مجله علمی پژوهشی «علوم و فناوری‌های پدافند غیرعامل»
سال چهارم، شماره۱، بهار ۱۳۹۲؛ ص ۱۴-۱

یک روش جدید پنهان‌نگاری تطبیقی با ظرفیت مقیاس‌پذیر و کیفیت بصری بالا

سید رحمان سلیمانی[۱]، سارا حق‌بین[۲]، مسعود نیازی ترشیز[۳*]

۱- کارشناس ارشد، ۲- کارشناس، ۳- استادیار دانشگاه آزاد اسلامی واحد مشهد

(دریافت: ۹۱/۰۱/۱۵، پذیرش: ۹۲/۰۲/۳۱)

چکیده

در این مقاله، یک روش پنهان نگاری تطبیقی جدید برای جاسازی داده‌های محرمانه در تصویر پیشنهاد شده است. روش پیشنهادی به کاربر این امکان را می‌دهد که با توجه به حجم اطلاعات محرمانه مورد نیاز برای انتقال به مقصد، پارامترهای الگوریتم را به‌نحوی تنظیم کند که علی‌رغم جاسازی اطلاعات محرمانه در کل پیکسل‌های تصویر، اختلال ایجاد شده ناشی از پنهان نگاری در تصویر را کاهش دهد. همچنین از این پارامترها می‌توان به‌عنوان یک کلید محرمانه در پنهان‌نگاری استفاده کرد. در این روش، با در نظر گرفتن سیستم حساسیت چشم انسان، تعداد بیت بیشتری از داده‌های محرمانه را در نواحی لبه‌ای تصویر به نسبت نواحی صاف و هموار آن جاسازی می‌شود. در روش پیشنهادی، بلاک‌ها بر اساس میزان پیچیدگی محلی پیکسل‌های داخل آن، به گروه‌های مختلفی تقسیم‌بندی می‌شوند و ظرفیت هر گروه بر اساس حجم کلی اطلاعات محرمانه تعیین می‌شود. همچنین این روش در برابر حملات آماری و هیستوگرامی پنهان‌شکنی از خود مقاومت نشان می‌دهد.

کلید واژه‌ها: **پنهان‌نگاری، تطبیقی، سیستم حساسیت چشم انسان، پنهان‌شکنی.**

A New Adaptive Steganographic Method with Scalable Capacity and High Vision Quality

S. R. Soleimani, S. Haghbin, M. Niazi*
Islamic Azad University-Mashad Branch
(Received: 03/04/2012; Accepted: 21/05/2013)

Abstract

In the present paper, a new adaptive steganographic method has been proposed to embed secret data in an image. Proposed method allows the user to set algorithm parameters in a way that reducing the distortion resulted from stegnanography in the image in spite of embedding secret data in all pixels of image, considering size of secret data required for sending to destination. These parameters can be also used as a secret steganographic key. In this method, considering the human vision system, more secrete data bits are embedded in edged areas of image than in its smooth ones. In the proposed method, blocks are classified into different groups based on the extent of local complexity of pixels, and the capacity of each group is determined by total size of secret data. This method is also resistant to statistical and histogram steganalysis attack.

Keywords: Steganography, Adaptive, Human Vision System, Stegana.

* Corresponding Author E-mail: masood.niazi@gmail.com

۱. مقدمه

امروزه با گسترش روزافزون فن‌آوری اطلاعات و ارتباطات، جهان از طریق داده‌های دیجیتالی به‌سوی دنیای دیجیتال و ارتباطات پیش می‌رود. در این میان نقش اینترنت به‌عنوان یک کانال ارتباطی عمومی، هر روز در دنیای ارتباطات پررنگ‌تر می‌شود. علاوه بر این، برقراری امنیت و ایجاد ارتباطات محرمانه، با توجه به ساختار عمومی و مشترک این کانال‌ارتباطی، از اهمیت ویژه‌ای برخوردار است.

به‌طورکلی دو روش عمده برای ایجاد یک ارتباط محرمانه، رمزنگاری و پنهان‌نگاری است [۱]. در رمزنگاری، داده‌های محرمانه توسط یک یا چند کلید رمزنگاری به داده‌های مبهم و غیرقابل خواندن تبدیل می‌شوند و هدف اصلی آن، پنهان نمودن محتوای یک پیام محرمانه است. لازم به ذکر است که خود ارتباط محرمانه پنهان نمی‌شود. غیرقابل فهم بودن این‌گونه داده‌ها، توجه افراد متخاصم را به خود جلب می‌کند و حس کنجکاوی و خرابکارانه آنها را نیز ممکن است برانگیزد. برای غلبه بر این مشکل می‌توان در کنار رمزنگاری، از پنهان‌نگاری نیز استفاده کرد که هدف آن، پنهان کردن ارتباطات محرمانه به‌وسیله قرار دادن اطلاعات محرمانه در یک رسانه پوششی است به‌طوری که کمترین تغییرات قابل فهم برای چشمان انسان در آن رسانه بروز کند و نتوان موجودیت پیام پنهان‌شده در آن را، حتی به‌صورت احتمالی آشکار ساخت.

به دلیل اینکه با استفاده از پنهان‌نگاری می‌توان اطلاعات محرمانه و استراتژیک را در یک رسانه پوشانه مخفی کرد و همچنین بدون جلب توجه دشمن و افراد متخاصم این اطلاعات محرمانه را بر روی کانال‌های ارتباطی عمومی انتقال داد، در بحث پدافند غیرعامل[1] و استتار اطلاعات محرمانه و استراتژیک، هنر پنهان‌نگاری از اهمیت ویژه‌ای برخوردار است. در حقیقت، استفاده از پنهان‌نگاری در انتقال و ذخیره نمودن اطلاعات محرمانه، یک لایه امنیتی به سیستم‌های نوین اطلاعاتی اضافه می‌کند.

یک روش ایده‌آل در پنهان‌نگاری، روشی است که در عین حال که دارای ظرفیت جاسازی بالایی باشد، کیفیت تصویری مطلوبی نیز برای تصویر استگو (تصویر حاصل از جاسازی بیت‌های محرمانه در تصویر پوشانه) ایجاد کند و در برابر حملات مختلف پنهان‌شکنی[2] نیز مقاوم باشد [۲]. معمولاً بین نرخ جاسازی و کیفیت تصویر استگو موازنه‌ای برقرار است، به این صورت که با افزایش ظرفیت جاسازی، کیفیت تصویر استگو کاهش پیدا می‌کند و برعکس. در نتیجه مطلوب است قبل از مرحله جاسازی، حجم داده‌های محرمانه را تا حد امکان با استفاده از روش‌های مختلف فشرده‌سازی کاهش داد.

برخلاف روش‌های غیرتطبیقی در پنهان‌نگاری [۶-۳] که تعداد بیت قابل جاسازی در هر پیکسل ثابت است، در روش‌های تطبیقی [۱۰-۷] ظرفیت جاسازی پیکسل‌ها در نواحی مختلف تصویر متفاوت است. روش‌های تطبیقی با بهره‌گیری از ضعف سیستم بینایی انسان، سعی در جاسازی تعداد بیت‌بیشتری از اطلاعات محرمانه را در پیکسل‌های لبه‌ای تصویر دارند، زیرا چشمان انسان نسبت به تغییرات ایجاد شده در این نواحی، حساسیت کمتری دارد و می‌توان بدون ایجاد تغییرات قابل رؤیت در تصویر، تعداد بیت بیشتری از داده‌های محرمانه را در نواحی لبه‌ای تصویر مخفی کرد [۱۱].

ساده‌ترین و رایج‌ترین روش جاسازی در پنهان‌نگاری تصاویر، روش جاسازی LSB یا همان بیت کم‌ارزش[3] است که پیام را در بیت‌های کم‌ارزش هر پیکسل از تصویر پوشانه جاسازی می‌کند. تاکنون روش‌های پنهان‌نگاری بسیاری بر مبنای این روش ارائه شده است [۱۴-۱۲]. در این روش‌ها، تعداد بیت ثابتی از داده‌های محرمانه، با همان تعداد بیت از کم‌ارزش‌ترین بیت‌های هر پیکسل جایگزین می‌شود. اگرچه در این روش ظرفیت جاسازی بالا است ولی با افزایش تعداد بیت‌های جاسازی شده در هر پیکسل، انحراف[4] ایجاد شده در تصویر استگو افزایش می‌یابد، درنتیجه می‌توان با روش‌های گوناگون پنهان‌شکنی [۱۶-۱۵] وجود پیام محرمانه را در تصویر استگو تشخیص داد. در روش غیرتطبیقی ارائه شده توسط چنگ و همکارانش [۱۷]، برای آنکه دنباله بیتی به طول n را در یک بلاک دو پیکسلی از تصویر پوشانه جاسازی کنیم، در این دنباله تعداد بیت‌ها با مقدار ۱ را در پیکسل سمت چپ و نحوه قرارگیری و چیدمان این بیت‌ها در دنباله را با استفاده از یک تابع ترکیب[5] در پیکسل سمت راست جاسازی می‌کنیم. در این روش ظرفیت جاسازی تمام بلاک‌های تصویر پوشانه ثابت و برابر n بیت است. همچنین در این روش، مقدار انحراف ایجاد شده در تصویر استگو توسط یک تابع پیمانه کاهش پیدا می‌کند.

یکی از معروف‌ترین روش‌های پنهان‌نگاری تطبیقی، روش PVD[6] [۷] است. در این روش، با استفاده از تغییر اختلاف مقدار دو پیکسل مجاور در تصویر پوشانه، بیت‌های محرمانه در پیکسل‌های تصویر پوشانه جاسازی می‌شوند. ضعف این روش در این است که اطلاعات محرمانه فقط در جفت پیکسل‌هایی قابل جاسازی هستند که پس از عملیات پنهان‌نگاری مقادیر پیکسل‌های آنها دچار سرریز[7] یا فروریز[8] نشوند. یعنی مقدار پیکسل از محدوده مجاز آن (برای تصاویر با عمق بیتی b بیت، بازه ۰ تا 2^b-1) تجاوز نکند. برای رفع این مشکل، در روش [۸]، با استفاده از یک تابع پیمانه کیفیت تصویر استگو به میزان چشم‌گیری بهبود پیدا کرد و مشکل سرریز و فروریز نیز از بین رفت، ولی با این وجود ظرفیت جاسازی در این روش همچنان محدود بود. پس از آن، در [۱۸] با ایجاد تغییراتی در انتخاب پیکسل‌های همسایه، ظرفیت جاسازی در روش [۸] تا حدودی افزایش پیدا کرد. در [۱۹]، روشی مشابه با روش [۸] پیشنهاد شد که

[1] Passive Defense
[2] Steganalysis

[3] Least Significant Bit
[4] Distortion
[5] Combined Function
[6] Pixel Value Differencing
[7] Overflow
[8] Underflow

بر خلاف آن، قوانین جایگزینی بیت‌ها در این روش با استفاده از قوانین رنگ‌آمیزی گراف‌ها تعیین می‌شد. در [۲۰]، روشی پیشنهاد داد که بر پایه سنجش انحراف ایجاد شده در تصویر پوشانه استوار و از ظرفیت جاسازی و کیفیت بصری بالایی برخوردار بود. در روش [۲۱] که ترکیبی از روش‌های LSB و PVD است، با وجود ظرفیت جاسازی بالا، این روش نسبت به روش PVD در برابر حمله پنهان‌شکنی معروف RS [۱۵] شکست خورد. دلیل این شکست در [۲۲] بیان شده است.

