مروری بر روش‌های نهان‌نگاری در JPEG و بررسی امنیت آن‌ها

فاطمه‌السادات جمالی دینان
محمّد رضایی، مریم بیگ‌زاده و الهه بیات
پژوهشکده پردازش هوشمند علائم

چکیده

فرمت JPEG پرکاربردترین قالب تصویری در ارتباطات دیجیتال است و در طی سال‌های اخیر روش‌های نهان‌نگاری متنوعی برای آن ارائه شده است. هدف از این تحقیق معرّفی و ارائه‌ی اطّلاعات همه‌جانبه و کاملی در مورد روش‌های نهان‌نگاری در تصاویر JPEG و دسته‌بندی این روش‌ها و ارائه‌ی راهکارهایی برای بالابردن امنیت آن‌ها با توجه به ساختار پوشانه می‌باشد. در این راستا عوامل تأثیرگذار در امنیت، روش‌های نهان‌نگاری در JPEG که وابسته به پوشانه می‌باشد، مثل اثر دوبارفشرده‌سازی، فرکانس مکانی، ضریب‌کیفیت و... شناسایی شده و به‌صورت تئوری و تجربی مورد ارزیابی قرار گرفته است. علاوه‌بر این کلیه‌ی الگوریتم‌ها و نرم‌افزارهای نهان‌نگاری موجود در این فرمت، معرفی شده و از دیدگاه‌های مختلف، ارزیابی و دسته‌بندی شده‌اند. برخی از این الگوریتم‌ها در نرم‌افزار Stegotest پیاده‌سازی شده است و اثر تخریب ناشی از نهان‌نگاری در روش‌های موجود مقایسه شده است.

واژگان کلیدی: تصاویر JPEG، سیستم نهان‌نگاری، نهان‌کاوی، امنیت.

۱- مقدمه

نهان‌نگاری[1] واژه‌ای یونانی به معنی نوشته‌ی استتار شده می‌باشد؛ و درواقع علم و هنر پنهان‌کردن ارتباط به‌وسیله‌ی قراردادن پیام در یک پوشانه[2] است؛ به‌گونه‌ای که کم‌ترین تغییر قابل کشف را در آن ایجاد نماید و نتوان وجود پیام پنهانی را در رسانه، حتّی به‌صورت احتمالی آشکار ساخت *(ساتیش۲۰۰۴، ص ۵۷۸-۵۹۰)*.

در برابر نهان‌نگاری، دانش نهان‌کاوی[3] که هنرِ کشفِ وجودِ ارتباطِ پنهان است، قرار دارد. هدف از نهان‌کاوی، تمیزدادن رسانه‌های حاوی اطّلاعات پنهان از رسانه‌ی عادی است.

به‌طور کلی در سیستم‌های اختفای اطّلاعات، چند ویژگی مهم ازجمله مقاومت[4]، ظرفیت[5]، امنیت[6]، شفّافیت[7]، پیچیدگی[8] برای ارزیابی و مقایسه‌ی الگوریتم‌های جاسازی توسط پتیتکولاس *(فابین، پتیتکولاس۱۹۹۹، ص ۵۷۴-۵۷۹)* تعریف شده است؛ که در این میان چهار شاخص اصلی ظرفیت، امنیت (به مفهوم عدم کشف وجود پیام در رسانه نهان‌نگار حتی به‌صورت احتمالی)، شفّافیت و مقاومت اهمیّت ویژه‌ای دارند.

در هر حال باید توجّه داشت که امکان بهینه‌سازی تمام شاخص‌ها، هم‌زمان وجود ندارد و با بهبود یکی، امکان تضعیف یک یا چند شاخص دیگر وجود خواهد داشت.

تصاویر، مهم‌ترین رسانه‌ی مورد استفاده، به‌خصوص در اینترنت هستند *(آندرسون۱۹۹۸،ص۴۷۴-۴۸۱)*؛ که با توجّه به محدودیت درکِ بصری انسان از تغییرات صورت گرفته در آن‌ها، به‌عنوان یکی از بهترین رسانه‌های پوشانه در نهان‌نگاری معرفی شده‌اند. در این میان، تصاویر JPEG به

[1] Steganography
[2] Cover image
[3] Steganalysis
[4] robustness
[5] capacity
[6] Security
[7] Transparency
[8] Complexity

دلیل داشتن حجم کم و کیفیت مناسب، بیشتر از سایر فرمت‌های تصویری در اینترنت و صفحات وب مورد استفاده قرار می‌گیرند *(المحمد۲۰۰۸،ص۵۴۴-۵۴۹)*؛ در بررسی اخیری که بر روی تصاویر موجود در اینترنت از طریق سایت google انجام دادیم، مشخّص شد که ۴۴٪ تصاویر موجود در اینترنت از نوع JPEG، ۳۳٪ از نوع GIF، ۲۲٪ از نوع PNG، ۰/۸٪ از نوع BMP و بقّیه متعلّق به سایر فرمت‌ها مثل TIF،SWF, MNG,PGM و... می‌باشند. استفاده‌ی روزافزون از فرمت JPEG باعث شده تا الگوریتم‌های نهان‌نگاری و نهان‌کاوی مربوط به این فرمت از سایر فرمت‌ها بیشتر و پرکاربردتر باشد.

در این مقاله عوامل مؤثر را بر امنیتِ سیستم‌های نهان‌نگاری در فرمت JPEG، با توجّه به ساختار پوشانه مورد بررسی و مطالعه قرار داده‌ایم؛ و اثر برخی از آن‌ها را به‌صورت ریاضی و تجربی اثبات کرده و بدین ترتیب راهکارهایی نوین برای افزایش امنیت سیستم نهان‌نگاری پیشنهاد داده‌ایم. علاوه‌بر این، کلیه‌ی روش‌های موجودِ نهان‌نگاری را در تصاویر JPEG، بررسی و آن‌ها را از دیدگاه‌های مختلفی طبقه‌بندی کرده‌ایم؛ که این طبقه‌بندی‌ها در نوع خود، جدید و بی‌نظیر است. در ادامه در بخش دوم، استاندارد فرمت JPEG را مورد بررسی قرارداده‌ایم. در بخش سوم به معرفی عوامل مؤثّر در امنیت سیستم نهان‌نگاری در تصاویرJPEG پرداخته‌ایم. بخش چهارم به معرفی الگوریتم‌های نهان‌نگاری در تصاویرJPEG اختصاص دارد و در بخش پنجم نتیجه‌گیری مباحث مطرح شده بیان شده است.

۲- استاندارد JPEG

با مطالعهٔ ساختار JPEG عوامل متعددی را می‌توان یافت، که در تأمین امنیت نهان‌نگاری در آن مؤثرند. در راستای تأمین این هدف در این بخش در ابتدا استاندارد JPEG را مورد مطالعه و بررسی قرار داده‌ایم.

۲- ۱- مراحل فشرده سازی به روش JPEG

در سال ۱۹۹۲، استاندارد JPEG به‌منظور فشرده‌سازی تصاویر ثابت[1] رنگی و سیاه‌وسفید توسط گروه JPEG[2] معرّفی شد؛ در این فرآیند در ابتدا فضای رنگ تصویر از RGB به YCbCr تبدیل می‌شود:

$$\begin{aligned} Y &= 0.299R + 0.587G + 0.114B \\ C_b &= -0.1687R - 0.3313G + 0.5B + 128 \\ C_r &= 0.5R - 0.4187G - 0.0813B + 128 \end{aligned} \quad (۱)$$

مرحله‌ی بعدی، نمونه‌برداری از مؤلّفه‌های رنگ و کاهش وضوح مکانی آن‌ها به‌منظور بهینه‌سازی فرآیند فشرده‌سازی است. بعد از نمونه‌برداری، هر کانال به قالب‌های ۸×۸ تقسیم می‌شود و مؤلّفه‌های Y و Cb و Cr هر قالب با استفاده از تبدیل کسینوسی گسسته‌ی هنجار شده‌ی استاندارد، به حوزه‌ی فرکانس برده می‌شوند.

$$G_{u,v} = \alpha(u)\alpha(v)\times \sum_{x=0}^{7}\sum_{y=0}^{7} g_{x,y}\cos\left[\frac{\pi}{8}(x+\frac{1}{2})u\right]\cos\left[\frac{\pi}{8}(y+\frac{1}{2})v\right] \quad (۲)$$

که در آن $g_{x,y}$ مقادیر پیکسل‌ها در مختصات x و y، و $G_{u,v}$ مقادیر ضرایب DCT در مختصات u وv می‌باشد. u معرف فرکانس‌های مکانی افقی برای مقادیر صحیح $0 < u < 8$ و v معرف فرکانس‌های مکانی عمودی برای مقادیر صحیح $0 < v < 8$ است؛ $\alpha(n)$ (مقادیر هنجارسازی) برابر هستند با:

$$\alpha(n) = \begin{cases} \sqrt{\frac{1}{8}} & n = 0 \\ \sqrt{\frac{2}{8}} & otherwise \end{cases} \quad (۳)$$

سپس فرآیند چندی‌سازی با تقسیم هر جزء فرکانسی بر یک ثابت و گردکردن آن به نزدیک‌ترین عدد صحیح انجام می‌شود. ماتریس چندی‌سازی مؤلّفه‌ی شدّت روشنایی از رابطه‌ی چهار و ماتریس مؤلّفه‌های رنگ از رابطه‌ی پنج به‌دست می‌آید:

$$C_y(w_x, w_y) = \quad (۴)$$

$$\begin{bmatrix} 16 & 11 & 10 & 16 & 24 & 40 & 51 & 61 \\ 12 & 12 & 14 & 19 & 26 & 58 & 60 & 55 \\ 14 & 13 & 16 & 24 & 40 & 57 & 69 & 56 \\ 14 & 17 & 22 & 29 & 51 & 87 & 80 & 62 \\ 18 & 22 & 37 & 56 & 68 & 109 & 103 & 77 \\ 24 & 35 & 55 & 64 & 81 & 104 & 113 & 92 \\ 49 & 64 & 78 & 87 & 103 & 121 & 120 & 101 \\ 72 & 92 & 95 & 98 & 112 & 100 & 103 & 99 \end{bmatrix}$$

[1] Continuous-tone still images
[2] Joint Photographic Experts Group

$$C_{C_bC_r}(w_x,w_y)= \tag{۵}$$

$$\begin{bmatrix} 17 & 18 & 24 & 47 & 99 & 99 & 99 & 99 \\ 18 & 21 & 26 & 66 & 99 & 99 & 99 & 99 \\ 24 & 26 & 56 & 99 & 99 & 99 & 99 & 99 \\ 47 & 66 & 99 & 99 & 99 & 99 & 99 & 99 \\ 99 & 99 & 99 & 99 & 99 & 99 & 99 & 99 \\ 99 & 99 & 99 & 99 & 99 & 99 & 99 & 99 \\ 99 & 99 & 99 & 99 & 99 & 99 & 99 & 99 \\ 99 & 92 & 99 & 99 & 112 & 100 & 103 & 99 \end{bmatrix}$$

البته عامل دیگری هم در فرآیند فشرده‌سازی دخالت دارد و آن ضریب کیفیّت است. درنهایت ضرایب نهایی از رابطه‌ی شش به‌دست می‌آیند:

$$F_q(w_x,w_y)=\left\lfloor \frac{F(w_x,w_y)}{S(w_x,w_y)}+\frac{1}{2} \right\rfloor \qquad w_x,w_y=0,..,7 \tag{۶}$$

که در آن $F(w_x,w_y)$ ضرایب DCT چندی نشده و $F_q(w_x,w_y)$ ضرایب DCT چندی‌شده می‌باشد. و $S(w_x,w_y)$ پله‌های چندی‌ساز وابسته به فرکانس می‌باشند و از رابطه‌ی ۷ به‌دست می‌آیند:

$$S(w_x,w_y)= \tag{۷}$$

$$\begin{cases} \max\left(\left\lfloor \frac{200-2Q}{100}C(w_x,w_y)+\frac{1}{2} \right\rfloor,1\right) & 50\le Q\le 100 \\ \left\lfloor \frac{50}{Q}C(w_x,w_y)+\frac{1}{2} \right\rfloor & 0\le Q\le 50 \end{cases}$$

که در آن Q ضریب‌کیفیّت است و $C(w_x,w_y)$ برای ضرایب شدّت روشنایی از رابطه‌ی چهار و برای مؤلّفه‌های رنگ از رابطه‌ی پنج به‌دست می‌آید؛ در خاتمه یک مرحله‌ی کدگذاری مبتنی بر آنتروپی[1] روی تصویر انجام می‌شود.

۳-عوامل مؤثّر بر امنیت نهان‌نگاری در تصاویر JPEG

با توجّه به ساختار JPEG فضاهای خاصّی برای جاسازی اطّلاعات در آن وجود دارد. به‌طورکلی الگوریتم‌های نهان‌نگاری در JPEG را می‌توان به سه گروه اصلی تقسیم‌بندی کرد؛ برخی از روش‌های نهان‌نگاری در JPEG بر اساس ویژگی‌های ساختار فایل ایجاد شده و نهان‌نگاری در آن‌ها در نواحی خاصی از فایل، مثل سرآیند[2] فایل و... انجام می‌شوند. گروه دوم شامل روش‌هایی است که در آن‌ها جاسازی اطّلاعات به‌گونه‌ای مقاوم در برابر فشرده‌سازی JPEG انجام می‌شود و درنهایت تصویر گنجانه، فشرده می‌شود *(فردریک۲۰۰۵، ص۶۷-۸۱، سولانکی۲۰۰۷، لی۲۰۰۶، ص۱۰۰۵۰-۱۰۰۵۳)*. گروه سوم که عمده‌ی روش‌های نهان‌نگاری در JPEG در این دسته قرار می‌گیرد، شامل روش‌هایی است که با استاندارد JPEG تطابق یافته‌اند؛ یعنی ابتدا پوشانه به قالب[3]های ۸×۸ تقسیم می‌شود و تبدیل DCT روی هر قالب اعمال شده و فرآیند فشرده‌سازی روی آن انجام می‌شود؛ سپس نهان‌نگاری به‌طور معمول با دست‌کاری ضرایب DCT قالب‌های ۸×۸ صورت می‌گیرد *(چانگ۲۰۰۲، ص۱۲۳-۱۳۸، لی۲۰۰۳، ص۹۶۷-۹۸۱، مونیراجان۲۰۰۴، ص۲۸۶-۲۹۱، رانگرانگ۲۰۰۶،ص۳۶۵-۳۶۸، سِنگ۲۰۰۴، ص۱۴-۱۶، وانگ۲۰۰۱،ص۳۰۹-۳۴۰)*. در این تحقیق به‌طور خاص روی عوامل تأثیرگذار در امنیت روش‌های گروه سوم که وابسته به ساختار پوشانه می‌باشد؛ متمرکز شده‌ایم و اثر آن‌ها را به‌صورت تئوری و تجربی مورد ارزیابی و تحلیل قرار داده‌ایم.

برای تهیه‌ی پایگاه داده‌ی لازم جهت آزمایش و ارزیابی، از یک سری تصویر با بافت متنوع و ابعاد ۳۰۰۰×۲۰۰۰، که توسط دوربین Nikon تهیه شده بودند، استفاده گردید. از بین تصاویر موجود، تعداد ۲۰۰۰ تصویر برش‌یافته به ابعاد ۶۷۰×۵۰۰ ، ۶۷۰×۵۰۰، ۹۶۰×۷۲۰ و ۹۶۰×۷۲۰ تهیه و به فرمت BMP ذخیره گردید؛ سپس این تصاویر با ضریب کیفیت‌های مختلفی چون (۲۵، ۳۰، ۴۵، ۵۰، ۶۰، ۷۰، ۸۰، ۸۵، ۹۰ و ۹۹) به فرمت JPEG تبدیل شدند. به این ترتیب، در مجموع تعداد ۲۰۰۰۰ پوشانهٔ JPEG با ۱۰ ضریب کیفیت مختلف و نیز ۲۰۰۰ تصویر BMP پوششی تولید شد. از این ۲۰۰۰ تصویر در هر مجموعه، ۱۰۰۰ تصویر برای تعلیم مدل‌های SVM و ۱۰۰۰ تصویر برای آزمایش در نظر گرفته شدند.

به‌منظور بررسی امنیت از یک نرم‌افزار نهان‌کاو کور استفاده کرده‌ایم که در آن شانزده مدل را با طبقه‌بندی‌کننده‌ی SVM با مجموع ۱۸۵ ویژگی از ویژگی‌های به‌دست آمده از DCT و مارکوف مبتنی بر ایده‌های الهام گرفته شده از *(وانگ۲۰۰۱، ص۳۰۹-۳۴۰، یونی۲۰۰۶)* تعلیم داده‌ایم.

