دوفصل‌نامه علمی منادی امنیت فضای تولید و تبادل اطلاعات (افتا)
سال ۱۴۰۱، جلد ۲۰، شماره ۲ (۶۱-۶۸)
https://monadi.isc.org.ir

ارائه‌شده در نوزدهمین کنفرانس بین‌المللی انجمن رمز ایران در دانشگاه گیلان، ۹ و ۱۰ شهریور ۱۴۰۱

نهان‌نگاری تصویر مبتنی بر حوزه موجک با ایده جاسازی در نواحی با تغییرات زیاد زیربانده‌های فرکانس بالا★

وجیهه ثابتی* و معصومه سبحانی سوادرودباری

گروه مهندسی کامپیوتر، دانشکده مهندسی، دانشگاه الزهرا، تهران، ایران

اطلاعات مقاله

کلمات کلیدی:
نهان‌نگاری
نهان‌کاوی
تبدیل موجک گسسته
تبدیل موجک عدد صحیح

dor: 20.1001.1.24763047.1401.11.2.7.6

نوع مقاله: پژوهشی

چکیده

نهان‌نگاری، علم و هنر پنهان‌سازی وجود ارتباط است. در نهان‌نگاری با پنهان کردن اطلاعات در یک رسانه دیجیتال، وجود ارتباط از دید فرد متخاصم مخفی می‌ماند. ایده روش‌های تطبیقی در حوزه‌ی مکان، جاسازی بیشتر در نواحی لبه تصویر است. در این روش‌ها، نواحی‌ای از تصویر که تغییرات بیشتری دارند، در اولویت جاسازی قرار دارند. از طرفِ دیگر روش‌های حوزه تبدیل موجک، برای مطابقت با سیستم بینایی انسان، جاسازی را در زیربانده‌های فرکانس بالا انجام می‌دهند. ایده پیشنهادی در این مقاله، جاسازی با اولویت بیشتر در نواحی‌ای از زیربانده‌های فرکانس بالای حاصل از تبدیل موجک است که تغییرات زیادی دارند. ابتدا با توجه به طول داده، یک حد آستانه تعیین می‌شود که براساس آن نواحی مناسب جاسازی در هر زیربانده فرکانس بالا شناسایی می‌شود و سپس فرآیند جاسازی در آن انجام می‌شود. این فرآیند به نحوی است که گیرنده نیز می‌تواند با تکرار آن، داده را به صورت کامل استخراج کند. نتایج پیاده‌سازی نشان می‌دهد در روش پیشنهادی استفاده از تبدیل موجک عدد صحیح نسبت به تبدیل موجک گسسته موفقیت بیشتری را به همراه دارد. کیفیت تصویر خروجی روش پیشنهادی، نسبت به روش‌های حوزه تبدیل مورد مقایسه، بالاتر و امنیت آن بیشتر است.

© ۱۴۰۱ انجمن رمز ایران

۱ مقدمه

با گسترش ارتباطات دیجیتالی و نیاز به برقرای ارتباطات امن، رمزنگاری[1] و مخفی‌سازی داده[2] به عنوان دو راهکار اصلی در سیستم های امنیت اطلاعات[3] استفاده می‌شوند. نهان‌نگاری[4] و ته‌نقش نگاری[5] روش‌های شناخته شده در علم مخفی‌سازی داده هستند. اگرچه این روش‌ها مفاهیم مشابهی دارند، اما تفاوت‌هایی در اهداف آنها وجود دارد. رمزنگاری برای پنهان کردن معنای پیام رد و بدل شده از افراد غیرمجاز، نهان‌نگاری برای پنهان کردن وجود ارتباط از افراد غیرمجاز و ته‌نقش‌نگاری برای اهدافی مانند حفظ حق کپی، اثبات مالکیت و ... استفاده می‌شود [۱].

روش‌های نهان‌نگاری روش‌هایی هستند که هدف آنها پنهان کردن یک پیام سرّی در یک رسانه میزبان (مانند صوت، تصویر، فیلم، ...) است به نحوی که وجود پیام سرّی برای کسی غیر از گیرنده پیام، قابل کشف نباشد. فرستنده در یک ارتباط سرّی با استفاده از نهان‌نگاری در تصویر،

★از کمیته علمی نوزدهمین کنفرانس بین‌المللی انجمن رمز ایران برای داوری این مقاله تشکر می‌شود.

*نویسنده مسئول
آدرس‌های رایانامه: v.sabeti@alzahra.ac.ir (وجیهه ثابتی)، masomehsobhani@gmail.com (معصومه سبحانی سوادرودباری)

© ۱۴۰۱ تمامی حقوق متعلق به انجمن رمز ایران است.

[1] cryptography [2] information hiding [3] information security system [4] steganography [5] watermarking

فرآیند جاسازی داده را در تصویر میزبان [1] و گیرنده، فرآیند استخراج داده را از تصویر نهان‌نگاری‌شده [2] انجام می‌دهد. در مقابل، برای کشف حضور داده پنهان در یک رسانه، دانشی به نام نهان‌کاوی [3] بوجود آمده است [۲].

