مجله علمی - پژوهشی "پدافند الکترونیکی و سایبری"
سال چهارم، شماره ۲، تابستان ۱۳۹۵، ص ۲۱- ۱۵

بهبود ظرفیت و شفافیت در روش نهان‌نگاری Mod4

عباسعلی حسنی[۱]، حمید دهقانی*[۲]، مهدی دهقانی[۳]، رضا اصفهانی[۴]

۱- کارشناس ارشد، دانشگاه جامع امام حسین(ع)، ۲ – دانشیار، دانشگاه صنعتی مالک اشتر، ۳- دکتری کامپیوتر، دانشگاه جامع امام حسین(ع)، ۴- دانشجوی دکتری، دانشگاه جامع امام حسین(ع)

(دریافت: ۹۴/۰۹/۳۰، پذیرش: ۹۵/۰۳/۱۷)

چکیده

برقراری ارتباط پنهان و امن از نیازهای ضروری در فضای سایبر است. نهان‌نگاری اطلاعات بهترین روشی است که امنیت ارتباط در شبکه‌های عمومی مانند اینترنت را فراهم می‌کند. روش نهان‌نگاری Mod4 از جمله روش‌های مطرح حوزه تبدیل کسینوس است، که به‌شکلی متفاوت از روش‌های گذشته پیام را درون تصویر جاسازی می‌کند. در این روش همبستگی بین ضرایب به‌خوبی حفظ می‌شود، و در برابر نهان‌کاوی کور مقاوم است. در این مقاله بهبود روش نهان‌نگاری Mod4، یعنی افزایش ظرفیت و شفافیت، به‌عنوان دو معیار اصلی در نهان‌نگاری صورت گرفته است. در روش پیشنهادی با تغییر اندازه قالب‌های ضرایب کسینوس، و با تعیین شروط مناسب برای انتخاب قالب‌های معتبر، شفافیت بیش از ۵ درصد و ظرفیت بیش از ۶۸ درصد افزایش یافته است. برای ارزیابی شفافیت تصاویر نهانه در روش پیشنهادی، و مقایسه با روش اصلی Mod4، از دو معیار PSNR و SSIM استفاده شده است.

واژه‌های کلیدی: نهان‌نگاری، ظرفیت، شفافیت، Mod4، JPEG

۱- مقدمه

تا کنون روش‌های گوناگونی برای نهان‌نگاری اطلاعات ارائه شده است. نهان‌نگاری در دو حوزه مکان و حوزه تبدیل انجام می‌شود. حوزه مکان شامل آن دسته از روش‌هایی است که بیت‌های پیام بین بیت‌های میزبان جاسازی می‌شوند، به‌عنوان مثال در روش جاگذاری کم‌ارزش‌ترین بیت[۱]، بیت‌های پیام در کم ارزش‌ترین بیت هر پیکسل گنجانده می‌شوند. حوزه تبدیل شامل آن دسته از روش‌هایی است که بیت‌های پیام روی مقادیر ضرایب تبدیل مورد نظر پخش می‌گردد. در این روش‌ها از تبدیل‌هایی مانند تبدیل کسینوسی گسسته[۲] و تبدیل موجک[۳] و غیره استفاده می‌شود. از بین قالب‌های مختلف تصویر، قالب JPEG به دلیل ویژگی‌هایی نظیر فشرده‌سازی بالا در کنار حفظ کیفیت مطلوب تصویر، از پرکاربردترین فرمت‌های تصویر بوده و اکثر تصاویری که از طریق اینترنت مبادله می‌شوند، با فرمت JPEG ذخیره می‌شوند. قالب تصویری مذکور با توجه به استفاده از تبدیل کسینوسی گسسته جهت فشرده‌سازی، قابلیت لازم برای نهان‌نگاری در فضای تبدیل را دارا است. راه مخفی کردن بیت‌ها در ضرایب کسینوسی، قرار دادن آن‌ها در بیت‌های با کمترین ارزش ضرایب است.در این روش تعداد زیادی از ۶۴ ضریب تبدیل کسینوسی گسسته در هر قطعه ۸×۸ از پیکسل‌های تصویر صفر هستند و تغییر تعداد زیادی صفر به مقادیر غیر صفر، بر نرخ فشرده‌سازی تصویر و شفافیت آن تأثیر منفی می‌گذارد. به‌همین دلیل است که ظرفیت نهان‌نگاری در حوزه تبدیل، کمتر از ظرفیت نهان‌نگاری در حوزه مکان است. اما دلیل رویکرد به روش‌های حوزه تبدیل این است که آشکارناپذیری (شفافیت) و مقاومت در این حوزه نسبت به نهان‌نگاری در حوزه مکان بیشتر است.

