Journal of Soft Computing and Information Technology (JSCIT)
Babol Noshirvani University of Technology, Babol, Iran
Journal Homepage: jscit.nit.ac.ir
Volume 9, Number 3, Fall 2020, pp. 55-66
Received: 05/21/2019, Revised: 02/29/2020, Accepted: 03/06/2020

Adaptive Image Steganography in the Difference Value of Discrete Cosine Transform Coefficients

Vajiheh Sabeti[1*], Sara Ahmadi[2]
1*- Department of Engineering and Technology, Alzahra University, Tehran, Iran.
2- Department of Engineering and Technology, Alzahra University, Tehran, Iran.
[1*]v.sabeti@alzahra.ac.ir and [2]sara.ahmadi@gmail.com

Corresponding author address: Vajiheh Sabeti, Faculty of Engineering and Technology, Alzahra University, Tehran, Iran, Post Code: 1993893973.

Abstract- Steganography is the science and art to conceal the existence of communication, by hiding information in a digital media, the existence of communication is hidden from the enemy's point of view. steganography in the frequency transform coefficients and in particular the discrete cosine transform (DCT), due to its low detection capability, is one of the most common and active areas of steganography among researchers. But most of the methods in this area have used embedding directly in the DCT coefficients. The main purpose of the proposed method in this paper is to suggest a different embedding platform in this field. In the proposed embedding method, the DCT transformation coefficients are coupled and embedding is on the difference value of each couple. The embedding is done in such a way that the receiver can extract the data completely by calculating the difference in the value of the neighboring pairs. The proposed method is an adaptive method because the number of embedded bits in each pair of coefficients is dependent on the difference between them. The results of various experiments show that the proposed method, with the preservation of the quality of the stego image at a desirable level and having a reasonable embedding capacity, is less likely to be detected in relation to the existing steganalysis attacks.

Keywords- Steganography, Steganalysis, Image, Discrete cosine transform.

مجله علمی پژوهشی رایانش نرم و فناوری اطلاعات
دانشگاه صنعتی نوشیروانی بابل
صفحه مجله: jscit.nit.ac.ir
جلد ۹، شماره ۳، پائیز ۱۳۹۹ ، صفحه ۵۵-۶۶
دریافت: ۱۳۹۸/۰۲/۳۱، بازنگری: ۱۳۹۸/۱۲/۱۰، پذیرش: ۱۳۹۸/۱۲/۱۶

نهان‌نگاری تطبیقی تصاویر در مقدار اختلاف ضرایب کسینوس گسسته

وجیهه ثابتی*[۱]، سارا احمدی[۲]
*۱- دانشکده فنی و مهندسی، دانشگاه الزهرا، تهران، ایران.
۲- دانشکده فنی و مهندسی، دانشگاه الزهرا، تهران، ایران
[1*]v.sabeti@alzahra.ac.ir, [2]sara.ahmadi@gmail.com

* نشانی نویسنده مسئول: وجیهه ثابتی، تهران، خیابان ده ونک، دانشگاه الزهرا، دانشکده فنی و مهندسی، کد پستی: ۱۹۹۳۸۹۳۹۷۳

چکیده- نهان‌نگاری علم و هنر پنهان‌سازی وجود ارتباط است، بدین صورت که با پنهان کردن اطلاعات در یک رسانه دیجیتال وجود ارتباط از دید فرد متخاصم پنهان می‌ماند. نهان‌نگاری در ضرایب تبدیلات فرکانسی و به صورت خاص تبدیل کسینوس گسسته (DCT)، به دلیل قابلیت کشف کمتر، یکی از رایج‌ترین و فعال‌ترین حوزه‌های نهان‌نگاری در میان محققان است. اما اکثر روش‌های موجود در این حوزه از جاسازی مستقیم در ضرایب DCT استفاده کرده‌اند. هدف اصلی روش پیشنهادی در این مقاله، پیشنهاد یک بستر جاسازی متفاوت در این حوزه است. در روش پیشنهادی جاسازی در مقدار اختلاف زوج ضریب حاصل از تبدیل DCT انجام می‌شود. جاسازی به نحوی انجام می‌شود که گیرنده می‌تواند با محاسبه اختلاف مقدار زوج‌های همسایه، داده را به صورت کامل استخراج کند. روش پیشنهادی یک روش تطبیقی محسوب می‌شود، زیرا تعداد بیت‌های قابل جاسازی در هر زوج ضریب متغیر و وابسته به مقدار اختلاف آن‌ها است. نتایج آزمایش‌های مختلف نشان می‌دهد روش پیشنهادی با حفظ کیفیت تصویر نهان نگاری شده در حد مطلوب و داشتن یک ظرفیت جاسازی مناسب، احتمال کشف کمتری در برابر حملات نهان کاوی موجود دارد.

واژه‌های کلیدی: نهان‌نگاری، نهان‌کاوی، تصویر، تبدیل کسینوس گسسته

۱- مقدمه

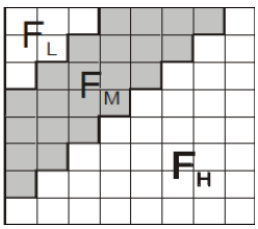
امنیت ارتباطات مساله مهمی است که امروزه به عنوان چالش اصلی در زمینه ارتباطات مطرح می‌شود. رمزنگاری و نهان‌نگاری دو روش برای تامین امنیت با دو سطح امنیتی مختلف، خصوصا در شبکه‌های ناامن، محسوب می‌شوند. رمزنگاری از یک سو حافظ امنیت است و از سوی دیگر گاهی وجود همین رمز نوعی نشت اطلاعات به حساب می‌آید و باید از یک سطح پوششی استفاده نمود. هدف از نهان‌نگاری در دنیای کامپیوتر مخفی کردن وجود ارتباط است، بدین مفهوم که اطلاعات درون یک رسانه دیجیتال پنهان می‌شود به طوری که گمانی مبنی بر وجود اطلاعات درون این رسانه برانگیخته نشود. از میان رسانه‌های مختلف، تصویر، به علت ظرفیت بالا، تنوع حجم و قالب و نیز فراگیر بودن بیشتر مورد توجه قرار گرفته است و یکی از مهم‌ترین رسانه‌ها در زمینه نهان نگاری محسوب می‌شود [۱].

فرستنده در یک ارتباط سرّی با استفاده از نهان‌نگاری، فرآیند جاسازی داده در تصویر میزبان را انجام می‌دهد و تصویر نهان نگاری شده را تولید و ارسال می‌کند. در مقابل گیرنده، فرآیند استخراج داده را از تصویر نهان‌نگاری شده انجام می‌دهد. در طراحی یک روش نهان‌نگاری خوب سه الزام اصلی مورد نیاز است که عبارتند از: شفافیت ادراکی، ظرفیت حمل و امنیت. شفافیت ادراکی یعنی رسانه نهان‌نگاری شده و رسانه میزبان نباید از نظر ادراکی تفاوتی داشته باشند. ظرفیت حمل به مفهوم حداکثر تعداد بیت‌هایی که می‌تواند در رسانه میزبان مخفی شود، اشاره دارد. امنیت نیز یعنی حملات نهان‌کاوی موجود قادر به کشف تصاویر

نهان‌نگاری شده تولید شده بوسیله این روش نباشند [۲].

نهان‌نگاری در دو حوزه مکان و حوزه تبدیل انجام می‌شود. الگوریتم‌های نهان‌نگاری در حوزه مکان، پیام را به طور مستقیم در شدت نور پیکسل‌های تصویر جاسازی می‌کنند. مزیت اصلی این روش‌ها بالا بودن ظرفیت جاسازی است اما در عین حال این روش‌ها روی کیفیت تصویر نهایی تاثیر می‌گذارند و خطر حملات آماری را افزایش می‌دهند. در الگوریتم‌های حوزه تبدیل، تصویر ابتدا به حوزه تبدیل منتقل شده و سپس پیام در ضرایب تبدیل جاسازی می‌شود. این روش‌ها نسبت به روش‌های مکانی، روش‌های پیچیده‌تری محسوب شده که احتمال کشف را کاهش می‌دهند اما ظرفیت جاسازی در آن‌ها کمتر است [۳].

معمولا به دلیل حجیم بودن فایل‌های تصویر، استفاده از فشرده سازی امری ضروری است. اما فشردگی تصویر پس از انجام جاسازی پیام، یکپارچگی پیام مخفی شده را از بین می‌برد و بازیابی آن غیر ممکن می‌شود. برای غلبه بر این مشکل از جاسازی پیام حین انجام عملیات فشرده‌سازی استفاده می‌شود. تبدیل DCT یکی از مهم‌ترین تبدیلات در فرایند فشرده‌سازی مانند JPEG است. تبدیل DCT تصویر را به نواحی با درجه اهمیت متفاوت با توجه به ویژگی‌های بصری، تقسیم می‌نماید: ضرایب فرکانس پایین، ضرایب فرکانس متوسط و ضرایب فرکانس بالا [۴]. در ماتریس ضرایب DCT فرکانس ضرایب از چپ به راست و از بالا به پایین افزایش می‌یابد. بخش فرکانس پایین تصویر نسبت به تغییرات بسیار حساس بوده و بخش اصلی تصویر را شامل می‌شود. بخش فرکانس بالای تصویر مقاومت کمی را داراست تا جایی که می‌توان تصویر را در این نواحی فشرده نمود. نواحی فرکانس متوسط مکان‌های مناسبی برای جاسازی هستند، زیرا تغییرات در این نواحی کمتر به چشم آمده و نیز کمتر در معرض فشرده‌سازی، برش و پردازش قرار دارند [۵].



