نهان‌کاوی در تصاویر JPEG بر مبنای دسته‌بندی ویژگی‌های آماری و تصمیم‌گیری دو مرحله‌ای

مریم بیگ‌زاده ، محمد رضایی و فاطمه‌السادات جمالی دینان
پژوهشکده پردازش هوشمند علائم

چکیده

در این مقاله روش جامعی برای نهان‌کاوی در تصاویر JPEG معرّفی می‌شود. در این روش پس از بررسی دقیق اثر فرآیندهای پنهان‌نگاری گوناگون بر مشخصّات آماری تصویر، ویژگی‌های بهینه‌ای از تصویر استخراج می‌شود که توانایی بالایی در ایجاد تمایز بین دو گروه تصاویر طبیعی و پنهان‌نگار دارند. علاوه بر استخراج ویژگی‌های بهینه، در یک تصمیم‌گیری سلسله‌مراتبی دقّت تشخیص به‌شکل قابل توجهی افزایش یافته است. در این مقاله نشان می‌دهیم که آمارگان مرتبهٔ اوّل ضرایب DCT (مانند هیستوگرام) بیشتر در حمله به روش‌های پنهان‌نگاری جای‌گذاری در LSB (مانند JSTEG، OUTGUESS، JPHide&Seek و StegHide) موفق‌تر از آمارگان مرتبهٔ دوم (مانند انواع همبستگی‌ها) عمل می‌کنند. همچنین مشخصات آماری مرتبهٔ دوم در تشخیص سایر روش‌های پنهان‌نگاری در حوزهٔ ضرایب DCT (بالاخص روش‌های تطبیق LSB، روش MB1، SSIS و روش مبتنی بر کوانتیزیشن) عملکرد بهتری از مشخصّات آماری مرتبهٔ اوّل دارند. علاوه بر آن، روش نهان‌کاوی معرفی شده با نگاه جامع به انواع روش‌های پنهان‌نگاری موجود، مشخّص می‌کند که نقاط ضعف هر یک در مقابل حملات آماری گوناگون چیست و چگونه می‌توان به روش‌های جاسازی امن‌تر دست پیدا کرد. نتایج تجربی نشان می‌دهد که دقّت این روش در مقایسه با روش‌های رقیب، بهتر بوده و در عین حال از جامعیت و تعمیم‌پذیری بالاتری برخوردار است. آزمایش‌ها روی مجموعهٔ دوهزارتایی از تصاویر JPEG با ضرایب کیفیت متنوع انجام شده و روش معرفی شده، قادر بوده است که شش روش پنهان‌نگاری معمول (JSteg، OutGuess، F5، MB1، Sequential LSB matching و Random LSB Matching) را با دقّت بیش از ۸۰٪ در نرخ‌های جاسازی بیش از ۲۰٪ تشخیص دهد. طبقه‌بندی‌کننده‌های مورد استفاده برای طبقه‌بندی از نوع SVM هستند.

کلیدواژه‌ها: نهان‌کاوی تصاویر *JPEG*، حمله به پنهان‌نگاری، جای‌گذاری در *LSB*، تطبیق *LSB*، دسته‌بندی ویژگی‌ها.

۱- مقدمه

پنهان‌نگاری عبارت است از هنر جاسازی یک پیغام پنهانی در یک رسانهٔ دیجیتال (به‌خصوص در هنگام عبور از یک شبکهٔ اطّلاعاتی مانند اینترنت)، به‌نحوی که تشخیص آن به سهولت امکان‌پذیر نباشد [۱]. در چند سال اخیر شاهد پیشرفت‌های زیادی در ارائهٔ انواع روش‌های پنهان‌نگاری بوده‌ایم. در مقابل، روش‌های حمله به رسانه‌های مشکوک (نهان‌کاوی) نیز به همین سرعت در حال پیشرفت و گسترش هستند [۲]. نهان‌کاوی در اغلب موارد عبارت است از تشخیص وجود یا عدم پیغام پنهانی در یک رسانهٔ دیجیتال (در اینجا تصویر). از این نظر نهان‌کاوی می‌تواند نوعی مسألهٔ طبقه‌بندی تلقی شود.

از میان انواع ساختار[1]های تصویری، فرمت JPEG به‌دلایل متعددی از محبوبیت بیشتری در تبادل اطلاعات تصویری برخوردار است. این فرمت متداول‌ترین روش برای ذخیره‌سازی تصاویر و عکس‌های مناظر طبیعی محسوب می‌شود. این مسأله به دو علت محقق شده است: ۱) توانایی حفظ کیفیت بصری تصویر، ۲) ایجاد امکان فشرده‌سازی با نرخ بالا. درنتیجه تصاویر JPEG، اغلب تصاویری با کیفیت بصری مطلوب و در مقایسه با فرمتی مانند BMP دارای حجم کمی هستند. در بررسی ساده‌ای که با یک جستجو در

1 Image formats

گوگل انجام دادیم، مشخص گردید که حدود ۴۴٪ از کلّ تصاویر موجود در اینترنت از نوع JPEG، ۳۳% از نوع Gif، ۲۲% از نوع PNG و ۱٪ از نوع BMP (و سایر فرمت‌ها) هستند. این آمار که توسط سایر محققان نیز به شیوه‌های دیگری تأئید می‌شود، اهمیت و میزان بالای تبادل تصاویر JPEG را در سطح اینترنت مشخّص می‌کند. از این‌رو تاکنون روش‌های متعددی برای پنهان‌نگاری در تصاویر JPEG معرّفی شده‌اند. به‌همین جهت، ارائهٔ یک روش نهان‌کاوی مناسب برای حمله به پنهان‌نگاری در تصاویر JPEG اهمّیت فوق‌العاده‌ای دارد، و هدف این تحقیق نیز معرفی روش نهان‌کاوی مناسبی برای حمله به پنهان‌نگاری در JPEG است.

محققان در حوزهٔ نهان‌کاوی، بیشتر به سوی ارائهٔ روش‌های همه‌جانبه و جامع نهان‌کاوی[1] روی آورده‌اند. این روش‌ها نوعی مسألهٔ طبقه‌بندی محسوب می‌شوند که در آن‌ها سعی می‌شود بردار ویژگی مناسبی از تصویر استخراج شود که به بهترین شکل ممکن قادر باشد اثر پنهان‌نگاری (اعوجاج ایجاد شده) را مستقل از روش و الگوریتم پنهان‌نگاری بازنمایی کند. مهم‌ترین ویژگی این روش‌های نهان‌کاوی این است که بر اساس شناسایی مشخصات آماری تصاویر دو گروه طبیعی و پنهان‌نگار، قادر هستند تصاویر پنهان‌نگاری شده با روش‌های نادیده را نیز تا حدّی تشخیص دهند و این برای یک نهان‌کاو بسیار ارزشمند است. علّت این امر آن است که هر روش پنهان‌نگاری با توجّه به تغییری که در تصویر اعمال می‌کند، بردار ویژگی استخراج شده را به سوی ناحیه‌ای از فضای ویژگی منحرف می‌کند که جدای از ناحیهٔ متناظر با تصاویر طبیعی است [۳]. به‌طورکلی می‌توان گفت ویژگی مناسب برای نهان‌کاوی، ویژگی است که دو شرط مهم را بر آورده کند [۴]:

۱. نسبت به پنهان‌نگاری حساس باشد.

۲. نسبت به محتوای خود سیگنال حامل[2] نسبتاً غیرحساس باشد.

با توجّه به دو نکتهٔ فوق، مشخص می‌شود بهترین ویژگی‌هایی که قادر هستند هر دو شرط فوق را در نهان‌کاوی تصاویر برآورد، ویژگی‌هایی است که از *تفاضل* مشخّصات آماری خود تصویر پوششی با مشخّصات آماری تصویر پنهان‌نگار حاصل شده باشد.

به‌طورکلّی از آن‌جا که انرژی سیگنال حامل (در اینجا تصویر پوششی) خیلی بزرگ‌تر از سیگنال پنهانی[3] (پیغام) است، تشخیص تغییرات جزئی ایجادشده در تصویر پنهان‌نگار کار ساده‌ای نیست. تغییرات ناشی از پنهان‌نگاری نسبت به تفاضل تصویر پنهان‌نگار و تصویر پوششی حساس‌تر است تا خود تصویر پوششی. بنابراین بسیار مطلوب خواهد بود اگر بتوانیم تصویر پوششی اصلی (حامل) را در دست داشته باشیم و سپس با محاسبهٔ تفاوت بین آن و تصویر پنهان‌نگاری شده به ویژگی حساس مورد نظر خود دست یابیم [۵].

امّا مسألهٔ اصلی این است که نهان‌کاو به‌طورمعمول به تصویر پوششی اولیه دسترسی ندارد. از این‌رو دست به تخمین رسانهٔ پوششی می‌زند. یکی از مهم‌ترین و مشهورترین روش‌های تخمین تصویر پوششی JPEG، روشی است که توسط *فریدریش* و همکاران وی [۶-۹، ۳، ۱] معرّفی شده و دراصطلاح کالیبراسیون[4] نام دارد. این روش، مشخصات آماری مرتبهٔ اول تصویر پوششی را با دقّت بسیار خوبی تخمین می‌زند. توضیحات بیشتر راجع به کالیبراسیون در بخش ۳-۳ ارائه خواهد شد.

علاوه بر دو نکتهٔ کلی مطرح شده راجع به ویژگی‌های مناسب برای نهان‌کاوی، مسألهٔ دیگر در تعریف و انتخاب ویژگی، بررسی اثر الگوریتم‌های مختلف پنهان‌نگاری روی تصویر است. شناسایی این اثرات و سپس تلاش برای کمّی سازی آن‌ها می‌تواند منجر به تعریف ویژگی‌های مؤثر گردد.

در مورد تصاویر JPEG، پنهان‌نگاری عمدتاً در ضرایب DCT کوانتیزه شده انجام می‌شود. انواع ایده‌های پنهان‌نگاری در حوزهٔ ضرایب DCT به‌نوعی، مقادیر این ضرایب را تحت تأثیر قرار می‌دهند. در برخی موارد، مانند روش‌های جای‌گذاری در LSB[5]، الگوی این تغییرات تقریباً قابل پیش‌بینی است و مبنای حملاتی مانند تست χ^2 قرار می‌گیرد. اما در موارد دیگری که روش‌های پنهان‌نگاری امن‌تری مورد استفاده قرار گرفته باشد (مانند الگوریتم‌های تطبیق LSB[6] و نیز F5)، پیش‌بینی این تغییرات چندان ساده نیست و لازم است رویکرد دیگری برای حمله به آن اتخاذ گردد. همچنین خاطر نشان می‌سازیم که پنهان‌نگاری در پیکسل‌های تصویر JPEG بسیار نا امن است و در ظرفیت‌های بسیار پایین هم به‌راحتی قابل کشف است و

[1] Blind steganalysis methods
[2] Carrier signal

[3] Hidden signal
[4] Calibration
[5] LSB flipping (LSB replacement)
[6] LSB matching

به‌طورمعمول در این حوزه در تصاویر JPEG پنهان‌نگاری انجام نمی‌شود [۱۰]. با این حال سیستم پیشنهادی در این مقاله، قادر است این موارد را نیز به‌خوبی تشخیص دهد.

در این مقاله یک سیستم جامع نهان‌کاوی برای تصاویر JPEG معرفی خواهد شد که ویژگی‌های بارز آن را می‌توان به‌شکل زیر خلاصه کرد:

- دسته‌بندی روش‌های مختلف پنهان‌نگاری در گروه‌های معنادار بر حسب اثری که در مشخصات آماری تصویر می‌گذارند.
- انتخاب ویژگی‌های مناسب و بهینه بر اساس اثرات مختلف روش‌های پنهان‌نگاری گوناگون بر تصویر.
- تصمیم‌گیری سلسله مراتبی روی دسته‌های مختلف ویژگی‌ها به‌منظور بالا بردن دقت و سرعت سیستم نهان‌کاو.
- بررسی اثر ضریب کیفیت روی دقّت سیستم و سپس انتخاب یک چارچوب بهینه برای به‌کارگیری مدل‌های تعلیم‌یافته روی ضرایب کیفیت مختلف.

در این روش، برای ارزیابی ویژگی‌ها، سعی شده مقایسه‌ای با بهترین و مشهورترین روش‌های موجود در نهان‌کاوی تصاویر JPEG انجام شود که شباهت‌هایی به چارچوب پیشنهادی نیز دارند. به این منظور کارهای تحقیقاتی فریدریش [۶-۹، ۳، ۱] و *یون. کیو. شی.* [۲] مبنا قرار گرفته‌اند. نتایج نهایی سیستم با نتایج گزارش‌شده توسط این دو گروه، مقایسه شده و موارد شباهت و تفاوت با آن‌ها مورد بحث قرار گرفته است.

در ادامهٔ این مقاله، در بخش دو مروری بر روش‌های نهان‌کاوی در حوزهٔ تصاویر JPEG خواهیم داشت. سپس در بخش سه جزئیات روش پیشنهادی تشریح می‌گردد. در بخش چهار نتایج و ارزیابی روش ارائه خواهد شد. در پایان و در بخش پنج بحث، جمع‌بندی و ارایهٔ پیشنهادها صورت خواهد گرفت.