در یک سیستم نهان‌نگاری، پارامترها یا معیارهای سنجش میزان کارایی، عبارتند از:

- **مقاومت**[۴]: به میزان حفظ پیام در برابر تغییرات قابل اعمال بر روی تصویر نهان‌نگاری شده (نهانه) اطلاق می‌گردد.
- **ظرفیت**[۵]: به میزان حجم اطلاعات قابل مخفی‌کردن در داخل پوشانه (تصویر قبل از نهان‌نگاری)، ظرفیت نهان‌نگاری اطلاق می‌گردد.

* رایانامه نویسنده مسئول: hamid_deh@yahoo.com

1- Least Significant Bit (LSB)
2- Discrete Cosine Transform
3- Wavelet
4- Robustness
5- Capacity

- **شفافیت**[1]: به میزان عدم تشخیص، یا آشکارناپذیر بودن پیام مخفی در تصویر پوشانه اطلاق می‌گردد. آشکارپذیری بیان می‌دارد که تا چه اندازه تصویر حاوی اطلاعات مشخص و گویا می‌باشد در حقیقت امنیت یک سیستم نهان‌نگاری در همین مسئله شفافیت نهفته است، و هر قدر شباهت پوشانه و نهانه، بیشتر باشد امنیت این سیستم در سطح بالاتری قرار دارد.

شکل (۱). سه شاخص اصلی نهان نگاری

سه ویژگی فوق به‌طور بسیار تنگاتنگی در ارتباط با یکدیگر هستند. بدین معنی که با ثابت فرض کردن ویژگی اول و افزایش ویژگی دوم ویژگی سوم کاهش خواهد یافت (شکل ۱) [۱].

در این تحقیق برای بررسی میزان شفافیت از دو معیار PSNR[2] و SSIM[3] استفاده شده است. SSIM معیاری است که جهت سنجش مشابهت ساختاری دو تصویر قبل از نهان‌نگاری و پس از نهان‌نگاری استفاده می‌شود.

نهان‌نگاری به روش Mod4 از جمله روش‌های مطرح در حوزه تبدیل کسینوسی است و مزیت اصلی آن نسبت به روش‌های دیگر حوزه تبدیل، مقاومت آن در برابر نهان‌کاوی کور[4] است [۲].

در این مقاله بهبود روش نهان‌نگاری Mod4، یعنی افزایش ظرفیت و شفافیت به‌عنوان دو معیار اصلی ارزیابی نهان‌نگاری، صورت گرفته است.

در این روش از ضرایب کسینوسی مجاور هم که تشکیل یک گروه از ماتریس‌های ۲×۲ می‌دهد (GQC[5]) استفاده می‌گردد. با توجه به شرایط مربوطه، تعداد GQC های معتبر مشخص می‌شوند و از طریق کوتاه‌ترین مسیر تغییر، جاسازی انجام می‌گردد.

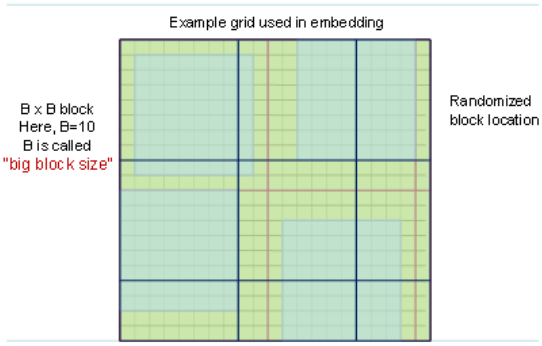
آنچه در ادامه ارائه می‌گردد به این صورت است: در بخش ۲ به بررسی برخی از کارهای مرتبط پرداخته شده است. در بخش ۳، روش نهان‌نگاری Mod4 به طور مختصر بیان می‌شود. سپس در بخش ۴، روش پیشنهادی توضیح داده می‌شود. در بخش ۵، نتایج شبیه‌سازی ارائه شده است، و در انتها در بخش ۶، نتیجه‌گیری و پیشنهاد برای ادامه کار ارائه گردیده است.

۲- کارهای مرتبط

در این بخش اشاره‌ای به برخی کارهای صورت گرفته در حوزه تبدیل بر مبنای تصاویر JPEG داریم. سپس به بررسی بعضی از روش‌هایی که به نوعی با روش پیشنهادی مرتبط هستند، می‌پردازیم.

