نشانه‌گذاری نیمه‌شکننده مبتنی بر تبدیل موجک ترفیع و نزدیک‌ترین همسایه جهت تشخیص دستکاری در تصاویر رنگی و خاکستری

بهروز بلوریان حقیقی[۱]، کارشناس ارشد؛ امیرحسین طاهری‌نیا[۲]، استادیار

۱- گروه کامپیوتر - دانشکده مهندسی - دانشگاه فردوسی مشهد - مشهد - ایران - b.bolourian@stu.um.ac.ir

۲- گروه کامپیوتر - دانشکده مهندسی - دانشگاه فردوسی مشهد - مشهد - ایران - taherinia@um.ac.ir

چکیده: امروزه حجم زیادی از داده‌های چندرسانه‌ای به راحتی از طریق اینترنت در دسترس همه است و به سهولت با استفاده از ابزارهای پردازش تصویر می‌تواند تغییر داده یا اصلاح شوند. نشانه‌گذاری رقمی یک فناوری در حال توسعه برای اطمینان و تسهیل اعتبار داده‌ها، امنیت و محافظت از حق تألیف رسانه‌های رقمی است. یکی از کاربردهای نشانه‌گذاری رقمی احراز صحت ناحیه دستکاری شده است. روش‌های نشانه‌گذاری رقمی که جهت تشخیص ارائه شده‌اند، قادرند با استفاده از اطلاعاتی که از قبل در رسانه تعبیه شده است پی به صحت و یکپارچگی تصویر دریافت‌شده ببرند. در این مقاله روشی جهت شناسایی ناحیه دستکاری در تصاویر رنگی و خاکستری ارائه شده است. در روش پیشنهادی ابتدا به تصویر تبدیل موجک ترفیع اعمال و لبه‌های افقی را به بلوک‌های کوچک غیرهمپوشان تجزیه نموده و نشانه دودویی را با چندی‌سازی دو ضریب بیشینه در بلوک‌های حاصل جاسازی می‌کنیم. جهت استخراج نشانه، مجموعه از ویژگی‌های آماری از هر بلوک استخراج شده و به‌عنوان داده آموزشی در اختیار الگوریتم یادگیری قرار می‌گیرد. جهت استخراج نشانه با بالاترین همبستگی از الگوریتم نزدیک‌ترین همسایه استفاده شده است. درنهایت نشانه استخراج‌شده با نشانه اصلی مقایسه و ناحیه دستکاری مشخص می‌شود. نتایج نشان می‌دهد که روش پیشنهادی توانایی شناسایی ناحیه دستکاری با دقت بالا، تحت حملات مختلف مانند بهبود تباین، فیلترگاوسی، نویز نمک-فلفل، تیزکردن، فشرده‌سازی و حتی اعمال حملات به صورت ترکیبی را دارد.

واژه‌های کلیدی: نشانه‌گذاری، احراز صحت، تشخیص دستکاری، جاسازی و استخراج نشانه، موجک ترفیع، K نزدیک‌ترین همسایه.

Semi-Fragile Watermarking for Tamper Detection of Color and Gray Images Based On Lifting Wavelet Transform and Nearest Neighbor

B. Bolourian Haghighi[1], MSc; A. H. Taherinia[2], Assistant Professor

1- Department of Computer, Faculty of Engineering, Ferdowsi University of Mashhad, Mashhad, Iran, Email: b.bolourian@stu.um.ac.ir
2- Department of Computer, Faculty of Engineering, Ferdowsi University of Mashhad, Mashhad, Iran, Email: taherinia@um.ac.ir

Abstract: Today, a large number of multimedia data are easily accessible via the Internet and can be changed or modified simply by using image processing tools. Digital watermarking is a developing technology to ensure and facilitate data validation and security and also protect the copyright of digital media. One of the applications of digital watermarking is authenticating and detecting tampered region. Digital watermarking methods have been proposed for detection, are able to authenticate and check the integrity of the received image by utilizing the information that is already embedded in the media. In this paper, a new method is proposed for the detection of tampered region in the color and grayscale images. In the proposed method, at first, a lifting wavelet transform is applied to the image. Afterward, the horizontal edges are divided into the non-overlapping small blocks and then, the binary watermark is embedded in blocks by quantitating the two maximum factors. To extract the watermark, a set of statistical parameters are calculated for each block and considered as training data for the learning algorithm. For extracting the maximum correlation watermark, the nearest neighbor algorithm is used. Finally, the obtained watermark will be compared with the original watermark and the tampered region will be detected. The experimental results show that the proposed method is capable of detecting tampering area with high accuracy under various attacks such as histogram equalization, Gaussian filter, salt and pepper noise, sharpening, compression, and even combination attacks.

Keywords: Watermarking, authentication, tamper detection, embed and extract watermark, lifting wavelet, k-nearest neighbor.

تاریخ ارسال مقاله: ۱۳۹۵/۰۸/۱۷
تاریخ اصلاح مقاله: ۱۳۹۵/۱۱/۰۳ و ۱۳۹۵/۱۱/۱۴
تاریخ پذیرش مقاله: ۱۳۹۶/۰۱/۱۵
نام نویسنده مسئول: امیرحسین طاهری‌نیا
نشانی نویسنده مسئول: ایران - مشهد - دانشگاه فردوسی مشهد - دانشکده فنی مهندسی.

۱- مقدمه

با گسترش تبادلات الکترونیکی در دنیای اینترنت و فراگیر شدن آن، لزوم استفاده از رایانه و انواع شبکه‌های ارتباطی رایانه‌ای برای تسریع در کار ارسال و دریافت اسناد و مدارک، بیش‌ازپیش احساس می‌شود. دسته‌ای از اسناد مذکور تصاویر هستند؛ یکی از چالش‌های مهم در این زمینه، حفظ امنیت و یکپارچگی تصویر از لحاظ سندیت و هویت فرستنده آن، از طریق این‌گونه شبکه‌های ارتباطی می‌باشد. بنابراین می‌توان گفت در ارتباطات الکترونیکی، ارسال و دریافت تصویر نیز جهت حفظ امنیت، مستلزم امضای الکترونیکی منحصربه‌فرد است که بتوان به کمک آن صحت و اصالت تصویر دریافت‌شده را ثابت نمود. نشانه‌گذاری رقمی، فناوری در حال توسعه برای اطمینان و تسهیل اعتبار داده‌ها، امنیت و محافظت از حق‌تالیف رسانه‌های رقمی است [۱]. نشانه‌گذاری به‌عنوان یک روش در حفاظت حق‌نشر و جلوگیری از تکثیر غیرقانونی اطلاعات، روش مناسبی محسوب می‌شود. این روش‌ها سعی دارند با جاسازی اطلاعات در سیگنال میزبان یا به‌عبارتی رسانه، حق‌نشر، صحت و یکپارچگی تصویر را تضمین کنند [۲]. روش‌های نشانه‌گذاری از جنبه‌های مختلف به شرح زیر طبقه‌بندی می‌شوند.