برای اندازه‌گیری خطای آشکارسازی از رابطه‌ی ۸ استفاده کرده‌ایم که در *(فردریک ۲۰۰۵، ص۶۷-۸۱،*

[1].Entropy encoding
[2] Header
[3] Block

فردیک ۲۰۰۷، ص۳-۱۴، کودوفسکی ۲۰۰۸، ص۱-۱۳) هم بدان اشاره شده است:

$$P_E = \frac{P_{FA} + P_{FR}}{2} \quad (۸)$$

که در آن P_{FA} احتمال تشخیص نادرست پوشانه‌ها به‌عنوان گنجانه‌ها و P_{FR} احتمال انتخاب گنجانه‌ها به جای پوشانه است.

۳-۱- تأثیر کانال

در تصاویر JPEG با سه کانال روبرو هستیم؛ یک کانال مربوط به مؤلفه‌های شدّت روشنایی می‌باشد و دو کانال باقی‌مانده مربوط به مؤلّفه‌های رنگ می‌باشند؛ حال به‌راستی بین ضرایب موجود در مؤلّفه‌های شدّت‌روشنایی و رنگ، کدام ضرایب برای نهان‌نگاری مناسب‌ترند؟

به سه دلیل عمده‌ی زیر می‌توان اعلام کرد که مؤلفه‌های شدّت روشنایی مناسب‌ترند:

۱- با توجّه به این‌که، این مؤلّفه‌ها به‌هنگام فشرده‌سازی با ضرایب چندی‌سازی بزرگتری، چندی می‌شوند؛ لذا در ساختار آن‌ها یک سری صفرهای به‌هم‌پیوسته مشاهده می‌کنیم که با نهان‌نگاری در آن‌ها، این ساختار پیوسته به هم می‌خورد و نهان‌نگاری در آن‌ها مشهود می‌شود.

۲- در مؤلّفه‌های رنگ اگر ضرایب (۰ و ۱و ۱-) و DC را کنار بگذاریم؛ تعداد ضرایب باقی مانده، در عمل خیلی ناچیز است. لذا ظرفیت جاسازی در آن‌ها بسیار پایین است. (جدول ۱) تعداد میانگین ضرایب مناسب نهان‌نگاری را در ده گروه ی JPEG با ضریب کیفیت‌های متفاوت، برای سه کانال Y، Cbو Cr نشان می‌دهد.

(جدول۱) تعداد میانگین ضرایب مناسب جاسازی در سه کانال Y،Cb،Cr برای ده گروه تصویر نمونه با ضریب کیفیت‌های متفاوت.

گروه تصویری	ضریب کیفیت	کانال Y	کانال C_b	کانال C_r
۱	۲۵	۴۶۷۱	۶۳	۱۸
۲	۳۰	۹.۵×۱۰^{۳}	۱۴۶.۷	۵۳
۳	۴۵	۱.۴×۱۰^{۴}	۴۳۶	۱۷۹
۴	۵۰	۱.۸×۱۰^{۴}	۶۵۰.۱	۲۹۲.۲
۵	۶۰	۱.۹×۱۰^{۴}	۶۰۱.۴	۲۸۹.۷
۶	۷۰	۲.۳×۱۰^{۴}	۹۹۸.۵	۵۰۴.۱
۷	۸۰	۲.۶×۱۰^{۴}	۱.۶۳×۱۰^{۳}	۹۱۲.۵
۸	۸۵	۳.۰۲×۱۰^{۴}	۱.۹۲×۱۰^{۳}	۱.۰۴×۱۰^{۳}
۹	۹۰	۵.۱×۱۰^{۴}	۶.۲۲×۱۰^{۳}	۴.۲۱×۱۰^{۳}
۱۰	۹۹	۱.۱×۱۰^{۵}	۱.۹۷×۱۰^{۴}	۱.۶۳×۱۰^{۴}

۳ - اگر تغییری در ضرایب AC مؤلّفه‌های رنگ ایجاد کنیم از آن‌جا که مقادیر ماتریس چندی‌سازی مربوط به آن‌ها بزرگ است؛ خطای ناشی از جاسازی در آن‌ها بیشتر از ضرایب شدّت‌روشنایی است. این اثر در بخش ۳-۲ به‌صورت ریاضی اثبات شده است و برای اثبات شهودی آن هم در (جدول ۲) مقادیر میانگین PSNR گروه‌های تصویری مورد آزمایش را برای روش نهان‌نگاری مبتنی بر تطبیق کم‌ارزش در سه حالت مختلف نشان می‌دهد در گروه (الف) تغییرات روی کانال Y، در گروه (ب) تغییرات روی کانال C_b و در گروه (ج) تغییرات روی کانال C_r انجام شده است. لازم به ذکر است تعداد تغییرات انجام شده روی هر سه کانال، مساوی است و از رابطه‌ی ۹ به‌دست می‌آید:

$$NC = \min(\text{cap}(Y), \text{cap}(C_b), \text{cap}(C_r)) \quad (۹)$$

که در آن cap بیانگر بیشینه، ظرفیت جاسازی در کانال مورد نظر می‌باشد.

در (جدول ۳) خطای نرم‌افزار نهان‌کاو را در سه حالت نهان‌نگاری در سه کانال برای تصاویر گروه شش (تصاویری با ضریب‌کیفیت هفتاد) آورده‌ایم. ملاحظه می‌شود خطای نرم‌افزار نهان‌کاو در برابر روش‌های نهان‌نگاری در کانال Y بیشتر از دو مؤلِفه‌ی شدّت رنگ است؛ و این مسأله مطابق با انتظار ما است.

(جدول۲) مقادیر میانگین PSNR برای سه کانال در ۱۰ گروه تصویر JPEG نمونه برای روش نهان‌نگاری مبتنی بر تطبیق بیت کم ارزش (تعداد تغییرات انجام شده در هر سه کانال مساوی و از رابطهٔ ۹ به‌دست‌آمده است.)

گروه تصویر	ضریب کیفیت	NC	PSNR		
			Y	C_b	C_r
۱	۲۵	۱۰.۲۳	۶۵.۷	۵۹.۶	۶۰.۹
۲	۳۰	۴۰	۶۵	۵۸	۵۹
۳	۴۵	۱۵۱.۸	۶۲.۳	۵۵.۵	۵۵.۸
۴	۵۰	۲۵۷.۷	۶۱.۵	۵۳.۹	۵۵.۳
۵	۶۰	۲۶۱.۰۳	۶۲.۵	۵۴.۷	۵۶.۱
۶	۷۰	۴۶۰.۷	۶۰.۸	۵۳.۱	۵۴.۱
۷	۸۰	۸۴۹.۷	۶۰.۷	۵۳.۲	۵۴.۲
۸	۸۵	۹۵۴.۲	۵۹.۱	۵۶.۶	۵۷.۷
۹	۹۰	۳.۹×۱۰^{۳}	۵۷	۵۵	۵۶
۱۰	۹۹	۵.۸×۱۰^{۴}	۵۶	۵۵	۵۶

(جدول۳) مقایسه‌ی خطای نرم افزار نهان‌کاوی در سه کانال مختلف از تصویر(ضریب‌کیفیت هفتاد) برای روش نهان‌نگاری مبتنی بر تطبیق بیت کم ارزش. مقادیر P_{FR}، P_{FA}، P_E به ترتیب احتمال انتخاب گنجانه‌ها به‌جای پوشانه، احتمال تشخیص نادرست پوشانه‌ها به‌عنوان گنجانه‌ها و خطای نهایی نرم‌افزار نهان‌کاو هستند. (تعداد تغییرات انجام شده در هر سه کانال مساوی و از رابطه‌ی نه به‌دست آمده است.) کلیه‌ی مقادیر به درصد بیان شده‌اند.

کانال	Y	C_b	C_r
P_{FR}	۳۴	۳۲	۳۱
P_{FA}	۳۳	۳۳	۳۱
P_E	۳۳.۵	۳۲.۵	۳۱

۳-۲- تأثیر ضریب کیفیت

فرض کنید تصویری در اختیار دارید و می‌خواهید در ضرایب DCT آن نهان‌نگاری کنید؛ در این‌جا ضرایب DCT یک بلوک ۸×۸ از تصویر را با ماتریس A نمایش می‌دهیم.

$$A=\{a_{ijk}\} \quad i,j=1,...,8 \quad k=1,...,3 \qquad (۱۰)$$

که در آن k=1 معرف ضرایب مربوط به شدّت روشنایی و k=2,3 ضرایب مربوط به مؤلّفه‌های شدّت رنگ می‌باشند؛ ضرایب قرار گرفته در ماتریس B از مؤلّفه‌های ماتریس A پس از چندی‌سازی و گردکردن آن‌ها حاصل شده است:

$$B=\{b_{ijk}\} \quad i,j=1,...,8 \quad k=1,...,3 \qquad (۱۱)$$

با فرض صرف‌نظر کردن از خطای چندی‌سازی، می‌توان گفت مقادیر ماتریس A برابر است با:

$$A=\{a_{ijk} \simeq b_{ijk}\times S_k(i,j)\} \qquad (۱۲)$$
$$i,j=1,...,8 \quad k=1,...,3$$

که در آن S_k معرف ماتریس چندی‌سازی وابسته به کلید است و از رابطه‌ی شش بدست می‌آید.

با فرض این‌که جاسازی در ضرایب DCT چندی‌شده، انجام گرفته و مقدار هر ضریب پس از جاسازی به اندازه‌ی d تغییر کرده باشد، داریم:

$$b'_{ijk}=b_{ijk}+d \qquad (۱۳)$$

که در آن d یک عدد صحیح است و برای نهان‌نگاری در حالت تغییر بیت کم‌ارزش، مقدار d=± 1 خواهد بود. لذا ماتریس 'A که معرّف ضرایب DCT یک قالب ۸×۸ از تصویر، پس از جاسازی پیام می‌باشد، برابر است با:

$$A'=\{a'_{ijk}=b'_{ijk}\times S_k(i,j)\} \qquad (۱۴)$$

بنابراین می‌توان خطای ناشی از جاسازی در یک قالب ۸×۸ را برابر گرفت با:

$$Diff_k=\sum_{i=1}^{8}\sum_{j=1}^{8}\left|a_{ijk}-a'_{ijk}\right| \quad k=1...3 \qquad (۱۵)$$

با جای‌گذاری روابط ۱۳ و ۱۴ در ۱۵ داریم:

$$Diff_k=\sum_{i=1}^{8}\sum_{j=1}^{8}\left|a_{ijk}-a'_{ijk}\right| \qquad (۱۶)$$
$$=\sum_{i=1}^{8}\sum_{j=1}^{8}\left|b_{ijk}\times S_k(i,j)-(b_{ijk}+d)\times S_k(i,j)\right|$$
$$=\sum_{i=1}^{8}\sum_{j=1}^{8}\left|-d\times S_k(i,j)\right| \quad k=1...3$$

با توجّه به رابطه‌ی ۱۶ اغتشاش ناشی از نهان‌نگاری با d و s_k متناسب است.

که در آن d معرّف تغییرات ناشی از جاسازی است؛ لذا در مواردی که ضریب تغییر نکرده، برابر صفر و در حالت جای‌گذاری در بیت کم ارزش ضرایب، برابر ۱ یا ۱- می‌باشد.

$$Diff_k=\sum_{i=1}^{8}\sum_{j=1}^{8}\left|S_k(i,j)\right| \quad k=1...3 \qquad (۱۷)$$

s_k باتوجّه به رابطه‌ی هفت با ضریب‌کیفیت، رابطه‌ی عکس دارد. به‌عبارت دیگر با افزایش ضریب‌کیفیت اندازه‌ی s_k کاهش پیدا می‌کند؛ از سوی دیگر با ماتریس چندی‌سازی اوّلیه رابطه‌ی مستقیم دارد. لذا می‌توان نتیجه گرفت که در تصاویر با کیفیت بهتر، خطای ناشی از جاسازی، کمتر از تصاویر با کیفیت پایین‌تر است.

از آن‌جایی که ضرایب ماتریس چندی‌ساز در مؤلّفه‌های شدّت رنگ، بزرگتر از مؤلّفه‌های شدّت روشنایی است، لذا نهان‌نگاری در مؤلّفه‌های شدّت رنگ، اعوجاج بیشتری نسبت به مؤلّفه‌های شدّت روشنایی ایجاد می‌کند و این همان چیزی است که در بخش ۳-۱ به آن اشاره شد.

در ادامه، برای سنجش اعوجاج ناشی از جاسازی در این تصاویر، مقادیر PSNR میانگین را برای ده گروه تصویری مختلف در ازای روش نهان‌نگاری مبتنی بر تطبیق بیت کم‌ارزش محاسبه کردیم (جدول ۴).

یادآور می‌شویم، تعداد تغییرات از رابطه‌ی ۱۸ به‌دست می‌آید:

$$NC=\min(cap_i) \quad i=1,...,11 \qquad (۱۸)$$

که در آن cap بیان‌گر حداکثر ظرفیت جاسازی در هر گروه است. از (جدول ۴) می‌توان به همان نتایجی رسید که

به‌صورت ریاضی اثبات شد. با افزایش کیفیت تصویر، اعوجاج ناشی از جاسازی کاهش می‌یابد.

(جدول ۴)مقادیر PSNR میانگین برای ده گروه تصویر نمونه با ضریب کیفیّت‌های متفاوت در ازای تغییرات ثابت و روش نهان‌نگاری تطبیق بیت کم ارزش

گروه‌های تصویر	۱	۲	۳	۴	۵	۶	۷	۸	۹	۱۰
ضریب کیفیت	۲۵	۳۰	۴۵	۵۰	۶۰	۷۰	۸۰	۸۵	۹۰	۹۹
PSNR	۴۴	۳۹	۴۷	۵۰	۵۳	۶۴	۶۶	۶۶	۶۶	۸۸

البته خاطر نشان می‌سازیم که تصاویر با کیفیّت پایین‌تر، خود به‌صورت ذاتی، نوفه‌ای[1] هستند و تشخیص پوشانه و گنجانه از هم در این دسته از تصاویر، توسط نرم‌افزارهای نهان‌کاو مشکل است؛ ولی این مسأله منافاتی با آن‌چه که ما در این بند مطرح کردیم ندارد.

برای نشان دادن تجربی این اثر، خطای نرم افزار نهان‌کاو را در نهان‌نگاری در ده ضریب کیفیت مختلف در (جدول ۵) آورده‌ایم.

۳-۳- تأثیر دوبار فشرده‌سازی

برای توضیح تأثیر دوبار فشرده‌سازی روی هیستوگرام تصویر از تابع یک‌بعدی x(t) بهره می‌گیریم:

$$x(t)=\{t_i\}, i \in N \qquad (۱۹)$$

سیگنال چندی‌شده با پله‌ی a را با $x_a(t)$ را نمایش می‌دهیم:

$$x_a(t)=\left\{t_i'=\left\lfloor\frac{t_i}{a}\right\rfloor\right\}, i \in N \qquad (۲۰)$$

با توجّه به رابطه‌ی بالا مقادیر موجود در بازه‌ی $\left[(at_i+(a-1)),...,(at_i)\right]$ از x(t) روی t_i' در تابع $x_a(t)$ قرار خواهد گرفت؛ لذا اگر هیستوگرام $x(t)$ را با h نمایش دهیم و هیستوگرام $x_a(t)$ را با h' نمایش دهیم داریم:

$$h'(t)=\sum_{k=0}^{a-1} h(at'+k) \qquad (۲۱)$$

$$0<at'+k<256$$

بنابراین در هیستوگرام سیگنال چندی‌شده با پله‌ی a به‌طور دقیق a بین وجود دارد. حال فرض کنید سیگنال $x(t)$ را دوبار با پله‌های b وa چندی نموده‌ایم، بنابراین داریم:

$$x_{ba}(t')=\left\{t_i'=\left\lfloor\left\lfloor\frac{t_i}{a}\right\rfloor\times\frac{a}{b}\right\rfloor\right\} \qquad (۲۲)$$

باتوجّه به این‌که باید مقادیر t_i' مقادیر صحیحی باشند، لذا بایستی داشته باشیم:

$$t_i' \le \left\lfloor\frac{t_i}{a}\right\rfloor\times\frac{a}{b}<t_i'+1 \qquad (۲۳)$$

بنابراین:

$$t_i'\times\frac{b}{a}\le\left\lfloor\frac{t_i}{a}\right\rfloor<(t_i'+1)\times\frac{b}{a} \qquad (۲۴)$$

و از آن‌جا که $\left\lfloor\frac{t_i}{a}\right\rfloor$ هم مقداری صحیح است، با استفاده از تابع ceil می‌توان گفت:

$$\left\lceil t_i'\times\frac{b}{a}\right\rceil\le\left\lfloor\frac{t_i}{a}\right\rfloor<\left\lceil(t_i'+1)\times\frac{b}{a}\right\rceil-1 \qquad (۲۵)$$

بنابراین حدّ پایین هیستوگرام در حالت جدید برابر است با:

$$\left\lfloor\frac{t_{\min}}{a}\right\rfloor=\left\lceil t_i'\times\frac{b}{a}\right\rceil \qquad (۲۶)$$

$$t_{\min}=a\left\lceil t_i'\times\frac{b}{a}\right\rceil$$

t_{max} هم از رابطه‌ی ۲۷ به‌دست می‌آید:

$$t_{\max}=\left(\left(\left\lceil(t_i'+1)\times\frac{b}{a}\right\rceil-1\right)\times a\right)+(a-1) \qquad (۲۷)$$

$$=\left\lceil\frac{b}{a}(t_i'+1)\right\rceil\times a-1$$

و از این‌جا می‌توان نتیجه گرفت که تعداد بین‌های هیستوگرام برای تصاویر دوبار فشرده‌شده برابر است با:

$$n(t)=t_{\max}-t_{\min}+1 \qquad (۲۸)$$

$$=a\left(\left\lceil\frac{b}{a}(t_i+1)\right\rceil-\left\lceil\frac{b}{a}t_i\right\rceil\right)$$

$$n(t)=n(t+kb)$$

توجّه کنید که n(t) یک تابع متناوب با دوره‌ی تناوب b است. که در آن k برابر همه‌ی مقادیر صحیح می‌باشد. بدین‌ترتیب می‌توان نتیجه گرفت که با دوبار فشرده‌سازی یک سیگنال، اغتشاش‌های متناوب در هیستوگرام تصویر دوبار فشرده‌شده، رخ خواهد داد که احتمال آشکارسازی را توسط نرم‌افزارهای نهان‌کاو بالا خواهد برد.