در طراحی یک روش نهان‌نگاری خوب سه الزام اصلی مورد نیاز است که عبارتند از: شفافیت ادراکی [4]، ظرفیت جاسازی و امنیت [5]. شفافیت ادراکی یعنی رسانه نهان‌نگاری شده و رسانه میزبان نباید از نظر بصری تفاوتی داشته باشند. منظور از ظرفیت حمل، حداکثر تعداد بیت‌هایی است که می‌تواند در رسانه میزبان مخفی شود. امنیت نیز یعنی حملات نهان‌کاوی موجود قادر به کشف تصاویر نهان‌نگاری‌شده‌ی تولید شده بوسیله این روش نباشند [۳]. در یکی از متداول‌ترین دسته‌بندی‌ها، روش‌های نهان‌نگاری به دو دسته جاسازی در حوزه مکان و حوزه تبدیل تقسیم می‌شوند. معمولا تصاویر نهان‌نگاری‌شده‌ی حاصل از روش‌های دامنه مکانی کیفیت بهتری نسبت به روش‌های دامنه تبدیل دارند و ظرفیت جاسازی روش‌های مکانی نیز بیشتر است. اما معمولا این روش‌ها امنیت پایین‌تری نسبت به روش‌های حوزه تبدیل دارند [۴].

الگوریتم‌های نهان‌نگاری براساس روش تعیین ظرفیت جاسازی هر پیکسل، به دو دسته تطبیقی [6] و غیر تطبیقی تقسیم شده‌اند [۵]. در روش‌های غیرتطبیقی، ظرفیت جاسازیِ هر پیکسل ثابت و مستقل از نواحی اطراف آن است. دسته دوم، روش‌های تطبیقی است که ظرفیت هر پیکسل با توجه به پیکسل‌های همسایه مشخص می‌شود. ایده اصلی این روش‌ها جاسازی بیشتر در نواحی لبه تصویر و جاسازی کمتر در نواحی یکنواخت تصویر است [۶، ۷]. روش تطبیقی بر مبنای پیچیدگی (CBL [7]) یکی از روش‌های تطبیقی موفق است [۸].

جاسازی در نواحی فرکانس بالا در روش‌های حوزه تبدیل را می‌توان معادل ایده‌ی جاسازی در نواحی لبه تصویر در روش‌های حوزه مکان دانست. اما آیا انتخاب ضرایب زیربانده‌های فرکانس بالا برای جاسازی هیچ اولویتی ندارند؟ به عبارت دیگر جاسازی در چه ضرایبی از زیربانده‌های فرکانس بالا منجر به تولید یک تصویر نهان‌نگاری شده با کیفیت بهتر و امنیت بالاتر می‌شود؟ برخلاف بعضی از روش‌های نهان‌نگاری حوزه موجک که هیچ اولویتی در انتخاب ضرایب حوزه موجک درنظر نگرفته‌اند، بعضی از روش‌ها از این ایده استفاده کرده‌اند که بزرگی ضرایب فرکانس بالا، متناظر با شدت لبه‌ها در حوزه مکان است و به همین دلیل در ضرایب بزرگتر، داده بیشتری جاسازی کرده‌اند [۹، ۱۰]. اما در این مقاله یک ایده جدید برای نحوه انتخاب ضرایب فرکانس بالا ارائه شده است. ایده پیشنهادی در این مقاله، انتخاب ضرایبی است که در نواحی یکنواخت زیرباند فرکانس بالا قرار دارند. مهم‌ترین چالش روبروی روش‌های با ایده تطبیقی، امکان شناسایی مجدد نواحی انتخاب شده برای جاسازی توسط گیرنده است.

حوزه تبدیل مورد بررسی در این مقاله تبدیل موجک گسسته (DWT [8]) و تبدیل موجک عدد صحیح (IWT [9]) است. ابتدا تصویر با استفاده از یکی این تبدیل‌ها به حوزه فرکانسی برده می‌شود و سپس داده موردنظر در ضرایب زیرباند HH جاسازی می‌شود. اولویت جاسازی در ضرایب زیرباند HH یکسان نیست و مناطقی از HH که تغییرات بیشتری دارند، در اولویت جاسازی قرار می‌گیرند. تعیین اولویت به نحوی است که گیرنده نیز با دریافت تصویر نهان‌نگاری‌شده می‌تواند این اولویت را تشخیص دهد و داده جاسازی شده را به صورت کامل استخراج کند.

در ادامه، در بخش ۲، تعدادی از کارهای حوزه تبدیل موجک مرور می‌شود. در بخش ۳، مراحل الگوریتم جاسازی و استخراج روش پیشنهادی و در بخش ۴، نتایج پیاده‌سازی و مقایسه این روش ارائه می‌شود. در بخش انتهایی نیز نتیجه‌گیری و پیشنهاداتی برای ادامه کار ارائه می‌شود.

۲ مرور کارهای مرتبط

تبدیل‌های DWT و IWT از شناخته شده‌ترین روش‌های مورد استفاده در نهان‌نگاری هستند. در حوزه DWT، تبدیل موجک Haar ساده‌ترین نوع تبدیل موجک است. چهار باند به دست آمده از این تبدیل عبارتند از: نوار تقریب (LL)، نوار عمودی (LH)، نوار افقی (HL) و نوار جزئیات مورب (HH). نوار تقریب شامل ضرایب موجک فرکانس پایین می‌باشد که بخش قابل توجهی از تصویر دامنه مکان را تشکیل می‌دهد. نوارهای دیگر (نوارهای جزئیات) شامل ضرایب فرکانس بالا هستند که جزئیات لبه‌های تصویر دامنه مکان را نشان می‌دهند [۱۳].