برحسب مقاومت- یکی از ویژگی‌های مهم روش‌های نشانه‌گذاری مقاومت آن‌ها در برابر حملات می‌باشد [۳]. از این دیدگاه این روش‌ها را به سه دسته اصلی تقسیم می‌کنند. درصورتی که نشانه جاسازی‌شده نسبت به حملات مقاوم بوده و پس از حمله هم بتوان آن را به درستی از تصویر استخراج نمود، مقاوم[۱] تلقی می‌شود؛ اگر در برابر حملات و دستکاری مقاوم نبوده و با انجام تغییرات نشانه از بین برود، نشانه‌گذاری شکننده[۲] محسوب می‌شود و درنهایت درصورتی که در برابر برخی از حملات غیرعمدی مانند فشرده‌سازی مقاوم باشد و در روند استخراج نشانه در برابر این قبیل حملات چالشی ایجاد نشود، در دسته روش‌های نیمه‌شکننده[۳] قرار می‌گیرد.

برحسب مشاهده‌پذیری- روش‌های نشانه‌گذاری از دیدگاه مشاهده‌پذیری یا قابل درک بودن به دو دسته قابل مشاهده و غیرقابل مشاهده تقسیم می‌شوند [۳]. اگر نشانه برای همه قابل مشاهده باشد، مثل درج یک آرم بر روی یک تصویر، نشانه‌گذاری قابل مشاهده است. در مقابل، اگر نشانه جاسازی‌شده در محتوا قابل مشاهده نباشد و تنها توسط الگوریتم خاص قابل استخراج باشد، روش غیرقابل مشاهده می‌باشد، که به مراتب امنیت بیش‌تری نسبت به قابل مشاهده دارد.

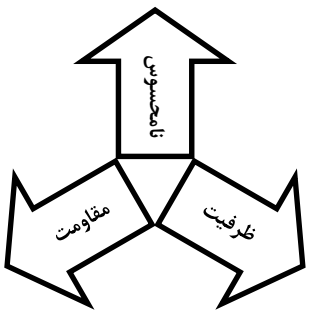
برحسب نوع نشانه- نشانه جاسازی‌شده در سیگنال میزبان خود به دو نوع نویزی و تصویر دسته‌بندی می‌شود [۳]. در نوع نویزی، از انواع نویز همانند گاوسی و تصادفی استفاده می‌شود. نوع تصویر نیز، تصاویر دودویی و آرم‌هایی برای جاسازی در محتوا میزبان می‌باشد.

برحسب ظرفیت و گنجایش اطلاعات- ظرفیت سیستم نشانه‌گذاری عبارت است از حداکثر میزان اطلاعات که می‌توان در رسانه جاسازی نمود [۳]. تعداد بیت‌های نشانه در یک پیام را بار مفید[۴] و حداکثر تکرار بار مفید در یک تصویر ظرفیت الگوریتم نشانه‌گذاری را مشخص می‌کند.

برحسب حوزه نشانه‌گذاری- طبقه‌بندی مهم دیگری که در روش‌های نشانه‌گذاری اهمیت به‌سزایی دارد، حوزه تعبیه نشانه می‌باشد [۴]. از این جهت، به حوزه مکان و فرکانس تقسیم می‌شوند. در حوزه مکان تغییرات مستقیماً بر روی پیکسل اعمال می‌شود. نمونه‌ای از روش‌های این حوزه می‌توان به جاسازی نشانه در بیت‌های کم ارزش پیکسل‌ها اشاره کرد. در مقابل روش‌های حوزه فرکانس با تغییر ضرایب فرکانس نشانه را در سیگنال جاسازی می‌کنند. تبدیل‌ها کسینوسی و موجک نمونه از تبدیلات حوزه فرکانس هستند. روش‌های این حوزه معمولاً نسبت به روش‌های استفاده‌شده در حوزه مکان پیچیده‌تر هستند، ولی عملکرد بهتری در برابر حملات دارند.

برحسب فرآیند تشخیص- اگر جهت استخراج نشانه به تصویر اصلی نیاز باشد، نشانه‌گذاری بینا[۵] نامیده می‌شود؛ درصورتی‌که به هیچ اطلاعاتی جهت استخراج نشانه نیاز نباشد، نشانه‌گذاری کور[۶] تلقی می‌شود. در دسته سوم، اگر به اطلاعاتی مانند نشانه اصلی جهت استخراج نشانه نیاز باشد، نشانه‌گذاری نیمه‌کور[۷] است [۴].

مصالحه بین ویژگی‌ها- یک اصل اساسی نشانه‌گذاری، استخراج افزونگی در تصاویر برای تعبیه اطلاعات نشانه می‌باشد. نشانه‌گذاری این امکان را با تعبیه اطلاعات اضافی در بخش‌های زائد مهیا می‌کند. علاوه‌براین، همانند شکل ۱، افزایش مقاومت نشانه به‌طور معمول نیاز به تحریف بیش‌تر تصویر و افزایش افزونگی دارد. این عمل باعث کاهش غیرقابل مشاهده بودن و به احتمال زیاد منجربه حذف در برابرحملات مخرب می‌شود، درنتیجه در طراحی روش‌های نشانه‌گذاری باید مصالحه و توازنی بین این سه ویژگی‌ها برقرار باشد.



شکل ۱: مصالحه بین مقاومت، ظرفیت، نامحسوس

با توجه به فراگیر شدن اینترنت در سال‌های اخیر و رقمی شدن تصاویر و حساسیت داده‌ها، تشخیص تصاویر رقمی دستکاری شده اهمیت بالایی دارد؛ برای مثال دستکاری یک تصویر در اخبار و عدم تشخیص آن می‌تواند منجر به تحریف واقعیت شود[۵]. روش‌های شناسایی دستکاری تصاویر رقمی به مجموعه‌ای از الگوریتم‌هایی اشاره دارد که صرف‌نظر از ابزارها و درجه پیچیدگی تلاش مشترک همه آن‌ها تضمین صحت تصاویر رقمی است. تصاویر رقمی روزمره در نشریات، روزنامه‌ها، گردش الکترونیکی پول و اسناد حقوقی انتقال می‌یابند و عدم

توجه به صحت آن‌ها می‌تواند صدمات جدی را به طیف وسیعی از کاربران فناوری اطلاعات و ارتباطات وارد آورد. یکی از روش‌های مناسب جهت مغلوب کردن این چالش‌ها بهره‌گیری از نشانه‌گذاری می‌باشد.

