پنجمین کنفرانس انجمن رمز ایران
انجمن رمز ایران
Iranian Society of Cryptology
۲۴ الی ۲۶ مهر ماه ۱۳۸۶ دانشگاه علم و صنعت ایران

پنهان نگاری در حوزه تبدیل با استفاده از بلاک بندی شبه تصادفی

مجتبی مهدوی
دانشگاه صنعتی اصفهان
mahdavi@ec.iut.ac.ir

شادرخ سماوی
دانشگاه صنعتی اصفهان
samavi96@ec.iut.ac.ir

وجیهه ثابتی
دانشگاه صنعتی اصفهان
vajiheh.Sabeti@gmail.com

چکیده: تاکنون روش‌های متعددی برای پنهان‌نگاری در تصاویر پیشنهاد شده است. این روش‌ها از دو حوزه مکانی و تبدیل برای جاسازی داده استفاده می‌کنند. روش‌های جاسازی در حوزه مکان معمولاً برای تصاویر BMP و روش های جاسازی در حوزه تبدیل معمولاً برای تصاویر JPEG استفاده می‌شوند. بسیاری از این روش‌ها با استفاده از حملات موجود به راحتی شکسته می‌شوند. روش جدید پیشنهادی در این مقاله، برای جاسازی در تصاویر BMP از حوزه تبدیل استفاده می‌کند و برای مقابله با حملات شناخته شده، از ایده بلاک بندی با ابعاد شبه تصادفی بهره می‌برد. در واقع با پنهان کردن محدوده بلاک‌ها از دید حمله کننده، در برابر حملات ارائه شده برای روش‌های Jsteg و OutGuess ایستادگی می‌کند. نتایج پیاده سازی صحت عملکرد و امنیت روش پیشنهادی را تایید می‌کند.

واژه های کلیدی: پنهان‌نگاری، پنهان‌شکنی، حوزه تبدیل، تصاویر BMP، پوشانه، گنجانه

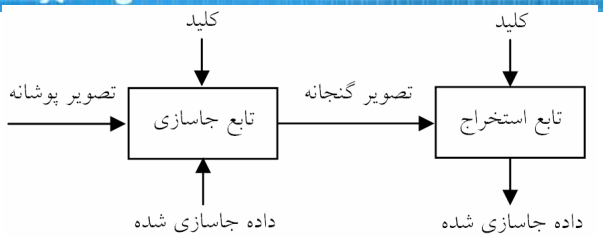
۱- مقدمه

پنهان‌نگاری[1] شاخه‌ای از علم مخفی‌سازی اطلاعات[2] است. در پنهان‌نگاری، پیام سری به گونه‌ای ارسال می‌شود که وجود آن غیر قابل کشف باشد. پنهان‌نگاری هنر و علم پنهان کردن ارتباطات است. در پنهان‌نگاری، پیام سری داخل شئ پوششی[3] به گونه‌ای مخفی می‌شود که قابل کشف نباشد. در صورتی که شخص سومی به وجود پیام مخفی در شئ پوشش شک کند، روش پنهان‌نگاری شکست خورده است[1].

اگرچه رمزنگاری و ته‌نقش نگاری[4] نیز مفاهیمی مشابه پنهان نگاری دارند، اما تفاوت‌هایی بین این سه شاخه مخفی‌سازی اطلاعات وجود دارد. در رمزنگاری، هدف غیر قابل فهم بودن پیام برای شخص سوم است و پیام رمزی ممکن است گمان گیرنده نامرتبط را برانگیزد. از طرف دیگر در ته‌نقش نگاری، پیام مرتبط با خود پوشش است و برای اهدافی مانند حفظ حق کپی، اثبات مالکیت و... استفاده می‌شود. اما در پنهان-نگاری پوشش تنها یک وسیله برای پنهان کردن ارتباط است و وجود ارتباط باید غیرقابل کشف باشد[2].

تصاویر، معمولترین رسانه پوششی است که برای پنهان‌نگاری استفاده می‌شود. در زمینه پنهان‌نگاری تصاویر، بعضی از اجزاء از اهمیت خاصی برخوردارند. شکل ۱، اجزاء مختلف پنهان نگاری و ارتباط بین آن‌ها را نشان می‌دهد[3].

1 steganography
2 Information Hiding
3 Cover media
4 Watermarking



شکل ۱: مدل کلی سیستم‌های پنهان‌نگاری در تصاویر

معمولا برای استفاده بهتر از ظرفیت تصویر و بعلاوه دلایل امنیتی، اعمال دو ماژول فشرده سازی و رمز نگاری روی داده مورد نظر قبل از انجام تابع جاسازی صورت می گیرد.

با رواج یافتن روش‌های پنهان‌نگاری، علم دیگری با عنوان پنهان شکنی[5] رونق یافت. پنهان شکنی، روش‌هایی برای حمله و شکست الگوریتم‌های پنهان‌نگاری است. برای یک ارتباط سری، تنها کشف و اثبات وجود داده مخفی در تصویر گنجانه، حمله موفق به حساب می‌آید. روش‌های پنهان شکنی برای اثبات وجود داده پنهانی، از تغییرات ویژگی‌های آماری تصویر استفاده می‌کنند که در اثر استفاده از روش‌های پنهان-نگاری ایجاد شده‌اند[5].