در تبدیل معکوس موجک گسسته، ممکن است برخی از اطلاعات هنگام استخراج داده محرمانه از دست بروند و منجر به شکست سیستم مخفی‌سازی شود. برای جلوگیری از این مشکل از تبدیل IWT استفاده می‌شود. در این تبدیل یک مجموعه داده صحیح به مجموعه داده صحیح دیگری نگاشت می‌شود و مشکل استخراج وجود ندارد [؟ ، ۱۴] در ادامه تعدادی از روش‌های نهان‌نگاری در حوزه تبدیل موجک بررسی می‌شود.

در [۹]، دو روش در دامنه‌های مکان و تبدیل ارائه شده است. در این روش ضرایب فرکانسی IWT به قالب‌های ۳ × ۳ تقسیم شده‌اند. ضرایب گوشه هر قالب، شدت لبه بودن کل قالب را نشان می‌دهد و می‌توانند تعداد بیت‌های مخفی که می‌تواند در ضرایب دیگر قالب تعبیه شود، را تعیین کنند. جاسازی در قالب‌های لبه با استفاده از تابع XOR انجام می‌شود. به این ترتیب، با توجه به عدم تغییر ضرایب گوشه در هر قالب، گیرنده نیز می‌تواند بدون خطا داده‌ها را استخراج کند. با افزایش طول داده، از کیفیت خروجی‌های این روش کاسته می‌شود

در [۱۵]، با استفاده از الگوریتم ژنتیک، رویکرد جدیدی برای پنهان کردن داده‌ها در حوزه تبدیل ارائه شده است. بر خلاف روش‌های دیگر که تبدیل مشخصی مانند موجک عدد صحیح را برای شروع فرآیند جاسازی انتخاب می‌کنند، در این روش از یک فضای تبدیل ثابت استفاده نشده

[1] host image [2] stego image [3] steganalysis [4] imperceptibility [5] security [6] adaptive methods [7] Complexity Based LSB-M (CBL) [8] Discrete Wavelet Transform (DWT)

[9] Integer Wavelet Transform (IWT)

است و هر بار با توجه به اطلاعات مخفی و تصویر میزبان انتخاب می‌شود. تصاویر میزبان با استفاده از مفهوم تبدیل موجک تطبیقی و الگوریتم ژنتیک به یک دامنه تبدیل مناسب نگاشت می‌شود. در فضای بدست آمده، اطلاعات مخفی موردنظر در ضرایب تبدیل که نمایانگر لبه‌های تصویر در حوزه مکان هستند، جاسازی می‌شود. بنابراین تصویر میزبان کمترین تغییر و به عبارت دیگر بیشترین سازگاری را با سیستم بینایی انسان دارد. نتایج شبیه سازی نشان می‌دهد که این روش پیشنهادی نسبت به کارهای قبلی در معیار PSPNR عملکرد بهتری دارد.

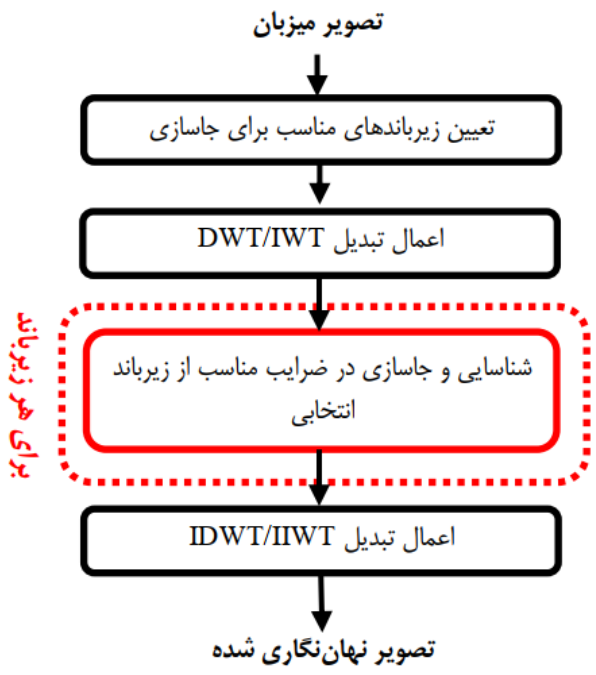
در [۱۰] روش جدیدی با ایده جاسازی بیشتر در ضرایب لبه ارائه شده است. در این روش، پس از اعمال تبدیل IWT روی تصویر میزبان، از بیت‌های پر ارزش ضرایب تبدیل برای تصمیم‌گیری در مورد چگونگی جاسازی استفاده شده است. جاسازی به گونه‌ای انجام می‌شود که تغییری در بیت‌های پر ارزش B ضرایب ایجاد نشده و با توجه به این بخش از ضرایب، گیرنده می‌تواند از تصمیمات فرستنده آگاهی داشته و داده‌های جاسازی شده را استخراج کند. در این روش، ضرایب با توجه به مقدار خود، طبقه بندی شده و هر گروه مقدار مشخصی از اطلاعات مخفی را حمل می کند. اگرچه این روش بر اساس معیارهای PSNR برتری قابل توجهی نسبت به روش‌های مقایسه شده ندارد، اما PSPNR بالاتری دارد.