در تشخیص دستکاری تصاویر ابتدا یکپارچگی و صحت تصاویر بررسی شده و سپس ناحیه دستکاری مشخص می‌شود[۶، ۷]. اکثر روش‌های تشخیص دستکاری تصاویر بر روی زیربلوک‌های تصویر انجام می‌شوند. هرچه این بلوک‌ها بزرگ‌تر باشند، شامل اطلاعات بیش‌تری هستند و موجب خطای تشخیص دستکاری کم‌تری می‌شوند ولی توانایی تعیین ناحیه دقیق دستکاری پایین می‌آید[۸].

حملاتی که به‌منظور دستکاری بر روی رسانه صورت می‌گیرد به دو دسته عمدی و غیرعمدی تقسیم می‌شوند. از انواع حملات غیرعمدی می‌توان به فشرده‌سازی، بهبود تباین[۸]، تیزکردن، فیلتر گاوسی، نویز نمک-فلفل و تبدیلات هندسی اشاره نمود. روش‌های پیشنهادی باید در برابر این قبیل حملات مقاوم بوده و پس از اعمال این عملیات قادر به استخراج نشانه باشند. از انواع دستکاری‌ها می‌توان به ترکیب دو تصویر[۹]، رونوشت مکان[۱۰] و افزودن، تحریف و حذف اشیا در تصویر اشاره کرد.

در این مقاله به جهت بهبود امنیت و کیفیت تصویر نشانه‌گذاری‌شده و همچنین مقاومت نشانه در برابر حملاتی مانند فشرده‌سازی، عملیات پایه پردازش تصویر، ترکیبی و تشخیص دستکاری رونوشت مکان و به‌منظور افزایش نرخ صحت تشخیص ناحیه دستکاری روش نشانه‌گذاری مبتنی بر تبدیل موجک ترفیع و الگوریتم یادگیری نزدیک‌ترین همسایه پیشنهاد شده است. علاوه‌براین، جهت جلوگیری از تخریب نشانه، غیرقابل پیش‌بینی بودن مکان جازسازی‌شده و تأمین امنیت از نگاشت‌های آشوبی استفاده شده است. نتایج نشان‌دهنده، ایمنی و تأثیر بهتر در تشخیص ناحیه دستکاری‌شده در هنگام اعمال حملات ذکرشده می‌باشد. به‌طورکلی روش پیشنهادی ارائه‌شده نسبت به سایر روش‌ها در چهار عامل برتری مطلق دارد. ۱) نرخ بالا در تشخیص ناحیه دستکاری در حضور حملات ذکرشده، ۲) توانایی نشانه‌گذاری در تصاویر خاکستری و رنگی، ۳) مقاومت در برابر حمله رونوشت مکان، ۴) وضوح تصویر مناسب تصویر نشانه‌گذاری‌شده، ۵) عدم نیاز به تصویر اصلی جهت استخراج نشانه.

ادامه این مقاله به ترتیب زیر بیان می‌شود. در بخش بعدی کارهای پیشین مورد بررسی قرار می‌گیرد، سپس در بخش ۳ و ۴، به ترتیب الزامات و روش پیشنهادی معرفی و تشریح شده است. درنهایت نتایج حاصل از اجرای روش بر روی تصاویر مختلف در قسمت ۵ بررسی شده و بخش ۶ بیانگر نتیجه‌گیری حاصل شده است.

۲- پیشینه کارهای مرتبط

تاکنون راهکارهای زیادی جهت نشانه‌گذاری و تشخیص دستکاری ارائه شده است که در زیر به‌طور خلاصه برخی از آن‌ها بیان شده‌اند. در [۹]، به یک روش تشخیص دستکاری سلسله مراتبی پرداخته شده است. طبق این روش تشخیص ناحیه دستکاری‌شده طی سه مرحله انجام می‌شود. اگر ناحیه دستکاری‌شده در مرحله اول تشخیص داده نشد، با احتمال نزدیک به ۹۰ درصد در مراحل دو و سه تشخیص داده می‌شود. اشکال عمده این روش این است که نسبت به خطا در پیکسل‌ها بسیار حساس است. در [۱۰]، از حوزه مکان جهت نشانه‌گذاری استفاده شده است. اگرچه کیفیت تصویر نشانه‌گذاری‌شده تا حدی مناسب است، اما ضعف اساسی روش عدم مقاومت در برابر حملات مختلف است. در بسیاری از روش‌ها مانند [۱۱، ۱۲] تشخیص ناحیه دستکاری از طریق قرار دادن بیت‌های نشانه احراز صحت، در بیت‌های کم ارزش سایر بلوک‌ها صورت می‌گیرد. در این روش‌ها اگر بلوک‌هایی که شامل بیت نشانه، سایر بلوک‌ها هستند تخریب شوند، شناسایی دستکاری تصویر مقدور نخواهد بود.

در [۱۳]، نشانه‌گذاری در حوزه تبدیل کسینوسی گسسته صورت می‌گیرد، به این ترتیب که نشانه در ضرایب فرکانس‌های میانی پنهان شده و سپس تبدیل معکوس کسینوسی گسسته انجام می‌شود. این روش نسبت به تغییرات تباین و فیلترهای میان‌گذر مقاوم هستند، ولی نسبت به چرخش و تغییر مقیاس و حمله رونوشت مکان ضعف دارند.

روش‌هایی مانند [۱۴]، که نشانه‌گذاری را در حوزه تبدیل فوریه گسسته انجام می‌دهند، برخلاف روش‌های که از تبدیل کسینوسی گسسته استفاده می‌کنند، در برابر چرخش و تغییر مقیاس مقاوم هستند، ولی نیازمند محاسبات پیچیده‌تری می‌باشند. همچنین در [۱۵]، از یک شیوه تشخیص دستکاری استفاده شده که در آن از اطلاعات لبه‌ها که با موجک دوسطحی به دست می‌آید، برای جاسازی نشانه استفاده شده و با استفاده از بسته موجک ناحیه دستکاری‌شده مشخص می‌شود. در [۱۶، ۱۷] نیز دو روش بر اساس استفاده از کدکردن آستانه بلوک و تجزیه مقادیر تکین پیشنهاد شده است. هر دو این روش‌ها نمی‌توانند ناحیه دستکاری‌شده را به خوبی شناسایی کنند. مقاله [۱۸]، یک نشانه از تصویر اصلی را توسط قانون وبر، ایجاد می‌کند. این روش تصویر را به بلوک‌های مجزا تقسیم می‌کند و پیکسل‌های مرکزی آن‌ها برای نشانه‌گذاری انتخاب می‌شود. در این روش جاسازی نشانه در حوزه مکان است.

