مجله ماشین‌بینایی و پردازش‌تصویر
سال چهارم، شماره اول، تابستان ۱۳۹۶

نهان نگاری ایمن مبتنی بر جاسازی ماتریسی جهت افزایش نرخ و بازدهٔ جاسازی

علیرضا پورمحمدعلی[۱]، مریم پورمحی‌آبادی[۲] و حسین نظام‌آبادی‌پور[۳]

چکیده

با پنهان‌سازی بیت‌های محرمانه در یک سیستم نهان نگاری تصویر، تصاویر حامل اطلاعات محرمانه دچار اعوجاج می‌شوند. این امر منجر به احتمال ظن دشمن به وجود پیام محرمانه در این تصاویر می‌شود. جاسازی ماتریسی از طریق تقسیم تصویر پوششی به بلوک‌های با طول مشخص و اعمال تغییرات محدود در هر بلوک، به کاهش اعوجاج ناشی از پنهان‌سازی اطلاعات محرمانه کمک می‌کند. با این حال، استفاده از این ساختار منجر به محدود شدن ظرفیت اطلاعات قابل پنهان سازی در تصاویر پوششی می‌شود. در این مقاله، ظرفیت سیستم جاسازی ماتریسی از طریق اصلاح روش فن افزایش می‌یابد. با افزایش حداکثر تعداد تغییرات در یک بلوک به ازای پنهان‌سازی تعداد بیت محرمانهٔ مشخص در هر بلوک، طول بلوک تصویر پوششی کاهش یافته و از این رو، نرخ جاسازی افزایش می‌یابد. همچنین به ازای ظرفیت یکسان، اعوجاج کاهش و بازدهٔ جاسازی افزایش می‌یابد. در این روش، تصاویر حامل با کیفیت مطلوب و PSNR بالا حاصل می‌شود. از طرفی، روش پیشنهادی منجر به افزایش مقاومت در برابر پنهان‌شکنی می‌شود. این امر، احتمال ظن دشمن به وجود پیام محرمانه در تصاویر حامل را کاهش داده و امنیت را افزایش می‌دهد. نتایج شبیه‌سازی، حاکی از عملکرد مناسب روش پیشنهادی در مقایسه با سایر روش‌های موجود در این زمینه است.

کلید واژه‌ها

نهان نگاری، جاسازی ماتریسی، نرخ جاسازی، بازدهٔ جاسازی، پنهان‌شکنی، PSNR

۱ مقدمه

با توجه به پیشرفت سیستم‌های ارسال اطلاعات دیجیتال و بهره‌مندی از کانال‌های عمومی همچون اینترنت، استفاده از ساختارهای ایمن جهت تبادل اطلاعات مهم و محرمانه در این‌گونه کانال‌ها اجتناب‌ناپذیر است.

نهان نگاری[1] علمی است که به ارسال اطلاعات محرمانه در کانال عمومی می‌پردازد، به گونه‌ای که دشمنی که به کانال دسترسی دارد، از وجود اطلاعات محرمانه و انتقال این گونه اطلاعات مطلع نشود. در رمزنگاری[2]، دشمن از وجود اطلاعات محرمانهٔ رمزشده در حین انتقال از طریق کانال مطلع بوده و دغدغهٔ آن، نحوهٔ رمزگشایی این اطلاعات رمزشده است. اما نهان نگاری با پنهان کردن حتی حضور اطلاعات محرمانه در فرآیند انتقال از طریق کانال، در پی افزایش ایمنی سیستم ارسال اطلاعات است [۱-۳]. به منظور پنهان سازی اطلاعات محرمانه در تصویر پوششی[3]، از دو

این مقاله در فروردین‌ماه ۱۳۹۵ دریافت، در تیرماه ۱۳۹۵ بازنگری و در مهرماه ۱۳۹۵ پذیرفته شد.

[۱] دانشگاه شهید باهنر کرمان، دانشکده مهندسی برق،
رایانامه: a.pmohamadali@eng.uk.ac.ir
[۲] دانشگاه شهید باهنر کرمان، دانشکده مهندسی برق،
رایانامه: pourmahyabadi@uk.ac.ir
[۳] دانشگاه شهید باهنر کرمان، دانشکده مهندسی برق،
رایانامه: nezam@uk.ac.ir

نویسنده مسئول: مریم پورمحی‌آبادی

[1] Steganography
[2] Cryptography
[3] Cover image

حوزهٔ مهم مکان[1] و تبدیل[2] استفاده می‌شود. در حوزهٔ مکان، پیکسل‌های تصویر پوششی مستقیما تحت اصلاح قرار گرفته، اما در حوزهٔ تبدیل ابتدا بر روی مقادیر پیکسل‌های پوششی، روابط ریاضی اعمال و سپس اصلاح بر روی ضرایب حاصل انجام می‌شود. مهم‌ترین روش مورد استفاده در حوزهٔ مکان روش LSB[3] است. اگرچه استفاده از این روش، منجر به دست یابی به ظرفیت و کیفیت بیشتر می‌شود، لیکن به راحتی می‌توان از طریق حملات پنهان شکنی[4] و تحلیل‌های آماری، به وجود پیام محرمانه در تصویر حامل[5] پی برد. از دیدگاه یک دشمن، پنهان شکنی هنر جلوگیری از ارتباطات پنهانی است. به عبارتی، به فرآیند تشخیص وجود اطلاعات محرمانه حین فرآیند ارسال، همچنین تشخیص و استخراج پیام محرمانه، پنهان شکنی می‌گویند [۴-۸].

جاسازی ماتریسی[6] یکی از شاخه‌های نهان نگاری است که به کاهش تغییرات ناشی از جاسازی پیام محرمانه در تصاویر پوششی می‌انجامد. این مفهوم برای اولین بار توسط کراندال[7] بیان شد. در این ساختارها، تصویر پوششی به بلوک‌های با طول مشخص تقسیم می‌شود. سپس با ساز و کاری مشخص، تعداد محدودی از درایه‌های هر بلوک اصلاح شده و پیام محرمانه از طریق این اصلاحات در تصویر پوششی، پنهان می‌شود. هدف اصلی این گونه ساختارها، افزایش بازدهٔ جاسازی[8] و کاهش اعوجاج تصاویر حامل ضمن دست‌یابی به نرخ جاسازی[9] مناسب است. طبق تعریف، تعداد متوسط بیت‌های محرمانه که به ازای یک تغییر جاسازی می‌شود، بازدهٔ جاسازی نامیده می‌شود. همچنین نرخ جاسازی، برابر با تعداد بیت محرمانه‌ای است که می‌تواند در هر پیکسل پنهان شود [۹-۱۱].

کارهای مختلفی در زمینهٔ جاسازی ماتریسی و کاربردهای آن انجام گرفته است. وستفلد[10] به معرفی یک روش جاسازی ماتریسی تحت عنوان الگوریتم F5 پرداخته است [۱۲]. در این روش، برای جاسازی پیام محرمانه، ابتدا تصویر پوششی به بلوک‌های با طول ثابت و مشخص تقسیم می‌شود. سپس تابع هش[11] برای بلوک‌های بدست آمده حساب می‌شود.

تسنگ[12] بخشی از یک تصویر پوششی باینری را استفاده کرده و پیام محرمانه را در آن پنهان می‌کند [۱۳]. ابتدا دو ماتریس باینری و ماتریس وزن، تولید و بین فرستنده و گیرنده به اشتراک گذاشته می‌شوند. سپس بر اساس این دو ماتریس، فرآیند جاسازی اطلاعات صورت می‌گیرد. فردریش[13] و سوکال[14]، به منظور افزایش بازدهٔ جاسازی در پنهان سازی پیام محرمانهٔ بزرگ[15]، از دو شیوه برای جاسازی ماتریسی در سیستم‌های نهان نگاری عملی استفاده کردند [۱۴]. اولی بر اساس کدهای سیمپلکس[16] و کدهای ساخته شده از آن‌ها عمل کرده و دومی از کدهای خطی تصادفی[17] با ابعاد کوچک استفاده می‌کند.

در [۱۵] جهت افزایش بازدهٔ جاسازی در تصاویر دیجیتال، هر رقم اطلاعات محرمانه در یک سیستم نوشتاری 2n+1 تایی[18] بوسیلهٔ n پیکسل پوششی حمل می‌شود. در این حالت، حداکثر یک پیکسل به میزان یک واحد افزایش و یا کاهش می‌یابد.

