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

پنهان‌نگاری پر ظرفیت با حداقل سازی تغییرات هیستوگرام تصویر

مجتبی مهدوی
دانشکده برق و کامپیوتر
دانشگاه صنعتی اصفهان
mahdavi@ec.iut.ac.ir

شادرخ سماوی
دانشکده برق و کامپیوتر
دانشگاه صنعتی اصفهان
samavi96@cc.iut.ac.ir

وجیهه ثابتی
دانشکده برق و کامپیوتر
دانشگاه صنعتی اصفهان
sabeti@ec.iut.ac.ir

محمود مدرس هاشمی
دانشکده برق و کامپیوتر
دانشگاه صنعتی اصفهان
modarres@cc.iut.ac.ir

چکیده: تا کنون روش‌های متعددی برای پنهان نگاری در تصویر پیشنهاد شده‌است. بسیاری از روش‌های ارائه شده از جاسازی در بیت کم ارزش پیکسل‌های تصویر (*LSB-F* و *LSB-M*) استفاده می‌کنند. روش پیشنهاد شده در این مقاله ترکیب دو ایده جاسازی پرظرفیت و وفقی با روش *LSB-M* ساده است. به عبارت دیگر، روش افزایش ظرفیت را با استفاده از ایده وفقی به گونه‌ای اصلاح می‌کنیم که تغییرات هیستوگرام را نسبت به روش پرظرفیت کاهش دهد و از طرف دیگر، ظرفیت جاسازی را نسبت به روش *LSB-M* وفقی افزایش دهد. نتایج شبیه‌سازی نشان می‌دهد که روش ارائه شده، بدون کاهش ظرفیت جاسازی در تصویر کلیه حملاتی را ناکام می‌گذارد که با بررسی هیستوگرام تصویر قصد حمله به این روش را دارند.

واژه های کلیدی: پنهان نگاری، جاسازی پرظرفیت، جاسازی وفقی

۱- مقدمه

هدف تکنیک‌های پنهان نگاری کامپیوتری، درج و ارسال پیام محرمانه از طریق رسانه دیجیتال است، بگونه‌ای که هیچ ظنی مبنی بر ارسال اطلاعات برانگیخته نشود. در واقع هدف اصلی، مخفی کردن وجود اطلاعات سری در یک رابطه است. پیام موردنظر در یک شئ پوشانه[1] مخفی می‌شود. از پنهان کردن پیام در شئ پوشانه، شئ استگو[2] تولید می‌شود[1].

تصاویر از مهمترین رسانه‌های مورد استفاده در اینترنت هستند. از آنجایی که درک انسان از تغییرات در تصاویر محدود است، تصاویر به عنوان نوعی رسانه پوششی مناسب در پنهان نگاری محسوب می‌شوند. پیام محرمانه می‌تواند به صورت تصویر یا متن و یا سیگنال کنترل و یا هر چیزی باشد که به صورت رشته بیتی از صفر و یک بیان شود.

الگوریتم‌های پنهان نگاری متعددی برای ساختارهای مختلف تصاویر ارائه شده است. به طور کلی روش‌های پنهان نگاری در تصویر از الگوریتم جاسازی[3] و الگوریتم استخراج[4] بیت‌ها تشکیل شده‌اند. معمولاً الگوریتم‌های جاسازی، شامل سه گام هستند: پیدا کردن بیت‌های افزونه، انتخاب زیر مجموعه‌ای از

1 Cover media
2 Stego madia

3 Embedding
4 Extraction

بیت‌های افزونه برای جاسازی پیام و جاسازی بیت‌های پیام در بیت‌های افزونه انتخاب شده[2].

با وجود این که بسیاری از روش‌های پنهان‌نگاری در کیفیت تصویر تأثیر چشمگیری ایجاد نمی‌کنند، اما تغییر ویژگی‌های آماری تصویر باعث کشف آن‌ها می‌شود. حمله کردن به روش‌های پنهان‌نگاری هدف پنهان شکنی[1] است. به عبارت دیگر، پنهان شکنی دانش کشف اطلاعات پنهان است[3].

تاکنون روش‌های پنهان‌نگاری متعددی برای درج اطلاعات در تصویر ارائه شده است. تعدادی از این روش‌ها براساس جاسازی پیام در بیت‌های کم ارزش پیکسل‌های تصویر کار می‌کنند[3]. معمولاً در این روش‌ها از یک مولد اعداد شبه تصادفی[2] به منظور افزایش سطح امنیت استفاده می‌شود. در دسته دیگری از روش‌ها از حوزه تبدیل برای پنهان‌نگاری استفاده می‌گردد. تبدیل‌های *DCT* [4,5] و *Wavelet* [6] از تبدیل‌های مهمی هستند که برای پنهان‌نگاری در تصاویر مورد استفاده قرار گرفته‌اند.

