ششمین کنفرانس بین المللی انجمن رمز ایران
۱۵ و ۱۶ مهر ماه ۱۳۸۸، دانشگاه اصفهان
انجمن رمز ایران
دانشگاه اصفهان

پنهان‌نگاری ادراکی در تصاویر JPEG بر مبنای استفاده از ماتریس میانگین مجذور خطای کوانتیزاسیون

امیررضا طاهری، محسن گواهی، محمد رضایی

پژوهشکده پردازش هوشمند علائم

amirreza.taheri@gmail.com, mg_znu@yahoo.com, rezaei@rcisp.com

چکیده

در این مقاله، روش جدیدی برای جاسازی اطلاعات محرمانه در تصاویر JPEG ارائه شده است. بر خلاف روش JSteg و روش‌های مشابه که به علت پنهان‌نگاری، هیستوگرام ضرایب تبدیل کسینوسی گسسته تصویر پوشانه از حالت توزیع گوسی گسسته خارج می‌شود در روش جدید، هیستوگرام تصویر پوشانه حالت توزیع گوسی گسسته خود را حفظ می‌نماید. در این روش به منظور افزایش امنیت، از ضرایب صفر، یک و 2LSB ضرایب جهت پنهان‌نگاری استفاده می‌شود. بر این اساس در یک بلوک ۸×۸ از تصویر، ضرایب تبدیل کسینوسی گسسته ای جهت پنهان‌نگاری استفاده می‌شوند که میانگین مجذور خطای (MSE) کمتری ایجاد نمایند. با توجه به اینکه مکان‌های پنهان‌نگاری بر اساس کمینه شدن میانگین مجذور خطا انتخاب می شوند، لذا این روش یک روش ادراکی است. نتایج پنهان‌نگاری مؤید به دست آمدن ظرفیت بیشتر، امنیت بالاتر و کیفیت بهتر در مقایسه با JSteg و OutGuess می‌باشد.

واژه‌های کلیدی

پنهان نگاری، حملات آماری،کوانتیزاسیون، JPEG ، DCT ، MSE.

۱- مقدمه

هدف روش‌های پنهان‌نگاری[1]، پنهان کردن اصل وجود ارتباط محرمانه به وسیله قرار دادن پیام در یک رسانه است. این کار باید به گونه‌ای صورت گیرد که کمترین تغییرات قابل کشف را در آن ایجاد نماید. اگر تکنیک پنهان نگاری به گونه ای باشد که دیگران متوجه سوءظنی به رسانه حامل داده شوند آنگاه، هدف این تکنیک با شکست مواجه شده است[1].

پنهان‌نگاری همانند رمزنگاری[2]، به عنوان راهکاری جهت حفظ امنیت اطلاعات محسوب می‌شود. تفاوت اساسی پنهان‌نگاری و رمزنگاری را می‌توان در این دانست که هدف رمزنگاری مخفی نمودن محتویات پیام است و نه اصل وجود و یا اطلاع دیگران از تبادل پیام، اما در پنهان‌نگاری هدف مخفی کردن هرگونه نشانه‌ای از وجود پیام است.

اگرچه از تمام فرمت‌های دیجیتالی می‌توان جهت پنهان‌نگاری استفاده نمود، اما فرمت‌هایی برای این کار مناسب به نظر می‌رسند که درجه افزونگی[3] آنها بالاتر باشد[1]. منظور از درجه افزونگی تعداد بیت هایی است که دقتی، بیش از حد لازم(غیر ضروری) را برای نمایش، ارائه می‌کنند. با توجه به این نکته عکس و صوت بیشتر از سایر فرمت ها برای این امر مورد استفاده قرار می‌گیرند. گستردگی استفاده از تصاویر رایانه‌ای از یک طرف و محدویت درک چشمی انسان از تغییرات در تصاویر از طرف دیگر، این رسانه را بستر مناسبی برای پنهان‌نگاری ساخته است. تکنیک‌های پنهان‌نگاری در تصاویر به دو گروه جاسازی در حوزه مکان و حوزه فرکانس تقسیم می‌شوند[1,2]. در حالت اول اطلاعات درون مقادیر پیکسل‌های تصویر پنهان می‌شوند و در حالت دوم از ضرایب فرکانسی حاصل از تبدیلاتی مانند DFT، DCT وDWT جهت پنهان‌نگاری استفاده می‌گردد[2]. به طور کلی باید در

[1] Steganography.

[2] Cryptography

[3] Redundancy.

طراحی یک سیستم پنهان‌نگار ویژگی‌های زیر مورد توجه قرار بگیرد[1,3]:

ظرفیت[۱]: حداکثر اطلاعاتی را گویند که می‌توان در تصویر پنهان نمود. این ویژگی در تکنیک‌های پنهان‌نگاری نسبت به نشانه‌گذاری[۲] اهمیت بیشتری دارد.