روش نهان‌نگاری که در مرجع [۳] به آن اشاره شده، روش Jsteg است. الگوریتم نهان‌سازی آن، بیت با کمترین ارزش ضرایب کسینوسی را از آغاز و به صورت متوالی با بیت‌های پیام جایگزین می‌نماید. این روش دارای کلید مخفی نیست. بنابراین هر کس که به سیستم نهان‌نگاری واقف باشد، می‌تواند به پیام مخفی دست یابد [۴]. در روش JQTM که در مرجع [۵] بیان شده است، به جای استفاده از ماتریس چندی‌سازی استاندارد JPEG، از ماتریس اصلاح‌شده استفاده می‌شود. مهم‌ترین مزیت این روش نسبت به Jsteg ظرفیت ذخیره‌سازی اطلاعات در تصویر می‌باشد. این روش دارای نرخ فشرده‌سازی کمتری نسبت به Jsteg می‌باشد، و به‌دلیل استفاده از جایگزینی کم‌ارزش‌ترین بیت توسط حملات مبتنی بر کم‌ارزش‌ترین بیت قابل تشخیص است. OutGuess یک روش نهان‌نگاری است که روش Jsteg را با استفاده از یک مولد اعداد تصادفی یا شبه‌تصادفی برای انتخاب ضرایب کسینوسی بهبود می‌بخشد. در این روش نیز کم‌ارزش‌ترین بیت ضرایب کسینوسی انتخاب شده، با بیت پیام به روش Jsteg جایگزین می‌شود. اشکال این روش این است که توسط حملات آماری قابل شناسایی است [۱]. در مرجع [۶]، روش نهان‌نگاری F5 ارائه گردیده است. این روش بهبود یافته روش‌های F3 و F4 است. در این روش تغییرات ضرایب کسینوسی به کمترین مقدار خود خواهد رسید. در روش F5 برخلاف روش‌های Jsteg، Outguess، F3 و F4 پیام در کل تصویر به‌صورت گسترده و پخش، نهان‌نگاری می‌شود. عدم مقاومت در برابر حملات آماری، یکی از اشکلات این روش است. روش نهان‌نگاری YASS در سال ۲۰۰۷ و در مرجع [۷] معرفی شد. این روش پایه و اساس روشی است که در مرجع [۸] به آن پرداخته شده است. اساس روش YASS بر مبنای تغییر اندازه قالب ضرایب کسینوسی است. در این روش ابتدا تصویر به قالب‌های B×B ناهم‌پوشان تفکیک می‌شود که ابعاد آن از یک قالب JPEG بزرگتر است (B>8). سپس در هر قالب، زیرقالب‌هایی به ابعاد ۸×۸ به‌روش شبه‌تصادفی انتخاب می‌شود (شکل ۲). مهم‌ترین مزیت این روش مقاومت در برابر نهان‌کاوی کور است [۷].

1- Transparency
2- Peak Signal Noise Ratio (PSNR)
3- Structural Similarity Index Measure (SSIM)
4- Blind
5- A **G**roup of **Q**uantized DCT **C**oefficients (GQC)



شکل (۲). نحوه انتخاب قالب ها در روش YASS

با توجه به توضیحات بالا، روشن است که تغییر اندازه قالب ضرایب کسینوسی را می‌توان به‌عنوان یکی از راه‌های بهبود نهان‌نگاری، به‌ویژه در برابر نهان‌کاوی کور مورد توجه قرار داد. در این تحقیق نیز تغییر قالب‌های ضرایب کسینوسی، جهت بهبود روش Mod4 مورد توجه واقع شده است.

ایده اولیه روش نهان‌نگاری Mod4 در سال ۲۰۰۵ ارائه گردید [۹]. سپس در مرجع [۱۰]، این روش به‌طور کامل‌تری بیان شد. ویژگی ممتاز روش Mod4 ، مقاومت آن در برابر نهان‌کاوی کور است [۱۰].

در مرجع [۱۱] ایده جاسازی چند پیام در یک تصویر با استفاده از روش Mod4 مورد بحث واقع شده است. نویسنده مقاله اخیر با استفاده از شروط قابل تعریف در روش Mod4 امکان جاسازی چند پیام مختلف در یک تصویر را مورد بحث قرار داده است. لذا یکی از مواردی که در این تحقیق جهت بهبود روش Mod4 مورد توجه قرار گرفته، تغییر هدفمند در پارامترهای[۱] $Ø_1$، $Ø_2$، τ_1 و τ_2، برای یک پیام است. در مرجع [۱۲] مقاله‌ای تحت عنوان نهان‌نگاری در صوت با استفاده از روش Mod4 ، چگونگی نهان‌نگاری در فایل‌های صوتی با استفاده از روش Mod4 مورد بحث واقع شده است. در مرجع [۱۳] نهان‌نگاری در تصویر با استفاده از روش Mod4 بر اساس کنتراست تصویر ارائه گردیده است. تفاوت اصلی این روش با روش مطرح شده در مرجع [۱۰]، در نحوه انتخاب قالب‌های ۲×۲ معتبر[۲] است. در روش مذکور، یک قالب در صورتی معتبر است که تفاضل مقدار متوسط بین پیکسل‌های آن قالب از یک مقدار متوسط (حداقل کنتراست) بالاتر باشد. با توجه به مقدار سطح آستانه (حداقل کنتراست)، تعداد قالب‌های معتبر و در نتیجه ظرفیت و شفافیت تصویر قابل تغییر است.

