پنهان‌شکنی تصویر براساس ویژگیهای ماتریس هم‌وقوعی

مجتبی ابوالقاسمی[1] حسن آقائی‌نیا[2] کریم فائز[3]
۱- دانش‌آموخته کارشناسی ارشد، دانشکده مهندسی برق - دانشگاه صنعتی امیرکبیر- تهران- ایران
mo_abolghasemi@aut.ac.ir
۲- دانشیار، دانشکده مهندسی برق - دانشگاه صنعتی امیرکبیر - تهران- ایران
aghaeini@aut.ac.ir
۳- استاد، دانشکده مهندسی برق- دانشگاه صنعتی امیرکبیر - تهران- ایران
kfaez@aut.ac.ir

چکیده: در این مقاله دو روش پنهان‌شکنی جدید بر اساس ماتریس هم‌وقوعی تصویر ارائه شده است. نشان داده شده است که با استفاده از ویژگیهای استخراج شده از این ماتریس می‌توان تمایز بین تصاویر پوشانه و گنجانه را انجام داد. این ویژگیها شامل انرژی، انتروپی، تباین، گشتاور تفاضل معکوس، بیشینه احتمال و هم‌بستگی است. با استفاده از دسته‌بندی کنندهٔ SVM، جداسازی تصاویر گنجانه و پوشانه انجام گردید. در روش دوم عناصر قطری ماتریس هم‌وقوعی مستقیما به عنوان ویژگی استفاده شده و برای کاهش ابعاد ویژگی نیز ایده حذف تعدادی از بیتهای با ارزش قبل از محاسبه ماتریس هم‌وقوعی بکار گرفته شد. آزمایشاتی بر روی ۱۸۰۰ تصویر برای آلگوریتمهای پنهان‌نگاری LSB و LSB وفقی (LSBM) با نرخهای مختلف انجام گردید. چند روش پنهان‌شکنی نیز جهت مقایسه پیاده گردید و برای مقایسه بر روی پایگاه تصویر یکسان آزمایش شد. بررسی های انجام شده نشان می‌دهد روشهای پیشنهادی برای پنهان‌شکنی نسبت به روشهای قبلی نتایج بهتری را بدست می‌دهد و ویژگیهای در نظر گرفته شده برای پنهان‌شکنی مناسب می‌باشند.

کلمات کلیدی: پنهان‌نگاری، پنهان‌شکنی، ماتریس هم‌وقوعی, درج **LSB** و **LSB** وفقی.

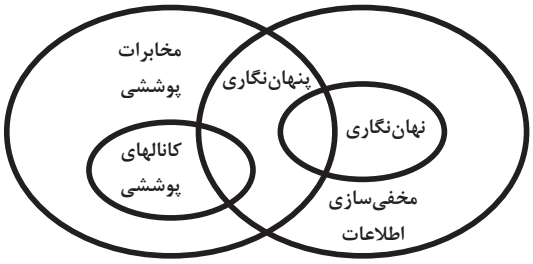
تاریخ دریافت مقاله : ۱۳۸۷/۷/۲۶
تاریخ پذیرش مقاله : ۱۳۸۸/۸/۵
نام نویسنده‌ی مسئول : مجتبی ابوالقاسمی
نشانی نویسنده‌ی مسئول : ایران – تهران - میدان نوبنیاد - شهرک شهید چمران بلوک ۱۹ طبقه ۵ واحد ۸

۱- مقدمه

طی سالها مخفی‌سازی اطلاعات[1] از حالت هنر نوشتن پوششی به زمینهٔ علمی برای تحقیقات تبدیل شده است. ایدهٔ کلی مخفی‌کردن اطلاعات در محتوای دیجیتال, کلاس وسیعتری است که کاربردهایی خارج از حیطهٔ پنهان‌نگاری را نیز شامل می‌شود [1]. روشهای مخفی‌سازی اطلاعات شامل دو کلاس عمدهٔ نهان‌نگاری[2] و پنهان‌نگاری[3] است (شکل ۱). از یک دیدگاه کلی، نهان‌نگاری را می‌توان به دو نسل تقسیم نمود [2]. نسل اول[4] روشهایی هستند که معمولاً روی کل حوزه رسانه انجام می‌شود. این روشها معمولاً در حوزه‌های مکانی و یا تبدیل (مانند DWT،DCT) عمل درج پیام صورت می‌گیرد و در مقابل حملاتی که هندسهٔ رسانه را تحت تاثیر قرار نمی‌دهند مقاومت خوبی دارند. اما معمولاً در مقابل حملات و پردازشهای هندسی مانند چرخش، مقیاس کردن و انتقال، به علت از دست رفتن انطباق در زمان آشکارسازی علامت، کارایی کمتری دارند. نسل دوم نهان‌نگاری روشهایی است که به منظور افزایش مقاومت و نامرئی بودن و غلبه بر مشکلات نسل اول بر اساس ویژگیهای ناحیه‌ای[5]، یا آلگوریتمهای همزمان کننده توسعه یافته‌اند [3].

هدف اصلی در نهان‌نگاری مقاوم کردن آلگوریتم در برابر حملات مختلف ذکر شده است و دو بحث امنیت و ظرفیت اهمیت کمتری دارد در حالی که در پنهان‌نگاری برعکس می‌باشد امنیت و ظرفیت هدف اصلی است. در واقع پنهان‌نگاری علم و هنر ارتباطات مخفی است. یک سامانه پنهان‌نگاری، پیام مخفی را در یک رسانه پوششی به گونه‌ای مخفی می‌سازد، که هیچ گمان و سوءظنی را جهت استراق‌سمع تحریک نکند. در گذشته مردم برای پوشش پیام از خالکوبی‌ها یا جوهرهای نامرئی در ارتباطات مخفی استفاده می‌کردند. در حال حاضر فن‌آوری‌های شبکه و رایانه، کانالهای ارتباطی سهل‌الوصولی را برای ارتباطات محرمانه فراهم نموده است.

در چند سال اخیر پنهان‌نگاری داده به یک زمینه تحقیقاتی فعالی تبدیل شده است که به دنبال آن زمینه جذاب دیگری تحت عنوان پنهان‌شکنی[6] نیز بوجود آمد. در واقع برای جلوگیری از هر گونه ارتباطات محرمانه از پنهان‌شکنی، با آشکارسازی وجود پیام مخفی در رسانه، (پنهان‌شکنی غیرفعال [4]) یا استخراج و ردیابی آن (پنهان‌شکنی فعال [5]) استفاده می‌گردد.



شکل(۱): ارتباط بین پنهان‌نگاری و مخفی‌سازی [1].