۲- مرور سوابق

در مورد حمله به روش‌های پنهان‌نگاری، ایده‌های متعدّدی توسط محققان مطرح شده است. این ایده‌ها در طیف بسیار متنوعی قرار دارند: از روش‌های عمومی (مستقل از روش و حوزهٔ پنهان‌نگاری) گرفته [۴، ۱۱-۱۸] تا روش‌های خاصّ حمله به یک روش پنهان‌نگاری خاص [۱۹-۲۲]. در این میان، گروهی از محققان سعی داشته‌اند نگاهی مجزا به تصاویر JPEG داشته باشند و یک سری مشخصّات آماری را روی ضرایب DCT بسنجند (ر.ک. بخش۲-۲). در این روش‌ها - که می‌توان آن‌ها را "روش‌های عمومی حمله به پنهان‌نگاری در JPEG" تلقی کرد- اثر الگوریتم‌های مختلف پنهان‌نگاری روی ضرایب DCT مطالعه می‌شود و محققان به‌دنبال یافتن شباهت این آثار و ارایهٔ روشی کلی برای تشخیص و حمله به آن‌ها هستند.

در ادامهٔ این بخش، مرور مختصری بر انواع روش‌های نهان‌کاوی قابل استفاده برای تصاویر JPEG خواهیم داشت.

۲-۱- روش‌های نهان‌کاوی عمومی

در مرجع [۱۱] می‌توان مروری بر انواع روش‌های نهان‌کاوی عمومی را ملاحظه نمود. برخی از مهم‌ترین آن‌ها عبارتند از: استفاده از معیارهای کیفیت تصویر (IQM)[1]، گشتاورهای مرتبهٔ بالاتر ضرایب ویولت زیرباندها[2]، گشتاورهای تابع مشخصهٔ هیستوگرام زیرباندهای ویولت[3] و نیز مرکز ثقل تابع مشخصهٔ هیستوگرام[4] [۱۱]. از این میان، روش‌های عمومی که در حوزهٔ تصاویر JPEG کاربرد و عملکرد بهتری دارند، اغلب بر اساس استخراج ویژگی‌های مبتنی بر تبدیل ویولت [۱۲، ۴] و یا تبدیل کانتورلت[5] [۱۷] استوار هستند.

یکی از مشهورترین روش‌های عمومی مبتنی بر ویولت، روش معرّفی شده توسط *فرید*[6] [۱۲] است که از آمارگان مرتبهٔ بالاتر ضرایب ویولت استفاده می‌کند. اساس این روش، چنین است که در آن فرض می‌شود در یک تصویر طبیعی، ضرایب ویولت زیرباندهای مختلف به یکدیگر وابسته‌اند و بر اثر پنهان‌نگاری، این همبستگی‌ها کاهش می‌یابد. در این روش، تابع تبدیل ویولت هار تا سه مرحله به تصویر اعمال می‌شود و به‌کمک یک تخمین‌گر خطی، ضرایب ویولت زیرباندهای فرکانس میانی و فرکانس بالا در یک مقیاس[7]، از روی زیرباندهای مجاور خود در همان مقیاس و نیز زیرباندهای متناظرشان از مقیاس‌های ریزتر تخمین زده می‌شوند. سپس یک سری گشتاورهای آماری از روی خود ضرایب ویولت و نیز سیگنال خطای این تخمین خطّی محاسبه می‌گردد. این گشتاورها که درمجموع، یک بردار ویژگی ۷۲ تایی (برای هر کانال رنگ در فضای RGB یا برای

[1] Image Quality Metrics
[2] Higher Order Moments of Wavelet Sub band Coefficients
[3] Moments of Wavelet Characteristic Function
[4] Histogram Characteristic Function Center Of Mass (HCF-COM)
[5] Contourlet
[6] Farid. H.
[7] scale

سطوح روشنایی تصویر سیاه و سفید) را تشکیل می‌دهند، برای طبقه‌بندی به یک طبقه‌بندی‌کنندهٔ خطّی (مانند FLD[1]) و یا SVM[2] سپرده می‌شود.

روش عمومی دیگری که مبتنی بر تبدیل ویولت است، روش معرّفی شده توسط یون. کیو. شی و همکاران وی[3] است [۴] که از گشتاورهای آماری تابع مشخّصهٔ (تبدیل فوریهٔ) هیستوگرام زیرباندهای ویولت استفاده می‌کند. فرض اصلی این روش این‌چنین است که "هیستوگرام ضرایب ویولت بر اثر پنهان‌نگاری نرم‌تر می‌شود". بنابراین معیارهایی برای سنجش میزان تغییرات این هیستوگرام‌ها تعریف می‌شود که میزان نرمی هیستوگرام را بازنمایی می‌کند. این معیارها عبارتند از گشتاورهای مرتبهٔ n (n=1,2,3) تابع مشخصهٔ هیستوگرام ضرایب ویولت، که متناسب هستند با مشتق nام خود هیستوگرام ضرایب. این گشتاورها درمجموع یک بردار ۳۹تایی را تشکیل می‌دهند که برای طبقه‌بندی به یک طبقه‌بندی‌کننده، مانند طبقه‌بندی‌کنندهٔ سادهٔ *بیز*[4]سپرده می‌شوند [۴]. نمونه‌های بهبودیافتهٔ این روش نیز بعدها توسط همین گروه و سایر محققان معرّفی شده است که برای کسب اطلاعات بیشتر در این باره، می‌توان به مراجع [۱۴-۱۶] مراجعه نمود.

۲-۲- روش‌های عمومی تصاویر JPEG

روش‌های عمومی معرّفی شده در بخش (۲-۱) اختصاصی به تصاویر JPEG ندارند و برای سایر فرمت‌ها مانند BMP و GIF نیز قابل استفاده‌اند، زیرا مشخّصات استخراج شده در آن‌ها از اطّلاعات حوزهٔ مکان تصاویر به‌دست می‌آید. همان‌گونه که پیش‌تر نیز اشاره شد، گروه دیگری از ایده‌های موجود در پی رسیدن به نگاهی عمومی برای تصاویر JPEG هستند. از این دسته، دو روش مهم را می‌توان نام برد: روش سنجش همبستگی‌های درون بلوکی و بین بلوکی ضرایب DCT [۲] و روش استخراج آمارگان از حوزهٔ ضرایب DCT [۸]. این دو ایده که تاکنون در زمینهٔ نهان‌کاوی تصاویر JPEG بسیار موفّق بوده‌اند، در ادامه به‌اختصار معرّفی خواهند شد.

یون. کیو. شی و همکاران وی، معیاری برای اندازه‌گیری همبستگی ضرایب DCT در داخل یک بلوک[5] ۸*۸ و نیز همبستگی ضرایب DCT هم فرکانس در دو بلوک مجاور[6]، در نظر گرفته‌اند [۲]. این محققان همبستگی‌های فوق را به‌کمک ماتریس‌های احتمال گذر *مارکوف*[7] و نیز مفهوم ماتریس‌های رخداد توأم[8] اندازه گرفته‌اند. بردارهای ویژگی به‌دست آمده در نهایت یک بردار پنجاه‌تایی است که به‌کمک طبقه‌بندی‌کننده SVM طبقه‌بندی می‌شود. این روش روی ۷۰۵۶ تصویر JPEG با ضرایب کیفیت متنوع از ۶۰ تا ۹۰، آزمایش‌شده و برای روش‌های پنهان‌نگاری OUTGUESS، MB1 و F5 نتایج رضایت‌بخشی از آن گزارش شده است [۲].

روش مهم دیگر برای حمله به پنهان‌نگاری در حوزهٔ تصاویر JPEG و ضرایب DCT، روشی است که توسط *توماس پونی و جسیکا فریدریش*[9] پیشنهاد شده است. در این روش، یک مجموعهٔ متنوع از مشخصات آماری، اعم از آمارگان مرتبهٔ اوّل مانند هیستوگرام‌های کلّی و فرکانسی ضرایب DCT، و نیز گشتاورهای مرتبه‌های بالاتر مانند همبستگی‌ها و ماتریس‌های رخداد توأم، از ضرایب DCT تصویر، استخراج می‌شود. در این روش نوعی تخمین تصویر پوششی (به‌شیوهٔ کالیبراسیون) صورت می‌گیرد و براساس بردار تفاضل بین مجموعه ویژگی‌های تصویر مشکوک ورودی و تصویر پوششی تخمینی، بردار ویژگی نهایی تشکیل می‌شود [۶-۹، ۳، ۱].

مشخّصات آماری مورد استفادهٔ پونی و فریدریش درمجموع یک بردار ویژگی ۲۷۴ تایی را تشکیل می‌دهد (۱۹۳ ویژگی که توسط خود افراد این گروه پیشنهاد شده است، به‌همراه ۸۱ ویژگی دیگر که بر مبنای ویژگی‌های پیشنهادی در [۱۹] انتخاب شده و اندکی با مشخّصات معرّفی‌شده در [۲] متفاوت است). بردارهای ویژگی برای گروه‌های مختلف تصویری (با ضرایب کیفیت و روش‌های پنهان‌نگاری گوناگون) استخراج می‌شوند. سپس برای هر دسته تصویر، به‌کمک طبقه‌بندی‌کننده‌های SVM، یک سری مدل‌های مجزا تعلیم داده می‌شود؛ یعنی برای تصاویر پنهان‌نگار به شش شیوهٔ F5، OUTGUESS، MB1، MB2، JPHide&Seek، StegHide و با ۳۴ ضریب کیفیت مختلف (منتخب از ۶۳ تا ۹۸)، در مجموع ۲۰۴ = ۶*۳۴ مدل به دست می‌آید.

1 Fisher Linear Discriminant
2 Support Vector Machine
3 Yun. Q. Shi. et. al.
4 Naïve Bayes Classifier
5 Intra block correlations

6 Inter block correlations
7 Markov Transition Matrix
8 Co-occurrence matrix
9 Tomas Pevny & Jessica Fridrich

پس از تعلیم طبقه‌بندی‌کننده‌ها، تصمیم‌گیری برای یک بردار ویژگی مجهول ابتدا براساس انتخاب مدل متناظر با ضریب کیفیت آن تصویر و سپس بر مبنای برآیند رأی طبقه‌بندی‌کننده‌های مربوط به روش‌های گوناگون پنهان‌نگاری (شش روش) انجام می‌شود. نتایج گزارش شده توسط این گروه، برای این دسته از روش‌های پنهان‌نگاری خاص، نتایج بسیار خوبی است [۸]. این نتایج در ادامهٔ این مقاله مورد بحث قرار خواهد گرفت و با روش ما مقایسه خواهد شد.

۲-۳- روش‌های مربوط به الگوریتم‌های خاص

علاوه بر رویکردهای کلّی که در دو بخش قبل بررسی شدند، گروهی از روش‌های نهان‌کاوی نیز هستند که برای حمله به یک الگوریتم خاص پنهان‌نگاری طراحی شده‌اند. درحقیقت آن‌چه در مطالعهٔ این گروه از ایده‌های نهان‌کاوی برای ما اهمیت دارد، آن است که بدانیم محققان مختلف برای حمله به یک روش پنهان‌نگاری خاص، چه راهی را در پیش گرفته‌اند و چگونه از اثرات مخرب آن در آمارگان تصویر به سود خود بهره‌برداری کرده‌اند. روش‌های حمله به الگوریتم‌های خاص پنهان‌نگاری، بسیار متنوع است. از آن میان می‌توان به دو روش مشهور تست χ^2 [۲۴] و روش خاصّ حمله به F5 [۲۰] اشاره کرد. تست χ^2 ابزاری برای حمله به جای‌گذاری در LSB محسوب می‌شود و علاوه‌بر حوزهٔ DCT در سایر حوزه‌ها نظیر مکان و پالت[1] نیز کاربرد و عمومیت دارد. روش F5 یکی از شیوه‌های مهم و امن پنهان‌نگاری محسوب می‌شود و در مقابل حملات معمول مانند تست χ^2 مقاوم است. از این رو شناسایی روش نهان‌کاوی خاص F5 حائز اهمیت است.

تست χ^2 یک حملهٔ آماری است که در ابتدا برای حمله به جای‌گذاری ترتیبی در LSB (مانند روش JSTEG در تصاویر JPEG و روش EzStego در تصاویر GIF) معرفی شد [۲۴]. جای‌گذاری در LSB اثرات قابل پیش‌بینی روی مقادیر ضرایب DCT می‌گذارد. این اثرات بدین شکل است:

- مقادیر زوج یا بدون تغییر باقی می‌مانند، یا به مقدار فردی که یکی بیشتر از خود آن ضریب است، تغییر می‌یابند.
- مقادیر فرد یا بدون تغییر باقی می‌مانند، یا به مقدار زوجی که یکی کمتر از خود آن ضریب است، تغییر می‌یابد.

بر همین اساس، می‌توان گفت که پس از پنهان‌نگاری به‌شیوهٔ جای‌گذاری در LSB، جفت مقدارهای مجاور و مرتبط در هیستوگرام ضرایب DCT یعنی ($h(2k), h(2k+1)$) به یکدیگر نزدیک‌تر شده و به اصطلاح هیستوگرام نرم‌تر می‌شود. نسخهٔ تعمیم‌یافتهٔ χ^2 برای حمله به جای‌گذاری تصادفی در LSB ضرایب DCT (مانند OUTGUESS) قابل استفاده است [۲۵].

روش F5 (و مشتقات آن) یکی از امن‌ترین روش‌های پنهان‌نگاری محسوب می‌شود. این روش از طرفی نوعی تطبیق LSB محسوب می‌شود (و بنابراین نحوهٔ تغییرات ضرایب در آن شبیه به روش‌های جای‌گذاری در LSB نیست)، و از طرف دیگر تغییراتی که به تصویر اعمال می‌کند به نسبت ۳ به ۷ در مقایسه با تغییرات ناشی از روش‌های معمول تطبیق LSB کمتر است. اما این روش از یک ضعف مهم رنج می‌برد و آن، افزودن صفر به ضرایب DCT تصویر است. همین مسئله برای حمله به آن توسط فریدریش مورد استفاده قرار گرفته است [۲۰]. وی با تخمین تصویر پوششی (به‌کمک کالیبراسیون) و سپس نوشتن رابطهٔ نحوهٔ تغییرات احتمالی هیستوگرام تصویر، قبل و بعد از پنهان‌نگاری به رابطه‌ای دست می‌یابد که به‌کمک آن می‌تواند تخمینی از طول پیغام را به دست آورد.