به‌طور کلی در روش‌های پنهان‌نگاری تطبیقی، از روش‌های گوناگونی برای تشخیص لبه در تصاویر استفاده می‌شود. به‌عنوان مثال در [۹]، با محاسبه اختلاف میانگین پیکسل‌های همسایه نسبت به یک پیکسل هدف، درجه لبه‌ای بودن هر پیکسل مشخص می‌شود. در این روش هرچه تعداد بیشتری از پیکسل‌های همسایه نسبت به یک پیکسل هدف درنظر گرفته شود، به نواحی بافت تصویر بیشتر توجه می‌شود و کیفیت تصویر استگو افزایش پیدا می‌کند. در روش [۲۳] با بهره‌گیری از منطق فازی لبه‌ها در تصویر پوشانه شناسایی می‌شود. همچنین در روش [۱۰] نیز با محاسبه مقدار انحراف معیار پیکسل‌های داخل هر بلاک، مقدار لبه‌ای بودن هر بلاک برای جاسازی بیت‌های محرمانه در آن مشخص می‌شود.

روش پیشنهاد شده در این مقاله، روش غیرتطبیقی ارائه شده توسط چنگ و همکارانش [۱۷] را بهبود می‌دهد و همچنین به کمک مکانیزم جاسازی در روش غیر تطبیقی پیشنهادی، با استفاده از سنجش میزان پیچیدگی محلی برای هر بلاک و تعیین ظرفیت جاسازی در آن، یک روش تطبیقی با ظرفیت مقیاس‌پذیر و کیفیت بصری مطلوب پیشنهاد داده شده است.

۲. روش‌های مرتبط

در این بخش به بیان دو روش مشهور تطبیقی و غیرتطبیقی در پنهان‌نگاری پرداخته می‌شود. در قسمت اول به‌صورت مختصر روش تطبیقی PVD معرفی می‌شود، سپس در قسمت بعدی به توصیف کامل روش غیرتطبیقی چنگ و همکارانش [۱۷] پرداخته خواهد شد. این روش، مبنای فرآیند جاسازی بیت‌های محرمانه در روش تطبیقی پیشنهادی این تحقیق است.

۲-۱. روش PVD

در این روش، ابتدا تصویر پوشانه به بلاک‌های دو پیکسلی غیرهمپوشان تقسیم‌بندی شده که نحوه پیمایش بلاک‌ها به‌صورت سطر به سطر و به شکل زیگزاگ است. سپس بلاک‌ها بر حسب مقدار اختلاف موجود (d) میان دو پیکسل درون بلاک،به دسته‌های مختلفی تقسیم‌بندی می‌شوند. بدین صورت که بازه ۰ تا ۲۵۵ به بازه‌های مختلفی بر حسب توان‌هایی از ۲ تقسیم می‌شوند و به هر بازه اندیسی (k) نسبت داده می‌شود. در هر بلاک با توجه به اینکه قدر مطلق اختلاف دو پیکسل درون بلاک متعلق به کدام بازه است اندیس گروه مورد نظر به آن بلاک منسوب می‌شود. اگر حد بالا و پایین بازه k را u_k و l_k در نظر گرفته شود، آنگاه طول بازه برابر با $w_k=u_k-l_k+1$ است و ظرفیت جاسازی در این بازه به‌صورت $n=\log w_k$ تعریف می‌شود.

فرض می‌شود p_i و p_{i+1} دو پیکسل همسایه در یک بلاک با مقادیر روشنایی g_i و g_{i+1} باشد، مقدار اختلاف d در این بلاک برابر است با $g_{i+1} - g_i$. همچنین d به بازه k با ظرفیت n بیت تعلق دارد. برای جاسازی بیت‌های محرمانه، باید مقدار اختلاف دو پیکسل درون بلاک تغییر یابد. بدین منظور برای جاسازی یک دنباله بیتی به‌طول n در یک بلاک، مقدار اختلاف جدید (d') طبق رابطه زیر محاسبه می‌شود: (در این رابطه b برابر مقدار ده دهی دنباله بیتی است).

$$d' = \begin{cases} I_k + b & d \geq 0 \\ -(I_k + b) & d < 0 \end{cases} \quad (۱)$$

سپس با استفاده از تابع f مقادیر جدید پیکسل‌های بلاک استگو (g'_i,g'_{i+1}) طبق رابطه (۲) محاسبه می‌شود و با مقادیر قبلی آن جایگزین می‌شود (m برابر d'-d است).

$$(g'_i, g'_{i+1}) = f((g'_i, g'_{i+1}), m) = \begin{cases} (g_i - \lceil m/2 \rceil), g_{i+1} + \lfloor m/2 \rfloor) & d \text{ is odd} \\ (g_i - \lceil m/2 \rceil), g_{i+1} + \lceil m/2 \rceil) & d \text{ is even} \end{cases} \quad (۲)$$

مقادیر جدید پیکسل‌های درون بلاک باید به‌گونه‌ای تغییر یابند که مقدار اختلاف دو پیکسل از بازه k تجاوز نکند.

برای بازیابی اطلاعات محرمانه در این روش، عکس عملیات جاسازی انجام می‌شود. یعنی ابتدا مقدار اختلاف دو پیکسل درون هر بلاک محاسبه شده و بازه‌ای که این مقدار اختلاف به آن تعلق می‌گیرد مشخص می‌شود. سپس با کم‌کردن مقدار ابتدای بازه k از مقدار اختلاف دو پیکسل و همچنین محاسبه تعداد بیت جاسازی شده در بلاک ($\log_2 K$) و تبدیل نتیجه حاصل به معادل باینری آن، بیت‌های محرمانه از بلاک مورد نظر استخراج می‌شود.

۲-۲. روش غیرتطبیقی

در این روش نحوه بلاک‌بندی و پیمایش بلاک‌ها، همانند روش PVD است. در یک بلاک‌دو پیکسلی، پیکسل سمت چپ l_iو پیکسل سمت راست r_i نامیده می‌شود و تنها روش پنهان‌نگاری غیرتطبیقی ارائه شده تا کنون است که هر دنباله از بیت‌های محرمانه را در دو پیکسل از تصویر پوشانه جاسازی می‌کند [۱۷]. به‌همین دلیل این روش در جاسازی بیت‌های محرمانه در تصاویر از انعطاف‌پذیری بالایی برخوردار است.

به‌عنوان مثال، در روش‌های دیگر در هر پیکسل از تصویر ۱، ۲ یا ۳ بیت از اطلاعات محرمانه را می‌توان پنهان نمود ولی در این روش اگر در هر جفت پیکسل ۳ بیت از بیت‌های محرمانه پنهان شود، به‌طور متوسط در هر پیکسل ۱/۵ بیت از داده‌های محرمانه پنهان خواهد شد.

در این روش، برای آنکه دنباله بیتی به طول n بیت در یک بلاک دو پیکسلی از تصویر پوشانه جاسازی شود، تعداد بیت‌ها با مقدار ۱ در این دنباله را در l_i، و عددی که نشان‌دهنده نحوه قرارگیری این بیت‌ها در دنباله است را با استفاده از یک تابع ترکیب در r_i جاسازی می‌شود. ظرفیت جاسازی تمام بلاک‌های تصویر پوشانه در این روش ثابت و برابر n بیت است.

اگر دنباله بیتی در یک بلاک جاسازی شده به‌صورت $S_n=b_{n-1}b_{n-2}\ldots b_1b_0$ در نظر گرفته شود و تعداد بیت‌ها با مقدار ۱ در این دنباله برابر k باشد، آنگاه تعداد حالت‌های ممکن برای قرارگیری k بیت از داده‌های محرمانه با مقدار ۱ در دنباله‌ای به طول n برابر ترکیب C_k^n است. با استفاده از رابطه (۳) می‌توان نحوه قرارگیری بیت‌های محرمانه در دنباله را با استفاده از یک تابع ترکیب مشخص کرد:

$$f(S_n)=\sum_{i=1}^{n-1} b_i C_{N(i)}^{i} \qquad (۳)$$

در رابطه (۳)، b_i مقدار iامین بیت از رشته بیتی S_n است. $N(i)$ نیز برابر تعداد بیت‌های ۱ موجود در رشته S_n از بیت شماره ۱ تا بیت iام است. مقادیر جدید پیکسل‌های l_i و r_i (l'_i و r'_i)، به صورتی تغییر پیدا می‌کنند که مقادیر k و $f(S_n)$ به‌دست آمده برای دنباله S_n، در روابط زیر صدق کنند:

$$K = l'_i \bmod(n+1) \qquad (۴)$$

$$f(S_n)=r'_i \bmod C_k^n \qquad (۵)$$

با توجه به روابط (۵ و ۴)، بیشینه انحراف ایجاد شده پس از جاسازی بیت‌های محرمانه در پیکسل‌های l_i و r_i، به‌ترتیب برابر $\lfloor (n+1)/2 \rfloor$ و $\lfloor C_k^n/2 \rfloor$ است. هنگام استخراج اطلاعات، با استفاده از رابطه‌های (۵ و ۴) و در اختیار داشتن مقدار n می‌توان به‌راحتی مقادیر k و $f(S_n)$ را برای هر بلاک از تصویر پوشانه به‌دست آورد. سپس با اعمال تابع معکوس f^{-1} طبق رابطه (۶)، می‌توان دنباله بیتی جاسازی شده در آن بلاک را استخراج کرد. در این رابطه، num با مقدار $f(S_n)$ مقداردهی اولیه می‌شود و $C_0^0=1$ و $n\geq 1$است.

$$f^{-1}(num,n,k)= \begin{cases} f^{-1}(num,n-1,k)+'0' & if\ \ num<C_k^{n-1} \\ f^{-1}(num-C_k^{n-1},n-1,k-1)+'1' & if\ \ num\geq C_k^{n-1},(n-1)\geq k \\ f^{-1}(num,n-1,k-1)+'1' & if\ \ (n-1)<k \end{cases} \qquad (۶)$$

در این روش، بیت‌های محرمانه برخلاف روش LSB به‌طور مستقیم در هر پیکسل جاسازی نمی‌شود، بلکه با استفاده از توابع پیمانه و ترکیب، به‌طور ضمنی در مقادیر پیکسل‌های هر بلاک پنهان می‌شوند.

۳. روش پیشنهادی

الگوریتم پیشنهادی پنهان‌نگاری تطبیقی در این مقاله از دو مرحله جاسازی داده‌های محرمانه (که توسط کاربر در مبدأ انجام می‌شود) و استخراج داده‌های محرمانه (که توسط کاربر دریافت کننده در مقصد اجرا می‌شود) تشکیل شده است.