[1] Noise

برای آزمایش گنجانه‌ها، با ضریب کیفیّت متفاوتی از ضریب کیفیّت تصویر ورودی، ذخیره کردیم؛ همان‌گونه که در (جدول ۶) مشاهده می‌کنید با دوبار فشرده‌سازی خطای نرم‌افزار نهان‌کاو بالا می‌رود که بخش عمده‌ای از این خطا ناشی از تشخیص پوشانه‌های دوبار فشرده‌شده به‌عنوان گنجانه است. ولی آن‌چه که حائز اهمیت است این است که در این حالت احتمال این‌که نرم‌افزار نهان‌کاو، تصویر ورودی را به‌عنوان گنجانه انتخاب کند بالا است. لذا برای امنیت بیشتر بهتر است از چنین تصاویری برای جاسازی استفاده نشود.

(جدول ۵) خطای نرم‌افزار نهان‌کاو برای ده گروه تصویر نمونه با ضریب کیفیّت‌های متفاوت. برای دو روش جاسازی R-LSB-M,OutGuess, در نرخ جاسازی ۲۰ و ۸۰. مقادیر P_{FR}، P_{FA}، P_E به ترتیب احتمال انتخاب گنجانه‌ها به‌جای پوشانه، احتمال تشخیص نادرست پوشانه‌ها به‌عنوان گنجانه‌ها و خطای نهایی نرم‌افزار نهان‌کاوهستند. کلیه‌ی مقادیر به درصد بیان شده اند.

گروه تصویر	ضریب کیفیت	OutGuess 20%			OutGuess 80%			Random LSB Matching 20%			Random LSB Matching 80%		
		P_{FR}	P_{FA}	P_E	P_{FR}	P_{FA}	P_E	P_{FR}	P_{FA}	P_E	P_{FR}	P_{FA}	P_E
۱	۲۵	۴۱.۵	۶۱.۵	۵۱.۵	۱۲	۶۱.۵	۳۶.۷۵	۳۷.۵	۶۱.۵	۴۹.۵	۵.۵	۶۱.۵	۳۳.۵
۲	۳۰	۵۲.۵	۴۴.۵	۴۸.۵	۱۵	۴۴.۵	۲۹.۷۵	۴۴	۴۴.۵	۴۴.۲۵	۱۰	۴۴.۵	۲۷.۲۵
۳	۴۵	۴۸.۵	۴۶	۴۷.۲۵	۱۶.۵	۴۶	۳۱.۲۵	۳۸	۴۶	۴۲	۶.۵	۴۶	۲۶.۲۵
۴	۵۰	۱۹.۵	۵۱.۵	۳۵.۵	۴.۵	۵۱.۵	۲۸	۲۲.۵	۵۱.۵	۳۷	۶.۵	۵۱.۵	۲۹
۵	۶۰	۲۴.۵	۵۱.۵	۳۸	۲	۵۱.۵	۲۶.۷۵	۳۰.۵	۵۱.۵	۴۱	۴	۵۱.۵	۲۷.۷۵
۶	۷۰	۲۰.۵	۵۱	۳۵.۷۵	۴.۵	۵۱	۲۷.۷۵	۲۲.۵	۵۱	۳۶.۷۵	۴.۵	۵۱	۲۷.۷۵
۷	۸۰	۱۴.۵	۴۲	۲۸.۲۵	۱.۵	۴۲	۲۱.۷۵	۳۱.۵	۴۲	۳۶.۷۵	۲	۴۲	۲۲
۸	۸۵	۱۹.۵	۴۰.۵	۳۰	۲	۴۰.۵	۲۱.۲۵	۲۲.۵	۴۰.۵	۳۱.۵	۳.۵	۴۰.۵	۲۲
۹	۹۰	۱۹.۵	۳۱.۵	۲۵.۵	۰	۳۱.۵	۱۵.۷۵	۳۸	۳۱.۵	۳۴.۷۵	۰	۳۱.۵	۱۵.۷۵
۱۰	۹۹	۱۶.۵	۴۸	۳۲.۲۵	۰	۴۸	۲۴	۲۳	۴۸	۳۵.۵	۰.۵	۴۸	۲۴.۲۵

(جدول ۶) خطای نرم‌افزار تحلیل تحت تأثیر دوبار فشرده‌سازی در چهار ظرفیت جاسازی متفاوت؛ که در آن $\frac{QF_{out}}{QF_{in}}$ نسبت ضریب کیفیّت تصویر تولیدی به تصویر اولیه است. مقادیر P_{FR}، P_{FA}، P_E به‌ترتیب احتمال انتخاب گنجانه‌ها به جای پوشانه، احتمال تشخیص نادرست پوشانه‌ها به‌عنوان گنجانه‌ها و خطای نهایی نرم‌افزار نهان‌کاو هستند. کلیه‌ی مقادیر به درصد بیان شده‌اند.

ظرفیت جاسازی	٪۱۰			٪۲۰			٪۳۰			٪۸۰		
$\frac{QF_{out}}{QF_{in}}$	P_{FR}	P_{FA}	P_E	P_{FR}	P_{FA}	P_E	P_{FR}	P_{FA}	P_E	P_{FR}	P_{FA}	P_E
$\frac{20}{70}$	۷.۶	۹۰	۴۸.۸	۵.۸	۹۰	۴۷.۹	–	۹۰	–	۲.۹	۹۰	۴۶.۴
$\frac{30}{70}$	۶	۹۱	۴۸.۵	۶	۹۱	۴۸.۵	–	۹۱	–	۳.۵	۹۱	۴۷.۲
$\frac{50}{70}$	۰.۷	۹۹	۴۹.۵	–	۹۹	–	۰.۷	۹۹	۴۹.۸	۰.۲	۹۹	۴۹.۶
$\frac{60}{70}$	۰.۳	۹۹	۴۹.۶	–	۹۹	–	۰.۲	۹۹	۴۹.۶	۰.۰۹	۹۹	۴۹.۵
$\frac{70}{70}$	۲۷	۳۳	۳۰	۱۵	۳۳	۲۲.۵	۵	۳۳	۱۹	۰.۰۹	۳۳	۱۶.۵۴
$\frac{80}{70}$	۰.۰۹	۹۹	۴۹.۵	–	۹۹	–	۰	۹۹	۴۹.۵	۰	۹۹	۴۹.۵
$\frac{99}{70}$	۰	۱۰۰	۵۰	–	۱۰۰	–	۰	۱۰۰	۵۰	۰	۱۰۰	۵۰

۳-۴- تأثیر بافت

در سیستم‌های نهان‌نگاری سیگنال پیام قبل از جاسازی، ابتدا فشرده و سپس رمز می‌شوند. چنین داده‌هایی شبیه به رشته‌ای از بیت‌ها هستند که دارای توزیع دوجمله‌ای با P=۰/۵ می‌باشند. درواقع می‌توان گفت که سیگنال پیام شبیه به یک نوفه‌ی تصادفی است. بهترین مکان برای جاسازی این نوفه‌ی تصادفی، مناطقی از تصویر است که خود طبیعتی نوفه‌مانند و به‌طور کامل تصادفی داشته باشند، با نهان‌نگاری در چنین مناطقی می‌توان گفت که تغییر محسوسی در تصویر ایجاد نخواهد شد.

نتایج آزمایش‌های انجام شده، نشان می‌دهند ضرایب DCT، در قالب‌هایی از تصویر که حاوی لبه‌های تیز هستند و هم‌چنین قالب‌های یکنواخت (نواحی با گرادیان کم)، خیلی تصادفی نیست. به عبارت دیگر همبستگی بین ضرایب موجود در این قالب‌ها قابل توجّه است.

این اثر در (جدول ۷) نشان داده شده است. بدین منظور سه گروه تصویر را در نظر گرفته‌ایم، گروه (الف) حامل تصاویر یکنواخت، گروه (ب) تصاویر شلوغ با لبه‌های تیز و مشخص، و گروه (ج) حاوی تصاویر شلوغ با طبیعت نوفه‌ای هستند؛ سپس مقادیر DCT آن‌ها را محاسبه کرده و در ادامه آنتروپی ضرایب DCT هر تصویر را که معرّف میزان تصادفی بودن آن‌ها است، به‌دست آورده‌ایم. همان‌گونه که مشاهده می‌کنید میزان تصادفی بودن مقادیر DCT در گروه (ج) از سایر گروه‌ها بیشتر است؛ لذا به‌نظر می‌رسد که بهترین مناطق برای نهان‌نگاری در تصویر، مناطق شلوغ تصویر با طبیعت نوفه‌ای و تصادفی است. چراکه نهان‌نگاری در تصاویر گروه (الف) و (ب) باعث از بین رفتن همبستگی بین ضرایب DCT می‌شود و درواقع اثر نهان‌نگاری مشهود خواهد شد. به‌عبارت‌دیگر نرم‌افزارهای نهان‌کاوی می‌توانند این گروه از تصاویر نهان‌نگار را با دقّت بالاتری آشکار کنند. به‌منظور آزمایش هم تعداد ششصد تصویر (یک‌صد تصویر پوشانه و یک‌صد گنجانه از هر گروه) را انتخاب کرده و خطای تشخیص نرم‌افزار نهان‌کاو را در (جدول ۸) آورده‌ایم. ملاحظه می‌کنید امکان رخداد خطا توسط نرم‌افزار نهان‌کاو در گروه (ج) از دو گروه دیگر بیشتر است و این مطابق با انتظار ما است.

(جدول۷) مقادیر آنتروپی ضرایب سه گروه تصویر(گروه (الف) حامل تصاویر یکنواخت گروه (ب) تصاویر شلوغ با لبه‌های تیز و مشخص و گروه (ج) حاوی تصاویر شلوغ با طبیعت نوفه‌ای هستند)

ج	ب	الف	گروه‌های تصویری
۶	۴	۲	آنتروپی میانگین ضرایب DCT

(جدول ۸) خطای نرم‌افزار نهان‌کاو برای نهان‌نگاری با نرخ جاسازی ۲۰٪، روش جاسازی تطبیق بیت کم‌ارزش، مقادیر P_{FR} ، P_{FA} ، P_E به‌ترتیب احتمال انتخاب گنجانه‌ها به‌جای پوشانه، احتمال تشخیص نادرست پوشانه‌ها به‌عنوان گنجانه‌ها و خطای نهایی نرم‌افزار نهان‌کاو هستند. کلیهٔ مقادیر به درصد بیان شده‌اند.

گروه‌های تصویری	P_{FR}	P_{FA}	P_E
گروه الف	۵.۵	۳۱.۵	۱۸.۵
گروه ب	۳.۵	۴۰	۲۱.۷۵
گروه ج	۰.۵	۶۱.۵	۳۱

۳-۵- تأثیر فرکانس مکانی

در این زیربخش، قصد داریم تأثیر فرکانس مکانی را روی امنیت بررسی کنیم. به‌عبارت دیگر به‌دنبال پاسخ این سؤال هستیم که آیا استفاده از ضرایب در برخی از باندهای فرکانسی، امنیت روش جاسازی را بالا می‌برد؟ همان‌گونه که می‌دانید ضرایب DCT چندی‌شده جزء یکی از سه گروه زیر است:

۱- ضرایب DC، ۲- ضرایب AC برابر با صفر، ۳- ضرایب AC مخالف صفر

ضرایب DC معرف میانگین روشنایی هر قالب باشد، لذا تغییر آن‌ها باعث اعوجاج بصری در تصویر می‌شود. بیش‌تر ضرایب AC برابر صفر در فرکانس‌های میانی یا بالا قرار دارند؛ لذا تغییر آن‌ها ساختار پیوسته‌ی صفرها را به هم خواهد زد و خود دلیلی بر وجود بیت پنهانی در تصویر است. امّا بیش‌تر ضرایب AC را غیر صفر در فرکانس‌های پایین و میانی رخ می دهند؛ حال سؤال این است که آیا آشفتگی آن‌ها تأثیر قابل توجهی روی تصویر خواهدگذاشت؟

با توجّه به جدول چندی‌سازیِ تصاویر JPEG، ضرایب فرکانس پایین با پله‌ی چندی‌ساز کوچک‌تری نسبت به ضرایب با فرکانس بالا چندی می‌شوند. لذا نهان‌نگاری در آن‌ها اعوجاج کمتری را ایجاد خواهد نمود این اثر از رابطه‌ی ۱۶ هم حاصل می‌شود که در آن خطای بین گنجانه و پوشانه را به‌دست‌آورده‌ایم، در این حالت در شرایطی که $S_i \geq S'_i$ باشد می‌توان نتیجه گرفت که $D_i \geq D'_i$ است؛ به‌عبارت‌دیگر نهان‌نگاری در ضرایب فرکانس بالا که در آن‌ها درایه‌ی ماتریس چندی‌سازی بزرگ‌تر است؛ خطای بیشتری نسبت به نهان‌نگاری در ضرایب فرکانس پایین و میانی ایجاد می‌کند.

(جدول۹) خطای نرم‌افزار نهان‌کاو، در دو حالت نهان‌نگاری به روش تطبیق بیت کم ارزش در کل تصویر و نهان‌نگاری در زیر باندهای فرکانس پایین تعداد تغییرات انجام شده در هر دو حالت یکسان است، مقادیر P_{FR} ، P_{FA} ، P_E به‌ترتیب احتمال انتخاب گنجانه‌ها به جای پوشانه، احتمال تشخیص نادرست پوشانه‌ها به‌عنوان گنجانه‌ها و خطای نهایی نرم‌افزار نهان‌کاو هستند. نتایج در ده ظرفیت متفاوت گزارش شده است.

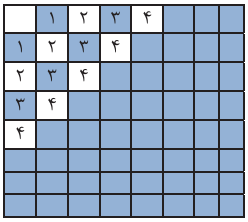
روش جاسازی	LSBFlipping نهان نگاری در زیر باند ۱-۳			LSBFlipping نهان نگاری معمولی به صورت تصادفی در کل تصویر			LSBMatching نهان نگاری در زیر باند ۱-۳			LSBMatching نهان نگاری معمولی به صورت تصادفی در کل تصویر		
ظرفیت جاسازی	P_{FR}	P_{FA}	P_E	P_{FR}	P_{FA}	P_E	P_{FR}	P_{FA}	P_E	P_{FR}	P_{FA}	P_E
۱۰	۳۳	۶۶	۴۹.۵	۲۷	۶۶	۴۶.۵	۳۳	۶۶	۴۹.۵	۱۳	۶۶	۳۹.۵
۲۰	۳۳	۶۶	۴۹.۵	۲۴	۶۶	۴۵	۳۳	۶۶	۴۹.۵	۱۳	۶۶	۳۹.۵
۳۰	۳۳	۶۶	۴۹.۵	۲۴	۶۶	۴۵	۳۳	۶۶	۴۹.۵	۱۳	۶۶	۳۹.۵
۴۰	۳۳	۶۶	۴۹.۵	۲۴	۶۶	۴۵	۳۷	۶۶	۵۱.۵	۱۳	۶۶	۳۹.۵
۵۰	۳۳	۶۶	۴۹.۵	۲۴	۶۶	۴۵	۳۳	۶۶	۴۹.۵	۱۲	۶۶	۳۹
۶۰	۳۳	۶۶	۴۹.۵	۲۴	۶۶	۴۵	۳۲	۶۶	۴۹.۵	۱۳	۶۶	۳۹.۵
۷۰	۳۳	۶۶	۴۹.۵	۲۴	۶۶	۴۵	۳۳	۶۶	۴۹.۵	۱۲	۶۶	۳۹
۸۰	۳۳	۶۶	۴۹.۵	۲۴	۶۶	۴۵	۳۳	۶۶	۴۹.۵	۱۲	۶۶	۳۹
۹۰	۳۳	۶۶	۴۹.۵	۲۴	۶۶	۴۵	۳۷	۶۶	۵۱.۵	۱۲	۶۶	۳۹
۱۰۰	۳۳	۶۶	۴۹.۵	۲۴	۶۶	۴۵	۳۳	۶۶	۴۹.۵	۱۲	۶۶	۳۹

با هدف آشکار شدن این اثر، در یک آزمایش از تصاویر گروه شش با ضریب کیفیت هفتاد استفاده کرده‌ایم و در آن‌ها یک‌بار نهان‌نگاری به روش تطبیق کم‌ارزش در سه باند فرکانس مکانی ۱-۳ (شکل۱) و یک‌بار دیگر در کل تصویر انجام شده است.