۳- روش پیشنهادی

در انتهای بخش مقدمه، برخی ویژگی‌ها و نقاط قوت روش خود را بر شمردیم. در این بخش، ضمن معرفی جزئیات روش خود، این نقاط قوت و وجوه تمایز را به‌شکل دقیق‌تری بررسی می‌کنیم. مطالعهٔ ایده‌های گوناگون نهان‌کاوی و نیز انواع روش‌های پنهان‌نگاری، نشان داد که نه‌تنها بسیاری از روش‌های پنهان‌نگاری متنوعی که تاکنون معرفی شده‌اند، ماهیتاً با یکدیگر متفاوت نیستند، بلکه می‌توان ادعا کرد که هنگام جاسازی پیغام، اثر یکسان و مشابهی بر تصویر می‌گذارند. با این نگاه می‌توان انواع روش‌های پنهان‌نگاری مهم را که به‌طورمعمول در ارزیابی روش‌های نهان‌کاوی نیز مبنا قرار می‌گیرند، در سه دستهٔ اصلی طبقه بندی کرد:

۱) روش‌های جای‌گذاری در LSB و به‌طورکلی روش‌هایی که مشخّصات آماری مرتبهٔ اوّل تصویر (هیستوگرام) را تحت تأثیر قرار می‌دهند؛ مانند JSTEG، OUTGUESS، StegHide، MB1[2] و MB2، روش JPHide&Seek و ...

[1] palette

[2] Model Based

۲) روش‌های تطبیق LSB، مانند تطبیق ترتیبی یا تصادفی LSB ضرایب DCT، روش‌های F3، F4،F5 و نسخه‌های بهبود یافتهٔ آن (مانند nsF5) [۲۶].

۳) روش‌هایی که لزوماً در LSB ضرایب پنهان‌نگاری نمی‌کنند یا نمی‌توان آن‌ها را به صورت مستقیم در یکی از دو دستهٔ فوق قرار داد، مانند روش‌های مبتنی بر کوانتیزیشن (PQ)[1]، روش‌های جاسازی در تفاضل ضرایب (PVD)[2] [۲۷]، افزودن نویز به تصویر در حوزهٔ مکان و پنهان‌نگاری در تصویر نویزی (به منظور کاهش همبستگی‌های محلی ضرایب DCT) [۲۸-۲۹]، روش مبتنی بر پخش طیف (SSIS)[3] [۳۰]، روش YASS[4] (روشی مقاوم در برابر اثرات بلوکی شدن تصویر) [۲۲]، روش‌های پنهان‌نگاری در حوزهٔ تبدیل (مانند تبدیل ویولت) و ...

روش‌های گروه یک (که اغلب از نوع جای‌گذاری در LSB هستند) اغلب روی مشخّصات آماری مرتبهٔ اول تصویر تأثیر می‌گذارند. به‌همین جهت مشخّصات آماری نظیر هیستوگرام کلّی ضرایب DCT، یا هیستوگرام فرکانس‌های خاص می‌تواند وجه تمایز خوبی برای شناسایی این گروه باشد. در مقابل، روش‌های گروه دو به طور معمول اثرات خود را در آمارگان مرتبه اول نشان نمی‌دهند و اثر آنها در مشخصات آماری مرتبه دوم بیشتر نمود پیدا می‌کند. این مسأله به خصوص در مورد روش‌های تطبیق LSB صادق است.

روش‌های گروه سه اثرات متفاوتی دارند و می‌توانند در مشخصات آماری مرتبهٔ اول یا دوم مؤثر باشند. به‌عنوان مثال، از میان روش‌های پنهان نگاری گروه سه روش SSIS[5] که برای جبران حمله به هیستوگرام ارائه شده (و بر مبنای افزودن نویز عمل می‌کند)، روش حمله به آن مبتنی است بر مفهوم همبستگی و همین ماتریس‌های رخداد توأم. این مسألهٔ در مراجع [۳۱-۳۲] به‌طورکامل جزء روش‌های خاص بیان شده است. برای حمله به روش PVD نیز همان‌گونه که در مرجع [۳۳] مطرح شده است، می‌توان از مفهوم هیستوگرام استفاده کرد. علّت این امر آن است که بر اثر پنهان‌نگاری به شیوهٔ PVD، هیستوگرام تصویر اصلی با هیستوگرام تصویر پنهان‌نگار، به‌طور کامل متفاوت است و قابل شناسایی است [۳۳].

در این تحقیق، فرضیات فوق در آزمایشهای متعددی روی مجموعه‌های مختلف تصویری به تأیید رسید و درنهایت یک ساختار تصمیم‌گیری سلسله‌مراتبی شامل دو بخش[6] اصلی، انتخاب گردید. شیوهٔ این تصمیم‌گیری بدین شرح است که ابتدا مشخصات A (اغلب شامل مشخصات آماری مرتبه دوم) از تصویر استخراج می‌شوند و در بخش A ارزیابی می‌شوند. به‌دلیل آن‌که خطای FP[7] بخش A بسیار کم است، اگر این بخش رأی به پنهان‌نگار بودن تصویر داد، آن را پذیرفته و در غیر این صورت، وارد بخش B خواهیم شد. بخش B به بررسی مشخصات آماری B اختصاص دارد. در صورت ورود به بخش B، رأی نهایی توسط این بخش صادر خواهد شد.

یکی از مواردی که به‌عنوان نقطهٔ قوت و وجه تمایز روش خود با سایرین برشمردیم، عبارت است از "بررسی اثرات روش‌های مختلف پنهان‌نگاری بر مشخصات آماری تصویر". این آثار را می‌توان به‌خوبی در آمارگان مرتبهٔ اول و دوم تصویر مشاهده کرد. از جمله اثراتی که پنهان‌نگاری می‌تواند بر مشخصات آماری مرتبهٔ اول تصویر داشته باشد، نرم‌تر شدن هیستوگرام است. همچنین اثر روش‌های مختلف پنهان‌نگاری در مشخصات آماری مرتبه دوم، می‌تواند به صورت کاهش همبستگی‌های حوزهٔ مکان یا حوزهٔ تبدیل (ویولت، DCT و یا فوریه) دیده شود. اثری مانند نرم‌تر شدن هیستوگرام، می‌تواند نمودهای مختلفی داشته باشد و بنابراین روش‌های مختلفی برای سنجش این تغییر قابل تعریف است و سایر محققان نیز به آن‌ها اشاره‌هایی داشته‌اند. برخی از نمودهای نرم‌تر شدن هیستوگرام عبارت است از:

- نزدیک‌تر شدن دو مقدار مرتبط و مجاور در هیستوگرام بر اثر جای‌گذاری در LSB (مشابه حملهٔ χ^2).
- کاهش مقدار مرکز ثقل تابع مشخصهٔ هیستوگرام (کاهش محتوای فرکانس بالای هیستوگرام). این ایده در [۳۲، ۳۴-۳۵] مورد استفاده قرار گرفته است.
- نرم‌ترشدن هیستوگرام ضرایب ویولت تصویر (کاهش گشتاورهای مرتبهٔ بالای تابع مشخصهٔ هیستوگرام ضرایب ویولت). این ایده در [۱۴-۱۶] مورد استفاده قرار گرفته است.
- کاهش بیشینه‌هایی نسبی و افزایش مینیمم‌های نسبی در هیستوگرام. این ایده در [۳۶] نیز مورد استفاده قرار گرفته است.

[1] Perturbed Quantization
[2] Pixel Value Differencing
3 Spread Spectrum Image Steganography
[4] Yet Another Steganographic Scheme
[5] Spread Spectrum Image Steganography
[6] module
[7] False Positive

با توجّه به مباحث فوق، به این نتیجه رسیدیم که برای آشکارسازی اثرات گوناگون روش‌های پنهان‌نگاری مختلف لازم است از جنبه‌های متفاوتی به تصویر و مشخصات آماری آن نگریسته شود. به‌عبارت دیگر، برای حمله به هر یک از آثار پنهان‌نگاری، لازم است دسته‌ویژگی خاصی از تصویر استخراج شود. به‌طورکلی می‌توان گفت، انواع ویژگی‌هایی که از ضرایب DCT استخراج می‌شوند، قابل تقسیم به دو گروه عمده هستند:

۱. مشخصات آماری مرتبه اول: مانند هیستوگرام‌های کلی، هیستوگرام‌های مربوط به برخی فرکانس‌های خاص، ...
۲. مشخصات آماری مرتبهٔ دوم: مانند انواع روش‌های محاسبهٔ همبستگی بین ضرایب DCT تصویر به شیوه‌های مختلف مثل سنجش واریانس، ماتریس‌های رخداد توأم و ...

تمامی روش‌های مطرح شده را برای نهان‌کاوی در حوزهٔ JPEG (و در یک نگاه کلی، در تصویر) را می‌توان در یکی از دو گروه فوق جای داد. محققان مختلف به شیوه‌های گوناگونی روی مقادیر هیستوگرام و همبستگی بحث کرده و ایده‌هایی ارائه داده‌اند.

مسألهٔ قابل طرح دیگر در حوزهٔ نهان‌کاوی تصاویر JPEG، بحث ضریب کیفیت تصاویر ورودی است. روش‌های نهان‌کاوی موجود به‌شدت تحت تأثیر ضریب کیفیت تصاویر تعلیم و تست هستند. همان‌طور که پیش‌تر نیز اشاره شد، در همین راستا، فریدریش و همکاران وی بحث ضریب کیفیت را در سیستم خود به‌شکل بسیار مفصلی درنظرگرفته‌اند و برای ۳۴ ضریب کیفیت مختلف، طبقه‌بندی‌کننده‌های مجزایی را تعلیم داده‌اند. این کار مستلزم صرف وقت بسیار زیادی در مراحل تعلیم و تست است و نیز از عمومیت سیستم می‌کاهد.

در مقابل، آن‌چه ما در این تحقیق انجام داده‌ایم بدین صورت است که برای تصاویر با ضرایب کیفیت ۲۵، ۴۵، ۵۲، ۶۹، ۷۷، ۸۳، ۹۰، ۹۹ سیستم‌های مجزایی تعلیم داده‌ایم (یعنی تنها ۸ ضریب کیفیت در مقابل ۳۴ عدد سیستم فریدریش). سپس از ضریب کیفیت ۲۵ تا ۹۹، ۸ ناحیهٔ مختلف را متناظر با این هشت ضریب کیفیت در نظر گرفته‌ایم. در صورت برخورد با یک تصویر جدید، بر حسب این‌که ضریب کیفیت تصویر در کدام بازه است، مدل مربوط به یکی از این هشت مقدار انتخاب می‌شود و برای تصمیم‌گیری مورد استفاده قرار می‌گیرد.

مزّیت دیگر روش ما آن است که با دسته‌بندی روش‌های پنهان‌نگاری، تنها دو "دسته روش" را در نظر گرفته‌ایم و به تعداد ۲*۸ = ۱۶ مدل SVM در کل سیستم دست یافته‌ایم. این در حالی است که فریدریش برای "۶ روش" پنهان‌نگاری مختلف، مدل‌های SVM مجزایی را تعلیم داده است و با احتساب ۳۴ ضریب کیفیت، درمجموع به ۲۰۴ سیستم دست یافته است.

در ادامهٔ این بخش، ویژگی‌های مورد استفاده را در هر یک از اجزای سیستم را معرّفی کرده و علل کارآیی هر یک را مورد بحث قرار خواهیم داد. در هر مورد مقایسه‌ای با روش فریدریش [۸] یا یون. کیو. شی [۲] انجام خواهد شد.

۳-۱- بخش A: ویژگی‌های مبتنی بر همبستگی ضرایب DCT

برای حمله به روش‌های تطبیق LSB بهتر است از مفهوم همبستگی ضرایب DCT استفاده شود. اساس این ایده چنین است که در یک تصویر طبیعی، ضرایب DCT داخل یک بلوک ۸*۸ نسبت به همدیگر همبسته‌اند. همچنین ضرایب DCT هم فرکانس در بلوک‌های مجاور نیز نسبت به یکدیگر همبستگی‌هایی دارند. این همبستگی‌ها بر اثر پنهان‌نگاری کاهش می‌یابد، زیرا نوعی بی‌نظمی به تصویر افزوده می‌شود. ملاک‌های مختلفی برای سنجش همبستگی بین ضرایب DCT وجود دارد که از آن جمله می‌توان به مقادیر واریانس، مجموع قدر مطلق تفاضل ضرایب و همچنین مجموع مربعات تفاضل‌های ضرایب اشاره کرد. امّا می‌توان گفت موفق‌ترین معیار همبستگی که تاکنون توسط محققان در حوزهٔ نهان‌کاوی مورد استفاده قرار گرفته معیاری به نام **ماتریس رخداد** توأم است.

ماتریس رخداد توأم نوعی بیان کمی از نحوهٔ بروز و رخداد جفت مقادیر مختلف در فواصل و به زاویه‌های مختلف از یکدیگر است. ماتریس رخداد توأم، نه‌تنها در مورد ضرایب DCT بلکه در حوزهٔ مکان نیز برای نهان‌کاوی مورد استفاده قرار گرفته است [۱۸، ۳۷].