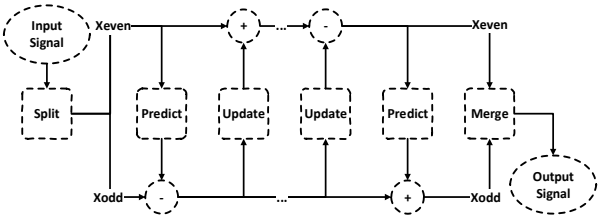
در [۱۹]، یک نشانه دودویی و خلاصه‌ای از تصویر با تغییر ضرایب موجک به‌عنوان نشانه جاسازی شده است و از تصویر نیم-تن[۱۱] برای به‌دست آوردن نسخه‌ای از تصویر با وضوح پایین استفاده می‌شود. درنهایت تصویر حاصل را با تصویر اصلی مقایسه و ناحیه دستکاری‌شده را مشخص می‌کند. این شیوه در برابر حملات عمدی مقاومت بالایی دارد، اما دقت معیار شباهت در آن پایین‌تر از روش پیشنهادشده توسط این مقاله می‌باشد. در [۲۰]، روشی کارا جهت تشخیص و بازیابی ناحیه تخریب‌شده برپایه تجزیه مقادیر تکین ارائه شده است که نشانه را در بیت‌های کم ارزش پیکسل‌های تصویر تعبیه می‌کند. این امر نقطه ضعف روش در برابر حملات مختلف ازجمله فشرده‌سازی محسوب می‌شود.

۳- الزامات

۳-۱- طرح‌واره موجک ترفیع

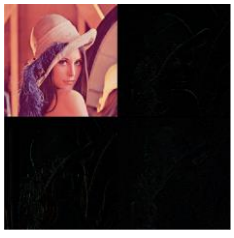
طرح‌واره موجک ترفیع(LWS)، تبدیل موجک مرسوم را به موجک‌های نسل دوم تعمیم می‌دهد و یک روش انعطاف‌پذیر جهت ایجاد تبدیل‌های موجک خطی و غیرخطی است[۲۱]. از اساسی‌ترین ویژگی طرح‌واره موجک ترفیع محاسبات در حوزه زمان است که دارای دو مزیت اساسی می‌باشد. ابتدا این که نیاز به تشکیل تبدیل فوریه به‌عنوان پیش نیاز ندارد و دوم اینکه این روش زیرساخت‌های الگوریتمی مهیا می‌کند که توانایی ساخت سیگنال و اعمال تبدیل معکوس به سهولت فراهم می‌شود.

سه گام اساسی در طرح‌واره ترفیع عبارت‌اند از تقسیم، پیش‌بینی و به‌روزرسانی. در مرحله تقسیم، ابتدا نمونه‌های سیگنال را به دو مجموعه زوج و فرد جدا می‌کند. زیرمجموعه‌های زوج و فرد در مجموعه اصلی پراکنده هستند و اگر ورودی دنباله‌ای تصادفی نباشد، بین مقادیر نزدیک به هم همبستگی وجود دارد. به دست آوردن وابستگی‌ها یا ساختارهایی در داده، هدف اصلی در هر بازنمایی فشرده است. در مرحله پیش‌بینی هر نمونه‌ی فرد با استفاده از تعدادی نمونه‌های زوج اطراف آن پیش‌بینی می‌شود. اختلاف بین مقادیر واقعی نمونه‌های فرد و پیش‌بینی آن‌ها به‌عنوان جزئیات ضرایب در نظر گرفته می‌شود. اگر جریان ورودی به‌طور کامل از ساختار در نظر گرفته شده در قانون پیش‌بینی تبعیت کند، همه‌ی جزئیات صفر می‌شوند. درنتیجه جزئیات انحراف سیگنال از ساختار فراهم شده و متعلق به سطح مقیاس جاری می‌باشد. این بدین معنی است که آن‌ها باید از سیگنال حذف شوند تا یک نوع هموارتر با مقیاس پایین ترحاصل شود. در مرحله به‌روزرسانی نمونه‌های زوج بر مبنای جزئیات به‌دست‌آمده اصلاح می‌شوند، طوری که ویژگی‌های بارز سیگنال اولیه را در تقریب‌هایش حفظ کند. خروجی مرحله به‌روزرسانی، ضرایب تقریب هستند، که نوع هموارتر سیگنال ورودی را می‌دهند. شکل ۲، شمای کلی طرح‌واره ترفیع را نشانه می‌دهد.



شکل ۲: شمای کلی طرح‌واره ترفیع مستقیم و معکوس

شکل ۳، اعمال تبدیل موجک ترفیع صحیح با استفاده از فیلتر هار را برروی تصویر $Lena$ نشان می‌دهد.



شکل ۳: تبدیل موجک ترفیع صحیح

۳-۲- نگاشت آشوبی[۱۲]

یکی از راه‌های حفاظت از اطلاعات، رمز نمودن آن است. الگوریتم‌های آشوبی با دارا بودن ویژگیهایی مانند حساسیت به شرایط اولیه، قطعیت و عدم پیش‌بینی آماری، انتخاب مناسب جهت تأمین امنیت روش‌های نشانه‌گذاری می‌باشند. به‌طورکلی روش‌های آشوبی دارای یک فرآیند قطعی هستند، ولی در ظاهر یک فرآیند تصادفی به‌نظر می‌رسند. به‌دلیل این ویژگی‌ها استفاده از این روش‌ها در نشانه‌گذاری منجر به بهبود امنیت می‌شود، به‌گونه‌ای که از دید مهاجم مکان تعبیه نشانه تصادفی به‌نظر می‌رسد، درحالیکه از دید گیرنده اصلی تعریف‌پذیر می‌باشد.

۳-۲-۱- نگاشت منطقی[۱۳]

میشل فایگن در سال ۱۹۷۴ در آزمایشگاه ملی در آمریکا مشغول به بررسی یک نگاشت منطقی[۱۰] با رابطه:

$$x_{n+1} = r x_n (1 - x_n) \quad (۱)$$

بود. رابطه (۱) وابسته به r بوده و از یک فرم غیرخطی مربعی ساده استفاده می‌کند. او در خلال بررسی‌های خود، متوجه شد که این معادله ساده، علاوه‌بر پاسخ‌های قابل انتظار، دارای پاسخ‌های تناوبی دیگری نیز هست که فقط با تغییر r حاصل می‌شود. اگر r، از یک مقدار مشخصی بیش‌تر شود، پاسخ این سیستم آشوب گونه خواهد شد.