شکل ۱: یک بلاک DCT [۶]

جاسازی در دامنه DCT به سادگی با تغییر ضرایب DCT، برای مثال تغییر کم ارزش‌ترین بیت هر ضریب، انجام می‌شود. یکی از محدودیت‌های جاسازی در دامنه DCT، این است که بسیاری از ۶۴ ضریب صفر هستند و تغییر بسیاری از صفرها به مقدار غیر صفر، روی نرخ فشرده سازی تأثیر دارد. به همین دلیل تعداد بیت‌هایی که می‌تواند در دامنه DCT جاسازی شود، کمتر از تعداد بیت‌هایی است که می‌تواند به روش LSB جاسازی شود. بعلاوه، ظرفیت جاسازی به نوع تصویر استفاده شده نیز بستگی دارد، چون بنابر بافت تصویر، تعداد ضرایب غیر صفر DCT متفاوت است [۷].

تا به حال روش‌های مختلفی برای جاسازی در ضرایب DCT پیشنهاد شده است. روش‌های Jsteg [۸]، OutGuess [۹]، F3، F4 و F5 [۱۰] از ساده ترین و قدیمی ترین روش‌ها در این حوزه هستند. اگرچه تغییر ضرایب DCT، اثرات بینایی غیر قابل تشخیصی ایجاد می‌کند، اما تغییرات آماری ناشی از آن، قابل کشف هستند. هدف روش‌های نهان‌کاوی استفاده از همین نقاط ضعف و ارائه یک حمله برای کشف روش‌های نهان‌نگاری است. برای نمونه در [۱۱] روشی برای کشف OutGuess و در [۱۲]، روشی برای کشف F5 ارائه شده است. تمام این روش‌ها فقط توانایی جاسازی حداکثر یک بیت در هر ضریب غیر صفر DCT را دارند. بهبود سه معیار کیفیت تصویر نهان-نگاری شده، ظرفیت جاسازی و امنیت روش‌های نهان‌نگاری در ضرایب DCT هدف اصلی محققان در ارائه روش‌های جدید در این حوزه می‌باشد. اما با توجه به تضاد موجود در بین این سه هدف، معمولا دستیابی به روشی که علاوه بر ظرفیت جاسازی بالاو حفظ کیفیت تصویر نهان‌نگاری شده، احتمال کشف کمتری توسط حملات داشته باشد تقریبا غیر ممکن است. زیرا در اثر جاسازی بیشتر، تأثیرات آماری ناشی از فرآیند جاسازی در تصویر افزایش می‌یابد و در نتیجه احتمال موفقیت روش‌های نهان‌کاوی برای کشف وجود داده بیشتر می‌شود. بنابراین باید به دنبال روشی بود که علاوه بر داشتن یک ظرفیت و کیفیت تصویر نهان‌نگاری شده مناسب، امنیت خوبی در برابر حملات موجود داشته باشد. هدف اصلی در این مقاله ارائه روشی با این ویژگی است.

با مطالعه روش‌های مختلف، می‌توان دو رویکرد موفق برای روش های نهان‌نگاری موجود عنوان کرد. رویکرد اول، شامل روش‌هایی است که تلاش می‌کنند کارایی جاسازی را افزایش دهند. به عبارت دیگر، هدف آنها کاهش تغییرات لازم برای جاسازی یک داده با طول مشخص در تصویر میزبان است. روش DCT-M3 [۱۳]، یک نمونه از این روش‌ها است. اما تغییرات در نواحی یکنواخت نسبت به تغییرات در نواحی لبه بسیار راحت‌تر کشف می‌شوند. بنابراین فقط افزایش کارایی جاسازی، برای تضمین امنیت نهان‌نگاری کافی نیست. در رویکرد دوم، روش‌هایی قرار می‌گیرند که به دنبال حداقل کردن انحراف اضافه شده به تصویر میزبان نسبت به تصویر نهان‌نگاری شده هستند. در این روش‌ها هزینه تغییر پیکسل‌ها در نواحی مختلف تصویر متفاوت درنظر گرفته می‌شود [۱۴-۱۶]. روش پیشنهادی در این مقاله، با ایده جاسازی بیت‌های کمتر در نواحی یکنواخت و جاسازی بیشتر در نواحی لبه، از رویکرد دوم پیروی می‌کند.

تفاوت روش پیشنهادی و روش‌های موجود، در نحوه تعیین ظرفیت جاسازی در ضرایب DCT و نحوه جاسازی داده است. در اکثر روش‌های موجود، ظرفیت جاسازی در تمام ضرایب DCT غیر صفر برابر درنظر گرفته شده است، اما یکی از ایده‌های اصلی روش پیشنهادی در این مقاله انتخاب ظرفیت جاسازی در ضرایب DCT غیر صفر به صورت متغیر و با توجه به ضرایب DCT همسایه است. به همین دلیل روش پیشنهادی یک روش تطبیقی است. ایده دیگر، جاسازی در مقدار اختلاف زوج ضریب DCT به جای جاسازی مستقیم در ضرایب DCT است. این ایده در حوزه مکان تحت عنوان روش PVD [۱۷] ارائه شده است. در روش پیشنهادی، با توجه به مقدار اختلاف زوج ضریب DCT، ظرفیت جاسازی در آنها تعیین می‌شود و سپس مقدار زوج ضریب DCT به نحوی تغییر می‌کند که گیرنده بتواند داده اصلی را از اختلاف زوج ضریب جدید استخراج کند. بدین ترتیب بستر جاسازی در روش پیشنهادی، اختلاف زوج ضریب DCT است. برای ظرفیت جاسازی در این روش دو دیدگاه مختلف بیان می‌شود، بعلاوه برای نحوه بازه‌بندی در روش پیشنهادی نیز دو گزینه وجود دارد. بنابراین روش پیشنهادی با الگوریتم کلی یکسان، در چهار حالت مختلف معرفی می‌شود و نتایج آنها با هم مقایسه می‌شود.

در ادامه، در بخش ۲، تعدادی از روش‌های مرتبط نهان‌نگاری در حوزه DCT بررسی می‌شوند. در بخش ۳، الگوریتم روش پیشنهادی در چهار حالت مختلف به صورت کامل شرح داده می‌شود. در بخش ۴، نتایج آزمون و مقایسه روش‌های پیشنهادی با الگوریتم‌های موجود براساس پارامترهای مختلف بحث می‌شود و در بخش ۵، نتیجه گیری نهایی ارائه می‌شود.

۲- مرور کارهای مرتبط

تا به حال روش‌های نهان‌نگاری بسیاری در هر دو حوزه مکان و تبدیل پیشنهاد شده است. این روش‌ها از لحاظ معیارهای کیفیت تصویر نهان‌نگاری شده، ظرفیت جاسازی و امنیت متفاوت هستند. با توجه به حوزه اصلی این مقاله، یعنی جاسازی در ضرایب تبدیل DCT، در ادامه تعدادی از روش‌های نهان‌نگاری در این ضرایب معرفی می‌شود و نقاط ضعف و قوت آنها بررسی می‌شود.

LSB Flipping و LSB Matching دو روش رایج در حوزه مکان است و براساس ایده این دو روش، روش‌هایی در حوزه تبدیل نیز پیشنهاد شده است. در روش LSB Flipping، بیت کم‌ارزش پیکسل‌های تصویر میزبان با بیت‌های پیام جاگذاری می‌شوند. روش Jsteg، از همین ایده برای جاسازی در ضرایب DCT استفاده می‌کند. الگوریتم جاسازی به این صورت است که کم ارزش‌ترین بیت ضرایب DCT را با داده پیام جاگذاری می‌کند. برای جلوگیری از کاهش نرخ فشرده‌سازی، در این روش در ضرایب صفر جاسازی انجام نمی‌شود. با توجه به اینکه هنگام انجام فرآیند استخراج، نمی‌توان بین ضریب صفری که از جاسازی در آن پرهیز شده است و ضریب صفر تولید شده در اثر جاسازی بیت صفر در ضریبی با مقدار یک تمایزی قائل شد، اجازه جاسازی در بیت‌های با مقدار یک نیز وجود ندارد [۸].

روش LSB Matching که به نام Plus Minus 1 (PM1) نیز شناخته می‌شود، احتمال کشف کمتری نسبت به LSB Flipping دارد. در این روش نیز پیام محرمانه در کم‌ارزش‌ترین بیت تصویر جاسازی می‌شود. با این تفاوت که در طول فرایند جاسازی ابتدا بیت پیام با کم‌ارزش‌ترین بیت پیکسل مقایسه می‌شود، اگر بیت پیام با بیت پیکسل برابر بود، پیکسل بدون تغییر باقی می‌ماند. اما در صورت عدم تطابق به مقدار پیکسل به صورت تصادفی یک واحد اضافه یا کم (۱+ یا ۱-) می‌شود.

Yu و همکارانش در سال ۲۰۰۹، ایده PM1 را برای جاسازی در ضرایب DCT پیشنهاد کردند [۱۸]. در این روش برای کمتر شدن احتمال کشف، از الگوریتم ژنتیک برای انتخاب هدفدار افزایش یا کاهش مقدار ضریب استفاده کرده‌اند به نحوی که مقدار تابع برازندگی انتخاب شده (متناسب با مفهوم Blockiness) کمترین مقدار شود. نتایج نشان داده که این روش از جهت حفظ معیار Blockiness و هیستوگرام ضرایب DCT موفق بوده است. اما ظرفیت جاسازی آن مشابه Jsteg و کمتر از ۱bpnz (یک بیت در هر ضریب AC غیر صفر) است.