برخی از مزیت‌های روش نهان‌نگاری Mod4 نسبت به روش‌های دیگر عبارت است از:

- مقاومت در برابر نهان‌کاوی کور [۱۰]
- نحوه جاسازی پیام در آن به‌شکلی است که حداقل تغییرات روی ضرایب کسینوسی صورت می‌گیرد.
- هم‌بستگی ضرایب در این روش به‌خوبی حفظ می‌شود.

در ادامه روش Mod4 را تشریح می‌کنیم.

۳- روش نهان‌نگاری Mod4

در این بخش با توجه به شکل (۳)، روش Mod4 توضیح داده می‌شود [۱۰].

۳-۱- یافتن قالب‌هایی برای جاسازی

قالب‌های ۸×۸ از ضرایب کسینوسی چندی‌سازی شده[۳] که آنها را F_{QT} می‌نامیم از ماتریس داده تصویر JPEG، استخراج می‌شود. هر F_{QT} از ۱۶ گروه ۲×۲ از ضرایب کسینوسی مجاور هم تشکیل شده است. قالب‌ها[۴] (گروه‌ها) را به‌گونه‌ای انتخاب می‌کنیم که هم‌پوشانی صورت نگیرد. یک قالب معتبر[۵] است اگر شروط (۱) و (۲) برقرار باشند:

$$|\{x: x \in GQC, x > Ø_1\}| \geq \tau_1 \quad (۱)$$

$$|\{x: x \in GQC, x < -Ø_2\}| \geq \tau_2 \quad (۲)$$

$Ø_1$ و $Ø_2$ اندازه ضرایب و τ_1 و τ_2 تعیین‌کننده تعداد (حداقل) ضرایب مثبت و منفی هستند.

۳-۲- تخمین ظرفیت جاسازی

قالب‌های معتبر از F_{QT} ها استخراج می‌شوند و در آرایه‌ای به‌نام β به ترتیب اتخاذ به‌وسیله کلید محرمانه k ذخیره می‌شوند. هنگامی‌که همه قالب‌های معتبر استخراج شدند، اندازه β تعیین کننده ظرفیت جاسازی (Ω) در تصویر پوشانه است. اندازه Ω به کیفیت تصویر، مقادیر $Ø_1$ و $Ø_2$ و دو آستانه مثبت τ_1 و τ_2 وابسته است. Ω (ظرفیت) دو برابر تعداد قالب‌های معتبر است زیرا در هر قالب دو بیت جاسازی می‌شود.

۳-۳- فرایند جاسازی پیام

$Mod(b_i, 4)$ یعنی باقی‌مانده حاصل‌جمع ضرایب در هر قالب

۱- $Ø_1$ و $Ø_2$ اندازه ضرایب و τ_1 و τ_2 تعیین‌کننده تعداد (حداقل) ضرایب مثبت و منفی هستند.

2- valid GQC2×2

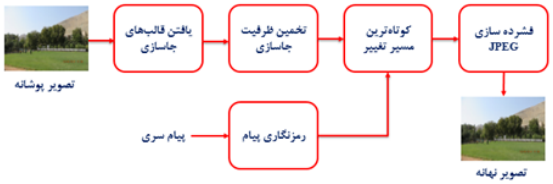
3- qDCT
4- GQC
5- vGQC

معتبر، تقسیم بر ۴ را به‌دست می‌آوریم[۱]. اکنون یک جفت‌بیت از پیام (xy_i) را در نظر گرفته و ضرایب قالب معتبر را طوری تغییر می دهیم که $Mod(b`_i, 4)$ برابر با xy_i شود[۲]. برای تغییر ضرایب از روش SRM[۳] (کوتاه‌ترین مسیر تغییر) استفاده می‌شود [۱۰]. به‌همین ترتیب مابقی پیام را در بقیه قالب‌های معتبر جاسازی می‌کنیم. سپس قالب‌های معتبر جدید را به جای اول (جایی‌که از آنجا استخراج شده بودند) برگردانده و تصویر جدید (حاوی پیام) را بازسازی می‌کنیم.

پس از این مرحله و شکل‌گیری قالب‌های $F`_{QT}$، ادامه استاندارد فشرده‌سازی JPEG اعمال می‌گردد و سرانجام تصویر نهان‌نگاری شده (نهانه)، حاصل می‌گردد.