مقدار PSNR میانگین در حالت طبیعی۶۳ و در حالتی که از سه باند فرکانس پایین استفاده کرده‌ایم ۶۵ است و این مسأله مطابق با انتظار ما است.

میزان خطای نرم‌افزار نهان‌کاو در ظرفیت‌های مختلف برای حالتی که از باندهای فرکانسی خاصّی استفاده می‌شود در مقایسه با نهان‌نگاری به‌صورت تصادفی در کل تصویر برای تصاویر مذکور در (جدول ۹) آورده شده است.

لازم به ذکر است که میزان تغییرات در هر دو حالت برابر است و از رابطه‌ی ۲۹ به‌دست می‌آید:



(شکل ۱) ضرایب با فرکانس‌های مکانی مثل هم در یک بلوک DCT

$$cap = cap(SF_{1-3}) \times Payload_{in} \qquad (۲۹)$$

که در آن $cap(SF_{1-3})$ معرف حداکثر ظرفیت جاسازی در باندهای فرکانسی ۱-۳ است.

همان‌گونه که انتظار داشتیم، خطای نرم‌افزار نهان‌کاو در حالت انتخاب باندهای فرکانسی پایین‌تر بیشتر از حالتی است که نهان‌نگاری به‌صورت تصادفی در کلّ تصویر انجام می‌شود، لذا انتخاب هوشمندانه‌ی ضرایب جاسازی با توجّه به فرکانس مکانی آن در افزایش امنیت مؤثّر است.

۴- الگوریتم‌های نهان‌نگاری در JPEG

با توجّه به ساختار این فرمت که در بخش دوم به آن اشاره شد، فضاهای خاصّی برای جاسازی اطّلاعات در تصویر JPEG وجود دارد. همان‌طور که پیش از این آورده‌ایم، ما روش‌های نهان‌نگاری در JPEG را در سه گروه اصلی تقسیم‌بندی نموده‌ایم؛ در این بخش قصد داریم مروری بر روش‌های موجود نهان‌نگاری در JPEG داشته باشیم و آن‌ها را از جنبه‌های مختلف دسته‌بندی کنیم لذا در ابتدا روش‌های نهان‌نگاری را در JPEG که بر اساس ویژگی‌های ساختار فایل

ایجاد شده‌اند، مورد بررسی و تحلیل قرار می‌دهیم؛ در ادامه، روش‌های نهان‌نگاری در ضرایب DCT را شرح خواهیم داد؛ سپس در مورد روش‌های نهان‌نگاری در حوزه‌ی متفاوت، ولی مقاوم به فشرده‌سازی JPEG توضیحاتی را ارائه خواهیم کرد.

۴-۱- نهان‌نگاری در JPEG با استفاده از ویژگی‌های ساختار فایل

در این روش‌ها که به‌طور معمول روش‌های ساده و ناامنی هستند، نهان‌نگاری در بخش‌هایی از فایل صورت می‌گیرد که با توجّه به ساختار این فرمت ایجاد شده است.

الف-نهان‌نگاری در فراداده[1]

یک راه برای نهان‌نگاری در تصویر JPEG، قراردادن اطّلاعات در مکان‌های مربوط به فراداده است. فراداده درواقع اطّلاعاتی است که در مورد یک محصول خاص داده می‌شود و شامل نکاتی درباره‌ی تصویر و دوربین عکاسی می‌باشد *(وانگ۲۰۰۴،ص۷۶-۸۲)*؛ به‌عنوان مثال در مورد دوربین‌های عکاسی یک سری اطّلاعات الحاقی[2] شامل مدل دوربین، زمان ایجاد عکس، وضوح تصویر و... به سرآیند فایل اضافه می‌شود.

ب-اضافه‌کردن پیام به انتهای فایل

روش دیگر برای نهان‌نگاری اضافه‌کردن اطّلاعات به انتهای فایل JPEG است؛ در این حالت پیام در انتهای فایل تصویر JPEG بعد از برچسب EOI (که شاخص انتهایی تصویر است.) اضافه می‌شود. از آن‌جا که طول مربوط به فایل اصلی در سرآمد ثبت شده است، مشکلی در بازکردن تصویر مذکور نخواهیم داشت. در ادامه، روش ساده‌ای را برای اضافه‌کردن اطّلاعات به انتهای فایل JPEG در محیط ویندوز می‌آوریم:

۱- فایل پنهانی و فایل تصویر ورودی با فرمت JPEG را انتخاب کنید.

۲- برای راحتی کار بهتر است هر دو فایل را در یک مسیر به‌عنوان مثال درایو C قرار دهید.

۳- Command Prompt را از مسیر Start - All Programs - Accessories - Command Prompt انتخاب کنید.

۴- در پنجره‌ی Dos برای آن‌که به درایو C دسترسی پیدا کنید، عبارت "cd \" را تایپ کنید.

۵- حال کافی است عبارت "copy /B original.JPEG + secretfiles.zip new.JPEG", را تایپ نمایید.

که در آن original.JPEG پوشانه‌ی ورودی، secretfiles.zip پیام مورد نظر و new.JPEG گنجانه می‌باشد؛ B/ معرف باینری‌کردن است.

طی این فرآیند درواقع پیام پنهانی در مد دودویی[3] را به انتهای فایل JPEG اضافه می‌کنیم، لذا اندازه‌ی فایل بعد از جاسازی زیاد می‌شود. هنگامی که تصویر JPEG را باز می‌کنیم؛ طول داده‌ی مربوط به تصویر از سرآمد فایل تصویر خوانده می‌شود و پیام پنهانی که به انتهای آن اضافه شده نادیده گرفته می‌شود. بازیابی پیام در این روش بسیار ساده است؛ کافی است قالب گنجانه را به نوع پیام تبدیل کنید تا پیام مورد نظر را بازیابی نمایید. به‌عنوان مثال اگر نوع پیام zip است، کافی است فرمت گنجانه را به zip تغییر دهید، حال به‌راحتی به پیام موردنظر می‌رسید.

روشن است که روش‌های این گروه، نه تنها هیستوگرام تصویر را تغییر نمی‌دهند، بلکه تأثیر مشاهده‌ای هم روی تصویر به جا نخواهند گذاشت؛ ولی به‌هرحال روش‌های ناامنی به حساب می‌آیند و با یک بررسی ساده می‌توان گنجانه‌ها را از پوشانه‌ها متمایز کرد.

برخی از نرم‌افزارهای نهان‌نگاری مثل Comuflag، Jpegx، Data Stash از این شیوه بهره می‌برند. البتّه نرم‌افزارهایی چون Sarc و Stegosui قادر به تحلیل چنین روش‌هایی هستند[4].

۴-۲- نهان‌نگاری در ضرایب DCT قالب‌ها ۸×۸

بیشتر روش‌های نهان‌نگاری در تصاویر JPEG با استاندارد آن تطابق یافته‌اند؛ یعنی پوشانه ابتدا به قالب‌های ۸×۸ تقسیم می‌شود و تبدیل DCT روی هر قالب اعمال شده و فرآیند فشرده‌سازی روی آن انجام می‌شود؛ سپس نهان‌نگاری به‌طور معمول با دستکاری ضرایب DCT قالب‌های ۸×۸ صورت می‌گیرد *(لی۲۰۰۳، لی۲۰۰۶، رانگرانگ۲۰۰۶، سنگ۲۰۰۴، وانگ۲۰۰۱، المحمد۲۰۰۸، چانگ۲۰۰۲)*. روش‌های موجود در این گروه را از دیدگاه‌های مختلفی می‌توان طبقه‌بندی نمود.

یک دیدگاه برای دسته‌بندی این روش‌ها، راهکار جاسازی به‌کارگرفته‌شده در آن است؛ بر این اساس، روش‌های نهان‌نگاری را می‌توان به دو دسته‌ی روش‌های

[1] Metadate
[2] Extended file information(EXIF)
[3] Binary
[4] آدرس اینترنتی نرم‌افزارهای مذکور در انتهای مقاله ذکر شده است.

مبتنی بر تغییر بیت‌های کم‌ارزش و روش‌های مبتنی بر چندی‌سازی طبقه‌بندی نمود.

۴-۲-۱-روش‌های مبتنی بر تغییر بیت کم‌ارزش

به‌طور معمول برای جاسازی در ضرایب DCT از روش‌های مبتنی بر تغییر بیت‌های کم‌ارزش استفاده می‌شود؛ دو گروه عمده از این روش‌ها، روش‌های مبتنی بر جاسازی بیت کم‌ارزش (LSB-F[1]) و روش‌های تطبیق بیت کم‌ارزش (LSB-M[2]) هستند.

الف- روش‌های مبتنی بر جایگزینی بیت کم‌ارزش

در روش LSB-F، تنها کم‌ارزش‌ترین بیت هر ضریب تغییر می‌کند؛ به‌عبارت دیگر در این روش، کم‌ارزش‌ترین بیت ضرایب DCT پوشانه با بیت‌های پیام، بازنویسی می‌شوند؛ البته روش‌های مطرح شده در این گروه را می‌توان به دو دسته روش‌های جاسازی ترتیبی و تصادفی دسته‌بندی نمود.

ب- روش‌های جاسازی ترتیبی

در روش‌های جاسازی ترتیبی، انتخاب ضرایب از ابتدای تصویر و به‌صورت ترتیبی و پشت سرهم انجام می‌شود. اوّلین روشی که بر این اساس معرّفی شد، روش Jsteg *(درک اوقام ۲۰۰۲)* است در این روش ضرایب DCT (به‌جز ۱و۰و۱-) استفاده می‌شود *(پرووس۲۰۰۳، ص۳۲-۴۴)*. با افزایش نسبت فشرده‌سازی تعداد ضرایب (۱و۰و۱-) افزایش می‌یابد و درنتیجه ظرفیت نهان‌نگاری کم می‌شود *(سنگ۲۰۰۴، ص۱۲-۱۷)*. این روش نسبت به حمله‌های مشاهده‌ای مصون است، ولی به‌راحتی می‌توان آن را آشکار کرد و از آن‌جا که الگوریتم نیازی به رمز مشترک ندارد، درنتیجه هر شخصی که سیستم نهان‌نگاری را بشناسد، می‌تواند پیام پنهان‌شده به این روش را استخراج کند. البته نسخه‌های بهبود یافته‌ای از این روش هم وجود دارد به‌طور مثال در *(چانگ۲۰۰۲،ص۱۲۳-۱۳۸)* برای بالابردن ظرفیّت نهان‌نگاری و تولید تصاویر گنجانه، با کیفیت بهتر، روشی براساس Jsteg ارائه شده است. از دیگر روش‌های این گروه می‌توان به روش *(لی ۲۰۰۷)* اشاره کرد که از ایده‌ی مطرح شده توسط *(وانگ۲۰۰۴)* الهام گرفته شده‌است؛ آن‌ها با اعمال تغییراتی روی جدول چندی‌سازی ظرفیت، جاسازی روش Jsteg را افزایش داده‌اند و برای بهبود کیفیت گنجانه از ضرایب فرکانس میانی، برای جاسازی استفاده می‌کنند؛ به‌عبارت دیگر پیام تنها در ۳۶ ضریب موجود از یک قالب ۸×۸ پنهان می‌شود.

ج- روش‌های جاسازی تصادفی

در روش‌های جاسازی تصادفی، انتخاب ضرایب به‌صورت تصادفی و براساس یک کلید انجام می‌شود.

اوّلین روشی که بر این اساس معرفی شد، روش OutGuess 0.1 *(نیلز پرووس ۲۰۰۳)* است. که در آن ضرایب DCT چندی‌شده، به‌صورت شبه‌تصادفی (با استفاده از یک کلید) انتخاب می‌شوند. درادامه، بیت‌های LSB آن‌ها با بیت‌های پیام جایگزین خواهند شد؛ در این روش بدون داشتن کلید یا کلمه‌ی عبور نمی‌توان پیام پنهانی را استخراج کرد. از دیگر روش‌های جاسازی مبتنی بر جایگزینی بیت‌های پیام در کم‌ارزش‌ترین بیت ضرایب، می‌توان به روش‌های مطرح شده توسط *(سالی۲۰۰۴و۲۰۰۵)*، *(پونی۲۰۰۸)*، *(اسچاپ۲۰۰۳)* و *(ایگرز۲۰۰۲)* اشاره نمود.

(ساتیش۲۰۰۴، ص۵۷۸-۵۹۰) در مورد تحلیل آن دسته از الگوریتم‌های نهان‌نگاری که از بیت‌های کم‌ارزش پیکسل‌های تصویر به‌صورت پشت سرهم برای جاسازی استفاده می‌کنند، با استفاده از آزمایش $\chi 2$ روش دقیقی ارائه کرده است که براساس به‌وجود آمدن جفت‌رنگ‌هایی که تعداد رخداد آن‌ها در تصویر برابر است، عمل می‌کند. جاگذاری در بیت کم‌ارزش باعث نرم شدن فرکانس عناصر یک زوج مقدار نسبت به یکدیگر می‌شود؛ بنابراین هنگامی که پیام مخفی شده به‌اندازه‌ی کافی بزرگ باشد، جاسازی بیت‌های پیام با توزیع یکنواخت، تفاوت فراوانی بین رنگ‌های همسایه را در هیستوگرام، کاهش می‌دهد و از این واقعیت که به‌طور آماری توزیع زوج مقدارها یکسان می‌شود در حمله استفاده می‌کنند؛ این حمله بر مبنای همین تغییرات، وجودِ داده‌ی مخفی را تشخیص می‌دهد. البته درصورتی‌که از تمام ظرفیت تصویر استفاده نشود و داده‌ها به‌صورت شبه‌تصادفی در تصویر پراکنده باشند، کارآیی این روش کاهش می‌یابد. *(پرووس۲۰۰۱)* ادعا می‌کند که می‌توان این روش را برای وقتی که داده‌ها به‌صورت تصادفی در تصویر قرار می‌گیرند، اصلاح کرد.

ب- روش‌های مبتنی بر تطبیق بیت کم‌ارزش[3]

در روش تطبیق بیت کم‌ارزش نیز هدف یکسان کردن LSB ضرایب، با بیت‌های پیام است؛ اما ممکن است برای رسیدن

[1] LSB Flipping (LSB_F)
[2] LSB Matching (LSB-M)
[3] LSB-M

به این هدف چند بیت از ضریب تغییر یابد؛ درواقع در این جا دیگر الزامِ تغییرِ حداکثر یک بیت از ضریب، وجود ندارد. امّا باید به این نکته نیز توجّه شود که این تغییرات تا جایی مجاز است که تأثیرات قابل مشاهده‌ای روی تصویر ایجاد نکنند. در این روش در صورت تطابق بیت داده با بیت کم‌ارزش ضریب، تغییری در ضریب ایجاد نمی‌شود؛ درصورت عدم تطابق، مقدار ضریب به‌صورت تصادفی کاهش یا افزایش می‌یابد؛ به‌همین دلیل این روش با عنوان روش جاسازی ۱± نیز شناخته می‌شود *(وستفلد۲۰۰۲)*.

البته در این روش‌ها نیز جاسازی می‌تواند به‌صورت ترتیبی یا تصادفی انجام شود. ازجمله روش‌های مبتنی بر تطبیق LSB می‌توان به (میلیکانین۲۰۰۶، ص۲۸۵-۲۸۷، لی۲۰۰۶، ص۱۰۰۵۰-۱۰۰۵۳، لی۲۰۰۸، فرانز۲۰۰۲) اشاره نمود.

با توجّه به این‌که روش LSB-M از ایجاد POV[1] در هیستوگرام جلوگیری می‌کند؛ در برابر حملات مربوط به روش‌های جایگزینی LSB مقاوم است. در مورد تحلیل روش‌های LSB-M نیز حملاتی مطرح‌شده است؛ امّا هیچ‌کدام از آن‌ها به‌طور کامل موفّق نبوده‌اند *(مارول۱۹۹۸،ص۴۸-۶۱، فردریک۲۰۰۳،ص۱۹۱-۲۰۲)*.

۴-۲-۲- روش‌های مبتنی بر چندی سازی

در این دسته از روش‌ها، جاسازی اطّلاعات با چندی‌سازی ضرایب انجام می‌شود *(ایگرز۲۰۰۲،ص۲۶-۳۷ - چِن۲۰۰۱، ص۱۴۲۳-۱۴۴۳)*. به‌طور مثال در روش ارائه شده توسط ایگرز از دو چندی‌ساز برای جاسازی در ضرایب استفاده می‌شود؛ یکی برای جاسازی بیت‌هایی از پیام که برابر صفر هستند و دیگری برای جاسازی بیت‌هایی از پیام که برابر یک هستند.