۳-۲-۲- نگاشت متقابل[۱۴]

نگاشت متقابل [۲۴]، یک نگاشت آشوبی دوبعدی می‌باشد، که توسط دو نگاشت آشوبی یک‌بعدی بی‌نظم همانند:

$$\begin{cases} x_i = 1 - \alpha y_{i-1}^2 \\ y_i = \cos(\beta arccos x_{i-1}) \end{cases} \quad (۲)$$

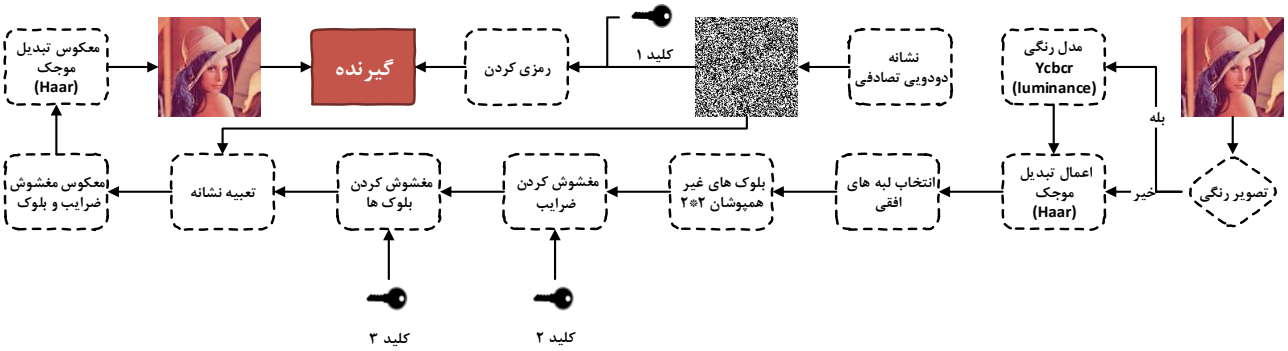
ساخته شده است. در رابطه (۲)، $x, y \in [-1, 1]$ و α و β پارامترهای کنترلی هستند. این نگاشت دارای خواص زیر می‌باشد.

- این نگاشت آشوبی است زمانی‌که $\alpha = 2$ و $\beta = 6$.
- مقدار میانگین دنباله $\{x_i\}$ و $\{y_i\}$ تولیدشده توسط این نگاشت برای همه مقادیر اولیه x_0 و y_0، صفر هستند.
- دنباله $\{(x_n, y_n)\}(n = 0,1, \dots)$ با توجه به مقدار اولیه قراردادی (x_0, y_0)، می‌تواند توسط این نگاشت ساخته شود. به‌طور مشابه، مقدار اولیه دیگر $(\acute{x}_0, \acute{y}_0)$، دنباله $\{(\acute{x}_n, \acute{y}_n)\}(n = 0,1, \dots)$ را ایجاد می‌کند، درنتیجه، همبستگی بین توالی تقریباً صفر است.

۴- روش پیشنهادی

در این بخش به تشریح روش پشنهادی می‌پردازیم. در این روش برای جاسازی نشانه از تبدیل موجک ترفیع استفاده شده است. علت استفاده از این تبدیل جهت جاسازی نشانه، عدم حساسیت زیاد به تغییر ضرایب و کیفیت مطلوب تصویر نشانه‌گذاری‌شده درمقایسه با تصویر اصلی می‌باشد. از طرفی از دیگر مزایا موجک ترفیع صحیح نسبت به موجک سنتی می‌توان به سرعت بالا و عدم نیاز به حافظه بالا، اشاره کرد، که

این ویژگی‌ها شرایط اجرا روش پیشنهادی را بر روی دستگاه‌های که از لحاظ سخت‌افزار ضعیف می‌باشند را فراهم می‌کند. از طرفی جهت استخراج نشانه از الگوریتم یادگیری، نزدیک‌ترین همسایه [۲۷، ۲۸]، استفاده شده که توانایی آموزش و تعمیم‌پذیر بالا و همچنین قابلیت استخراج نشانه با بیش‌ترین همبستگی در هنگام اعمال حملات مختلف به تصویر را دارد.



شکل۴: فرآیند کلی ساخت و تعبیه نشانه روش پیشنهادی

۴-۱- ساخت و تعبیه نشانه جهت احراز صحت

اندازه تصاویر استفاده‌شده در این مقاله $N \times M$ پیکسل فرض شده است، که در آن M و N مضربی از ۴ هستند. مراحل ساخت و تعبیه نشانه همان‌طور که در شکل ۴ نشان داده شده به شرح زیر است.

۱) توسط $Key1$ دنباله دودویی تصادفی W به اندازه $\frac{N}{4}\times\frac{M}{4}$ ایجاد می‌کنیم.

۲) اگر تصویر رنگی است، به مدل رنگی $Ycbcr$ تبدیل شده و باند روشنایی[۱۵] را استخراج و آن را $Gray$ می‌نامیم.

۳) یک سطح تبدیل موجک ترفیع صحیح، بر روی $Gray$ اعمال کرده و زیر باند فرکانس افقی را استخراج کرده و آن را $CH1$ می‌نامیم.

۴) با استفاده از نگاشت متقابل و توسط $Key2$ ضرایب $CH1$ را مغشوش نموده و سپس ضرایب حاصل را به بلوک‌های ۲×۲ غیرهمپوشان تقسیم نموده و به‌وسیله $Key3$ این بلوک‌ها را جابه‌جا می‌کنیم؛ حاصل را $SCH1$ نامیده و به مرحله بعد می‌رویم.

۵) اکنون $SCH1$ را به بلوک‌های غیرهمپوشان ۲×۲ تقسیم نموده، سپس μ و Dif_i^{max} در هر بلوک را طبق روابط:

$$\mu = \left[\frac{\sum_{i=1}^{length_w} Dif_i^{max}}{length_w}\right] \quad (۳)$$

$$Dif_i^{max} = \left|Coef_i^{first} - Coef_i^{second}\right| \quad (۴)$$

محاسبه می‌کنیم. در رابطه (۳)، $length_w$ تعداد بلوک‌های $SCH1$، یا به‌عبارتی تعداد بیت‌های نشانه و Dif_i^{max} طبق رابطه (۴) محاسبه و بیانگر اختلاف دو ضریب بیشینه در بلوک i می‌باشد. همچنین $Coef_i^{first}$ و $Coef_i^{second}$ به ترتیب نشان‌دهنده اولین و دومین ضریب بیشینه در بلوک i می‌باشد.

۶) طبق الگوریتم ۱، برای هر بلوک i در $SCH1$، W را جاسازی می‌کنیم.

۷) بلوک‌ها و ضرایب $SCH1$، به ترتیب توسط $Key3$ و $Key2$ و با استفاده از نگاشت متقابل، به صورت معکوس جابه‌جا شده و بلوک‌ها و ضرایب در موقعیت اولیه خود قرار می‌گیرد.

۸) در نهایت، تبدیل معکوس موجک صحیح، را اعمال و تصویر نشانه‌گذاری را به دست می‌آوریم. سپس، جهت تأمین امنیت نشانه، آن را توسط نگاشت منطقی مغشوش و همراه تصویر نشانه‌گذاری جهت احراز صحت ارسال می‌کنیم.