۳-۱. جاسازی داده‌های محرمانه

فرآیند جاسازی داده‌های محرمانه در تصویر پوشانه، شامل مراحل بلاک‌بندی، تعیین پارامترهای الگوریتم، جاسازی بیت‌های محرمانه و تعیین کلید پنهان‌نگاری است. در گام جاسازی، اطلاعات محرمانه توسط یک روش پیشنهادی پنهان‌نگاری غیرتطبیقی در بلاک‌های تصویر پوشانه جاسازی می‌شود که به‌شرح زیر است:

بلاک‌بندی: در این مرحله تصویر پوشانه به بلاک‌های چهار پیکسلی غیرهمپوشان با ابعاد ۲×۲ پیکسل تقسیم‌بندی می‌شود. برای افزایش امنیت می‌توان در این مرحله با استفاده از یک کلید[1] (هسته ابتدایی در تولید اعداد شبه تصادفی)، ترتیب پیمایش بلاک‌ها را در مرحله جاسازی مشخص کرد. بدین ترتیب بدون دانستن این کلید نمی‌توان نحوه پیمایش بلاک‌ها را به‌طور صحیحی تشخیص داد و در پی آن نمی‌توان بیت‌های محرمانه را به‌ترتیبی صحیح از بلاک‌های تصویر استگو استخراج کرد.

تعداد کل بلاک‌های موجود در یک تصویر پوشانه با ابعاد M×N پیکسل، طبق رابطه (۷) تعیین می‌شود. در این رابطه، پارامتر t تعداد کل بلاک‌ها را نشان می‌دهد:

$$t=\frac{M\times N}{4} \qquad (۷)$$

اگر تعداد کل بیت‌های پیام محرمانه‌که باید در تصویر پوشانه پنهان شود را T در نظر بگیریم، آنگاه میانگین ظرفیت جاسازی در هر بلاک[2] ($AvgC_{bpB}$) بر اساس رابطه (۸) محاسبه می‌شود:

$$AvgC_{bpB}=\frac{T}{t} \qquad (۸)$$

به‌کمک این مقدار، می‌توان تعیین کرد که به‌طور متوسط چه تعداد بیت باید در هر بلاک پنهان شود تا بتوان تمام بیت‌های محرمانه را در تصویر پوشانه مخفی کرد.

تعیین پارامترهای الگوریتم: در این مرحله، بلاک‌های تصویر پوشانه برحسب میزان پیچیدگی محلی پیکسل‌ها در هر بلاک به گروه‌های مختلفی تقسیم‌بندی می‌شود. تعداد گروه‌ها برحسب مورد می‌تواند بین ۲ تا ۴ گروه تغییر کند. اگر تعداد گروه‌ها ۱ در نظر گرفته شود، آنگاه این روش به یک روش غیرتطبیقی تبدیل می‌شود. زیرا در این حالت ظرفیت جاسازی تمامی بلاک‌های تصویر پوشانه باهم یکسان خواهند شد. ظرفیت جاسازی بلاک‌های متعلق به هر گروه را می‌توان به‌کمک مقدار $AvgC_{bpB}$، که توسط رابطه (۸) تعیین می‌شود مشخص کرد. ظرفیت جاسازی گروه‌ها به‌گونه‌ای تعیین

[1] Seed
[2] Average Capacity (Bit Per Block)

می‌شود که همیشه مقدار $AvgC_{bpB}$ برابر میانگین ظرفیت تمام گروه‌ها شود. برای مثال اگر تعداد گروه‌ها ۳ در نظر گرفته شود (gr_1,gr_2,gr_3)، آنگاه ظرفیت جاسازی در بلاک‌های متعلق به گروه ۲ (گروه میانه) $\lceil AvgC_{bpB} \rceil$ در نظر گرفته می‌شود و ظرفیت جاسازی گروه‌های ۱ و ۳ را نیز می‌توان با اختلاف ۱ تا ۴ واحد از ظرفیت گروه ۲ انتخاب کرد، به‌نحوی که میانگین ظرفیت جاسازی هر ۳ گروه برابر ظرفیت جاسازی در گروه ۲ شود.

برای مثال اگر مقدار $AvgC_{bpB}$ برابر ۷/۴ باشد، آنگاه ظرفیت جاسازی گروه‌های ۱، ۲ و ۳ را می‌توان به‌ترتیب از راست به چپ (۶، ۸ و ۱۰) و یا (۵، ۸ و ۱۱) انتخاب کرد.

برای تعیین میزان پیچیدگی موجود در هر بلاک، از نظر قرار گرفتن در نواحی لبه یا مسطح تصویر پوشانه، ابتدا مقدار انحراف معیار را برای چهار پیکسل موجود در داخل هر بلاک طبق رابطه (۹) محاسبه می‌شود. در این رابطه $(x_{i,1}, x_{i,2}, x_{i,3}, x_{i,4})$ $x_{i,j}$، نشان‌دهنده پیکسل‌های داخل بلاک i و m_i برابر میانگین مقادیر پیکسل‌های داخل بلاک iام است. دلیل اینکه در مخرج کسر رابطه (۹) به‌جای تعداد پیکسل‌های داخل هر بلاک (یعنی ۴)، از عدد ۳ استفاده شده است، این است که در ریاضیات آماری هنگامی‌که تعداد داده‌ها کم باشد برای محاسبه مقدار انحراف معیار، در مخرج کسر به‌جای N (تعداد کل داده‌ها)، از N-1 استفاده می‌شود [۲۴].

$$\text{deviate}_{b_i} = \sqrt{\sum_{j=1}^{4} \frac{(x_{i,j} - m_i)^2}{3}} \qquad (۹)$$

هر چه اختلاف بین مقادیر پیکسل‌ها از مقدار میانگین چهار پیکسل‌داخل بلاک بیشتر باشد، مقدار انحراف معیار در آن بلاک بیشتر است و پیکسل‌های تشکیل دهنده آن بلاک، بیشتر در نواحی لبه‌ای تصویر قرار می‌گیرند. با افزایش مقدار انحراف معیار در هر بلاک، مقاومت پیکسل‌های داخل آن بلاک نسبت به ایجاد تغییرات پس از جاسازی بیت‌های محرمانه بیشتر خواهد شد و می‌توان تعداد بیت بیشتری از داده‌های محرمانه را بدون ایجاد تغییرات قابل فهم برای چشمان انسان در آن بلاک پنهان کرد.

برای تعیین این موضوع که هر بلاک از نظر پیچیدگی، متعلق به کدام گروه‌است، مقدار انحراف معیار در هر بلاک، با تعدادی مقادیر آستانه‌ای مقایسه می‌شود. همیشه تعداد کل مقادیر آستانه‌ای باید یکی کمتر از تعداد کل گروه‌های موجود باشد. برای مثال با فرض انتخاب ۳ گروه، مقدار انحراف معیار در هر بلاک، طبق رابطه (۱۰) با دو مقدار آستانه‌ای th_1 و th_2 مقایسه می‌شود تا گروهی که بلاک مورد نظر به آن تعلق می‌گیرد و در پی آن ظرفیت جاسازی در آن بلاک به‌دست آورده شود.

$$gr_{b_i} = \begin{cases} 1 & if \quad 0 \le deviate_{b_i} < th_1 \\ 2 & if \quad th_1 \le deviate_{b_i} < th_2 \\ 3 & if \quad th_2 \le deviate_{b_i} \end{cases} \qquad (۱۰)$$

برای محاسبه دو مقدار آستانه‌ای th_1 و th_2، به‌گونه‌ای که ظرفیت مورد تقاضای کاربر را برآورده سازد، ابتدا باید بر اساس ظرفیت جاسازی در هر گروه و حجم کل داده‌های محرمانه،تعداد کل بلاک‌هایی که باید به هر یک از این گروه‌ها تعلق گیرد تا ظرفیت جاسازی در تصویر پوشانه برابر حجم کل داده‌های محرمانه کاربر شود مشخص شود. بدین منظور باید درصد فراوانی نسبی بلاک‌های متعلق به هر گروه را در تصویر پوشانه، طبق رابطه (۱۱) تعیین شود. در این رابطه cap_{gri} و P_{gri}، به‌ترتیب برابر ظرفیت گروه i و درصد فراوانی گروه i در کل تصویر پوشانه است.

$$\begin{aligned} Capacity &= t \times (P_{gr1} \times cap_{gr1} \\ &+ P_{gr2} \times cap_{gr2} + P_{gr3} \times cap_{gr3}) \end{aligned} \qquad (۱۱)$$

در این رابطه، حالت‌های مختلفی برای تأمین ظرفیت مورد تقاضای کاربر وجود دارد که بنابر مورد باید یکی از این حالات انتخاب شود. هر کدام از این حالات در مقایسه با حالت‌های دیگر کیفیت تصویر متفاوتی را نتیجه خواهد داد. شرایط $0\% \le P_{gr1}, P_{gr2}, P_{gr3} \le 100\%$ و $P_{gr1}+P_{gr2}+P_{gr3}=1$ باید همیشه میان درصد فراوانی نسبی گروه‌ها در رابطه بالا برقرار باشد. پس از تعیین مقادیر P_{gri}، برای محاسبه مقادیر آستانه‌ای th_1 و th_2 باید مقادیر انحراف معیار تمام بلاک‌های تصویر به‌صورت صعودی مرتب شده و در آرایه‌ای (dev) ذخیره شود. سپس طبق روابط (۱۳ و ۱۲) و با جایگذاری این مقادیر به‌عنوان اندیس در آرایه ذکر شده، مقادیر th_1 و th_2 را با فرض داشتن ۳ گروه به‌راحتی می‌توان محاسبه کرد.

$$th_1 = dev[P_{gr1} \times t] \qquad (۱۲)$$

$$th_2 = dev[P_{gr1} \times t + P_{gr2} \times t] \qquad (۱۳)$$

جاسازی: در این مرحله پس از تعیین پارامترهای مورد نیاز، بیت‌های محرمانه را بر اساس ظرفیت مشخص شده برای هر بلاک جاسازی می‌شود. برای جاسازی دنباله بیتی S_n در یک بلاک چهار پیکسلی، $\lceil n/2 \rceil$ بیت را در جفت پیکسل بالایی و $\lfloor n/2 \rfloor$ بیت را در جفت پیکسل پایینی مطابق روش پنهان‌نگاری غیرتطبیقی پیشنهادی زیر جاسازی می‌شود. در اینجا با اضافه کردن یک روال کاهش اختلال در روش چنگ و همکارانش [۱۷]، یک روش پنهان‌نگاری غیرتطبیقی جدید ارائه خواهد شد.