ژانگ[19] و همکارانش، یک طرح جاسازی دو لایه را مطرح کرده‌اند [۱۶]. به منظور تعیین اضافه و یا کم کردن مقادیر عددی پیکسل‌ها جهت جاسازی اطلاعات محرمانه، مکانیزم «Wet paper coding» معرفی شده است. با استفاده از دومین بیت کم ارزش، اطلاعات محرمانهٔ اضافی قابل انتقال بوده و از این رو، بازده و نرخ جاسازی افزایش می‌یابد.

مرجع [۱۷]، یک طرح نهان نگاری پیام محرمانهٔ بزرگ را معرفی می‌کند که در آن با استفاده از کد همینگ[20] (۴و۷) و ماتریس بررسی توازن[21]، بیت‌ها به صورت گروهی طبقه‌بندی می‌شوند. سپس، با استفاده از جاسازی LSB ساده، کم ارزش‌ترین بیت از هر هفت پیکسل تصویر پوششی، با یکی از رشته بیت‌های هفت بیتی جایگزین می‌شود. اگرچه کیفیت تصویر حامل کمی کاهش می‌یابد، اما نرخ جاسازی تا ۰/۹۹ بیت بر پیکسل افزایش می‌یابد.

در [۱۸]، روشی مبتنی بر جاسازی ماتریسی در حالت نهان نگاری فعال، بیان و از یک کد تصحیح خطا برای رفع مشکل عدم استحکام سیستم در مقابل خطا و حمله در کانال استفاده می‌شود. همچنین، برای کاهش قدرت آشکارسازی، از شیوه‌ای مبتنی بر

[1] Spatial domain
[2] Transforms domain
[3] Least Significant Bit
[4] Steganalysis
[5] Stego image
[6] Matrix Embedding (ME)
[7] Crandall
[8] Embedding efficiency
[9] Embedding rate
[10] Westfeld
[11] Hash function

[12] Tseng
[13] Fridrich
[14] Soukal
[15] Large payloads
[16] Simplex codes
[17] Random linear codes
[18] (2n + 1)-ary notational system
[19] Zhang
[20] Hamming code
[21] Parity check matrix

انتخاب تصادفی بلوک‌های DCT استفاده می‌شود. در این روش، بیت‌های محرمانه با استفاده از کدگذاری RA[1] کد می‌شوند.

جهت بهبود عملکرد روش نهان نگاری F5، محققان یک الگوریتم جاسازی ماتریسی بسط یافته را مطرح کرده‌اند که در آن به منظور پنهان کردن تعداد بیت محرمانهٔ بیشتر در تعداد مشخصی از بیت‌های تصویر پوششی، تغییراتی در تابع هش جاسازی ماتریسی ایجاد شده است [۱۹]. در این حالت، با استفاده از بسط چند لایه‌ای، بازده و نرخ جاسازی افزایش می‌یابند.

مرجع [۲۰] یک روش نهان نگاری سریع را برای سیستم‌های نهان نگاری بلادرنگ[2] تحت عنوان گسترش ماتریسی[3] ارائه می‌کند. این شیوه، منجر به کاهش پیچیدگی محاسباتی جاسازی ماتریسی مبتنی بر کدهای خطی تصادفی می‌شود. در این‌جا، با افزودن تعدادی ستون مرجع به ماتریس بررسی توازن، یک الگوریتم نهان نگاری سریع مطرح می‌شود.

در [۲۱]، فن[4] و همکارانش، روشی جهت بهبود بازدهٔ جاسازی جاسازی معرفی کرده‌اند که بهبود یافتهٔ روش [۱۳] است. با تغییر مقدار تنها یک پیکسل از بلوک به میزان یک واحد، تعداد بیت قابل جاسازی به ازای حداکثر یک تغییر، افزایش می‌یابد.

لیو[5] و همکارانش، با استفاده از پیچیدگی بلوک و جاسازی ماتریسی، یک الگوریتم نهان نگاری تطبیقی را معرفی کرده‌اند [۲۲]. تصویر پوششی به بلوک‌های هشت پیکسلی تقسیم شده، سپس بر اساس میزان پیچیدگی و با استفاده از کدهای خطی جاسازی ماتریسی، بیت‌های محرمانه به صورت تطبیقی جاسازی می‌شوند.

کیم[6] و یانگ[7] یک روش نهان نگاری بر اساس کد همینگ (۳و۵) ، ارائه کرده‌اند [۲۳]. با این روش، امکان جاسازی سه بیت محرمانه در پنج پیکسل تصویر پوششی و دست‌یابی به نرخ جاسازی ۰/۵۹۹، همچنین کیفیت بصری بیشتر تصاویر حامل فراهم شده است. این روش اگرچه نسبت به حالت جاسازی ماتریسی عادی (۳و۷)، چگالی تغییرات و اعوجاج بیشتری دارد، اما از نرخ و بازدهٔ جاسازی بیشتری برخوردار است.

مرجع [۲۴] با استفاده از کد همینگ و کد خطی تصادفی، یک الگوریتم سریع جاسازی ماتریسی را معرفی کرده است. بازدهٔ جاسازی روش پیشنهادی با روش‌های جاسازی ماتریسی مرسوم مشابه بوده، اما از پیچیدگی محاسباتی کمتری در نرخ‌های جاسازی پایین و متوسط برخودار است.

مرجع [۲۵] با هدف کاهش قابلیت آشکارسازی تصاویر حامل در حوزهٔ تبدیل، تصویر پوششی را به ضرایب مورفولوژیکی[8] نگاشت می‌کند. سپس بیت‌های محرمانه با جایگشت و به صورت جاسازی ماتریسی F5 در تصویر پوششی پنهان می‌شوند. استفاده از جاسازی ماتریسی، تعداد تغییرات لازم برای پنهان کردن بیت‌های محرمانه در ضرایب را به حداقل می‌رساند.

در این مقاله، روشی جهت افزایش حداکثر ظرفیت جاسازی ماتریسی تا میزان دو بیت بر پیکسل، جهت بازیابی بدون اتلاف پیام محرمانه ارائه می‌شود. این روش، که به نوعی بهبود یافتهٔ روش فن ([۲۱]) است، با کاهش طول هر بلوک تصویر پوششی خاکستری به ازای پنهان‌سازی تعداد بیت محرمانهٔ مشخص در هر بلوک، تعداد کل بلوک‌های پوششی و بنابراین تعداد کل بیت‌های محرمانهٔ قابل جاسازی در تصویر پوششی را افزایش می‌دهد. بنابر این حداکثرِ نرخ جاسازی تا دو برابر افزایش می‌یابد. به منظور کاهش تعداد عناصر هر بلوک، حداکثر تغییر ممکن در هر بلوک به دو تغییر افزایش می‌یابد. هدف از روش پیشنهادی، افزایش نرخ و بازدهٔ جاسازی و در عین حال، دست‌یابی به اعوجاج اندک تصاویر حامل و مقاومت بیشتر در مقابل حملات پنهان‌شکنی است. در ادامه و در بخش دوم، الگوریتم پایهٔ مورد استفاده در این مقاله معرفی می‌شود. سپس فرآیند روش جاسازی ماتریسی پیشنهادی، در بخش سوم توضیح داده می‌شود. بخش چهارم، نتایج شبیه‌سازی را ارائه می‌دهد، سپس تحلیل و مقایسه نتایج حاصل صورت می‌گیرد. در بخش آخر نیز، جمع بندی و نتیجه‌گیری ارائه خواهد شد.