جاسازی در بیت کم ارزش سطح روشنایی پیکسل‌ها از ساده‌ترین روش‌های پنهان‌نگاری است. در این روش، داده‌ای که باید جاسازی شود پس از فشرده سازی و رمز شدن، در سطح روشنایی پیکسل موردنظر جاسازی می‌شود. این جاسازی به یکی از دو روش *LSB-F*[3] و *LSB-M*[4] انجام می‌شود. در روش *LSB-F*، کم ارزش‌ترین بیت پیکسل با بیت پیام جاگذاری می‌شود. در این روش فقط کم ارزش‌ترین بیت هر پیکسل در صورت نیاز تغییر می‌کند. اما در روش *LSB-M*، ممکن است برای جاسازی یک بیت، چند بیت از پیکسل تغییر کند. در این روش در صورت عدم تطابق بیت کم ارزش پیکسل با داده مورد نظر، مقدار پیکسل به صورت تصادفی کاهش یا افزایش می‌یابد[7].

جاسازی به روش *LSB-F*، جفت رنگ‌ها یا زوج مقادیری *(POV)*[5] در هیستوگرام تصویر ایجاد می‌کند که تعداد رخداد آن‌ها در تصویر برابر است. به همین دلیل این روش در برابر حملاتی آسیب پذیر است که هیستوگرام را بررسی می‌کنند. χ^2 از معروفترین این حملات است[8]. اما با توجه با این‌که روش *LSB-M* از ایجاد *POV* در هیستوگرام جلوگیری می‌کند، در برابر حملات ارائه شده برای *LSB-F* مقاوم است. تا به حال بر علیه *LSB-M* نیز حملاتی مطرح گردیده است، اما هیچ کدام از آنها کاملاً موفق نبوده‌اند. برخی از این حملات در [9,10] آورده شده است.

امنیت و ظرفیت دو فاکتور مهم در روش‌های پنهان‌نگاری هستند[3]. روش‌های پیشنهاد شده در [11] و [12] را به منظور افزایش ظرفیت و امنیت روش *LSB-M* ارائه داده‌ایم. روش پیشنهادی در این مقاله ترکیبی از این دو ایده است. به عبارت دیگر، روش افزایش ظرفیت [11] را با استفاده از ایده وفقی[12] به گونه‌ای اصلاح می‌کنیم که تغییرات هیستوگرام را نسبت به روش پرظرفیت کاهش دهد و از طرف دیگر، ظرفیت جاسازی را نسبت به روش *LSB-M* وفقی افزایش دهد.

در بخش۲ و ۳، روش‌های ارائه شده در مراجع [11] و [12] بررسی می‌شود. سپس در ادامه روش پیشنهادی با عنوان روش *LSB-M* وفقی پرظرفیت معرفی می‌شود. در بخش ۵، نتایج پیاده سازی این روش و مقاومت آن در برابر چند حمله ارائه می‌شود.

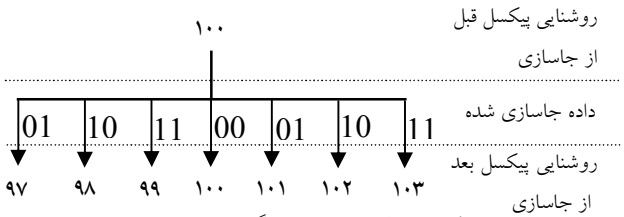
۲- روش افزایش ظرفیت

روش *LSB-M* به دلیل ماهیت تقارنی خود در برابر حملات علیه روش جاگذاری در بیت های کم ارزش مقاوم است. اما این روش تنها قابلیت جاسازی یک بیت در هر پیکسل تصویر سطح خاکستری یا در هر پیکسل هر جزء رنگی تصویر رنگی را دارد. هدف اصلی ایده ارائه شده در *[11]*، افزایش ظرفیت جاسازی روش تطابق بیتی و حفظ ویژگی مقاوم بودن این روش است. در ادامه از این روش با عنوان *H-LSB-M*[6] نام می بریم. در این روش پیشنهادی می‌توان در هر پیکسل تصویر سطح خاکستری یا در هر پیکسل هر جزء رنگی تصویر رنگی، m بیت را جاسازی کرد. برای جاسازی m بیت در هر پیکسل، مقدار پیکسل در بازه $[-(2^m-1),(2^m-1)]$ می‌تواند تغییر کند.