استفاده از بیت‌های کم ارزش پیکسل‌های تصویر از روش‌های معمول در پنهان‌نگاری است. دو گروه عمده از این روش‌ها LSB-F[6] و LSB-M[7] هستند. در روش LSB-F داده موردنظر مستقیماً در بیت کم ارزش قرار داده می‌شود. اما در روش LSB-M، در صورت عدم تطابق بیت کم ارزش با داده موردنظر، مقدار پیکسل به صورت تصادفی یک واحد افزایش یا کاهش داده می‌شود. در واقع در این روش محدودیت تغییر حداکثر یک بیت از مقدار پیکسل وجود ندارد. ظرفیت مناسب و عدم حساسیت چشم به تغییرات بیت کم ارزش از مزایای این دسته از روش‌ها است[6].

مقاومت کم روش‌های جاسازی در حوزه مکان تصویر در مقابل تغییرات متداول روی تصاویر مانند نویز، فشرده سازی و بعلاوه حملات آماری شناخته شده باعث شده است که در بعضی از روش‌ها از حوزه تبدیل برای جاسازی پیام استفاده شود. از معروفترین روش‌های جاسازی در حوزه تبدیل می-توان به روش‌های Jsteg، Outgess و F5 [7,8] اشاره کرد. این روش‌ها برای پنهان نگاری در تصاویر JPEG از حوزه DCT استفاده می‌کنند. البته این روش‌ها نیز با موفقیت شکسته شده-اند[9,10].

روش ارائه شده در [11]، از جدیدترین روش‌هایی است که برای جاسازی در تصاویر JPEG پیشنهاد شده است. در این روش از فضای فرکانسی تصویر قبل از مرحله فشرده سازی JPEG، برای پنهان‌نگاری استفاده می‌شود. در این روش ابتدا تصویر BMP با استفاده از تبدیل DCT به فضای فرکانسی برده می‌شود و پنهان نگاری در ضرایب آن انجام می‌شود. سپس عکس تبدیل انجام شده و تصویر به فضای مکانی برگردانده می‌شود. تصویر حاصل تحت فشرده سازی JPEG قرار می‌گیرد و ادعا می‌شود که تصویر حاصل دارای پیام پنهان شده است. نتایج ارائه شده در [11] مقاومت این روش در برابر حملات موجود در [9,10] را نشان می دهد.

روش ارائه شده در [11]، در برابر حملات کوری[8] تست نشده است که به تصاویر JPEG حمله می‌کنند.حملاتی مانند [12-15] ادعا می‌کنند که تمام روش‌های شناخته شده جاسازی در JPEG را می‌توانند کشف کنند. روش ارائه شده در [15] با استخراج ۲۷۴ خصیصه متفاوت از تصویر JPEG و با استفاده از یک شبکه عصبی که بر روی طیف وسیعی از تصاویر JPEG آموزش دیده است، عرصه پنهان نگاری در تصاویر JPEG را بسیار تنگ کرده است.

اکثر روش‌های پنهان‌نگاری که تا به حال پیشنهاد شده‌اند، برای جاسازی در تصاویر BMP از حوزه مکان و برای جاسازی در تصاویر JPEG از حوزه DCT استفاده می‌کنند. ایده ارائه شده در این مقاله ترکیبی از این دو روش است. در واقع در روش جدید پیشنهاد می‌شود که برای جاسازی در تصاویر BMP از حوزه تبدیل استفاده شود.

در اکثر روش‌هایی که از حوزه تبدیل برای جاسازی استفاده می‌کنند نوعی بلاک‌بندی وجود دارد. در صورتی که این بلاک بندی برای حمله کننده مشخص باشد، حمله کننده می‌تواند به بسیاری از خواص آماری بلاک دسترسی پیدا کند و آن ها را برای اجرای حمله‌ای موفق استفاده نماید. در واقع یکی از دلایل موفقیت روش‌های حمله به جاسازی در حوزه فرکانس وجود بلاک‌های هم‌اندازه و منظم می‌باشد.

[5] Steganalysis
[6] LSB Flipping (LSB_F)
[7] LSB Matching (LSB-M)
[8] Blind Steganalysis

در بخش ۲، روش پشنهادی با عنوان "پنهان‌نگاری در حوزه تبدیل تصاویر BMP با استفاده از بلاک بندی شبه تصادفی" را معرفی می‌کنیم. این روش را به اختصار PRB[9] می‌نامیم. در این بخش علاوه بر بیان الگوریتم کلی این روش و شرح چگونگی رفع مشکل جاسازی در حوزه تبدیل، دلایل مقاومت این روش در برابر حملات شناخته شده را نیز بررسی می‌کنیم. در بخش۳، نتایج پیاده سازی این روش ارائه می‌شود.

۲- معرفی روش پیشنهادی (PRB)

روش‌های جاسازی در بیت‌های کم ارزش پیکسل‌ها (LSB-F و LSB-M) معمولاً از حوزه مکانی تصاویر BMP استفاده می‌کنند. اما روش‌های جاسازی در حوزه تبدیل معمولاً روی ضرایب تبدیل DCT در تصاویر JPEG اعمال می‌شوند. در روش جدیدی که در این مقاله پیشنهاد می‌کنیم برای جاسازی در تصاویر BMP از حوزه تبدیل و با بلوک بندی شبه تصادفی استفاده می‌کنیم.