۲ الگوریتم فن

به منظور بهبود بازدهٔ جاسازی در روش تسنگ، فن و همکارانش، روش جدیدی را ارائه کرده‌اند [۲۱]. در روش تسنگ، حداکثر تغییرات مجاز در هر بلوک، دو تغییر است و بلوک‌های تصویر پوششی به صورت بیتی است. در روش فن [۲۱]، عناصر بلوک‌های تصویر پوششی به صورت پیکسل‌های خاکستری بوده و تعداد تغییرات لازم برای پنهان‌سازی تعداد بیت مشخص در هر بلوک به حداکثر یک واحد کاهش می‌یابد. در این حالت، علاوه بر کاهش تغییرات، تعداد بیت قابل جاسازی در هر بلوک نیز افزایش می‌یابد. از این رو، بازدهٔ جاسازی در این روش نسبت به دیگر روش‌های جاسازی ماتریسی افزایش یافته است. با فرض اینکه ابعاد هر بلوک تصویر پوششی $m\times n$ بوده و تعداد بیت قابل جاسازی در هر بلوک برابر با r تعریف شود، مقدار r بر اساس رابطهٔ زیر بدست آمده و بیت‌های محرمانه به بلوک‌های r بیتی تقسیم می‌شوند.

$$r=\left\lfloor \log_2(2*m*n) \right\rfloor \qquad (۱)$$

همچنین، باید یک ماتریس وزن W تعریف و بین فرستنده و گیرنده به اشتراک گذاشته شود. این ماتریس دارای ابعاد $m\times n$ بوده

[1] Repeat Accumulate
[2] Real-time
[3] Matrix extending
[4] Fan
[5] Liu
[6] Kim
[7] Yang
[8] Morphological

و تمام اعداد بازهٔ $[0, 2^{r-1}]$ حداقل یک‌بار در این ماتریس آمده‌اند. به منظور تعیین محل اصلاح در هر بلوک، با فرض این که هر بلوک تصویر پوششی به صورت F_i و هر بلوک پیام محرمانه به صورت $B_i=[b_1,b_2,...,b_r]$ در نظر گرفته شود، یک مقدار اختلاف d طبق رابطه زیر محاسبه می‌شود.

$$d \equiv (b_1 b_2 ... b_r)_2 - SUM(F_i \otimes W) \pmod{2^r} \qquad (۲)$$

در این رابطه، $(b_1 b_2 ... b_r)_2$ مقدار دهدهی نظیر رشته بیت B_i و $\otimes$ نشانهٔ ضرب درایه به درایه در دو ماتریس است. همچنین، SUM بیانگر جمع تمامی درایه‌های یک ماتریس با یکدیگر و علامت mod به معنای محاسبهٔ باقیماندهٔ عدد بدست آمده بر 2^r است اکنون، بر اساس مقدار d بدست آمده، محل اصلاح در بلوک F_i تعیین می‌شود. چنان چه عدد d برابر با صفر باشد، نیازی به اصلاح بلوک F_i نیست؛ در غیر این صورت باید ماتریس F_i اصلاح شود. در این حالت، یک پیکسل از بلوک F_i اصلاح شده و مقدار آن به اندازهٔ یک واحد افزایش و یا کاهش می‌یابد. باید اصلاح به نحوی صورت گیرد که شرط زیر حاصل شود (F_i' حالت اصلاح شدهٔ بلوک F_i است).

$$SUM(F_i' \otimes W) \equiv (b_1 b_2 ... b_r)_2 \pmod{2^r} \qquad (۳)$$

بنابراین، برای بازیابی پیام محرمانه در گیرنده کافی است بلوک‌های F_i' بدست آمده از تصویر حامل، در رابطهٔ $SUM(F_i' \otimes W) \pmod{2^r}$ قرار گرفته و عدد حاصل از هر بلوک به فرم باینری r بیتی تبدیل شود. با کنار هم قرار دادن رشته بیت‌های r بیتی حاصل، پیام محرمانه بدست می‌آید. لازم به ذکر است، با توجه به اینکه در مرحلهٔ اصلاح بلوک‌ها، هر پیکسل تصویر پوششی ممکن است به میزان یک واحد افزایش و یا کاهش یابد، بنابراین در اولین گام از اجرای این الگوریتم، تمام پیکسل‌هایی که برابر با ۲۵۵ هستند به ۲۵۴ و پیکسل‌هایی که برابر با صفر هستند به یک تغییر می‌کنند. مثال زیر نحوهٔ فرآیند جاسازی و بازیابی اطلاعات محرمانه را نشان می‌دهد.

مثال ۲-۱:

چنان چه ابعاد هر بلوک تصویر پوششی برابر با ۳×۳ و بلوک‌های F_i و B_i و ماتریس وزن W به صورت زیر باشند،

$$F_i=\begin{bmatrix}12 & 66 & 7\\ 90 & 112 & 114\\ 240 & 230 & 78\end{bmatrix},\quad W=\begin{bmatrix}1 & 2 & 3\\ 4 & 5 & 6\\ 7 & 8 & 1\end{bmatrix},\quad B_i=1001$$

بر اساس رابطهٔ ۲ مقدار اختلاف d به صورت زیر بدست می‌آید.

$$SUM(F_i \otimes W)=5367=7 \pmod{2^4}$$
$$\Rightarrow d=(1001)_2-SUM=9-7=2$$

اکنون، با توجه به مقدار بدست آمده برای d، باید دو واحد به مجموع اضافه شود؛ که بر اساس W تعریف شده، باید درایهٔ $(1, 2)$ به میزان یک واحد افزایش یابد. بنابراین بلوک اصلاح شدهٔ F_i' به فرم زیر خواهد بود.

$$F_i'=\begin{bmatrix}12 & 67 & 7\\ 90 & 112 & 114\\ 240 & 230 & 78\end{bmatrix}$$

به منظور بازیابی B_i کافی است رابطهٔ زیر اعمال شود.

$$SUM(F_i' \otimes W) \pmod{2^4}=9=(1001)_2=(b_1 b_2 b_3 b_4)_2=(B_i)_2$$

۳ روش پیشنهادی

در روش جاسازی ماتریسی فن، ماتریس وزن W شامل همهٔ مقادیر صفر تا 2^{r-1} حداقل برای یک مرتبه است. بنابراین، ماتریس مذکور دارای عناصری اضافی خواهد بود. در این روش، هر بلوک تصویر پوششی حداکثر به میزان یک واحد تغییر می‌کند. در طرح جاسازی ماتریسی پیشنهادی، حداکثر تغییرات یک بلوک تصویر پوششی، به میزان دو واحد است. بنابراین، از یک ماتریس وزن W به ابعاد $1*p$ استفاده می‌شود که هریک از مقادیر صفر تا $2^{r-1}-1$ ، حداقل یکبار در آن وجود دارد. از این رو، تصویر پوششی به بلوک‌های با ابعاد $1*p$ پیکسلی F_i تقسیم می‌شود. در این‌جا، مقدار r طبق رابطه زیر بدست می‌آید.

$$r=\lfloor \log_2(p+1) \rfloor+1 \qquad (۴)$$

در واقع، باتوجه به امکان حداکثر دو تغییر در هر بلوک تصویر پوششی، طول بلوک‌های تصویر پوششی برای پنهان سازی تعداد مشخصی از بیت‌های محرمانه کاهش یافته است.

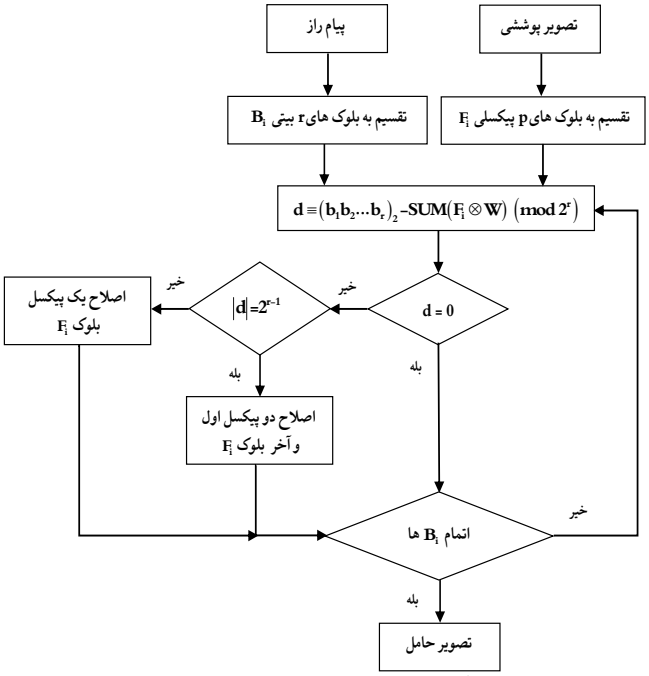
فلوچارت فرآیند جاسازی اطلاعات محرمانه در شکل ۱ آمده است. همچنین شبه کد مربوط به این فرآیند در شکل ۲ نشان داده شده است. بر این اساس، ابتدا تصویر پوششی به بلوک‌های $1*p$ پیکسلی F_i و پیام محرمانه به بلوک‌های r بیتی $B_i=[b_1,b_2,...,b_r]$ تقسیم می‌شوند. سپس برای هر بلوک، مقدار d به صورت زیر محاسبه می‌شود.

$$d \equiv (b_1 b_2 ... b_r)_2 - SUM(F_i \otimes W) \pmod{2^r} \qquad (۵)$$

چنان‌چه d مخالف صفر باشد، پیکسل‌های بلوک F_i باید اصلاح شوند. اگر $|d| \neq 2^{r-1}$ باشد، یکی از پیکسل‌های بلوک اصلاح شده و به میزان یک واحد افزایش و یا کاهش می‌یابد. در غیر این صورت، باید دو پیکسل اول و آخر از بلوک اصلاح شوند. فرآیند مذکور تا اتمام گروه‌های r بیتی B_i ادامه می‌یابد.