1 Steganalysis
2 Pseudo Random Number Generator (PRNG)
3 Least Significant Bit Flipping (LSB-F)
4 Least Significant Bit Matching (LSB-M)
5 Pair Of Value (POV)
6 High capacity LSB Matching (H-LSB-M)

در حالت $m=1$، بازه تغییر مساوی $[-1,1]$ است که معادل همان روش *LSB-M* است. انتخاب m برای هر تصویر باید به صورتی باشد که علاوه بر غیر قابل مشاهده بودن تغییرات ایجاد شده در تصویر پوشانه، حملات آماری موفق ارائه شده نیز برای این روش ناموفق باشند. نتایج ارائه شده در مقاله اصلی نشان می‌دهد که برای اغلب تصاویر انتخاب $m=3$ و حتی در مواردی برای تصاویر بزرگ، انتخاب $m=4$ مناسب است.

الگوریتم کامل روش *H-LSB-M* را در مرجع *[11]* ارائه کرده‌ایم. در اینجا با یک مثال چگونگی انجام این روش را توضیح می‌دهیم. فرض کنید قصد داریم برای جاسازی داده در تصویری از این روش با پارامتر $m=2$ استفاده کنیم. بنابراین می‌توانیم در هر بیت از این تصویر ۲ بیت جاسازی کنیم. پس داده موردنظر می‌تواند ۴ حالت مختلف *00(0)*، *01(1)*، *10(2)* و *11(3)* را داشته باشد. اگر پیکسل انتخاب شده برای جاسازی داده دارای سطح روشنایی ۱۰۰ باشد، بعد از جاسازی هر کدام از این داده‌ها، پیکسل یکی از مقادیر نشان داده شده در شکل ۱ را خواهد داشت. با توجه به پارامتر $m=2$، بدیهی است که بازه تغییرات $[-3,3]$ است.



شکل ۱: مثالی برای رفتار الگوریتم *H-LSB-M*

همان گونه که در شکل نشان داده شده است، در صورتی که داده مورد نظر برای جاسازی در پیکسل ۱۰۰، *00* باشد نیازی به تغییر مقدار پیکسل نیست. اما در حالتی که داده مورد نظر *01* باشد، دو انتخاب وجود دارد. می‌توان پیکسل ۱۰۰ را به ۱۰۱ یا به ۹۷ تغییر داد. مقدار ۱۰۱ و ۹۷ نزدیکترین اعداد به ۱۰۰ هستند که دو بیت کم ارزش آن‌ها *01* می‌باشد. این انتخاب کاملاً به صورت تصادفی انجام می‌شود. یعنی برای جاسازی داده *01* در ۱۰۰، با احتمال *0.5* پیکسل ۱۰۰ به ۱۰۱ و با احتمال *0.5* پیکسل ۱۰۰ به ۹۷ تبدیل می‌شود. به همین ترتیب برای جاسازی داده *10*، دو انتخاب ۱۰۲ و ۹۸ و برای جاسازی داده *11*، دو انتخاب ۱۰۳ و ۹۹ وجود دارد. در این روش انتخاب بین دو گزینه ممکن کاملاً به صورت تصادفی انجام می‌شود.

نتایج ارائه شده در مقاله اصلی نشان می‌دهد که اهداف اصلی ارائه دهندگان، افزایش ظرفیت روش *LSB-M* و حفظ ویژگی مقاوم بودن در برابر حملات شناخته شده، به خوبی برآورده شده است.

۳- روش *LSB-M* وفقی

در روش *LSB-M* در صورتی که نیاز به تغییر مقدار یک پیکسل باشد، امکان انتخاب دو گزینه مختلف وجود دارد. این انتخاب به صورت کاملاً تصادفی انجام می‌شود. اگرچه این روش برخلاف روش *LSB-F*، در هیستوگرام تصویر زوج مقدار (*POV*) ایجاد نمی‌کند، اما در حملات مختلف ارائه شده تاکنون ادعا شده است که این روش جاسازی نیز تغییرات قابل کشفی در هیستوگرام تصاویر ایجاد می کند. برای مثال روش حمله وستفلد براساس تغییراتی است که جاسازی به روش *LSB-M* در تعداد جفت روشنایی‌های شبیه به هم ایجاد می‌کند*[8]*. همچنین اندروکر در *[9]* ادعا می‌کند که پنهان‌نگاری به این روش باعث نرم شدن هیستوگرام و جابجایی مرکز ثقل تبدیل فوریه هیستوگرام به سمت چپ می‌شود. اگرچه آزمایشات نشان می‌دهد که حملات موجود، حملات بسیار کامل و جامعی نیستند*[12]*، اما برای بهتر کردن این روش پیشنهاد می‌کنیم از انتخاب های هدفدار به جای انتخاب‌های تصادفی استفاده شود.