۳ روش پیشنهادی

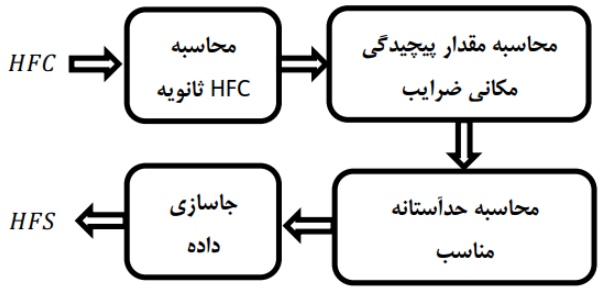
با جاسازی در ضرایب فرکانس بالا در حوزه تبدیل، تغییرات در نواحی لبه تصویر اعمال می‌شود که مکان‌های مناسب‌تری برای جاسازی هستند. اما نحوه انتخاب از میان این ضرایب و اولویت بندی آنها برای شرکت در فرآیند جاسازی داده یک چالش مهم است. در این مقاله یک روش نهان‌نگاری حوزه تبدیل پیشنهاد شده است که ایده اصلی آن جاسازی در نواحی با تغییر زیاد در زیربندهای فرکانس بالای حاصل از تبدیل موجک تصویر است. در واقع در روش پیشنهادی، زیربند فرکانس بالا مانند یک تصویر فرض شده است و در این تصویر، نواحی یکنواخت و لبه شناسایی شده و جاسازی در ضرایبی انجام می‌شود که در نواحی غیریکنواخت از زیربند فرکانس بالا قرار دارد. برای رسیدن به این هدف باید این نواحی توسط فرستنده شناسایی شود و بعلاوه روش شناسایی به نحوی باشد که گیرنده نیز بتواند دقیقا همین نواحی را در تصویر دریافتی شناسایی کند و داده جاسازی شده را به صورت کامل استخراج کند. با توجه به موفقیت ایده روش CBL در انجام این کار در حوزه مکان، از ایده همین روش در روش پیشنهادی استفاده شده است.

الگوریتم کلی روش پیشنهادی در شکل ۱ نمایش داده شده است. این روش به گونه‌ای است که در هر دو حوزه IWT و DWT قابل اجرا است و مراحل الگوریتم تفاوتی ندارد، اما در بخش نتیجه‌گیری عملکرد این دو حالت نسبت به هم سنجیده می‌شود و مشخص خواهد شد کدام یک از این تبدیل‌ها برای اجرای الگوریتم پیشنهادی مناسب‌تر است.

مراحل الگوریتم جاسازی در روش پیشنهادی عبارتند از:



شکل ۱. مراحل الگوریتم جاسازی روش پیشنهادی



شکل ۲. مراحل جاسازی داده در یک زیربند فرکانسی

(۱) انتخاب زیربند مورد نظر برای جاسازی (با توجه به طول داده محرمانه)

(۲) اعمال تبدیل موجک گسسته دو بعدی (یا تبدیل موجک عدد صحیح) بر روی تصویر میزبان

(۳) یافتن مکان‌های مناسب برای جاسازی و انجام عملیات جاسازی (برای هر زیربند به صورت مستقل)

(۴) اعمال تبدیل معکوس موجک گسسته (IDWT [1]) (یا معکوس موجک عدد صحیح (IIWT [2]))

اگر طول داده از ضرایب زیربند HH بلاک‌ها کمتر است، استفاده از زیربند HH برای جاسازی داده کافی است، در غیر این صورت می‌توان داده را در هر سه زیربند HH، HL و LH پخش کرد. اگر بیشتر از یک زیربند برای جاسازی انتخاب شود، مرحله ۳ برای هر زیربند انتخابی یک بار اجرا می‌شود. برای کامل شدن الگوریتم جاسازی لازم است مرحله ۳ شرح داده شود.

در شکل ۲، مراحل لازم برای اجرای مرحله ۳ نمایش داده شده است. HFC، زیربند فرکانس بالای انتخابی از تصویر میزبان است که باید

[1] Inverse Discrete Wavelet Transform (IDWT) [2] Inverse Integer Wavelet Transform (IIWT)

```
set PRNG seed;
for each cefficient HFC(i,j)
    r ← random number ∈ [0,1];
    if HFC(i,j) is odd then
        if r ≤ 0.5 then
            HFC'(i,j) ← HFC(i,j) + 1;
        else
            HFC'(i,j) ← HFC(i,j) − 1;
        end if
    else
        HFC'(i,j) ← HFC(i,j);
    end if
end for
```

شکل ۳. الگوریتم تشکیل HFC ثانویه

عملیات جاسازی داده در آن اجرا شود. ضرایب حاصل از جاسازی داده، زیرباند فرکانس بالای متناظر در تصویر نهان‌نگاری شده را تشکیل می‌دهد که با HFS نشان داده شده است.

فرستنده جهت تشخیص ضرایبِ مناسب برای جاسازی از HFC ثانویه (HFC') استفاده می‌کند. برای تشکیل HFC'، ضرایب زوج HFC مستقیماً در HFC' قرار می‌گیرند و ضرایب فرد، به صورت تصادفی یک واحد افزایش یا کاهش یافته و سپس در HFC' قرار می‌گیرند. الگوریتم این عملیات در شکل ۳ نشان داده شده است.

خط ابتدایی این الگوریتم، مقداردهی هسته‌ی ابتدایی تابع تولید اعداد شبه تصادفی است. فرستنده از مقدار ابتدایی استفاده شده در این مرحله، در مرحله جاسازی داده نیز استفاده می‌کند و بعلاوه همین مقدار را به عنوان کلید در اختیار گیرنده قرار می‌دهد تا گیرنده نیز بتواند همین روند را تکرار کند. درغیراین صورت، گیرنده قادر به استخراج کامل داده جاسازی شده نیست.