در این روش، ابتدا باید تمام مقادیر پیکسل‌های تصویر پوششی که برابر با صفر هستند به یک تبدیل شوند. همچنین، اگر p مخالف یک باشد، مقادیر ۲۵۵ باید به ۲۵۴ کاهش یابند؛ چرا که در مرحلهٔ اصلاح بلوک‌ها، هر پیکسل تصویر پوششی ممکن است به میزان یک واحد افزایش و یا کاهش یابد. طبق قرارداد، اگر p برابر با یک بوده و نیاز به دو اصلاح در بلوک تصویر پوششی باشد، مقدار پیکسل به میزان دو واحد "افزایش" می‌یابد. بنابراین،

اگر p برابر با یک باشد، ابتدا پیکسل‌هایی که برابر با ۲۵۵ و یا ۲۵۴ هستند به ۲۵۳ کاهش می‌یابند.



شکل۱ فلوچارت فرآیند جاسازی اطلاعات محرمانه در روش پیشنهادی

Algorithm: The embedding procedure for proposed ME

Inputs: cover image C, secret message S (Ns bits),
cover block size p, secret block size r, weight matrix W
Begin:
j=1
for i=1:r:Ns-r+1

$(b_1 b_2 ... b_r) = S(i : i + r - 1)$

$F = C(j : j + p - 1)$

$d \equiv (b_1 b_2 ... b_r)_2 - SUM(F \otimes W) \pmod{2^r}$

if $d \neq 0$ & $|d| \neq 2^{r-1}$

$F(|d|) = F(|d|) + sign(d) \times 1$

elseif $|d| = 2^{r-1}$

$F(1) = F(1) + 1$

$F(p) = F(p) + 1$

end if

$Stg(j : j + p - 1) = F$

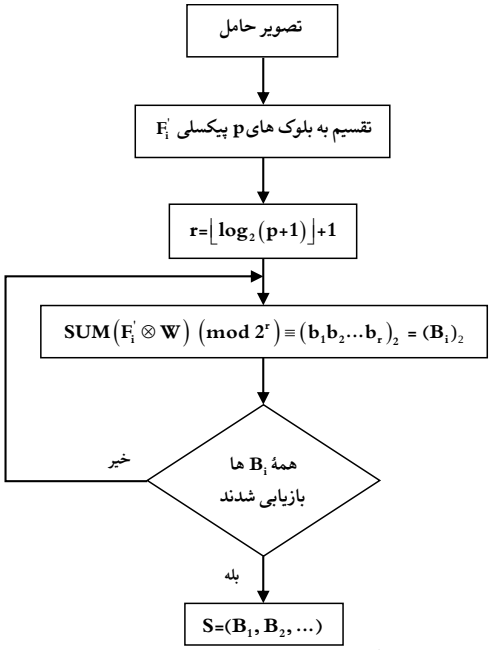
j=j+p
end for
End
Output: stego image Stg

شکل۲ شبه‌کد فرآیند جاسازی اطلاعات محرمانه در روش پیشنهادی

شکل ۳، فلوچارت مربوط به بازیابی پیام محرمانه در گیرنده را نشان می‌دهد. همچنین شبه کد مربوط به فرآیند بازیابی در شکل ۴ آمده است. به منظور بازیابی اطلاعات محرمانه، ابتدا تصویر حامل به بلوک‌های 1*p پیکسلی F_i' تقسیم می‌شود. سپس، برای هر گروه p پیکسلی حامل، مقدار SUM محاسبه می‌شود. یک گروه r بیتی محرمانه (B_i) به صورت زیر بدست می‌آید.

$$SUM(F_i' \otimes W) \pmod{2^r} \equiv (b_1 b_2 ... b_r)_2 = (B_i)_2 \quad (۶)$$

این فرآیند تا بازیابی تمامی گروه‌های r بیتی B_i ادامه می‌یابد. در نهایت، این گروه‌ها به هم ملحق شده و پیام محرمانهٔ اولیهٔ S را حاصل می‌کنند. همانطور که مشخص است، استفاده از ساختار پیشنهادی، منجر به بازیابی بدون اتلاف پیام محرمانه در گیرنده می‌شود.



شکل۳ فلوچارت فرآیند بازیابی اطلاعات محرمانه در روش پیشنهادی

Algorithm: The extraction procedure for proposed ME

Inputs: stego image Stg, cover block size p,
secret block size r, weight matrix W
Begin:
for i=1:r:Ns-r+1

$F' = Stg(j : j + p - 1)$

$(b_1 b_2 ... b_r)_2 \equiv SUM(F' \otimes W) \pmod{2^r}$

$S(i : i + r - 1) = (b_1 b_2 ... b_r)$

end for
End
Output: secret message S

شکل۴ شبه‌کد فرآیند بازیابی اطلاعات محرمانه در روش پیشنهادی

در اینجا، به منظور درک بهتر ساز و کار روش پیشنهادی، دو مثال مطرح می‌شود.

مثال ۳-۱:

با فرض p=7 ، از رابطه ۴، مقدار r به صورت زیر محاسبه می‌شود:

$$r=\lfloor \log_2(7+1) \rfloor + 1 = 4$$

و با فرض این که رشته بیت محرمانهٔ B_i و بلوک F_i به صورت زیر باشند،

$$F_i=[100\ 56\ 89\ 114\ 252\ 80\ 120],\ B_i=1010$$

و با در نظر گرفتن W به صورت زیر،

$$W=[1\ 2\ 3\ 4\ 5\ 6\ 7]$$

مقادیر SUM و d به صورت زیر محاسبه می‌شوند:

$$SUM(F_i \otimes W)=3515=11(\mathrm{mod}\ 2^4)$$

$$\Rightarrow d=(1010)_2\text{-SUM}=10-11=-1 \Rightarrow |d| \neq 2^{r-1}$$

بنابر این بلوک F_i به این صورت اصلاح می‌شود که پیکسل اول از بلوک F_i که متناظر با مقدار یک در ماتریس وزن W است، به میزان یک واحد کاهش می‌یابد.

$$F_i'=[99\ 56\ 89\ 114\ 252\ 80\ 120]$$

به منظور بازیابی کافی است F_i' در رابطه زیر قرار گیرد.

$$SUM(F_i' \otimes W)\ (\mathrm{mod}\ 2^4)=10=(1010)_2=(b_1b_2b_3b_4)_2=B_i$$

مثال ۳-۲:

چنان‌چه این بار بلوک محرمانه به صورت $B_i=0011$ باشد، مقدار d به صورت زیر بدست می‌آید:

$$d=(0011)_2\text{-SUM}=3-11=-8 \Rightarrow |d|=2^{r-1}$$

بنابر این، برای اصلاح بلوک F_i باید پیکسل اول و آخر از بلوک به میزان یک واحد افزایش یابند. بلوک اصلاح شده به صورت زیر بدست می‌آید.

$$F_i'=[101\ 56\ 89\ 114\ 252\ 80\ 121]$$

در مرحلهٔ بازیابی، مطابق رابطهٔ زیر رشته بیت B_i استخراج می‌شود.

$$SUM(F_i' \otimes W)\ (\mathrm{mod}\ 2^4)=3=(0011)_2=(b_1b_2b_3b_4)_2=B_i$$

۴ پیاده‌سازی، تحلیل و ارزیابی نتایج

۴-۱ پایگاه داده

جهت پیاده‌سازی روش پیشنهادی، ۱۰ تصویر پوششی استاندارد مطابق شکل ۵، همچنین پایگاه دادهٔ [۲۶] مورد استفاده قرار می‌گیرند. تصویر محرمانهٔ مورد استفاده نیز در شکل ۶ آمده است. تمام تصاویر، به صورت خاکستری ۸بیتی مورد استفاده قرار گرفته‌اند. لازم به ذکر است، به منظور حفظ کیفیت طبیعی تصاویر پوششی، برش ۵۱۲×۵۱۲ پیکسلی از تصاویر پایگاه دادهٔ [۲۶] مورد استفاده قرار می‌گیرد.