در روش ارائه شده در *[12]*، معیاری برای هدفدار کردن این انتخاب‌ها پیشنهاد شده است. در ادامه بحث از این روش با عنوان *A-LSB-M*[1] یاد می‌کنیم. هدف اصلی در این روش، اصلاح روش *LSB-M* به گونه‌ای است که تفاوت هیستوگرام تصویر پوشانه و تصویر میزبان حداقل شود. بدین ترتیب هیستوگرام تصویر میزبان به تصویر پوشانه نزدیکتر می‌شود و بنابراین حملات آماری که بر مبنای تغییر هیستوگرام کار می‌کنند، قادر به کشف این روش نیستند.

فرض کنید هیستوگرام تصویر پوشانه را H و هیستوگرام تصویر استگو فعلی حاصل از جاسازی i بیت از داده را H'

1 Adaptive LSB Matching (A-LSB-M)

بنامیم و بعلاوه پیکسل با روشنایی k برای جاسازی $(i+1)$ امین بیت از پیام، به صورت شبه تصادفی، انتخاب شده باشد. در صورتی که نیاز به تغییر روشنایی پیکسل باشد، باید روشنایی $k-1$ یا $k+1$ جایگزین آن شود. برای انجام این انتخاب، دو پارامتر زیر محاسبه می‌شود:

$$d_1 = h_{k+1} - h'_{k+1} \quad , \quad d_{-1} = h_{k-1} - h'_{k-1}$$

d_1 و d_{-1} به ترتیب تفاوت بین هیستوگرام تصویر استگو فعلی و تصویر پوشانه را نشان می‌دهد. برای حداقل کردن تغییرات هیستوگرام، مقداری باید انتخاب شود که در حال حاضر بیشترین تغییر را دارد. به عبارت دیگر، در صورتی که $d_{-1} > d_1$ باشد، روشنایی k به $k-1$ و در غیراین‌صورت، روشنایی k به $k+1$ تبدیل می‌شود.

علاوه بر امکان تطبیق در این روش، ایده مطرح شده دیگر بزرگتر کردن بازه تغییرات مجاز در روش تطبیق بیتی برای انجام هر چه بهتر این تطابق است. در روش پیشنهادی، پارامتر q تعداد انتخاب‌های ممکن را نشان می‌دهد. در ساده‌ترین حالت، مانند روش *LSB-M*، این پارامتر برابر ۲ است. یعنی برای هر تغییر، ۲ انتخاب ممکن (افزودن ۱ یا ۱-) وجود دارد. بازه تغییرات در این حالت *[-1,+1]* است. تفاوت این حالت با روش *LSB-M* در این است که به جای انتخاب تصادفی، حالتی انتخاب می شود که تغییرات هیستوگرام را کم کند. با تبدیل بازه تغییرات به *[-3,+3]*، برای هر تغییر ۴ انتخاب ممکن (افزودن ۱، ۳، ۱- یا ۳-) وجود خواهد داشت. انتظار می‌رود با بزرگتر کردن بازه تغییرات مجاز، انتخاب‌ها به گونه‌ای انجام شود که تغییرات هیستوگرام کمتر شود. نتایج ارائه شده نشان می دهد که برای حالت q=۶ تغییرات هیستوگرام بهتر از شرایطی است که q= ۴ انتخاب شود. بزرگتر کردن بازه تا حدی امکان پذیر است که تغییرات بوجود آمده در تصویر برای چشم قابل درک نباشد.

۴- روش پیشنهادی *LSB-M* وفقی پرظرفیت

ایده اصلی روش *H-LSB-M [11]*، جاسازی بیش از یک بیت داده در هر پیکسل تصویر است. مبنای روش *A-LSB-M [12]*، بیشتر کردن تعداد انتخاب‌های ممکن و ارائه معیاری برای انتخاب به گونه‌ای است که تغییرات هیستوگرام را حداقل کند. روشی که در اینجا پیشنهاد می‌شود، ترکیبی از این دو ایده است. بدین ترتیب روش افزایش ظرفیت را با استفاده از ایده وفقی به گونه‌ای اصلاح می‌کنیم که تغییرات هیستوگرام را نسبت به روش اصلی کمتر کند. بنابراین انتظار می‌رود که روش جدید علاوه بر افزایش دادن ظرفیت جاسازی در هر پیکسل از یک بیت به چند بیت، نسبت به روش مرجع *[11]* در برابر حملات مبتنی بر هیستوگرام مقاوم‌تر باشد. روش جدید را *LSB-M* وفقی پرظرفیت یا *AH-LSB-M*[1] نامگذاری می‌کنیم.