در مرحله بعد برای هر ضریب در HFC ثانویه یک معیار پیچیدگی مکانی با عنوان $Dif(i,j)$ محاسبه می‌شود. مقدار این پارامتر نشان دهنده چگونگی ناحیه‌ای است که این ضریب در آن قرار گرفته است. برای محاسبه این معیار، اطراف هر ضریب یک پنجره ۳×۳ درنظرگرفته می‌شود. مقدار $Dif(i,j)$ برابر مجموع قدرمطلق تفاوت هر ضریب با ضریب‌های همسایه است که پیچیدگی مکانی ضریب را نشان می‌دهد. با توجه به این روش محاسبه، هر چه $Dif(i,j)$ بزرگتر باشد، نشان می‌دهد که ضریب موردنظر در یک ناحیه با تغییرات بیشتری واقع شده است و کوچکتر بودن این معیار نشان دهنده یکنواخت‌تر بودن ناحیه همسایگی ضریب موردنظر است. بنابراین، ضرایب با معیار پیچیدگی مکانی بیشتر برای جاسازی مناسب‌تر هستند.

معیار پیچیدگی یک معیار نسبی است و با توجه به مقدار آن به طور مطلق نمی‌توان یک پیکسل را متعلق به یک ناحیه یکنواخت یا غیر یکنواخت نامید. بنابراین در گام سوم، برای تصمیم‌گیری در مورد جاسازی کردن یا نکردن در یک ضریب به یک حد آستانه (T) برای معیار پیچیدگی نیاز است. ضرایب با معیار پیچیدگی بیشتر از حد آستانه، متعلق به ناحیه لبه و مناسب برای جاسازی تشخیص داده می‌شود و بالعکس.

مقدار T، طبق فرمول (۱) محاسبه می‌شود:

$$T = \max\{t_\circ : |\{(i,j): Dif(i,j) \geq t_\circ\}| \geq L \qquad (۱)$$

مقدار T به تصویر میزبان و مقدار L که طول داده مورد نظر برای جاسازی است بستگی دارد. به عبارت دیگر این مقدار در تصاویر میزبان مختلف و به ازای Lهای مختلف، متفاوت است.

در آخرین مرحله باید داده مورد نظر را در ضرایب مناسب جاسازی کرد. جاسازی داده در بیت کم ارزش(LSB [1]) ضرایبی که مقدار پیچیدگی بزرگتر از T دارند، انجام می‌شود. شبه کد شکل ۴ الگوریتم جاسازی را نشان می‌دهد. d، دنباله داده‌ای است که باید در HFC جاسازی شود. HFC' در مراحل قبلی ساخته شد و خروجی این مرحله HFS است. برای تبدیل هر ضریب HFC به یک ضریب در HFS سه حالت وجود دارد: (۱) اگر مقدار معیار پیچیدگی مکانی ضریب کمتر از T است، در HFS کپی می‌شود. (۲) درغیر این صورت، اگر بیت داده موردنظر برای جاسازی در این ضریب صفر باشد، ضریب متناظر آن در HFC'، در HFS کپی می‌شود. (۳) در غیر این صورت، ضریب متناظر آن در HFC' با توجه به عدد تصادفی تولید شده، یک واحد افزایش یا کاهش یافته و سپس در HFS کپی می‌شود.

فرستنده پس از ساخت HFS و اجرای تبدیل معکوس مناسب، تصویر نهان‌نگاری شده را تولید می‌کند.

لازم به ذکر است که گیرنده برای استخراج داده جاسازی شده باید تمام مراحل شکل ۱ را روی تصویر دریافتی تکرار کند، با این تفاوت که پس از شناسایی ضرایب مناسب برای جاسازی، از طریق محاسبه باقیمانده تقسیم این ضرایب بر ۲، داده جاسازی شده در هر ضریب را شناسایی کند. از کنار هم قرار دادن این بیت‌ها، رشته داده جاسازی شده به صورت کامل بازسازی می‌شود.

۴ نتایج پیاده سازی

در بخش قبل دو روش حوزه تبدیل ارائه شد که براساس نوع تبدیل مورد استفاده، CBL-DWT و CBL-IWT نام‌گذاری شده‌اند. این روش‌ها در

[1] Least Significant Bit (LSB)

```
set PRNG seed;
k ← 0;
for each cefficient HFC(i,j)
    r ← random number ∈ [0,1];
    if Dif(i,j) < T
        HFS(i,j) ← HFC(i,j);
    else
        if HFC'(i,j) mod 2 ≠ d(k)
            if r ≤ 0.5 then
                HFS(i,j) ← HFC'(i,j) − 1;
            else
                HFS(i,j) ← HFC'(i,j) + 1;
            end if
        else
            HFS(i,j) ← HFC'(i,j);
        end if
        k ← k + 1;
    end if
end for
```

شکل ۴. الگوریتم جاسازی داده

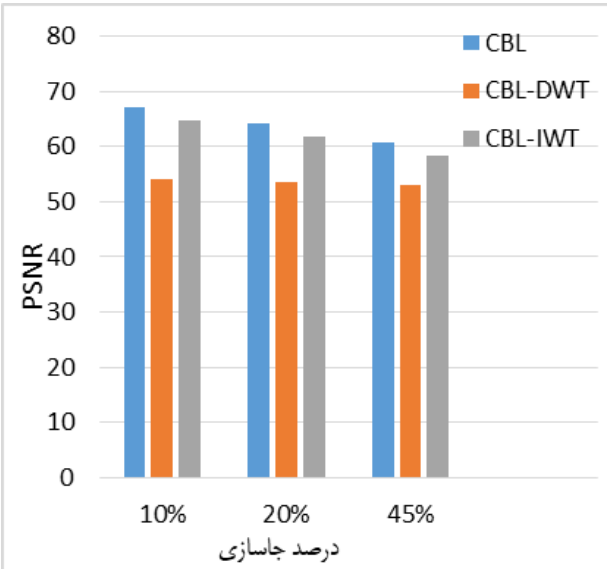
نرم‌افزار Matlab پیاده‌سازی شد و برای مقایسه آن‌ها، تست‌های مختلفی انجام شد که در ادامه نتایج مهم‌ترین تست‌های انجام شده ارائه می‌شود.