۴-۲ معیارهای ارزشیابی

۴-۲-۱ پارامترهای جاسازی ماتریسی

با توجه به تعاریف نرخ و بازدهٔ جاسازی که در بخش یک مطرح شد، روابط مربوط به پارامترهای جاسازی ماتریسی به صورت زیر است:

نرخ جاسازی R:

$$R=\frac{r}{p} \qquad (۷)$$

بازدهٔ جاسازی E:

$$E=\frac{R}{D} \qquad (۸)$$

در رابطهٔ فوق، D چگالی تغییرات است. برای مثال، در وضعیتی که حداکثر یک عضو از بلوک به میزان یک واحد تغییر می‌کند (تنها افزایش و یا تنها کاهش برای هر عضو مجاز باشد)، امکان p+1 رخداد وجود دارد؛ یک رخداد مربوط به عدم تغییر در بلوک و p رخداد مربوط به تغییر هر کدام از p پیکسل بلوک است. در این صورت، چگالی تغییرات D به صورت زیر خواهد بود:

$$D=\frac{\frac{p}{p+1}.1+\frac{1}{p+1}.0}{p}=\frac{1}{p+1} \qquad (۹)$$

شکل۵ تصاویر پوششی

شکل۶ تصویر محرمانه

۴-۲-۲ PSNR و MSSIM

برای بررسی تأثیر روش پیشنهادی بر کیفیت تصاویر حامل، از معیار PSNR[1] استفاده می‌شود. این معیار بر حسب dB به صورت زیر محاسبه می‌شود [۲۷]:

$$PSNR=10\times\log\left(\frac{C_{max}^2}{MSE}\right) \qquad (۱۰)$$

$$MSE=\frac{1}{M\times N}\sum_{x=1}^{M}\sum_{y=1}^{N}\left(S_{xy}-C_{xy}\right)^2 \qquad (۱۱)$$

در این رابطه، x, y مختصات تصویر، M, N ابعاد تصویر و S_{xy} ,C_{xy} به ترتیب تصاویر پوششی و حامل هستند. با توجه به استفاده از تصاویر خاکستری، C_{max} برابر با ۲۵۵ است. هر چه اختلاف بین تصاویر پوششی و حامل بیشتر باشد، MSE[2] افزایش یافته و PSNR کاهش می‌یابد. بنابراین، PSNR بیشتر به معنای اعوجاج کمتر و کیفیت بیشتر تصاویر حامل بدست آمده است.

همچنین بمنظور اندازه‌گیری تشابه بین تصاویر پوششی و حامل، از شاخص SSIM[3] استفاده می‌شود. SSIM مطابق رابطهٔ زیر تعریف می‌شود [۲۸]:

$$SSIM(x,y)=\frac{(2\mu_x\mu_y+C_1)(2\sigma_{xy}+C_2)}{(\mu_x^2+\mu_y^2+C_1)(\sigma_x^2+\sigma_y^2+C_2)} \qquad (۱۲)$$

در رابطهٔ فوق، μ_i شدت متوسط سیگنال i، σ_i انحراف معیار سیگنال i و σ_{xy} کواریانس x,y است. همچنین C_1, C_2 ثابت‌های پایداری هستند. بر این اساس، MSSIM[4] به صورت زیر بیان می‌شود:

$$MSSIM(X,Y)=\frac{1}{M}\sum_{j=1}^{M}SSIM(x_j,y_j) \qquad (۱۳)$$

در این رابطه، X,Y تصاویر اصلی و اعوجاج یافته، M تعداد پنجره‌های تصویر و x_j ,y_j مربوط به پنجرهٔ jام تصاویر هستند. هر چه این شاخص به یک نزدیک‌تر باشد، شباهت بین دو تصویر بیشتر است. این شاخص به تفصیل در [۲۸] مورد بررسی قرار گرفته است.

[1] Peak Signal to Noise Ratio
[2] Mean Squared Error
[3] Structural SIMilarity
[4] Mean SSIM

۴-۲-۳ پنهان‌شکنی AUMP

در [۲۹] یک روش پنهان‌شکنی تحت عنوان AUMP[5]، به منظور آشکارسازی حضور بیت‌های محرمانه در تصاویر خاکستری مطرح شده است. در این مقاله، یک تست آماری تطبیقی جهت دست‌یابی به احتمال بالا در آشکارسازی حضور بیت‌های محرمانه بیان شده است. در این تست، توزیع احتمال مستقل از پارامترهای مجهول تصویر است. با استفاده از روابط و مدل سازی‌های آماری، تابع توان[6] β_φ بوسیلهٔ احتمال آشکارسازی بیت‌های محرمانه تعریف شده و بر اساس آن، تحلیل تصاویر صورت می‌گیرد. جزئیات مربوط به روابط و محاسبات در [۲۹] آمده است.

۴-۳ ارزیابی عملکرد روش پیشنهادی

در این مقاله، از سه روش LSB ساده، F5 و روش فن برای قیاس و ارزیابی عملکرد روش پیشنهادی استفاده می‌شود. در روش LSB ساده، بیت‌های کم ارزش هر پیکسل تصویر پوششی با بیت‌های محرمانه جایگزین می‌شوند. روش فن نیز در بخش دوم، مورد بررسی قرار گرفت.

در روش F5، چنانچه بلوک n بیتی تصویر پوششی به صورت $a=a_1,a_2,\ldots,a_n$ باشد، تابع هش به صورت زیر تعریف می‌شود.

$$f:f(a)=\bigoplus_{i=1}^{n}a_i.i \qquad (۱۴)$$

در این رابطه، i به صورت باینری r بیتی قرار داده می‌شود. علامت $\oplus$ بیان‌گر یای انحصاری است و f یک رشتهٔ r بیتی خواهد بود. اگر طبق رابطهٔ زیر، مقدار هش f و رشتهٔ r بیتی محرمانهٔ s، یای انحصاری[7] شده و سپس رشته باینری حاصل به دهدهی تبدیل شود، مکان بیت اصلاح شونده در بلوک a مشخص می‌شود.

$$y=s\oplus f(a) \qquad (۱۵)$$

چنانچه مقدار دهدهی y = 0 باشد، نیازی به تغییر در بیت‌های بلوک نبوده، در غیر اینصورت بیت y ام از بلوک a باید برعکس شود.

۴-۴ تحلیل و مقایسه

۴-۴-۱ نرخ و بازدهٔ جاسازی

نرخ جاسازی و بازدهٔ جاسازی دو ویژگی مهم جهت بررسی عملکرد روش پیشنهادی هستند. شکل‌های ۷ و ۸ منحنی‌های مربوط به نرخ و بازدهٔ جاسازی را بر حسب pهای مختلف برای سه روش جاسازی ماتریسی F5، فن و روش پیشنهادی نشان می‌دهند.

[5] Asymptotically Uniformly Most Powerful
[6] Power function
[7] Exclusive or (XOR)

همانطور که مشاهده می‌شود، هر دو روش فن و روش پیشنهادی از نرخ و بازدهٔ جاسازی بیشتری نسبت به روش F5 برخوردارند. بر طبق منحنی نرخ جاسازی، روش پیشنهادی از نرخ جاسازی بالاتری نسبت به روش فن، خصوصا در مقادیر کوچک p، بهره می‌برد. این امر امکان دست‌یابی به طرح نهان نگاری ماتریسی با ظرفیت بالا را فراهم می‌آورد.

با توجه به اینکه در روش پیشنهادی، در حالت ظرفیت بهینه (کمترین p برای پنهان کردن r بیت جهت دست‌یابی به حداکثر ظرفیت)، تعداد درایه‌های بلوک تصویر پوششی نسبت به روش فن به میزان یک واحد کاهش می‌یابد، بنابراین نرخ جاسازی افزایش می‌یابد. پس از طرفی، اعوجاج در روش پیشنهادی اندکی افزایش یافته (به علت احتمال رخداد حداکثر دو تغییر) و از طرف دیگر نرخ افزایش می‌یابد. با توجه به اینکه بازدهٔ جاسازی بصورت نسبت نرخ بر اعوجاج ($E=R/D$) تعریف می‌شود، افزایش نرخ در جهت جبران کاهش بازدهٔ ناشی از افزایش اعوجاج عمل می‌کند. بنابراین همانطور که در شکل ۸ مشاهده می‌شود، منحنی‌های بازدهٔ جاسازی دو روش فن و پیشنهادی نزدیک به هم هستند. لازم به ذکر است، نحوهٔ تاثیر افزایش اعوجاج ناشی از این روش، در بخش ۴-۴-۳ مورد بررسی قرار می‌گیرد.