در پژوهش دیگری ایده جاسازی تطبیقی در خود ضرایب DCT به کار گرفته شده است که الگوریتم Shield نامیده شده است [۱۹]. در این روش پس از اعمال DCT و کوانتیزه کردن مقادیر، از ضرایب صفر و یک صرف نظر شده و از میان ضرایب غیر صفر برای جاسازی انتخاب می‌شوند. با توجه به مقدار ضرایب، تعداد بیت برای جاسازی درون هر ضریب تعیین می‌شود. انتخاب تعداد بیت برای هر ضریب بر اساس جدول ۱ صورت می‌پذیرد.

جدول ۱: تعداد بیت قابل جاسازی در [۱۹]

تعداد بیت‌ها	مقادیر DCT کوانتیزه شده
۱	۲-۸
۲	۹-۱۶
۳	۱۷-۳۱
۴	۳۲-۶۴
۵	> ۶۵

همان طور که مشاهده می‌شود، در ضرایبی که مقدار بیشتری دارند تعداد بیت قابل جاسازی بیشتر بوده و در ضرایب کوچکتر تعداد بیت کمتری پنهان می‌شود. نتایج حاصل از این روش نشان

می‌دهد این روش ظرفیت جاسازی را افزایش داده است.

در [۲۰]، روشی با ظرفیت بسیار بالا برای تصاویر رنگی پیشنهاد شده که از جاسازی ناحیه‌ای تطبیقی سراسری بهره می‌برد. ایده اصلی، تطبیق نواحی استفاده شده برای جاسازی داده در هر بلاک DCT با میزان همبستگی مقادیر تصویر در آن بلاک است. افزایش ظرفیت جاسازی مزیت اصلی این روش در مقایسه با روش‌های حوزه مکان و تعدای از روش‌های حوزه DCT است. اما در این روش، کیفیت تصویر نهان نگاری شده حدود ۳۰db است و در مورد میزان امنیت این روش در برابر حملات نهان کاوی هیچ آزمونی انجام نشده است.

در [۱۳]، یک الگوریتم جدید برای جاسازی در ضرایب DCT تصاویر JPEG پیشنهاد شده است که DCT-M3 نامیده شده است. هدف این روش حداقل کردن تغییرات تصویر میزبان است. در این روش، دو ضریب DCT از هر بلاک ۸×۸ انتخاب می‌شود. مکان این دو ضریب با توجه به کلید توافق شده بین فرستنده و گیرنده و به صورت یکسان در تمام بلاک‌ها است. سپس با توجه به سه معیار شامل حاصل باقیمانده تقسیم اختلاف این دو ضریب DCT بر ۳، زوج یا فرد بودن ضریب DCT اول و مقدار داده دو بیتی مورد نظر برای جاسازی، نحوه تغییر حداکثر یک واحدی در دو ضریب به گونه ای مشخص شده است که گیرنده با توجه به پیمانه ۳ اختلاف دو ضریب DCT و زوج یا فرد بودن ضریب اول، به راحتی قادر به استخراج دو بیت داده جاسازی شده است. مهم ترین دستاورد این روش حداقل کردن تغییرات حاصل از جاسازی داده در تصویر است. اما این روش به شدت ظرفیت جاسازی را کاهش داده است و در ظرفیت جاسازی بسیار پایین، امنیت بالاتری نسبت به روش ساده LSB دارد.

در [۲۱]، روشی پیشنهاد شده است که MPS نامیده شده است. در این روش، در هر بلاک ۴ تا مجموعه سه‌تایی از ضرایب DCT درنظر گرفته می‌شود. در هر مجموعه سه‌تایی، به صورت تصادفی یکی از ضرایب به عنوان شاخص انتخاب می‌شود. این انتخاب به نحوی انجام می‌شود که گیرنده نیز بتواند ضریب شاخص در هر مجموعه را تشخیص دهد. در ضریب شاخص، داده ای ذخیره نمی‌شود. از دو ضریب دیگر، جاسازی در کوچکترین ضریب انجام می‌شود. در این روش، تعداد بیت قابل جاسازی در ضریب منتخب به عنوان یک کلید بین فرستنده و گیرنده توافق شده است. اجازه جاسازی از ۱ تا ۸ بیت در ضریب منتخب وجود دارد. بدین ترتیب، در صورت جاسازی n بیت ($1 \le n \le 8$) در هر ضریب، در هر بلاک $4 \times n$ بیت داده جاسازی می‌شود.

در [۲۲]، روش جاسازی در LSB ضرایب DCT فرکانس متوسط پیشنهاد شده است. ضرایب DCT فرکانس پایین و بالا بدون تغییر می‌مانند. عدم تغییر ضرایب فرکانس پایین، کیفیت نواحی یکنواخت تصویر میزبان را حفظ می‌کند و عدم تغییر ضرایب فرکانس بالا، کیفیت لبه های تصویر میزبان را حفظ می‌کند. در این روش ادعا شده است که با تغییر ضرایب فرکانس میانی، تصویر نهان‌نگاری شده با کیفیت بالاتر تولید می‌شود و بعلاوه تصویر نهان‌نگاری شده در برابر حملات نهان‌کاوی مقاوم‌تر است. در ادامه از این روش به عنوان MedFreq نام برده می‌شود.

روش‌های بسیار دیگری نیز وجود دارند که از جاسازی در ضرایب DCT استفاده کرده اند. تعدادی از آنها از ترکیب نهان‌نگاری و رمز نگاری برای ایجاد امنیت بیشتر در انتقال پیام استفاده کرده‌اند [۲۳و۲۴]. بعضی از روش‌های دیگر نیز در حوزه نهان‌نگاری برگشت پذیر از جاسازی در ضرایب DCT استفاده کرده‌اند که با مبحث اصلی این مقاله متفاوت است و به همین دلیل با جزئیات به بررسی آنها پرداخته نشده است [۲۵ و ۲۶].

۳- روش پیشنهادی

انتخاب مکان جاسازی و نحوه جاسازی کلیدی‌ترین مولفه‌ها در یک روش نهان‌نگاری است که ضامن موفقیت روش خواهد بود. حوزه‌ی DCT امکان تفکیک تصویر به گروه‌های فرکانسی مجزا شامل فرکانس بالا، پایین و متوسط را فراهم می‌کند و بدین ترتیب می‌توان مناسب ترین مکان‌ها برای جاسازی را انتخاب کرد. نواحی فرکانس پایین معادل نواحی یکنواخت تصویر است که تغییرات در این نواحی به راحتی قابل تشخص است و مکان مناسبی برای جاسازی به شمار نمی‌رود. نواحی فرکانس متوسط و بالا معادل نواحی لبه در تصویر است که تغییرات به وجود آمده در این نواحی سخت‌تر قابل تشخیص است. مشابه این مفهوم را در حوزه مکان نیز می‌توان دید. اختلاف مقدار دو پیکسل واقع در ناحیه لبه زیاد است در حالی که اختلاف مقدار برای دو پیکسل در ناحیه یکنواخت تصویر کم است. بر همین مبنا روشی برای نهان‌نگاری در حوزه مکان تحت عنوان PVD ارائه شده است [۱۷].

در روش پیشنهادی داده مخفی درون اختلاف مقدار ضرایب DCT همسایه پنهان می‌شود. مقدار داده قابل پنهان‌سازی به صورت پویا و براساس میزان اختلاف دو ضریب تعیین می‌شود. در روش پیشنهادی برای جاسازی مقدار داده یکسان به طور کلی دو دیدگاه متفاوت از منظر ظرفیت جاسازی می‌توان متصور شد. دیدگاه اول در مورد نحوه جاسازی این است که میزان تغییرات در اختلاف زوج ضریب بیشتر باشد (تعداد بیت بیشتری در هر زوج ضریب جاسازی شود)، اما تعداد زوج‌های کمتری تغییر کند. دیدگاه دوم این است که میزان تغییرات در اختلاف زوج ضریب کمتر باشد (تعداد بیت کمتری در هر زوج ضریب جاسازی شود)، اما تعداد

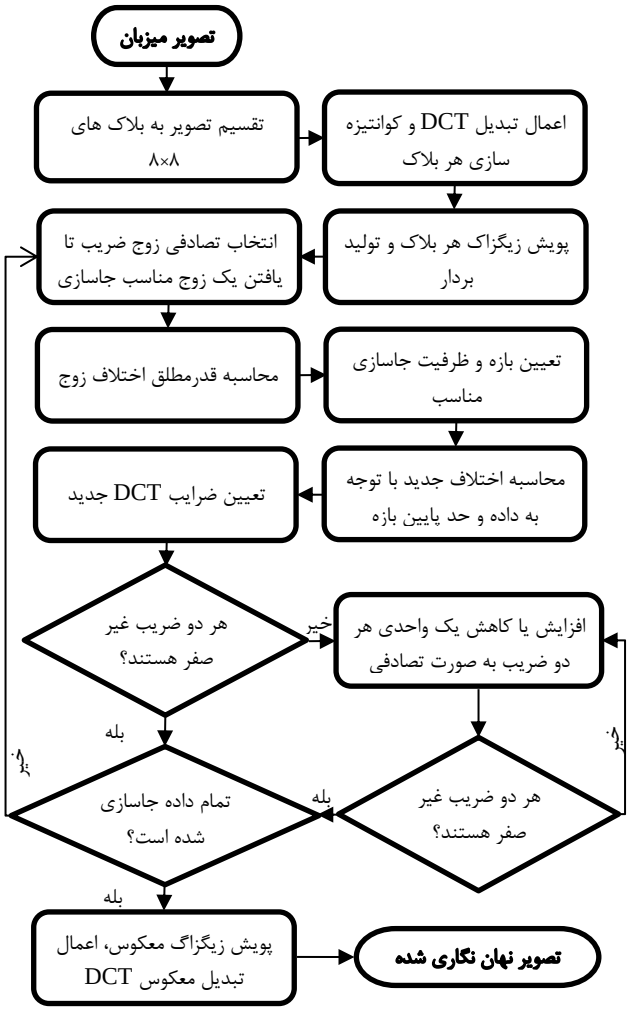
زوج‌های بیشتری تغییر کنند. به طور کلی این مصالحه در عموم روش‌های نهان‌نگاری مطرح است و باید بررسی شود کدام دیدگاه نتیجه بهتری در پی دارد. از طرف دیگر در روش پیشنهادی، مبنای تعیین ظرفیت هر زوج ضریب، بازه بندی مقدار اختلاف‌ها است. این بازه‌بندی می‌تواند برای کل تصویر ثابت باشد و یا هر بار برای کم کردن اثرات جاسازی، از بازه‌بندی متغیر استفاده کرد. با توجه به این دو مبحث، در ادامه چهار روش جدید پیشنهاد می‌شود که الگوریتم کلی آنها یکسان است و تفاوت آنها در نحوه بازه‌بندی و تعیین ظرفیت زوج ضریب است. این چهار روش عبارتند از:

۱- ADCT_FR_LC: نهان‌نگاری تطبیقی در ضرایب DCT با بازه‌بندی ثابت و ظرفیت کم
۲- ADCT_FR_HC: نهان‌نگاری تطبیقی در ضرایب DCT با بازه‌بندی ثابت و ظرفیت بالا
۳- ADCT_VR_LC: نهان‌نگاری تطبیقی در ضرایب DCT با بازه‌بندی متغیر و ظرفیت کم
۴- ADCT_VR_HC: نهان‌نگاری تطبیقی در ضرایب DCT با بازه‌بندی متغیر و ظرفیت بالا

الگوریتم کلی روش پیشنهادی در شکل ۲ نمایش داده شده است. در ادامه الگوریتم جاسازی و استخراج در این روش‌ها به صورت کامل بررسی می‌شود.

۳-۱ الگوریتم جاسازی

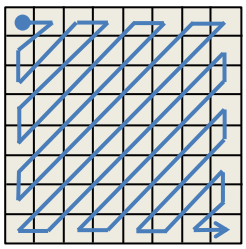
در گام اول باید تصویر میزبان که یک تصویر سطح خاکستری است، را به بلاک‌های ۸×۸ تقسیم بندی کرد و تبدیل DCT را روی هر بلاک اعمال کرد. نتیجه اعمال تبدیل DCT روی هر بلاک، یک بلاک ۸×۸ از ضرایب DCT است. این ضرایب در هر بلاک با C_i ($\{i = 1, \dots, 64\}$) نشان داده می‌شوند. در یک بلاک ۸×۸ حاصل از تبدیل DCT، اولین مولفه هر بلاک (C_1)، عنصر DC و مولفه فرکانس پایین بلاک محسوب می‌شود و نباید هیچ گونه تغییری در آن ایجاد کرد، زیرا این مولفه کلیت بلاک را در خود جای داده است. سپس ضرایب DCT هر بلاک ۸×۸ به صورت زیگزاگ پویش شده و درون یک بردار ریخته می‌شوند. در شکل ۳، نحوه انجام پیمایش زیگزاگ یک بلاک به همراه شبه کد تولید آن نمایش داده شده است. ورودی این شبه کد، یک بلاک به نام DCT_BLOCK و خروجی بردار Zigzag است.



شکل ۲: روندنمای الگوریتم جاسازی روش پیشنهادی

در گام بعدی هر دو ضریب کنار هم در بردار زیگزاگ تشکیل یک زوج ضریب را می‌دهند به نحوی که این زوج ضریب‌ها با یکدیگر همپوشانی ندارند، به عبارت دیگر هر ضریب فقط در یک زوج شرکت می‌کند. با توجه به اینکه ضریب اول هر بلاک قابل جاسازی نیست و با حذف آن ۶۳ ضریب باقی می‌ماند، بنابراین ۳۱ زوج تشکیل می‌شود. ضریب ۶۴ ام در هیچ زوجی شرکت نمی‌کند و با توجه به صفر بودن این ضریب هیچ ظرفیتی از دست نمی‌رود. بنابراین بهتر است این ضریب در تشکیل بردار زیگزاگ نادیده گرفته شود، به همین دلیل در فرآیند ساخت بردار زیگزاگ در کد شکل ۳، ضریب ابتدایی و انتهایی بلاک DCT نادیده گرفته شده است. زوج i ام، $Pair(i)$، شامل ضرایب $2i$ و $2i+1$ است که در فرمول ۱ نحوه تشکیل آن نشان داده شده است.

$$Pair\ (i) = (C_{2i}, C_{2i+1}) \quad i \in \{1,2, \dots ,31\} \qquad (۱)$$



```
Input: DCT_Block
Output: Zigzag
t = 0;
for d = 3 : 15
   for i = 1 : 8
      for j = 1 : 8
         if ( (i+j) == d) )
            t = t + 1;
            if ( mod (d,2) == 0)
               Zigzag (t) = DCT_Block (j,d-j);
            else
               Zigzag (t) = DCT_Block (d-j,j);
            endif;
         endif;
      endfor;
   endfor;
endfor;
```

شکل ۳: پویش زیگزاگ و کد تولید آن برای یک بلاک ۸×۸

برای انتخاب زوج‌های مورد نظر برای جاسازی، از یک تابع شبه تصادفی استفاده می‌شود تا بتوان داده را به طور یکنواخت در سطح تصویر پخش نمود. این تابع شبه تصادفی نیاز به یک هسته ابتدایی دارد که اگر مقدار آن به عنوان کلید در اختیار گیرنده قرار گیرد، گیرنده می‌تواند زوج ضریب استفاده شده برای جاسازی را به راحتی پیدا کند. پس از انتخاب زوج ضریب، اگر یک یا هر دو ضریب انتخاب شده مقدار صفر باشد از آن زوج صرف نظر شده و زوج دیگری انتخاب می‌شود. عدم جاسازی در ضرایب صفر، قاعده کلی روش‌های نهان نگاری در ضرایب DCT است. در یک بلاک DCT عناصر زیر قطر اصلی عموما صفر هستند که از جاسازی درون آن‌ها پرهیز می‌شود. فرض کنید زوج i ام، $Pair(i)$، برای انجام جاسازی انتخاب شده است. در گام بعد باید با استفاده از فرمول ۲، قدر مطلق اختلاف مقدار زوج محاسبه شود تا از آن به عنوان معیاری برای محاسبه تعداد بیت قابل جاسازی در آن استفاده کرد.

$$Delta\big(Pair(i)\big) = |\, C_{2i+1} - C_{2i}| \qquad (۲)$$

در این مرحله براساس مقدار اختلاف زوج ضریب انتخاب شده، مقدار داده‌ای که باید در آن جاسازی شود، تعیین می شود. بدین منظور محدوده قدر مطلق اختلاف ممکن در چند بازه دسته‌بندی می‌شود و به هر بازه یک اندیس k نسبت داده می‌شود. حد بالا، پایین و ظرفیت هر بازه به ترتیب U_k، L_k و N_k نامیده می‌شود. دو دیدگاه برای تعیین بازه‌ها وجود دارد: ثابت و متغیر. در دیدگاه اول یک بازه بندی ثابت برای کل تصویر میزبان انتخاب و استفاده می‌شود. اما در دیدگاه دوم، حد بالا و پایین بازه‌ها در هر بلاک متغیر است. در مورد تعداد بیت جاسازی نیز طبق توضیحات قبل، دو دیدگاه وجود دارد. بر همین اساس در جدول ۲، بازه‌بندی و ظرفیت بازه‌ها در دو روش با بازه‌بندی ثابت ارائه شده است.

جدول ۲: پارامترهای دو روش پیشنهادی با بازه بندی ثابت

روش پیشنهادی	حد پایین	حد بالا	ظرفیت جاسازی
ADCT_FR_LC	$L_1 = 0$	$U_1 = 7$	$N_1 = 1$
	$L_2 = 8$	$U_2 = 15$	$N_2 = 1$
	$L_3 = 16$	$U_3 = 31$	$N_3 = 2$
	$L_4 = 32$	$U_4 = 63$	$N_4 = 3$
ADCT_FR_HC	$L_1 = 0$	$U_1 = 7$	$N_1 = 3$
	$L_2 = 8$	$U_2 = 15$	$N_2 = 3$
	$L_3 = 16$	$U_3 = 31$	$N_3 = 4$
	$L_4 = 32$	$U_4 = 63$	$N_4 = 5$

اما برای افزایش امنیت می‌توان از بازه‌های متغیر استفاده کرد. به عبارت دیگر، بازه‌های متناظر بلاک‌های مختلف، می‌توانند متفاوت باشند و با استفاده از یک کلید رمز $\beta \in [0.1]$ محاسبه شوند. این پارامتر به صورت شبه تصادفی برای هر بلاک انتخاب می‌شود و سپس حدود پایین و بالای بازه k ام طبق روابط ۳ و ۴ محاسبه می‌شوند. W_k، نشان دهنده طول بازه k ام است که توسط فرمول ۵ قابل محاسبه است.

$$L'_k = L_k + \lfloor \beta . W_k \rfloor \qquad (۳)$$

$$U'_k = U_k + \lfloor \beta . W_{k+1} \rfloor \qquad (۴)$$

$$W_k = U_k - L_k + 1 \qquad (۵)$$

در روش ADCT_VR_LC، بعد از محاسبه حدود هر بازه از ظرفیت‌های جاسازی مشابه روش ADCT_FR_LC و روش ADCT_VR_HC، نیز از ظرفیت‌های جاسازی مشابه روش ADCT_FR_HC که در جدول ۲ ذکر شد، استفاده می‌کنند.