قابلیت مشاهده[۳]: اطلاعات باید طوری در تصویر جاسازی گردند که تغییرات بین تصویر پوشانه[۴] و تصویر گنجانه[۵] توسط سیستم بصری انسان قابل مشاهده و درک نباشد.

مقاومت[۶]: این ویژگی بیان‌گر آن است که پیغام پنهان شده در اثر تغییرات عمدی یا سهوی (نظیر اثرات کانال انتقال) روی تصویر گنجانه تا چه حد مقاوم می‌باشد و قابل بازیابی است.

امنیت[۷]: این ویژگی مهمترین هدف پنهان‌نگاری است و بیان‌گر پوشیده ماندن وجود پیغام در تصویر است. با آشکار شدن وجود پیغام عملاً هدف پنهان‌نگاری نقض شده است.

چهار ویژگی فوق با هم در تعامل هستند و بهبود یک فاکتور، سه فاکتور دیگر را تحت تاثیر قرار می‌دهد. به عنوان مثال افزایش ظرفیت باعث تضعیف امنیت، کاهش مقاومت و کیفیت پنهان‌نگار می‌شود. لذا با توجه به کابرد مورد نظر بعضی تقویت و بعضی تضعیف می‌گردند. با توجه به این ویژگی‌ها، پنهان‌نگاری در حوزه فرکانس مقاومت بیشتر[3] و پنهان‌نگاری در حوزه مکان ظرفیت بیشتری را در اختیار قرار می‌دهد. تصاویر JPEG یکی از فرمت‌های معروف می‌باشند که به دلیل ارائه فشرده‌سازی خوب به وفور مورد استفاده قرار می‌گیرند. به همین دلیل پنهان‌نگاری اطلاعات در این تصاویر مورد توجه قرار گرفته است[1].

در این مقاله ویژگی‌های این نوع تصاویر مورد بررسی قرارگرفته و یک روش پنهان‌نگاری که ظرفیت و امنیت بالاتر و میانگین مجذور خطای کمتری را نسبت به الگوریتم‌های مشابه JSteg و OutGuess تولید می‌نماید، ارائه شده است.

ادامه مقاله به این صورت سازماندهی شده است: در بخش دوم فشرده‌سازی JPEG و ویژگی‌های تصویر JPEG مورد بررسی قرار گرفته است، در بخش سوم الگوریتم JSteg معرفی شده است، در بخش چهارم الگوریتم پیشنهادی تشریح شده است، در بخش پنجم نتایج مشاهدات و پیاده‌سازی الگوریتم پیشنهادی نشان داده شده است، در بخش ششم امنیت الگوریتم پیشنهادی مورد تست قرار گرفته است و در نهایت در بخش آخر نتیجه‌گیری آورده شده است.

۲- فشرده‌سازی JPEG

فشرده‌سازی JPEG شامل دو مرحله فشرده‌سازی بااتلاف[۸] و بدون بدون اتلاف[۹] روی تصویر می‌باشد. مرحله تبدیل کسینوسی گسسته و کوانتیزاسیون مرحله بااتلاف فشرده‌سازی و کدگذاری هافمن مرحله بدون اتلاف JPEG می‌باشد. فرآیند JPEG را می‌توان یک فیلتر پایین گذر در نظر گرفت که فرکانس‌های بالای موجود در تصویر را حذف می‌نماید[4]. این کار با انجام عمل کوانتیزاسیون روی ضرایب DCT[۱۰] بلاک های ۸×۸ از تصویر انجام می‌گردد. با توجه به این که در مرحله کوانتیزاسیون بخشی از اطلاعات تصویر دور ریخته می‌شوند، لذا این مرحله باید در طراحی سیستم پنهان‌نگار مورد توجه قرارگیرد. عمل کوانتیزاسیون شامل تقسیم ضرایب DCT بر ضرایب ماتریس کوانتیزاسیون شکل(۱) و گرد نمودن حاصل تقسیم می‌باشد. اگر بلاک JPEG توسط جداول کوانتیزاسیون Q_N ($1\le N\le 100$)تولید شده باشد و سپس این بلاک را مجدداً توسط جداول کوانتیزاسیون دیگری مانند Q_K تولید نمائیم، آنگاه در صورتی بلاک اولیه را می‌توان بازیابی‌نمود که شرط $K\le N$ برقرار باشد.