الگوریتم ۱: جاسازی بیت‌های نشانه در ضرایب $SCH1$

INPUT: Block coefficient of $SCH1$

While $i < length_w$
  If w_i equal to 1 then
    If Dif_i^{max} less than or equal to max(μ, T) then
      $Coef_i^{first} = Coef_i^{first} + T$
    Else
      $Coef_i^{first} = Coef_i^{first}$
    End if
  Else
    $Coef_i^{first} = Coef_i^{first} - Dif_i^{max}$
  End if
End while

OUTPUT: Watermarked $SCH1$

۴-۲- احراز صحت و یکپارچگی

پس از دریافت تصویر از کانال ارتباطی باید از صحت آن اطمینان حاصل شود، لذا برای این کار مراحل زیر را دنبال می‌کنیم. مراحل ساخت و تعبیه نشانه همان‌طور که در شکل ۵ نشان داده شده به شرح زیر است.

الگوریتم دارای دو واحد اصلی به شرح زیر می‌باشد.

۱) واحد ساخت و تعبیه نشانه که وظیفه ساخت نشانه احراز صحت را برعهده دارد و در گام بعد نشانه را در ضرایب موجک ترفیع، جهت استفاده در واحد احراز صحت تعبیه می‌کند.

۲) واحد احراز صحت و یکپارچگی تصویر که با دریافت نشانه، تصویر نشانه‌گذاری‌شده را از لحاظ دستکاری و تخریب بررسی می‌کند.

۴-۲-۱- استخراج ویژگی

۱) اگر تصویر رنگی است، آن را به مدل رنگی $Ycbcr$ تبدیل نموده و زیرباند روشنایی را استخراج کرده و آن را $Gray$ می‌نامیم.

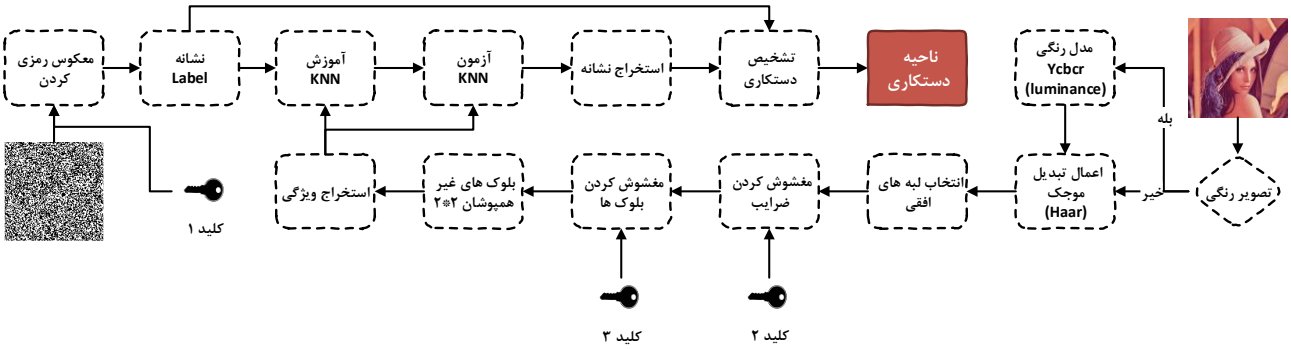
۲) یک سطح تبدیل موجک ترفیع صحیح، بر روی $Gray$ اعمال کرده و زیر باند فرکانس افقی را استخراج کرده و آن را $CH1$ می‌نامیم.

۳) توسط $Key2$ و $Key3$ همانند مرحله تعبیه، ضرایب و بلوک‌های $CH1$ را مغشوش نموده و حاصل را $SCH1$ نامیده و به مرحله بعد می‌رویم.

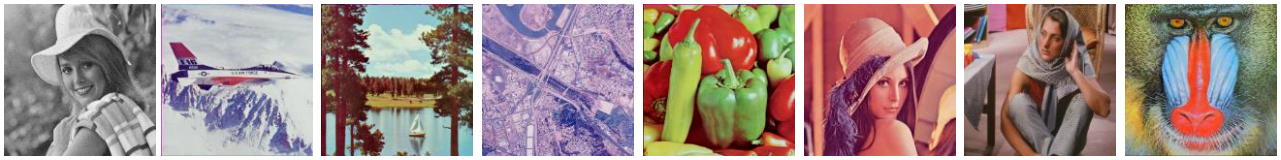
۴) بردار آماری $S_i = \{S(1)_i, \dots, S(10)_i\}$ با ابعاد $10 \times \frac{N}{4} \times \frac{M}{4}$ را برای هر بلوک i در $SCH1$، به کمک استخراج ویژگی‌های آماری مانند درجه اوج[۱۶]، چولگی[۱۷]، بی‌نظمی[۱۸]، انحراف‌معیار، میانگین، واریانس، مد، میانه، کوواریانس و تابع چگالی احتمال تشکیل می‌دهیم.

۵) ضرایب هر بلوک i در $SCH1$ را استخراج کرده و بردار ضرایب $C_i = \{C(1)_i, C(2)_i, C(3)_i\}, C(4)_i\}$ را با ابعاد $4 \times \frac{M}{4} \times \frac{N}{4}$ تشکیل می‌دهیم.

۶) از ترکیب بردارهای آماری(S) و ضرایب(C)، بردار ویژگی $F_i = \{S(1)_i, S(2)_i, \dots, S(10)_i, C(1)_i, \dots, C(4)_i\}$ با ابعاد $14 \times \frac{M}{4} \times \frac{N}{4}$ را ایجاد می‌کنیم.



شکل ۵: فرآیند کلی احراز صحت تصویر روش پیشنهادی

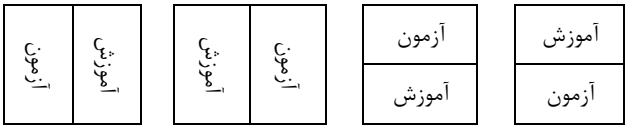


الف) *Baboon* ب) *Barbara* ج) *Lena* د) *Pepper* ه) *Santiago* و) *Lake* ز) *F16* ح) *Elaine*

شکل ۶: تصاویر متعارف بررسی‌شده

۴-۲-۲- آموزش و آزمون

۱) F را همانند شکل ۷، به نواحی مساوی تقسیم می‌کنیم.



شکل ۷: تقسیم بلوک‌های $SCH1$ برای آموزش و آزمایش

۲) همانند شکل ۷، به کمک نشانه ارسال شده $Watermark_{receive}$، که برچسب بلوک‌ها تلقی می‌شود، با استفاده از KNN، عملیات آزمایش و آزمون را بروی F انجام می‌دهیم؛ ترتیب عملیات به شرح زیر است.