در گام بعد، با توجه به روش مورد نظر برای جاسازی و بر اساس این که $Delta\big(Pair(i)\big)$ در چه بازه‌ای قرار گرفته است، تعداد بیت مناسب از پیام برای جاسازی انتخاب شده و تبدیل به معادل دهدهی می‌شود. فرض کنید این اختلاف در بازه k ام قرار گرفته باشد و M_i، معادل دهدهی N_k بیت از پیام است که برای جاسازی انتخاب شده است. حال باید مقدار اختلاف جدید هر زوج ضریب متناسب با مقدار داده‌ای که باید در آن جاسازی شود، تعیین شود. در روش‌های ADCT_FR_HC و ADCT_VR_HC برای محاسبه مقدار اختلاف جدید از فرمول ۶ استفاده می‌شود.

$$\text{New Delta}\,\big(\text{Pair(i)}\big) = \begin{cases} L_k + M_i & if\ \ Delta\big(Pair(i)\big) \geq 0 \\ -(L_k + M_i) & if\ \ Delta\big(Pair(i)\big) < 0 \end{cases} \qquad (۶)$$

اما در روش‌های ADCT_FR_LC و ADCT_VR_LC نحوه محاسبه مقدار اختلاف جدید متفاوت است. ابتدا پارامتر F که برابر اختلاف مقدار دهدهی شده N_k بیت از پیام و مقدار دهدهی N_k بیت کم ارزش اختلاف مقدار اصلی است، توسط فرمول ۷، محاسبه می‌شود.

$$F\big(Pair(i)\big) = M_i - \left(\frac{Delta\big(Pair(i)\big)}{2^{N_k}}\right) \qquad (۷)$$

اگر F عددی مثبت باشد، آن‌گاه دو گزینه برای مقدار اختلاف جدید وجود دارد که طبق رابطه ۸ قابل محاسبه است.

$$New\ Delta\ (Pair(i)) = \begin{cases} Delta\ (Pair(i)) + F(Pair(i)) \\ Delta\ (Pair(i)) - (2^{N_k} - F(Pair(i))) \end{cases} \quad (۸)$$

اگر F عددی منفی باشد، آن‌گاه دو گزینه برای مقدار اختلاف جدید طبق رابطه ۹ قابل محاسبه است.

$$New\ Delta\ (Pair(i)) = \begin{cases} Delta\ (Pair(i)) + F(Pair(i)) \\ (Delta\ (Pair(i)) + 2^{N_k}) + F(Pair(i))) \end{cases} \quad (۹)$$

حال باید تصمیم گرفت که از بین دو گزینه محاسبه شده، کدام یک از اختلافات مناسب‌تر است. برای انتخاب اختلاف مقدار جدید، اگر فقط یکی از اختلاف‌های بدست آمده درون بازه اختلاف قبلی قرار داشته باشد، آن اختلاف به عنوان اختلاف مقدار نهایی منظور می‌شود. اما اگر هر دو اختلاف به دست آمده درون بازه قرار داشته باشند، هر کدام که به اختلاف مقدار اصلی نزدیک‌تر باشد، انتخاب می‌شود.

بعد از محاسبه مقدار اختلاف جدید که در چهار روش پیشنهادی کمی متفاوت بود، در تمام روش‌ها در گام بعد باید مقدار زوج ضریب به نحوی تغییر کند که اختلاف مقدار آن‌ها با اختلاف مقدار جدید محاسبه شده در مرحله قبل یکسان شود. برای رسیدن به این هدف ابتدا از فرمول‌های ۱۰، ۱۱ و ۱۲ استفاده می‌شود.

$$D(Pair(i)) = New\ Delta\ (Pair(i)) - Delta\ (Pair(i)) \quad (۱۰)$$

$$if\ |D(Pair(i))|\%2 \neq 0 \rightarrow \begin{cases} New\ C(i) = C(i) - ceil\left(\frac{D(Pair(i))}{2}\right) \\ New\ C(i+1) = C(i+1) - floor\left(\frac{D(Pair(i))}{2}\right) \end{cases} \quad (۱۱)$$

$$if\ |D(Pair(i))|\%2 = 0 \rightarrow \begin{cases} New\ C(i) = C(i) - floor\left(\frac{D(Pair(i))}{2}\right) \\ New\ C(i+1) = C(i+1) + ceil\left(\frac{D(Pair(i))}{2}\right) \end{cases} \quad (۱۲)$$

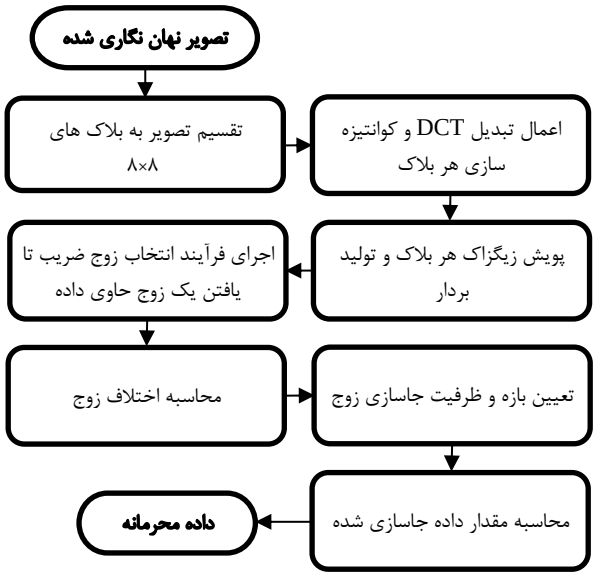
بعد از محاسبه مقادیر جدید زوج ضریب، این مقادیر جدید جایگزین مقادیر قبلی در بردار زیگزاگ می‌شوند. اگر در طی فرایند جاسازی ضریب صفری تولید شد، به طور تصادفی به هر دو ضریب عدد یک اضافه شده و یا از آن‌ها کسر می‌شود. این کار تا زمانی ادامه خواهد داشت که هر دو ضریب غیر صفر شوند. بعد از اطمینان از جاسازی همه بیت‌های پیام فرایند جاسازی به اتمام رسیده و در ادامه باید تصویر نهان‌نگاری ساخته شود. ابتدا معکوس روال پویش زیگزاگ انجام شده تا تصویر به حالت بلاک‌های ۸×۸ برگشت داده شود. سپس تبدیل معکوس DCT روی هر بلاک DCT اجرا می‌شود تا تصویر نهان‌نگاری شده تولید شود.

۳-۲ الگوریتم استخراج

هر الگوریتم جاسازی، نیاز به یک الگوریتم استخراج مناسب دارد که گیرنده بتواند از طریق آن داده جاسازی شده را به طور کامل استخراج کند. الگوریتم استخراج روش پیشنهادی در شکل ۴ نشان داده شده است. گیرنده مراحل ساخت بلاک‌های ۸×۸، اعمال تبدیل DCT روی بلاک‌ها و پویش زیگزاگ آنها را مشابه فرآیند جاسازی روی تصویر دریافتی انجام می‌دهد. حال با استفاده از کلیدی که در مرحله جاسازی جهت انتخاب تصادفی زوج ضریب استفاده شده بود، به همان زوج ضریب دسترسی یافته و اختلاف مقدار هر زوج را محاسبه می‌کند. فرض کنید هر ضریب DCT در تصویر نهان نگاری شده، SC_i و زوج ضریب، $SPair(i)$ نامیده شود. اختلاف مقدار دو ضریب با رابطه ۱۳ محاسبه می‌شود.

$$SDelta(SPair(i)) = SC_{2i+1} - SC_{2i} \quad (۱۳)$$

گیرنده پس از محاسبه اختلاف مقدار زوج ضریب در تصویر نهان نگاری شده، باید تعیین کند این اختلاف به کدام بازه تعلق دارد. گیرنده با اطلاع از روش جاسازی، اطلاعات حدود بالا، پایین و ظرفیت جاسازی بازه‌ها را دارد. فرض کنید اختلاف محاسبه شده به بازه k ام تعلق داشته باشد. اگر روش جاسازی ADCT_FR_HC یا ADCT_VR_HC باشد، با استفاده از حد پایین بازه مقدار دهدهی پیام قابل استخراج است.



شکل ۴: روندنمای الگوریتم استخراج روش پیشنهادی

فرمول استخراج در ۱۴ ذکر شده است.

$$M_i = \begin{cases} SDelta(SPair(i)) - L_k & SDelta(SPair(i)) \geq 0 \\ -(Delta(SPair(i))) - L_k & SDelta(SPair(i)) < 0 \end{cases} \quad (۱۴)$$

در روش‌های ADCT_FR_LC و ADCT_VR_LC برای استخراج معادل دهدهی پیام از تعداد بیت‌های قابل جاسازی در هر بازه استفاده می‌شود. در این دو روش باید برای این کار از فرمول ۱۵ استفاده کرد.

$$M_i = SDelta\big(SPair(i)\big)\%2^{N_k} \quad (۱۵)$$

پس از این مرحله گیرنده باید با تبدیل دهدهی به دودویی به معادل N_k بیتی پیام جاسازی شده دست یابد.