۳- الگوریتم پنهان‌نگاری JSteg

JSteg یکی از روش‌های شناخته شده‌ای است که روی تصاویر JPEG عمل پنهان‌نگاری را انجام می‌دهد [5]. در این روش اطلاعات بعد از رمزنگاری، درون LSB[۱۱] ضرایب DCT کوانتیزه شده مخفی می‌گردند. عمل پنهان‌نگاری با پیمایش زیگزاگ ضرایب DCT کوانتیزه شده (شکل۲) و جاسازی در ضرایبی که صفر،۱و۱- نیستند انجام می‌گردد. با توجه به این که بعد از عمل کوانتیزاسیون تعداد زیادی از ضرایب به صفر،۱و۱- تبدیل می‌شوند لذا ظرفیت پنهان‌نگاری این الگوریتم محدود می‌گردد[6]. البته شایان ذکر است که تغییر زیاد در ضرایب فرکانسی در مرحله کوانتیزاسیون تغییرات فاحشی را روی بلاک بازیابی شده ایجاد می‌نماید[7]. در [6] الگوریتمی جهت بالا بردن ظرفیت JSteg ارائه گریده ولی در عوض مقاومت الگوریتم قربانی شده است. از

۱ Capacity
۲. Watermarking
۳. Visibility
۴. Robustness
۵. Cover
۶. Stego
۷. Security

۸. Lossy
۹. Lossless
۱۰. Discrete Cosine Transform
۱۱. Least Significant Bit

طرفی مشکل اصلی این الگوریتم امنیت آن می‌باشد. وستفلد و فیتزمن در [8] روشی را با استفاده از آزمون Chi square روی ضرایب تبدیل کسینوسی گسسته کوانتیزه شده ارائه کرده‌اند که توسط آن می‌توان به راحتی تصاویر پوشانه را شناسایی کرد.

(u, v)	0	1	2	3	4	5	6	7
0	16	11	10	16	24	40	51	61
1	12	12	14	19	26	58	60	55
2	14	13	16	24	40	57	69	56
3	14	17	22	29	51	87	80	62
4	18	22	37	56	68	109	103	77
5	24	35	55	64	81	104	113	92
6	49	64	78	87	103	121	120	101
7	72	92	95	98	112	100	103	99

شکل ۱: ماتریس کوانتیزاسیون استاندارد

$$\begin{bmatrix} 25 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

شکل ۲: نمونه یک بلاک ۸×۸ بعد از کوانتیزاسیون

۴- الگوریتم پیشنهادی

۴-۱ ماتریس MSE

با توجه به اینکه در روش JSteg از LSB ضرایب غیر صفر و یک جهت جاسازی استفاده می‌شود لذا در حملات آماری این ضرایب مورد تحلیل آماری قرار گرفته و به راحتی تصاویر گنجانه آشکار می‌شوند. لذا اگر تدابیری اندیشیده شود که بتوان از ضرایب صفر، یک و 2LSB ضرایب نیز استفاده شود به نظر می‌رسد بتوان ضعف‌های این الگوریتم را بهبود بخشید. با توجه به اینکه بعد از مرحله کوانتیزاسیون JPEG مقادیر زیادی صفر و یک تولید می‌شود انتخاب این ضرایب جهت جاسازی باید به نحو کنترل شده‌ای صورت گیرد، چراکه از تمام ضرایب به علت از بین رفتن کیفیت تصویر نمی‌توان برای جاسازی پیغام استفاده کرد. با توجه به این نکته میزان خطای حاصل از تغییر هرضریب از ضرایب تبدیل کسینوسی گسسته کوانتیزه بین بلاک اصلی و بلاک بازیابی شده مورد بررسی قرار گرفت. این کار با تغییر یک واحد از ضرایب و محاسبه میانگین مجذور خطا بین بلاک اصلی و بلاک بازیابی شده صورت گرفت. نتیجه این بررسی به صورت ماتریسی بنام ماتریس میانگین مجذور خطا (MSE) در شکل (۳) ارائه شده‌است هر آرایه این ماتریس معرف مقدار میانگین مجذور خطای حاصل از تغییر یک واحد ضریب کسینوسی کوانتیزه شده برای آن آرایه می‌باشد. با توجه به این ماتریس می‌توان هر یک از ضرایب تبدیل کسینوسی گسسته را تغییر داد و میانگین مجذور خطای تولید شده برای بلاک بازیابی شده را در نظر گرفت. میانگین مجذور خطای حاصل از تغییر چندین ضریب نیز برابر جمع مقادیر متناظر با همان ضرایب در ماتریس MSE می‌باشد. اگرچه این ماتریس به ازای تغییر یک واحد از ضرایب تولید شده است در صورتی که ضریبی بیش از یک واحد تغییر نماید می‌توان میانگین مجذور خطای حاصل را با توجه به این ماتریس محاسبه نمود. مثلا میانگین مجذور خطای حاصل از تغییر 2LSB ضرایب برابر حاصلضرب ماتریس MSE در عدد چهار می‌باشد.