بطور کلی روشهای پنهان‌شکنی را می‌توان به دو دستهٔ کلی خاص[7] و عام[8] (کور[9]) تقسیم نمود. روشهای خاص برای آشکارسازی وجود پیام، برای یک روش خاص پنهان‌نگاری ارائه شده است از جمله این روشها می‌توان تشخیص جفت‌شدگی مقادیر پیکسلی (PoV)[10] [6] و یا RS[11] [7] را نام برد. در حالی که در روشهای عام سعی می‌شود قابلیت آشکارسازی وجود پیام برای مجموعه‌ای از روشهای پنهان‌نگاری ایجاد گردد. از جملهٔ این روشها می‌توان IQM[12] [8]، BSM[13] [9]، WBS[14] [10] و FBS[15] [11] را نام برد. در این روشها آمارگانهایی به عنوان ویژگی از پایگاه دادهٔ تصاویر پوشانه و گنجانه استخراج می‌گردد و با استفاده از دسته‌بندی‌کننده‌های SVM[16] یا FLD[17] عمل جداسازی پوشانه و گنجانه صورت می‌گیرد. در روشهای IQM و BSM به ترتیب از معیارهای کیفیت تصویر و معیارهای شباهت باینری به عنوان ویژگی استفاده شده است. این ویژگیها در روش WBS، گشتاورهای استخراج شده از زیربانده‌های تبدیل موجک می‌باشند و در روش FBS مجموعه ای از ضرایب DCT استخراج می‌گردد.

آقایان سالیوان[18] [12] و زُوان[19] [13] روشهایی را برای پنهان‌شکنی بر اساس ماتریس هم‌وقوعی ارائه نموده‌اند. هردو از عناصر ماتریس هم‌وقوعی به عنوان ویژگی استفاده کرده‌اند. آقای سالیوان تعداد ۱۲۹ عنصر ماتریس یعنی تعدادی از روی قطر اصلی (۶۳ عنصر) و تعدادی نیز از عناصر با بیشترین احتمال وقوع (۶۶ عنصر) به عنوان ویژگی استفاده نمود. او از این ویژگیها برای پنهان‌شکنی روشهای پنهان‌نگاری طیف گسترده استفاده نمود. آقای زُوان از عناصر قطر اصلی و دو قطر فرعی بالای قطر اصلی ماتریس هم‌وقوعی (یعنی ۱۰۱۸ عنصر) به عنوان ویژگی استفاده کرد. جهت کاهش ابعاد ویژگی نیز از روش CNPCA[20] را بکار برده است. ایشان نشان داده است که این روش پنهان‌شکنی LSB را به خوبی انجام می‌دهد ولی برای LSB وفقی نتایجی ارائه نشده است.

همانطور که خانم فردریک نیز ذکر کرده است [14], بهترین ویژگیها برای پنهان‌شکنی وقتی حاصل می‌گردد که مستقیما در حوزه درج شده محاسبه گردند. برای مثال برای تصاویر JPEG ویژگیها بایستی از ضرایبDCT به جای حوزه مکانی بدست آیند. این اصل با مقایسه چند روش پنهان‌شکنی عام در مراجع [16,15] تایید شده

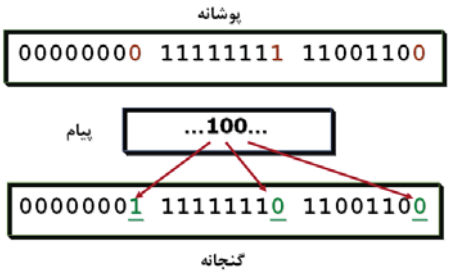
است. بنابراین پنهان‌شکنی عام با توجه به حوزه درج قابل تقسیم بندی است (یعنی پنهان‌شکنی حوزه مکانی و JPEG). با پذیرش این اصل در این مقاله ما بر روی پنهان‌شکنی روشهایی که در حوزه مکانی عمل درج را صورت می‌دهند متمرکز شده ایم. بنابراین نتایج نیز با نتایج روشهای پنهان‌شکنی مکانی مقایسه شده است.

در مقالات قبلی ما روشهایی برای پنهان‌شکنی روشهای پنهان‌نگاری LSB و LSBM بر اساس ویژگیهای استخراج شده از ماتریس هم‌وقوعی تصویر ارائه نموده‌ایم [17,18]. در این مقاله ضمن توسعه کارهای قبلی به دقت با روشهای پنهان‌شکنی که قبلا ارائه گردیده است, مقایسه شده است. در بخش بعدی روشهای درج مکانی شرح داده می شود. در بخش سوم مروری بر ماتریس هم‌وقوعی می‌شود، تاثیر روشهای درج مکانی LSB وفقی روی صفحات بیتی تصویر در بخش چهارم بررسی می‌گردد. در بخش پنجم روش استخراج ویژگیها برای دو روش پنهان‌شکنی پیشنهادی ارائه می‌گردد. نتایج تجربی بدست‌آمده و مقایسه با روشهای پنهان‌شکنی قبلی نیز در بخش ششم آورده شده است. در بخش پایانی نیز بحث و نتیجه‌گیری صورت گرفته است.

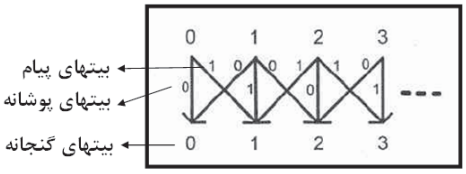
۲- پنهان‌نگاری مکانی

شناخته‌شده‌ترین آلگوریتم پنهان‌نگاری بر اساس لایه بیت کمترین ارزش[۲۱] تصویر می‌باشد که تحت عنوان روش LSB گفته می‌شود. این قبیل روشها از این واقعیت استفاد می‌کنند که لایه LSB تصویر شبیه نویز تصادفی است و تغییر آن اثری روی کیفیت تصویر ایجاد نمی‌کند. با توجه به شکل ۲، در روش LSB، بیت با کمترین ارزش پیکسلها با پیامی که باید ارسال شود جایگزین می‌شود. بیتهای پیام می‌تواند روی کل تصویر با به صورت تصادفی پخش شود و یا در محلهای خاصی از تصویر درج گردند. این کار باعث توزیع بیتها بصورت مساوی می‌شود بنابراین به طور متوسط فقط نصف LSBها تغییر می‌یابند.