۴- نتایج پیاده سازی

روش‌های پیشنهادی در متلب ۲۰۱۶ پیاده سازی شده است. برای مقایسه روش‌های نهان نگاری معیارهایی وجود دارد که می‌توان در سه دسته اصلی کیفیت تصویر نهان‌نگاری شده، ظرفیت جاسازی و میزان مقاومت در برابر حملات تقسیم بندی کرد. هدف از آزمون ها شناخت بهترین روش از میان چهار روش پیشنهادی و بعلاوه مقایسه کارایی این روش‌ها در برابر روش‌های قبلی است. در مقایسه‌ها از روش‌های Jsteg (به عنوان روش مبنایی در حوزه DCT) و Shield [۱۹] (به عنوان یک روش جاسازی چند بیتی تطبیقی در خود ضرایب DCT) و سه روش جدیدتر شامل DCT-M3 [۱۳]، MPS [۲۱] و MedFreq [۲۲] استفاده شده است. نتایج آزمون ارائه شده برای تمام روش‌های مورد مقایسه، میانگین حاصل از ۲۰۰ تصویر آزمون از سایت http://lear.inrialpes.fr است که شامل تصاویر فرمت JPEG است. این تصاویر رنگی با ابعاد مختلف هستند و قبل از اجرای الگوریتم جاسازی، تبدیل به تصاویر سطح خاکستری شده‌اند. برای دسترسی به ضرایب DCT تصاویر از Jpeg toolbox استفاده شده است. مقایسه‌ها در سه سطح جاسازی مختلف انجام شده است. واحد جاسازی در ضرایب DCT با bpnz بیان می‌شود که به معنای تعداد بیت جاسازی شده به ازای هر ضریب DCT غیر صفر است. برای مثال، ۰/۱bpnz به معنای جاسازی ۰/۱ بیت در هر ضریب غیر صفر است. به عبارت دیگر اگر تبدیل DCT تصویر، ۱۰۰۰ ضریب غیر صفر داشته باشد، در سطح جاسازی ۰/۱bpnz، پیامی به طول ۱۰۰ بیت در آن جاسازی می‌شود. با مقایسه روش‌های نهان‌نگاری مختلف در یک سطح جاسازی یکسان، طول پیام جاسازی شده در تصویر توسط روش‌های نهان‌نگاری موردنظر یکسان است و بنابراین این ارزیابی نقاط ضعف و قوت روش‌ها را به صورت واقعی‌تر منعکس می‌کند.

قبل از ارائه نتایج، در مورد پیام محرمانه استفاده شده در آزمون های مختلف باید این نکته ذکر شود که پیام محرمانه علیرغم شکل ظاهری خود باید به صورت یک رشته بیتی بیان شود. در روش های نهان نگاری برای افزایش امنیت ارتباط باید فرستنده دو عملیات فشرده سازی و رمز کردن را روی داده بیتی اعمال کند. فشرده‌سازی، باعث حذف افزونگی‌های موجود در آن و در نتیجه جلوگیری از اتلاف ظرفیت تصویر می‌شود. از طرف دیگر، رمز کردن، باعث از بین رفتن وابستگی‌های میان بیت‌ها و تبدیل پیام به یک دنباله تقریبا تصادفی می‌شود. به همین دلیل در آزمون ها، از یک دنباله بیتی صفر و یک تصادفی تولید شده از طریق تابع rand در متلب به عنوان پیام استفاده شده است.

۴-۱ کیفیت تصویر نهان‌نگاری شده

برای مقایسه کیفیت تصویر نهان‌نگاری شده معیارهای مختلفی وجود دارد. یکی از این معیارها، معیار MSE است که نشان دهنده میانگین خطای مربعات است. منظور از خطا، تفاوت تصویر میزبان و نهان‌نگاری شده است. مقدار این شاخص همواره مثبت است و هرچه مقدار آن به صفر نزدیکتر باشد، نشان دهنده میزان خطای کمتری است. معیار دوم، معیار PSNR است که مقادیر بزرگتر PSNR، نشان دهنده کیفیت بهتر تصویر نهان‌نگاری شده است. SSIM، میزان شباهت ساختاری تصویر نهان‌نگاری شده با میزبان را نشان می‌دهد. منظور از اطلاعات ساختاری، وابستگی متقابل پیکسل‌ها خصوصا در مورد پیسکل‌هایی است که بسیار به هم نزدیک هستند. SSIM در رنج ۱- تا ۱+ تعریف می‌شود و برای تصاویر ایده‌آل این مقدار به عدد ۱ نزدیک‌تر است.

میانگین سه معیار MSE، PSNR و SSIM برای چهار روش پیشنهادی و دو روش Jsteg و Shield [۱۹] در جدول ۳ ارائه شده است. در این جدول، در هر سطح جاسازی بهترین نتیجه با قرمز، دومین نتیجه با سبز و سومین نتیجه با آبی مشخص شده است. با توجه به اینکه در روش Jsteg هر ضریب DCT حداکثر یک واحد تغییر می‌کند، بنابراین انتظار می‌رود که این روش بتواند بهترین سطح را در پارامترهای کیفیت تصویر کسب کند. نتایج ارائه شده در جدول ۳ این ادعا را تایید می‌کند. در تمام سطوح جاسازی و برای تمام پارامترهای کیفیت تصویر نهان‌نگاری‌شده، Jsteg بهترین نتیجه را دارد. اما در روش‌های پیشنهادی نیز با توجه به اینکه در روش ظرفیت کم با جاسازی تعداد بیت کم، تغییرات کمتری به ضرایب DCT تحمیل می‌شود، بنابراین روش‌های ADCT_VR_LD و ADCT_FR_LC توانستند نتایج بهتری

جدول ۳: میانگین معیارهای MSE، PSNR و SSIM در ۲۰۰ تصویر برای چهار روش پیشنهادی، Jsteg و Shield

Parameter	bpnz	Jsteg	Shield [۱۹]	ADCT_FR_LC	ADCT_FR_HC	ADCT_VR_LC	ADCT_VR_HC
MSE	۰/۱	۱/۵۶۵۲	۴/۷۸۶۲	۲/۷۷۵۲	۵/۸۸۴۳	۲/۷۳۷۶	۱۶/۱۱۱۴
	۰/۰۵	۰/۷۸۷۸	۲/۴۰۴۶	۱/۳۹۸۵	۲/۹۱۷۳	۱/۳۷۷۲	۸/۱۰۷۵
	۰/۰۱	۰/۱۶۱۰	۰/۴۸۲۲	۰/۲۷۹۷	۰/۵۸۱۰	۰/۲۷۸۹	۱/۵۸۲۶
PSNR	۰/۱	۴۷/۱۳۳۸	۴۱/۹۲۵۶	۴۴/۶۴۱۹	۴۱/۳۵۶۸	۴۴/۷۳۲۴	۴۰/۰۰۴۷
	۰/۰۵	۵۰/۱۰۸۳	۴۴/۹۱۵۲	۴۷/۶۱۳۸	۴۴/۴۱۰۸	۴۷/۷۰۳۰	۴۰/۰۳۱۸
	۰/۰۱	۵۷/۰۱۱۸	۵۱/۹۰۱۲	۵۴/۶۲۶۶	۵۱/۴۱۶۸	۵۴/۶۸۰۳	۴۷/۱۵۹۱
SSIM	۰/۱	۰/۹۸۹۶	۰/۹۸۲۳	۰/۹۸۴۷	۰/۹۷۶۴	۰/۹۸۴۶	۰/۹۵۰۷
	۰/۰۵	۰/۹۹۴۷	۰/۹۹۰۸	۰/۹۹۳۲	۰/۹۸۸۰	۰/۹۹۲۲	۰/۹۷۴۴
	۰/۰۱	۰/۹۹۸۹	۰/۹۹۸۱	۰/۹۹۸۴	۰/۹۹۷۶	۰/۹۹۸۴	۰/۹۹۴۸

نسبت به بقیه روش‌ها کسب کنند. با توجه به اینکه بحث تعیین ظرفیت بازه‌ها در این دو روش تقریبا یکسان است، بنابراین نتایج این دو روش تقریبا مساوی است که نشان می‌دهد اگر در فرآیند جاسازی، کیفیت تصویر نهان‌نگاری شده برای فرستنده بسیار مهم است باید از دیدگاه دوم در مورد نحوه جاسازی استفاده کند. به عبارت دیگر، بهتر است میزان تغییرات در اختلاف زوج ضریب کمتر باشد (تعداد بیت کمتری در هر زوج ضریب جاسازی شود)، اما تعداد زوج‌های بیشتری تغییر کنند.

در آزمون دیگر دو روش برتر پیشنهادی با روش های DCT-M3 [۱۳]، MPS [۲۱] و MedFreq [۲۲] از نظر پارامترهای کیفیت تصویر نهان‌نگاری شده مقایسه شده‌اند که نتایج در جدول ۴ نشان داده شده است. با توجه به اینکه روش DCT-M3 علاوه بر جاسازی فقط دو بیت در هر بلاک، موفق به کاهش تغییرات لازم برای جاسازی داده شده است، بنابراین این روش از لحاظ معیارهای کیفیت تصویر نهان‌نگاری شده نسبت به دو روش برتر پیشنهادی موفق‌تر است. اما کیفیت تصویر نهان‌نگاری شده حاصل از روش های MPS [۲۱] و MedFreq [۲۲] پایین‌تر از دو روش پیشنهادی است.