ویژگی ماتریس MSE این است که مستقل از تصویر پوشانه و تنها وابسته به ماتریس کوانتیزاسون استاندارد می‌باشد. اما چرا چنین ادعایی درست می‌باشد:

۴-۲ اثبات مستقل بودن ماتریس MSE از تصویر

می‌دانیم میانگین مجذور خطا (MSE) برای تصویر از رابطه زیر محاسبه می‌شود:

$$MSE = \left(\frac{1}{N}\right)^2 \sum_{i=1}^{N}\sum_{j=1}^{N}(x_{ij} - \bar{x}_{ij})^2 \qquad (۱-۲-۴)$$

در معادله فوق x_{ij} مقدار پیکسل‌های تصویرپوشانه، $\bar{x}_{ij}$ مقدار پیکسل‌های تصویر گنجانه و N تعداد پیکسل‌ها می‌باشد، منظور از تصویر گنجانه در اینجا، یک واحد تغییر در یک ضریب از ضرایب ماتریس تبدیل کوسینوسی گسسته کوانتیزه (با توجه به شکل ۱) می‌باشد. با توجه به اینکه مقادیر فوق را می‌توان از تبدیلات کسینوسی معکوس بدست آورد داریم:

$$x(i,j) = \sum_{u=0}^{7}\sum_{v=0}^{7} C(u)C(v)DCT(u,v) \cos\left[\frac{(2u+1)i\pi}{16}\right]\cos\left[\frac{(2v+1)j\pi}{16}\right] \qquad (۲-۲-۴)$$

$$\bar{x}(i,j) = \sum_{u=0}^{7}\sum_{v=0}^{7} C(u)C(v)\overline{DCT}(u,v) \cos\left[\frac{(2u+1)i\pi}{16}\right]\cos\left[\frac{(2v+1)j\pi}{16}\right] \qquad (۳-۲-۴)$$

که در آن :

$$C(v) = C(u) = \begin{cases} \frac{1}{\sqrt{8}} & u = 0 \\ \sqrt{\frac{2}{8}} & 0 < u \le 7 \end{cases} \qquad (۴-۲-۴)$$

با یک واحد تغییر در ماتریس ضرایب DCT کوانتیزه برای یک ضریب داریم :

$$\overline{DCT(m, n)} = DCT(m, n) + Q(m, n) \qquad ۵-۲-۴.$$

با جایگذاری رابطه (۴-۱-۵) در رابطه (۴-۱-۳) و در نهایت با جایگذاری دو رابطه (۴-۱-۳) و (۴-۱-۲) در رابطه (۴-۱-۱) و ساده‌سازی به رابطه زیر می‌رسیم:

۶-۲-۴.

$$MSE = \left(\frac{1}{N}\right)^2 \sum_{i=1}^{N}\sum_{j=1}^{N} \sum_{u=0}^{7}\sum_{v=0}^{7} C^2(u)C^2(v)Q^2(u,v) \cos^2\left[\frac{(2u+1)i\pi}{16}\right]\cos^2\left[\frac{(2v+1)j\pi}{16}\right]$$

با توجه به اینکه تنها یک ضریب تغییرکرده، بنابراین به جز در یک ضریب در بقیه‌ی ضرایب مقدار DCT و $\overline{DCT}$ با هم برابر هستند در نتیجه رابطه (۴-۱-۶) به صورت زیر ساده می‌شود:

۷-۲-۴.

$$MSE = \left(\frac{1}{N}\right)^2 \sum_{i=1}^{N}\sum_{j=1}^{N} C^2(m)C^2(n)Q^2(m,n) \cos^2\left[\frac{(2m+1)i\pi}{16}\right]\cos^2\left[\frac{(2n+1)j\pi}{16}\right]$$

که در رابطه (۴-۲-۷) $Q(m,n)$، ضریبی از ضرایب ماتریس کوانتیزاسیون استاندارد(شکل۱) می‌باشد که یک واحد تغییر کرده است. با ضرب MSE در عبارت $\left(\frac{N}{8}\right)^2$ جدول شکل (۳) نتیجه می‌شود.

مقدار MSE(i,j) در این ماتریس بیانگر آن است که به ازای یک واحد تغییر در ضریب $Q_{DCT}(i,j)$ (شکل۱)، میانگین خطایی برابر MSE(i,j) (جدول شکل۳) در بلاک بازیابی شده ایجاد خواهد شد. با توجه به این ماتریس، تغییر در محل‌های (۱،۳) و (۱،۲) کمترین مقدار خطا را برای بلاک بازیابی شده ایجاد خواهد نمود و این امر مستقل از تصویر خواهد بود. لذا این محل‌ها گزینه‌های بهتری نسبت به محل (۱و۱) (DC سیگنال) جهت پنهان‌نگاری می‌باشند. با توجه به این امر می‌توان از ضعف JSteg در مواجه با بعضی از بلاک ها بهره جست. برای مثال بلاک شکل(۲) را در نظر بگیرید. JSteg در این بلاک حداکثر یک بیت را مخفی می نماید و میانگین خطایی برابر ۴ برای بلاک بازیابی شده حاصل می گردد. در حالی که می توان دو بیت داده را در LSB محلهای (۱،۳) و (۱،۲) مخفی نمود و میانگین خطایی کمتر از ۴ را بدست آورد.