در روش LSBM به جای جایگزینی بیتهای پیام، اگر بیت پیام با بیت LSB پیکسل تطابق داشته باشد هیچ عملی انجام نمی‌شود، در غیر اینصورت به صورت تصادفی مقدار یک واحد از پیکسل کم یا اضافه می‌شود (شکل ۳). برای روش LSB روشهای پنهان‌شکنی ارائه شده است اما برای روش LSBM هنوز روش جامعی که برای نرخهای پایین نیز جوابگو باشد هنوز ارائه نشده است و پنهان‌شکنی روش LSBM مشکلتر از LSB است [19].



شکل(۲): روش درج LSB [20].



شکل (۳): روش درج LSBM [21].

۳- ماتریس هم‌وقوعی

ماتریس هم‌وقوعی از سطوح خاکستری، GLCM[۲۲]، ابتدا توسط هارالیک[۲۳] معرفی شده است [22]. ماتریس هم‌وقوعی رخداد همزمان سطوح خاکستری مختلف را در موقعیتهای مکانی مشخص در تصویر را توصیف می‌نماید. از این ماتریس برای استخراج مشخصات آماری مرتبه دوم بافت استفاده شده است. یک ماتریس وقوع همزمان سطوح خاکستری G_d برای یک بردار جابجایی $d(d_x,d_y)$ به این صورت زیر تعریف می‌شود [15]:

$$G_d(i,j)=\left|((r,s),(t,v)\middle|I(r,s)=i,I(t,v)=j\right| \qquad (۱)$$

در آن $(r,s)(t,v)\in N\times N$ هستند و $(t,v)=(r+d_x,s+d_y)$ و $|.|$ عدد اصلی مجموعه است. عنصر (i,j)ام از ماتریس G_d، تعداد رویدادهای سطوح خاکستری i و j هستند که از هم به اندازه d فاصله دارند. به عنوان مثال شکل ۴-ب ماتریس GLCM را برای داده‌های ماتریس ۴-الف را نشان می‌دهد که در جهت صفر درجه و با یک همسایگی محاسبه شده است.

۴- میزان تاثیر درج پیام روی صفحات بیتی تصویر

از آنجایی که روشهای پنهان‌نگاری معمولاً بیتهای پیام را در بیتهای افزونه پوشانه درج می‌نمایند انتظار می‌رود که بیشتر تغییرات در اثر درج پیام روی بیتهای کم ارزش تصویر صورت پذیرد. برای تحقیق این موضوع ۱۰۰۰ تصویر گنجانه با روش LSB وفقی (LSBM) [15] مورد بررسی قرار گرفت. نرخهای درج متفاوت نیز در نظر گرفته شده و میزان تغییرات در صفحات بیتی روی ۱۰۰۰ تصویر متوسط‌گیری شده و نتایج در شکل ۵ آورده شده است. شکل ۵-الف میزان تغییرات بیتهای هر صفحه بیتی را نشان می‌دهد.

ملاحظه می‌شود برای بیتهای باارزش این مقدار به شدت کاهش می‌یابد. شکل ۵-ب درصد تغییرات در هر صفحه بیتی را نشان می‌دهد و در شکل ۵-ج نیز درصد تجمیعی این تغییرات را نمایش می‌دهد. از شکل ۵-ج ملاحظه می‌گردد بیش از ۹۰ درصد تغییرات در چهار بیت اول (کم ارزش) تصویر ایجاد می‌گردد.

1	2	4	8
1	3	5	5
5	5	7	1
6	7	1	2
8	1	2	5

(الف)

	1	2	3	4	5	6	7	8
1	0	3	1	0	0	0	0	0
2	0	0	0	1	1	0	0	0
3	0	0	0	0	1	0	0	0
4	0	0	0	0	0	0	0	1
5	0	0	0	0	2	0	1	0
6	0	0	0	0	0	0	1	0
7	2	0	0	0	0	0	0	0
8	1	0	0	0	0	0	0	0

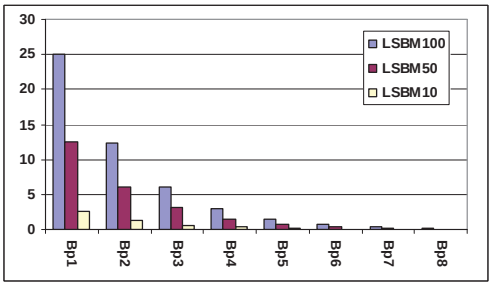
(ب)

شکل (۴): الف) مقادیر اعداد، ب) ماتریس GLCM

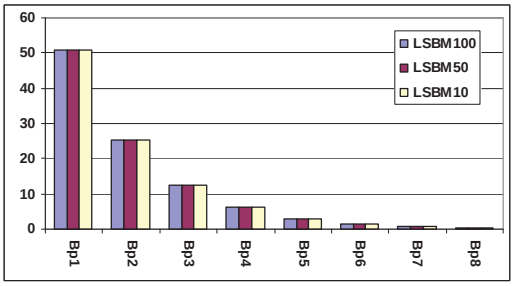
۵- روشهای پنهان‌شکنی پیشنهادی

۵-۱- پنهان‌شکنی بر اساس ویژگیهای ماتریس هم‌وقوعی

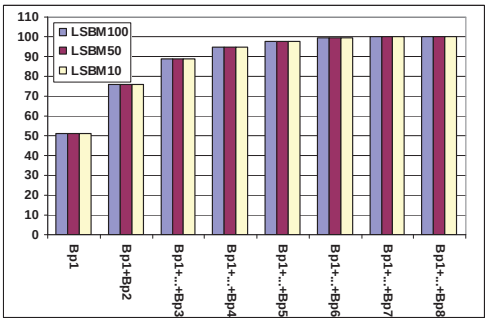
ماتریس هم‌وقوعی بر مبنای تخمین درجهٔ دوم مشروط تابع چگالی احتمال می‌باشند. ماتریس هم‌وقوعی یک تصویر طبیعی به صورت قطری توزیع می‌شود چون پیکسلهای مجاور همبستگی زیادی دارند. بعد از عمل درج به علت کاهش این همبستگی، تمرکز زیاد روی قطر اصلی ماتریس هم‌وقوعی کاهش یافته و پراکندگی روی آن ایجاد می‌شود [12]. این موضوع را می‌توان از شکل ۶ ملاحظه کرد.