استفاده از ماتریس رخداد توأم برای سنجش همبستگی‌های درون بلوکی و بین بلوکی ضرایب DCT ابتدا توسط یون. کیو. شی و همکاران وی پیشنهاد گردید [۲] و سپس همین گروه تحقیقاتی، به‌شکل دیگری مفهوم رخداد توأم را به‌کار بردند [۱۹]. همچنین فریدریش و همکاران وی نیز از ایدهٔ موجود در [۱۹] در کنار روش خود بهره گرفتند [۸]. در این قسمت بحث می‌کنیم که شیوهٔ مورد استفاده در مرجع [۲] به این علّت که برمبنای منطق صحیح‌تری استوار است، عملکرد بهتری خواهد داشت و به‌همین جهت در روش خود از آن استفاده نموده‌ایم. در این روش، ابتدا ضرایب DCT داخل یک بلوک ۸*۸ به‌ترتیب زیگزاگی چیده می‌شوند و در یک بردار قرار می‌گیرند (شکل۱-الف). از بین ۶۴ مقدار موجود در این بردار، با کنار گذاشتن ضریب DC، تنها L مقدار AC اول آن انتخاب می‌شود و برای محاسبات بعدی مورد استفاده قرار می‌گیرد. بردار L=9تایی حاصل در سطری از ماتریس مارکوف قرار می‌گیرد [۲].

ماتریس مارکوف عبارت است از ماتریسی که هر سطر آن شامل بردار L تایی متناظر با بلوک ۸*۸ای از ضرایب DCT کوانتیزه‌شدهٔ تصویر است. ترتیب قرار گرفتن ضرایب بلوک‌ها در سطرهای ماتریس مارکوف به‌نحوی است که بلوک‌های مجاور در راستای افقی در سطرهای کنار هم قرار می‌گیرند. در پایان یک ردیف اسکن افقی تصویر، بلوک بعدی را بلوک زیری آخرین بلوک ردیف بالایی انتخاب می‌کنیم. یعنی به‌عنوان‌مثال درانتهای ردیف اوّل، به‌جای برگشتن به‌سمت چپ ردیف دوم، اسکن ردیف دوم را از سمت راست به چپ انجام می‌دهیم، ردیف سوم را از چپ به راست و ... به همین ترتیب مطابق (شکل ۱-ب) عمل می‌کنیم. به‌طورکلّی می‌توان گفت این نحوهٔ چینش ضرایب بلوک‌ها در داخل ماتریس مارکوف، بیشتر ناظر به اندازه‌گیری همبستگی‌های بین ضرایب DCT در بلوک‌های مجاور افقی است.

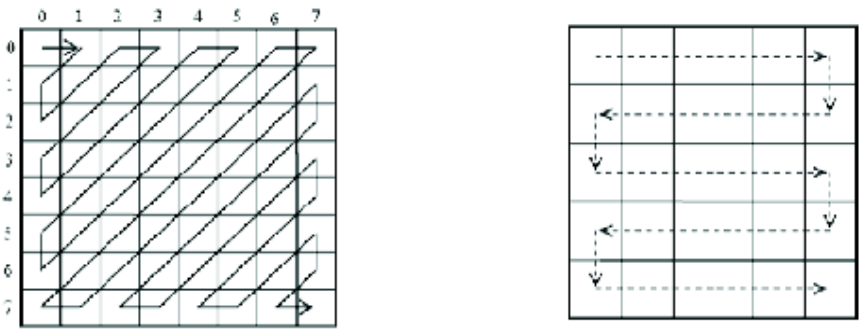
براین‌اساس، ماتریس مارکوف حاوی مقادیری خواهد بود که در هر سطر آن ضرایب منتخب یک بلوک ۸*۸ در کنار هم قرار گرفته‌اند و در سطرهای متوالی آن ضرایب هم فرکانس بلوک‌های مجاور در کنار هم قرار دارند (شکل ۲). به‌کمک ماتریس مارکوف، همبستگی درون بلوکی براساس ماتریس رخداد توأم افقی ماتریس مارکوف (رابطهٔ ۱) و همبستگی بین بلوکی بر اساس ماتریس رخداد توأم عمودی ماتریس مارکوف (رابطهٔ ۳)، قابل محاسبه هستند [۲]. در این روابط C_{ij}ها عبارتند از ضرایب DCT تصویر. همچنین منظور از δ در روابط ۱ و ۳ تابع دلتای دیراک است که در رابطهٔ ۲ تعریف شده است.

توضیح این نکته نیز ضروری به‌نظر می‌رسد که ماتریس رخداد توأم بر اساس تعداد تکرارهای مقادیر ضرایب DCT در وضعیت مکانی خاصی نسبت به هم، انجام می‌گیرد. از این رو به‌منظور کاهش حجم محاسبات، یک آستانه‌گذاری اوّلیه روی مقادیر ضرایب انجام می‌شود؛ به این نحو که ضرایب کوچک‌تر از T– به T– و ضرایب بزرگ‌تر از T به T برش داده می‌شوند. این کار، خطای چندانی به سیستم نمی‌افزاید؛ زیرا بخش عمدهٔ ضرایب DCT تصویر دارای دامنه‌ای کمتر از T=4 هستند [۲، ۸]. پس از این آستانه‌گذاری، ماتریس مارکوف مربوط به دامنهٔ ضرایب DCT تشکیل و همبستگی‌های درون بلوکی (یک بردار ۲۵تایی) و بین بلوکی (یک بردار ۲۵تایی) محاسبه می‌شوند و برای هر تصویر، یک بردار ویژگی ۵۰تایی به دست می‌آید.

مقادیر ماتریس رخداد توأم بر اثر پنهان‌نگاری نسبت به حالت طبیعی تغییر می‌کنند و همین تغییرات وجه تمایز تصاویر طبیعی و پنهان‌نگار خواهد بود. در توضیح این نکته می‌توان گفت به‌طورکلّی انتظار می‌رود مقادیر موجود در امتداد قطر اصلی ماتریس رخداد توأم دارای مقادیر بزرگتری نسبت به نواحی دور از قطر آن باشند.

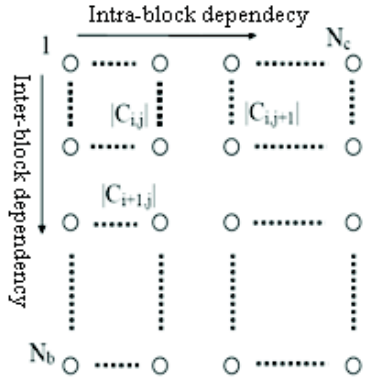
به عبارت دیگر، انتظار می‌رود ضرایب هم‌فرکانس در دو بلوک مجاور (در حالت سنجش همبستگی بین بلوکی)، دامنه‌ای شبیه به هم داشته باشند. بر اثر پنهان‌نگاری این تجمع ماتریس رخداد توأم حول قطر به‌هم می‌ریزد و همین مبنای تشخیص تصاویر طبیعی از پنهان‌نگار می‌شود.

نکتهٔ دیگر آن که سنجش همبستگی بین بلوکی، علاوه بر راستای افقی، می‌تواند در راستاهای عمودی و قطری نیز انجام گیرد که فعلاً در این تحقیق از آن صرف نظر شده است. علّت این صرف نظر کردن نیز آن است که ویژگی‌های مربوط به همبستگی در راستای بلوک‌های افقی جوابگوی کاربرد مورد نظر ما بوده و بنابراین برای صرفه جویی در وقت، نیازی به محاسبهٔ همبستگی در راستاهای دیگر نبوده است؛ امّا واضح است که سنجش همبستگی‌ها در سایر راستاها اطّلاعات مفید بیشتری را به دست خواهد داد.



ب الف

(شکل۱): نحوهٔ انتخاب ضرایب DCT در محاسبهٔ همبستگی‌های درون بلوکی و بین بلوکی. الف) ترتیب اسکن بلوک‌های ۸*۸ تصویر، ب) ترتیب اسکن ضرایب داخل یک بلوک ۸*۸ (ترتیب زیگزاگی) [۲].



(شکل۲): نحوهٔ تشکیل ماتریس مارکوف با استفاده از چینش خاص ضرایب DCT [۲]

$$p_h(|C_{i,j+1}|=n\,|\,|C_{i,j}|=m)=\frac{\sum_{i=1}^{N_b-1}\sum_{j=1}^{N_c-1}\delta(|C_{i,j}|=m,|C_{i,j+1}|=n)}{\sum_{i=1}^{N_b-1}\sum_{j=1}^{N_c-1}\delta(|C_{i,j}|=m)} \quad (۱)$$

$$\delta(x)=\begin{cases}1 & x=true\\ 0 & otherwise\end{cases} \quad (۲)$$

$$p_v(|C_{i+1,j}|=n\,|\,|C_{i,j}|=m)=\frac{\sum_{i=1}^{N_b-1}\sum_{j=1}^{N_c-1}\delta(|C_{i,j}|=m,|C_{i+1,j}|=n)}{\sum_{i=1}^{N_b-1}\sum_{j=1}^{N_c-1}\delta(|C_{i,j}|=m)} \quad (۳)$$

همچنین بردارهای ویژگی پنجاه تایی به‌دست آمده برای تصاویر طبیعی و پنهان‌نگار، در مرحلهٔ تعلیم به‌شکل مستقیم به کار رفته‌اند. به‌عبارت دیگر حالت تفاضلی (تفاوت بین تصویر اصلی و تصویر پوششی تخمین زده شده) را در نظر نگرفته‌ایم. این کار به دو دلیل انجام شده است: اوّل این‌که همان‌گونه که در مقدمه ذکر شد، روش کالیبراسیون تنها قادر است مشخصات آماری مرتبهٔ اوّل (هیستوگرام) تصویر پوششی را به‌خوبی تخمین بزند و بحثی راجع به حفظ

مشخصات آماری مرتبهٔ دوم ندارد. دوم این‌که استفاده از بردارهای ویژگی خود تصاویر (و نه بردارهای تفاضلی) بین گروه‌های مختلف تصویری عملکرد قابل قبولی از خود نشان داده است که نیاز به تست روش تخمین تصویر پوششی را از بین می‌برد. امّا بحث بررسی امکان ارائهٔ یک روش تخمین مناسب برای تصویر پوششی با حفظ مشخصات آماری مرتبهٔ دوم و کاربرد آن برای ویژگی‌های مزبور می‌تواند به‌عنوان یک پیشنهاد برای ادامهٔ تحقیقات در نظر گرفته شود.

همان‌گونه که در مقدمهٔ این بخش گفته شد، از این دسته‌ویژگی برای تعلیم بخش اول سیستم نهان‌کاوی نهایی خود و بیشتر با هدف تشخیص روش‌های تطبیق LSB در حوزهٔ ضرایب DCT از آن استفاده کردیم. البته این روش در مورد تصاویر پنهان‌نگاری شده به‌شیوهٔ جای‌گذاری در LSB نیز پاسخ‌های به نسبه قابل قبولی داشته است، اما در مورد تطبیق LSB دقت تشخیص صحیح[33] آن بالاتر و خطای FP آن نیز کمتر است.

توجیه این مسأله بسیار قابل تأمل است. این موضوع به‌طوردقیق همان چیزی است که در آزمایش‌های ما در نهان‌کاوی در حوزهٔ مکان نیز دیده و تأیید شده است. یعنی برای تشخیص پنهان‌نگاری به‌شیوهٔ تطبیق LSB در حوزهٔ مکان نیز ویژگی‌های مرتبهٔ دوم (از جنس همبستگی) قوی‌تر از ویژگی‌های مرتبه اوّل عمل می‌کنند.

۳-۲- بخش B: مشخصات آمـاری مرتبـه اول ضرایب DCT

با توجّه به توضیحات گذشته می‌توان گفت روش‌های جای‌گذاری در LSB ضرایب DCT، بیشتر روی هیستوگرام و مشخّصات آماری مرتبهٔ اوّل مؤثّر هستند. اگر در مواردی مانند روش‌های پنهان‌نگاری MB1 و OUTGUESS هیستوگرام کلّی تصویر اصلاح شود، باز هم هیستوگرام‌های ضرایب فرکانس‌های خاص تحت تأثیر قرار می‌گیرند. از این رو برای حمله به این گروه از روش‌های پنهان‌نگاری، درصدد شناسایی مشخّصات آماری مناسبی برآمدیم. فریدریش و پونی [۶-۹، ۳، ۱]، مجموعهٔ مفصلی از مشخصات آماری را پیشنهاد کرده‌اند. بررسی ویژگی‌های پیشنهادی توسط پونی و فریدریش [۸] نشان داد که برخی از این ویژگی‌ها از یکدیگر مستقل نبوده و به‌عبارت دیگر با یکدیگر همپوشانی دارند. به‌همین جهت درصدد بر آمدیم با بررسی دقیق هر دسته ویژگی، تنها مواردی را که وجود آن‌ها معنادار است و تأثیر مثبتی بر نهان‌کاوی خواهد داشت شناسایی کرده و بقیه را از مجموعه حذف کنیم. در ادامهٔ این بخش به معرفی و توجیه علّت استفاده از هر دسته ویژگی خواهیم پرداخت. ویژگی‌های پیشنهادی توسط پونی و فریدریش ۲۷۴ عدد برای هر تصویر است که در اینجا تنها ۱۳۵ مقدار آن مورد استفاده قرار می‌گیرد.