- نیمه بالایی آموزش، نیمه پایینی آزمون. $Watermark1_{down}$
- نیمه بالایی آزمون، نیمه پایینی آموزش. $Watermark1_{up}$
- نیمه راست آزمون، نیمه چپ آموزش. $Watermark2_{right}$
- نیمه راست آموزش، نیمه چپ آزمون. $Watermark2_{left}$

۳) حال طبق روابط:

$$Watermark1 = Watermark1_{down} + Watermark1_{up} \quad (۵)$$

$$Watermark2 = Watermark2_{right} + Watermark2_{left} \quad (۶)$$

$Watermark1$ و $Watermark2$ را محاسبه می‌کنیم.

در رابطه (۵)، $Watermark1_{down}, Watermark1_{up}$ و در رابطه (۶) $Watermark2_{left}, Watermark2_{right}$ را با هم الحاق می‌کنیم.

۴) نشانه درج شده در ضرایب را طبق رابطه:

$$Watermark_{extract} = Watermark1 \; Or \; Watermark2 \quad (۷)$$

به‌دست می‌آوریم.

۴-۲-۳- احراز صحت

۱) ناحیه دستکاری‌شده را طبق رابطه:

$$Tamper_{Region} = Watermark_{extract} \oplus Watermark_{receive} \quad (۸)$$

به دست می‌آوریم. در رابطه (۸)، $Watermark_{extract}$، نشانه استخراج‌شده با استفاده از رابطه (۷) می‌باشد.

۲) پیکسل‌هایی که در $Tamper_{Region}$، طول اتصال آن‌ها کم‌تر از ۳ بوده و هیچ همسایه همجوار ۸گانه ندارند را حذف می‌کنیم و $Tamper_{Region}$ را به‌روز می‌کنیم.

۳) عمل بستن از سری عملیات ریخت‌شناسی را با فیلتر شکل ۸، به‌صورت عمودی و افقی بر روی $Tamper_{Region}$ اعمال و آن را به‌روز

می‌کنیم. هدف این است که حفره‌های خالی در بین بلوک‌های دستکاری‌شده را به‌عنوان بلوک تخریب‌شده علامت بزنیم.

۱	۱	۱	۱

شکل ۸: فیلتر عمل بستن عملیات ریخت شناسی

۴) در $Tamper_{Region}$، نواحی که طول اتصال کم‌تر از L بوده و همسایه همجوار ۴گانه ندارند، حذف و $Tamper_{Region}$ را به‌روز می‌کنیم.

۵) در انتها، $Tamper_{Region}$ را به تصویر اصلی تعمیم می‌دهیم.

۵- نتایج آزمایش‌ها

جهت پیاده‌سازی روش پیشنهادی، ۸ تصویر مطابق شکل ۶ مورد استفاده قرار می‌گیرند. اندازه تمام تصویر ۵۱۲×۵۱۲ می‌باشد و تمامی آن‌ها به غیر از تصویر $Elaine$ به‌صورت رنگی و با فرمت BMP ذخیره شده‌اند. تمامی آزمایش‌ها بر روی سیستم با پردازنده $Intel\ Core\ i5-520M$ انجام شده است. زمان محاسبات برای مراحل آموزش، جاسازی و استخراج نشانه در جدول ۱ نشان داده شده است. همان‌طور که مشاهده می‌شود، مجموع زمان مصرفی روش پیشنهادی نسبت به روش‌های مشابه کم‌تر است. زمان مناسب و عملیات ساده، منجر به اجرا روش بر روی دستگاه‌های دارای توان پایین و سخت‌افزار ضعیف می‌شود.

جدول ۱: زمان (ثانیه) محاسبات برای تصویر $Lena$

روش	آموزش	جاسازی	استخراج	مجموع
پیشنهادی	۰/۰۴	۰/۴۴	۱/۱۳	۱/۶۱
[۲۹]	۰/۰۲	۱/۶۲	۰/۰۱	۱/۶۵
[۳۰]	۰/۰۲	۱/۶۵	۰/۰۱	۱/۶۸

بر اساس آزمایش‌های صورت‌گرفته و به جهت برقراری مصالحه بین مقاومت و کیفیت تصویر نشانه‌گذاری‌شده، پارامتر $T = ۱۱$ در نظر گرفته شده است. با افزایش T مقاومت نشانه در برابر حملات مختلف افزایش می‌یابد، اما کیفیت بصری تصویر نشانه‌گذاری کاهش می‌یابد. همچنین با بررسی انجام‌شده، نزدیک‌ترین همسایه در مقابل سایر الگوریتم‌های یادگیری ماشین مانند بردار پشتیبان در پیش‌بینی و تشخیص ناحیه دستکاری در هنگام وقوع حمله برتری مطلق دارد. در آزمایش‌های انجام‌شده مقدار $K = ۱۵$ که نشان دهنده تعداد همسایه‌ها و همچنین $L = ۵$ که طول نواحی متصل همجوار ۴گانه می‌باشد، در نظر گرفته شده است.

جدول ۲، فهرستی از مقادیر $PSNR$ و $SSIM$ تصاویر نشانه‌گذاری‌شده، روش پیشنهادی و برخی دیگر روش‌ها را نشان می‌دهد. معیارهای ارزیابی کیفیت تصویر، برای روش پیشنهادی نسبت به روش‌های دیگری که حتی در برابر حملات مقاوم نیستند، به مراتب بالاتر است. بنابراین تصویر نشانه‌گذاری‌شده، کیفیت بصری بهتری را حفظ می‌کند.

به‌عنوان نمونه، تصویر $Lena$ که یکی از تصاویر معمول حوزه پردازش تصویر است و در جدول ۲، برای تمامی مراجع مقدار کیفیت تصویر نشانه‌گذاری‌شده برای این تصویر گزارش شده است، روش پیشنهادی برتری مطلق دارد.

جداول ۳ تا ۶ به مقایسه همبستگی[۱۹]، نرخ خطا بیتی[۲۰] و تعداد پیکسل‌های که به اشتباه دستکاری تشخیص داده شده‌اند، اشاره دارد. این معیارها بین نشانه جاسازی و استخراج‌شده، برای تصاویر مختلف خاکستری و رنگی که تحت حملات فشرده‌سازی و عملیات پایه پردازش تصویر قرار گرفته‌اند، فهرست شده است. علاوه‌براین، مقادیر $PSNR$ و $SSIM$، بین تصویر نشانه‌گذاری و تصویر تحت اعمال حمله، گزارش شده است تا کارایی روش پیشنهای در برابر این کاهش کیفیت چشم‌گیر که ناشی از تخریب سیگنال می‌باشد، نشان داده شود. به طورکلی، در روش پیشنهادی، نشانه استخراج‌شده دارای همبستگی مناسب با نشانه تعبیه شده است، که این امر منجر به افزایش نرخ صحت تشخیص ناحیه دستکاری‌شده و کاهش خطا در هنگام اعمال حملات مختلف می‌شود.