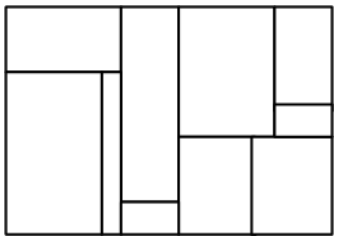
الگوریتمی که ارائه می‌دهیم برای تصاویر خاکستری می‌باشد ولی می‌توان آنرا برای تصاویر رنگی نیز تعمیم داد. تصاویر RGB را می توان سه سطح خاکستری در نظر گرفت.

دراین بخش ابتدا الگوریتم کلی روش پیشنهادی را معرفی می‌کنیم. سپس در ادامه مشکلات جاسازی پیام در ضرایب DCT و راه حل‌های پیشنهادی برای رفع آن‌ها را بررسی می‌کنیم. در انتها نیز دلایل مقاومت این روش در برابر حملات گوناگون را شرح می‌دهیم.

۲-۱- کلیات PRB

روش پیشنهادی در این مقاله برای تصاویر BMP قابل استفاده است و در گروه روش‌های جاسازی در حوزه تبدیل قرار می‌گیرد. الگوریتم کلی این دسته از روش‌ها بدین ترتیب است که ابتدا تصویر با استفاده از یکی از تبدیل‌های موجود به فضای فرکانسی برده می‌شود. بعد از جاسازی در ضرایب فرکانسی، عکس تبدیل موردنظر بر روی تصویر اعمال شده و تصویر به فضای مکانی برگردانده می‌شود[2].

نکته مهم در روش PRB این است که بلاک‌بندی به صورت شبه تصادفی انجام می‌شود. ابعاد هر بلاک به صورت شبه تصادفی با استفاده از یک مولد اعداد شبه تصادفی انتخاب می‌شود. این اعداد به گونه‌ای است که گیرنده تصویر گنجانه قادر به تولید مجدد آن‌ها باشد و بتواند بلاک‌بندی را دقیقاً مانند فرستنده انجام دهد. در شکل۲، مثالی از بلاک‌بندی یک تصویر نمایش داده شده است. در بخش ۲-۳ در مورد دلایل استفاده از بلاک بندی با ابعاد تصادفی بحث می‌شود.



شکل ۲: مثالی از بلاک‌بندی با ابعاد شبه تصادفی تصویر

الگوریتم PRB ابتدا تصویر BMP را به بلاک‌هایی با ابعاد شبه تصادفی تقسیم بندی می‌کنیم. سپس روی هر بلاک تبدیل موردنظر را اعمال می‌کنیم. در این پیاده سازی از تبدیل DCT به این منظور استفاده شده است، اما امکان انتخاب تبدیل‌های دیگر نیز وجود دارد. سپس در ضرایب تبدیل هر بلاک جاسازی را انجام می‌دهیم. جاسازی می‌تواند به روش‌های مختلفی انجام شود. روش‌های LSB-F و LSB-M از ساده‌ترین روش‌هایی است که می‌تواند در این مرحله استفاده شود. جاسازی در ضرایب DCT دارای مشکلاتی است که این مشکلات و راه حل‌هایی برای رفع آن در زیر بخش بعدی بررسی می‌شود. پس از انجام جاسازی، عکس تبدیل را روی بلاک اعمال کرده و بلاک حاصل را در مکان متناظر با تصویر پوشانه در تصویر گنجانه قرار می‌دهیم.

۲-۲- جاسازی با PRB

الگوریتم PRB بعد از اعمال تبدیل DCT روی هر بلاک، پیام سری را در ضرایب تبدیل جاسازی می‌کند. بعد از انجام جاسازی باید با اعمال تبدیل معکوس، بلاک را به حوزه مکانی برگرداند. این انتظار وجود دارد که گیرنده نیز با انجام تبدیل DCT روی بلاک بتواند داده پنهان شده را به روش مناسب از ضرایب تبدیل استخراج کند، اما در عمل این گونه نیست. دلیل این مشکل آن است که عکس تبدیل DCT بر روی ضرایب حاوی داده سری، اعداد صحیح تولید نمی‌کند. در حالی که مقادیر پیکسل‌ها باید اعدادی صحیح باشند. بنابراین لازم است که ضرائب مورد نظر به نزدیکترین عدد صحیح کوانتیزه شوند. در این صورت گیرنده با گرفتن تبدیل

[9] Pseudo Random Blocking

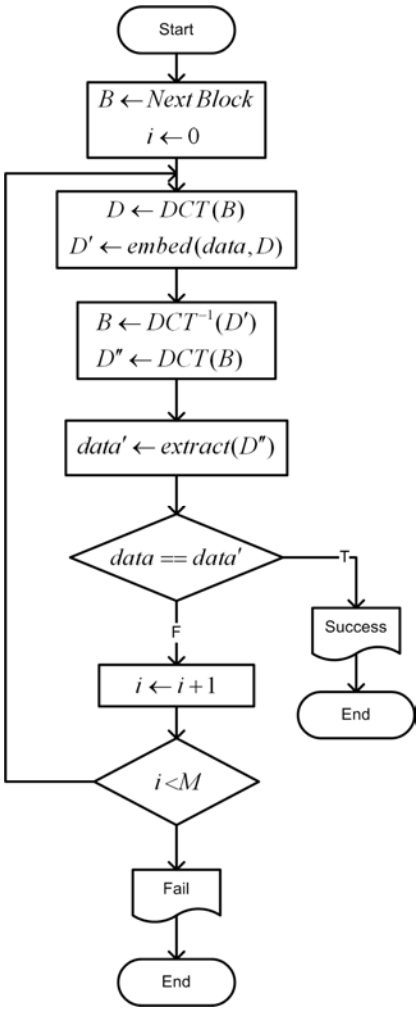
DCT به همان ضرایبی نخواهد رسید که در اثر جاسازی ایجاد شده‌اند و پیام بدرستی استخراج نخواهد شد.