همان‌طور که گفته شد با استفاده از رابطه (۳) می‌توان به‌کمک یک تابع ترکیب، نحوه قرارگیری بیت‌ها با مقدار ۱ را در یک دنباله بیتی مشخص کرد. با توجه به رابطه (۵)، بیشینه مقدار به‌دست آمده برای تابع ترکیب C_k^n هنگامی است که k=n/۲ باشد. (در حالتی که n فرد باشد $k = \lfloor n/2 \rfloor . \lceil n/2 \rceil$). در این حالت با افزایش مقدار پیمانه دامنه تغییرات مجاز r_i نیز افزایش پیدا می‌کند و در نهایت موجب کاهش کیفیت تصویر استگو می‌شود. علاوه بر این، در حالتی که k=n و یا k=0 باشد، دیگر نیازی به استفاده از رابطه (۷) و تغییر پیکسل r_i نیست، زیرا تنها یک حالت برای قرارگیری بیت‌ها در دنباله وجود

خواهد داشت. درنتیجه می‌توان حالت‌های مختلفی را که K=n/۲ است و مقدار C_k^n نیز بالا است را تحت یک الگوی مشخص به حالت‌هایی که k=0 یا k=n است نگاشت داد و تغییرهای ایجاد شده در r_i را کاهش داد. در این حالت مقدار r'_i طبق رابطه (۱۴) محاسبه می‌شود. در این رابطه c برای مقادیر مختلف n، متفاوت است. (مثلاً در حالت‌هایی که n برابر ۵ و ۶ است c برابر ۵ و ۱۴ است). برای مثال در جدول (۱) این مقادیر برای حالت n=۵ مشاهده می‌شود:

$$f'(S_n) = r'_i \bmod n \quad if \quad (k=\lfloor n/2 \rfloor or \lceil n/2 \rceil) and \quad f(S_n) > c \quad (۱۴)$$

در جدول (۱) با اعمال این نگاشت، بیشینه انحراف ایجاد شده در r_i از ۵ واحد به ۲ واحد کاهش پیدا می‌کند. با استفاده از این روش، مقدار PSNR تصویر حاصل نسبت به روش چنگ و همکارانش حدود ۱dB افزایش پیدا می‌کند.

پس از جاسازی بیت‌های محرمانه داخل هر بلاک، باید مقدار انحراف معیار بلاک جدید با مقدار انحراف معیار بلاک اولیه در تصویر پوشانه در یک گروه قرار گیرد تا در مقصد به هنگام استخراج داده‌ها ظرفیت جاسازی هر بلاک استگو به‌طور صحیحی تشخیص داده شود. اگر گروه متعلق به بلاک استگو با بلاک اولیه متفاوت باشد، باید با استفاده از تابع پیمانه، حالت‌های مختلف دیگری را که می‌توان برای مقادیر پیکسل‌ها انتخاب کرد بررسی شود تا در نهایت بلاک جدید در همان گروهی قرار گیرد که بلاک تصویر پوشانه در آن قرار داشت.

جدول ۱. جدول نگاشت برای حالت n=۵

S_5	k	$f(S_n)$	Map to	K'	$f'(S_n)$
۰۰۰۰۰	۰	۰	→	۰	۰
۱۰۰۰۱	۲	۶	→	۰	۱
۱۰۰۱۰	۲	۷	→	۰	۲
۱۰۱۰۰	۲	۸	→	۰	۳
۱۱۰۰۰	۲	۹	→	۰	۴
۱۱۱۱۱	۵	۰	→	۵	۰
۱۰۱۱۰	۳	۶	→	۵	۱
۱۱۰۰۱	۳	۷	→	۵	۲
۱۱۰۱۰	۳	۸	→	۵	۳
۱۱۱۰۰	۳	۹	→	۵	۴

تعیین کلید پنهان‌نگاری: برای جاسازی و استخراج داده‌های محرمانه در تصویر پوشانه، دانستن ظرفیت هر گروه، تعداد گروه‌ها، حجم کل داده‌ها، مقادیر آستانه‌ای و عددی که به‌عنوان کلید در تولید اعداد تصادفی برای به‌دست آوردن ترتیب پیمایش بلاک‌ها استفاده شده است الزامی است. از این مقادیر می‌توان به‌عنوان یک دیکدر برای استخراج داده‌های محرمانه در این روش استفاده کرد و این مقادیر را به دنبال داده‌های محرمانه در تصویر پوشانه جاسازی کرد. اندازه این دیکدر بسیار ناچیز است و بخش بسیار کوچکی از ظرفیت جاسازی تصویر پوشانه را به‌خود اختصاص می‌دهد که می‌توان از آن صرف‌نظر کرد. از ترتیب پیمایش بلاک‌هایی که دیکدر در آنها جاسازی شده و همچنین طول پیام دیکدر، می‌توان به‌عنوان یک کلید محرمانه در این روش پنهان‌نگاری استفاده کرد. با وجود این کلید، امنیت روش تطبیقی پیشنهادی افزایش می‌یابد چرا که استخراج داده‌های محرمانه از تصویر استگو بدون دانستن مقدار این کلید ممکن نخواهد بود.

۳-۲. استخراج داده‌های محرمانه

روند استخراج داده‌های محرمانه از تصویر استگو به طور دقیق عکس روند جاسازی داده‌ها است. در ابتدا همانند مرحله جاسازی، تصویر استگو را به بلاک‌های چهار پیکسلی غیرهمپوشان تقسیم‌بندی کرده و سپس با استفاده از کلید پنهان‌نگاری، دیکدر از تصویر پوشانه استخراج می‌شود. با در اختیار داشتن دیکدر، تمام پارامترهایی که برای استخراج داده‌های محرمانه مورد نیاز است را در اختیار خواهیم داشت. سپس بر اساس ترتیب پیمایش بلاک‌ها، مقدار انحراف معیار در هر بلاک با استفاده از رابطه (۹)، محاسبه می‌شود. به‌کمک مقدار انحراف معیار بلاک و مقادیر آستانه‌ای‌طبق رابطه (۱۰)، گروه‌هایی که بلاک‌ها به آن تعلق می‌گیرند را مشخص کرده و پس از تعیین گروه‌ها با استفاده از مقادیر ظرفیت هر گروه که در دیکدر موجود است، تعداد بیتی که در هر بلاک از تصویر استگو جاسازی شده است تعیین می‌شوند.

با مشخص شدن ظرفیت هر بلاک، می‌توان تعداد بیتی را که در هر یک از جفت پیکسل‌های بلاک جاسازی شده است تعیین کرد به‌طوری‌که $\lceil n/2 \rceil$ بیت در جفت پیکسل بالایی و $\lfloor n/2 \rfloor$ بیت در جفت پیکسل پایینی جاسازی شده است. سپس با استفاده از روابط (۵ و ۴)، مقادیر k و $f(S_n)$ برای هر جفت از پیکسل مشخص می‌شود. اگر در جداول نگاشت، درآیه‌ای برای این مقادیر وجود داشت آنگاه مقادیر جدید k و $f(S_n)$ جایگزین مقادیر قبلی آن شده و در پایان با استفاده از رابطه (۶) دنباله بیتی‌که در آن بلاک جاسازی شده است استخراج می‌شود. در نهایت، داده‌های محرمانه از کنار هم قرار دادن دنباله‌های بیتی به‌دست آمده از هر بلاک استخراج می‌شود.

به‌عنوان مثال فرض می‌شود رشته S_9=۱۰۱۱۰۱۰۰۱ را در بلاک زیر با مقدار انحراف معیار ۴/۰۸۲و مقادیر آستانه th_1= و th_2= جاسازی کنیم:

۱۰۰	۱۰۸
۱۰۱	۱۰۷

با توجه به رابطه (۱۰)، این بلاک در گروه ۲ قرار می‌گیرد و باید پس از عملیات جاسازی نیز در همین گروه قرار گرفته شود. رشته ۱۰۱۱۰را در جفت پیکسل بالایی و رشته ۱۰۰۱ در جفت پیکسل پایینی پنهان می‌شود. چون در رشته اول n=۵ و k=۳ و $f(S_n)$=۶ است و این مقادیر در جدول نگاشت n=۵ نیز قرار دارند، درنتیجه

مقادیر k و $f(S_n)$ به‌ترتیب به ۵ و ۱ تغییر پیدا می‌کنند و با استفاده از رابطه (۱۴) در جفت پیکسل بالایی پنهان می‌شوند. پیکسل سمت چپ مقادیر ۹۵،۱۰۱،۱۰۷و ...، و پیکسل سمت راست مقادیر ۱۰۱،۱۰۶،۱۱۱و ...، را می‌توانند اختیار کنند.

$$f(10110)=\sum_{i=1}^{5-1} b_i C^i_{N(i)} = 1\times C^1_1 + 1\times C^2_2 + 0\times C^3_2 + 1\times C^4_3 = 6$$

برای جفت پیکسل پایینی با رشته ورودی ۱۰۰۱ نیز مشابه روش بالا عمل شود. بعد از مشخص شدن مقادیر ممکن برای هر جفت پیکسل در بلاک، حالتی که کمترین تغییر را در بلاک اولیه ایجاد می‌کند انتخاب کرده و مقدار انحراف معیار آن محاسبه می‌شود.

۱۰۱	۱۰۶
۱۰۲	۱۰۵

مقدار انحراف معیار بلاک جدید ۲/۳۸ است که در گروه ۱ قرار می‌گیرد. بنابراین حالت بعدی که کمترین تغییرات را در بلاک استگو ایجاد می‌کند انتخاب کرده و مقدار انحراف آن را محاسبه نموده و با دو مقدار آستانه مقایسه می‌شود. در این حالت مقدار انحراف ۴/۵ است که این مقدار در گروه ۲ قرار گرفته و با بلاک تصویر پوشانه در یک گروه قرار می‌گیرند و بلاک استگوی نهایی به‌دست می‌آید.

۹۹	۱۰۶
۹۷	۱۱۱

۴. نتایج پیاده‌سازی

در این بخش، نتایج به‌دست آمده از پیاده‌سازی روش پیشنهادی در این مقاله بررسی می‌شود. این نتایج با استفاده از نرم‌افزار MATLAB ۷/۱ برروی سیستم عامل Windows XP به‌دست آمده است. سخت‌افزار مورد استفاده در این پیاده‌سازی نیز شامل CPU ۳۰۰۰ AMD با ۲GB حافظه RAM است.

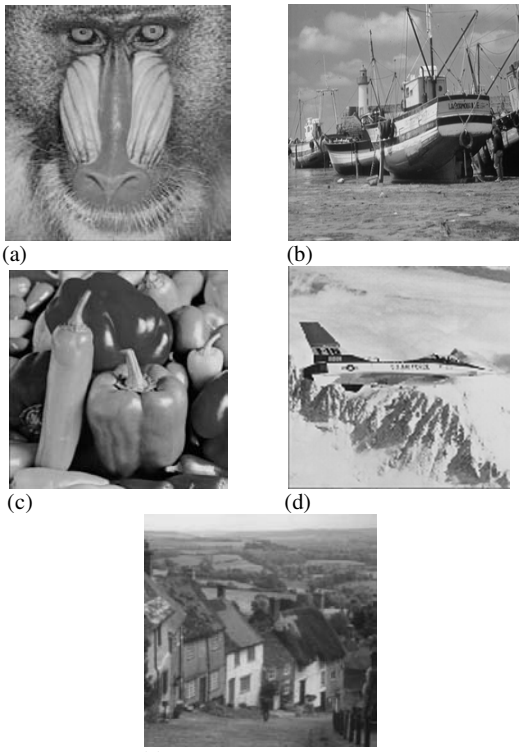
برای ارزیابی روش پیشنهادی از پنج تصویر پوشانه مشهور "Baboon", "GoldHill", "Plain", "Pepper","Boat" در مقیاس خاکستری با ابعاد ۵۱۲×۵۱۲ استفاده شده است (شکل ۱). همچنین به‌عنوان داده‌های محرمانه، از دنباله‌ای از اعداد شبه تصادفی که توسط نرم‌افزار Matlab تهیه شده، استفاده می‌شودکه می‌تواند نشانگر داده‌های محرمانه پس از عملیات فشرده‌سازی و رمزنگاری باشند.