۴-۲-۳- روش‌های انطباقی

روش‌های انطباقی درواقع روش‌هایی هستند که به‌منظور خاصّی طراحی شده‌اند. این دسته از روش‌ها به‌طور معمول خود را با ویژگی‌های ساختار JPEG تطبیق داده‌اند.

ازجمله‌ی این روش‌ها، روش‌های مبتنی بر مدل می‌باشند *(لی۲۰۰۰،ص۲۸۸-۲۹۴، راسی۲۰۰۹، التركی۲۰۰۱، ص۲۲۸-۲۳۳)*. در این الگوریتم‌ها ویژگی‌های آماری تصویر مدل می‌شود و طی فرآیند جاسازی حفظ خواهند شد. به‌عنوان مثال *(سالی۲۰۰۴)* در روش MB1، برای مدل کردن ضرایب AC از تابع توزیع عمومی Cauchy[2] استفاده می‌کند؛ بدین ترتیب ضرایب تصویر به دو بخش کلی (اجزایی که تغییر آن تأثیر کمی روی تصویر دارند (LSB) و اجزایی که تغییر آن تأثیر فاحشی روی تصویر دارد (MSB)) تقسیم می‌شوند و درنهایت بیت‌های پیام جایگزین بیت‌های LSB می‌شود. *(بوهم۲۰۰۴)* روشی برای شکستن این الگوریتم مطرح کرده است. سالی برای بهبود روش خود روش نهان‌نگاری MB2 را مطرح کرد که در آن اثر قالبی‌شدن هم حفظ شده است؛ البته این روش هم در *(الریک۲۰۰۸،ص۱۲۷-۱۴۲)* تحلیل شده است. در همین اواخر روش PSB با هدف بهبود روش‌های مبتنی بر مدل، به کمک مدلی بهتر و انتخاب دقیق‌تر ضرایب جاسازی پیشنهاد شده است؛ این روش در واقع ترکیبی از روش F5 *(وستفلد۲۰۰۱،ص۲۸۹-۳۰۲)* و روش‌های مبتنی بر مدل می‌باشد.

از دیگر روش‌های این گروه می‌توان به آن دسته از روش‌های نهان‌نگاری اشاره کرد که در آن‌ها تغییرات ناشی از نهان‌نگاری را با نوفه‌ای گوسی وکم‌دامنه که ممکن است در اثر عوامل مختلف (مثل نوفه‌ی حاصل از دستگاه تصویربرداری) به‌طور طبیعی در تصویر وجود داشته باشد، مدل می‌کنند، و بدین ترتیب سعی می‌کنند امنیت را افزایش دهند؛ چرا که برای تحلیل‌کننده، تشخیص این‌که نوفه‌ی ایجاد شده حاصل از نهان‌نگاری یا توسط دستگاه تصویر برداری است، مشکل می‌باشد. ازجمله‌ی این روش‌ها می‌توان روش‌های *(فرانز۲۰۰۵، ص۱۸۹-۲۰۳، مارول۱۹۹۸، ص۴۸-۶۱، فردریک۲۰۰۳،ص۱۹۱-۲۰۲)* را بیان کرد؛ البته بایستی خاطر نشان کنیم که روش تحلیل *(هارمسن۲۰۰۳)* قادر است این الگوریتم‌ها را تحلیل کند. چراکه اساس روش هارمسن بر این فرض بنا نهاده شده که اثر نوفه‌ی جمع شونده‌ی مستقل، بر روی هیستوگرام تصویر به‌صورت فیلتر پایین‌گذر است؛ لذا هیستوگرام گنجانه، نرم‌تر از پوشانه است و بدین‌ترتیب طبقه‌بندی‌کننده به‌راحتی می‌تواند بین تصویر گنجانه و پوشانه تمایز برقرار کند.

مهم‌ترین هدف یک سیستم نهان‌نگاری، امنیت یا عدم‌آشکارشدن آن است که در صورت آشکارشدن، هدف نهان‌نگاری نقض می‌شود. لذا در یک دسته‌بندی دیگر می‌توان روش‌ها را بر اساس این‌که از چه راهکاری برای افزایش امنیت استفاده کرده‌اند، طبقه‌بندی کرد.

[1] Pair Of Values

[2] Generalized Cauchy distribution

۴-۲-۴- روش‌های مبتنی بر اصلاح مشخصات آماری تصویر

روش‌های نهان‌نگاری در بیت‌های کم‌ارزش، جزء ساده‌ترین روش‌ها می‌باشند و ظرفیّت زیادی را برای جاسازی ایجاد می‌کنند؛ به‌طوری که در مواردی، بدون آن‌که چشم متوجّه جاسازی شود، می‌توان تا ۵۵٪ حجم فایل تصویر را با داده پر کرد *(سنگ۲۰۰۴،ص۱۲-۱۷)*.

عیب عمده‌ی این روش‌ها این است که به‌طور معمول مشخصات آماری تصویر را به‌هم‌می‌زنند و بدین ترتیب در برابر تحلیل‌های آماری بسیار شکننده هستند. به‌عنوان مثال *(وینر۲۰۰۰)* نشان‌داده است که ضرایب DCT توزیع زنگی شکل دارند که با نهان‌نگاری به روش Jsteg این توزیع به‌هم‌می‌خورد. لذا برخی از محققان روش‌های مبتنی بر بازسازی آماری را مطرح کرده‌اند که در تعدادی از آن‌ها از تعریف کچین *(کچین ۱۹۹۸)* برای بالا بردن امنیت استفاده شده است *(رانگرانگ۲۰۰۶،ص۳۶۵-۳۶۸)*. و درواقع تلاش می‌کنند که اطّلاعات را در تصویر، به‌گونه‌ای پنهان کنند که مشخّصات آماری تصویر قبل و بعد جاسازی مشابه هم باشد *(ایگرز۲۰۰۲، ص۲۶-۳۷، سولانکی۲۰۰۶، نود۲۰۰۵، سالی۲۰۰۴، ص۱۵۴-۱۶۷، سالی۲۰۰۵، ص۱۶۷-۱۹۰، پرووس۲۰۰۱، ص۱-۱۱)*.

پرووس*(پرووس ۲۰۰۱)* جزء اوّلین کسانی بود که ایده‌ی خنثی‌کردن تغییرات هیستوگرام را ارائه کرد. او به‌جای آن‌که از تمام ظرفیت تصویر برای نهان‌نگاری استفاده کند، از نصف ظرفیت برای نهان‌نگاری و از نصف دیگر آن برای تصحیح هیستوگرام استفاده کرده است؛ البتّه در این روش ظرفیت نهان‌نگاری در تصویر کاهش چشم‌گیری می‌یابد. *(ایگر و همکارانش در سال۲۰۰۲)* روش دیگری را برای نهان‌نگاری با حفظ مشخصات آماری با روابط ریاضی پیشرفته ارائه کردند که به HPDM[1] مشهور است (برند گایرود، دانشگاه استنفورد). *(فرانز و همکارانش در سال۲۰۰۲)* سعی کردند پیام را با توزیع تصویر، مدل کنند. برخی دیگر از محققان درصدد آن بوده‌اند که K-Ldivergence را کمینه کنند *(سولانکی۲۰۰۶، گیلون۲۰۰۲، مولین۲۰۰۴، سولانکی۲۰۰۵، سولانکی۲۰۰۶،ص ۱۲۱-۱۲۴)*.

گروه دیگر اساس کار خود را مبتنی بر اصلاح مشخصات آماری مرتبه‌ی دوم ضرایب DCT قرار داده‌اند؛ به‌عنوان مثال *(سرکار و همکارانش در سال ۲۰۰۷)*، روشی را مبتنی بر اصلاح مشخصات آماری مرتبه‌ی دوم ضرایب DCT ارائه کردند *(سرکار۲۰۰۷،ص۲۷۷-۲۸۰)*. عدّه‌ای نیز در تلاش بوده‌اند که تغییرات ناشی از جاسازی را به‌گونه‌ای اعمال کنند که توزیع گنجانه تا حدّ امکان مشابه با پوشانه باشد؛ ازجمله‌ی این روش‌ها می‌توان به روش PQ فردریک *(فردریک ۲۰۰۶،ص۱۰۲-۱۱۰، فردریک۲۰۰۴، ص۴-۱۵)*، روش‌های مبتنی بر مدل که در آن‌ها نه تنها هیستوگرام مرتبه‌ی اوّل کلّ ضرایب DCT اصلاح می‌شود، بلکه هیستوگرام زیربانده‌ای DCT نیز اصلاح می‌شود، یا روش‌های مبتنی بر مدولاسیون اتّفاقی[2] *(فردریک۲۰۰۲، ص۱۹۱-۲۰۲، فردریک۲۰۰۳، ص۱۹۱-۲۰۲)* اشاره کرد.

نقطه‌ضعف اصلی روش‌های مبتنی بر اصلاح مشخّصات آماری این است که:

ایده‌ی بازسازی آماری، تنها زمانی مفید خواهد بود که امکان بازسازی همه‌ی آماره‌های اساسی تصویر وجود داشته باشد و حفظ هیستوگرام ضرایب DCT در کلّ تصویر به‌تنهایی کافی نیست؛ چراکه وابستگی بین ضرایب یک قالب و هم‌چنین بین قالب‌های مختلف بسیار پیچیده است؛ از سوی دیگر اصلاح هیستوگرام، خود می‌تواند وابستگی‌هایی ایجاد کند که امکان آشکارسازی را افزایش دهد *(پونی۲۰۰۷،ص۳-۴، یون.کیو.شی۲۰۰۶)*؛ علاوه‌بر این بازسازی آماری بازده جاسازی را در برخی از روش‌ها پایین می‌آورد؛ از سوی دیگر در روش‌هایی که ضرایب را با توزیع خاصّی مدل می‌کنند این سؤال مطرح است که این تخمین تا چه حد با توزیع اصلی مطابقت دارد *(بوهم۲۰۰۴،ص۱۲۵-۱۴۰، الریک۲۰۰۸، ص۱۲۷-۱۴۲)*.

۴-۲-۵-روش‌های مبتنی بر کاهش اعوجاج ناشی از جاسازی

این گروه شامل روش‌هایی هستند که به‌دنبال کاهش اعوجاج ناشی از جاسازی می‌باشند (فردریک۲۰۰۶،ص۲-۱۰، کیم۲۰۰۶)؛ البتّه راه‌کارهای مختلفی می‌توان بدین منظور ارائه کرد *(کودوفسکی۲۰۰۸،ص۳-۱۴)*.

یکی از این راه‌کارها کاهش تعداد تغییرات ناشی از جاسازی می‌باشد. به‌عنوان مثال در برخی از الگوریتم‌ها از روش‌های مبتنی بر کدگذاری برای کاهش تغییرات ناشی از جاسازی استفاده می‌کنند؛ ازجمله مهم‌ترین این روش‌ها

[1] Histogram-preserving data mapping

[2] Stochastic modulation

می‌توان به روش F5 اشاره کرد که در آن وستفلد *(وستفلد۲۰۰۱)*، از ایده‌ی ماتریس کدگذاری مطرح‌شده توسط کراندل *(کراندل۱۹۹۸)*، بهره گرفته است؛ در این روش طی فرآیند جاسازی، مقدار ضریب DCT مورد نظر تنها یک واحد کاهش می‌یابد و جاسازی در ضریب غیر صفر انجام می‌شود. در این روش، چنان‌چه حین جاسازی، یک ضریب صفر شود (که این اتّفاق تنها در مورد ضرایب با مقادیر ۱ و ۱- خواهد افتاد) مقدار صفر رها می‌شود (پدیده‌ی انقباض)، و بیت پیام مورد نظر دوباره پنهان می‌گردد؛ البتّه بایستی یادآور شویم که پدیده‌ی انقباض، تأثیر منفی روی هیستوگرام ضرایب DCT خواهد داشت و درواقع روشی که تکنیک F5 با آن شکسته شده از همین اثر منفی آن روی هیستوگرام ضرایب DCT کمک گرفته است *(فردریک۲۰۰۳، ص۳۱۰-۳۲۲)*. با هدف رفع مشکلات F5 بهبودهایی روی آن انجام گرفت *(فردریک۲۰۰۶، کیم۲۰۰۶، فردریک۲۰۰۷، کودوفسکی۲۰۰۸)*، افراد بسیاری با هدف کاهش اعوجاج از روش‌های جاسازی مبتنی بر کدگذاری استفاده کرده‌اند؛ به‌عنوان مثال *(کیم در سال ۲۰۰۶)* به‌منظور کاهش اعوجاج ناشی از جاسازی، تغییراتی بر روی روش تغییر ضرایب در ماتریس جاسازی داده است تا اعوجاج ناشی از جاسازی کمینه گردد. در روش ارائه شده در *(فردریک۲۰۰۶،ص۱۰۲-۱۱۰، فردریک۲۰۰۴، ص۴-۱۵، فردریک۲۰۰۷،ص۲۰-۲۱)* از روش کدگذاری Wetpaper استفاده شده است که با استفاده از آن، علاوه‌بر این‌که اعوجاج ناشی از جاسازی کاهش می‌یابد، بازده‌ی جاسازی هم افزایش می‌یابد. *(ویلیامز و همکارانش درسال ۲۰۰۵)* از کدهای همینگ و کد گولوی سه تایی[1] استفاده کرده‌اند *(ویلیامز۲۰۰۵،ص۱۲۰۹-۱۲۱۴)*. *(زنگ و همکارانش در سال۲۰۰۶)* و *(فردریک و همکارانش در سال۲۰۰۷)* به‌طور مستقل روش جاسازی مبتنی بر کدهای همینگ سه تایی را ارائه کرده‌اند *(زنگ۲۰۰۶،ص۷۸۱-۷۸۳، فردریک۲۰۰۷، ص۱۵۴۷-۱۵۴۹)*. *(میلیکانین و همکارانش درسال ۲۰۰۶)* ایده‌ی کدگذاری بسیار ساده‌ای را ارائه کردند؛ که امکان پنهان‌کردن دو بیت پیام در دو ضریب با یک تغییر را فراهم آورده است. *(وانگ و همکارانش در سال‌های ۲۰۰۷ و ۲۰۰۸)* روشی را مبتنی بر ماتریس جاسازی بازگشتی ترکیبی HRME[2] ارائه کردند *(وانگ۲۰۰۷، ص۱۵۵-۱۶۰، وانگ۲۰۰۸)*. اگر چه برخی از این روش‌ها برای تصاویر با فرمت‌های دیگر مطرح شده است، امّا همه‌ی آن‌ها در فرمت JPEG هم قابل استفاده است. درمجموع می‌توان گفت که استفاده از الگوریتم‌های مرتبط با ایده‌ی کدگذاری، بازده‌ی جاسازی و امنیت الگوریتم نهان‌نگاری را افزایش می دهد. در *(بیربراور۲۰۰۸،ص۱-۲۲)* نشان داده شده است که عملکرد کدهای غیرخطی در نهان‌نگاری نسبت به کدهای خطی بهتر است.

در مواردی دیگر طی یک فرآیند تکراری تلاش می‌کنند تا اعوجاج ناشی از جاسازی را با بهینه‌سازی یک تابع برازندگی کاهش دهند؛ گروهی به‌منظور تحقق این آرمان از الگوریتم ژنتیک بهره برده‌اند؛ میلانی فرد و همکارانش در *(میلانی فرد۲۰۰۶،ص۲۲-۲۳)* روشی را برای بهبود روش OutGuess با استفاده از الگوریتم ژنتیک ارائه کردند، *(لیفنگ و همکارانش در سال۲۰۰۹)* از ویژگی قالبی‌شدن در تصویر به هنگام جاسازی استفاده کرده‌اند و تابع برازندگی مبتنی بر این اثر را بهینه می‌کنند و بدین ترتیب نحوه‌ی تغییر ضرایب را تعیین‌می‌کنند *(لیفنگ۲۰۰۹،ص۳۹۳-۴۰۰)*. البتّه این واقعیّت وجود دارد که با نهان‌نگاری اثر قالبی‌شدن افزایش می‌یابد؛ زیرا نهان‌نگاری و تغییر ضرایب DCT نوعی گسستگی (یا عدم همبستگی) بین بلوک‌های مجاور ایجاد می‌کند؛ ولی نکته اینجاست که خود فرآیند فشرده‌سازی JPEG هم این‌اثر را ایجاد می‌کند که در تصاویر با ضریب‌کیفیت پایین این اثر مشهودتر است؛ لذا تمایز برقرار کردن بین آن دو مشکل می‌باشد.

در *(کودوفسکی۲۰۰۸،ص۱-۱۳)* عوامل مؤثّر بر امنیت در نهان‌نگاری در تصاویر JPEG مثل الگوریتم جاسازی، اثر فرکانس‌های مکانی، بافت تصویر و... مورد بررسی قرار گرفته شده است. در برخی از تحقیقات برای بالابردن امنیت، محدودیت‌هایی را روی پارامترهای تعیین کننده قرار می‌دهند *(فردریک۲۰۰۵،ص۶۷-۸۱، ساکای۲۰۰۸، امیرالزمان ۲۰۰۸)*.