۳-۴- فرایند استخراج روش Mod4

فرایند استخراج درشکل (۴) نمایش داده شده است. دریافت‌کننده تصویر، ابتدا همه قالب‌های معتبر را با توجه به پارامترهای Ø1، Ø2، τ1 و τ2 و همچنین با توجه به کلید محرمانه k، استخراج می‌کند. سپس برای استخراج پیام مورد نظر، حاصل $Mod(b_i,4)$، یعنی باقی‌مانده حاصل‌جمع ضرایب در هر قالب معتبر تقسیم بر ۴ را به‌دست می‌آورد. دو بیتی حاصل، دو بیت از پیام می‌باشد. ادامه کار به‌همین ترتیب برای مابقی قالب‌های معتبر ادامه می‌یابد تا تمام پیام استخراج شود.



شکل (۳). نمودار جاسازی روش نهان‌نگاری Mod4 [۱۱]

شکل (۴). نمودار استخراج روش نهان‌نگاری Mod4 [۱۱]

۴- روش پیشنهادی برای بهبود Mod4:

آنچه در این تحقیق جهت بهبود Mod4 مورد توجه قرار گرفته، بهبود ظرفیت و شفافیت تصویر به‌عنوان دو معیار اصلی در نهان‌نگاری است. البته مقاومت به‌عنوان یکی از پارامترهای نهان‌نگاری در این روش، بدون تغییر می‌باشد، زیرا تغییراتی که در روش Mod4، جهت افزایش ظرفیت و شفافیت صورت گرفته به‌صورتی نیست که مقاومت را تحت تاثیر قرار دهد. در عمل هم بعضی از حملات مانند چرخش ($k\pi/2$) و فشرده کردن تصویر، جهت ارزیابی مقاومت نهان‌نگاری آزمایش شد، که پس از آنکه تصویر به حالت اولیه برگشت، پیام به‌درستی قابل استخراج بود. البته مهم‌ترین معیاری که در نهان‌نگاری حائز اهمیت است، معیار شفافیت می‌باشد، زیرا هر چه شفافیت بالاتر باشد، امنیت نهان‌نگاری بیشتر است. معیار مقاومت بیشتر در نشان‌گذاری[۴] مورد بحث واقع می‌شود [۱].

در روش پیشنهادی برای بهبود ظرفیت، اندازه قالب ضرایب به‌صورت ۲×۱ در نظر گرفته می‌شوند، زیرا در این حالت، از حداکثر ضرایب برای جاسازی استفاده می‌شود. همچنین به منظور بهبود شفافیت، اندازه قالب ضرایب به‌صورت ۴×۴ در نظر گرفته شده است، زیرا در این حالت هم‌بستگی ضرایب بیشتر حفظ می‌شود و کمترین تغییرات روی مجموعه ضرایب مربوط به قالب صورت می‌گیرد، و در نتیجه شفافیت بیشتر خواهد شد.

پس هر چه اندازه قالب ضرایب بزرگ‌تر انتخاب شود، شفافیت بیشتر می‌شود، اما در صورت انتخاب قالب بزرگ‌تر از ۴×۴، حداکثر یک قالب معتبر در هر F_{QT}، خواهیم داشت، و با توجه به این‌که در هر قالب معتبر تنها دو بیت جاسازی می‌شود، لذا ظرفیت بسیار کم می‌شود که مطلوب نیست. بنابراین مناسب‌ترین حالت برای بهبود شفافیت، انتخاب اندازه قالب ضرایب، به صورت ۴×۴ است. در ادامه، روش پیشنهادی با توجه به شکل (۳) تشریح می‌شود.

۴-۱- بهبود ظرفیت

مرحله اول بهبود روش نهان‌نگاری Mod4 بهبود ظرفیت است که در ادامه مراحل کار توضیح داده می‌شود:

۱. ابتدا قالب‌های F_{QT} شامل ضرایب کسینوسی چندی‌سازی شده، از تصویر پوشانه استخراج می‌شود.
۲. مطابق (شکل ۵) هر یک از قالب‌های F_{QT} به ۳۲ قالب ۲×۱ غیرهم‌پوشان[۵] تقسیم می‌شود.
۳. یک قالب معتبر است اگر حداقل یکی از شروط (۳) یا (۴) را داشته باشد ($Ø_1= Ø_2=1$ ،τ_1 Or $\tau_2 =1$):

$$|\{x: x \in GQC, x > 1\}| \geq \quad (۳)$$

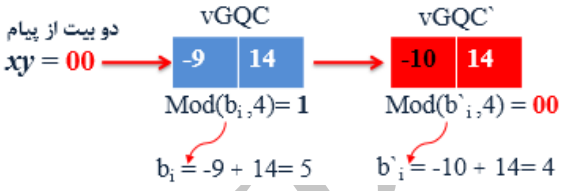
$$|\{x: x \in GQC, x < -1\}| \geq 1 \quad (۴)$$