کیفیت تصویر نهان‌نگاری‌شده یکی از مهم‌ترین عامل‌ها در نهان‌نگاری است که معیارهای مختلفی برای سنجش آن وجود دارد. در گام اول جهت مقایسه دو روش پیشنهادی با روش CBL حوزه مکان، معیارهای کیفیت بصری PSNR، شباهت ساختاری (SSIM) و همبستگی (CF) برای دو تصویر نمونه Baboon و Peppers در سه سطح جاسازی ۲۵٪، ۵۰٪ و ۷۵٪ (از ظرفیت زیرباند HH تصویر) محاسبه شده و نتایج در جدول ۱ نشان داده شده است. بررسی نتایج نشان می‌دهد که طبق انتظار، روش CBL حوزه مکان قادر به تولید تصاویر نهان‌نگاری‌شده با کیفیت بالاتری نسبت به دو روش پیشنهادی حوزه تبدیل است. اما از میان دو روش پیشنهادی حوزه تبدیل، روش CBL-IWT موفق‌تر از روش CBL-DWT است که به دلیل تخریب کمتر این نوع تبدیل موجک است.

برای بررسی کامل‌تر، در شکل ۵، میانگین معیار PSNR در سه روش جاسازی برای ۲۰۰ تصویر تست پایگاه داده NRCS در سه سطح جاسازی مختلف نشان داده شده است که CBL مکانی بهترین عملکرد و CBL-IWT در رتبه دوم قرار دارد.

درصد جاسازی	تصویر	روش جاسازی	CF	SSIM	PSNR
۲۵٪	Baboon	CBL	۰٫۹۹۹۹۹	۰٫۹۹۹۹۹	۶۳٫۲۰
		CBL-DWT	۰٫۹۹۹۹۴	۰٫۹۹۹۲۱	۵۳٫۵۳
		CBL-IWT	۰٫۹۹۹۹۸	۰٫۹۹۹۹۶	۶۰٫۴۳
	Peppers	CBL	۰٫۹۹۹۹۹	۰٫۹۹۹۹۹	۶۳٫۱۹
		CBL-DWT	۰٫۹۹۹۹۶	۰٫۹۹۹۲۰	۵۳٫۴۵
		CBL-IWT	۰٫۹۹۹۹۹	۰٫۹۹۹۴۳	۶۰٫۷۱
۵۰٪	Baboon	CBL	۰٫۹۹۹۹۸	۰٫۹۹۹۹۷	۶۰٫۲۲
		CBL-DWT	۰٫۹۹۹۹۳	۰٫۹۹۹۱۶	۵۲٫۸۳
		CBL-IWT	۰٫۹۹۹۹۷	۰٫۹۹۹۸۸	۵۷٫۵۸
	Peppers	CBL	۰٫۹۹۹۹۹	۰٫۹۹۹۸۵	۶۰٫۱۹
		CBL-DWT	۰٫۹۹۹۹۶	۰٫۹۹۴۶۱	۵۲٫۷۹
		CBL-IWT	۰٫۹۹۹۹۸	۰٫۹۹۸۴۸	۵۷٫۹۵
۷۵٪	Baboon	CBL	۰٫۹۹۹۹۷	۰٫۹۹۹۹۶	۵۸٫۴۲
		CBL-DWT	۰٫۹۹۹۹۲	۰٫۹۹۹۰۲	۵۲٫۲۴
		CBL-IWT	۰٫۹۹۹۹۵	۰٫۹۹۹۶۴	۵۵٫۹۷
	Peppers	CBL	۰٫۹۹۹۹۸	۰٫۹۹۹۶۰	۵۸٫۴۱
		CBL-DWT	۰٫۹۹۹۹۵	۰٫۹۹۳۷۶	۵۲٫۲۰
		CBL-IWT	۰٫۹۹۹۹۷	۰٫۹۹۷۲۰	۵۶٫۳۶

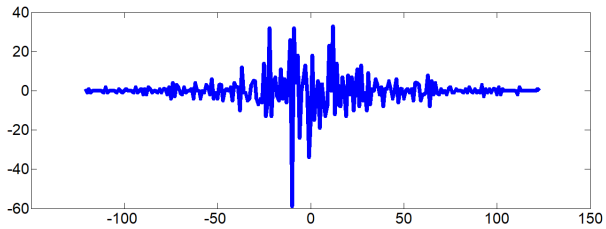
جدول ۱. معیارهای CF، SSIM و PSNR دو تصویر نمونه در سه سطح جاسازی مختلف با سه روش جاسازی متفاوت