دستهٔ اوّل ویژگی‌ها، عبارت است از هیستوگرام ضرایب DCT در کل تصویر (هیستوگرام نرمالیزه شده نسبت به تعداد کلّ ضرایب DCT کوانتیزه شدهٔ تصویر). از آن‌جا که بخش زیادتری از ضرایب DCT دارای دامنه‌ای کمتر از ۴ یا ۵ هستند، از میان ستون‌های هیستوگرام[34]، تنها ستون‌های مربوط به مقادیر بین ۵- تا ۵ در نظر گرفته شده (۱۱ مقدار) و مابقی دور ریخته می‌شوند (رابطهٔ ۴) [۸]. در این رابطه d_{ij}ها ضرایب DCT تصویر و H_kها میزان فراوانی هر یک از مقادیر d_{ij} می‌باشد. این مجموعه‌ویژگی می‌تواند اثر جایگذاری در LSB ضرایب DCT و تبدیل جفت مقدارهای متوالی مرتبط را به‌یکدیگر به‌خوبی نمایش دهد. این مجموعهٔ یازده تایی برای تصویر اصلی و تصویر کالیبره (تخمین تصویر پوششی) محاسبه شده و بردار تفاضل آن‌ها به‌صورت نرمالیزه شده بین بیشینه و کمینه خودش، به‌عنوان بخشی از بردار ویژگی نهایی محاسبه می‌گردد.

دستهٔ دوم ویژگی‌هایی که توسط پونی و فریدریش پیشنهاد شد و در اینجا استفاده از آن را غیر ضروری دانسته‌ایم، هیستوگرام ضرایب DCT در فرکانس‌های خاصی از هر بلوک (و نه تمامی فرکانس‌ها مانند حالت قبل) است. فلسفهٔ انتخاب این ویژگی‌ها عبارت است از امکان حمله به روش‌های پنهان‌نگاری که هیستوگرام کلی تصویر را اصلاح می‌کنند؛ امّا هیستوگرام‌های فرکانس‌های خاص را لزوماً حفظ نمی‌کنند. برای استخراج این دسته از ویژگی‌ها، پنج ضریب AC فرکانس پایین اوّل در نظر گرفته شده و به‌ازای هر کدام، یک هیستوگرام یازده‌تایی (فقط با در نظر گرفتن مقادیر بین ۵- و ۵) محاسبه می‌شود (رابطهٔ ۵) [۸]. در این رابطه h_k^{ij} ها عبارتند از مقادیر فراوانی ضرایب d_{ij} در فرکانس kام. هر دستهٔ یازده‌تایی هم برای تصویر اصلی و هم برای تصویر پوششی تخمینی محاسبه و خطای این دو گروه در هر دستهٔ یازده‌تایی بین بیشینه و کمینه آن دسته نرمالیزه می‌شود. بنابراین در این قسمت ۵۵ ویژگی تولید

[33] True Positive

[34] Histogram bins

خواهد شد. در این تحقیق، از این ۵۵ ویژگی صرف نظر شده است زیرا با مجموعه‌ویژگی‌های بعدی (دستهٔ سوم) هم‌پوشانی دارد.

دستهٔ سوم ویژگی‌ها، ۹۹ مقدار هستند که تحت عنوان ۹ هیستوگرام **دوگان**[35] نام‌گذاری می‌شوند. هیستوگرام‌های دوگان، از جنبهٔ دیگری بازگوکنندهٔ همان مقادیر ستون‌های هیستوگرام‌های فرکانس‌های AC منتخب هستند. برای محاسبهٔ این هیستوگرام‌های دوگان، ابتدا در سرتاسر تصویر در ۹ موقعیت از ۶۴ موقعیت موجود در یک بلوک ۸*۸ (۹ موقعیت متناظر با ۹ ضریب AC فرکانس پایین اوّل)، می‌شماریم که چند بار مقدار i (i=-5, ...,5) تکرار شده است. بنابراین برای هر یک از این ۹ موقعیت، یک مجموعهٔ یازده‌تایی (مقادیر g_{ij}^{d}) داریم که در مجموع، ۹۹ ویژگی را تشکیل می‌دهند (رابطهٔ ۶) [۸]. همین مقادیر برای تصویر تخمینی نیز محاسبه و خطای نرمالیزه شدهٔ آن‌ها به‌عنوان ۹ بردار یازده‌تایی دیگر ذخیره می‌گردد.

ویژگی‌های بعدی که به‌نوعی ویژگی‌های مرتبهٔ دوم را تشکیل می‌دهند عبارتند از سه مقدار عددی[36] و یک بردار ۲۵ تایی. ویژگی‌های عددی عبارتند از یک مقدار به‌نام "تغییر" (واریاسیون)[37] و دو مقدار دیگر تحت عنوان "میزان بلوکی شدن تصویر[38] که به‌نحوی تفاوت‌های بین مقادیر DCT دو بلوک مجاور را می‌سنجند. اساس بهره‌گیری از آن‌ها این است که پنهان‌نگاری سبب ایجاد نوعی ناپیوستگی در ساختار بلوک‌های ۸*۸ تصویر می‌شود و این معیارها می‌توانند گسستگی‌های مزبور را بازنمایی کنند [۸].

دسته‌ویژگی ۲۵ تایی بعدی نوعی ماتریس رخداد توأم است که به‌نوعی همبستگی درون بلوکی را برای بلوک‌های ۸*۸ تصویر محاسبه می‌کند. فرق این همبستگی درون بلوکی با ویژگی‌های معرفی شده در بخش ۳-۱ این است که در اینجا همهٔ فرکانس‌های داخل بلوک درنظر گرفته می‌شود، درحالی‌که در حالت قبل تنها فرکانس‌های خاصی (فرکانس‌های پائین AC) مورد نظر بود. همچنین در اینجا برای مقادیر بین ۲- تا ۲ (۵ مقدار) در بلوک‌های ۸*۸ ماتریس رخداد توأم محاسبه می‌شود و ۲۵ مقدار تولید می‌شود (در حالت قبل برای دامنهٔ ضرایب بین ۰ تا ۴ همبستگی محاسبه شده و ۲۵ مقدار به‌دست می‌آمد) [۸]. رابطهٔ هفت نحوهٔ محاسبهٔ این بردار ویژگی را نشان می‌دهد.

در این رابطه، D_{ij}^{I}ها ضرایب DCT تصویر I بوده و I_c و I_r به‌ترتیب نمایان‌گر تصاویر پوششی و پنهان‌نگار هستند.

فریدریش و پونی، از یک بردار ویژگی ۸۱ تایی دیگر نیز علاوه‌بر ۱۹۳ ویژگی فوق استفاده کرده‌اند [۸] که ما در این تحقیق از آن صرف نظر نموده‌ایم. این مجموعه‌ویژگی نوعی سنجش همبستگی ضرایب DCT تصویر است که در آن ابتدا شمای ضرایب DCT بلوک‌های تصویر در قالب یک ماتریس هم‌اندازهٔ خود تصویر در کنار یکدیگر قرار می‌گیرند و ماتریس J را تشکیل می‌دهند. به‌عبارت دیگر، هر بلوک ۸*۸ از ماتریس J معادل است با یک بلوک ۸*۸ از ضرایب DCT متناظر با موقعیت آن بلوک در تصویر اصلی. سپس ماتریس رخداد توأم ضرایب در راستاهای افقی، عمودی، و دو قطر محاسبه‌شده و از این ماتریس‌ها میانگین‌گیری می‌شود و ماتریس رخداد توأم نهایی M را تشکیل می‌دهد (این ماتریس برای مقادیر بین ۴- تا ۴ محاسبه می‌شود و بنابراین دارای ۹*۹=۸۱ مقدار است). این کار بر اساس ایدهٔ مطرح شده در [۱۹] توسط یون. کیو. شی. انجام شده است که تعمیمی است بر [۲]. درحقیقت این نویسندگان با این کار سعی داشته‌اند نوعی همبستگی درون بلوکی و بین بلوکی را به‌شکل توأم محاسبه نمایند.

این رویکرد دارای اشکالاتی است: به‌عنوان مثال، با این نحوهٔ برخورد با ضرایب DCT، در مرز بلوک‌ها دو ضریب غیر هم فرکانس و به‌طورکامل نامرتبط با یکدیگر در نظر گرفته شده و سعی می‌شود همبستگی آن‌ها محاسبه گردد. این درحالی است که رویکرد قبلی که برای سنجش همبستگی ضرایب در نظر گرفته بودیم هوشمندانه‌تر است، زیرا اوّل این‌که همبستگی‌های درون بلوکی را از همبستگی‌های بین بلوکی تفکیک می‌کند و دوم این‌که در سنجش همبستگی‌های بین ضرایب DCT دو بلوک مجاور، ضرایب هم فرکانس را با هم در نظر می‌گیرد.

با توجّه به توضیحات دو بخش ۳-۱ و ۳-۲ درنهایت پنجاه ویژگی برای بخش اول و ۱۳۵ ویژگی برای بخش دوم انتخاب گردید که برای استفاده در سیستم نهایی به‌صورت مجزا در یک ساختار سلسله مراتبی به کار می‌رود.

۳-۳- تخمین مشخّصات آماری مرتبهٔ اول تصویر پوششی به کمک کالیبراسیون

پیش‌تر توضیح داده شد که مشخّصات آماری سیگنال تفاضل (بین تصویر اصلی و تصویر پوششی تخمینی) بهتر از

[35] Dual histograms
[36] Scalar
[37] Variation
[38] Image Blockiness

از آن، مدل SVM متناظر با آن انتخاب شده و به‌کار می‌رود. این کار یک تفاوت اساسی با کار فریدریش [۸] دارد و آن اینکه به جای تعلیم ۳۴ مدل برای ۳۴ *ضریب کیفیت*، تنها از ۸ مدل برای ۸ *بازه* از ضرایب کیفیت استفاده شده است.

انتخاب ساختار سلسله مراتبی برای تصمیم‌گیری به چند دلیل انجام شده است و مزایایی دارد. اوّل این‌که باعث افزایش سرعت نهان‌کاوی می‌شود و در مواردی که تشخیص پنهان‌نگاری با تعداد محدودی ویژگی امکان‌پذیر است، نیازی به استخراج ویژگی‌های دیگر نیست. دوم این‌که این کار قابلیت اطمینان روش را بالا می‌برد و می‌تواند مشخص کند که روش پنهان‌نگاری چگونه اثری بر مشخصات آماری تصویر داشته است و در کدام زیرگروه از روش‌های پنهان‌نگاری جای می‌گیرد.

راجع به ساختار سلسله مراتبی تصمیم‌گیری باید گفت این کار تا حدودی شبیه به طبقه‌بندی درختی است. شباهت آن‌ها از این جهت است که ابتدا بر اساس یک سری از مشخصّات تصویر، تصمیم‌گیری می‌شود که تصویر پنهان‌نگار هست یا خیر. همان‌طورکه در (شکل‌های ۴ و ۵) دیده می‌شود، برای ارزیابی یک تصویر مجهول ابتدا در بخش اوّل پنجاه ویژگی (از نوع همبستگی ضرایب DCT در داخل یک بلوک و نیز بین بلوک‌های مجاور) از تصویر استخراج می‌شود.

این پنجاه ویژگی به مدل SVM متناظر با ضریب کیفیت تصویر سپرده می‌شود و راجع‌به آن تصمیم‌گیری می‌شود. اگر در بخش اوّل، رأی به پنهان‌نگار بودن تصویر داده شد، این تصمیم را قبول می‌کنیم و فرآیند نهان‌کاوی را خاتمه یافته می‌دانیم. در غیر این صورت به بخش دوم می‌رویم. علت اعتماد به رأی بخش اوّل، درصد بالای دقت تشخیص صحیح (TP) و درصد پایین خطای تشخیص غیرصحیح (FP) آن است. در بخش دوم، ۱۳۵ ویژگی دیگر از تصویر استخراج می‌شود (ویژگی‌هایی که بیشتر بر مشخصات آماری مرتبه اول ضرایب DCT تکیه دارند) و مدل SVM متناظر با ضریب کیفیت تصویر انتخاب شده و برای تصمیم‌گیری نهایی از آن استفاده می‌شود.

۴- نتایج تجربی و ارزیابی‌ها

۴-۱- پایگاه دادگان تصویری

برای تهیهٔ تصاویر لازم جهت آزمایش و ارزیابی روش نهان‌کاوی پیشنهادی، تعدادی تصویر که توسط دوربین از مناظر مختلف تهیه و به ابعاد ۳۰۰۰*۲۰۰۰ ذخیره شده بودند، جمع‌آوری گردید. این تصاویر در ابتدا به فرمت غیر فشردهٔ TIF ذخیره شدند. از بین تصاویر موجود، تعداد ۲۰۰۰ تصویر برش یافته به ابعاد ۶۷۰*۵۰۰ ، ۵۰۰*۶۷۰ ، ۷۲۰*۹۶۰ و ۹۶۰*۷۲۰ تهیه گردید. سپس این تصاویر توسط نرم افزار فوتوشاپ با ضرایب کیفیت مختلف به فرمت JPEG تبدیل شدند. ضرایب کیفیت مورد استفاده در جدول ۱ ارائه شده‌اند. به این ترتیب، در مجموع تعداد ۱۶۰۰۰ تصویر پوششی JPEG با ۸ ضریب کیفیت مختلف تولید شد. از این تعداد، در هر دستهٔ ۲۰۰۰ تایی، ۱۰۰۰ تصویر برای تعلیم مدل‌های SVM، و ۱۰۰۰ تصویر برای تست در نظر گرفته شدند. این تصاویر از نظر پیچیدگی و محتوا نیز بسیار متنوع هستند.