بیشترین تأثیر این مشکل در کم ارزش‌ترین بیت‌های ضرایب تبدیل رخ می‌دهد. بنابراین نمی‌توان به ثابت ماندن کم ارزش-ترین بیت ضرایب تبدیل اعتماد کرد و استفاده از آن برای جاسازی باعث نابود شدن داده جاسازی شده می‌شود. برای حل این مشکل، می‌توان پیام موردنظر را در دومین بیت کم ارزش ضرایب DCT جاسازی کنیم. بدین ترتیب احتمال خراب شدن بیت حاوی داده در اثر اعمال تبدیل معکوس کمتر می‌شود. اما آزمایشات مختلف نشان می‌دهد که این احتمال صفر نیست. بنابراین هنوز هم خطر از دست رفتن داده جاسازی شده وجود دارد و نیاز به تغییری داریم تا پیام مورد نظر به طور کامل استخراج شود.

آزمایشات مختلف نشان می‌دهد که اگر جاسازی پیام در ضرایب DCT بلاک را تکرار کنیم، با احتمال بسیار زیاد بعد از تعدادی تکرار قادر به استخراج کامل پیام از ضرایب DCT هستیم. بنابراین بعد از هر بار جاسازی باید عملیات استخراج انجام شود و آزمایش شود که "آیا گیرنده قادر به استخراج پیام موجود در این بلاک است؟". عملیات جاسازی و استخراج را تا زمانی تکرار می‌کنیم که استخراج پیام امکان پذیر باشد. باید به این نکته توجه شود که در هر تکرار، جاسازی پیام مجدداً در بلاکی انجام می‌شود که در اثر جاسازی مرحله قبل تولید شده است.

همچنین ذکر این نکته لازم است که چنین عملی باعث تجمع خطا در بلاک تصویر نمی‌گردد. زیرا این فرایند باعث همگرایی به ضرایبی می‌گردد که بتوان داده سری را از آن استخراج کرد. نتایج آزمایشات گوناگون این نکته را تأیید کرده است. شکل ۳، الگوریتم جاسازی را نشان می‌دهد.

مطابق شکل۳، ابتدا یک بلاک انتخاب می‌گردد (B) که در مرحله تولید بلاک‌های با ابعاد شبه تصادفی تولید شده است. سپس از آن DCT اخذ می‌گردد (D) و داده موردنظر (data) در ضرایب بدست آمده جاسازی می‌شود (embed(data,D)). اکنون باید مطمئن شویم که داده جاسازی شده قابل استخراج است. از ضرایبی که پس از جاسازی بدست آمده است (D')، تبدیل معکوس DCT اخذ می‌کنیم و در B قرار می-دهیم و دوباره از آن DCT می‌گیریم (D'') و داده پنهان شده را از آن استخراج می‌کنیم (extract).



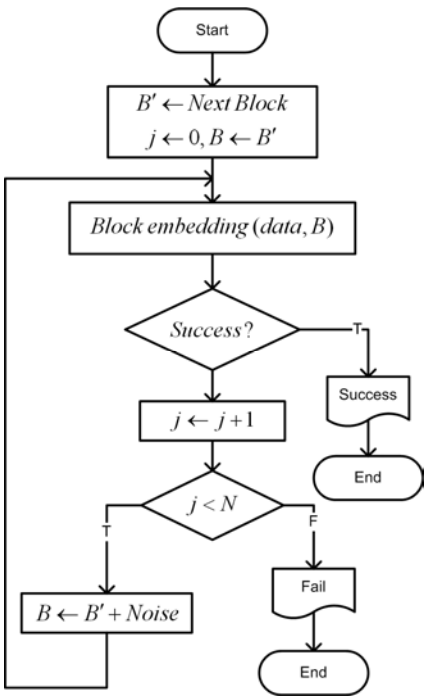
شکل۳: پروسه جاسازی در یک بلاک (*Block embedding (data,B)*)

در صورتی که داده استخراج شده ($data'$) و داده پنهان شده برابر باشند، کار جاسازی در این بلاک پایان یافته است (success). در غیر این صورت، عملیات را با B دوباره تکرار می‌کنیم. با تکرار جاسازی در یک بلاک نیز ممکن است نتوان داده مورد نظر را جاسازی نمود (fail). به همین منظور تعداد این تکرار را با حداکثر مقداری مانند M محدود می‌کنیم. در مورد M در بخش ۳ توضیحات بیشتری ارائه خواهد شد.

در روش بیان شده می‌توان از تمام ضرایب DCT برای جاسازی استفاده کرد. در صورتی که تعداد بیت‌های داده‌ای که قرار است جاسازی شود، کمتر از ابعاد تصویر باشد، به همان نسبت از ضرایب کمتری برای جاسازی استفاده می‌کنیم. برای مثال، اگر طول داده بر حسب بیت، نصف تعداد پیکسل‌های تصویر باشد (هر پیکسل از تصویر معادل یک ضریب DCT

است)، از نیمی از ضرایب هر بلاک برای جاسازی استفاده می‌کنیم.