شکل ۵. معیار PSNR سه روش جاسازی برای تصاویر NRCS

درصد جاسازی	[۹] PSPNR	[۹] PSNR	[۱۰] PSPNR	[۱۰] PSNR	[CBL-IWT] PSPNR	[CBL-IWT] PSNR
۱۰٪	۶۴٫۷۶	۷۶٫۶۹	۶۳٫۸۰	۷۷٫۲۳	۶۴٫۵۹	۸۲٫۳۳
۲۰٪	۶۱٫۵۰	۷۱٫۹۲	۶۰٫۶۶	۷۴٫۰۱	۶۱٫۷۱	۷۹٫۵۹
۴۵٪	۵۶٫۹۱	۶۴٫۴۵	۵۶٫۷۹	۶۶٫۹۹	۵۸٫۳۷	۷۷٫۰۸

جدول ۲. مقایسه روش پیشنهادی با دو روش حوزه تبدیل موجود براساس معیارهای PSNR و PSPNR



شکل ۶. اختلاف میان PDH تصویر میزبان و PDH تصویر نهان‌نگاری شده حاصل از جاسازی ۲۵٪

در گام بعد، دو روش حوزه تبدیل موجود شامل [۹] و [۱۰] برای مقایسه با روش پیشنهادی انتخاب شدند. برای این مقایسه علاوه بر معیار PSNR از معیار PSPNR نیز استفاده شده است [۱۰]. اگرچه امکان معرفی کامل این معیار در اینجا وجود ندارد، فقط به این نکته اشاره می‌شود که روش‌هایی که در نواحی لبه تصویر جاسازی می‌کنند و با سیستم بینایی انسان مطابقت بیشتری دارند، معیار PSPNR بالاتری کسب می‌کنند.

در جدول ۲، میانگین معیارهای PSNR و PSPNR برای تصاویر پایگاه داده SIPI برای دو روش قبلی و موفق‌ترین روش پیشنهادی (CBL-IWT) در سه سطح جاسازی نشان داده شده است. این نتایج نشان دهنده برتری کامل روش پیشنهادی در معیار PSPNR است. بعلاوه با افزایش ظرفیت جاسازی برتری معیار PSNR حاصل از روش CBL-IWT بیشتر نمایان می‌شود.

برای تحلیل میزان امنیت روش پیشنهادی، ابتدا از تحلیل PDH [1] (یک بستر استخراج پارامترهای نهان‌کاوی) استفاده شده است. بررسی اختلاف میان PDH های تصویر Lena و تصویر حاصل از جاسازی ۲۵٪ (شکل ۶) نشان می‌دهد که در روش پیشنهادی اختلاف میان پیکسل‌های مجاور در اثر جاسازی تغییر بسیار ناچیزی دارد و این روش در برابر تمام حملاتی که برمبنای پارامترهای مستخرج از PDH کار می‌کنند، ایمن است.

در آخرین تحلیل از حمله SPAM به عنوان یک حمله موفق موجود استفاده شده است. برای سنجش میزان تأثیر استفاده از ایده CBL در حوزه تبدیل، امنیت روش پیشنهادی با روش LSB-IWT و CBL مقایسه شده است. در LSB-IWT برای جاسازی در ضرایب IWT از روش LSB ساده استفاده شده است و ایده یافتن نواحی لبه در آن وجود ندارد. دقت

[1] Pixel Difference Histogram (PDH)

درصد جاسازی	LSB-IWT دقت	CBL دقت	CBL-IWT دقت
۱۰٪	۵۳٫۲۸	۵۱٫۵۰	۵۱٫۳۵
۲۵٪	۵۷٫۷۰	۵۴٫۲۰	۵۲٫۶۷
۴۵٪	۶۶٫۱۴	۶۰٫۲۵	۵۷٫۷۶

جدول ۳. دقت کشف سه روش نهان‌نگاری با حمله SPAM در سه سطح جاسازی مختلف

کشف این سه روش توسط SPAM در جدول ۳ نشان داده شده است. بررسی این نتایج نشان می‌دهد اگرچه روش CBL در معیارهای کیفیت تصویر نهان‌نگاری شده نسبت به روش پیشنهادی برتری دارد، اما روش پیشنهادی در برابر حمله SPAM احتمال کشف کمتر و به عبارت دیگر، امنیت بیشتری نسبت به CBL مکانی دارد. بعلاوه امنیت بیشتر روش CBL-IWT نسبت به LSB-IWT نشان می‌دهد که برای جاسازی در ضرایب حوزه موجک بهتر است از ضرایبی استفاده شود که در نواحی لبه قرار دارند.

۵ نتیجه‌گیری

تبدیل موجک یکی از رایج‌ترین تبدیل‌های مورد استفاده در روش‌های نهان‌نگاری است. برخلاف بسیاری از روش‌های نهان‌نگاری حوزه تبدیل موجود که در فرآیند جاسازی اولویت خاصی برای انتخاب ضرایب فرکانس بالای حاصل از تبدیل تعریف نمی‌کنند، روش پیشنهادی به دنبال شناسایی نواحی با تغییرات زیاد در زیربانده‌های فرکانس بالای حاصل از تبدیل موجک و جاسازی در این نواحی است. برای بررسی امکان جاسازی در هر ضریب، از یک همسایگی ۳×۳ اطراف آن استفاده شده و در صورتی که مجموع اختلافات ضرایب همسایه با این ضریب از یک حد آستانه بیشتر باشد، آن ضریب مناسب جاسازی تشخیص داده می‌شود. حد آستانه براساس طول داده موردنظر مشخص می‌شود. نتایج پیاده سازی نشان می‌دهد اگرچه استفاده از این ایده در حوزه مکان در تولید تصاویر نهان‌نگاری شده با کیفیت بالا موفق‌تر است اما برای حوزه تبدیل، استفاده از تبدیل IWT به همراه این ایده نسبت به DWT برتر است. روش پیشنهادی موفق به جاسازی در لبه‌های تصویر شده است و نسبت به روش‌های حوزه تبدیل از PSNR و PSPNR بالاتری برخوردار است. در آینده می‌توان از ترکیب الگوریتم‌های بهینه‌سازی با ایده پیشنهادی در حوزه تبدیل استفاده کرد.