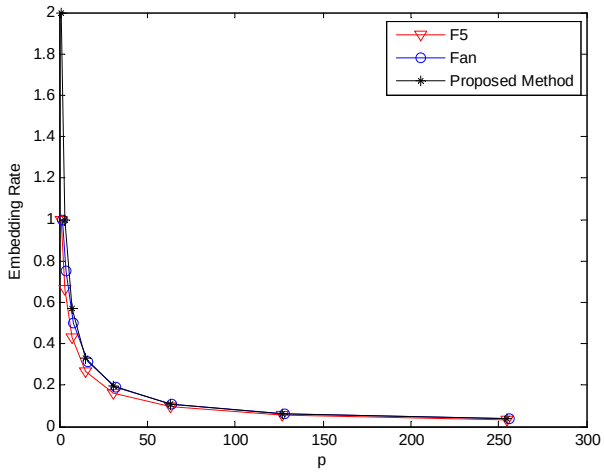
همچنین مطابق شکل ۸، در ظرفیت یکسان یک بیت بر پیکسل (نرخ جاسازی برابر)، بازدهٔ جاسازی روش فن و روش پیشنهادی به ترتیب برابر با ۲/۶۶ و ۳ است. بنابراین، تحت نرخ جاسازی یکسان، بازدهٔ جاسازی روش پیشنهادی بیشتر است.

جدول ۱ ، تأثیر روش پیشنهادی بر افزایش نرخ جاسازی را به صورت دقیق‌تر نشان می‌دهد. در این جدول، تعداد بیت قابل جاسازی در سه روش F5، فن و روش پیشنهادی در یک تصویر پوششی با ابعاد ۵۱۲×۵۱۲ پیکسل در حالات مختلف (r, p) مورد مقایسه قرار گرفته است (در هر روش، حد پایین p به ازای r مشخص، جهت دست‌یابی به حداکثر نرخ جاسازی مورد استفاده قرار گرفته است). همانطور که ملاحظه می‌شود، استفاده از ساختار پیشنهادی موجب افزایش ظرفیت سیستم نهان نگاری، به ویژه در مقادیر کوچک‌تر p می‌شود. نکتهٔ حائز اهمیت، حداکثر ظرفیت سیستم در روش پیشنهادی است که نسبت به روش‌های F5 و فن به ترتیب ۳ و ۲ برابر افزایش یافته است.

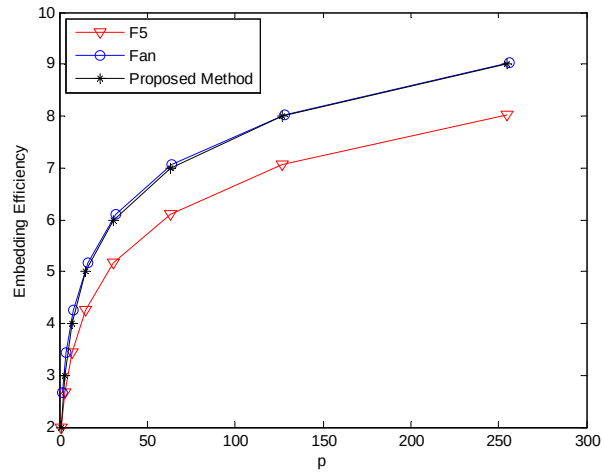
۴-۴-۲ کیفیت تصاویر حامل

با توجه به عدم بهره‌مندی روش‌های ماتریسی پیشین از ظرفیت ۲ بیت بر پیکسل، روش پیشنهادی با روش LSB ساده مقایسه می‌شود. جدول ۲ نتایج مربوط به میزان متوسط PSNR و MSSIM تصاویر حامل را در دو روش LSB ساده و جاسازی ماتریسی پیشنهادی، با ظرفیت یکسان دو بیت بر پیکسل برای تصاویر استاندارد و همچنین پایگاه دادهٔ [۲۶] نشان می‌دهد (تصاویر پوششی با ابعاد ۵۱۲×۵۱۲ و تصویر محرمانه با ابعاد ۲۵۶×۲۵۶). نتایج نشان می‌دهد که روش پیشنهادی با کاهش تغییرات تصویر پوششی، PSNR تصویر حامل را حدود ۱/۸ dB افزایش داده و MSSIM نیز به میزان ایده‌آل یک نزدیک‌تر شده است.

همچنین جدول ۳، مقادیر متوسط PSNR و MSSIM تصاویر حامل در روش‌های F5، روش فن و روش پیشنهادی، تحت ظرفیت یکسان یک بیت بر پیکسل را مقایسه می‌کند. ابعاد تصویر محرمانهٔ مورد استفاده در این قسمت به صورت ۱۲۸×۲۵۶ است. با توجه به کاهش تغییرات تصویر پوششی در روش پیشنهادی، PSNR تصاویر حامل نسبت به روش F5 حدود ۱/۷ dB افزایش می‌یابد.



شکل۷ مشخصه نرخ جاسازی در روش‌های مختلف



شکل۸ منحنی بازدهٔ جاسازی در روش‌های مختلف

با توجه به نتایج بدست آمده، کیفیت تصاویر حامل در روش پیشنهادی نسبت به روش فن در ظرفیت برابر یک بیت بر پیکسل (حداکثر ظرفیت ممکن در روش فن) افزایش یافته است. علت این امر را می‌توان در منحنی شکل ۸ جستجو کرد. همانطور که بیان شد، در ظرفیت یک بیت بر پیکسل، که معادل حالت (2,2) در روش فن و (3,3) در روش پیشنهادی است، بازدهٔ جاسازی روش فن و روش پیشنهادی به ترتیب برابر با ۲/۶۶ و ۳ است. بنابراین، با توجه به نرخ جاسازی یکسان یک بیت بر پیکسل در دو

روش، اعوجاج ایجاد شده در تصویر پوششی در روش پیشنهادی نسبت به روش فن کمتر است. از این رو، کیفیت تصاویر پوششی بهبود یافته و طبق جدول ۳ نیز، PSNR در روش پیشنهادی تقریبا به میزان ۰/۵ dB نسبت به روش فن افزایش می‌یابد. همانطور که ملاحظه می‌شود، شاخص MSSIM نیز نسبت به دو روش F5 و فن، بهبود یافته و به یک نزدیک‌تر می‌شود. زمان اجرای برنامه در شرایط یکسان، برای روش‌های F5، فن و پیشنهادی به ترتیب برابر با ۲۳/۶، ۷/۶ و ۵/۲ حاصل شده است.

جدول۱ مقایسه تعداد بیت قابل جاسازی در روش‌های مختلف

Method	F5	فن	روش پیشنهادی
r=2	۱۷۴۷۶۲	۲۶۲۱۴۴	۵۲۴۲۸۸
r=3	۱۱۲۳۴۷	۱۹۶۶۰۸	۲۶۲۱۴۴
r=4	۶۹۹۰۵	۱۳۱۰۷۲	۱۴۹۷۹۶
r=5	۴۲۲۸۱	۸۱۹۲۰	۸۷۳۸۱

جدول۲ مقایسهٔ PSNR و MSSIM در ظرفیت دو بیت بر پیکسل

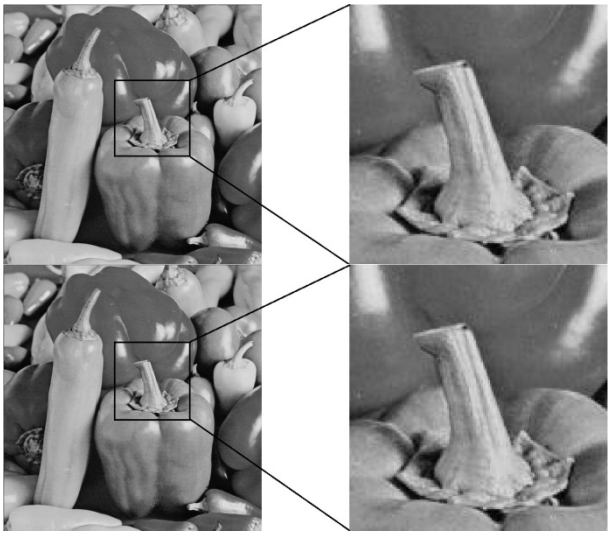
Method	Simple LSB	Proposed Method
PSNR	۴۴/۵۴	۴۶/۳۴
MSSIM	۰/۹۸۲۴	۰/۹۸۹۶