در بسیاری از تصاویر با تعداد تکرار کم به هدف مورد نظر می‌رسیم، اما در تعدادی از تصاویر حتی با انجام این تکرار قادر به استخراج کامل پیام از بلاک نیستیم. اگر جاسازی مکرر پیام در ضرایب DCT، مشکل استخراج کامل پیام را رفع نکند، می‌توان نتیجه گرفت که نوعی همبستگی در پیکسل‌های بلاک وجود دارد که باعث این مشکل شده است. برای حل این مشکل می‌توانیم با استفاده از یک تغییر این همبستگی را کاهش دهیم. این تغییر به صورت افزودن یک نویز تصادفی با توان بسیار پایین به بلاک مورد نظر است. این نویز می‌تواند به صورت کاهش یا افزایش یک واحدی در مقدار پیکسل‌ها باشد. برای جلوگیری از تجمع خطا در بلاک، نویز را به بلاک اصلی (B) در هر گام اضافه می‌کنیم. فلوچارت کامل روش جاسازی با بهبودهای موردنظر در شکل ۴ نشان داده شده است.



شکل ٤: فلوچارت کامل جاسازی در یک بلاک

مطابق فلوچارت نمایش داده شده در شکل۴، ابتدا یک بلاک با ابعاد شبه تصادفی را انتخاب می‌نماییم (B') و یک کپی از آن (B) را به پروسه جاسازی در یک بلاک (Block embedding) ارسال می‌کنیم(شکل ۳). در صورت عدم موفقیت در جاسازی مقداری نویز با توان کم به بلاک می‌افزاییم و عملیات را دوباره تکرار می‌کنیم. تعداد این تکرار را نیز با مقدار حداکثر (N) محدود می‌کنیم.

در بخش ۳، نتایج آزمایشات مختلف برای انتخاب مناسب M و N مناسب در تصاویر ارائه می‌شود. بلاکی که بعد از N بار اضافه کردن نویز و در هر بار نویز اضافه کردن با M تکرار جاسازی، نتواند پیام را بعد از تبدیل معکوس حفظ کند، نمی‌تواند در این روش استفاده شود. احتمال وجود این بلاک‌ها در تصاویر بسیار کم است. تصویری که چنین بلاکی داشته باشد برای پنهان‌نگاری با روش پیشنهادی مناسب نیست.

حملات موجود در [2,9,10] باعث شده است که جاسازی در حوزه فرکانس DCT به روش‌های معمول قابل کشف باشد. اما در این مقاله ادعا می‌شود که با وجود جاسازی در حوزه DCT، روش پیشنهادی PRB در مقابل حملات موجود مقاوم است. در این بخش دلایل این ادعا بررسی می‌شود.

در حمله به روش Jsteg [2] از این ویژگی استفاده شده است که جاسازی در ضرایب DCT باعث تغییر هیستوگرام ضرایب می شود. این خطر برای روش پیشنهادی ما وجود ندارد. راه حل استفاده شده برای رفع این خطر، استفاده از بلاک‌بندی با ابعاد شبه تصادفی است که دو مزیت مهم دارد. اولا آنکه، حمله کننده به محدوده بلاک‌ها دسترسی ندارد. بنابراین امکان استفاده از هیستوگرام ضرایب DCT بلاک‌ها برای حمله کننده وجود ندارد. بدین ترتیب تغییرات احتمالی در هیستوگرام ضرایب DCT بلاک‌ها از دسترس حمله کننده پنهان است. بنابراین روش پیشنهادی در برابر حمله ارائه شده در مرجع [2] و تمام حملاتی مقاوم است که بر مبنای تغییرات هیستوگرام کار می‌کنند.

۲-۳- بررسی دلایل مقاومت PRB

حملات موجود در [2,9,10] باعث شده است که جاسازی در حوزه فرکانس DCT به روش‌های معمول قابل کشف باشد. اما در این مقاله ادعا می‌شود که با وجود جاسازی در حوزه DCT، روش پیشنهادی PRB در مقابل حملات موجود مقاوم است. در این بخش دلایل این ادعا بررسی می‌شود.

در حمله به روش Jsteg [2] از این ویژگی استفاده شده است که جاسازی در ضرایب DCT باعث تغییر هیستوگرام ضرایب

می شود. این خطر برای روش پیشنهادی ما وجود ندارد. راه حل استفاده شده برای رفع این خطر، استفاده از بلاک‌بندی با ابعاد شبه تصادفی است که دو مزیت مهم دارد. اولا آنکه، حمله کننده به محدوده بلاک‌ها دسترسی ندارد. بنابراین امکان استفاده از هیستوگرام ضرایب DCT بلاک‌ها برای حمله کننده وجود ندارد. بدین ترتیب تغییرات احتمالی در هیستوگرام ضرایب DCT بلاک‌ها از دسترس حمله کننده پنهان است. بنابراین روش پیشنهادی در برابر حمله ارائه شده در مرجع [2] و تمام حملاتی مقاوم است که بر مبنای تغییرات هیستوگرام کار می‌کنند.