۴-۲-۶-روش‌های مقاوم در برابر حملات خاص

از زمانی که روش‌های نهان‌نگاری مطرح شد و به‌دنبال آن الگوریتم‌های نهان‌کاوی ارائه گردید، همواره یک رقابت بین آن دو وجود دارد. بسیاری از روش‌ها با ایده‌ی مقاوم‌بودن در برابر حملات خاص شکل‌گرفته‌اند؛ به‌عنوان مثال می‌توان از روش F3 یاد کرد که جای خود را به F4 داد و سپس درنهایت F5 ارائه شد *(ساتیش۲۰۰۴،ص۵۸۷-۵۹۰، وانگ۲۰۰۲،ص۸۱-۸۴)*. از نمونه‌های دیگر این گروه می‌توان

[1] Ternary Hamming and Golay codes
[2] Hybrid Recursive Matrix Encoding

به روش OutGuess اشاره کرد که برای مقابله با نقاط ضعف Jsteg مطرح شده است یا روش LSB-GEA *(هوانگ ۲۰۰۷)* که با هدف شکست حمله‌ی X2 ارائه شده است.

۴-۲-۷- روش‌های بی اتلاف

در برخی از کاربردها مثل کاربردهای قضایی، پزشکی و نظامی، علاوه‌بر پیام، بازیابی پوشانه با استفاده از گنجانه اهمّیت زیادی دارد. روش‌هایی را که بدین طریق عمل می‌کنند، روش‌های بی‌اتلاف[1]، برگشت‌پذیر[2]، بدون خطا[3] یا معکوس‌پذیر[4] می‌گویند *(لی ۱۹۹۸، ص ۹۶۷-۹۸۱)*.

از جمله‌ی این روش‌ها می‌توان به روش‌های *(وو۲۰۰۹، ص۱۹۶۶-۱۹۷۳، بارتن۱۹۹۷، فردریک۲۰۰۱، ص۲۲۳-۲۲۷)* اشاره کرد. بارتن (۱۹۹۷) اوّلین کسی بود که الگوریتمی بی‌اتلاف به‌منظور نشانه‌گذاری[5] در رسانه‌های دیجیتال شامل تصاویر JPEG و کدهای MPEG ارائه کرد. در سال ۲۰۰۱ فردریک و همکارانش دو روش بی‌اتلاف برای نهان‌نگاری در تصاویر JPEG ارائه کردند: روش اوّل مبتنی بر فشرده‌سازی بی‌اتلاف، رشته‌بیت‌های به‌دست آمده از ضرایب DCT چندی‌شده است؛ و روش دوم ماتریس چندی‌سازی را تغییر می‌دهد تا به یک روش فشرده‌سازی بی‌اتلاف برسد. *(چنگ و همکارانش در سال ۲۰۰۹)* روشی بی‌اتلاف را برای نهان‌نگاری در ضرایب DCT چندی شده ارائه نمودند.

در یک دسته‌بندی دیگر روش‌های نهان‌نگاری در JPEGرا می‌توان به دو گروه روش‌های نهان‌نگاری در ضرایب DCT چندی‌شده و چندی‌نشده تقسیم نمود.

۴-۲-۸-نهان‌نگاری در ضرایب چندی‌شده

در روش‌هایی که از ضرایب DCT چندی‌شده برای نهان‌نگاری استفاده می‌شود، به‌طور معمول تصاویر ورودی از نوع JPEG هستند. اوّلین روشی که برای جاسازی داده در تصاویر JPEG ارائه شد، براساس جاسازی اطّلاعات در ضرایب DCT چندی‌شده عمل می‌کرد؛ در این روش از همه‌ی ۶۴ ضریب DCT موجود در یک قالب برای جاسازی تنها یک بیت پیام استفاده می‌شد؛ بنابراین ظرفیت نهان‌نگاری در آن بسیار پایین بود به‌طور مثال برای یک تصویر ۲۵۶×۲۵۶ تایی تنها امکان جاسازی ۴۰۹۶ بیت وجود داشت *(کوبایاشی۱۹۹۹، ص۱۴۶۹-۱۴۷۶، نوگاچی۲۰۰۰، ص۵۷۷-۵۸۰)*. مارول *(مارول ۲۰۰۰)* روشی مبتنی بر میانگین را برای جاسازی یک بیت در یک قالب ۸×۸ ضرایب DCT چندی‌شده شده ارائه کرد. روش‌های دیگری چون *(ژاکوبسن۲۰۰۲، سولانکی۲۰۰۳، سولانکی۲۰۰۲)* در این حوزه قرار می‌گیرند.

۴-۳-نهان‌نگاری در حین فرآیند فشرده‌سازی

در برخی از روش‌ها حین فرآیند جاسازی، تصویر فشرده‌نشده‌ی اوّلیه مورد نیاز است و فرآیند جاسازی حین فشرده‌سازی انجام می‌شود؛ به‌طور معمول از اطّلاعات اضافی حاصله برای بالا بردن امنیت و کاهش اثرات ناشی از جاسازی استفاده می‌کنند؛ ازجمله‌ی این روش‌ها می‌توان به روش PQ اشاره کرد که توسط *(فردریک و همکارانش در سال‌های ۲۰۰۴ و۲۰۰۷)* ارائه شده است و در برابر برخی از روش‌های تحلیل، مقاوم است *(خرازی۲۰۰۵،ص۱۷-۲۰)*. البتّه در *(گل۲۰۰۷،ص۲۰۵-۲۰۸)* روشی برای تحلیل PQ ارائه شده است.

۴-۴- نهان‌نگاری در حوزه‌ی متفاوت

در این روش‌ها ابتدا جاسازی اطّلاعات در یک حوزه‌ی دیگر (مثل حوزه‌ی مکان یا حوزه‌ی تبدیل) به‌گونه‌ای مقاوم در برابر فشرده‌سازی JPEG انجام می‌شود؛ چراکه فشرده‌سازی در تصویر، اعوجاج‌هایی ایجاد می‌کند که می‌توانند به پیام آسیب برسانند، درنهایت گنجانه فشرده می‌شود *(فردریک۲۰۰۵، ص۶۷-۸۱، سولانکی۲۰۰۷، لی۲۰۰۶،ص۱۰۰۵۰-۱۰۰۵۳)*.

در مورد روش‌های نهان‌نگاری در حوزه‌ی مکان (پیکسل‌های تصویر)، *(فردریک در سال۲۰۰۱)* نشان داده که پیام پنهان شده در فضای پیکسلی یک تصویر که در قبل به فرمت JPEG بوده، حتی اگر به کوچکی یک بیت باشد، قابل کشف است. این کار با انجام آزمایش سازگاری JPEG برای هر قالب ۸×۸ صورت می‌گیرد؛ لذا روش‌های نهان‌نگاری در حوزه‌ی مکان مورد توجه نیستند و روش‌های نهان‌نگاری در حوزه‌های دیگر مثل حوزه‌ی تبدیل، مورد توجّه قرار می‌گیرند.

یکی از نکاتی که باعث می‌شود سیستم‌های نهان‌کاوی بتوانند وجود پیام پنهانی را در یک تصویر آشکار

[1] Lossless
[2] Reversible
[3] Distortion-free
[4] Invertible
[5] Authentication

کنند، همبستگی بین ضرایب مجاور تبدیل کسینوسی گسسته است و این‌که در طیف فرکانسی تصاویر طبیعی، بیشتر انرژی در فرکانس‌های پایین متمرکز است. یک راه‌حل برای غلبه بر این مسأله، اضافه‌کردن نوفه به تصویر در فضای مکانی و سپس بردن تصویر به حوزه‌ی تبدیل و جاسازی بیت‌ها در ضرایب حوزه‌ی تبدیل است *(الترکی۲۰۰۱،ص۲۲۸-۲۳۳)*.

از دیگر روش‌های مطرح شده با این ویژگی، روش YASS *(سولانکی۲۰۰۷و۲۰۰۸)* است. در اکثر روش‌هایی که از حوزه‌ی تبدیل برای جاسازی استفاده می‌کنند، نوعی قالب‌بندی وجود دارد. درصورتی‌که این قالب‌بندی برای حمله‌کننده مشخص باشد، حمله‌کننده می‌تواند به بسیاری از خواص آماری قالب، دسترسی پیدا کند و از آن‌ها برای اجرای حمله‌ای موفق استفاده کند؛ درواقع یکی از دلایل موفّقیت روش‌های حمله به جاسازی در حوزه‌ی فرکانس، وجود قالب‌های هم‌اندازه و منظّم می‌باشد. لذا در این دسته از روش‌ها ابتدا تصویر با قالب‌های $m\times n$ که در آن‌ها $m>8,n>8$ می‌باشد قالب‌بندی می‌شود؛ آن‌گاه قالب ۸×۸ به شکل تصادفی در قسمتی از قالب بزرگ‌تر انتخاب شده و سپس روی آن تبدیل DCT اعمال می‌شود و سپس فرآیند جاسازی ادامه می‌یابد. با توجّه به آن‌که تصویر گنجانه بعد از جاسازی پیام وارد فرآیند فشرده‌سازی می‌شود، مشخّصات آماری گنجانه حاصل با ویژگی‌های آماری تصویر طبیعی مطابقت دارد. لذا این الگوریتم در مقابل روش‌های تحلیل عمومی که به‌نوعی بر ویژگی‌های درجه‌بندی یا ویژگی‌هایی مبتنی بر نوفه تکیه دارند، به‌طور کامل مقاوم است *(کودوفسکی ۲۰۰۸، ص۱-۱۸)*؛ با این وجود در *(CCITT،۱۹۹۲)* روشی خاصّی، به‌منظور تحلیل این الگوریتم ارائه شده است.

از دیگر روش‌های نهان‌نگاری در حوزه‌ی DCT که نسبت به فشرده‌سازی JPEG مقاوم است، می‌توان به روش‌های معرّفی شده توسط لانگلار *(لانگلار۲۰۰۰)* و هرناندز *(هرناندز۲۰۰۰)* اشاره نمود.

برخی از روش‌ها از حوزه‌ی موجک برای نهان‌نگاری استفاده می‌کنند و در این حوزه، روش جاسازی مقاومی نسبت به فشرده‌سازی JPEG ارائه کرده‌اند *(میروالد۲۰۰۱، اینووه۱۹۹۸، چی۱۹۹۸، سالی۲۰۰۴)*؛ که البتّه تحلیل این روش‌ها، با الگوریتم‌های مطرح شده توسط فرید امکان‌پذیر است *(فرید۲۰۰۲،ص۹۰۵-۹۰۸)*.

(دولیزچاور و همکارانش در سال ۲۰۰۳) روش نهان‌نگاری بی‌اتلاف مبتنی بر تئوری Patchwork را که نسبت به فشرده‌سازی JPEG مقاوم است، بیان کردند که درواقع تنها روش نهان‌نگاری بی‌اتلافِ مقاوم، نسبت به فشرده‌سازی JPEG است *(لو۲۰۰۵)*.

به‌طورکلی اگرچه در این دسته از روش‌ها به‌دلیل عبور تصویر گنجانه از فرآیند فشرده‌سازی، تصویر گنجانه‌ی نهایی، مشخّصات آماری مشابه با پوشانه دارد؛ ولی خاطر نشان می‌سازیم که برای بازگشت‌پذیر بودن آن بایستی پیام را با روش مقاوم نسبت به فشرده‌سازی پنهان نمود؛ که همین امر خود می‌تواند باعث تجمّع خطا در تصویر شود و امنیت را کاهش دهد.

(جدول۱۰) لیست نرم‌افزارهای نهان‌نگاری در تصاویر JPEG که منبع اصلی آن‌ها در اختیار نیست.

نام نرم‌افزار	فرمتهای پشتیبان	نرم‌افزار نهان‌کاو
Crypto123	JPEG,BMP	-
IBM DLS	PNG،BMP, GIF, JPEG,	-
Invisible Secrets	JPEG	StegSpy
Info Stego	JPEG, GIF,BMP	-
Syscop	JPEG	-
StegMark	JPEG,GIF,BMP,PNG,TGA,TIF	-
JPEGx	JPEG	StegSpy
DCT-Steg	JPEG	-
EikonAmark	JPEG	-
AppendX	JPEG, GIF,PNG	Stegdetect

(جدول۱۱) فهرست نرم‌افزارهای نهان‌نگاری در تصاویر JPEG که منبع اصلی آن‌ها در اختیار است.

نام نرم‌افزار	نویسنده	فرمت	جاسازی	رمزنگاری	تحلیل
Camera Shy	_	JPEG,	LSB	_	_
F5	AndreasWestfeld	JPEG,GIF,BMP	LSB	_	Fridrich'sAlgorithm,Stegdetect
JP Hide and Seek	_	JPEG,	_	_	StegSpy
Jsteg JPEG	Derek Upham	JPEG,	LSB	_	X^2t,Stegdetect-Fridrich'sAlgorithm
OutGuess v.0.13b	Provos,Honeyman	JPEG,	LSB	RC4	X2 (ev),Stegdetect,StegBreak
OutGuess v.0.2b	Provos,Honeyman	JPEG,	LSB	RC4	-Fridrich's Algorithm
Steghide	_	JPEG, BMP,WAV			_
JSteg-Shell	John Korejwa	JPEG,	LSB	RC4	X^2 –test,StegBreak
JPhide	AllanLatham	JPEG,		Blowfish	Stegdetect,X^2,StegBreak

۴-۵- نرم‌افزارهای نهان‌نگاری در JPEG

با توجّه به کاربردی بودن فرمت JPEG، تعداد نرم‌افزارهای نهان‌نگاری و نهان‌کاوی که قابلیت کار با این فرمت را دارند زیاد است. برخی از مقالات مشخّصات نرم‌افزارهای نهان‌نگاری در رسانه‌های مختلف را جمع‌آوری نموده‌اند *(حیاتی۲۰۰۶)*. در این قسمت برخی از نرم‌افزارهای موجود را که قادر به نهان‌نگاری در تصاویر با فرمت JPEG هستند معرّفی می‌کنیم.

به‌طورکلی نرم‌افزارهای موجود را می‌توان به دو گروه نرم‌افزارهایی که منبع اصلی[1] آن‌ها در اختیار است و نرم‌افزارهایی که منبع اصلی آن‌ها در اختیار نیست، طبقه‌بندی نمود.

در مورد روش‌هایی که منبع اصلی آن‌ها در اختیار نیست؛ ارزیابی بر اساس فرمت‌هایی که پشتیبانی می‌کنند و هم‌چنین نرم‌افزارهای که می‌توانند این روش‌ها را تحلیل کنند؛ انجام شده است. فهرست این نرم‌افزارها در (جدول ۱۰) آورده شده است[2]. برخی از این نرم‌افزارها در هنگام نوشتن این مقاله در دسترس بودند، یعنی امکان دسترسی به آن‌ها و سایت آن‌ها وجود داشت و البتّه برخی از آن‌ها مثل DCT-Steg، EikonAmark ، AppendX در اختیار نبودند.

در مورد روش‌هایی که منبع اصلی آن‌ها در اختیار است[3]، ارزیابی و مقایسه بر اساس نکات زیر انجام شده است:

۱- فرمت‌هایی که علاوه‌بر JPEG پشتیبانی می‌کنند.

۲- روشی که برای جاسازی استفاده شده است.

۳- نوع رمزنگاری پیام.

۴- روش‌هایی که می‌توان با آن تصاویر گنجانه‌ی تولید شده را تحلیل کرد.

فهرست این روش‌ها در (جدول ۱۱) آمده است.

۴-۶- پیاده‌سازی برخی از روش‌ها

به‌منظور ارزش‌یابی و ارزیابی روش‌های نهان‌نگاری، در نرم‌افزار Stegotest برخی از الگوریتم‌های نهان‌نگاری چون جای‌گذاری ترتیبی در کم‌ارزش‌ترین بیت ضرایب DCT (S-LSB-F)، جای‌گذاری تصادفی در کم‌ارزش‌ترین بیت ضرایب DCT (R-LSB-F)، جایگذاری‌های مبتنی بر مدل MB1 و MB2، روش F5، روش تطبیق کم‌ارزش‌ترین بیت به شکل ترتیبی S-LSB-M و نیز روش تطبیق کم‌ارزش‌ترین بیت به شکل تصادفی R-LSB-M پیاده‌سازی شده‌اند.

در (شکل‌های ۲ تا ۵) مقادیر PSNR صد تصویر گنجانه در چهار ضریب‌کیفیت (۴۵، ۷۰، ۸۵، ۹۹) برای روش‌های مطرح شده، آورده شده است.