(الف)



(ب)



(ج)

شکل (۵): تغییرات بیتهای پیکسلهای تصویر در اثر درج LSBM با نرخهای درج متفاوت، الف) متوسط میزان تغییر بیتها برای هر صفحه بیتی، ب) درصد تغییرات برای هر صفحه بیتی، ج) درصد تجمیعی تغییرات بیتها

پس از محاسبه ماتریسهای GLCM از روی هر تصویر ویژگیهایی استخراج گردیده و به عنوان بردارهای ویژگی جهت آموزش و آزمون استفاده می‌گردد. به عبارتی برای هر تصویر چهار ماتریس هم‌وقوعی G1، G2، G3 و G4 را در جهت‌های مختلف صفر، ۴۵، ۹۰ و ۱۳۵ درجه محاسبه می‌کنیم. از روی هر ماتریس هم‌وقوعی ویژگیهای زیر را استخراج می‌کنیم [23]:

$$E = \sum_{i,j} g_{ij}^2 \qquad (۲)$$

$$En = \sum_{i,j} g_{ij} \log g_{ij} \qquad (۳)$$

$$C = \sum_{i,j} |i-j| g_{ij}^2 \qquad (۴)$$

$$IDM = \sum_{\substack{i,j \\ i \neq j}} \frac{g_{ij}^2}{|i-j|} \quad (۵)$$

$$MP = \max(g_{ij}) \quad (۶)$$

$$Corr = \sum_{i,j} \frac{(i-\mu)(j-\mu)g_{ij}}{\sigma^2} \quad (۷)$$

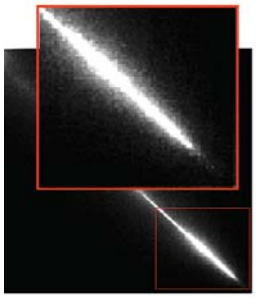
که در آن E: تابع انرژی، En: تابع انتروپی، C: تابع کنتراست، IDM[۲۴]: گشتاور تفاضل معکوس، MP[۲۵]: احتمال ماکزیمم و Corr: تابع هم‌بستگی است. پس از محاسبهٔ ویژگیها، از یک دسته‌بندی کننده برای آموزش و آزمون استفاده می‌گردد. بنابرین در مجموع ۲۴ ویژگی برای هر تصویر حاصل می‌گردد. این ویژگیها به عنوان ورودی دسته‌بند استفاده می‌گردد.

۵-۲- پنهان‌شکنی بر اساس حذف بیت و عناصر ماتریس هم‌وقوعی

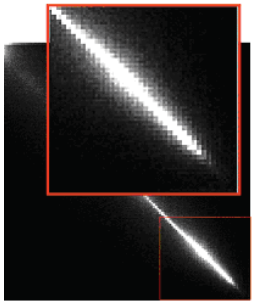
در اثر درج پیام در تصویر رخداد مقادیر پیکسلی در مجاور یکدیگر تغییر می‌کند و بنابراین تغییرات زیادی در ماتریس هم‌وقوعی ایجاد می‌گردد. با بکار بردن عناصر این ماتریس به عنوان ویژگی می‌توان بین پوشانه و گنجانه تمایز قائل شد. ماتریس هم‌وقوعی یک تصویر با ۸ سطح خاکستری یک ماتریس ۲۵۶*۲۵۶ عنصری (۶۵۵۳۶ عنصر) را بدست می‌دهد. استفاده از تمامی این عناصر ابعاد ویژگی را به شدت بالا می‌برد. همانطور که ملاحظه قبلا نیز ذکر گردید جهت کاهش ابعاد ویژگی سالیوان از ۱۲۹ عنصر این ماتریس و زُوان از ۱۰۱۸ عنصر ماتریس جهت پنهان‌شکنی استفاده نمودند.

در بخش ۴ نشان داده شد که بیشترین تغییرات در اثر درج پیام در بیتهای کم ارزش صورت می‌گیرد. بنابراین انتظار می رود با حذف بیتهای با ارزش[۲۶](MSB) تصویر قبل از محاسبه ماتریس هم‌وقوعی، اطلاعات مربوط به پیام (تغییرات ناشی از درج پیام) تا حد زیادی حفظ شود و در عین حال ابعاد ماتریس هم‌وقوعی به شدت کاهش یابد. برای مثال با حذف پنج بیت با ارزش تصویر ابعاد ماتریس هم‌وقوعی آن از ۶۵۵۳۶ به ۶۴ کاهش پیدا می‌کند. بنابراین p بیت با ارزش از تصویر را حذف نموده و چهار ماتریس هم‌وقوعی G1، G2، G3 و G4 را در جهت‌های مختلف صفر، ۴۵، ۹۰ و ۱۳۵ درجه محاسبه می‌نماییم و از روی آنها ماتریس G را بدست می‌آوریم:

$$G = (G1 + G2 + G3 + G4)/4 \quad (۸)$$



(الف)



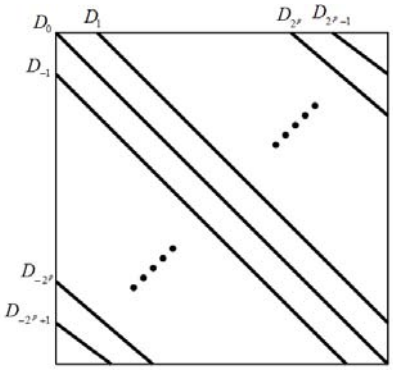
(ب)

شکل (۶): ماتریس هم‌وقوعی تصویر الف) تصویر پوشانه ب) تصویر گنجانه

به این ترتیب ابعاد این ماتریس $2^p \times 2^p$ خواهد بود (شکل ۷). بر خلاف روشهای سالیوان و زُوان ماتریس هم‌وقوعی با در نظر گرفتن تعداد رخدادهای نامتقارن محاسبه می‌کنیم. با توجه به شکل ۷ ما از کلیه عناصر ماتریس هم‌وقوعی به عنوان ویژگی استفاده می‌نماییم. در واقع اگر p صفحه بیتی در نظر گرفته شود با پشت سر هم قرار دادن عناصر قطری, بردار ویژگی به صورت زیر حاصل می‌گردد:

$$F = \{D_{-2^p+1}, ..., D_{-2}, D_{-1}, D_0, D_1, D_2, ..., D_{2^p+1}\} \quad (۹)$$

برای مثال اگر برای تعداد صفحه بیتی ۳, ۴, ۵ و ۶, ابعاد بردار ویژگی به ترتیب ۶۴, ۲۵۶, ۱۰۲۴ و ۴۰۹۶ خواهد بود.