در این مقاله، برای سنجش میزان کیفیت تصویر استگو از معیار کمّی PSNR[1] استفاده شده که طبق رابطه (۱۵) محاسبه می‌شود. در رابطه (۱۶) MSE برابر میانگین مربعات اختلاف مقادیر پیکسل‌های متناظر در تصویر پوشانه و تصویر استگو است.

$$PSNR = 10\log_{10}\frac{(2^b-1)^2}{MSE} dB \qquad (۱۵)$$

$$MSE = \left(\frac{1}{M\times N}\right)\sum_{i=0}^{M-1}\sum_{j=0}^{N-1}(C_{i,j}-S_{i,j})^2 \qquad (۱۶)$$

در این روابط، $C_{i,j}$ و $S_{i,j}$ به‌ترتیب برابر مقادیر پیکسل‌ها با مختصات i,j در تصویر پوشانه و تصویر استگو است. همچنین مقدار b نیز برابر عمق رنگ تصویر پوشانه است که در اینجا از تصاویر پوشانه با عمق رنگ ۸ بیت استفاده شده است. هنگامی‌که در تصاویر با مقیاس خاکستری مقدار PSNR بیشتر از dB باشد تفاوت بین تصویر پوشانه و تصویر استگو برای چشمان انسان قابل مشاهده نیست. یک مقدار PSNR بالا نشان می‌دهد که مقادیر پیکسلی تصویر استگو خیلی شبیه به تصویر پوشانه است.



شکل ۱. تصاویر پوشانه به‌کار رفته با ابعاد ۵۱۲×۵۱۲ [۲۵]
a) Baboon, b) Boat, c) Pepper, d) Plain, e) Goldhill

در جدول (۲) مقایسه نتایج پیاده‌سازی روش چنگ و همکارانش [۱۷] و روش غیرتطبیقی پیشنهادی در این مقاله نشان داده شده است. همان‌طور که در این جدول مشخص است، مقدار PSNR تصویر استگو در روش پیشنهادی غیرتطبیقی تحقیق حاضر بیشتر از روش غیرتطبیقی چنگ و همکارانش است.

در روش تطبیقی پیشنهادی تحقیق حاضر، پارامترهای مورد نیاز برای جاسازی اطلاعات را می‌توان بر حسب ظرفیت مورد تقاضای کاربر تعیین کردکه باعث می‌شود این روش از نظر ظرفیت مقیاس‌پذیر بوده و داده‌های محرمانه همیشه در تمام پیکسل‌های تصویر پوشانه پراکنده شوند. در شرایط مساوی هر چه تعداد گروه‌ها در تقسیم‌بندی بلاک‌ها بیشتر شود و فاصله بین گروه‌ها از نظر تعداد

[1] Peak Signal to Noise Ratio

بیت قابل جاسازی در هر گروه بیشتر شود، PSNR تصویر استگو حاصل کمتر می‌شود ولی با این وجود حساسیت چشم انسان نسبت به تشخیص انحراف در تصویر استگو کاهش پیدا می‌کند، در نتیجه باید تعادلی میان مقدار PSNR تصویر استگو حاصل و کیفیت بصری آن برقرار باشد. لازم به ذکر است که در آزمایشات این تحقیق، از سه گروه با اختلاف ظرفیت ۲ بیت استفاده شده است.

جدول ۲. مقایسه مقادیر PSNR بر حسب dB در حالتی که از تصویر Baboon به‌عنوان تصویر پوشانه استفاده شود.

$\|S_n\|$	ظرفیت (بیت)	PSNR (dB)	
		روش چنگ و همکارانش	روش پیشنهادی
۴	۵۲۴۲۸۸	۴۵	۴۵/۲۱۲
۵	۶۵۵۳۶۰	۴۱ /۶۵	۴۹۴۲/
۶	۷۸۶۴۳۲	۳۷ /۴۴	۳۸ /۴۸

جدول (۳)، نتایج آزمایش‌های گوناگون با مقادیر آستانه‌ای مختلف را برای روش پنهان‌نگاری تطبیقی پیشنهادی در ظرفیت‌های جاسازی مختلف نشان می‌دهد.

اگر هیستوگرام توزیع مقدار انحراف معیار بلاک‌های هر یک از تصاویر پوشانه رسم شود، می‌توان پیچیدگی تصویر پوشانه را از نظر تعداد نواحی لبه‌ای موجود در آن تعیین کرد. در این هیستوگرام هر چه مقادیر انحراف معیار بلاک‌ها در ناحیه وسیع‌تری بر روی نمودار توزیع شده باشد، تصویر پوشانه پیچیده‌تر و از نواحی لبه‌ای بیشتری تشکیل شده است.

با توجه به شکل (۲)، تصویر Baboon نسبت به دیگر تصاویر پوشانه به‌کار رفته در این مقاله پیچیده‌تر و دارای لبه‌های بیشتری است. از آنجایی‌که مقادیر انحراف معیار بلاک‌ها در تصویر Baboon در ناحیه وسیع‌تری بر روی نمودار توزیع شده است، مقادیر آستانه‌ای به‌دست آمده برای این تصویر در جدول (۳) نسبت به سه تصویر پوشانه دیگر بیشتر است. هر چه مقادیر آستانه بزرگ‌تر و فاصله آنها از هم بیشتر باشد، بلاک استگو حاصل پس از جاسازی بیت‌های محرمانه کمتر احتیاج به بازنگری و اصلاح پیدا می‌کند. در نتیجه تغییرات ایجاد شده در پیکسل‌های تصویر پوشانه کمتر می‌شود و مقدار PSNR تصویر استگوی حاصل در شرایط مساوی نسبت به سه تصویر پوشانه دیگر بیشتر خواهد شد.

شکل (۳) نشان دهنده اختلاف مقادیر پیکسل‌های متناظر در دو تصویر پوشانه و استگوی نظیر آن است. در این نوع تصاویر، هر چه اختلاف مقادیر دو پیکسل متناظر هم بیشتر باشد، پیکسل به‌دست آمده در تصویر تیره‌تر خواهد شد. با توجه به این شکل، می‌توان نتیجه گرفت که اختلاف مقادیر پیکسلی بین تصاویر پوشانه و استگو در نواحی لبه‌ای تصویر، بیشتر بوده است و تعداد بیت بیشتری از داده‌های محرمانه در این نواحی به نسبت نواحی صاف و هموار تصویر جاسازی شده است. از آنجایی‌که چشم انسان نسبت به تغییرات ایجاد شده در نواحی لبه‌ای تصویر به‌نسبت نواحی صاف و هموار آن، کمتر حساس است [۲۶]، تصاویر استگو ایجاد شده با استفاده از روش تطبیقی پیشنهادی، دارای کیفیت بصری بالایی هستند.

جدول (۴) مقایسه مقدار PSNR بین روش تطبیقی پیشنهادی و روش ارائه شده در مرجع [۱۹] را در شرایط تقریباً مساوی از نظر ظرفیت جاسازی نشان می‌دهد. در روش ارائه شده در مرجع [۱۹] به ویژگی‌های بافت تصویر توجهی نمی‌شود و مقاومت پیکسل‌های نواحی لبه‌ای تصویر نسبت به ایجاد تغییرات در مقادیر پیکسلی آنها نادیده گرفته می‌شود. به‌همین دلیل، کیفیت بصری تصویر استگوی حاصل در روش پیشنهادی تحقیق حاضر نسبت به این روش بسیار بالاتر است. در این روش بر اساس یک مقدار آستانه، در مورد جاسازی و یا عدم جاسازی بیت‌های محرمانه در پیکسل‌های تصویر پوشانه تصمیم‌گیری می‌شود. بنابراین در تمام پیکسل‌های تصویر پوشانه، بیت‌های محرمانه جاسازی نمی‌شود. علاوه بر این، همان‌گونه که در جدول (۴) مشخص است، مقدار PSNR تصویر استگو در روش پیشنهادی ما نسبت به روش ارائه شده در مرجع [۱۹] در ظرفیت‌های تقریباً برابر بالاتر است. در این جدول، پارامتر k برابر تعداد رنگ‌ها، و پارامتر th برابر حداکثر فاصله مجاز بین دو رأس از گراف، در مسئله رنگ‌آمیزی گراف است.

در جدول (۵) نتایج PSNR به‌دست آمده از روش تطبیقی پیشنهادی این تحقیق با نتایج به‌دست آمده در روش ارائه شده در مرجع [۲۰] برای چهار تصویر پوشانه مقایسه شده است. همچنین در این روش، در سطر اول و ستون اول از تصویر پوشانه اطلاعاتی جاسازی نمی‌شود. در این روش، برای تعیین ظرفیت جاسازی در هر پیکسل، تنها از دو پیکسل همسایه سمت بالا و سمت چپ پیکسل مذکور استفاده می‌شود. ولی در روش پیشنهادی تحقیق حاضر، ظرفیت جاسازی در هر بلاک بر اساس مقدار انحراف معیار بین چهار پیکسل موجود در هر بلاک تعیین می‌شود.

در روش ارائه شده در مرجع [۲۰]، در طول پیمایش تصویر پوشانه برای تعیین ظرفیت جاسازی پیکسل‌ها از مقادیر پیکسل‌های استگو همسایه یک پیکسل هدف که در مراحل قبلی به‌دست آمده است استفاده می‌شود و از بین انتخاب‌های ممکن برای مقدار نهایی پیکسل استگو، مقداری که کمترین اختلاف را با مقدار پیکسل هدف داشته باشد انتخاب می‌شود. در نتیجه، اگر پیکسلی در حین فرآیند جاسازی تغییرات زیادی نماید، این تغییرات در اطراف پیکسل مذکور انتشار پیدا می‌کند که در نهایت منجر به کاهش مقدار PSNR در تصویر استگو می‌شود. همان‌طور که در جدول (۵) مشخص است، مقدار PSNR در روش پیشنهادی، در ظرفیت‌های تقریباً برابر نسبت به روش اشاره شده [۲۰] بالاتر است. در این جدول $\lfloor \log_2 al \rfloor$، برابر حداقل تعداد بیت جاسازی شده در هر پیکسل از تصویر پوشانه است.

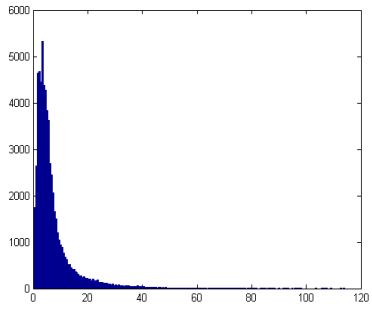
در جداول (۷ و ۶) نیز نتایج به‌دست آمده از روش پنهان‌نگاری

تطبیقی پیشنهادی، با روش‌های دیگر [۱۸ و ۸] مقایسه شده است. وجود چند مقدار آستانه‌ای برای تعیین سطوح بلاک‌های تصویر پوشانه و درنتیجه توجه بیشتر به نواحی بافت تصویر در روش تطبیقی پیشنهادی، باعث شده که با وجود ظرفیت‌های تقریباً یکسان، تصاویر استگو در روش پیشنهادی، از مقدار PSNR بالاتری در مقایسه با روش‌های ارائه شده در مراجع [۱۸ و ۸] برخوردار باشد.