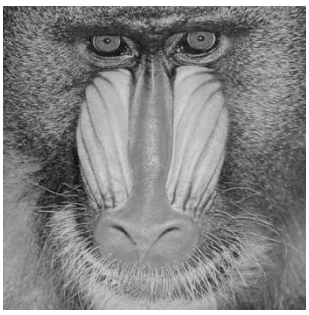
۴-۲- ظرفیت جاسازی

هر روش نهان‌نگاری ظرفیت جاسازی مشخصی دارد. منظور از ظرفیت جاسازی، حداکثر تعداد بیتی است که می توان با استفاده از این روش در هر تصویر جاسازی کرد. یک روش دیگر بیان ظرفیت جاسازی بر حسب bpnz است که حاصل تقسیم حداکثر تعداد بیت قابل جاسازی بر تعداد ضرایب DCT غیر صفر تصویر است. برای مقایسه ظرفیت جاسازی روش‌های پیشنهادی و روش‌های قبلی از سه تصویر سطح خاکستری نمونه با ابعاد ۵۱۲×۵۱۲ شامل Lena، Baboon و Peppers استفاده شده است که در شکل ۵ نمایش داده شده اند. نتایج این آزمون در جدول ۵ ارائه شده است. در این جدول برای هر روش و هر تصویر دو عدد ذکر شده است که عدد اولی حداکثر تعداد بیت قابل جاسازی و عدد دوم ظرفیت جاسازی بر حسب bpnz است. برای مثال روش Jsteg قابلیت جاسازی ۲۹۵۲۲ بیت در تصویر یا bpnz ۰/۷۱ در تصویر Lena را دارد.

با توجه به یکسان بودن ظرفیت جاسازی روش‌های ADCT_FR_LC و ADCT_VR_LC در جدول ۵ فقط یکی از این روش‌ها ذکر شده است. همین نکته در مورد روش‌های ADCT_FR_HC و ADCT_VR_HC نیز صادق است.

جدول ۴: میانگین معیارهای MSE، PSNR و SSIM در ۲۰۰ تصویر برای دو روش برتر پیشنهادی و روش های اخیر

Parameter	bpnz	DCT-M3[۱۳]	MPS [۲۱]	MedFreq[۲۲]	ADCT_FR_LC	ADCT_VR_LC
MSE	۰/۱	۱/۶۵۴۳	۳/۷۸۱۶	۹/۲۰۶۹	۲/۷۷۵۲	۲/۷۳۷۶
	۰/۰۵	۰/۷۹۹۱	۱/۸۶۹۷	۴/۶۱۴۸	۱/۳۹۸۵	۱/۳۷۷۲
	۰/۰۱	۰/۱۶۲۶	۰/۳۹۴۱	۰/۹۱۹۸	۰/۲۷۹۷	۰/۲۷۸۹
PSNR	۰/۱	۴۵/۹۸۳۳	۴۲/۴۰۲۵	۳۸/۷۹۷۳	۴۴/۶۴۱۹	۴۴/۷۳۲۴
	۰/۰۵	۴۹/۱۴۷۷	۴۵/۴۶۳۲	۴۱/۸۰۰۰	۴۷/۶۱۳۸	۴۷/۷۰۳۰
	۰/۰۱	۵۶/۰۹۵۹	۵۲/۲۴۰۶	۴۸/۷۹۸۴	۵۴/۶۲۶۶	۵۴/۶۸۰۳
SSIM	۰/۱	۰/۹۸۵۵	۰/۹۶۳۰	۰/۸۰۳۲	۰/۹۸۴۷	۰/۹۸۴۶
	۰/۰۵	۰/۹۹۳۰	۰/۹۸۰۴	۰/۸۷۷۶	۰/۹۹۲۲	۰/۹۹۲۲
	۰/۰۱	۰/۹۹۸۶	۰/۹۹۵۴	۰/۹۶۹۰	۰/۹۹۸۴	۰/۹۹۸۴


(الف) (ب) (ج)

شکل ۵: سه تصویر نمونه (الف) Lena (ب) Baboon (ج) Peppers

بررسی نتایج ارائه شده در جدول ۵ نشان می‌دهد که روش DCT-M3 کمترین ظرفیت و روش [۱۹] بیشترین ظرفیت را دارد که با توجه به الگوریتم جاسازی آنها این نتیجه قابل پیش بینی بود. روش های DCT-M3 [۱۳]، MPS [۲۱] و MedFreq [۲۲] در تمام تصاویر با ابعاد یکسان ظرفیت جاسازی یکسانی دارند ولی روش های دیگر با توجه به ویژگی‌های تصویر ظرفیت متغیری دارند. با توجه به وجود حملات عام موفق برای کشف روش‌های جاسازی، ظرفیت جاسازی بسیار بالا نمی‌تواند نقطه قوتی برای روش نهان نگاری باشد. زیرا در صورت استفاده از این درصد جاسازی بالا، حتما حملات با دقت بالایی قادر به کشف آن روش خواهند بود.

بنابراین اگر روشی بتواند داده کمی را به نحوی جاسازی کند که احتمال کشف آن پایین باشد، بسیار بهتر و کاربردی‌تر است نسبت به روشی که داده زیادی را با احتمال کشف بالا توسط حملات در تصویر جاسازی کند. بنابراین فاکتور بسیار مهم‌تر امنیت روش نهان‌نگاری است که در سطوح جاسازی یکسان سنجیده می‌شود.

جدول ۵: ظرفیت جاسازی روش‌های مختلف بر حسب بیت و bpnz در سه تصویر نمونه

	Peppers	Baboon	Lena
Jsteg	۳۰۱۷۴ (۰/۷۱ bpnz)	۷۱۶۶۵ (۰/۷۵ bpnz)	۲۹۵۲۲ (۰/۷۱ bpnz)
Shield [۱۹]	۱۴۶۸۷۲ (۳/۴۷ bpnz)	۲۹۱۹۴۵ (۳/۰۷ bpnz)	۱۳۹۴۸۱ (۳/۳۸ bpnz)
DCT-M3 [۱۳]	۸۱۹۲ (۰/۱۹ bpnz)	۸۱۹۲ (۰/۰۸ bpnz)	۸۱۹۲ (۰/۱۹ bpnz)
MPS [۲۱]	۱۶۳۸۴ (۰/۳۸ bpnz)	۱۶۳۸۴ (۰/۱۷ bpnz)	۱۶۳۸۴ (۰/۳۹ bpnz)
MedFreq [۲۲]	۱۳۱۰۷۲ (۳/۱۰ bpnz)	۱۳۱۰۷۲ (۱/۳۷ bpnz)	۱۳۱۰۷۲ (۳/۱۸ bpnz)
ADCT-FR_HC	۴۲۷۱۱ (۱/۰۱ bpnz)	۱۰۴۷۵۱ (۱/۱ bpnz)	۴۱۶۹۴ (۱/۰۱ bpnz)
ADCT-FR_LC	۱۴۱۳۴ (۰/۳۳ bpnz)	۳۴۳۰۷ (۰/۳۶ bpnz)	۱۳۷۴۸ (۰/۳۳ bpnz)

۳-۴ مقاومت در برابر حملات

یک روش نهان‌نگاری با ایجاد تغییراتی در تصویر میزبان، تصویر نهان نگاری شده را تولید می کند. حملات نهان‌کاوی برای کشف یک روش نهان‌نگاری از این تغییرات استفاده می‌کنند. هر چه این تغییرات بیشتر باشد، احتمال کشف آن روش نهان‌نگاری بیشتر است. یکی از پارامترهای عددی نشان دهنده دقت هر حمله، مقدار AUC است، که این معیار عبارت است از مساحت زیر نمودار ROC. این مساحت به گونه ای نرمالیزه می‌شود که مقدار آن برای یک روش کشف با موفقیت کامل، ۱ است. هر چه مقدار AUC به ۰/۵ نزدیکتر باشد، حمله مورد نظر ناموفق‌تر و در نتیجه روش جاسازی امن‌تر است. برای مقایسه امنیت روش‌های پیشنهادی و روش‌های قبلی از حمله SPAM [۲۷] استفاده شده است. مقدار AUC حاصل از این حمله برای روش‌های مختلف و در سه سطح جاسازی در جدول ۶ ارائه شده است. در این جدول، در هر سطح جاسازی بهترین نتیجه با قرمز، دومین نتیجه با سبز و سومین نتیجه با آبی مشخص شده است.

نکته ذکر شده در مورد عدم اهمیت ظرفیت جاسازی بالای روش به تنهایی در نتایج حاصل از حمله خود را نشان می‌دهد. با توجه به پیشرفت حملات نمی توان درصد جاسازی بالا را از روش نهان نگاری انتظار داشت، زیرا به راحتی توسط حملات کشف می‌شود و این درصدها قابل استفاده عملی نیستند. نتایج حاصل از حملات نشان می‌دهد اگر این روش‌ها برای درصدهای جاسازی بالاتر از ۰/۱ bpnz استفاده شوند، به راحتی قابل کشف خواهند بود.