۴-۲- تولید تصاویر پنهان‌نگار

برای تولید نمونه‌های مناسب پنهان‌نگار از تصاویر موجود، هفت روش پنهان‌نگاری مشهور و پنج نرخ جاسازی انتخاب گردید. به‌این‌منظور، نرم‌افزاری به نام نهان‌ساز در محیط ویژوال C++ نوشته‌ایم که قادر است روش‌های گوناگون پنهان‌نگاری را شبیه‌سازی کند و تصاویر پنهان‌نگار را به شکل انبوه به روش‌های گوناگون و با نرخ‌های جاسازی متفاوت تولید کند. نهان‌ساز قادر است هشت روش پنهان‌نگاری حوزهٔ JPEG، شش روش پنهان‌نگاری حوزهٔ مکان و دو روش پنهان‌نگاری حوزهٔ پالت را اجرا نماید.

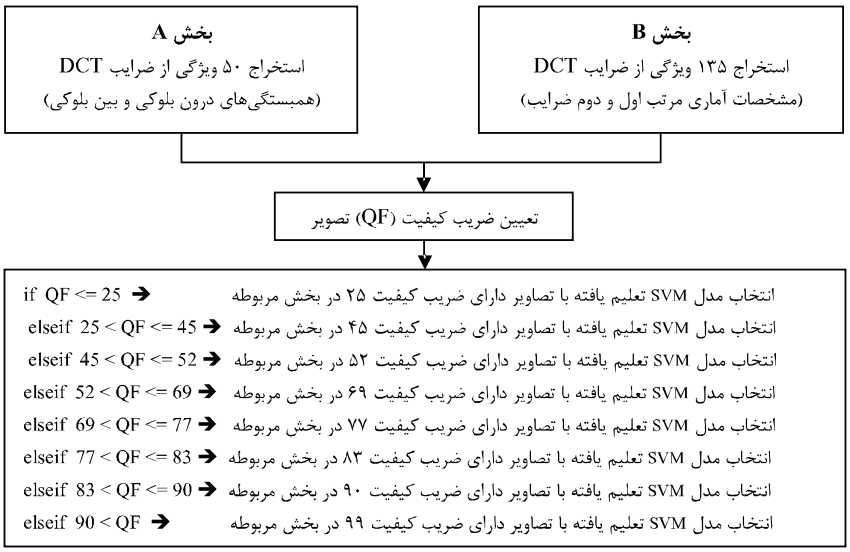
در این تحقیق انتخاب روش‌های پنهان‌نگاری برای تعلیم و تست، بر مبنای منطق خاصی بوده است: این‌که روش‌های متنوعی انتخاب شوند که جزء روش‌های متداول پنهان‌نگاری باشند و از نظر نوع اثرشان بر مشخصات آماری تصویر بتوانند در دسته‌های یکسانی قرار بگیرند.

روش‌های پنهان‌نگاری گروه اول که بیشتر به‌نوعی جای‌گذاری در LSB محسوب می‌شوند، عبارتند از JSTEG، OUTGUESS، MB1، MB2. در کنار این روش‌ها، سه روش تطبیق LSB نیز پیاده سازی شد که عبارتند از تطبیق LSB ترتیبی، تطبیق LSB تصادفی و F5. برای هر یک از این روش‌های پنهان‌نگاری، ۵ نرخ جاسازی ۲۰، ۴۰، ۶۰، ۸۰ و ۱۰۰٪ انتخاب گردید. بدین ترتیب تعداد کل تصاویر تولید شده در دادگان (با احتساب تصاویر پوششی) عبارت است از ۵۷۶۰۰۰ تصویر (۵*۷*۸*۲۰۰۰+۸*۲۰۰۰ = ۵۷۶۰۰۰).

برای روش‌های مختلف پنهان‌نگاری، نرخ جاسازی به صورت "تعداد ضرایب منتخب به کل ظرفیت ممکن" محاسبه شده است:

- ✓ کل ظرفیت = تعداد ضرایب AC غیر صفر.
- ✓ تعداد ضرایب منتخب = تعداد ضرایبی که برای جاسازی پیغام از بین کل ظرفیت ممکن، انتخاب شده‌اند و پنهان‌نگاری در آن‌ها انجام شده است.

در مورد دو روش JSTEG و OUTGUESS، به‌جز ضرایب DC و صفر، ضرایب ۱ و ۱- نیز هنگام پنهان‌نگاری از مجموعه کنار گذاشته می‌شوند



(شکل۵) : استخراج ویژگیهای مناسب برای تصویر ورودی در هر یک از بخش‌های سیستم و سپس تصمیم‌گیری بر اساس مدل تعلیم‌یافته روی ضریب کیفیت مربوطه.

۴-۳- نتایج عملی روی دادگان مختلف تصویری

در این بخش، نتایج اجرای روش سلسله‌مراتبی خود را بر روی پایگاه دادهٔ معرفی شده در بخش‌های ۴-۱ و ۴-۲ ارائه خواهیم نمود. سیستم نهان‌کاو ما دارای دو بخش اصلی است که در هر یک از آن‌ها ۸ مدل SVM تعلیم‌یافته برای هشت گروه ضریب کیفیت گوناگون، وجود دارد. برای تعلیم هر کدام از این مدل‌های SVM، از ۱۰۰۰ نمونه تصویر پوششی با ضریب کیفیت مشخص در یک سو، و ۱۰۰۰ نمونه تصویر منتخب (به شکل تصادفی) از بین تصاویر پنهان‌نگار متناظر با آن استفاده شده است.

در بخش اوّل برای بالابردن دقت و قابلیت اطمینان سیستم، تعلیم طبقه‌بندی‌کننده‌ها با تصاویر پنهان‌نگاری شده به‌شیوهٔ تطبیق LSB انجام شد. یعنی برای هر یک از هشت مدل SVM موجود در این بخش، ۱۰۰۰ تصویر پوششی (با ضریب کیفیت مشخص اوّل تا هشتم) در یک سو و ۱۰۰۰ تصویر پنهان‌نگار منتخب متناظر با آن در سوی دیگر استفاده شده است. انتخاب تصاویر پنهان‌نگار برای تعلیم، به‌صورت تصادفی بوده است. یعنی از بین ۱۰۰۰*۲*۵ = ۱۰۰۰۰ تصویر موجود (برای دو روش پنهان‌نگاری تطبیق LSB ترتیبی و تصادفی، و نیز ۵ نرخ جاسازی) تعداد هزار تصویر به‌شکل تصادفی انتخاب شده است؛ علّت این امر ایجاد توازن در طبقه‌بندی‌کننده SVM در هنگام تعلیم است، تا زیاد بودن تعداد نمونه‌های پنهان‌نگار، آن را در هنگام یادگیری به اشتباه نیندازد.

اگر چه انتخاب از بین روش‌ها و نرخ‌های جاسازی متنوع باعث می‌شود تعداد نمونه‌هایی که طبقه‌بندی‌کننده در هنگام تعلیم از هر گروه می‌بیند محدود باشد، امّا نتایج تجربی نشان می‌دهد که مدل‌های تعلیم یافته قادرند با دقّت خوبی تصاویر پنهان‌نگار را از روش‌ها و نرخ‌های جاسازی گوناگون تشخیص دهند. این نتایج در (جدول ۲) برای ضرایب کیفیت گوناگون در نرخ‌های جاسازی مختلف دیده می‌شود.

در بخش دوم نیز مشابه با بخش اوّل، هشت مدل SVM برای هشت ضریب کیفیت منتخب ساخته شد. در ساخت این مدل‌های تعلیم یافته نیز، تعداد هزار تصویر پوششی و هزار نمونهٔ پنهان‌نگار از همان ضریب کیفیت

درنظرگرفته شد. نمونه‌های پنهان‌نگار به‌صورت تصادفی از بین تصاویر جاسازی شده با سه روش پنهان‌نگاری و پنج نرخ جاسازی (در مجموع ۱۰۰۰*۵*۳ = ۱۵۰۰۰ تصویر) به‌صورت تصادفی انتخاب گردید (جدول ۳).

نکتهٔ قابل توجّه دیگر آن‌که آزمایش‌های ما نشان داد که اگرچه روش F5 نوعی تطبیق LSB محسوب می‌شود، امّا عملکرد بخش دوم (که بیشتر بر مبنای آمارگان مرتبهٔ اول و هیستوگرام ضرایب عمل می‌کند) در تشخیص F5 بهتر از عملکرد بخش اوّل (مبتنی بر آمارگان مرتبهٔ دوم) است. علت این امر آن است که الگوریتم F5 با آثاری همچون افزودن صفر به مجموعهٔ ضرایب DCT بعد از پنهان‌نگاری، در مشخصات آماری مرتبهٔ اوّل مانند هیستوگرام، نمود و ظهور بیشتری پیدا می‌کند. این در حالی است که الگوریتم F5 از این جهت یک الگوریتم امن تلقی می‌شود که تعداد تغییراتی که در ضرایب DCT ایجاد می‌کند کمتر از تغییرات سایر روش‌هاست. به‌همین جهت می‌توان گفت نسبت به سایر روش‌های تطبیق LSB، همبستگی را بهتر حفظ می‌کند. با توجه به مسائل فوق، روش F5 برای تعلیم و تست در بخش دوم مورد استفاده قرار گرفت.

علاوه‌بر آن، در مورد روش MB1 نیز اگر چه نوعی جای‌گذاری در LSB محسوب می‌شود و انتظار می‌رود در بخش دوم عملکرد بهتری داشته باشد، دیده شد که عملکرد بخش اول برای آن بهتر از بخش دوم است. علّت این امر آن است که الگوریتم MB1 با اصلاح مشخصات آماری مرتبهٔ اوّل، از قدرت ویژگی‌های مبتنی بر هیستوگرام در تشخیص خود (به‌خصوص در نرخ‌های جاسازی کمتر از ۴۰٪) می‌کاهد. اما در عین حال، این روش قادر نیست مشخّصات آماری مرتبهٔ دوم را نیز حفظ کند و کاهش همبستگی‌های محلی ناشی از الگوریتم MB1 سبب می‌شود بخش اوّل بتواند با دقّت بالاتری آن را تشخیص دهد.

همان‌طور که در (جداول ۲ و ۳) دیده می‌شود، در نرخ جاسازی ۲۰٪، دقّت تشخیص عموماً کمتر از ۶۰٪ است. این دقت با افزایش ضریب کیفیت تصاویر افزایش می‌یابد و در ضریب کیفیت ۹۹، به بیش از ۶۰٪ می‌رسد.

۴-۴- مقایسهٔ مشخصات سیستم با روش‌های رقیب

در این مقاله روش‌های محققین در مراجع [۹] و [۲] روی دادگان موجود، پیاده‌سازی و آزمایش شده است. این نتایج در (جدول ۴) به‌صورت درصد صحّت (دقت تشخیص صحیح: TP) نشان داده شده و با روش پیشنهادی خود ما (جدول ۴) مقایسه شده است. همان‌گونه که در (جدول ۴) دیده می‌شود، در شبیه سازی روش معرّفی شده در مرجع [۲]، دو نوع آزمایش انجام شده است: در آزمایش حالت یک، مطابق عملکرد نویسندگان در [۲]، برای هر روش پنهان‌نگاری و هر نرخ جاسازی به‌طور مجزّا تعلیم‌ها و آزمایش‌هایی انجام شده و درصدهای صحّت روی مجموعه‌های آزمایش بیان شده است. در آزمایش حالت دو، تمامی نرخ‌های جاسازی گوناگون از یک روش پنهان‌نگاری، برای تعلیم استفاده شده‌اند. شبیه‌سازی روش معرفی شده در [۹] نیز مطابق کار خود نویسندگان صورت گرفته و برای هر روش پنهان‌نگاری، نمونه‌هایی از نرخ‌های جاسازی گوناگون برای تعلیم استفاده شده‌اند. واضح است که در روش پیشنهادی در این مقاله، حالت عمومی‌تری هنگام تعلیم برقرار است و نمونه‌هایی از روش‌های گوناگون پنهان‌نگاری در نرخهای مختلف جاسازی، برای تعلیم استفاده شده‌اند. در ادامه مزایای سیستم پیشنهادی خود را نسبت به سایر محققین برخواهیم شمرد.

در فرآیند انتخاب و دسته‌بندی ویژگی‌های مناسب جهت نهان‌کاوی، این سیستم برتری‌هایی نسبت به نمونه‌های رقیب دارد، ازجمله آن‌که موارد غیر ضروری و دارای هم‌پوشانی حذف شده‌اند و ویژگی‌ها به‌طورکامل در جهت بازنمایی اثرات مخرب پنهان‌نگاری انتخاب شده‌اند.

علاوه‌بر آن، در فرآیند تعلیم و تست نیز مزایایی برای این سیستم قابل ذکر است. به عنوان مثال، به جای اینکه همچون عملکرد معرفی شده در [۲]، برای هر روش پنهان‌نگاری و هر نرخ جاسازی یک تعلیم و آزمایش مجزّا انجام شود یا اینکه مانند عملکرد پیشنهادی در [۸، ۹] برای هر روش خاص پنهان‌نگاری، یک مدل تولید گردد، برای چند روش پنهان‌نگاری گوناگون و در نرخ‌های مختلف، تنها یک مدل *همه‌جانبه و عمومی* تعلیم داده می‌شود. این کار تعمیم‌پذیری روش را در یک سیستم کاربردی بیشتر می‌کند و وابستگی مدل‌ها به تصاویر تعلیم و روش‌های پنهان‌نگاری به کار رفته در آن‌ها و نیز و نرخ جاسازی کاهش می‌یابد. مدلهای تعلیم‌یافته بدین شکل، قادرند الگوریتم‌های پنهان‌نگاری جدیدی را که عملکردی شبیه به یکی از شش روش MB1، Sequential & Random LSB Matching، JSteg، OutGuess و F5 دارند و سیستم تا به‌حال آن‌ها را ندیده است (مانند SSIS، PVD)، تشخیص دهد. لازم به ذکر است که شش روش پنهان‌نگاری فوق تنها از این جهت

انتخاب شده‌اند که نمایندهٔ گروه خاصی از روش‌های پنهان‌نگاری باشند و انتخاب آن‌ها برای تعلیم مدل‌ها به‌هیچ‌وجه با هدف تشخیص آن الگوریتم‌های خاص نبوده است.