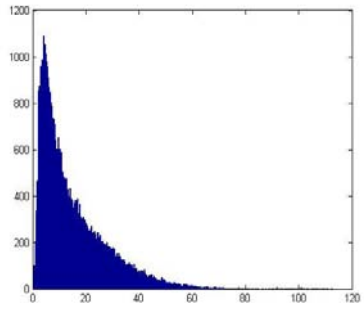
علاوه بر این، ظرفیت جاسازی در هر یک از دو روش بالا بسیار محدود است، در صورتی‌که در روش تطبیقی پیشنهادی، از نظر ظرفیت و کیفیت مقیاس‌پذیر بوده و می‌توان با تغییر پارامترها به ظرفیت مورد نظر کاربر دست پیدا کرد. همچنین در روش پیشنهادی، برخلاف روش ارائه شده در مرجع [۸] مشکل سرریز و فروریز بروز نمی‌کند.

جدول ۳. نتایج آزمایش‌های مختلف در روش تطبیقی پیشنهادی

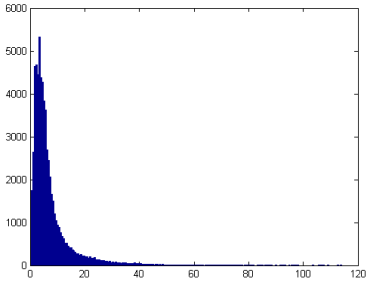
تصویر پوشانه	ظرفیت هر گروه	درصد فراوانی هر گروه	th_1 , th_2	ظرفیت	PSNR
Baboon	۴ ۶ ۸	۲۵ ۳۸ ۳۷	۵/۷ ،۱۵/۶۵	۴۰۹۱۰۲	۴۷/۴۲
	۳ ۵ ۷	۴۰ ۴۰ ۲۰	۸/۵۷ ،۲۴/۵۶	۳۰۱۵۱۸	۴۹/۵۶
	۶ ۸ ۱۰	۱۵ ۶۰ ۲۵	۴/۱۹ ،۲۸/۳۲	۵۲۴۳۰۰	۴۵/۱
	۴ ۸ ۱۲	۰ ۲۵ ۷۵	۰ ،۵/۷۳	۷۲۱۲۲۰	۳۹/۱۳
	۵ ۷ ۹	۲۶ ۴۹ ۲۵	۵/۹ ،۲۱/۴	۴۵۷۴۹۸	۴۶/۸
	۸ ۱۰ ۱۲	۴۰ ۴۰ ۱۵	۹/۶۹ ،۲۸/۲۶	۶۱۵۵۴۸	۴۲/۲۳
	۷ ۹ ۱۱	۴۰ ۴۰ ۲۰	۸/۵۶،۵۷/۲۴	۵۶۳۶۶۲	۴۳/۱۸
Boat	۴ ۶ ۸	۲۵ ۳۸ ۳۷	۲/۹۸ ،۶/۲۳	۴۰۹۴۶۶	۴۷/۳
	۳ ۵ ۷	۴۰ ۴۰ ۲۰	۴/۰۸ ،۹/۶۷	۳۰۲۲۲۰	۴۹/۳۷
	۶ ۸ ۱۰	۱۵ ۶۰ ۲۵	۲/۲۱ ،۸/۲۶	۵۳۸۲۴۶	۴۴/۵۵
	۴ ۸ ۱۲	۰ ۲۵ ۷۵	۰ ،۲/۹۸	۷۲۱۶۸۴	۳۹/۰۴
	۵ ۷ ۹	۲۶ ۴۹ ۲۵	۳ ،۸/۲۶	۴۵۸۰۱۲	۴۵/۹۸
	۸ ۱۰ ۱۲	۴۰ ۴۰ ۱۵	۴/۵ ،۱۱/۸۶	۶۱۶۲۹۸	۴۲/۱۱
	۷ ۹ ۱۱	۴۰ ۴۰ ۲۰	۴/۰۸ ،۸/۶۷	۵۶۸۵۳۲	۴۲/۸۹



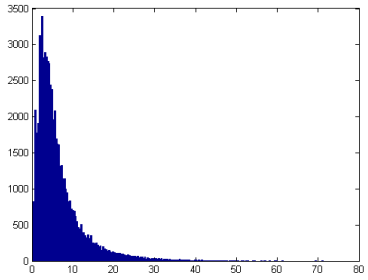
(Pepper)



(Baboon)

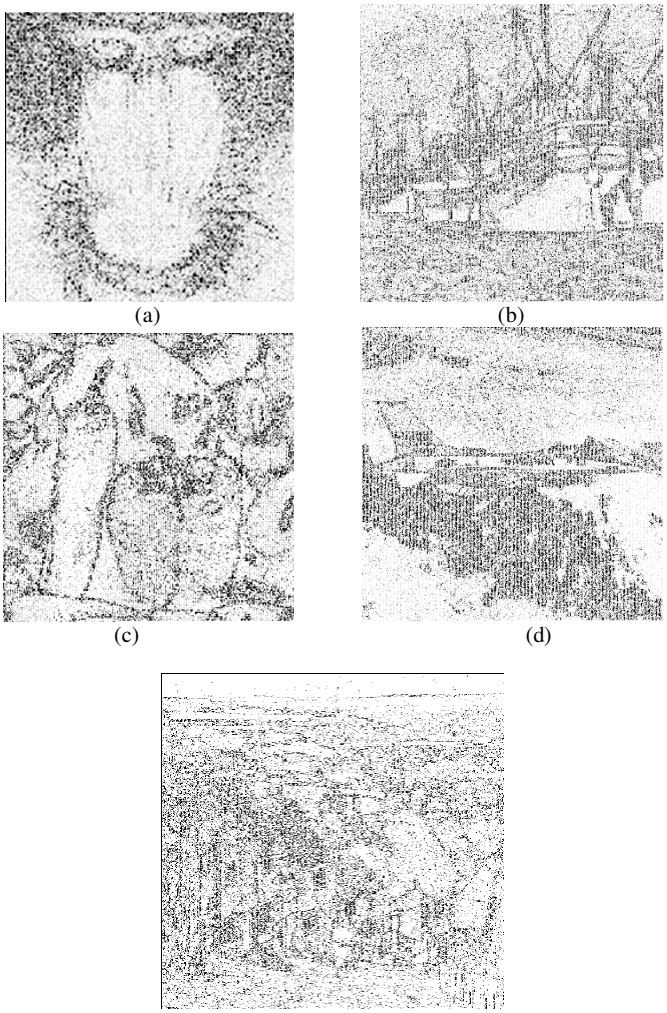


(Boat)



(GoldHill)

شکل ۲ . هیستوگرام پیچیدگی محلی بلاک‌ها در ۴ تصویر پوشانه (محور X نشان‌دهنده مقادیر انحراف معیار در بلاک‌ها و محور Y فراوانی نسبی این مقادیر را نشان می‌دهد)



شکل ۳. تصاویر به‌دست آمده از اختلاف مقادیر پیکسلی در تصاویر پوشانه و تصاویر استگو در روش تطبیقی پیشنهادی

جدول۴ . مقایسه نتایج به‌دست آمده در روش یو و همکارانش [۱۹] با روش پیشنهادی

تصویر پوشانه	روش یو و همکارانش [۱۹]			روش پیشنهادی			
	پارامترها	ظرفیت	PSNR	ظرفیت	گروه‌ها	th_1,th_2	PSNR
Baboon	K=۸ ,th=۸	۳۳۷۴۱۰	۴۷/۲۴	۳۵۴۰۸۶	۳ ۵ ۷	۵/۹ ،۱۶/۸۵	۴۸/۳۷
	K= ۱۶ ,th=۱۲	۴۵۹۴۵۶	۴۲/۸۷	۴۶۶۹۵۰	۵ ۷ ۹	۶/۵۵ ،۱۸/۲	۴۴/۴۶
	K=۱۶ ,th=۶	۴۴۵۹۸۰	۴۴/۳۶	۴۵۲۱۳۱	۵ ۷ ۹	۸/۵۷ ،۱۸/۲	۴۵/۹۳
	K=۱۶ ,th=۱۰	۵۲۴۲۸۸	۴۳/۸۷	۵۲۴۷۳۰	۶ ۸ ۱۰	۷/۵ ،۱۶/۴۵	۴۴/۵۱
	K=۳۲ ,th=۱۶	۶۵۴۶۵۵	۴۰/۷۴	۶۵۷۱۱۴	۸ ۱۰ ۱۲	۷/۴۴ ،۱۶/۸	۴۱/۰۸
Boat	K=۸ ,th= ۸	۳۳۹۷۳۲	۴۷/۳۹	۶۴۱۴۶۸	۳ ۵ ۷	۲/۹۸ ،۶/۴۸	۴۸/۵۵
	K=۱۶ ,th=۱۲	۴۵۱۲۰۸	۴۴/۴۷	۴۵۲۲۸۶	۵ ۷ ۹	۳/۳۶ ،۸/۲۶	۴۵/۹۹
	K=۱۶ ,th=۶	۴۵۰۲۲۰	۴۴/۳۸	۴۵۰۴۲۲	۵ ۷ ۹	۳/۴۱ ،۸/۳۲	۴۶/۰۲
	K=۱۶ ,th=۱۰	۵۲۴۲۸۸	۴۳/۸۹	۵۲۴۷۴۶	۶ ۸ ۱۰	۲/۲۸ ،۸/۲۶	۴۴/۶۸
	K=۳۲ ,th=۱۶	۶۵۵۲۰۵	۴۰/۸	۶۵۵۸۱۸	۸ ۱۰ ۱۲	۲/۹۸ ،۸/۲۶	۴۱/۱۱

جدول ۵. مقایسه نتایج به‌دست آمده در روش سیائو و همکارانش [۲۰] با روش پیشنهادی

تصویر پوشانه	روش سیائو و همکارانش			روش پیشنهادی			
	JND_al	ظرفیت	PSNR	ظرفیت	گروه‌ها	th_1,th_2	PSNR
Pepper	JND_2	۶۹۵۲۴۴	۳۵/۵۶	۶۹۶۴۶۴	۹ ۱۱ ۱۳	۳/۳ ،۵/۷۴	۳۹/۲۴
		۵۴۰۵۷۲	۴۱/۶۴	۵۴۱۷۶۶	۶ ۸ ۱۰	۲/۴۴ ،۴/۱۹	۴۴/۸۶
	JND_4	۷۵۳۱۷۸	۳۵/۷۷	۷۵۴۴۷۰	۱۰ ۱۲ ۱۴	۲/۵ ،۴/۵	۳۷/۹۴
		۶۶۴۹۶۴	۴۰/۳	۶۶۶۷۷۲	۸ ۱۰ ۱۲	۲/۶۳ ،۶/۶	۴۱/۴۱
Boat	JND_2	۶۵۷۴۶۸	۳۷/۰۲	۶۵۸۳۸۶	۸ ۱۰ ۱۲	۳/۲ ،۷/۲۵	۴۰/۸۹
		۵۴۰۹۸۶	۴۱/۰۱	۵۴۱۹۳۶	۶ ۸ ۱۰	۲/۸۷ ،۶/۳۸	۴۴/۱۷
	JND_4	۷۲۳۲۰۹	۳۷/۱۲	۷۲۳۸۷۸	۸ ۱۰ ۱۲	۱/۸۲ ،۳/۹۱	۳۹/۲۴
		۶۷۱۶۶۰	۳۹/۷۲	۶۷۳۳۳۰	۸ ۱۰ ۱۲	۲/۷۵ ،۶/۴۸	۴۰/۵۱