جدول۳ مقایسهٔ PSNR و MSSIM در ظرفیت یک بیت بر پیکسل

Method	F5 (1,1)	Fan (2,2)	Proposed Method (3,3)
PSNR	۵۱/۱۴	۵۲/۳۵	۵۲/۸۷
MSSIM	۰/۹۹۵۹	۰/۹۹۶۹	۰/۹۹۷۳

به منظور بررسی بیشتر کیفیت تصاویر حامل در روش پیشنهادی، مثال‌هایی از تصاویر پوششی و حامل به صورت عادی و بزرگ‌نمایی در شکل‌های ۹ و ۱۰ نشان داده شده است. با توجه به این که بیشترین اعوجاج در حالت p=1 رخ می‌دهد (حداکثر ظرفیت)، بررسی کیفیت بصری تصاویر حامل در حالت p=1 انجام می‌شود، که معادل با بدترین حالت از لحاظ اعوجاج است. در این جا، از تصاویر پوششی با ابعاد ۵۱۲×۵۱۲ و تصویر محرمانه با ابعاد ۲۵۶×۲۵۶ پیکسلی استفاده می‌شود. همانطور که مشاهده می‌شود، تصاویر حامل از کیفیت بصری بالایی برخوردار هستند. مطابق شکل‌های حاصل شده، امکان تشخیص اعوجاج در تصویر حامل نسبت به تصویر پوششی اصلی، از طریق سیستم بینایی انسان وجود ندارد.

لازم به ذکر است، بازیابی پیام محرمانه در روش پیشنهادی بصورت بدون اتلاف صورت گرفته و از این رو در تمامی حالات، PSNR بین تصاویر محرمانهٔ جاسازی شده و بازیابی شده برابر با بینهایت و MSSIM آن برابر با یک است.



شکل۹ تصاویر پوششی (بالا) و حامل (پایین) در حالت عادی و بزرگ‌نمایی

شکل۱۰ تصاویر پوششی (بالا) و حامل (پایین) در حالت عادی و بزرگ‌نمایی

۴-۴-۳ مقاومت در برابر پنهان‌شکنی

به منظور بررسی عملکرد روش‌های مختلف در زمینهٔ مقاومت در برابر پنهان‌شکنی، از منحنی ROC[1] استفاده می‌شود. پنهان‌شکن در نقاط آستانهٔ مختلف، تصاویر را به دو دستهٔ اصلی (دست-نخورده) و دست‌کاری شده تقسیم می‌کند. سپس منحنی ROC،

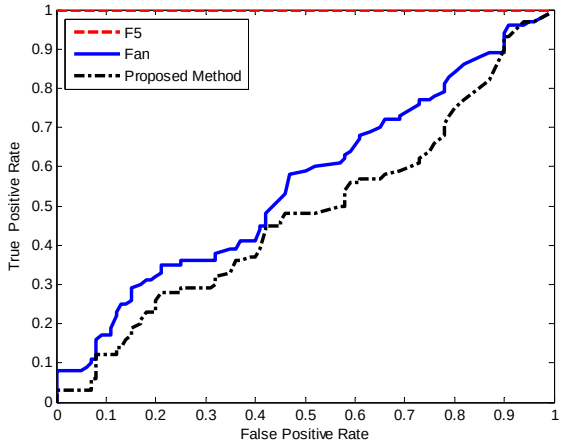
[1]Receiver Operating Characteristic

بصورت نرخ مثبت درست[1] (محور y) در برابر نرخ مثبت نادرست[2] (محور x) ترسیم می‌شود. هر چه منحنی مربوط به یک روش نهان نگاری به منحنی y=1 نزدیک‌تر باشد، مقاومت آن در برابر پنهان‌شکنی کمتر خواهد بود.

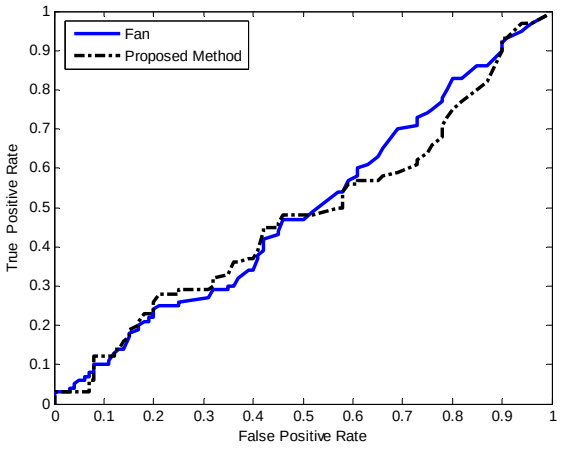
شکل ۱۱ منحنی ROC مربوط به روش‌های F5، فن و روش پیشنهادی را با استفاده از پنهان‌شکنی AUMP، تحت شرایط یکسان و در ظرفیت مشابه یک بیت بر پیکسل نشان می‌دهد. در این بخش، از تصاویر مربوط به پایگاه دادهٔ [۲۶] استفاده شده است.

همانطور که ملاحظه می‌شود، منحنی مربوط به روش پیشنهادی در قیاس با دو روش دیگر، از حالت y=1 دورتر بوده و بنابراین از امنیت بیشتری نسبت به آن‌ها برخوردار است.در مقابل، منحنی مربوط به روش F5 بر y=1 منطبق بوده، براحتی از طریق AUMP شناسایی می‌شود و بنابراین از امنیت پایینی در مقابل پنهان‌شکنی مذکور برخوردار است.

همانطور که مطرح شد، تعداد درایه‌های بلوک تصویر پوششی در روش پیشنهادی، نسبت به روش فن به میزان یک واحد کاهش یافته و بنابراین نرخ جاسازی افزایش می‌یابد. از طرفی به علت افزایش حداکثر تغییرات از یک به دو تغییر در هر بلوک، اعوجاج نیز افزایش می‌یابد. به منظور بررسی تاثیر این اعوجاج اضافی، منحنی ROC مربوط به روش فن در حالت $p=4$ و روش پیشنهادی در حالت $p'=p-1=3$، در شکل ۱۲ نشان داده شده است. همانطور که مشاهده می‌شود، افزایش اعوجاج ناشی از کاهش طول بلوک، ناچیز بوده و به کاهش امنیت سیستم نمی‌انجامد. به عبارتی در عین حفظ امنیت، نرخ جاسازی افزایش می‌یابد.



شکل۱۱ منحنی ROC روش‌های مختلف با استفاده از پنهان‌شکنی AUMP در ظرفیت یک بیت بر پیکسل



شکل۱۲ منحنی ROC روش فن (p=4) و روش پیشنهادی (p'=3)

در نهایت با توجه به نتایج شبیه‌سازی، روش پیشنهادی ضمن بهره‌مندی از کیفیت بصری و بازدهٔ جاسازی مناسب، از نرخ جاسازی بالاتری برخوردار است. از طرفی، روش پیشنهادی منجر به حصول مقاومت مطلوب در برابر پنهان‌شکنی و امنیت بیشتر در سیستم ارسال اطلاعات می‌شود.

۵ جمع‌بندی

در این مقاله، یک روش جاسازی ماتریسی به منظور افزایش نرخ و بازدهٔ جاسازی ارائه شده است. در روش فن، حداکثر تعداد تغییرات در هر بلوک تصویر پوششی به میزان یک واحد است. در روش پیشنهادی، با افزایش تغییرات به حداکثر دو واحد، ابعاد بلوک‌های تصویر پوششی به ازای پنهان سازی تعداد مشخصی از بیت‌های محرمانه، کاهش می‌یابد. این امر منجر به افزایش نرخ جاسازی و دست‌یابی به حداکثر ظرفیت دو بیت بر پیکسل، در تصویر پوششی می‌شود که دو برابر حداکثر ظرفیت در روش فن است.