تنها قید اعمال شده بر سیستم پیشنهادی، مربوط به ضریب کیفیت تصاویر JPEG است که برای ضرایب کیفیت مختلف، مدل‌های مختلفی تعلیم داده شده و در سیستم نهایی تعبیه شده است. البته این مسأله نیز در مقایسه با رویکرد پیشنهادی توسط فریدریش (که برای ۳۴ ضریب کیفیت گوناگون، ۳۴ مدل را تعلیم داده است)، متعادل‌تر است؛ زیرا برای هشت ضریب کیفیت مختلف در هر بخش، هشت مدل تعلیم داده شده است. بدین ترتیب، QF های موجود در بازهٔ i ام، مدل تعلیم‌یافتهٔ شمارهٔ i را به‌کار می‌برند. بنابراین، سیستم نهایی شامل هشت مدل در بخش اول و هشت مدل در بخش دوم خواهد بود.

۵- جمع‌بندی و نتیجه‌گیری

در این مقاله برای نهان‌کاوی در تصاویر JPEG، روش بهینه‌ای را معرفی نموده‌ایم که در مقایسه با سایر روش‌های نهان‌کاوی عملکرد بهتری دارد. در این روش، اثر فرآیندهای مختلف پنهان‌نگاری بررسی شده و در الگوریتم‌های مختلف پنهان‌نگاری، این اثرات دسته‌بندی شده‌اند. سپس برای آشکارسازی این اثرات و ایجاد تمایز بین دو گروه تصاویر طبیعی و پنهان‌نگار، یک مجموعه‌ویژگی بهینه انتخاب می‌شود که بیشتر شامل آمارگان مرتبهٔ اوّل و دوم تصویر می‌شود. این ویژگی‌ها براساس یک منطق مشخّص در ساختاری سلسله‌مراتبی برای تعیین پنهان‌نگار بودن یا نبودن یک تصویر مورد استفاده قرار می‌گیرد.

سیستم پیشنهادی دارای دو بخش اصلی است که از دسته‌ویژگی‌های مختلف و روش‌های پنهان‌نگاری متفاوتی ساخته شده‌اند. در این دیدگاه، روش‌های MB1، Sequential & Random LSB Matching در یک دسته قرار می‌گیرند (گروه A)، و روش‌های پنهان‌نگاری JSteg، OutGuess و F5 (و نمونه‌های مشابه آن‌ها) در یک دستهٔ دیگر قرار می‌گیرند (گروه B). بررسی این الگوریتم‌های پنهان‌نگاری نشان داد که روش‌های گروه A، بیشتر مشخصات آماری مرتبهٔ دوم تصویر را تحت تأثیر قرار می‌دهند و روش‌های گروه B، مشخصات آماری مرتبهٔ اول را تغییر می‌دهند. برهمین‌اساس، بخش اول سیستم نهان‌کاو پیشنهادی با تصاویر پنهان‌نگاری شده با الگوریتم‌های گروه A، و بخش دوم آن با تصاویر پنهان‌نگاری شده با الگوریتم‌های گروه B تعلیم و تست می‌شوند.

در هر بخش از سیستم نیز مشخصات متفاوتی از تصویر برای تعلیم و آزمایش مورد استفاده قرار می‌گیرد. دسته‌ویژگی‌های منتخب، به جای تشکیل یک بردار ویژگی واحد و تعلیم با یک طبقه‌بندی‌کننده مشترک، به دو بخش مجزا تقسیم می‌شوند. این دو بخش در یک ساختار درختی و سلسله‌مراتبی قرار می‌گیرند. استفاده از ساختار سلسله مراتبی سبب بالارفتن سرعت و نیز قابلیت اطمینان روش می‌گردد. بحث ضریب کیفیت تصاویر JPEG و اثر آن بر نتایج نهان‌کاوی نیز در این تحقیق به شکل عمومی‌تر و مناسب‌تری نسبت به سایر محققین در نظر گرفته شده است. نتایج به‌دست آمده از این روش نهان‌کاوی، برتری‌های قابل توجهی را نسبت به روش‌های رقیب به نمایش می‌گذارد.

جدول ۱: ضرایب کیفیت منتخب در تولید تصاویر پوششی JPEG از روی تصاویر TIFF اصلی.

ضرایب کیفیت منتخب در نرم‌افزار فوتوشاپ (۰-۱۲)	0	3	4	5	6	7	9	11
مقدار واقعی ضریب کیفیت (مقدار تقریبی)	25	45	52	69	77	83	90	99

جدول ۲: میانگین صحت سیستم برای بخش A (یعنی نرخ تشخیص صحیح برای تصاویر پنهان‌نگار، True Positive (TP) و برای تصاویر پوششی، True Negative (TN)). تعلیم روی هر ضریب کیفیت به‌صورت مجزا برای ۱۰۰۰ تصویر پوششی و ۱۰۰۰ تصویر پنهان‌نگار متناظر با آن‌ها انجام شده است. روش‌های پنهان‌نگاری مورد استفاده عبارتند از تطبیق LSB ترتیبی، تصادفی و روش MB1، نرخ‌های جاسازی نیز عبارتند از ۲۰، ۴۰، ۶۰، ۸۰ و ۱۰۰ درصد. نتایج موجود در جدول حاصل آزمایش این مدل‌های تعلیم یافته روی گروه‌های ۱۰۰۰ تایی از تصاویری غیر از نمونه‌های تعلیم می‌باشد.

QF	Payloads										
	0% (Cover)	20%		40%		60%		80%		100%	
		MB1	Seq and Rand LSB	MB1	Seq and Rand LSB	MB1	Seq and Rand LSB	MB1	Seq and Rand LSB	MB1	Seq and Rand LSB

	Matching		Matching		Matching		Matching		Matching		
100%	87.64	88.78	84.57	78.62	80.07	56.93	67.93	27.19	31.57	87.08	25
93.12	97.10	89.26	95.80	77.01	93.50	48.01	86.56	18.48	50.46	94.23	45
94.73	98.12	93.79	97.02	85.89	95.82	62.42	91.58	21.20	65.42	95.06	52
96.25	98.80	89.76	98.50	75.19	97.70	48.12	95.50	15.45	70.85	97.93	69
94.38	99.11	94.40	99.01	83.31	98.43	58.88	96.54	17.27	78.85	98.01	77
97.44	99.30	87.05	99.01	72.15	98.18	48.72	96.35	14.11	79.56	98.05	83
93.43	99.89	80.41	99.85	61.21	99.80	32.90	99.35	11.06	91.23	99.02	90
90.49	99.95	36.06	99.83	24.27	99.76	13.75	99.05	4.45	90.56	99.47	99

جدول ۳: میانگین صحت سیستم برای بخش B (یعنی نرخ تشخیص صحیح برای تصاویر پنهان‌نگار، True Positive (TP) و برای تصاویر پوششی، True Negative (TN). تعلیم روی هر ضریب کیفیت به صورت مجزّا برای ۱۰۰۰ تصویر پوششی و ۱۰۰۰ تصویر پنهان‌نگار متناظر با آن‌ها انجام شده است. روشهای پنهان‌نگاری مورد استفاده عبارتند از JSteg، OutGuess و F5، نرخ‌های جاسازی نیز عبارتند از ۲۰، ۴۰، ۶۰، ۸۰ و ۱۰۰ درصد. نتایج موجود در جدول حاصل آزمایش این مدل‌های تعلیم یافته روی گروه‌های ۱۰۰۰ تایی از تصاویری غیر از نمونه‌های تعلیم می‌باشد.

Payloads											QF
100%		80%		60%		40%		20%		0% (Cover)	
F5	JSteg, OG	F5	JSteg, OG	F5	JSteg, OG	F5	JSteg, OG	F5	JSteg, OG		
88.17	82.62	88.85	79.88	88.08	75.64	80.76	65.89	57.61	46.00	74.51	25
89.94	95.29	91.30	94.08	91.30	92.31	79.88	85.80	51.85	55.75	81.64	45
93.26	96.23	94.72	94.45	93.26	89.97	85.44	83.56	55.46	49.68	88.18	52
97.16	97.53	96.97	96.73	96.67	94.36	86.52	88.89	53.02	57.71	88.57	69
99.31	96.85	98.92	95.66	98.33	94.48	95.50	91.00	59.27	60.49	89.28	77
97.16	98.42	96.97	96.74	97.36	95.25	89.16	90.50	46.38	59.74	90.72	83
99.51	99.31	99.60	99.21	98.72	98.62	94.13	94.99	42.81	62.86	93.94	90
100	99.89	100	99.79	100	99.79	99.89	98.76	68.37	51.74	98.63	99

جدول ۴: مقایسهٔ درصد صحت روش پیشنهادی با دو نمونه از مهم‌ترین ایده‌های نهان‌کاوی معرفی شده در مراجع [۲] و [۹] برای تصاویر با ضریب کیفیت ۷۷. این مقایسه برای تصاویر پوششی و پنهان‌نگار با نرخ‌های مختلف جاسازی و سه روش پنهان‌نگاری F5، MB1 و OutGuess انجام شده است. در روش پیشنهادی تعلیم روی دسته‌های متنوعی از تصاویر پنهان‌نگار- با روش‌ها و نرخ‌های جاسازی مختلف- انجام شده است. برای روش معرّفی شده در مرجع [۲] دو حالت را در نظر گرفته‌ایم: ۱) تعلیم روی روش‌های پنهان‌نگاری و در هر نرخ جاسازی به شکل مجزا انجام گرفته است، ۲) تعلیم روی تمامی نرخ‌های جاسازی از یک روش خاص پنهان‌نگاری صورت گرفته است. در مورد روش مرجع [۹] نیز تعلیم وتست مشابه حالت ۲ فوق می‌باشد (شمای نرخ‌های جاسازی یک روش خاص پنهان‌نگاری).

MB1				F5				OutGuess				Payload
روش پیشنهادی	۲-[۲]	۱-[۲]	[۹]	روش پیشنهادی	۲-[۲]	۱-[۲]	[۹]	روش پیشنهادی	۲-[۲]	۱-[۲]	[۹]	
95.58	94.99	71.00	67.57	96.09	98.62	91	96.28	94.82	98.42	92	92.87	0%
67.79	31.40	73.60	40.72	82.81	61.13	94	76.66	74.20	63.19	93.81	75.44	20%
78.90	79.39	90.08	53.22	96.97	98.13	98.72	96.87	95.65	96.73	97.54	94.56	40%
93.62	93.81	95.19	62.89	98.63	99.90	99.21	99.12	97.24	98.91	98.52	96.35	60%
97.54	97.25	97.25	69.92	99.21	100	99.50	99.51	97.34	99.60	98.92	95.86	80%
98.72	98.52	98.74	78.80	99.70	100	99.60	99.41	97.54	99.60	98.82	97.64	100%

۶- منابع

[1] J. Fridrich, "Feature-Based Steganalysis for JPEG Images and its Implications for Future Design of Steganographic Schemes", Information Hiding, 6th International Workshop, LNCS 3200, PP 67-81, 2004.

[2] [2]

[3] D. Fu, Y. Q. Shi, D. Zou, G. Xuan, "JPEG Steganalysis Using Empirical Transition Matrix in Block DCT Domain", Workshop on Multimedia Signal Processing, Victoria, BC, Canada, 2006.

[4] T. Pevny, J. Fridrich, "Determining the stego algorithm for JPEG images", IEEE Proc.-Inf. Secur., vol. 153, No. 3, September 2006.

[5] T. Holotyak, J. Fridrich, S. Voloshynovskiy, "Blind Statistical Steganalysis of Additive

Conference on Image Processing (ICIP), Atlanta, GA, USA, October 2006.

[17] Y. Q. Shi, G. Xuan, Ch. Yang, J. Gao, Zh. Zhang, P. Chai, "Effective Steganalysis Based on Statistical Moments of Wavelet Characteristic Function", Proc. International Conference on Information Technology: Coding and Computing, (ITCC'05) IEEE, 2005.

[18] H. Sajedi, M. Jamzad, "A Steganalysis Method Based on Contourlet Transform Coefficients", Proc. International Conference on Intelligent Information Hiding and Multimedia Signal Processing, , PP. 245-248, 2008.

[19] X. Chen, Y. Wang, T. Tan, L. Guo, "Blind Image Steganalysis Based on Statistical Analysis of Empirical Matrix", Proc. 18th International Conference on Pattern Recognition (ICPR), 2006.

[20] Y. Q. Shi, C. Chen, W. Chen, "A Markov Process Based Approach to Effective Attacking JPEG Steganography", Information Hiding, 8th international Workshop, 2006.

[21] J. Fridrich, M. Goljan, D. Hogea, "Steganalysis of JPEG Images: Breaking the F5 algorithm", Fifth International Workshop on Information Hiding, (Noordwijkerhout, Netherlands), Springer Verlag, PP. 310-32, 2005.

[22] B. Li, F. Huang, J. Huang, "STEGANALYSIS OF LSB GREEDY EMBEDDING ALGORITHM FOR JPEG IMAGES USING COEFFICIENT SYMMETRY", IEEE, Proc. ICIP 2007.

[23] X. Yu, N. Babaguchi, "Breaking the YASS Algorithm via Pixel and DCT Coefficients Analysis", Japan Graduate School of Engineering, Osaka University, IEEE, 2008.