مراجع

[1] Kadhim, Inas Jawad, Premaratne, Prashan, Vial, Peter James, and Halloran, Brendan. Comprehensive survey of image steganography: Techniques, evaluations, and trends in future research. *Neurocomputing*, 335:299–326, 2019.

[2] Evsutin, Oleg, Melman, Anna, and Meshcheryakov, Roman. Algorithm of error-free information embedding into the dct domain of digital images based on the qim method using adaptive masking of distortions. *Signal Processing*, 179:107811, 2021.

[3] Yadav, Gyan Singh and Ojha, Aparajita. Hamiltonian path based image steganography scheme with improved imperceptibility and undetectability. *Applied Soft Computing*, 73:497–507, 2018.

[4] Kadhim, Inas Jawad, Premaratne, Prashan, and Vial, Peter James. High capacity adaptive image steganography with cover region selection using dual-tree complex wavelet transform. *Cognitive Systems Research*, 60:20–32, 2020.

[5] Hussain, Mehdi, Wahab, Ainuddin Wahid Abdul, Idris, Yamani Idna Bin, Ho, Anthony TS, and Jung, Ki-Hyun. Image steganography in spatial domain: A survey. *Signal Processing: Image Communication*, 65:46–66, 2018.

[6] Sunder, R, Eswaran, P, Rajan, A Nagalinga, and Poonkuntran, S. High capacity data embedding in images by pixel triplets matching. *International Journal of Computer Applications*, 975:8887, 2013.

[7] Hong, Wien and Chen, Tung-Shou. A novel data embedding method using adaptive pixel pair matching. *IEEE transactions on information forensics and security*, 7(1):176–184, 2011.

[8] Sabeti, Vajiheh, Samavi, Shadrokh, and Shirani, Shahram. An adaptive lsb matching steganography based on octonary complexity measure. *Multimedia tools and applications*, 64:777–793, 2013.

[9] Al-Dmour, Hayat and Al-Ani, Ahmed. A steganography embedding method based on edge identification and xor coding. *Expert systems with Applications*, 46:293–306, 2016.

[10] Miri, Aref and Faez, Karim. An image steganography method based on integer wavelet transform. *Multimedia Tools and Applications*, 77:13133–13144, 2018.

[11] Luo, Weiqi, Huang, Fangjun, and Huang, Jiwu. Edge adaptive image steganography based on lsb matching revisited. *IEEE Transactions on information forensics and security*, 5(2):201–214, 2010.

[12] Laishram, Debina and Tuithung, Themrichon. A novel minimal distortion-based edge adaptive image steganography scheme using local complexity: (beass). *Multimedia Tools and Applications*, 80(1):831–854, 2021.

[13] Zagade, Swapnali and Bhosale, Smita. Secret data hiding in images by using dwt techniques. *International Journal of Engineering and Advanced Technology*, 3(5), 2014.

[14] Muhuri, Pranab K, Ashraf, Zubair, and Goel, Swati. A novel image steganographic method based on integer wavelet transformation and particle swarm optimization. *Applied Soft Computing*, 92:106257, 2020.

[15] Miri, Aref and Faez, Karim. Adaptive image steganography based on transform domain via genetic algorithm. *Optik*, 145:158–168, 2017.

MonadiAfta-Bianual Scientific Journal for Cyberspace Security
2022, Volume 20, Number 2 (pp. 61–68)
https://monadi.isc.org.ir

Presented at the ISCISC 2022 in University of Giulan, Rasht, Iran

Wavelet-based Image Steganography using the Idea of Embedding in Areas of High Frequency Subbands with Large Variations★

Vajiheh Sabeti * and Masomeh Sobhani

Department of Computer Engineering, Faculty of Engineering, Alzahra University, Tehran, Iran

ARTICLE INFO.

Keywords:
steganography
steganalysis
discrete wavelet transform
integer wavelet transform

dor: 20.1001.1.24763047.1401.11.2.7.6

Type: research paper

ABSTRACT

Steganography is the science and art of hiding the existence of communication. In steganography, by hiding information in a digital media, the existence of communication remains hidden from the enemy's view. The idea of spatial-based adaptive methods is to embed more in the edge areas of the image. In these methods, areas of the image that have more changes are prioritized for embedding. On the other hand, wavelet-based methods perform embedding in high frequency subbands to match the human vision system. The proposed idea in this paper is embedding with higher priority in areas of high frequency subbands resulting from wavelet transform that have many changes. First, according to the length of the data, a threshold value is determined, based on which suitable embedding areas are identified in each high frequency subband, and then the embedding process is performed in them. This process is such that the receiver can extract the data completely by repeating it. The implementation results show that in the proposed method, the use of Integer Wavelet Transform (IWT) is more successful than Discrete Wavelet Transform (DWT). The quality of the resulted stego image is higher and its security is more than the other wavelet-based methods.

© 2022 ISC

★ The ISCISC 2022 Program Committee effort is highly acknowledged for reviewing this paper.
* Corresponding author
Email addresses: v.sabeti@alzahra.ac.ir (Vajiheh Sabeti), masomehsobhani@gmail.com (Masomeh Sobhani)
© 2022 ISC. All rights reserved.