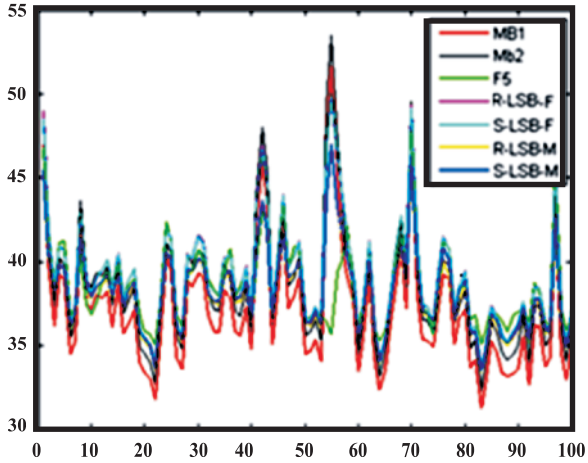
در (جدول ۱۲)، PSNR میانگین را برای دسته تصویرهای گنجانه در چهار ضریب‌کیفیت (۴۵، ۷۰، ۸۵، ۹۹) که از روش‌های نهان‌نگاری فوق در نرخ جاسازی ۱۰۰ تولید شده‌اند، آورده‌ایم.

در (جدول ۱۳) خطای نرم‌افزار نهان‌کاو برای چند روش مختلف برای تصاویر با ضریب‌کیفیت هفتاد نشان‌داده‌شده است.

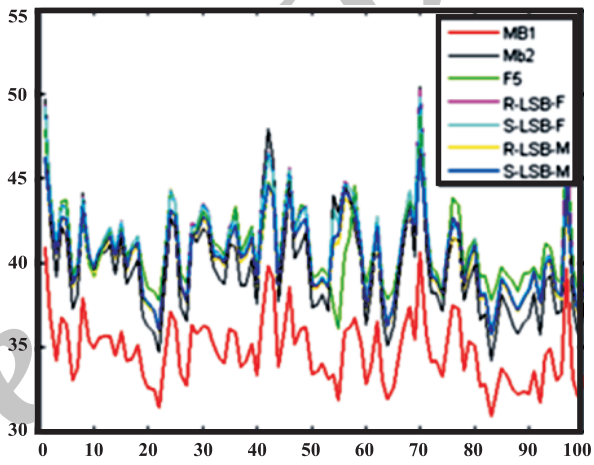
[1] Source

[2] آدرس اینترنتی نرم‌افزارهای مذکور در انتهای مقاله ذکر شده است.

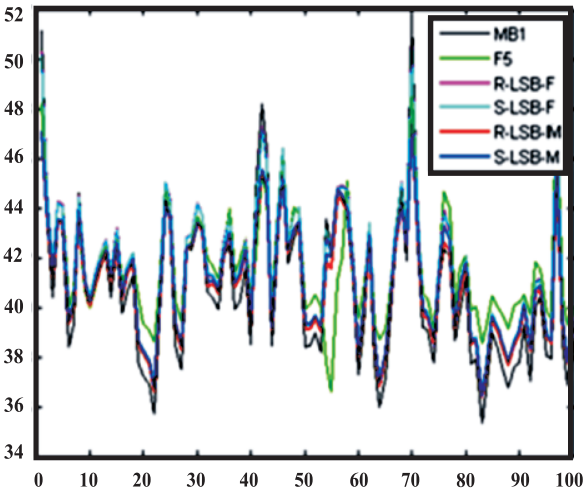
[3] آدرس اینترنتی نرم‌افزارهای مذکور در انتهای مقاله ذکر شده است.



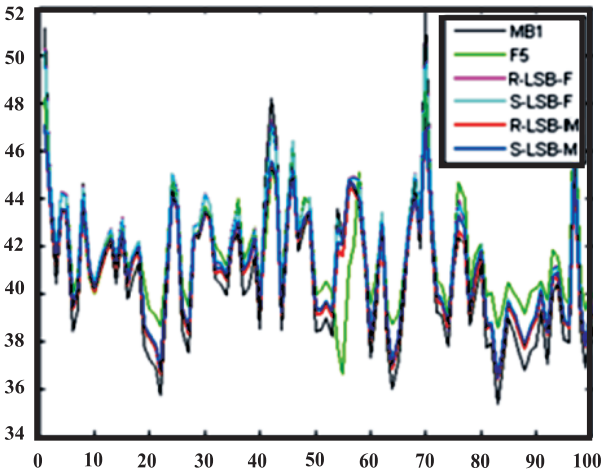
(شکل ۲) مقادیر PSNR برای صد تصویر با ضریب کیفیت ۴۵ و هفت روش جاسازی مختلف (منحنی افقی، شماره‌ی تصویر و منحنی عمودی مقادیر PSNR)



(شکل ۳) مقادیر PSNR برای صد تصویر با ضریب کیفیت ۷۰، و هفت روش جاسازی مختلف (منحنی افقی، شماره‌ی تصویر و منحنی عمودی مقادیر PSNR)



(شکل ۴) مقادیر PSNR برای صد تصویر با ضریب کیفیت ۸۵، و شش روش جاسازی مختلف (منحنی افقی، شماره‌ی تصویر و منحنی عمودی مقادیر PSNR)



(شکل ۵) مقادیر PSNR برای صد تصویر با ضریب کیفیت ۹۹ و شش روش جاسازی مختلف (منحنی افقی، شماره‌ی تصویر و منحنی عمودی مقادیر PSNR)

(جدول۱۲) PSNR میانگین برای هفت روش نهان‌نگاری (جای‌گذاری ترتیبی در LSB (S-LSB-F)، جای‌گذاری تصادفی در LSB (R-LSB-F)، تطبیق LSB به شکل ترتیبی S-LSB-M، تطبیق LSB به شکل تصادفی R-LSB-M ، جای‌گذاری‌های مبتنی بر مدل MB1 و MB2، روشF5) در نرخ جاسازی ۱۰۰ برای تصاویر ورودی با ضریب‌کیفیت‌های (۴۵، ۷۰، ۸۵، ۹۹)

QF Method	۴۵	۷۰	۸۵	۹۹
S-LSB-F	۳۹.۰۷	۴۰.۸۱	۴۱.۴۵	۴۵.۱۲
R-LSB-F	۳۹.۰۵	۴۰.۷۷	۴۱.۴۳	۴۵.۰۹
S-LSB-M	۳۸.۲۸	۴۰.۴	۴۱.۱۱	۴۵.۰۶
R-LSB-M	۳۸.۱۴	۴۰.۲۴	۴۰.۹۶	۴۴.۹۳
MB1	۳۸.۳۹	۳۹.۷۲	۴۰.۷۴	۴۳.۶۴
MB2	۳۷.۱۵	۳۴.۷۸	–	–
F5	۳۸.۵۳	۴۰.۹۲	۴۱.۵۸	۴۴.۸۶

۵- بحث و نتیجه‌گیری

بررسی و ارزیابی الگوریتم‌های نهان‌نگاری به‌شناسایی هر چه بهتر مزایا و معایب روش‌ها، ارائه‌ی حمله‌های موفّق و به‌علاوه پیشنهاد روش‌های نهان‌نگاری مقاوم‌تر منجر می‌شود.

در این مقاله با مطالعه و بررسی ساختار فرمت JPEG عوامل و ویژگی‌های مؤثّر در امنیت را که وابسته به پوشانه است، استخراج کرده و اثر هر یک را به‌صورت ریاضی و تجربی مورد تحلیل و ارزیابی قرار داده‌ایم؛ و بدین ترتیب راهکارهای عمومی برای افزایش امنیت در روش‌های نهان‌نگاری در JPEG را با توجّه به پوشانه معرّفی کردیم. سپس بازنگری جامعی برروی روش‌های نهان‌نگاری در این فرمت انجام شد و آن‌ها را در سه دسته: ۱-روش‌های نهان‌نگاری در JPEG با استفاده از ویژگی‌هایی ساختار فایل، ۲-روش‌های نهان‌نگاری در ضرایب DCT، ۳-روش‌های نهان‌نگاری حین فرآیند فشرده‌سازی، دسته‌بندی کرده‌ایم؛ و در هر گروه هم بسته به عواملی چون امنیت، کاربرد و... طبقه‌بندی‌های مختلفی انجام دادیم. هم‌چنین به‌منظور تحلیل و ارزیابی، الگوریتم‌های نهان‌نگاری موجود، نرم‌افزار Stegotest را طراحی کرده و برخی از الگوریتم‌ها را در قالب آن پیاده سازی کردیم. درادامه‌ی این تحقیق می‌توان سایر ویژگی‌های مؤثّر در امنیت سیستم‌های نهان‌نگاری در JPEG را مثل اثر تابع جاسازی، پیام و کلید را شناسایی کرد و بدین ترتیب به ارزیابی و تحلیل دقیق‌تر روش‌های یاد شده و نرم‌افزارهای معرّفی شده پرداخت.

(جدول ۱۳) خطای نرم‌افزار نهان‌کاو برای شش روش نهان‌نگاری (جای‌گذاری ترتیبی در LSB ضرایب DCT (S-LSB-F)، جای‌گذاری تصادفی در LSB ضرایب DCT (R-LSB-F)، جای‌گذاری مبتنی بر مدل MB1، روشF5، تطبیق LSB به شکل ترتیبی S-LSB-M و نیز تطبیق LSB به شکل تصادفی R-LSB-M) در۱۰ نرخ جاسازی برای تصاویر ورودی با ضریب کیفیت ۷۰. مقادیر P_{FR}، P_{FA}، P_E به ترتیب احتمال انتخاب گنجانه‌ها به جای پوشانه، احتمال تشخیص نادرست پوشانه‌ها به‌عنوان گنجانه‌ها و خطای نهایی نرم‌افزار نهان‌کاو هستند. نتایج در ۱۰ ظرفیت متفاوت گزارش شده است.

نرخ جاسازی	cover	F5		MB1		R-LSB-M		S-LSB-M		R-LSB-F		S-LSB-F	
	P_{FA}	P_{FR}	P_E	P_{FR}	P_E	P_{FR}	P_E	P_{FR}	P_E	P_{FR}	P_E	P_{FR}	P_E
۱۰	۳۳	-	-	-	-	۲۸	۳۰.۵	۲۵	۲۹	۲۷	۳۰	۲۴	۲۸.۵
۲۰	۳۳	۶۳.۳	۴۸.۱	۶۸.۶	۵۰.۸	۱۳	۲۳	۱۰	۲۱.۵	۱۵	۲۴	۱۱	۲۲
۳۰	۳۳	-	-	-	-	۳	۱۸	۱	۱۷	۵	۱۹	۳	۱۸
۴۰	۳۳	۵۸.۰۲	۴۵.۵	۶۹.۳	۵۱.۱	۱	۱۷	۰.۴	۱۶.۷	۲	۱۷.۵	۰.۹	۱۶.۹
۵۰	۳۳	-	-	-	-	۰.۶	۱۶.۸	۰.۳	۱۶.۶۵	۰.۹	۱۶.۹	۰.۳	۱۶.۶
۶۰	۳۳	۵۴.۰۶	۴۳.۵	۶۷.۸	۵۰.۴	۰.۵	۱۶.۷۵	۰.۳	۱۶.۶۵	۰.۲	۱۶.۶	۰.۳	۱۶.۶
۷۰	۳۳	-	-	-	-	۰.۲	۱۶.۶	۰.۴	۱۶.۷	۰.۲	۱۶.۶	۰.۲	۱۶.۶
۸۰	۳۳	۵۲.۴	۴۲.۷	۶۸.۸	۵۰.۹	۰.۱	۱۶.۵۵	۰.۱	۱۶.۵۵	۰.۲	۱۶.۶	۰.۰۹	۱۶.۵
۹۰	۳۳	-	-	-	-	۰.۲	۱۶.۶	۰.۱	۱۶.۵۵	۰.۰۹	۱۶.۵	۰.۲	۱۶.۶
۱۰۰	۳۳	۵۲.۲	۴۸.۱	۶۹.۱	۵۱.۰۵	۰.۲	۱۶.۶	۰.۰۹	۱۶.۵	۰.۱	۱۶.۵	۰.۳	۱۶.۶

۶- منابع

Almohammad, R M. Hierons, G Ghinea. 2008. High Capacity Steganographic Method Based Upon jpeg. Ares, Third International Conference on Availability, Reliability and Security, pp.544-549.

Alturki, F. and Mersereau, R. 2001. A Novel Approach for Increasing Security and Data Embedding Capacity in Images for Data Hiding Applications. Proc. ITCC, Las Vegas, NV, pp. 228–233.

Amiruzzaman, Md. Hyoung, JK.2008. Secure Steganographic Method. VIE 08, Printed and published by the IET.

Anderson, R.J. Petitcolas, F.A.P. 1998. On the Limits of Steganography. IEEE Journal of Selected Areas in Communications, Special Issue on Copyright and privacy Protection, Vol. 16,No.4, pp.474-481.

Barton, J. M. 1997. Method and apparatus for embedding authentication information within digital data. U.S. Patent5, 646 ,997.

Bernd. Girod. lecture notes, www.sta nford.e du/ class/ee392c/lectures/chapter05.pdf.

Bierbrauer, J. and Fridrich, J. 2008. Constructing good covering codes for applications in Steganography. lecture note in computer sience, Springer,Vol 4920,pp.1-22.

Bohme, R. and Westfeld, A. 2004. Breaking Cauchy model-based jpeg steganography with first order statistics. P. Samarati et al (Eds.): ESORICS 2004, LNCS 3193, pp. 125-140.

Cachin, C. 1998. An information-theoretic model for steganography'. In D. Aucsmith, editor, Information Hiding, 2nd International Workshop, Lecture Notes in Computer Science, Vol.1525 pp. 306–318.

CCITT T.81, Information technology. Digital compression and coding of continuous-tone still images. Requirements and guidelines September 1992 <http://www.w3.org/Graphics/jpeg/itu-t81.pdf>.Chae, J.J. Manjunath, B. S. 1008. A Robust Embedded Data from Wavelet Coefficients. SPIE: Storage and Retrievalfor Image and Video Databases VI, Vol.3312, pp.308-317.

Chang, C. C. Chen, T. S. and Chung, L. Z. 2002. A steganographic method based upon jpeg and quantization table modification", Information Sciences, Vol. 141, pp. 123-138.

Chen, B. and Wornell, G.W. 2001. Quantization index modulation: A class of provably good methods for digital watermarking and information embedding. IEEE Trans. on Information Theory, Vol.47, no.4, pp.1423-1443.

Crandall, R. Some Notes on Steganography. Posted on Steganography Mailing List (1998) http://os.inf.tu-dresden.de/ westfeld/crandall.pdf.

Vleeschouwer. De, Delaigle. J. F. and. Macq, B. 2003. Circular interpretation of bijective transformations in lossless watermarking for media asset management. IEEE Tran.Multimedia, Vol. 5, pp. 97-105.

Eggers, J.J. Bauml, R. and Girod, B. 2002. A communications approach to image steganography. Proceedings of SPIE, Vol. 4675, pp.26-37.

Fabien A.P.,Petitcolas J.Ross, 1999,evaluation of copyright systems",IEEE International Conference on multimedia computing and systems,Vol 1, pp.574-579,

Farid, H. 2002. Detecting hidden messages using higher-order statistical models. in Proc.ICIP2002, Vol. 2, pp. II–905–II–908.

Franz, E. 2002. Steganography preserving statistical properties. in 5th International Working Conference on Communication and Multimedia Security.

Franz, E. and Schneidewind, A.2005. Pre-processing for adding noise steganography. In M. Barni, J. Herrera,S. Katzenbeisser, and F. Pérez-González, editors, Proceedings, Information Hiding, 7th International Workshop,Volume 3727 of Lecture Notes in Computer Science, pp. 189–203.

Fridrich, J. 2005. Feature-based steganalysis for jpeg images and its implications for future design of steganographic schemes. In: Proceedings sixth information hiding workshop'04, LNCS 3200,Springer, New York, pp 67–81.

Fridrich, J. 2006. Minimizing the embedding impact in steganography. In J. Dittmann and J. Fridrich, editors, Proceedings ACM Multimedia and Security Workshop, Geneva, Switzerland, pp. 2–10.

Fridrich, J. and Goljan, M. 2002. Digital image steganography using stochastic modulation. in Proceedings of SPIE: Security, Steganography, and Watermarking ofMultimedia Contents IV, Santa Clara, CA, USA, pp. 191-202.

Fridrich, J. and Goljan, M. 2003. Secure digital image steganography using stochastic modulation. In E.J. Delp and P.W. Wong, editors, Proceedings SPIE, Electronic Imaging, Security, Steganography, and Watermarking of Multimedia Contents V, Santa Clara, CA, January 21–24, Vol. 5020, pp. 191–202.

Fridrich, J. and Lisonˇek, P. 2007. Grid coloring in steganography. IEEE Trans. Information. Theory, Vol. 53, no. 4, pp. 1547–1549.

Fridrich, J. Goljan, M. and Du, R. 2001 Steganalysis based on jpeg compatibility. SPIE Multimedia Systems and Applications IV, Denver, CO, August 20–24.

Fridrich, J. Goljan, M. and Du, R. 2001. Invertible Authentication Watermark for jpeg Images. ITCC 2001, Las Vegas, Nevada,pp. 223-27.