از طرفی، بازدهٔ جاسازی در روش پیشنهادی از شرایط مطلوب برخوردار است. بازدهٔ جاسازی در روش پیشنهادی نسبت به روش F5 و روش فن، در ظرفیت برابر یک بیت بر پیکسل افزایش یافته است. در شرایط برابر و در ظرفیت بالا (یک و دو بیت بر پیکسل)، روش پیشنهادی نسبت به روش‌های LSB ساده، روش F5 و روش فن کیفیت تصاویر حامل را افزایش می‌دهد. همچنین مقاومت در برابر پنهان‌شکنی افزایش می‌یابد. با افزایش کیفیت تصاویر حامل و مقاومت در برابر پنهان‌شکنی، احتمال تشخیص وجود پیام محرمانه در تصاویر حامل توسط دشمن، کاهش یافته و بنابراین امنیت سیستم افزایش می‌یابد. روش نهان نگاری مذکور، قادر به بازیابی کامل و بی اتلاف پیام محرمانه در گیرنده است. با توجه به نتایج بدست آمده، الگوریتم پیشنهادی از نرخ و بازدهٔ جاسازی بالا، همچنین تصاویر حامل با کیفیت و ایمنی مطلوب برخوردار است.

[1] True positive rate
[2] False positive rate

مراجع

[1] Tang, M., Hu, J., Song, W., *"A high capacity image steganography using multi-layer embedding"*, Optik-International Journal for Light and Electron Optics, Vol. 125, pp. 3972-3976, 2014.

[2] Cheddad, A., Condell, J., Curran, K., Mc Kevitt , P., *"Digital image steganography: Survey and analysis of current methods"*, Signal processing, Vol. 90, pp. 727-752, 2010.

[3] Goel, S., Rana, A., Kaur, M., *"Comparison of image steganography techniques"*, International Journal of Computers and Distributed Systems, Vol. 3, pp. 20-30, 2013.

[4] Kaur, R., Singh, B., *"Survey And Analysis of Various Steganographic Techniques"*, International Journal of Engineering Science and Advanced Technology, Vol. 2, pp. 561-566, 2012.

[5] Li, B., He, J., Huang, J., Shi, Y. Q., *"A survey on image steganography and steganalysis"*, Journal of Information Hiding and Multimedia Signal Processing, Vol. 2, pp. 142-172, 2011.

[6] Chanu, Y. J., Tuithung, T., Manglem Singh, K., *"A short survey on image steganography and steganalysis techniques"*, in Emerging Trends and Applications in Computer Science (NCETACS), 3rd National Conference on, pp. 52-55, 2012.

[7] Hussain, M., Hussain, M., *"A survey of image steganography techniques"*, International Journal of Advanced Science and Technology, Vol. 54, pp. 113-124, 2013.

[8] Hamid, N., Yahya, A., Ahmad, R. B., Al-Qershi, O. M., *"Image steganography techniques: an overview"*, International Journal of Computer Science and Security (IJCSS), Vol. 6, pp. 168-187, 2012.

[9] Crandall, R., *"Some notes on steganography"*, Posted on steganography mailing list, 1998.

[10] Lin, R.-D., Chang, C.-T., *"A compact covering method to exploit embedding capacity for matrix encoding"*, Information Sciences, Vol. 188, pp. 170-181, 2012.

[11] Gao, Y., Li, X., Zeng, T., Yang, B., *"Improving embedding efficiency via matrix embedding: a case study"*, in Image Processing (ICIP), 16th IEEE International Conference on, pp. 109-112, 2009.

[12] Westfeld, A., *"F5—a steganographic algorithm"*, in Information hiding, pp. 289-302, 2001.

[13] Tseng, Y.-C., Chen, Y.-Y., Pan, H.-K., *"A secure data hiding scheme for binary images"*, Communications, IEEE Transactions on, Vol. 50, pp. 1227-1231, 2002.

[14] Fridrich, J., Soukal, D., *"Matrix embedding for large payloads"*, Information Forensics and Security, IEEE Transactions on, Vol. 1, pp. 390-395, 2006.

[15] Zhang, X., Wang, S., *"Efficient steganographic embedding by exploiting modification direction"*, Communications Letters, IEEE, Vol. 10, pp. 781-783, 2006.

[16] Zhang, X., Zhang, W., Wang, S., *"Efficient double-layered steganographic embedding"*, Electronics letters, Vol. 43, pp. 482-483, 2007.

[17] Chang, C.-C., Kieu, T. D., Chou, Y.-C., *"A high payload steganographic scheme based on (7, 4) hamming code for digital images"*, in Electronic Commerce and Security, International Symposium on, pp. 16-21, 2008.

[18] Sarkar, A., Madhow, U., Manjunath, B., *"Matrix embedding with pseudorandom coefficient selection and error correction for robust and secure steganography"*, Information Forensics and Security, IEEE Transactions on, Vol. 5, pp. 225-239, 2010.

[19] Fan, L., Gao, T., Yang, Q., Cao, Y., *"An extended matrix encoding algorithm for steganography of high embedding efficiency"*, Computers & Electrical Engineering, Vol. 37, pp. 973-981, 2011.

[20] Wang, C., Zhang, W., Liu, J., Yu, N., *"Fast matrix embedding by matrix extending"*, Information Forensics and Security, IEEE Transactions on, Vol. 7, pp. 346-350, 2012.

[21] Fan, L., Gao, T., Cao, Y., *"Improving the embedding efficiency of weight matrix-based steganography for grayscale images"*, Computers & Electrical Engineering, Vol. 39, pp. 873-881, 2013.

[22] Liu, G., Liu, W., Dai, Y., Lian, S., *"Adaptive steganography based on block complexity and matrix embedding"*, Multimedia systems, Vol. 20, pp. 227-238, 2014.

[23] Kim, C., Yang, C.-N., *"Steganography based on grayscale images using (5, 3) hamming code"*, in Digital-Forensics and Watermarking, ed: Springer, pp. 588-598, 2014.

[24] Mao, Q., *"A fast algorithm for matrix embedding steganography"*, Digital Signal Processing, Vol. 25, pp. 248-254, 2014.

[25] Nazari, S., Eftekhari‐Moghadam, A. M., Moin, M. S., *"A novel image steganography scheme based on morphological associative memory and permutation schema"*, Security and Communication Networks, Vol. 8, pp. 110-121, 2015.

[26] http://www.shsu.edu/~qxl005/New/Downloads/

[27] Sharda, S., Budhiraja, S., *"Image steganography: a review"*, Int J of Emerg Technol Adv Eng, Vol. 3, pp. 707-710, 2013.

[28] Wang, Z., Bovik, A. C., Sheikh, H. R., Simoncelli, E. P., *" Image Quality Assessment: From Error Visibility to Structural Similarity"*, Image Processing, IEEE Transactions on, Vol. 13, pp. 600-612, 2004.

[29] Fillatre, L., *"Adaptive Steganalysis of Least Significant Bit Replacement in Grayscale Natural Images"*, Signal Processing, IEEE Transactions on, Vol. 60, pp. 556-569, 2012.

علیرضا پورمحمدعلی مدرک کارشناسی و کارشناسی ارشد خود را در رشتهٔ مهندسی برق از دانشگاه شهید باهنر کرمان به ترتیب در سال-های ۱۳۹۱ و ۱۳۹۴ دریافت نموده است. زمینه‌های تحقیقاتی مورد علاقهٔ او نهان‌نگاری تصویر، پردازش تصویر و بازشناسی الگو است.

مریم پورمحی‌آبادی تحصیلات خود را در دورهٔ کارشناسی در دانشگاه شهید باهنر کرمان ، دورهٔ کارشناسی ارشد در دانشگاه گیلان و دورهٔ دکتری در دانشگاه علم و صنعت ایران در رشتهٔ مهندسی برق-الکترونیک به ترتیب در سال‌های ۱۳۷۶، ۱۳۷۹ و ۱۳۸۸ به پایان رسانده است. وی هم اکنون استادیار بخش مهندسی برق دانشگاه شهید باهنر کرمان است. زمینه‌های پژوهشی مورد علاقهٔ او پردازش تصویر، پردازش سیگنال‌های نوری و طراحی ادوات نوری است.

حسین نظام‌آبادی‌پور تحصیلات خود را در دورهٔ کارشناسی مهندسی برق- الکترونیک در دانشگاه شهید باهنر کرمان در سال ۱۳۷۷ و در مقاطع کارشناسی ارشد و دکتری مهندسی برق- الکترونیک در دانشگاه تربیت مدرس به ترتیب در سال‌های ۱۳۷۹ و ۱۳۸۳ به پایان رسانده است. وی هم اکنون استاد بخش مهندسی برق دانشگاه شهید باهنر کرمان است. زمینه‌های پژوهشی مورد علاقهٔ او پردازش تصویر، بازشناسی الگو، کاربرد رایانش نرم در پردازش تصویر و روش‌های بهینه‌سازی ابتکاری است.