جدول ۶. مقایسه نتایج به‌دست آمده در روش ونگ و همکارانش [۸] با روش پیشنهادی

تصویر پوشانه	روش ونگ و همکارانش		روش پیشنهادی			
	ظرفیت	PSNR	ظرفیت	گروه‌ها	th_1 , th_2	PSNR
Baboon	۴۵۷۱۶۸	۴۰/۳	۴۵۷۴۹۸	۵ ۷ ۹	۵/۹ ، ۲۱/۴	۴۶/۰۵
Boat	۴۲۱۰۸۰	۴۲/۱	۴۲۲۳۱۸	۵ ۷ ۹	۴/۷۱ ، ۹/۶۷	۴۶/۷۶
Pepper	۴۰۷۲۵۶	۴۳/۳	۴۰۸۷۶۲	۴ ۶ ۸	۲/۲۱ ، ۴/۶۴	۴۷/۱۸
Plain	۴۰۳۵۹۲	۴۵/۳	۴۰۵۶۳۲	۴ ۶ ۸	۳/۳ ، ۵/۸۳	۴۶/۵۳
Goldhill	۴۱۲۸۲۴	۴۳/۵	۴۱۴۳۱۶	۴ ۶ ۸	۲/۲۱ ، ۴/۳۵	۴۷/۰۴

جدول ۷. مقایسه نتایج به‌دست آمده در روش یانگ و همکارانش [۱۸] با روش پیشنهادی

تصویر پوشانه	روش یانگ و همکارانش		روش پیشنهادی			
	ظرفیت	PSNR	ظرفیت	گروه‌ها	th_1 , th_2	PSNR
Baboon	۴۸۲۵۱۵	۶۴/۶۷	۴۵۷۴۹۸	۵ ۷ ۹	۵/۹ ،۲۱/۴	۴۶/۰۵
	۵۵۹۲۲۲	۳۴/۴۶	۵۶۳۶۶۲	۷ ۹ ۱۱	۸/۵۷ ،۲۴/۵	۴۳/۲۴
Pepper	۴۰۸۲۸۱	۴۰/۴۷	۴۰۸۷۶۲	۴ ۶ ۸	۲/۲۱ ،۴/۶۴	۴۷/۱۸
	۵۲۸۷۹۱	۳۶/۸۳	۵۳۰۱۰۶	۶ ۸ ۱۰	۲/۳۶ ،۵/۱۲	۴۴/۳۸
Boat	۴۱۰۱۹۹	۴۰/۷۴	۴۱۳۲۰۰	۴ ۶ ۸	۲/۲۶ ،۸/۳	۴۶/۹۹
	۵۲۷۸۴۶	۳۶/۵۴	۵۲۹۵۰۴	۶ ۸ ۱۰	۲/۱۵ ،۸/۳۹	۴۴/۳۱
GoldHill	۴۱۸۵۷۵	۴۰/۲۵	۴۱۸۳۵۸	۴ ۶ ۸	۲/۷۵ ،۵/۳۵	۴۷/۵۶
	۵۲۹۳۱۹	۳۷/۱۵	۵۲۹۹۳۸	۶ ۸ ۱۰	۳/۱ ،۶/۶	۴۵/۰۴

امنیت روش‌های ارائه شده در مراجع [۱۸ و ۸] به‌دلیل عدم وجود کلیدهای محرمانه پایین است، درحالی‌که در روش تطبیقی پیشنهادی، از چند کلید محرمانه برای جاسازی بیت‌های محرمانه در داخل تصویر پوشانه استفاده شده است. بنابراین، امنیت روش تطبیقی پیشنهادی تحقیق حاضر نسبت به دو روش دیگر بسیار بالاتر است.

در نهایت، نتایج مقایسات نشان می‌دهند که روش تطبیقی پیشنهادی از نقطه‌نظر ظرفیت جاسازی، و مقدار PSNR نسبت به روش‌های تطبیقی موجود برتری دارد.

در این قسمت مقاومت روش تطبیقی پیشنهادی در برابر روش‌های پنهان‌شکنی ارزیابی می‌شود.

روش تطبیقی پیشنهادی در این مقاله می‌تواند در برابر حمله مشهور پنهان‌شکنی RS [۱۵] از خود پایداری نشان دهد. همان‌طور که در جدول (۸) مشخص است، حمله پنهان‌شکنی RS، در تشخیص حضور پیام محرمانه جاسازی شده داخل تصاویر استگو تولید شده توسط روش تطبیقی پیشنهادی ناتوان است. در این جدول از ماسک‌های معمول M= [۰ ۱ ۱ ۰] و M=[۰ -۱ -۱ ۰] برای پیاده‌سازی الگوریتم RS استفاده شده است.

بر اساس الگوریتم RS [۱۵] و نتایج جدول (۸)، تعداد نسبی پیکسل‌های R_M و R_{-M}، S_M و S_{-M}، خیلی نزدیک به هم است. در

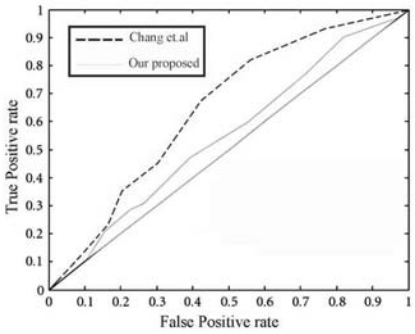
نتیجه الگوریتم پنهان‌شکنی RS نمی‌تواند حضور پیام محرمانه در تصاویر استگو به‌دست آمده از روش پنهان‌نگاری تطبیقی پیشنهادی را تشخیص دهد. علاوه بر این، با توجه به اینکه در شکل (۴) مساحت زیر منحنی ROC [۲۷] در روش پنهان‌نگاری پیشنهادی بیشتر است، بنابراین مقاومت روش پیشنهادی این تحقیق در مواجه با حمله RS نسبت به روش چنگ و همکارانش [۱۷] بیشتر و از امنیت بالاتری برخوردار است.

دسته دیگری از حملات پنهان‌شکنی بر پایه تحلیل هیستوگرام تصویر استگو عمل می‌کنند. در این روش‌ها هر چه هیستوگرام تصاویر استگو به هیستوگرام تصاویر پوشانه شبیه‌تر باشد، احتمال تشخیص وجود داده محرمانه در تصاویر استگو کاهش پیدا می‌کند و برعکس.

در شکل (۵) هیستوگرام تصاویر استگو و تصاویر پوشانه برای تعدادی از تصاویر رسم شده است. همان‌طور که در این شکل مشخص است، در هیستوگرام تصاویر پوشانه پس از جاسازی اطلاعات محرمانه تغییرات قابل توجهی اتفاق نیفتاده است. بنابراین، روش تطبیقی پیشنهادی مقاله حاضر، خصوصیات هیستوگرامی تصویر پوشانه را پس از جاسازی داده‌های محرمانه حفظ کرده است. در حالت کلی، برای نشان دادن میزان تشابه میان دو هیستوگرام تصویر، از ضریب همبستگی[1] بین دو هیستوگرام استفاده می‌شود. هر چه ضریب همبستگی به عدد ۱ نزدیک‌تر باشد، شباهت بین دو هیستوگرام بیشتر خواهد بود. ضریب همبستگی بین دو تصویر پوشانه و تصویر استگوی متناظر با آن، طبق رابطه زیر محاسبه می‌شود.

$$Corr = \frac{\sum_m \sum_n (C_{mn} - Avg(C_{mn}))(S_{mn} - Avg(S_{mn}))}{\sqrt{\left(\sum_m \sum_n (C_{mn} - Avg(C_{mn}))^2\right)\left(\sum_m \sum_n (S_{mn} - Avg(S_{mn}))^2\right)}} \quad (۱۷)$$

در این رابطه C_{mn} و S_{mn}، به‌ترتیب برابر مقدار پیکسلی تصویر پوشانه و تصویر استگو هستند. همچنین مقدار Avg(.)، برابر میانگین مقادیر تمام پیکسل‌های تشکیل‌دهنده تصویر خواهد بود.

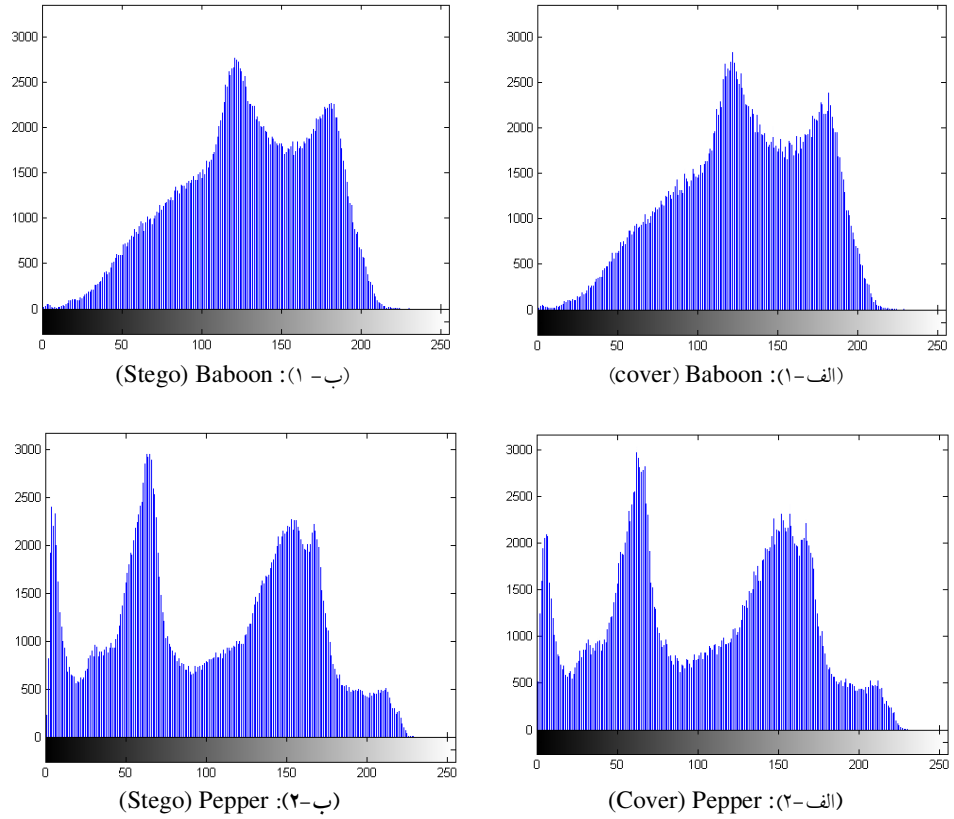


شکل ۴. منحنی‌های ROC برای نشان دادن کارایی حمله پنهان‌شکنی RS بر روی روش چنگ و همکارانش [۱۷] و روش تطبیقی پیشنهادی

جدول ۸. نتایج آماری به‌دست آمده از حمله RS بر روی تصاویر استگوی به‌دست آمده از روش پیشنهادی