شکل(۷): قطرهای ماتریس هم‌وقوعی به عنوان ویژگی

۶- نتایج تجربی

برای آزمون روشهای ارائه شده، پایگاه داده تصویر شامل ۱۸۰۰ تصویر مورد استفاده قرار گرفت. تعدادی از این تصاویر از اینترنت [25] گرفته شده و تعدادی نیز با دوربینهای دیجیتال توسط تیم ما از مناظر مختلف برداشت شده اند. این تصاویر با اندازه ۶۴۰*۴۸۰ پیکسل از مرکز تصاویر برش داده شده و به تصاویر با سطوح خاکستری تبدیل شدند. نمونه هایی از این تصاویر در شکل ۸ آورده شده است. با استفاده از آلگوریتمهای LSB با نرخهای درج مختلف ۰/۰۲، ۰/۱، ۰/۲، ۰/۳، ۰/۵، ۰/۷ و ۱ بیت بر پیکسل و همچنین آلگوریتم LSBM با نرخهای درج ۰/۱، ۰/۲ و ۰/۵ بیت بر پیکسل، تصاویر گنجانه بدست آمد. بنابراین در مجموع ۱۸۰۰۰ تصویر گنجانه حاصل گردید. با استفاده از آلگوریتمهای پیشنهادی بردارهای ویژگی را بدست آورده و از دسته‌بند SVM برای آزمونها استفاده نمودیم. در این آزمونها ما ابزار آماده LibSVM [26] با هسته[۲۷] گاووسی بکار برده و به صورت تصادفی نصف بردارها را برای آموزش و بقیه را برای آزمون استفاده نمودیم. نرخهای آشکارسازی درست پوشانه و گنجانه و نرخ آشکارسازی درست کلی را برای هر یک از نرخهای درج و ترکیب آنها بدست آوردیم که در ادامه نتایج ارائه شده است. این نتایج با ۱۰ تکرار دسته‌بندی و میانگین‌گیری حاصل شده است.

۶-۱- نتایج پنهان‌شکنی بر اساس ویژگیهای ماتریس هم‌وقوعی

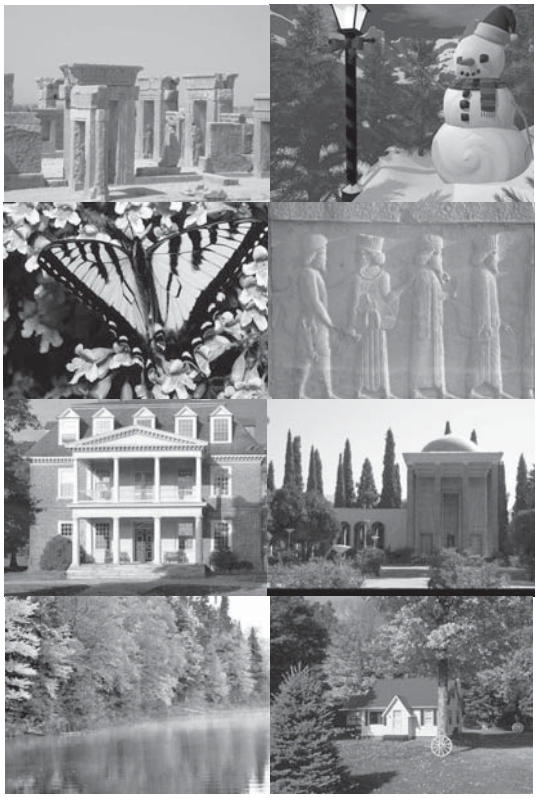
ابتدا روش ویژگیهای ماتریس هم‌وقوعی بر روی روش LSB با نرخهای درج مختلف به صورت مستقل آزمایش گردید که نتایج آن در جدول ۱ آورده شده‌اند. برای این منظور از ۹۰۰ تصویر برای آموزش و ۹۰۰ تصویر نیز برای آزمون استفاده شد. ملاحظه می‌گردد آلگوریتم توانسته است با دقت خوبی تصویر پوشانه و گنجانه را از یکدیگر جدا نماید.

در آزمایش دیگر از ۹۰۰۰ تصویر گنجانه ۱۵۰۰ تصویر را انتخاب نمودیم (برای هر آلگوریتم ۳۰۰ تصویر). در این آزمایش نیز به صورت تصادفی نصف تصاویر برای آموزش و نصف برای آزمون در نظر گرفته شد. نتایج این آزمایش در جدول ۱ ملاحظه می‌گردد. در این حالت نیز روش پیشنهادی با دقت مناسبی عمل می‌کند و نرخ ۹۸/۴ درصدی بدست می‌آید.

۶-۲- نتایج تجربی پنهان‌شکنی بر اساس عناصر ماتریس هم‌وقوعی و حذف بیت

به منظور اینکه کارایی روش ارائه شده را به ازای حذف صفحات بیتی مختلف آزمایش نماییم برای درج LSBM با نرخهای ۰/۱ تا ۱ بیت بر پیکسل آزمایشاتی انجام گردید. به عبارتی بردار ویژگی F با توجه به معادله ۹ برای هر تصویر به ازای حذف تعداد صفحات بیتی مختلف بدست آمد. در این آزمایشات برای حالتهای ۳، ۴ و ۵ صفحه بیتی کل عناصر بردار F به عنوان ویژگی انتخاب شدند و برای بیشتر از ۵ صفحه بیتی به علت افزایش بیش از حد ابعاد بردار ویژگی، این بردار به صورت زیر در نظر گرفته شد:

$$F = \{D_{-2}, D_{-1}, D_0, D_1, D_2\} \qquad (۱۰)$$



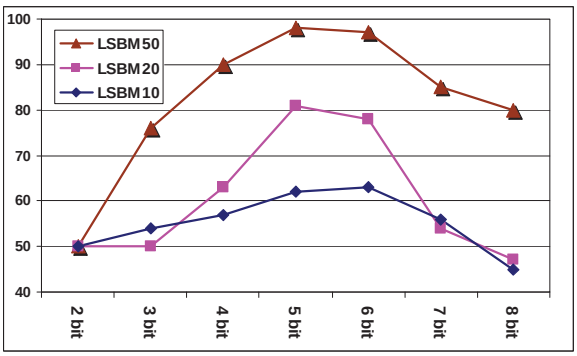
شکل ۸: نمونه‌هایی از تصاویر پایگاه داده

۹۰۰ بردار ویژگی پوشانه و بردارهای ویژگی گنجانه مرتبط به صورت تصادفی برای آموزش و ۹۰۰ بردار نیز برای آزمون انتخاب گردیدند. این نتایج برای نرخهای درج مختلف روش LSBM و تعداد صفحات بیتی متفاوت بدست آمد که در شکل ۹ آشکارسازی درست به ازای تعداد صفحات بیتی مختلف آورده شده است. در جدول ۲ نیز جزئیات مربوط به آشکارسازی درست به ازای ۵ و ۶ صفحه بیتی آورده شده است. از شکل ۹ ملاحظه می‌گردد که حذف صفحات بیتی با ارزش می‌تواند نرخ آشکارسازی درست را افزایش دهد اما حذف بیش از ۴ صفحه بیتی باعث از دست رفتن اطلاعات مربوط به درج پیام شده و نرخ خطا افزایش می‌یابد. بنابراین مصالحه ای بین حذف صفحات بیتی با ارزش و از دست رفتن اطلاعات پیام درج شده ایجاد می‌گردد. دیده می شود که برای حالت درج ۰/۱ bpp حذف دو صفحه بیتی

کمترین خطا را ایجاد نموده در حالی که برای حالتهای درج ۰/۲ bpp و ۰/۵ bpp حذف سه صفحه بیتی جوابهای بهتری بدست می‌دهد.