Fridrich, J. Goljan, M. and Holga, D. 2003. steganalysis of jpeg images: breaking the F5 algorithm. Lecture notes in computer scince, Vol. 2578, Springer, Berlin Heidelberg New York, pp. 310-322.

Fridrich, J. Goljan, M. and Soukal, D. 2004. Perturbed Quantization Steganography with Wet Paper Codes. in Proc. ACM Multimedia and Security Workshop, Magdeburg, Germany, pp. 4-15.

Kobayashi, H. Noguchi, Y. Kiya, H. 1999. A Method of Embedding Binary Data into jpeg Bitstreams. IEICE Trans. Information and Systems, Vol. J83-D, no. 2, pp. 1469-1476.

Kodovsky, J. and Fridrich, J. 2008. Influence of embedding strategies on security of steganographic methods in the jpeg domain. in: Proceedings of SPIE Electronic Imaging, Security, Forensics, Steganography, and Watermarking of Multimedia Contents X, San Jose, CA, Vol. 6819, pp. 1-13.

Langelaar, G. Setyawan, I. & Lagendijk, R.L. 2000. Watermarking Digital Image and Video Data, IEEE Signal Processing Magazine, pp.20-43.

Lee, Y.K. Chen, L.H. 2000. High capacity image steganographic model. Vision, Image and Signal Processing, IEE Proceedings, Vol 147,pp. 288-294.

Lee, Y.K. Hwei Chen, L. 1998. Secure Error-Free Steganography for jpeg Images . International journal of pattern recognition and artificial intelligence, Vol. 17, pp. 967-981.

Li, B. Huang, F. Huang, J. 2007. steganalysis of lsb greedy algorithm for jpeg images using coefficient symmetry. ICIP

Li, Q. Yu, C. and Chu, D. 2006. A Robust Image Hiding Method Based on Sign Embedding and FuzzyClassification. The Sixth World Congress on Intelligent Control and Automation. WCICA. pp.10050-10053.

Li, X. and Wang, J. 2007. A steganographic method based upon jpeg and particle swarm optimization algorithm. InformationSciences, Vol.177, No.15, pp3099-31091.

Li, X. Li, J. 2008. A new Blind Steganalysis method for jpeg Images. International Conference on Computer Science and Software Engineering.

Lifang, Y. Yao, Z. Rongrong, N. Zhenfeng, Z. 2009. PM1 steganography in jpeg images using genetic algorithm. Springer, Vol. 13, no. 4, pp 393-400.

Lu, C. S. 2005. multimedia security: steganography and digital watermarking techniques for protection intellectual property.

Marvel, L.M. Boncelet, C.G. and Retter, C.T. 1998. Reliable Blind Information Hiding for Images. Lecture Notes on Computer Science, Springer-Verlag, New York,Vol. 1525,No 199, pp. 48–61.

Marvel, L.M. Hartwig, G.W. and Boncelet, C. 2000. Compression-compatible fragile and semi-fragile tamper detection. In SPIE EI Photonics West, pp. 131-139.

Meerwald, P. & Uhl, A. 2001. A Survey of Wavelet-Domain Watermarking Algorithms. SPIE Symposium, Electronic Imaging, San Jose, CA, USA.

Mielikainen, J. 2006. LSB matching revisited. IEEE Signal Process. Lett., Vol. 13, no. 5, pp. 285–287.

MilaniFard. A, M. Akbarzadeh, R.T. Varasteh, A. 2006. A New Genetic Algorithm Approach for Secure jpeg Steganography. pp. 22–23.

Fridrich, J. Goljan, M. and Soukal, D. 2006. Wet paper codes with improved embedding efficiency. IEEE Transactions on Information Security and Forensics, Vol.1,No.1, pp.102–110.

Fridrich, J. Goljan, M. Lisonek, P. and Soukal, D. 2004. Writing on wet paper. in ACM workshop on Multimedia and Security,Magdeburg, Germany.

Fridrich, J. Kodovsky, J. and Pevny, T. 2007. Statistically undetectable JPEG steganography: Dead ends, challenges, and opportunities. In ACM Multimedia & Security Workshop, pages 3–14, September 20–21.

Guillon, P. Furon, T. and Duhamel, P. 2002. Applied public-key steganography. in Proceedings of SPIE: Security, Steganography, and Watermarking ofMultimedia Contents IV.

Gul, G. Dirik, A. E. Avcibas, S. 2007. Steganalytic Features for jpeg Compression Based Perturbed Quantization. Signal Processing Letters, IEEE Vol.14, pp.205-208.

Harmsen, J.J. and Pearlman, W. A. 2003. Steganalysis of Additive Noise Modelable Information Hiding. Proc. SPIE Electronic Imaging, Santa Clara.

Hayati, P. Potdar, V. Chang, E. 2006. A survey of steganographic and steganalytic tools for the digital forensicinvestigator.availablefrom: http://debii.curtin.edu.au/~pedram/images/docs/survey_of_steganography_and_steganalytic_tools.pdf

Hernandez, J.R. Amado, M. & PerezGonzalez, F. 200. DCTDomain Watermarking Techniques for Still Images: Detector Performance Analysis and a New Structure. IEEE Trans. Image Processing, Vol.9, pp. 55-68.

Inoue, H. Miyazaki, A. & Katsura, T. 1998. An Image Watermarking Method Based on the Wavelet Transform. Kyushu Multimedia System Research Laboratory, In: Proceedings ICIP'99, Kobe, Japan, October, Vol. 1, pp. 296–300.

Jacobsen, N. Solanki, K. Madhow, U. Manjunath, B. S. and S.Chandrasekaran. 2002. Image adaptive high Volume data hiding based on scalar quantization. In Proceedings of the IEEE Military Communications Conference (MILCOM), Anaheim, CA, USA.

Ker, D. Steganalysis of LSB Matching in Grayscale Images. 2005. IEEE SignalProcessing Letters, Vol. 12, No. 6.

Kharrazi, M. Sencar, H.T. Memon, N. 2005. Benchmarking Steganographic and Steganalytic Techniques. in Proc. Elec. Imaging, SPIE, Sequrity, Steganography, and Watermarking of Multimedia Contents VII, San Jose, CA, January 17,20.

Kim, Y. Duric, Z. and Richards, D. 2006. Modified matrix encoding technique for minimal distortion steganography. In N. Johnson and J. Camenisch, editors, Information Hiding, 8th International Workshop, Lecture Notes in Computer Science, Vol. 4437, Springer-Verlag, New York.

Sallee, P. 2005. Model-based methods for steganography and steganalysis. International Journal of Image Graphics, Vol.5,no. 1,pp.167–190.

Sarkar, A. Solanki, K. Madhow, U. et al. 2007. Secure steganography: statistical restoration of the second order dependencies for improved security. IEEE International Conference on Acoustics, Speech, and Signal Processing Honolulu, Hawaii, pp. 277–280.

Satish, K. Jayakar, T. Tobin, C. Madhavi, K. and Murali, K. 2004. Chaos based spread spectrum image Steganography. IEEE Transactions on ConsumerElectronics, Vol.50, pp.587-590.

Shi, Y.Q. Chen, C. and Chen, W. 2006. A Markov process based approach to effective attacking jpeg steganography. N. Johnson and J. Camenisch, editors, Information Hiding, 8th International Workshop, Volume 4437 of LNCS, Springer-Verlag, New York.

Solanki, K. Dabeer, O. Manjunath, B. S. Madhow, U. and Chandrasekaran, S. 2003. A joint source-channel coding scheme for image-in-image data hiding. In Proceedings of ICIP, pp. II-743-746.

Solanki, K. Jacobsen, N. Chandrasekaran, S. Madhow, U. and Manjunath, B. S. 2002. High-Volume data hiding in images: Introducing perceptual criteria into quantization based embedding. In Proceedings of ICASSP, Orlando,FL, USA.

Solanki, K. Sarkar, A. and Manjunath, B. S. 2007. YASS: yet another steganographic scheme that resists blind steganalysis. in 9th International Workshop on Information Hiding.

Solanki, K. Sarkar, A. and Manjunath, B. S. 2008. Further Study on YASS: Steganography Based on Randomized Embedding to Resist Blind Steganalysis. SPIE Security, Steganography, and Watermarking of Multimedia Contents (X) ,San Jose, California.

Solanki, K. Sullivan, K. Madhow, U. Manjunath, B. S. and Chandrasekaran, S. 2005. Statistical restoration for robust and secure steganography. in Proc. ICIP, pp. II 1118-21.

Solanki, K. Sullivan, K. Madhow, U. Manjunath, B. S. and Chandrasekaran, S. 2006. Provably secure steganography: Achieving zero K-L divergence using statistical restoration. In Proceedings ICIP, Atlanta, GA.

Sullivan, K. Solanki, K. Madhow, U. Manjunath, B. S. and Chandrasekaran, S. 2006. Determing achievable rates for secure, zero-divergence, steganography. in Proc. ICIP, pp.121-124.

Tseng, H. W. and Chang, C. C. 2004. Steganography using jpeg-compressed images. The Fourth InternationalConference on Computer and Information Technology, CIT '04, pp. 12-17, 14-16.

Tzschoppe, R. B¨auml, R. Huber, J. B. and Kaup, A. Steganographic system based on higher order statistics. in Proc. SPIE Vol. 5020, Security and

Moulin, P. and Briassouli, A. 2004. A stochastic QIM algorithm for robust, undetectable image watermarking. in Proceedings ICIP, Singapore.

Munirajan, V. K. Cole, E. and Ring, S. 2004. Transform domain steganography detection using fuzzy inferencesystems. In Proceedings of the IEEE Sixth International Symposium on Multimedia Software Engineering, pp. 286-291.

Noda, H. Niimi, M. and Kawaguchi, E. 2005. Application of QIM with dead zone for histogram preserving jpeg steganography. In Proceedings ICIP, Genova, Italy.

Noguchi, Y. Kobayashi, H. Kiya, H. 2000. A Method of Extracting Embedded Binary Data from jpeg Bitstreams Using Standard jpeg Decoder. Proceedings of IEEE International Conference on Image Processing, Vancouver,BC, Canada, Vol. 1, pp. 577-580.

Pevný, T. and Fridrich, J. 2007. Merging Markov and DCT features for multi-class jpeg steganalysis. In E.J. Delp and P.W. Wong, editors, Proceedings SPIE,Electronic Imaging, Security, Steganography, and Watermarking of Multimedia Contents IX, San Jose,CA, Vol. 6505, pp. 03–04.

Pevný, T. and Fridrich, J. 2008. Estimation of primary quantization matrix for steganalysis of double compressed jpeg images. In E. J. Delp and P. W. Wong, editors, Proceedings SPIE, Electronic Imaging, Security, Forensics, Steganography, and Watermarking of Multimedia Contents X, Vol. 6819, pp. 11-13.

Provos, N. and Honeyman, P. 2003. Hide and seek: An introduction to steganography. IEEE Security and Privacy, Vol.01,No.3,pp.32-44.

Provos, N. Honeyman, P. 2001. Detecting Steganographic Content on the Internet. CITI Technical Report, pp.01-11.

Rongrong, J. Hongxun, Y. Shaohui, L. Liang, W. and Jianchao, S. 2006. A New Steganalysis Method for Adaptive Spread Spectrum Steganography. In Proceedings of the International Conference on Intelligent Information Hiding and Multimedia Signal Processing, IIH-MSP '06,pp. 365-368.

Rossi, L. Garzia, F. and .Cusani, R. 2009. Peak-Shaped-Based Steganographic Technique for jpeg Images. EURASIP Journal on Information Security Vol.2009, Article ID 382310, 8 pages.

SAKAI, H. KURIBAYASHI, M. MORII, M. 2008. Adaptive Reversible Data Hiding for jpeg Images. International Symposium on Information Theory and its Applications, ISITA2008, Auckland, New Zealand.

Sallee, P. 2004. Model-based steganography. Digital Watermarking,2nd International Workshop, IWDW 2003, Seoul,Korea, Lecture Notes in Computer Science, Springer-Verlag, New York, Vol. 2939 ,pp.154–167.

ml
[jpegx]:
http://www.leetupload.com/dbindex2/index.php?dir=Win32/ .
[Sarc]:
www.sarc-wv.com/.
[stego suit]:
www.wetstonetech.com/.
[CameraShy]:
http://hacktivismo.com/projects/index.php/.
[F5]:
http://wwwrn.inf.tu-dresden.de/~westfeld/f5.html /.
http://linux01.gwdg.de/%7Ealatham/stego.html/.
http://www.nic.funet.fi/pub/crypt/steganography/.
http://www.outguess.org/download.php/.
[Steghide]:
http://steghide.sourceforge.net/
[Crypto123]:
http://www.kellysoftware.com/software/Crypto123.asp/
[IBMDLS]:
http://www.research.ibm.com/image_apps/commerce.html/.
[Invisible Secrets]:
http://www.neo-bytesolutions.com/
[Info Stego]:
http://www.antiy.net/infostego/
[Syscop]:
http://www.mediasec.com/html/en/products_services/syscop.htm /.
[StegMark]:
http://www.datamark-tech.com/index.htm
[jpegx]:
http://www.leetupload.com/dbindex2/index.php?dir=Win32/.
[DCT-Steg]:
www.jjtc.com/Steganography/tools.html
[EikonAmark]:
www.brothersoft.com/eikonamark-100523. html/.
[AppendX]:
www.appendx.org/.

Watermarking of Multimedia Contents V, (Santa Clara, CA).

Ullerich, C. Westfeld, A.2008. Weaknesses of MB2. Proceedings of the 6th International Workshop on Digital Watermarking, Lecture Notes In Computer Science, Vol. 5041, pp.127-142.

Upham, D. Jsteg. 2002. ftp://ftp. funet.fi/p ub / crypt /steganography/.

Wang, H. and Wang, S. 2004. Cyber warfare: Steganography vs. steganalysis. Communication of the ACM, Vol. 47, pp.76–82.

Wang, Z. and Bovik, A. C. 2002. A universal image quality index. IEEE Signal Processing Letters ,Vol.9,pp. 81–84.

Wang, Z. Bovik, A.C. Sheikh, H. R. and Simoncelli, E. P. 2004. Perceptual image quality assessment: From error visibility to structural similarity. IEEE Trans Image Processing, Vol. 13, no. 4, pp. 600-612.

Westfeld, A. 2001. High capacity despite better steganalysis (F5—a steganographic algorithm)", In I.S. Moskowitz, editor, Information Hiding, 4th International Workshop, Lecture Notes in Computer Science, Springer-Verlag, New York, Vol.2137, pp.289–302.

Westfeld, A. 2002. Detecting low embedding rates. in Proc. Inf. Hiding Workshop, Springer LNCS, Vol. 2578.

Willems, F. and Dijk, M. 2005. Capacity and codes for embedding information in gray-scale signals. IEEE Trans. Inf. Theory, Vol. 51, no. 3, pp.1209–1214.

Wong, K. and Tanaka, K. 2007. A steganographic method with recursive matrix encoding on selected blocks and DCT coefficients. Intl. Workshop on Smart Info-Media Systems in Bangkok, pp. 155 – 160.

Wong, K. and Tanaka, K. 2008. improvement of stegermelc with hybrid recursive matrix encoding. 2008 International Symposium on Intelligent Signal Processing and Communication Systems (ISPACS2008),Swissôtel Le Concorde, Bangkok, Thailand.

Wong, P. H. W. and Wong, J. W. C. 2001. A Data Hiding Technique in jpeg Compressed Domain. In Proceedings of SPIE Conference on Security and Watermarking of Multimedia Contents III, San Joes, CA, USA. Vol. 4314, pp. 309-340.

Wu, H.C. Lee, C.C. Tsai, C.S. 2009. A high capacity reversible data hiding scheme with edge prediction and difference expansion. pp. 1966-1973.

Zhang, X. and Wang, S. 2006. Efficient steganographic embedding by exploiting modification direction. IEEE Commun. Lett, Vol. 10, no. 11, pp. 781–783.

[Camouflage]:
http://camouflage.unfiction.com/.
[DataStash]:
http://www.skyjuicesoftware.com/software/ds_info.ht

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

نشانی رایانامک ایشان عبارت است از:

fjdinan@gmail.com

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

نشانی رایانامک ایشان عبارت است از:

rezaei.image@yahoo.com

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

نشانی رایانامک ایشان عبارت است از:

mbeigzadeh@gmail.com

الهه بیات مدرک کارشناسی خود را در رشته‌ی مهندسی برق - الکترونیک در سال ۱۳۸۵ از دانشگاه آزاد اسلامی (واحد تهران مرکز) و هم اکنون دانشجوی کارشناسی ارشد مهندسی فناوری اطّلاعات – مخابرات امن دانشگاه علم و صنعت ایران می‌باشد. زمینه‌های تحقیقاتی مورد علاقه‌ی وی پردازش تصویر و پنهان‌نگاری اطلاعات می‌باشد.

نشانی رایانامک ایشان عبارت است از:

elh.byt@gmail.com