۱ - bi مجموع ضرایب در هر قالب معتبر
۲ - b`i مجموع ضرایب در هر قالب معتبر جدید
3- Shortest route modification
4- Watermarking
5- GQC2×1

۴. با توجه به شروط (۳) و (۴)، قالب‌های معتبر از F_{QT}ها استخراج شده و در آرایه β بر اساس کلید محرمانه K ذخیره می‌شود.

۵. اکنون پیام مورد نظر به‌صورت زوج‌بیت در هر یک از قالب‌های معتبر بر اساس روش SRM، جاسازی می‌شود.

مثال:



۶. مابقی پیام نیز به‌همین صورت در قالب‌های معتبر جاسازی می‌شوند.

۷. سپس قالب‌های معتبر جدید به جای اولیه خود برگردانده می‌شوند، و پس اعمال فشرده‌سازی JPEG، تصویر نهانه حاصل می‌شود.

-120	-22	-16	5	1	1	-2	0
20	-10	-4	24	2	1	-1	0
-23	7	5	14	-1	-2	-2	-2
2	8	4	4	-6	-2	1	1
-9	14	1	-2	-5	0	1	0
2	4	0	-4	-2	2	0	1
-3	1	-3	-3	2	1	2	1
1	1	-3	1	2	2	0	0

شکل (۵). انتخاب قالب‌های ضرایب به‌صورت ۲×۱

۴-۲- بهبود شفافیت

مرحله دوم بهبود روش نهان‌نگاری Mod4، بهبود شفافیت است که در ادامه مراحل کار بیان می‌شود:

۱. ابتدا قالب‌های F_{QT} شامل ضرایب کسینوسی چندی‌سازی شده، از تصویر پوشانه استخراج می‌شود.

۲. مطابق شکل (۶) هر یک از قالب‌های F_{QT} به ۴ قالب ۴×۴ غیرهم‌پوشان[1] تقسیم می‌شود.

۳. یک قالب معتبر است اگر هر دو شرط (۳) و (۴) برقرار باشد (τ_1 And τ_2 =1). یعنی در هر قالب حداقل یک ضریب مثبت و حداقل یک ضریب منفی وجود داشته باشد.

۴. با توجه به بند قبل، قالب‌های معتبر از F_{QT}ها استخراج شده و در آرایه β بر اساس کلید محرمانه K ذخیره می‌شود.

۵. اکنون پیام مورد نظر به‌صورت زوج‌بیت در هر یک از قالب‌های معتبر بر اساس روش SRM جاسازی می‌شود.

۶. مابقی پیام نیز به‌همین صورت در بقیه قالب‌های معتبر جاسازی می‌شوند.

سپس قالب‌های معتبر جدید به جای اول خود برگردانده می‌شوند، و پس اعمال فشرده‌سازی JPEG، تصویر نهانه حاصل می‌شود.

-120	-22	-16	5	1	1	-2	0
20	-10	-4	24	2	1	-1	0
-23	7	5	14	-1	-2	-2	-2
2	8	4	4	-6	-2	1	1
-9	14	1	-2	-5	0	1	0
2	4	0	-4	-2	3	0	1
-3	1	-3	-3	4	1	2	1
1	1	-3	1	2	2	0	0

شکل (۶). انتخاب قالب‌های ضرایب به‌صورت ۴×۴

۵- نحوه انجام آزمایش و بررسی نتایج

در این تحقیق، شبیه‌سازی توسط نرم‌افزار متلب و بر روی مجموعه‌ای، شامل ۳۵ تصویر JPEG از مناظر گوناگون با اندازه‌های متفاوت و ابعاد 640x480 انجام شده است. نتایج بر مبنای نرخ نهان‌نگاری ۱۰۰٪ ظرفیت یک تصویر انجام شده است.

تذکر: در نمودارهای ارائه شده، ظرفیت بر حسب بیت و PSNR بر حسب دسی‌بل است، SSIM واحد ندارد و حداکثر مقدار آن یک است. در این نمودارها، میله‌ها به ترتیب از سمت چپ مربوط به حالت انتخاب اندازه قالب‌های ۱×۲، ۲×۲ و ۴×۴ است.