برای توضیح بهتر الگوریتم روش پیشنهادی را با مثالی مورد بررسی قرار می‌دهیم. فرض کنید تا به حال جاسازی $2i$ بیت از داده را انجام داده‌ایم و اکنون می‌خواهیم دو بیت داده بعدی را در پیکسلی با سطح روشنایی ۱۲۸ جاسازی کنیم و شرایط زیر وجود داشته باشد:

جدول۱: مثالی برای تعداد پیکسل‌های سطوح روشنایی مختلف قبل و بعد از جاسازی

سطح روشنایی / تعداد پیکسل	۱۲۵	۱۲۶	۱۲۷	۱۲۸	۱۲۹	۱۳۰	۱۳۱
h_k	۱۰۰	۱۰۰	۱۰۰	۱۰۰	۱۰۰	۱۰۰	۱۰۰
h'_k	۹۰	۱۰۰	۱۲۲	۱۰۰	۱۱۰	۱۰۵	۱۲۰

H، هیستوگرام تصویر پوشانه و H'، هیستوگرام تصویر استگو فعلی حاصل از جاسازی $2i$ بیت داده را نشان می‌دهد. برای حالت جاسازی دو بیت در هر پیکسل، چهار نوع داده *00*، *01*، *10* و *11* وجود دارد. برای جاسازی *00* در پیکسل با مقدار ۱۲۸ نیازی به تغییر نداریم. اما برای جاسازی هر کدام از داده‌های دیگر در این پیکسل دو گزینه ممکن وجود دارد. برای مثال، فرض کنید دو بیت داده مورد نظر برای جاسازی *01* باشد. دو انتخاب ممکن ۱۲۹ و ۱۲۵ است. اگر در جاسازی از روش افزایش ظرفیت استفاده می‌کردیم، انتخاب از بین این دو گزینه به صورت کاملاً تصادفی انجام می‌شد. اما با توجه به شرایط مذکور در جدول۱، اگر ۱۲۵ انتخاب شود، تعداد آن در تصویر استگو به ۹۱ می‌رسد و تفاوت آن با هیستوگرام تصویر پوشانه، ۹ می‌شود. اما اگر ۱۲۹ انتخاب شود، تعداد آن در تصویر استگو ۱۱۱ و تفاوت آن با هیستوگرام تصویر پوشانه، ۱۱ می‌شود.

1 Adaptive High capacity LSB Matching (AH-LSB-M)

بنابراین انتخاب ۱۲۵ در این شرایط باعث حداقل شدن تغییرات هیستوگرام می‌شود.

در حالت کلی، برای جاسازی دو بیت داده با مقدار a در پیکسلی با روشنایی k دو گزینه k_1 و k_2 وجود دارد. این دو گزینه به طریق زیر محاسبه می‌شوند:

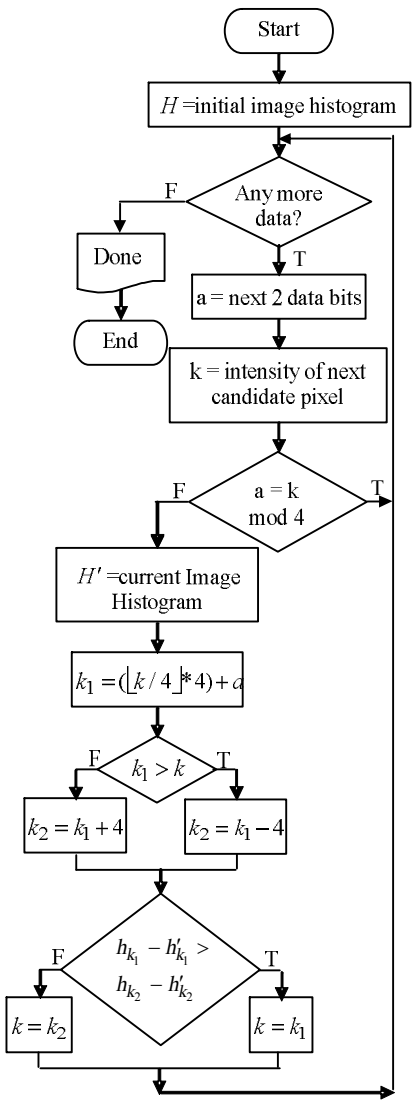
$$k_1 = (\lfloor k/4 \rfloor * 4) + a$$

$$k_2 = \begin{cases} k_1 - 4 & k_1 > k \\ k_1 + 4 & k_1 < k \end{cases}$$

انتخاب بین k_1 و k_2 به صورت زیر انجام می‌شود:

$$\begin{cases} select \;\; k_1 \;\; if \;\; (h_{k_1} - h'_{k_1}) > (h_{k_2} - h'_{k_2}) \\ else \quad select \;\; k_2 \end{cases}$$

این انتخاب در جهت کم کردن تغییرات هیستوگرام است. دیاگرام جاسازی به روش تشریح شده در شکل ۲ نشان داده شده است.