ثانیاً، پنهان کردن محدوده بلاک‌ها از دسترس حمله کننده، باعث می‌شود که امکان استفاده از حمله ارائه شده در مرجع [9] نیز وجود نداشته باشد. این حمله توسط Fridrich و همکارانش، برای حمله به روش جاسازی OutGuess [7] پیشنهاد شده است و می‌تواند طول پیام مخفی شده را نیز تعیین کند.

با توجه به بلاک‌بندی ۸×۸ در تبدیل DCT در تصاویر JPEG ، محاسبه اثر بلاکی شدن در مرز این بلاک‌ها مفید است. اما با استفاده از بلاک‌بندی تصادفی امکان محاسبه این معیار در مرز بلاک‌های واقعی استفاده شده در روش پیشنهادی برای حمله کننده وجود ندارد. بنابراین مزیت مهم دیگر بلاک‌بندی با ابعاد شبه تصادفی، عدم امکان محاسبه مقدار واقعی معیار "اثر بلاکی شدن" در تصویر گنجانه تولید شده است. بدین ترتیب روش پیشنهادی در برابر حمله [9] نیز مقاوم است.

۳- نتایج پیاده‌سازی

روش پنهان‌نگاری پیشنهادی با استفاده از نرم افزار Matlab 7.1 پیاده سازی شده است. در این روش پارامترهای مهم و مؤثری مانند حداکثر اندازه بلاک‌ها، تعداد تکرار گام جاسازی پیام در بلاک (M) و تعداد تکرار گام اضافه کردن نویز به بلاک (N) وجود دارد که انتخاب آن‌ها در اجرای روش مؤثر است. در این بخش تأثیر پارامترهای گوناگون بر یکدیگر با استفاده از آمارهای بدست آمده از پیاده‌سازی را بررسی می‌کنیم و در ادامه مقاومت مورد انتظار روش پیشنهادی در برابر حملات گوناگون را با نتایج حاصل از پیاده‌سازی مقایسه می‌کنیم.

تصاویر مختلفی برای تست روش پیشنهادی استفاده شده‌اند. اما نتایج ارائه شده در این مقاله تنها متعلق به تصویر تست "Peppers" است که در شکل ۵ نشان داده شده است.

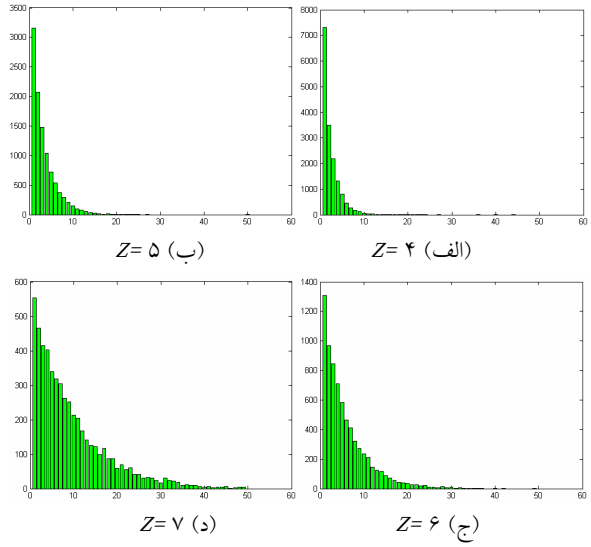
شکل۵: تصویر تست *"Peppers"*

۳-۱- انتخاب پارامترهای مختلف

در روش پیشنهادی ابعاد بلاک به صورت تصادفی انتخاب می‌شود. تجربیات گوناگون نشان می‌دهد که اندازه بلاک تأثیر مستقیم در مقادیر پارامترهای M و N دارد. به عبارت دیگر بلاک های کوچکتر به پارامترهای M و N کوچکتری نیاز دارند و احتمال موفقیت PRB برای آن‌ها بسیار بیشتر است. به همین دلیل یکی از پارامترهای مهم در روش پیشنهادی، حداکثر اندازه بلاک‌ها *(Z)* است.

با افزایش اندازه بلاک‌ها ، تعداد بلاک‌های تصویر کاهش می‌یابد. پس انتظار می‌رود که سرعت الگوریتم پیشنهادی بیشتر شود، زیرا جاسازی در بلاک‌های کمتری باید انجام شود. اما از طرف دیگر، بزرگتر شدن بلاک‌ها باعث می‌شود که پارامترهای M و N بزرگتری نیز استفاده شود. بنابراین افزایش اندازه بلاک‌ها دلیلی برای سریعتر شدن عملیات جاسازی نیست، بلکه در اکثر موارد به کندتر شدن عمیات منجر می‌شود.

برای بررسی رابطه پارامترهای M و Z در تصویر "Peppers"، بلاک‌بندی را با چند مقدار پارامتر M متفاوت انجام دادیم. در بلاک‌بندی‌های مختلف، تعداد تکرار عملیات جاسازی لازم در هر بلاک را اندازه‌گیری کرده ایم. شکل ۶، نتایج این آزمایش را برای چهار مقدار Z نشان می‌دهد. محور افقی در این نمودارها تعداد تکرار عملیات جاسازی برای یک بلاک و محور عمودی، تعداد بلاک‌ها برای هر تعداد تکرار است.