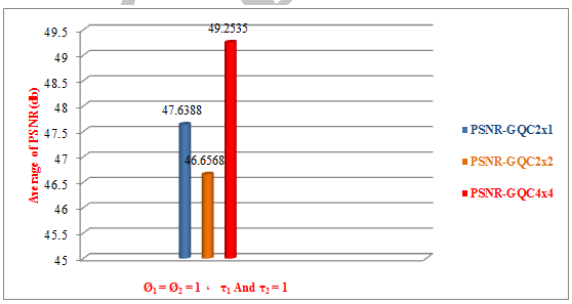
در شکل‌های (۹- ۷) مقایسه مقادیر متوسط PSNR، SSIM و ظرفیت روش پیشنهادی، با حالت انتخاب قالب‌های معتبر به‌صورت ۲×۲، ارائه شده است.

مطابق شکل (۷)، شفافیت تصویر در حالتی که قالب‌های ضرایب به‌صورت ۴×۴ یا ۱×۲ انتخاب شوند و τ_1 **And** τ_2=1 باشد، نسبت به‌حالتی که قالب‌ها به‌صورت ۲×۲ باشند، بیش از ۵ درصد افزایش می‌یابد، البته در حالت ۴×۴، به‌دلیل این‌که هم‌بستگی

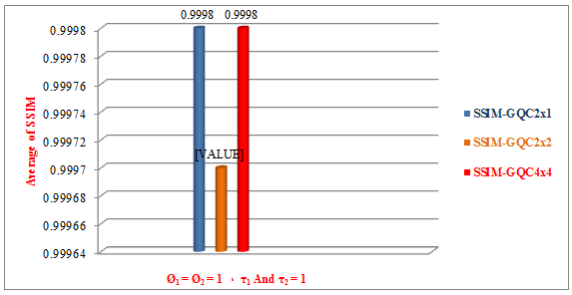
1- GQC4×4

ضرایب بیشتر حفظ می‌شود، شفافیت بهتر است. مطابق شکل (۸)، SSIM به‌عنوان یکی دیگر از معیارهای ارزیابی، نشان از کیفیت روش Mod4 و روش پیشنهادی دارد. مطابق شکل (۹) در صورتی‌که اندازه قالب‌های ضرایب به‌صورت ۱×۲ انتخاب شوند و τ_1 **or** τ_2=1 باشد ظرفیت بیش از ۶۸ درصد افزایش می‌یابد.

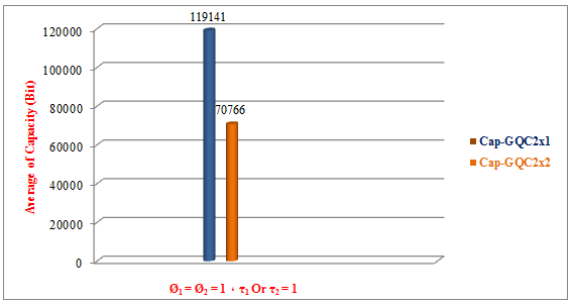
در شکل (۱۰) دو تصویر قبل از نهان‌نگاری و بعد از نهان‌نگاری (با جاسازی ۱۰۰٪ ظرفیت تصویر و در حالت حداکثری ظرفیت، یعنی τ_1 **or** τ_2=1، $Ø_1$=$Ø_2$=0) نمایش داده شده است، ($Ø_1$=$Ø_2$=0 یعنی در ضرایب 1 و 1- نیز جاسازی صورت گرفته است که این حالت به‌علت ظرفیت حداکثری، پایین‌ترین شفافیت را نسبت به حالت‌های دیگر دارد) همان‌طور که ملاحظه می‌شود تصویر نهانه از کیفیت بصری خوبی برخوردار است.



شکل (۷). مقایسه مقادیر متوسط PSNR روش پیشنهادی، با حالت انتخاب قالب‌های ضرایب به‌صورت ۲×۲



شکل (۸). مقایسه مقادیر متوسط SSIM روش پیشنهادی، با حالت انتخاب قالب‌های ضرایب به‌صورت ۲×۲



شکل (۹). مقایسه مقادیر متوسط ظرفیت روش پیشنهادی، با حالت انتخاب قالب‌های ضرایب به‌صورت ۲×۲

شکل (۱۰). تصویر پوشانه (سمت چپ)، و تصویر نهانه با حداکثر ظرفیت نهان‌نگاری (سمت راست)

۶- نتیجه‌گیری و پیشنهاد

با توجه به نتایج، و مباحث مطرح شده، در روش پیشنهادی با تغییر اندازه قالب ضرایب کسینوسی و همچنین با تغییر پارامترهای $Ø_1$، $Ø_2$، τ_1 و τ_2، می‌توان شفافیت و ظرفیت را متناسب با نیاز افزایش داد. طبق نتایجی که ارائه شد، در حالتی که قالب‌های ضرایب به‌صورت ۱×۲ انتخاب شوند و τ_1 **or** τ_2=1 ، باشد، ظرفیت بیش از ۶۸ درصد افزایش می‌یابد، و در حالتی‌که قالب‌های ضرایب به‌صورت ۴×۴ انتخاب شوند و τ_1 and τ_2=1 ، باشد، شفافیت بیش از ۵ درصد افزایش می‌یابد.