شکل ۲: فلوچارت پنهان نگاری به روش پر ظرفیت وفقی(AH-LSB-M)

در حالت استفاده از ۲ انتخاب بازه تغییرات مانند روش افزایش ظرفیت است. اما برای ایجاد امکان تطبیق بیشتر و کمتر شدن تغییرات هیستوگرام می‌توان تعداد انتخاب ها را به ۴ و حتی ۶ نیز افزایش داد. در حالت جاسازی ۲ بیتی با استفاده از ۴ انتخاب بازه تغییرات *[-7,+7]* و در حالت استفاده از ۶ انتخاب بازه تغییرات *[-11,+11]* امکان پذیر است.

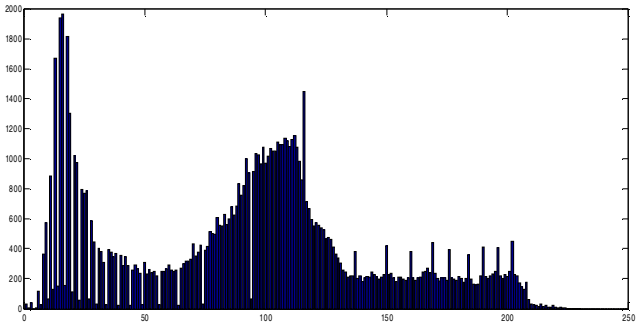
۵- نتایج پیاده‌سازی

الگوریتم *AH-LSB-M* در واقع ترکیبی از دو ایده افزایش ظرفیت و تطبیق است. بنابراین این روش برتری‌هایی بر هر دو روش *A-LSB-M* و *H-LSB-M* دارد. برتری روش افزایش ظرفیت وفقی در برابر روش *LSB-M* وفقی، در مقدار ظرفیت جاسازی است. این برتری از تعریف الگوریتم نشأت می‌گیرد. اما از طرف دیگر، ایده تطبیق باعث برتری این روش نسبت به روش افزایش ظرفیت می‌شود. برای نشان دادن این برتری، یکی از نتایج پیاده سازی را بررسی می‌کنیم.

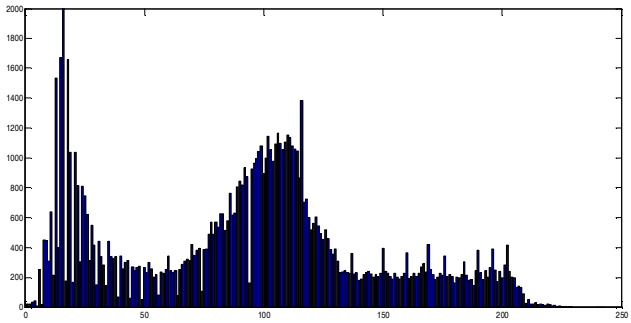
یکی از تصاویر تست مورد استفاده، تصویر *"Lena"* است که در شکل ۳ نشان داده شده است. یکی از راه‌های نشان دادن تفاوت روش‌ها، استفاده از هیستوگرام و بررسی تغییرات آن پس از اعمال هر یک از روش‌ها است. هیستوگرام تصویر *"Lena"* که به عنوان تصویر پوشانه استفاده شده است، در شکل ۴ نشان داده شده است.

شکل ۵، هیستوگرام تصویر تست بعد از جاسازی به روش *H-LSB-M* را نشان می‌دهد که در طی آن، در هر پیکسل از تصویر دو بیت داده جاسازی شده است. مقایسه هیستوگرام‌های قبل و بعد از جاسازی به روش *H-LSB-M* ، نشان دهنده تغییرات با

شکل ۳: تصویر *"Lena"*



شکل ۴: هیستوگرام تصویر "Lena"



شکل ۶: هیستوگرام تصویر "*Lena*" بعد از جاسازی به روش *AH-LSB-M*

معنی در اثر اعمال روش افزایش ظرفیت است. در روش حمله اندروکر[9]، از این تغییرات به عنوان نرم شدن هیستوگرام نامبرده شده است. اندازه‌گیری مرکز ثقل تبدیل فوریه هیستوگرام‌ها نیز این تغییر را تأیید می‌کند. مرکز ثقل تبدیل فوریه هیستوگرام در تصویر پوشانه *45.7* و در تصویر استگو حاصل از جاسازی به روش افزایش ظرفیت برابر *18.6* است. این کاهش در مرکز ثقل، نشانه نرم شدن هیستوگرام است.