شکل۶: تعداد تکرار عملیات جاسازی در بلاک های تصویر تست

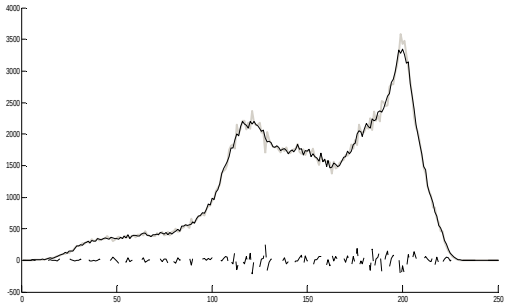
شکل ۶ به خوبی رابطه حداکثر اندازه بلاک و تعداد تکرار لازم برای عملیات جاسازی در یک بلاک را نشان می‌دهد. با توجه با این نمودارها اگر مقدار پارامتر M را بزرگتر از ۵۰ انتخاب کنیم، جاسازی در تمام بلاک‌ها بدون نیاز به مرحله اضافه کردن نویز، با موفقیت انجام می‌شود. اما اگر مقدار M کوچکتر از ۵۰ انتخاب شود، جاسازی در تعدادی از بلاک‌ها انجام پذیر نیست و بنابراین به مرحله اضافه کردن نویز نیاز است. انتخاب مقادیر کوچک M، باعث می‌شود تا نیاز به پارامتر N بزرگتری داشته باشیم. اما برای اکثر تصاویر تست شده با مقدار Z حداکثر ۱۰ و مقدار M برابر با ۵۰، پارامتر N با مقدار ۱۰ قابل قبول بوده است.

نتایج ارائه شده تا به حال با فرض جاسازی به روش LSB-M است، اما در صورتی که از LSB-F برای جاسازی استفاده کنیم، در شرایط مساوی برای مقدار Z، به پارامترهای M و N بزرگتری نسبت به روش LSB-M نیاز داریم. به عبارت دیگر اگر می‌خواهیم مقادیر M و N را افزایش ندهیم، باید از بلاک-بندی کوچکتری در روش LSB-F استفاده کنیم، در غیر این صورت احتمال موفقیت برای تصاویر مختلف کاهش می یابد.

۳-۲- مقاومت در برابر حملات

در بخش ۲-۳ دلایل مقاومت PRB در برابر بعضی از حملات شناخته شده به صورت تئوری بررسی شد. در این بخش نتایج تست برای تصویر "Peppers" ارائه می‌شود، که این مقاومت را تأیید می‌کند. با وجود جاسازی 256K بیت داده در این تصویر با ابعاد ۵۱۲×۵۱۲، کیفیت تصویر خروجی، کاملاً مشابه تصویر اصلی است.

از ساده‌ترین راه‌های نشان دادن تغییرات ایجاد شده در اثر یک روش پنهان‌نگاری، استفاده از هیستوگرام تصویر است. در شکل ۸، هیستوگرام تصویر "Peppers" قبل از جاسازی (خط کم رنگ) و بعد از جاسازی (خط پر رنگ) نشان داده شده است. بعلاوه خطوط نقطه چین در این نمودار تفاوت این دو هیستوگرام را نشان می دهد. همان گونه که مشاهده می‌شود، تغییر ایجاد شده در هیستوگرام بعد از جاسازی به روش پیشنهادی بسیار کم است.

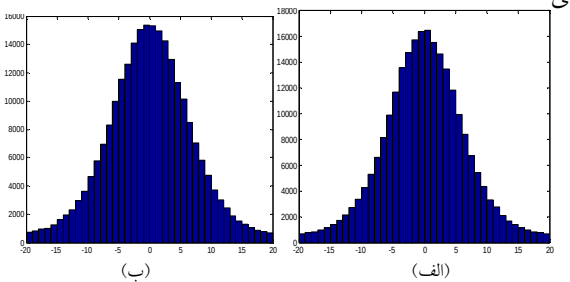


شکل۸: هیستوگرام تصویر تست قبل از جاسازی (خط کم رنگ) و بعد از جاسازی (خط پر رنگ) و تفاوت دو هیستوگرام (خطوط نقطه چین)

بررسی تغییرات هیستوگرام مبنای بعضی از روش‌های پنهان

در روش PRB علاوه بر هیستوگرام سطح روشنایی پیکسل‌ها، امکان تغییر هیستوگرام ضرایب DCT نیز وجود دارد. با توجه به این‌که بلاک‌بندی با ابعاد تصادفی انجام می‌شود، بنابراین امکان دستیابی به هیستوگرام ضرایب DCT هر بلاک به تنهایی وجود ندارد. پس تنها می‌توانیم از هیستوگرام ضرایب تبدیل DCT کل تصویر استفاده کنیم.

شکل ۱۰، هیستوگرام ضرایب DCT کل تصویر تست قبل و بعد از جاسازی را نشان می‌دهد. شباهت بسیار زیاد این دو هیستوگرام، استفاده از آن برای کشف وجود پیام را غیر ممکن می‌کند.



شکل۱۰: هیستوگرام ضرایب *DCT* کل تصویر تست (الف) قبل از جاسازی و (ب) بعد از جاسازی

یکی دیگر از حملات مطرح شده در بخش ۲-۳، حمله [9] است که دلایل مقاومت PRB در برابر آن ارائه شد. معیار "اثر بلاکی شدن" برای تصویر "Peppers" قبل از جاسازی طبق رابطه (۱) برابر ۸۲۸۶۳۷ است. در جدول ۱، مقدار این معیار بعد از جاسازی برای چند مقدار متفاوت پارامتر Z و دو روش جاسازی LSB-F و LSB-M آورده شده است. مقایسه این مقادیر نشان می‌دهد که تغییر این معیار در اثر جاسازی به روش پیشنهادی بسیار کم است و امکان استفاده از حمله [9] برای کشف آن وجود ندارد. بعلاوه مقادیر ارائه شده نشان می‌دهد که جاسازی به روش LSB-M و استفاده از بلاک بندی‌های کوچک‌تر، معیار "اثر بلاکی شدن" را بهتر حفظ می‌کند.