جدول(۱): نتایج روش پیشنهادی (ویژگیهای ماتریس هم‌وقوعی) برای آشکارسازی LSB با نرخهای درج مختلف (t=(tn+tp)/2).[۲۸]

نرخ آشکارسازی کل (t)	نرخ آشکارسازی پوشانه (tn)	نرخ آشکارسازی گنجانه (tp)	نرخ درج (bpp)
۹۲/۷	۹۹/۴	۸۶	۰/۲
۹۸/۶	۹۸/۸	۹۸/۴	۰/۳
۹۸/۷	۹۸/۶	۹۸/۸	۰/۵
۹۸/۸	۹۸/۶	۹۹	۰/۷
۹۹	۹۹/۱	۹۹/۱	۱
۹۸/۴	۹۷/۸	۹۹/۱	همه نرخهای درج



شکل (۹): نتایج آشکارسازی درست برای LSBM با نرخهای درج متفاوت و حالتهای مختلف حذف صفحات بیتی

جدول (۲): مقایسه دقت آشکارسازی برای پنهان‌شکنی LSBM با حذف بیتهای با ارزش (t=(tn+tp)/2)

حالت	LSBM (0.1 bpp)		
	tp	tn	t
5 bit	۵۵	۷۰	۶۲
6 bit	۵۶	۷۱	۶۳
حالت	LSBM (0.2 bpp)		
	tp	tn	t
5 bit	۸۴	۷۸	۸۱
6 bit	۷۳	۸۲	۷۸
حالت	LSBM (0.5 bpp)		
	tp	tn	t
5 bit	۹۹	۹۸	۹۸
6 bit	۹۹	۹۶	۹۷

آلگوریتم پیشنهادی دوم بر روی روشهای مختلف LSB با نرخهای درج مختلف ۰/۰۲، ۰/۱، ۰/۲، ۰/۵، ۰/۷ و ۱ بیت بر پیکسل بر روی روش درج LSB و با در نظر گرفتن فقط ۳ بیت کم ارزش به صورت مستقل آزمایش گردید که نتایج در جدول ۳ آورده شده‌اند. برای این آزمایشات نیز از ۹۰۰ تصویر برای آموزش و ۹۰۰ تصویر نیز برای آزمون و از دسته‌بندی کننده SVM استفاده شد. ملاحظه می‌گردد حتی برای نرخهای درج پایین نیز آلگوریتم توانسته است با دقت خوبی تصویر پوشانه و گنجانه را از یکدیگر جدا نماید.

در آزمایش دیگر برای نرخهای مختلف درج LSB (۰/۰۲ تا ۱ بیت بر پیکسل) ۱۸۰۰ تصویر گنجانه به صورت تصادفی انتخاب نمودیم (برای هر آلگوریتم ۲۵۷ تصویر). در این آزمایش نیز به صورت رندوم ۹۰۰ تصویر برای آموزش و ۹۰۰ تصویر برای آزمون در نظر گرفته شد. نتایج این آزمایش در جدول ۳ ملاحظه می‌گردد. در این حالت نیز روش پیشنهادی با دقت مناسبی عمل می‌نماید و نرخ ۹۴/۴ درصدی بدست می‌آید.

۶-۳- مقایسه نتایج با روشهای پنهان‌شکنی

به منظور مقایسه نتایج حاصله از دو روش پیشنهادی با روشهای پنهان‌شکنی قبلی ما روشهای فرید[۲۹] [27]، اَوکیباس[۳۰] [9] سالیوان [12] و زُوان [13] را پیاده نمودیم و بردارهای ویژگی را برای LSB با نرخهای درج ۰/۰۲ bpp و ۰/۱ و LSB وفقی بدست آوردیم. در اینجا نیز نصف بردارهای ویژگی برای آموزش و نصف دیگر برای دسته‌بند SVM استفاده گردید. نتایج مربوطه به ترتیب در جداول ۴ و ۵ آورده شده است. با مقایسه نتایج مشاهده می‌گردد نتایج حاصله برای دو روش پیشنهادی نسبت به روشهای پنهان‌شکنی که قبلا ارائه گردیده است، برتری قابل ملاحظه‌ای دارد.

برای LSBM نیز به ازای نرخهای درج ۰/۲ bpp و ۰/۳ همین کار صورت پذیرفته و در جدول ۳ نتایج ارائه شده‌اند. در این حالت نیز مشاهده می‌گردد نرخهای آشکارسازی درست برای دو روش پیشنهادی ما از نتایج سایر روشهای پنهان‌شکنی بیشتر می‌باشد.

۶-۴- مقایسه زمان محاسبه بردارهای ویژگی

جهت مقایسه سرعت آلگوریتمها به ازای ۱۰۰ تصویر مدت زمان استخراج ویژگیها را برای روشهای مختلف پنهان‌شکنی بدست آوردیم. نتایج این محاسبه در جدول ۶ آورده شده است. لازم به ذکر است که به جز کد برنامه روش BSM که به زبان C می‌باشد، بقیه برنامه‌ها با Matlab نوشته شده است و روی رایانه پنتیوم IV (۲/۸ GHz) اجرا گردیده‌اند. ملاحظه می‌گردد که زمان استخراج ویژگی برای این روشها تقریبا یکسان می‌باشد. بیشترین زمان را روشهای فرید و روش پیشنهادی اول دارند. زمان محاسبه ویژگیها برای روش پیشنهادی دوم

نسبت به سایر روشها به غیـر از زمـان محاسـبه BSM, قـدری کمتـر می‌باشد. البته زمان محاسبه BSM به دلیل اینکه بـه زبـان C نوشـته شده است کمتر می‌باشد.