4.00	1.89	1.56	4.00	9.00	25.00	40.64	58.14
2.25	2.25	3.06	5.64	10.56	52.56	56.25	47.26
3.06	2.64	4.00	9.00	25.00	50.76	74.39	49.00
3.06	4.51	7.56	13.14	40.64	118.2	100.0	60.06
5.06	7.56	21.39	49.00	72.25	185.6	165.7	92.64
9.00	19.14	47.26	64.00	102.5	169.0	199.5	132.2
37.5	64.00	95.06	118.2	165.7	228.7	225.0	159.3
81.0	132.2	141.0	150.0	196.0	156.2	165.7	153.1

شکل ۳: ماتریس MSE بر اساس ماتریس کوانتیزاسیون استاندارد

۴-۳ الگوریتم جاسازی

با توجه به مطالب ذکر شده، برای پنهان‌نگاری در یک بلاک ۸×۸ بهتر است از ضرایبی که مقدار خطای کمتری دارند استفاده شود. با این ایده در هنگام جاسازی می‌توان از ضرایب صفر و یک استفاده کرد. در الگوریتم JSteg عمل انتخاب ضرایب جهت پنهان‌نگاری به صورت پیمایش زیگزاگ انجام می‌گیرد و این امر در نظر گرفته نشده است. اما سوال مهمی که به ذهن می‌رسد این است که در هر بلاک چه تعداد از ضرایب می‌توانند تغییر کنند؟ به عبارتی دیگر یک بلاک تحمل حداکثر چه خطایی را دارد؟ با تست‌های که روی بلاک‌های تصاویر متعدد به عمل آمد و همچنین بهره‌گیری از الگوریتم JSteg مشخص شد که حداکثر خطای قابل تحمل برای یک بلاک رابطه مستقیمی با فرکانس-های اصلی تشکیل دهنده‌ی آن بلاک دارد. منظور از فرکانس‌های اصلی، ضرایب DCT می‌باشد که بعد از مرحله کوانتیزاسیون JPEG تبدیل به صفر یا یک نمی‌شوند. در نتیجه هر چقدر ضرایب بیشتری از فیلتر کوانتیزاسیون عبور کنند قابلیت آن بلاک برای پذیرش تغییرات بیشتر می‌باشد. با توجه به این امر برای هر بلاک مقداری بنام MAX_{MSE} در نظر گرفته شد. این مقدار برابر است با مجموع مقادیر متناظر ضرایب غیر صفر و یک بلاک، در ماتریس MSE. برای مثال در بلاکی که تنها ضریب DC غیر صفر و یک دارد، MAX_{MSE} برابر مقدار ۴ می‌باشد. در این بلاک می‌توان از ضرایبی برای پنهان‌نگاری استفاده کرد که در مجموع میانگین مجذور خطای (MSE) آنها بیشتر از ۴ نگردد. از آنجائیکه با تغییر هر یک از ضرایب صفر و یک، همچنان این ضرایب در بازه صفر و یک باقی می مانند، لذا پارامتر MAX_{MSE} را به درستی می‌توان در سمت گیرنده بازیابی نمود و با توجه به آن پیغام پنهان شده در بلاک مورد نظر را استخراج نمود. تا این مرحله ترتیب انتخاب ضرایب جهت جاسازی و اینکه چه تعداد از ضرایب انتخاب شوند مشخص شد. بنابراین در فرآیند جاسازی ابتدا حداکثر خطای قابل تحمل برای

بلاک محاسبه می‌شود، سپس عمل جاسازی با شروع از ضریب با کمترین خطا به سمت ضرایب با خطای بیشتر ادامه می‌یابد و با جاسازی در هر ضریب، مجموع خطای تولیدی محاسبه می‌شود تا بیشتر از مقدار حداکثر خطای قابل تحمل برای بلاک(MAX_{MSE}) نباشد. تا این مرحله الگوریتم پیشنهادی سه ویژگی اول یک سیستم پنهان‌نگار را به مراتب بهتر از الگوریتم JSteg تأمین می‌نماید، هرچند که ویژگی امنیت نیز به علت بهره جستن از ضرایب صفر و یک بهبود یافته است. به منظور افزایش امنیت الگوریتم پیشنهادی، 2LSB بعضی از ضرایب را جهت جاسازی مورد استفاده قرار می‌دهیم. اما سوال مطرح این است که در چه بلاک هایی از LSB و درچه بلاک هایی از 2LSB استفاده شود؟ از آنجایی که تغییر در 2LSB خطای بیشتر (۴ برابر) را نسبت به LSB به بلاک تحمیل می‌کند بنابراین باید در انتخاب بلاک‌هایی که قابلیت تغییر 2LSB را دارند، دقت شود تا ظرفیت الگوریتم قربانی امنیت نشود. برای این امر پارامتری به عنوان پارامتر توزیع (DP) را تعریف می‌کنیم. پارامتر توزیع مشخص می‌کند که در چه بلاک‌هایی از LSB و در چه بلاک هایی از 2LSB استفاده شود. این مقدار را بین بازه (۱۰۰، ۴) در نظر می‌گیریم که توسط کاربر به عنوان پارامتری اختیاری به سیستم پنهان‌نگار داده می‌شود. برای جاسازی در هر بلاک ابتدا مقدار MAX_{MSE} بلاک محاسبه و با پارامتر DP مقایسه می‌شود، در صورتیکه مقدار MAX_{MSE} بلاک بیشتر از پارامتر توزیع باشد در آن بلاک از 2LSB ضرایب و در غیر این صورت از LSB ضرایب جهت جاسازی پیغام استفاده می‌شود. با توجه به روند جاسازی، هر چه پارامترDP مقدار بزرگتری داشته باشد از 2LSB های کمتری استفاده خواهد شد. در ادامه جهت پیاده‌سازی الگوریتم جاسازی توجه به نکات ذیل ضروری به نظر می رسد:

نکته ۱: از آنجائیکه باید بتوان MAX_{MSE} را در سمت گیرنده از تصویرگنجانه بدرستی استخراج کرد، بنابراین نباید از ضرایبی که بعد از پنهان‌نگاری به صفر یا یک تبدیل می‌شوند استفاده کرد. لذا هنگام جاسازی در 2LSB ضرایب، از ضرایبی که در بازه [۳،۳-] قرار دارد استفاده نمی‌شود.

نکته ۲: می‌دانیم جاسازی بیت یک در ضرایب با مقدار صفر، منجر به یک شدن این ضرایب می‌شود. به دلیل فراوانی بیشتر این ضرایب در هیستوگرام تصویر پوشانه و استفاده از از آن‌ها در جاسازی، هیستوگرام تصویر دستخوش تغییرات محسوسی می‌شود. به منظور اجتناب از ایجاد چنین رفتاری، هنگام جاسازی، نیمی از این ضرایب به ۱و نیمی دیگر به ۱- تبدیل می‌شوند.

۵- نتایج آزمایشگاهی

نتایج حاصل از پیاده‌سازی توسط نرم افزار MATLAB بر روی تصاویر متعدد نشان می‌دهد که الگوریتم پیشنهادی ویژگی‌های یک سیستم پنهان‌نگار را به نحو مطلوبی تأمین می‌نماید. در جدول(۱) نتایج حاصل از پیاده‌سازی الگوریتم برای حالتی که فقط از LSB ضرایب استفاده شده، نشان داده شده‌است که گویای ظرفیت بالای الگوریتم مذکور نسبت به JSteg می‌باشد. در جدول(۲) بر اساس پارامتر توزیع(DP) از 2LSB ضرایب نیز استفاده شده‌است. نتایج موید ظرفیت قابل قبول این الگوریتم حتی در صورت استفاده از 2LSB ضرایب می‌باشد. علاوه بر این نتایج گویای آن است که هر چه مقدار پارامتر توزیع (DP) کمتر انتخاب شود درصد استفاده از 2LSB ها بیشتر و ظرفیت کمتر و سیستم در مقابل حملات مقاومتر می‌شود.

۶ - تست امنیت

همواره یکی از مطرح ترین ایده‌های پنهان‌نگاری، جاسازی در LSB حوزه‌های مختلف تصاویر بوده و هست. این امر به نوبه‌ی خود باعث طراحی چندین حمله به این روش شده است. توانایی کشف پیام در تصویر به طول پیام پنهان بستگی دارد. واضح است که هرچه مقدار اطلاعاتی که در یک تصویر قرار می‌دهیم کمتر باشد امکان کمتری هست که نشانه‌های قابل کشف به وجود آید. همانطور که در مرجع [8] توضیح داده شده است جایگذاری بیت یک (صفر) در ضرایبی با مقدار 2k آنها را به 2k+1 (2k) و جایگذاری بیت صفر (یک) در ضرایبی با مقدار 2k+1 آنها را به 2k (2k+1) تبدیل می‌کند. از آنجا که داده‌هایی که باید جاسازی شوند ابتدا فشرده و سپس رمز می‌شوند توزیع تعداد بیت‌های یک با توزیع تعداد بیت‌های صفر در آنها برابر است. برابری تقریبی تعداد یک‌ها و صفرها در داده‌هایی که باید جاسازی شوند باعث بوجود آمدن جفت مقادیری می‌شود که تقریبا مقداری مساوی دارند. بوجود آمدن این اثر را در شکل (۴) به وضوح می‌توان مشاهده کرد. می‌توان با مقایسه مقدار این جفت‌ها با مقدار تئوریک حاصل از تحلیل آماری, احتمال آنکه این جفت‌ها در اثر جاسازی تولید شده باشند را محاسبه کرد.