از جمله مواردی که برای ادامه کار پیشنهاد می‌شود، تهیه نرم‌افزاری است که با توجه به روش نهان‌نگاری Mod4 و روش‌های پیشنهادی در این تحقیق، به‌صورت هوشمند از میان بانک تصاویر، با توجه به اندازه پیام، تصویر مناسب را از لحاظ ظرفیت مورد نیاز و شفافیت حداکثری برای نهان‌نگاری پیام انتخاب نماید.

۶- مراجع

[1] Z. Safari Neshat, "Steganalysis of JPEG Image Format," Maleke Ashtar University, 2013 (In Persian).

[2] S. S. Jaber and H. A. Fadhil, "Survey On Recent Digital Image Steganography Techniques," School of Computer and Communication Engineering, University Malaysia Perlis, 2014.

[3] C. C. Chang, T. S. Chen, and L. Z. Chung, "A steganographic method based upon JPEG and quantization table modification," Information Sciences 141, 2002.

[4] X. Li and J. Wang, "A steganographic method based upon JPEG and particle swarm optimization algorithm," Information Sciences 177, 2007.

[5] H. Malekmohammadi and S. Ghaemmaghami, "Steganalysis of LSB Based Image Steganography Using Spatial and Frequency Domain Feature," IEEE, 2009.

[6] Andreas Westfeld, "F5-A Steganographic Algorithm High Capacity Despite Better Steganalysis," Institute for System Architecture, Dresden, Germany, Springer-Verlag Berlin Heidelberg, 2001.

[7] K. Solanki, A. Sarkar, and B. S. Manjunath, " YASS: Yet another steganographic scheme that resists blind steganalysis," in Proc. 9th International Information Hiding Workshop, Lecture Notes in Computer Science, vol. 4567, pp. 16-31, 2007.

[8] M. Dabgar and P. Muliya, "Resisting Blind Steganalysis in Real Time Covert Communication," International Journal of Computer Applications (0975 – 8887), vol. 120, no. 9, June 2015.

[9] X. Qi and K. Wong, "An adaptive DCT-based mod-4 steganographic method," in: IEEE Proceedings of ICIP, vol. II, Sep. 2005.

[10] K. Wong, X. Qi, and K. Tanaka, "A DCT-based Mod4 Steganographic Method," Signal Processing 87, pp. 1251–1263, 2007.

[11] K. Wong, K. Tanaka1, and X. Jun, "Multiple Messages Embedding Using DCT-Based Mod4 Steganographic Method," Springer-Verlag Berlin Heidelberg, 2006.

[12] K. Chakraborty, G. Sanyal, and A. Kundu, "Audio Steganography Using Mod4 Method," Journal of Computing, vol. 3, ISSUE 8, ISSN 2151-9617, August 2011.

[13] P. Suresh and S. Anathan, "Image steganography using mod4 embedding algorithm based on image contrast," International Journal of Current Research, vol. 33, Issue 6, pp. 134-138, June 2011.

Journal Of Electronical & Cyber Defence
Vol. 4, No. 2, 2016, Serial No.14

Improvement Capacity and Transparency, In Steganography Based On Mod4

A. A. Hassani, H. Dehghani*, M. Dehghani, R. Esfahani

*Malek Ashtar University of Technology

(Received: 21/12/2015, Accepted: 06/06/2016)

ABSTRACT

The secure and hidden communication, is one of the essential requirements in cyberspace. Steganography is the best approach, in which the communication security in common network like Internet, is provided. Steganography based on Mod۴ is one of the prevalent methods in DCT transformation domain which embeds the message in the image in different way from the past methods. In this method, correlation between coefficients is kept well and is robust against blind steganalysis .

The ultimate of this paper is to improve steganography based on Mod۴, that is, increasing capacity and transparency, as two principal criteria in steganography. In the proposed method, by changing the size of GQC blocks and by determining the suitable conditions for choosing the valid blocks, transparency is increased more than ۵ percent and capacity is increased more than ۶۸ percent.

For evaluation the stego images transparency in the proposed method, and comparing with basic Mod4 method, two criteria, PSNR and SSIM are used .

Keywords: Steganography, Capacity, Transparency, Mod4, JPEG

* Corresponding Author Email: hamid_deh@yahoo.com