پارامتر قابل اندازه‌گیری دیگر، مقدار خطای ایجاد شده در هیستوگرام است. این خطا را به صورت زیر تعریف می‌کنیم:

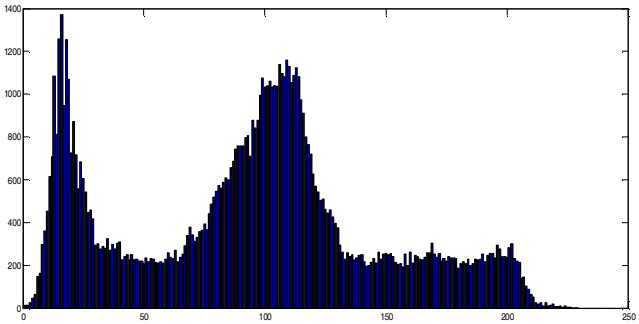
$$Error = \sqrt{\frac{\sum_{k=0}^{255} (h_k - h'_k)^2}{m * n}}$$

که m و n ابعاد تصویر هستند. خطای هیستوگرام تصویر استگو حاصل از جاسازی به روش *H-LSB-M* برای تصویر تست "*Lena*"، برابر *8.07* است.

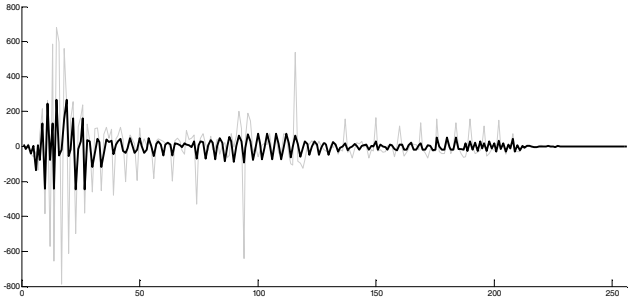
در آزمایش دوم برای جاسازی دو بیت در هر پیکسل از تصویر، از روش *AH-LSB-M* با ۲ انتخاب استفاده شده است، که هیستوگرام تصویر استگو نهایی درشکل ۶ نشان داده شده است. مقایسه هیستوگرام‌های نشان داده شده در شکل‌های ۴ و ۵ و۶، نشان می‌دهد که تغییرات هیستوگرام در اثر اعمال روش پیشنهادی نسبت به روش *H-LSB-M* کمتر است. مرکز ثقل تبدیل فوریه هیستوگرام تصویر استگو حاصل از جاسازی به روش پیشنهادی برابر *41* شده است، که بسیار نزدیک به مقدار این پارامتر در تصویر پوشانه است. به عبارت دیگر پدیده نرم شدن هیستوگرام در این روش رخ نمی‌دهد و حمله اندروکر در برابر این روش ناموفق است.

از طرف دیگر کاهش بسیار زیاد مقدار پارامتر خطا نیز تصدیق کننده کاهش تغییرات هیستوگرام در این روش است. خطای هیستوگرام تصویر استگو حاصل از جاسازی به روش *AH-LSB-M* برای تصویر تست "*Lena*"، برابر *3.01* شده است، که تقریباً نسبت به روش *H-LSB-M* ، *62%* کاهش داشته است.

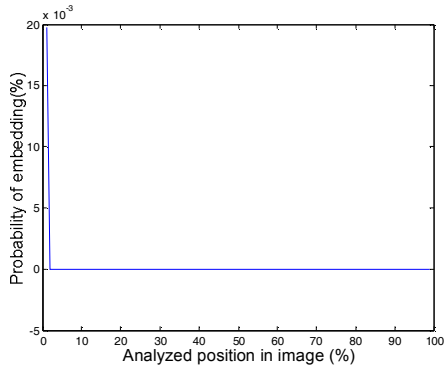
مهمترین هدف در روش *AH-LSB-M*، کم کردن تغییرات هیستوگرام در اثر جاسازی نسبت به روش *H-LSB-M* است. در شکل۷، نموداری وجود دارد که میزان تغییرات هیستوگرام در دو روش*H-LSB-M* (خطوط کم رنگ) و *AH-LSB-M* (خطوط پر رنگ) برای تصویر تست "*Lena*" را نشان می‌دهد. این نمودار نیز کاهش تغییرات هیستوگرام در روش *AH-LSB-M* را نشان می‌دهد. بنابراین با حفظ مقدار ظرفیت جاسازی، تغییرات هیستوگرام را نسبت به روش*A-LSB-M* کاهش داده‌ایم.