تصویر پوشانه	ظرفیت	R_m	R_{-m}	S_m	S_{-m}
Baboon	۶۱۵۵۴۸	۲۳۰۹۱	۲۳۰۷۴	۲۰۰۴۲	۲۰۰۱۰
Boat	۵۴۱۹۳۶	۲۳۲۶۷	۲۳۲۳۳	۱۸۲۶۱	۱۸۲۸۰
Pepper	۵۶۳۹۰۴	۲۳۳۰۹	۲۳۱۸۰	۱۶۶۷۷	۱۶۸۱۱
GoldHill	۵۳۰۰۵۰	۲۴۱۷۶	۲۴۰۸۰	۱۸۱۱۴	۱۸۲۸۸
Plain	۵۶۳۹۴۲	۲۳۱۳۵	۲۳۰۳۴	۱۵۷۴۱	۱۵۶۳۷

[1] Correlation Coefficient



شکل ۵. هیستوگرام تصاویر پوشانه و تصاویر استگو به‌دست آمده با استفاده از روش تطبیقی پنهان‌نگاری پیشنهادی. ۱) تصویر Baboon با ابعاد ۵۱۲×۵۱۲ پیکسل، با جاسازی ۵۲۴۶۵۲ بیت و ضریب همبستگی ۲/۰/۹۹۹۵ ۲) تصویر Pepper با ابعاد ۵۱۲×۵۱۲ پیکسل، با جاسازی ۶۱۹۳۴۸ بیت و ضریب همبستگی ۰/۹۹۹۶

۵. نتیجه‌گیری

در این مقاله، دو روش جدید پنهان‌نگاری غیرتطبیقی و تطبیقی ارائه شده است. در روش غیرتطبیقی پیشنهادی، با استفاده از توابع پیمانه و ترکیب تعداد ثابتی از بیت‌های محرمانه در داخل هر بلاک دو پیکسلی از تصویر پوشانه جاسازی شده است. در این روش، با کاهش مقدار پیمانه سیستم برای پیکسل سمت راست در داخل بلاک، اختلال‌های ایجاد شده در این پیکسل پس از جاسازی بیت‌های محرمانه تا حد زیادی کاهش داده شد. با کاهش تغییرات پیکسل‌ها در تصویر، اختلاف مقادیر پیکسلی بین پیکسل‌های تصویر پوشانه و پیکسل‌های تصویر استگو کاهش پیدا کرده که در نهایت منجر به افزایش کیفیت تصویر استگو می‌شود.

در روش تطبیقی پیشنهادی که بر پایه روش غیرتطبیقی پیشنهادی عمل می‌کند، بر اساس مقدار انحراف معیار در هر بلاک چهار پیکسلی، از تصویر پوشانه و با استفاده از چند مقدار آستانه، بلاک‌های تصویر پوشانه بر اساس پیچیدگی محلی موجود در هر بلاک، به گروه‌های مختلف و با ظرفیت‌های جاسازی متفاوت تقسیم شده است. در این روش با بهره‌گیری از ضعف سیستم بینایی انسان نسبت به تشخیص تغییرات در نواحی لبه تصویر، تعداد بیت بیشتری از داده‌های محرمانه در نواحی لبه تصویر نسبت به نواحی صاف و هموار آن جاسازی شده است. همچنین، ظرفیت جاسازی در روش تطبیقی پیشنهادی مقیاس‌پذیر است و با تغییر پارامترهای الگوریتم می‌توان به ظرفیت مورد نیاز کاربر دست پیدا کرد. بنابراین نرخ جاسازی و اختلال تصویر استگو را می‌شود با توجه به کاربردهای عملی پنهان‌نگاری تنظیم کرد. از آنجایی‌که تغییرات ایجاد شده در نواحی لبه‌ای تصویر نسبت به نواحی هموار آن بیشتر است، کیفیت بصری تصویر استگو حاصل افزایش می‌یابد. امنیت روش تطبیقی پیشنهادی نیز به‌دلیل استفاده از پارامترهای مختلف، که هر کدام از آنها می‌تواند نقش یک کلید محرمانه را بین کاربران معتبر مبدأ و مقصد بازی کند، بسیار بالا است. همچنین این روش در برابر حملات آماری و هیستوگرامی پنهان‌شکنی مقاوم است و در برابر حمله معروف پنهان‌شکنی RS از خود مقاومت نشان می‌دهد. آزمایش‌ها نیز نشان می‌دهند که روش تطبیقی پیشنهادی نسبت به روش‌های تطبیقی اخیر، به‌میزان قابل توجهی از لحاظ کیفیت بصری بهتر برای تصاویر استگو، ظرفیت جاسازی بالاتر، انعطاف پذیری بیشتر، امنیت بالاتر و تشخیص سخت داده‌های محرمانه، به‌دلیل وجود کلیدهای محرمانه زیاد برتری دارد.

با گذشت زمان و پیشرفت تکنیک‌های محاسباتی، به مرور از امنیت روش‌های پنهان‌نگاری کاسته می‌شود. به‌همین دلیل در هر

زمان نیاز به ارائه روش‌های جدید در این زمینه بیشتر احساس می‌شود.

امروزه در اینترنت، بیشتر از تصاویر رنگی نسبت به تصاویر خاکستری استفاده می‌شود. بنابراین می‌توان روش‌های پیشنهادی در زمینه پنهان‌نگاری در این مقاله را بر روی تصاویر رنگی که شامل سه طیف قرمز و سبز و آبی هستند، گسترش داد. علاوه بر این، از آنجا که روش پنهان‌نگاری تطبیقی در این مقاله از امنیت، کیفیت، و انعطاف بالایی برخوردار است می‌توان با استفاده از این الگوریتم، روش‌های پنهان‌نگاری غیرتطبیقی دیگر را به روش‌های تطبیقی تبدیل کرد.

۶. مراجع

[1] Chedad, A.; Condell, J.; Curran, K.; Kevitt, P. M. "Digital Image Steganography: Survey and Analysis of Current Methods"; Signal Proc. 2010, 90, 727–752.

[2] Li, B.; Huang, J.; Shi, Y. Q. "A Survey on Image Steganography and Steganalysis"; J. Inf. Hiding Multimedia Signal Proc. 2011, 2 ,142-172.

[3] Chan, C. K.; Cheng, L. M. "Hiding Data in Images By Simple LSB Substitution"; Pattern Recogn. 2004, 37, 469–474.

[4] Lin, C. C.; Tsai, W. H. "Secret Image Sharing with Steganography and Authentication"; J. Sys. Software 2004, 73, 405-414.

[5] Wang, S. J. "Steganography of Capacity Required Using Modulo Operator for Embeding Secret Image"; Appl. Math. Comput. 2005, 164, 99-116.

[6] Yang, C. H. "Inverted Pattern Approach to Improve Image Quality of Information Hiding by LSB Substitution"; Pattern Recogn. 2008, 41, 2674–2683.

[7] Wu, D. C.; Tsai, W. H. "A Steganographic Method for Images by Pixel-Value Differencing"; Pattern Recogn. Lett. 2003, 24, 1613-1626.

[8] Wang, C. M.; Wu, N. I.; Tsai, C. S.; Hwang, M. S. "A High Quality Steganographyic Method with Pixel-Value Differencing and Modulus Function"; J. Sys. Software 2008, 81, 150-158.

[9] Chang, C. C.; Tseng, H. W. "A Steganographic Method for Digital Images Using Side Match"; Pattern Recogn. Lett. 2004, 25, 1431–1437.

[10] Loa, D. C.; Wu, N. I.; Wang, C. M.; Lin, Z. H.; Tsai, C. S. "A Novel Adaptive Steganography Based on Local Complexity and Human Vision Sensitivity"; J. Syst. Software 2010, 83, 1236-1248.

[11] Mahajan, M.; Kaur, N. "Adaptive Steganography: A Survey of Recent Statistical Aware Steganography Techniques"; J. Comput. Network Inf. Sec. 2012, 10, 76-92.

[12] Tiwari, N.; Shandilya, M. "Evaluation of Various LSB Based Methods of Image Steganography on GIF File Format"; Int. J. Comput. Appl. 2010, 6, 1-4.

[13] Huang, W.; Zhao, Y.; Ni, R. R. "Block Based Adaptive Image Steganography Using LSB Matching Revisited"; J. Elec. Sci. Tech. 2011, 9 , 291-296.

[14] Khaire, S. S.; Nalbalwar, S. L. "Review: Steganography – Bit Plane Complexity Segmentation (Bpcs) Technique"; Int. J. Eng. Sci. Tech. 2010, 2, 4860-4868.

[15] Fridrich, J.; Goljan, M.; Du, R. "Reliable Detection of LSB Steganography in Grayscale and Color Images"; Proc. of ACM Workshop on Multimedia and Security 2011, 27-30.

[16] Westfeld, A.; Pfitzmann, A. "Attacks on Steganographic Systems"; 3th Int. Workshop on Information Hiding, (IH'99), Springer-Verlag, 1999, 61-76.

[17] Chang, C. C.; Lin, C. Y.; Wang, Y. Z. "New Image Steganographic Methods Using Run-Length Approach"; Inf. Sci. 2006, 176, 3393-3408.

[18] Yang, C. H.; Weng, C. Y.; Tso, H. K.; Wang, S. J. "A Data Hiding Scheme Using the Varieties of Pixel-Value Diffrencing in Multimedia Images"; J. Syst. Software 2011, 84 , 669-678.

[19] Yue, S.; Wang, Z. H.; Chang, C. Y.; Chang, C. C.; Li, M. C. "Image Data Hiding Schemes Based on Graph Coloring"; Ubiquitous Intelligence and Computing 2011, 8 , 476-489.

[20] Hsiao, J. Y.; Chang, C. T.; "An Adaptive Steganographic Method Based on Measurement of Just Noticeable Disortion Profile"; Image Vision Computing 2010, 29, 155-166.

[21] Wu, H. C.; Wu, N. I.; Tsai, C. S.; Hwang, M. S. "Image Steganographic Scheme Based on Pixel- Value Differencing and LSB Replacement Methods"; IEE P-Vis. Image Sign. 2005, 152, 611-615.

[22] Yang, C. H.; Wang, S. J.; Weng, C. Y. "Analysis of Pixel-Value-Differencing Scheme with LSB Replacement in Steganography"; Intelligent Inf. Hiding and Multimedia Signal Proc. (JIHMSP2007), 3, 445-448.

[23] Chang, C. C.; Lee, J. S.; Lee, T. H. N. "Hybrid Wet Paper Coding Mechanism for Steganography Employing N-Indicator and Fuzzy Edge Detector"; Digital Signal Proc. 2010, 20, 1286-1307.

[24] Eslami, Z.; Ahmadabadi, J. "Secret Image Sharing with Authentication-Chaining and Dynamic Embedding"; J. Syst. Software 2011, 84, 803-809.(In Persian)

[25] Images Database: http://cpsipi.usc.edu/database.

[26] Al-Shatnawi, A. M. "A New Method in Image Steganography with Improved Image Quality"; Applied Mathematical Sci. 2012, 79, 3907-3915.

[27] Andrew, D. K. "Quantitative Evaluation of Pairs and RS Steganalysis"; Security, Steganography, and Watermarking of Multimedia Contents 2004, 83-97.