جدول ۱: مقدار معیار "اثر بلاکی شدن" برای تصویر گنجانه تولید شده با مقادیر Z مختلف و روش های جاسازی متفاوت

Method \ Z	۴	۵	۶	۷
LSB-F	۸۳۹۳۱۱	۸۳۹۵۳۹	۸۴۲۴۴۱	۸۴۸۰۲۷
LSB-M	۸۳۸۰۱۹	۸۳۷۱۶۸	۸۳۸۹۳۳	۸۴۱۴۹۶

۴- نتیجه گیری

اگرچه جاسازی در حوزه مکانی تصاویر BMP و حوزه تبدیل تصاویر JPEG از روش‌های رایج پنهان‌نگاری است، اما در روش پیشنهادی PRB، از حوزه تبدیل تصاویر BMP برای جاسازی استفاده شده است. استفاده از حوزه تبدیل برای جاسازی به روش پیشنهادی مشکلاتی ایجاد می‌کند که در این مقاله راه حل‌هایی مانند جاسازی در دومین بیت کم ارزش، تکرار عملیات جاسازی در یک بلاک و در صورت حل نشدن مشکل، اضافه کردن نویز تصادفی به پیکسل‌های بلاک پیشنهاد شده است.

حملات مختلفی برای روش‌های جاسازی در حوزه فرکانس وجود دارد. استفاده از هیستوگرام ضرایب DCT و یا معیار "اثربلاکی شدن" در مرز بلاک‌ها از ابزار کشف پیام است. با توجه به بلاک‌بندی با ابعاد تصادفی در روش پیشنهادی، محدوده بلاک‌ها برای حمله کننده ناشناخته است و امکان استفاده از ابزار حمله برای حمله کننده وجود ندارد. نتایج پیاده سازی نیز مقاومت روش پیشنهادی در برابر حملات شناخته شده موجود را نشان می‌دهد.

۵- مراجع

[1] M. M. Amin, M. Salleh, S. Ibrahim, M.R Katmin and M.Z.I Shamsuddin, "Information Hiding using Steganography", 4th National Conference on Telecommunication TechnologyProceedings,2003.

[2] M. Kharrazi, H. T. Sencar and N. Memon, "Image Steganography: Concepts and Practice", WSPC/ Lecture Notes Series, April 22, 2004.

[3] B. Pitzmann,"Information Hiding Terminology", in Information Hiding, Springer Lecture Notes in Computer Science, Vol. 1174, pp. 347-350, 1996.

[4] B. ŞİMŞEK, "Steganography in JPEG Images", Dokuz Eylül University, İZMİR, July, 2004.

[5] N. Provos and P. Honeyman ,"Hide and Seek: An Introduction to Steganography", IEEE Security & Privacy, pp. 32-44, May-June, 2003.

[6] A. D. Ker, "Steganalysis of LSB Matching in Grayscale Images", IEEE Signal Processing Letters, Vol. 12, No. 6, June 2005.

[7] N. Provos, "Defending Against Statistical Steganalysis", Proc. 10th Usenix Security Symp, Usenix Assoc., pp. 323-335, 2001.

[8] A. Westfeld, "F5-A Steganographic Algorithm :High Capacity Despite Better Steganalysis", Proc. 4th Int'l Information Hiding Workshop, Springer-Verlog, Vol. 2137 , Berlin Heidelberg New York , pp.289-302, 2001.

[9] J. Fridrich, M. Goljan and D. Hogea, "Attacking the OutGuess", Proc. ACM Workshop Multimedia and Security 2002, ACM Press, 2002.

[10] J. Fridrich, M. Goljan and D. Holga,"steganalysis of JPEG images: breaking the F5 algorithm", Lecture notes in computer scince, Vol. 2578, Springer, Berlin Heidelberg New York, pp. 310-232,2003.

[11] احمدرضا نقش نیل‌چی، اعظم نادعلیان، نسرین رسولی، "شیوه‌ای جدید در پنهان‌نگاری مقاوم داده در تصاویر *JPEG*"، نشریه مهندسی برق و مهندسی کامپیوتر ایران، سال ۴، شماره ۱، ۱۳۸۵

[12] J. Fridrich. "Feature-based steganalysis for JPEG images and its implications for future design of steganographic schemes", 6th Information Hiding Workshop, Springer-Verlag, pp. 67-81, 2004.

[13] J. Fridrich and T. Pevn´y. "Towards multi–class blind steganalyzer for JPEG images", 4th International Data Hiding Workshop, Springer-Verlag, pp. 67-81, 2005.

[14] J. Fridrich and T. Pevn´y. "Multi–class blind steganalysis for JPEG images", Proceedings of SPIE Electronic Imaging, Security, Steganography, and Watermarking of Multimedia Contents VIII, 2006.

[15] T. Pevn´y and J. Fridrich," Merging Markov and DCT Features for Multi-Class JPEG Steganalysis", Proc. SPIE Electronic Imaging, Photonics West, January 2007.