اما در الگوریتم جدید به دلیل استفاده از ضرایب صفر ،یک و2LSB ضرایب، حالت گوسی گسسته هیستوگرام تصویر پوشانه با وجود افزایش ظرفیت حفظ شده‌است.

جدول ۱: میزان ظرفیت و PSNR الگوریتم پیشنهادی بدون استفاده از پازامتر توزیع DP

الف) مقدار PSNR هر دو الگوریتم بر روی تصاویر آزمایشی

تصویر	JSTEG	الگوریتم پیشنهادی
baboon	۳۵.۵۰	۳۵.۷۰
man	۳۸.۷۸	۳۹.۴۴
Lena	۳۸.۲۴	۳۸.۵۸
camera	۳۷.۶۵	۳۷.۸۳

ب)ظرفیت پنهان سازی دو الگوریتم بر روی تصاویر آزمایشی (بر حسب بیت)

تصویر	JSTEG	الگوریتم پیشنهادی
baboon	۳۳۱۶۵	۴۱۱۷۷
man	۱۹۶۰۷	۲۳۳۹۶
Lena	۵۳۷۳	۶۵۱۶
camera	۴۷۵۲	۶۳۰۰

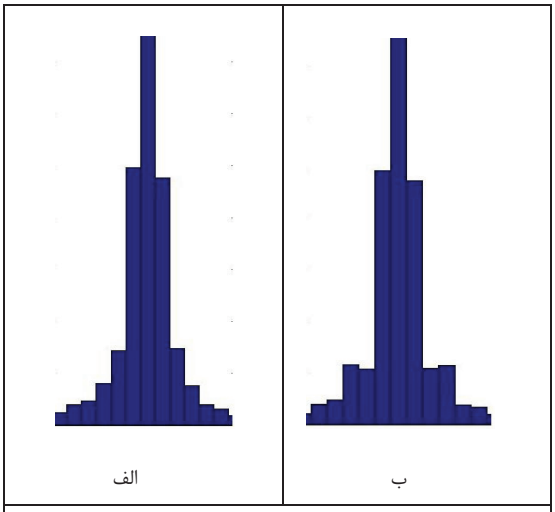
جدول ۲: میزان ظرفیت و PSNR الگوریتم پیشنهادی با استفاده از پازامتر توزیع DP

الف) مقدار PSNR هر دو الگوریتم بر روی تصاویر آزمایشی

تصویر	مقدار DP	الگوریتم پیشنهادی
baboon	۴۰	۳۵.۵۹
man	۲۵	۳۹.۲۳
Lena	۲۵	۳۸.۴۷
camera	۴۰	۳۷.۷۵

ب)ظرفیت پنهان‌نگاری الگوریتم پیشنهادی (بر حسب بیت)

تصویر	الگوریتم پیشنهادی	درصد استفاده از ضرایب صفر و یک	درصد استفاده از 2LSB ها
baboon	۳۲۷۸۳	۲۲.۵۹	۲۷.۴۱
man	۱۹۸۰۱	۲۵.۳۵	۱۴.۳۷
Lena	۵۱۱۷	۲۲.۶۸	۲۵.۴۷
camera	۵۱۹۶	۲۲.۷۴	۲۵.۳۸



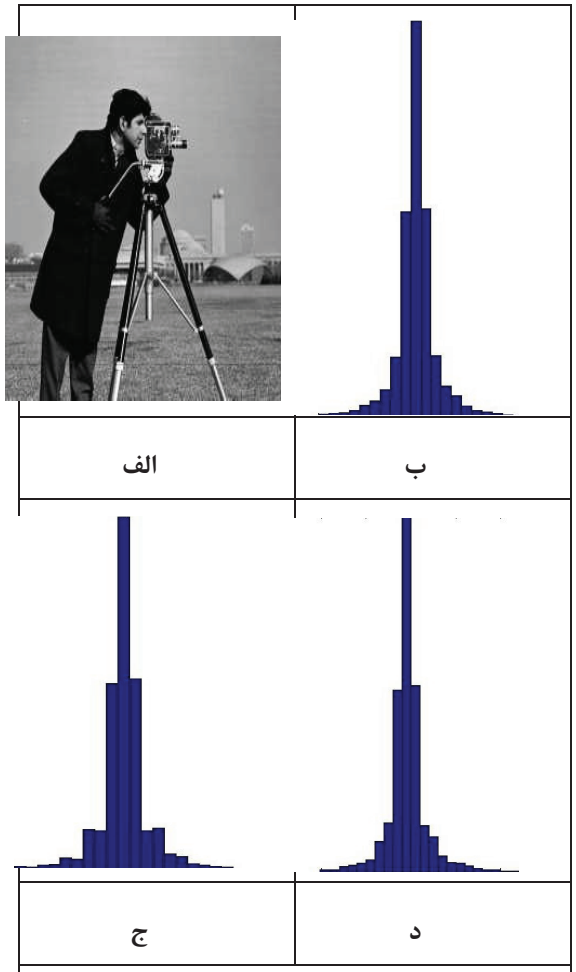
الف: هیستوگرام ضرایب کسینوسی گسسته برای تصویر اصلی Lena .
ب: هیستوگرام ضرایب کسینوسی گسسته برای تصویر حامل اطلاعات.