[24] D. Zou, Y. Q. Shi, W. Su, G. Xuan, "Steganalysis Based on Markov Model of Thresholded Prediction-Error Image", Proc. IEEE International Conference on Multimedia and Expo (ICME), Toronto, ON, Canada, 2006.

[25] A. Westfeld, A. Pfitzmann, "Attacks on Steganographic Systems, Breaking the Steganographic Utilities EzStego, JSteg, Steganos, and S-Tools—and Some Lessons Learned", Proc. Information Hiding—3rd Int'l Workshop, Springer Verlag, PP. 61–76, 1999.

[26] N. Provos, "Defending Against Statistical Analysis", Center for Information Technology Integration, University of Michigan, 1999.

[27] J. Fridrich, J. Kodovský, and T. Pevný. "Statistically undetectable JPEG steganography: Dead ends, challenges, and opportunities". In ACM Multimedia & Security Workshop, pages 3–14, September 20–21 2007.

[28] D.C. Wu and W.H. Tsai, "A steganographic method for images by pixel-value differencing", Pattern Recognition Letters, 2003.

[29] Ker, A. D.: Resampling and the Detection of LSB Matching in Colour Bitmaps. In: Delp, E. J., Wong, P. W. (eds.): Security, Steganography and Steganography Using Wavelet Higher Order Statistics", Proc. 9th IFIP TC-6 TC-11 Conference on Communications and Multimedia Security, Salzburg, Austria, September 19–21, 2005.

[6] F. Huang, B. Li, J. Huang, "Universal JPEG Steganalysis Based on Microscopic and Macroscopic Calibration", Proc. ICIP, PP. 2068-2071, IEEE 2008.

[7] T. Pevny, J. Fridrich, "Multi-class Blind Steganalysis for JPEG Images", Proc. SPIE Electronic Imaging, Photonics West, January 2006.

[8] T. Pevny, J. Fridrich, "Towards Multi-class Blind Steganalyzer for JPEG Images", Proc. International Workshop on Digital Watermarking, vol. 3710 of Lecture Notes in Computer Science, Siena, Italy, Springer-Verlag, Berlin, September 15–17, 2005.

[9] T. Pevny, J. Fridrich, "Multi-Class Detector of Current Steganographic Methods for JPEG Format",, Department of Electrical and Computer Engineering, Binghamton, 2008.

[10] T. Pevny, J. Fridrich, "Merging Markov and DCT Features for Multi-Class JPEG Steganalysis", In E.J. Delp and P.W. Wong, editors, Proc. SPIE, Electronic Imaging, Security, Steganography, and Watermarking of Multimedia Contents IX, vol. 6505, PP. 03–04 January 2007.

[11] J. Fridrich, M. Goljan, R. Du, "Steganalysis Based on JPEG Compatibility", Proc. Special Digital Watermarking Data Hiding, pp. 275-280, 2001: http://www.ssie.binghamton.edu/fridrich.

[12] X. Y. Luo, D. S. Wang, P. Wang, F. L. Liu, "A review on blind detection for image steganography", Signal Processing, doi:10.1016/j.sigpro.2008.03.016, (www.elsevier.com/locate/sigpro), 2008.

[13] S. Lyu, H. Farid, "Detecting Hidden Messages Using Higher-Order Statistics and Support Vector Machines" Proc. 5th International Workshop on Information Hiding, 2002.

[14] S. H. ZHAN, H. B. ZHANG, "BLIND STEGANALYSIS USING WAVELET STATISTICS AND ANOVA", Proc. 6th International Conference on Machine Learning and Cybernetics, Hong Kong, 19-22 August 2007.

[15] G. Xuan, Y. Q. Shi, J. F. Gao, D. Zou, Ch. Yang, Zh. Zhang, P. Chai, C. Chen, W. Chen, "Steganalysis Based on Multiple Features Formed by Statistical Moments of Wavelet Characteristic Functions", Springer-Verlag Berlin Heidelberg, LNCS 3727, PP. 262 – 277, 2005.

[16] C. Chen, Y. Q. Shi, W. Chen, G. Xuan, "STATISTICAL MOMENTS BASED UNIVERSAL STEGANALYSIS USING JPEG 2-D ARRAY AND 2-D CHARACTERISTIC FUNCTION", Proc. IEEE International

Watermarking of Multimedia Contents VII, Proc. of SPIE, San Jose, CA (2005) 1–15.
[30] Rainer B¨ohme, "Assessment of Steganalytic Methods Using Multiple Regression Models", Technische Universit¨at Dresden, Institute for System Architecture, Germany, 2005.
[31] L. M. Marvel, Jr. C. G. Boncelet, C. T. Retter, "Spread spectrum image steganography", IEEE Trans. on Image Processing, Vol. 8(8), PP. 1075-1083, 1999.
[32] K. Sullivan, U. Madhow, Sh. Chandrasekaran, B.S. Manjunath, "Steganalysis of Spread Spectrum Data Hiding Exploiting Cover Memory", in Proc. IST/SPIE 17th Annu. Symp. Electronic Imaging Science Technology, San Jose, CA, pp. 38–46, Jan. 2005.
[33] J. J. Harmsen, "STEGANALYSIS OF ADDITIVE NOISE MODELABLE INFORMATION HIDING", MASTER OF SCIENCE Thesis, Rensselaer Polytechnic Institute Troy, New York, April 2003.
[34] V. Sabeti, Sh. Samavi, M. Mahdavi, Sh. Shirani, "Steganalysis of Embedding in Difference of Image Pixel Pairs by Neural Network", The ISC (ISeCure) International Journal of Information Security, vol. 1, No. 1, PP. 17 - 26, January 2009.
[35] A. Ker, "Steganalysis of LSB matching in grayscale images," IEEE Signal Process. Lett., vol. 12, No. 6, PP. 441–444, June 2005
[36] X. Mankun, L. Tianyun, P. Xijian, "Steganalysis Of LSB Matching Based On Wavelet Denoising Estimation in Grayscale Image", Proc. 2nd International Conference on Future Generation Communication and Networking, IEEE, 2008.
[37] J. Zhang, I. J. Cox, G. Do¨err, "Steganalysis for LSB Matching in Images with High-frequency Noise", Proc. MMSP,PP. 385-388, IEEE, 2007.
[38] M. Abolghasemi, H. Aghainia, K. Faez, M. A. Mehrabi, "LSB Data Hiding Detection Based on Gray Level Co-Occurrence Matrix (GLCM)", *Proc. International Symposium on Telecommunications,* PP. 656-659 , *IEEE*, 2008

مریم بیگ‌زاده مدرک کارشناسی خود را در رشتهٔ مهندسی پزشکی- بالینی در سال ۱۳۸۵ از دانشگاه صنعتی امیرکبیر (پلی تکنیک تهران) و مدرک کارشناسی ارشد در رشتهٔ مهندسی پزشکی - بیوالکتریک را در سال ۱۳۸۷ از همان دانشگاه اخذ نموده است. زمینه‌های تحقیقاتی مورد علاقهٔ وی پردازش تصویر، بینایی ماشین و پردازش سیگنال‌های حیاتی می‌باشد.

نشانی (رایانامک) پست الکترونیکی ایشان عبارت است از: **mbeigzadeh@jmail.com**

محمّد رضایی مدرک کارشناسی خود را در رشتهٔ مهندسی برق - الکترونیک در سال ۱۳۷۵ از دانشگاه صنعتی امیرکبیر (پلی تکنیک تهران) و مدرک کارشناسی ارشد در رشتهٔ مهندسی پزشکی- بیوالکتریک را در سال ۱۳۸۲ از همان دانشگاه اخذ نموده است. زمینه‌های تحقیقاتی مورد علاقهٔ وی پردازش تصویر و ویدئو، کدینگ تصویر و ویدئو و همچنین بینایی ماشین می‌باشد.

نشانی (رایانامک) پست الکترونیکی ایشان عبارت است از: **rezaei.image@yahoo.com**

فاطمه السادات جمالی دینان مدرک کارشناسی خود را در رشتهٔ مهندسی برق- الکترونیک در سال ۱۳۸۳ از دانشگاه دکتر شریعتی و مدرک کارشناسی ارشد در رشتهٔ مهندسی پزشکی- بیوالکتریک را در سال ۱۳۸۶ از دانشگاه صنعتی خواجه نصیرالدین طوسی اخذ نموده است. زمینه‌های تحقیقاتی مورد علاقهٔ وی پردازش تصویر و سیگنال، بینایی ماشین و بازشناسی الگو می‌باشد.

نشانی (رایانامک) پست الکترونیکی ایشان عبارت است از: **jamalidinan@jmail.com**

این الگوریتم استفاده و با در نظرگرفتن اطّلاعات زمانی توالی تصاویر، عابر پیاده را ردگیری کرد. از مزایای این روش و استفاده از تصاویر مادون قرمز این است که می‌توان از این نوع نظارت برای مواقعی که نور کافی برای تصویربرداری وجود ندارد (مانند شب)، استفاده کرد.

۵- مراجع

[1] http://nncf.unl.edu/eldercare/info/seniordriving/nightdrive.html. Technical Report 6, Nebraska Highway Safety Program and the Lincoln-Lancaster County Health Department, July 2001.

[2] M Bertozzi, A Broggi, MD Rose, A Lasagni, "Infrared Stereo Vision-based Pedestrian Detection", Procs. IEEE Intelligent Vehicles Symposium, 2005.

[3] L. Zhao and C. Thorpe, "Stereo and neural network-based pedestrian detection," IEEE Trans. on Intelligent Transportation Systems, vol. 1, no. 3, pp. 148–154, Sept. 2000.

[4] C. Mertz, S. McNeil, and C. Thorpe, "Side collision warning systems for transit buses," in IEEE Intelligent Vehicle Symp., Oct. 2000.

[5] M. Bertozzi et al., "Pedestrian detection in infrared images," in Proc. IEEE Intelligent Vehicles Symp., Columbus, OH, pp. 662–667, June 2003.

[6] A. Broggi et al., "Shape-based pedestrian detection," in Proc. IEEE Intelligent Vehicles Symp., Dearbon, MI, pp. 215–220, 2000.

[7] Takayuki Tsuji, Hiroshi Hattori, Masahito Watanabe, and Nobuharu Nagaoka. "Development of night-vision system", IEEE Transactions on ITS, Vol. 3 No.3, pages 203-209, Sept. 2002.

[8] H. Elzein et al., "A motion and shape-based pedestrian detection algorithm," in Proc. IEEE Intelligent Vehicles Symp., Columbus, OH, pp. 500–504, June 2003.

[۹] م. محسنی، م. سریانی. تشخیص عابر پیاده در توالی تصاویر مادون قرمز با استفاده از SVM . کنفرانس ماشین بینایی و پردازش تصویر ایران، ۱۳۸۷.

[10] A. Mohan and T. Poggio, "Example-based object detection in images by components," IEEE Trans.Pattern Anal.Machine Intell., vol. 23, pp. 349–361, Apr. 2001.

[11] H. Nanda and L. Davis, "Probabilistic template based pedestrian detection in infrared videos," presented at the IEEE IntelligentVehicles Symp., Versailles, France, June 2002.

[12] B. E. Boser, I. M. Guyon and V. N.Vapnik, "A training algorithm for optimal margin classifiers", Proceedings of the fifth annual workshop on Computational learning theory, 1992.

[13] J. Davis and V. Sharma, "Background-Subtraction using Contour-based Fusion of Thermal and Visible Imagery," Computer Vision and Image Understanding, Vol 106, No. 2-3, 2007, pp. 162-182.

[14] OSU Thermal Pedestrian Database, http://www.cse.ohio-state.edu/otcbvs-bench/

[15] Support Vector Machine toolbox for Matlab Version 2.51, Anton Schwaighofer. January 2002.

محسن محسنی تحصیلات خود را در رشتهٔ ریاضی کاربرد در کامپیوتر در سال ۱۳۷۹ به پایان رسانید و مدرک کارشناسی ارشد در رشتهٔ مهندسی کامپیوتر گرایش هوش مصنوعی و روباتیک را در سال ۱۳۸۸ از دانشگاه علم و صنعت تهران اخذ نمود و هم اکنون عضو هیأت علمی و مدیر گروه کامپیوتر دانشگاه آزاد ملارد می‌باشد . حوزه پژوهشی مورد علاقهٔ وی پردازش تصویر می‌باشد .

نشانی (رایانامک) پست الکترونیکی ایشان عبارت است از: **M_mohseni@comp.iust.ac.ir**

محسن سریانی متولّد ۱۳۳۵ در مشهد است. او دورهٔ کارشناسی را در رشتهٔ مهندسی برق - الکترونیک در سال ۱۳۵۹ در دانشگاه علم وصنعت ایران به پایان رساند. در سال ۱۳۶۴ با بورس وزارت علوم، جهت ادامهٔ تحصیل به انگلستان رفت. مدارک کارشناسی ارشد و دکتری را به ترتیب در سال‌های ۱۳۶۶ و ۱۳۶۹ در رشهٔ مهندسی الکترونیک با تخصّص پردازش تصویر از دانشگاه هریوت- وات در شهر ادینبورگ اسکاتلند اخذ نمود. وی در حال حاضر استادیار گروه سخت افزار دانشکدهٔ مهندسی کامپیوتر دانشگاه علم و صنعت می‌باشد. زمینه‌های تحقیق مورد علاقهٔ او آنالیز و پردازش تصاویر، پردازش تصاویر ماهواره‌ای، معماری سیستم‌های کامپیوتری و شبکه‌های سنسور بیسیم هستند.

نشانی (رایانامک) پست الکترونیکی ایشان عبارت است از: **soryani@iust.ac.ir**