شکل ۵: هیستوگرام تصویر "*Lena*" بعد از جاسازی به روش *H-LSB-M*



شکل۷: تغییرات هیستوگرام در روش‌های *H-LSB-M* (کم رنگ) و *AH-LSB-M* (پر رنگ)



شکل۸: نتیجه اعمال حمله χ^2

با توجه به این که روش *AH-LSB-M* به نوعی تعمیم روش جاسازی وفقی است، بنابراین انتظار می‌رود که روش حمله χ^2 نیز قادر به کشف آن نباشد. شکل ۸ نتیجه حاصل از اعمال این حمله بر تصویر استگو تولید شده از روش *AH-LSB-M* را تأیید می‌نماید. این شکل نیز نشان دهنده عدم موفقیت این حمله در کشف تصویر استگو حاصل از این روش است.

با وجود ظرفیت جاسازی بیشتر در روش *AH-LSB-M* نسبت به *A-LSB-M*، اما تصویر استگو ایجاد شده در خروجی این روش تغییر محسوسی نمی‌کند. بدین ترتیب با وجود افزایش ظرفیت جاسازی در روش *AH-LSB-M*، این روش نسبت به حملات بصری نیز مقاوم است. برای مثال، شکل ۹، تصویر *"Lena"* بعد از جاسازی به روش *A-LSB-M* را نشان می‌دهد. در این تصویر با ابعاد ۳۰۰×۳۰۰، ۹۰۰۰۰ بیت داده جاسازی شده است. شکل ۱۰، تصویر *"Lena"* بعد از جاسازی ۱۸۰۰۰۰ بیت داده به روش *AH-LSB-M* را نشان می‌دهد. با وجود اینکه حجم داده جاسازی شده در شکل ۱۰ دو برابر شکل ۹ است، اما هیچ تغییر محسوسی در شکل رخ نداده است.

شکل۹: تصویر *"Lena"* بعد از جاسازی به روش *A-LSB-M*

شکل۱۰: تصویر *"Lena"* بعد از جاسازی به روش *AH-LSB-M*

۶- نتیجه‌گیری

پنهان سازی داده در بیت‌های کم ارزش پیکسل‌های تصویر از متداول‌ترین روش‌های پنهان‌نگاری است. در این مقاله روشی جدید با عنوان *AH-LSB-M* (*LSB-M* پرظرفیت وفقی) در این حوزه ارائه گردید که ظرفیت پنهان‌نگاری را افزایش می‌دهد. همچنین روش ارائه شده در مقابل حملات مبتنی بر هیستوگرام بسیار مقاوم می‌باشد، زیرا الگوریتم به صورتی رفتار خود را تنظیم می‌کند که تغییرات هیستوگرام حداقل می‌شود. نتایج شبیه سازی‌های انجام شده برتری الگوریتم پیشنهادی را نسبت به الگوریتم‌های *A-LSB-M* (*LSB-M* وفقی) و *H-LSB-M* (*LSB-M* پرظرفیت)نشان می‌دهد. همچنین حملات موجود و متداول روی الگوریتم پیشنهادی عمل نمی‌کنند.

۷- مراجع

[1] N.F. Johnson and S. Jajodia, "Exploring Steganography: Seeing the Unseen", *Computer*, Vol. 31, No. 2, pp.26–34, 1998.

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

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

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

[5] 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.

[6] سید احمد عمادی، عمادالدین فاطمی زاده، "ارائه یک روش نوین و تطبیقی استگانوگرافی با تبدیل موجک"، *چهاردهمین کنفرانس مهندسی برق*، دانشگاه صنعتی امیر کبیر، فرودین ۸۵

[7] A. Westfeld, "Detecting low embedding rates", *in Proc. Inf. Hiding Workshop, Springer LNCS*, vol. 2578, 2002.

[8] A. Westfeld and A. Pfitzman, "Attacks on Steganographic Systems", *Proc. 3rd Int'l Information Hiding Workshop , Springer-Verlag*, Berlin Heidelberg New York, pp. 61-76, 1999.

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

[10] A. Ker, "Improved detection of LSB steganography in grayscale images, *in Proc. Inf. Hiding Workshop, Springer LNCS*, vol. 3200, 2004.

[11] F. Mansoori, M. Mahdavi and S. Samavi, "Capacity Increase and Generalization of ±1 Embedding Steganographic Method", *4th Iranian conference on machine vision*, Iran, Feb 2007.

[12] مجتبی مهدوی، شادرخ سماوی، مسعود اخوت، صدیقه اکرمی، "روش پنهان نگاری تطبیقی بر اساس اغتشاش جمع شونده"، *پانزدهمین کنفرانس مهندسی برق ایران*، اردیبهشت ۱۳۸۶