شکل ۴: مقایسه هیستوگرام برای تصویرنمونه Lena

در شکل (۵) هیستوگرام ضرایب DCT کوانتیزه شده تصویر camera برای تصویر اصلی JPEG، تصویر تولید شده توسط JSteg و تصویر تولید شده توسط الگوریتم پیشنهادی ارائه شده است. نتایج گویای این واقعیت است که ضرایب تبدیل کسینوسی کوانتیزه شده که توسط الگوریتم پیشنهادی تغییر کرده‌اند همچنان توزیع یکنواخت گوسی خود را مانند تصویر JPEG اصلی حفظ نموده‌اند. روش پیشنهادی در برابر حمله آماری آزمون Chi square برای صد تصویر گنجانه برای ۵ ظرفیت مختلف (۳۰%، ۵۰% ، ۷۰% و۱۰۰% ظرفیت JSteg) در هر بار، مورد بررسی قرار گرفت و نتایج حاصل از آزمون Chi square [8] موید امنیت بالای روش بود.

۷- نتیجه‌گیری

ظرفیت پنهان‌نگاری بالا، کیفیت مطلوب، مقاومت در برابر اعمالی نظیر فشرده‌سازی و امنیت در برابر روش‌های آماری فاکتورهای اساسی می‌باشند که باید در سیستم‌های پنهان‌نگار مورد توجه قرار بگیرند. نکته‌ای که حائز اهمیت می‌باشد آن است که برآورده نمودن همه ویژگی‌ها به صورت همزمان بسیار دشوار بوده و با توجه به کابرد مورد نظر بعضی تقویت و بعضی تضعیف می‌گردند. اما ما با ارائه روش جدید مطرح شده، هر سه فاکتور کیفیت، امنیت و ظرفیت را افزایش دادیم. از آنجائیکه در الگوریتم پیشنهادی، MSE آستانه را برای بلاک، با توجه به ضرایب غیر صفر،یک محاسبه می‌نمودیم، لذا به نظر می‌رسد با تخمین دقیقتری از MSE آستانه برای یک بلاک، بتوان تغییرات ناشی از تغییر ضرایب را برای چشم انسان نامحسوس‌تر نمود. این کار را می‌توان با توجه به ویژگی‌های ظاهری تصویر مانند خشن بودن و یا آرام بودن تصویر انجام داد.



الف) تصویر camera . ب) هیستوگرام ضرایب کسینوسی کوانتیزه شده مربوط به تصویر الف. ج) هیستوگرام ضرایب کسینوسی کوانتیزه شده مربوط به تصویر حاصل از JSteg ، حامل ۴۷۵۲ بیت داده.د) هیستوگرام ضرایب کسینوسی کوانتیزه شده مربوط به تصویر حاصل از الگوریتم پیشنهادی حامل ۵۱۹۶ بیت داده.

شکل۵: مقایسه هیستوگرام برای تصویرنمونه camera

مراجع

[1] T Morkel, JHP Eloff and MS Olivier, 'An Overview of Image Steganography', in Proceedings of the Fifth Annual Information Security South Africa Conference (ISSA2005), Sandton, South Africa, June/July 2005.

[2] L.Chang. 'Issues in Information Hiding Transform Techniques',NRL Memorandum report ,2002. .www. citeseer.ist.psu.edu/564003.html.

[3] Fabien A. P. Petitcolas, Ross J. Anderson and Markus G. Kuhn 'Information Hiding-A Survy' Proceedings of the IEEE, special issue on protection of multimedia content, 87(7):1062-1078, July 1999.

[4] W.B. Pennebaker, J.L. Mitchell, 'JPEG :Still standard" Van Nostrand Reinhold, New York,1993.

[5] C.T. Hsu, J.L. Wu, 'Hidden digital watermarks in images', IEEE Transactions on Image Processing 8 (1) (1999) 58–68.

[6] Chin-Chen Chang a, Tung-Shou Chen b,1, Lou-Zo Chung 'A steganographic method based upon JPEG and quantization table modification', Information Sciences 141 (2002) 123–138.

[7] P.H.-W. Wong and O.C. Au, 'Data hiding and watermarking in JPEG compressed domain by DC coefficient modification,' in Proc. SPIE, vol.3971, pp.237–244, 2000.

[8] Westfeld, A., Pfitzman, A., “Attacks on Steganographic Systems”, Proc. 3rd Int’l Information Hiding Workshop , Springer-Verlog, Berlin Heidelberg New York, , pp. 61-76, 1999.