitz, M. "A History of Graph Entropy Measures"; Information Science 2011,181, 57-78.

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

Archive of SID

www.SID.ir