جدول (۳): نتایج پنهان‌شکنی برای روش پیشنهادی دوم به ازای نرخهای درج مختلف LSB

نرخ درج (bpp)	tp	tn	t
۰/۰۲	۷۶/۴	۷۸/۲	۷۷/۳
۰/۱	۹۲/۶	۹۲/۶	۹۲/۶
۰/۲	۹۵/۱	۹۶/۷	۹۵/۹
۰/۳	۹۷/۲	۹۶/۳	۹۶/۸
۰/۵	۹۸	۹۸/۶	۹۸/۳
۰/۷	۹۹/۲	۹۹/۴	۹۹/۳
۱	۹۹/۳	۹۹/۶	۹۹/۴
نرخهای مختلف	۹۳/۸	۹۵/۱	۹۴/۴

۷- نتیجه‌گیری

در این مقاله دو روش بر اساس ماتریس هم‌وقـوعی جهـت تمـایز تصاویر پوشانه و گنجانه و انجام پنهان‌شکنی ارائه شد. در روش اول بـا استفاده از ویژگیهـای اسـتخراج شـده از مـاتریس هـم‌وقـوعی تصـویر پنهان‌شکنی روشهای LSB صورت گرفت که نشان داده شد با نرخهای درج مختلف نرخ آشکارسازی بیش از ۹۴ درصد حاصل مـی شـود. در روش پیشنهادی دوم از عناصر قطری ماتریس به عنوان ویژگی استفاده گردید و جهت کاهش ابعاد بردار ویژگی نیز بیتهـای کـم ارزش حـذف گردید. در واقع از آنجایی که بیشـتر اطلاعـات تصـویر در صـفحات بـا ارزش قرار دارند با حذف بیتهای با ارزش بـه نـوعی فرآینـد اسـتخراج ویژگیها نسبتا مستقل از محتوای تصویر می‌گـردد. از طرفـی ملاحظـه گردید که با این کار اثرات مربوط به درج پیـام از بـین نرفتـه و حفـظ می‌گردد. بنابراین می‌توان گفت نسبت سیگنال درج شده بـه سـیگنال تصویر افزایش می‌یابد و این موضوع باعث افزایش نرخهای آشکارسازی درست می‌گردد. نتایج تجربی نیز ایـن موضـوع را تاکیـد نمـود. ضـمن اینکه ابعاد ویژگی حاصله در حد قابـل قبـول جهـت دسـته‌بنـدی نیـز می‌باشد. روشهای پیشنهادی با روشهای پنهـان‌شـکنی کـه قـبلا ارائـه گردیده است بر روی پایگاه داده یکسان مقایسـه گردیـد و نشـان داده شد این روشها نتایج بهتری را فراهم نمـوده اسـت. در کارهـای آینـده قصد داریم با ترکیب نمودن این روشـها و بهبـود دادن روشـهای ارائـه شده برای نرخهای درج پایینتر از ۰/۱ بیت بر پیکسل (LSBM) نتایج آشکارسازی بهتری بدست آوریم. همچنین ایده حذف بیتهای بـا ارزش را قبل از محاسبه ویژگیها بخصوص جهت پنهان‌شکنی تصـاویر JPEG آزمایش خواهیم نمود.

جدول (۴): مقایسه نتایج دسته‌بندی برای پنهان‌نگاری LSB و نرخهای درج مختلف ۰/۰۲ و ۰/۰۵ بیت بر پیکسل

روش پنهان‌شکنی	نرخ درج (bpp)	tn	tp	t
فرید	۰/۱	۵۱	۵۵	۵۳
	۰/۰۲	۴۲	۵۸	۵۱
سالیوان	۰/۱	۵۳	۴۹	۵۲
	۰/۰۲	۵۳	۴۷	۵۰
زُوان	۰/۱	۸۱	۸۵	۸۳
	۰/۰۲	۷۲	۷۸	۷۵
آوکیباس	۰/۱	۵۷	۶۳	۶۰
	۰/۰۲	۵۲	۵۸	۵۴
روش پیشنهادی ۱	۰/۱	۸۲	۸۸	۸۵
	۰/۰۲	۸۲	۸۰	۸۱
روش پیشنهادی ۲	۰/۱	۸۴	۹۲	۸۸
	۰/۰۲	۷۶	۷۸	۷۷

جدول (۵): مقایسه نتایج دسته‌بندی برای پنهان‌نگاری LSB وفقی و نرخهای درج مختلف ۰/۲ و ۰/۳ بیت بر پیکسل

روش پنهان‌شکنی	نرخ درج (bpp)	tn	tp	t
فرید	۰/۳	۳۷	۹۱	۶۴
	۰/۲	۲۳	۸۹	۵۶
سالیوان	۰/۳	۵۶	۷۴	۶۵
	۰/۲	۴۵	۶۲	۵۳
زُوان	۰/۳	۸۱	۸۹	۸۵
	۰/۲	۷۲	۷۸	۷۵
آوکیباس	۰/۳	۷۲	۷۸	۷۵
	۰/۲	۵۸	۶۶	۶۲
روش پیشنهادی ۱	۰/۳	۸۶	۸۸	۸۷
	۰/۲	۷۵	۸۱	۷۸
روش پیشنهادی ۲	۰/۳	۹۱	۹۳	۹۲
	۰/۲	۸۴	۷۸	۸۱

سپاسگزاری

این تحقیق تحت حمایتهای مادی و معنوی گروه صـنایع فضـایی صاایران و مرکز تحقیقات مخابرات ایـران (ITRC) قـرار گرفتـه اسـت. همچنین نویسندگان از آقای دکتر خـرّازی جهـت فـراهم نمـودن کـد برنامه BSM تشکر می نمایند.

جدول (۶): مقایسه سرعت محاسبه ویژگیها برای روشهای پنهان‌شکنی مختلف

روش پنهان‌شکنی	زمان محاسبه برای ۱۰۰ تصویر (ثانیه)	زمان محاسبه برای یک تصویر (ثانیه)
فرید	۴۳/۷	۴/۳۷
سالیوان	۳۴/۶	۳/۴۶
زُوان	۳۷/۳	۳/۷۳
اوکیباس	۱۶/۵	۱/۶۵
روش پیشنهادی ۱	۴۹/۱	۴/۹۱
روش پیشنهادی ۲	۳۲/۴	۳/۲۴

مراجع

[1] Mehdi Kharrazi, Husrev T. Sencar, and Nasir Memon, “Image Steganography: Concepts and Practice” WSPC/Lecture Notes Series, pp. 22-28, (2004).

[2] Chun-Shien Lu, Multimedia Security: Steganography and Digital Watermarking Techniques for Intelectual Property, IDEA GROUP PUBLISHING (2004).

[۳] ابوالقاسمی م.، آقائی‌نیا ح. "نهان‌نگاری تصاویر دیجیتال بر اساس ثبت تصویر و مقاوم در مقابل حملات RST" چهارمین کنفرانس انجمن رمز ایران، ص. ۱۲۶-۱۳۲، مهرماه ۱۳۸۶.