بررسی نتایج جدول ۶ نشان می‌دهد که در سطوح جاسازی مختلف، روش ADCT_VR_LC کمترین احتمال کشف، روش ADCT_FR_LC در رتبه دوم و روش Jsteg در رتبه سوم قرار دارد. این مقایسه دو نتیجه اصلی را در پی دارد که می توان از آن در طراحی روش‌های جاسازی جدید استفاده کرد. برتری این سه روش به معنای برتری ایده ایجاد تغییرات کمتر در واحد جاسازی

جدول ۶: معیار AUC در ۲۰۰ تصویر برای روش های مختلف

bpnz	Jsteg	Shield [۱۹]	DCT-M3 [۱۳]	MPS [۲۱]	Medfreq [۲۲]	ADCT_FR_LC	ADCT_FR_HC	ADCT_VR_LC	ADCT_VR_HC
۰/۱	۰/۹۱۵۲	۰/۹۶۲۴	۰/۹۸۵۲	۰/۹۸۹۱	۱	۰/۹۱۰۱	۰/۹۳۱۲	۰/۹۰۷۹	۰/۹۷۰۱
۰/۰۵	۰/۷۹۶۹	۰/۸۵۰۸	۰/۹۳۴۴	۰/۹۵۸۳	۱	۰/۷۷۰۹	۰/۸۴۷۶	۰/۷۶۰۱	۰/۹۴۵۵
۰/۰۱	۰/۵۵۸۳	۰/۵۷۵۵	۰/۷۰۰۴	۰/۷۰۲۹	۰/۹۴۳۵	۰/۵۵۳۴	۰/۵۹۱۹	۰/۵۵۳۲	۰/۶۴۲۳

است، هر چند در این حالت باید در واحدهای جاسازی بیشتری فرآیند جاسازی انجام شود. از طرف دیگر برتری روش‌های تطبیقی پیشنهادی نسبت به روش Jsteg نشان دهنده این است که با استفاده از اختلاف زوج ضریب (به جای خود ضرایب) به عنوان واحد جاسازی می‌توان امنیت روش را افزایش داد. اما از دلایل کشف بسیار بالای روش‌های [۱۳] و [۲۱] و [۲۲]، انتخاب مکان های جاسازی در تصاویر مختلف بدون توجه به ویژگی‌های آن مکان است و بعلاوه این روش‌ها در ضرایب DCT صفر نیز جاسازی انجام می دهند که باعث کشف راحت‌تر آنها می‌شود.

۵- نتیجه گیری

تبدیل DCT به عنوان یکی از پرکاربردترین تبدیلات در فرآیند فشرده سازی تصاویر Jpeg و محبوبیت این تصاویر در اینترنت به دلیل حجم کم، از علل جذب محققان زیادی به حوزه نهان‌نگاری در ضرایب DCT است. اگرچه روش‌های نهان‌نگاری در این حوزه نسبت به حوزه مکان قابلیت کشف کمتری دارند، اما با توجه به پیشرفت بسیار حملات نهان‌کاوی، نیاز به ایده‌هایی برای بهبود امنیت روش‌های نهان نگاری در ضرایب DCT حس می‌شود. تغییر بستر جاسازی، ایده اصلی روش پیشنهادی برای رسیدن به این هدف است. در روش پیشنهادی برخلاف اکثر روش‌های موجود، داده مورد نظر در اختلاف زوج ضریب DCT همسایه جاسازی می‌شود و تعداد بیت جاسازی در هر بار به صورت متغیر و با توجه به اختلاف زوج ضریب انتخاب می‌شود. نتیجه حاصل از مقایسه روش‌های پیشنهادی با دیدگاه‌های مختلف نشان دهنده برتری دیدگاه ایجاد تغییرات کمتر در واحد جاسازی است، هر چند در این حالت باید در واحدهای جاسازی بیشتری فرآیند جاسازی انجام شود. نتایج آزمون‌های مختلف نشان می‌دهد روش‌های ADCT_VR_LC و ADCT_FR_LC با پیروی از این دیدگاه، توانستند با حفظ کیفیت تصویر نهان‌نگاری شده در حد مطلوب و داشتن ظرفیت جاسازی مناسب، امنیت بیشتری در برابر حمله SPAM نسبت به روش‌های قبلی داشته باشند.

منابع

[1] I.J. Kadhim, P. Premaratne, P.J. Vial and B. Halloran, “Comprehensive Survey of Image Steganography: Techniques, Evaluations, and Trends in Future Research,” Neurocomputing, Vol. 335, pp. 299-326, 2019.

[2] M. Hussain, A.W.A. Wahab, Y.I.B. Idris, A.T. Ho and K.H. Jung, “Image Steganography in Spatial Domain: A Survey,” Signal Processing: Image Communication, Vol. 65, pp. 46-66, 2018.

[3] V. Sabeti, S. Samavi and S. Shirani, “An Adaptive LSB Matching Steganography Based on Octonary Complexity Measure,” Multimedia Tools and Applications, Vol. 64, No. 3, pp.777-793, 2013.

[4] S. Bhattacharyya, A. Khan and G. Sanyal, “DCT Difference Modulation (DCTDM) Image Steganography,” International Journal of Information & Network Security, Vol. 3, No. 1, pp. 40 – 63, 2014.

[5] A. Fkirin, G. Attiya and A. El-Sayed, “Steganography Literature Survey, Classification and Comparative Study,” Communications on Applied Electronics, Vol. 5, No. 10, 2016.

[6] J. Jeswani and D.T. Sarode, “A New DCT based Color Video Watermarking using Luminance Component,” IOSR Journal of Computer Engineering (IOSR-JCE), Vol. 16, No. 2, pp. 83–90, 2014.

[7] M. Kharrazi, H.T. Sencar and N. Memon, “Image Steganography: Concepts and Practice,” Lecture Note Series, Institute for Mathematical Sciences, National University of Singapore, 2004.

[8] N. Provos and P. Honeyman, “Hide and Seek: An Introduction to Steganography,” IEEE Security & Privacy, Vol. 1, No. 3, pp. 32-44, 2003.

[9] N. Provos, “Defending Against Statistical Steganalysis”. In Usenix security symposium, Vol. 10, pp. 323-336, 2001.

[10] A. Westfeld, “F5-A Steganographic Algorithm: High Capacity Despite Better Steganalysis”. In Information Hiding: 4th International Workshop, Vol. 2137, pp. 289, 2001.

[11] J. Fridrich, M. Goljan and D. Hogea, “Attacking the OutGuess”. In Proceedings of the ACM Workshop on Multimedia and Security, Vol. 2002, 2002.

[12] J. Fridrich, M. Goljan and D. Holga, “Steganalysis of JPEG Images: Breaking the F5 Algorithm”. In International Workshop on Information Hiding, pp. 310-323, 2003.

[13] A.A. Attaby, F.M. Mona, M. Ahmed and A. Alsammak, “Data hiding inside JPEG images with high resistance to steganalysis using a novel technique: DCT-M3,” Ain Shams Engineering Journal, 2017.

[14] T. Filler, J. Judas and J. Fridrich, “Minimizing Additive Distortion in Steganography using Syndrome-Trellis Codes,” IEEE Transactions on Information Forensics and Security, Vol. 6, No. 3, pp. 920-935, 2011.

[15] Y. Pan, J. Ni and W. Su, “Improved Uniform Embedding for Efficient JPEG Steganography”. In International Conference on Cloud Computing and Security, pp. 125-133, 2016.

[16] Q. Wei, Z. Yin, Z. Wang and X. Zhang, "Distortion Function Based on Residual Blocks for JPEG Steganography," Multimedia Tools and Applications, Vol. 77, No. 14, pp. 17875-17888, 2018.

[17] D.C. Wu and W.H. Tsai, "A Steganographic Method for Images by Pixel-Value Differencing," Pattern Recognition Letters, Vol. 24, pp. 1613–1626, 2003.

[18] L. Yu, Y. Zhao, R. Ni and Z. Zhu, "PM1 Steganography in JPEG Images Using Genetic Algorithm," Soft Computing, Vol. 13, No. 4, pp. 393–400, 2009.

[19] D. Bansal and R. Chhikara, "An Improved DCT Based Steganography Technique," International Journal of Computer Applications, Vol. 102, No. 14, 2014.

[20] T. Rabie and I. Kamel, "High-Capacity Steganography: A Global-Adaptive-Region Discrete Cosine Transform Approach," Multimedia Tools and Applications, Vol. 76, No. 5, pp. 6473-6493, 2017.

[21] A.S. Ansari, M.S. Mohammadi, and M.T. Parvez, "JPEG Image Steganography based on Coefficients Selection and Partition," International Journal of Image, Graphics & Signal Processing, Vol. 9, No.6, pp. 14-22, 2017.

[22] S. Khan, M.A. Irfan, A. Arif, S.T.H. Rizvi, A. Gul, M. Naeem and N. Ahmad, "On Hiding Secret Information in Medium Frequency DCT Components Using Least Significant Bits Steganography," CMES-Computer Modeling in Engineering & Sciences, Vol. 118, No. 3, pp. 529-546, 2019.

[23] E.H. Rachmawanto and C.A. Sari, "Secure Image Steganography Algorithm Based on DCT with OTP Encryption," Journal of Applied Intelligent System, Vol. 2, No. 1, pp. 1-11, 2017.

[24] Y.K. Singh and S. Sharma, "Image Steganography on Gray and Color Image Using DCT Enhancement and RSA with LSB Method". In International Conference on Inventive Computation Technologies (ICICT), Vol. 3, pp. 1-5, 2016.

[25] D. Hou, H. Wang, W. Zhang and N. Yu, "Reversible Data Hiding in JPEG Image Based on DCT Frequency and Block Selection," Signal Processing, Vol. 148, pp.41-47, 2018.

[26] F. Huang, X. Qu, H.J. Kim and J. Huang, "Reversible Data Hiding in JPEG Images," IEEE Transactions on Circuits and Systems for Video Technology, Vol. 26, No. 9, pp. 1610-1621, 2015.

[27] T. Pevny, P. Bas and J. Fridrich, "Steganalysis by Subtractive Pixel Adjacency Matrix," IEEE Transactions on Information Forensics and Security, Vol. 5, No. 2, pp. 215-224, 2010.