[۴] ابوالقاسمی م.، آقائی‌نیا ح. " پنهان شکنی تصویر بر اساس گشتاورهای زرنیک " پانزدهمین کنفرانس مهندسی برق ایران، ص. ۲۰-۱۵، ۲۸-۲۵ اردیبهشت ۸۶.

[5] R. Chandramouli, "A mathematical framework for active steganalysis", Multimedia Systems © Springer-Verlag, pp. 303–311 (2003).

[6] A. Ker “Quantitive evaluation of pairs and RS steganalysis,” in Proc. SPIE Security, Steganography,Watermarking Multimedia Contents, vol. 5306, E. J. Delp III and P. W. Wong, Eds., 2004, pp. 83–97.

[7] Jessica Fridrich, MiroslavGoljan, RuiDu “Detecting LSB Steganography in Color and Grayscale Images”, Multimedia and Security IEEE, pp.22-28 (2001).

[8] I. Avcibas, N. Memon, and B. sankur. “Steganalysis using image quality metrics”. Security and Watermarking of Multimedia Contents, San Jose, Ca., pp.221-229, (2001).

[9] I. Avcibas, M. Kharrazi, N. Memon, and B. Sankur. “Image steganalysis with Binary Similarity Measures”, to appear in EURASIP Journal on Applied Signal Processing, pp.645-648, (2005).

10] S. Lyu and H. Farid. “Detecting hidden messages using higher-order statistics and support vector machines.” 5th International Workshop on Information Hiding., pp. 31-35 (2002).

[11] J. Fridrich. “Feature-based steganalysis for jpeg images and its implications for future design of steganographic schemes”. Proc. 6th Information Hiding Workshop, Toronto, Canada, pp. 1007-1020, (2004).

[12] K. Sullivan, U. Madhow, S. Chandrasekaran, and B.S. Manjunath, “Steganalysis of Spread Spectrum Data Hiding Exploiting Cover Memory”, SPIE2005, vol. 5681, pp. 38-46, (2005).

[13] Guorong Xuan, Yun Q. Shi, Cong Huang, Dongdong Fu, Xiuming Zhu, Peiqi Chai, and Jianjiong Gao, "Steganalysis Using High-Dimensional Features Derived from Co-occurrence Matrix and Class-Wise Non-Principal Components Analysis (CNPCA)", IWDW 2006, LNCS 4283, pp. 49 – 60, (2006).

[14] M. Goljan, J. Fridrich, and T. Holotyak, “New blind steganalysis and its implications,” in Security, Steganography, and Watermarking of Multimedia Contents VIII, ser. Proceedings of SPIE, vol. 6072, pp. 607 201–1, (2006).

[15] Mehdi Kharrazi, Husrev T. Sencar, Nasir Memon, "Performance study of common image steganography and steganalysis techniques" Journal of Electronic Imaging 15(4), 041104, pp. 1-16, (2006).

[16] T. Pevny and J. Fridrich, “Towards Multi-Class Blind Steganalyzer for JPEG Images,” International Workshop on Digital Watermarking, LNCS vol. 3710, Springer-Verlag, pp. 39–53, 2005.

[۱۷] ابوالقاسمی م.، آقائی‌نیا ح. فائز ک.، مهرابی م. ع.، "پنهان شکنی تصویر بر اساس ویژگیهای ماتریس هم‌وقوعی" شانزدهمین کنفرانس مهندسی برق ایران، ۱۳۸۷ (ICEE2008).

[18] M. Abolghasemi, H. Aghainia, K. Faez, M. A. Mehrabi, ” Steganalysis of LSB Matching Based on Co-Occurrence Matrix and Removing Most Significant Bit Planes”, IIHMSP2008, China, pp.135-138, (2008).

[19] Andrew D. Ker, "Steganalysis of LSB Matching in Grayscale Images" IEEE Signal Processing Letters, VOL. 12, NO. 6, pp. 441-444, (2005).

[20] J. Harmsen and W. Pearlman, “Steganalysis of additive noise modelable information hiding,” in Security and Watermarking of Multimedia Contents. vol. 5020 of Proc. of SPIE, pp. 131–142, (2003).

[۲۱] مهدوی م.، سماوی ش.، اخوت م.، اکرمی ص. " **روش پنهان‌نگاری تطبیقی بر پایه اغتشاش جمع شونده**" پانزدهم ین کنفرانس مهندسی برق ایران، ص. ۱۱۴-۱۰۸، اردیبهشت ۸۶.

[22] R. M. Haralick, K.Shanmogam, and I. Distein, " Texture Features for Images Classification," IEEE Tean. Sys. Man Cybernetics, vol. 3, pp. 610-621, 1973, Proceeding of the IEEE, vol. 67, no. 5, pp 786-804, (1979).

[23] Erkki Oja and Kimmo Valkealahti, ”Compressing higher-order co-occurrences for texture analysis using the Self-organizing Map”, Neural Networks, Proceedings. vol.2, pp.1160-1164, (1995).

[24] David A. Clausi and M. Ed Jernigan, 'A Fast Method to Determine Co-Occurrence Texture Features" IEEE Transactions On Geoscience And Remote Sensing, Vol. 36, No. 1, pp.298-300, (1998).

[25] http://www.freefoto.net.

[26] C.-C. Chang and C.-J. Lin, "LIBSVM: a library for support vector machines," 2001. Software available at http://www.csie.ntu.edu.tw/~cjlin/libsvm.

[27] Farid H.: Detecting hidden messages using higher-order statistical models. Proceeding of the IEEE International Conference on Image Processing, Vol. II, New York, pp. 905 – 908, (2002).

زیرنویس‌ها

[1] Information Hiding
[2] Watermarking
[3] Steganography
[4] First Generation Watermarking (1GW)
[5] Region
[6] Steganalysis
[7] Specific
[8] Universal
[9] Blind
[10] Pairs of Values
[11] Regular/Singular
[12] Image Quality Metrics
[13] Binary Similarity Measure
[14] Wavelet Based Steganalysis
[15] Feature Based Steganalysis
[16] Support Vector Machine
[17] Fisher Linear Discrimination
[18] Sullivan
[19] Xuan
[20] Class-Wise Non-Principal Components Analysis
[21] Least Significant Bit
[22] Gray Level Co-Occurrence Matrix
[23] Haralick
[24] Inverse Difference Moment
[25] Maximum Probability
[26] Most Significant Bits
[27] Kernel
[28] tp: true positive, tn: true negative
[29] Farid
[30] Avcibas