در شکل ۹، کیفیت تصویر نشانه‌گذاری، همبستگی نشانه جاسازی و استخراج‌شده و همچنین تعداد بلوک‌های دستکاری تشخیص داده‌شده در تصویر $Lena$، پس از حمله‌ها مختلف، نشان داده شده است. نتایج به وضوح نشان می‌دهد که روش پیشنهادشده در برابر حملات مقاومت مطلوبی دارد و با استفاده از عملیات پس پردازش، بلوک‌های که به اشتباه به‌دلیل حملات، نامعتبر تشخیص داده شده‌اند، اصلاح شده و معتبر علامت گذاری می‌شود.

عملکرد روش پیشنهادی در برابر دستکاری‌های مختلف از قبیل حذف با ابعاد مختلف، ترکیب چند تصویر، اضافه کردن شی و رونوشت مکان تحت حملات مختلف مانند فشرده‌سازی، بهبود تباین، تیزکردن، فیلتر گاوسی و نمک-فلفل بر روی تصاویر رنگی و خاکستری رایج پردازش تصویر در اشکال ۱۰ تا ۱۴ گزارش شده است. در این اشکال، قسمت الف، تصویر نشانه‌گذاری‌شده را با دو معیار $PSNR$ و $SSIM$ نشان می‌دهد. بخش ب، به بازنمایی تصویر دستکاری و نوع حمله اعمال‌شده می‌پردازد. بخش‌های پ و ت، به ترتیب $Watermark_{receive}$ نشانه منتقل و $Watermark_{extract}$ نشانه استخراج‌شده از سیگنال را بازنمایی می‌کند. بخش ث و ج به مقایسه ناحیه دستکاری‌نشده بین نشانه منتقل و استخراج‌شده و همچنین مقایسه $Watermark1$ و $Watermark2$ اشاره دارد. قسمت‌های چ، ح و خ به ترتیب احراز صحت به کمک نشانه منتقل و استخراج شده، تعداد بلوک‌هایی که به اشتباه دستکاری تشخیص داده شده‌اند و $Tamper_{Region}$ ناحیه دستکاری‌شده پس از اعمال پس‌پردازش را نشان می‌دهد. درنهایت شکل د، تعمیم $Tamper_{Region}$ به شکل دستکاری‌شده را بازنمایی می‌کند.

نتایج به روشنی نشان می‌دهد که روش پیشنهادشده در برابر کلیه حملات انعطاف‌پذیر است و حتی اگر حملات به‌صورت ترکیبی بر روی تصویر نشانه‌گذاری‌شده اعمال شود، مجدداً با دقت مطلوبی ناحیه دستکاری‌شده را تشخیص می‌دهد و درنتیجه معیار غلط-مثبت به مراتب کم‌تر است. بر اساس ویژگی‌های ذکرشده، روش ارائه‌شده نسب به روش‌هایی که حتی در شناسایی درست و عاری از هرگونه خطا ناحیه دستکاری ضعف دارند، برتری مطلق دارد.

جدول ۲: مقایسه کیفیت تصویر نشانه‌گذاری‌شده روش پیشنهادی و [۱۹، ۲۰، ۲۲- ۲۶]، * عدم مقاومت در برابر حملات، $G = Gray, C = Color$

تصویر	روش پیشنهادی				[۱۹]		[۲۰] *	[۲۲] *	[۲۳] *		[۲۴] *	[۲۵] *	[۲۶]	
	C		G		G		G	G	C	G	G	G	G	
	PSNR	*SSIM*	*PSNR*	*SSIM*	*PSNR*	*SSIM*	*PSNR*	*PSNR*	*PSNR*	*PSNR*	*PSNR*	*PSNR*	*PSNR*	*SSIM*
Baboon	۳۵/۳۶	۰/۹۸۹۹	۴۰/۴۷	۰/۹۸۱۹	۳۵/۱۳	۰/۹۵	–	۴۰/۹۲	۴۴/۱۲	۳۷/۴۹	۴۰/۷۱	۴۴/۱۲	۲۷/۰۱	۰/۹۰
Barbara	۴۱/۳۱	۰/۹۹۵۳	۴۵/۳۰	۰/۹۸۹۰	–	–	–	۴۰/۹۴	۴۳/۶۷	–	–	۴۳/۶۷	–	–
Lena	۴۲/۱۸	۰/۹۹۸۴	۴۶/۴۰	۰/۹۸۵۲	۳۵/۰۲	۰/۷۸	۴۴/۲۲	۴۰/۹۵	۴۳/۸۸	۳۷/۵۹	۴۰/۷۳	۴۳/۸۸	۳۴/۶۷	۰/۹۵
Pepper	۴۲/۰۲	۰/۹۹۸۵	۴۶/۶۳	۰/۹۸۵۸	–	–	–	۴۰/۹۲	–	–	–	–	۳۴/۵۱	۰/۹۵
Santiago	۳۵/۰۹	۰/۹۸۸۵	۴۰/۱۶	۰/۹۸۴۷	–	–	–	–	–	–	–	–	–	–
Lake	۴۰/۰۰	۰/۹۹۴۷	۴۴/۲۹	۰/۹۸۵۷	–	–	–	۴۰/۹۴	–	–	۴۰/۵۸	–	–	–
F16	۴۱/۶۸	۰/۹۷۹۵	۴۶/۰۵	۰/۹۸۲۶	۳۵/۱۶	۰/۸۶	–	–	–	–	۴۰/۸۶	–	۳۲/۸۱	۰/۹۱
Elaine	–	–	۴۵/۴۱	۰/۹۸۱۶	–	–	۴۴/۱۷	–	۳۷/۴۹	–	–	–	۳۴/۷۹	۰/۹۳
میانگین	۳۹/۶۶	۰/۹۹۲۱	۴۴/۳۴	۰/۹۸۴۶	۳۵/۱۰	۰/۸۶	۴۴/۱۹	۴۰/۹۳	۴۳/۸۹	۳۷/۵۲	۴۰/۷۲	۴۳/۸۹	۳۲/۷۵	۰/۹۲
انحراف معیار	۳/۱۱	۰/۰۰۶۸	۲/۵۹	۰/۰۰۲۵	۰/۰۷	۰/۰۸	۰/۰۳	۰/۰۱	۰/۲۲	۰/۰۵	۰/۱۱	۰/۲۲	۳/۳۱	۰/۰۲

جدول ۳: مقایسه نشانه جاسازی و استخراج‌شده تحت حملات مختلف، بدون دستکاری (تصویر خاکستری)

حمله	بهبود تباین					فیلتر گاوسی۳×۳، $\sigma = ۰/۷$					تیزکردن با گاوسی $\sigma = ۵$				
تصویر	*PSNR*	*SSIM*	*NC*	*BER*	*Fa*	*PSNR*	*SSIM*	*NC*	*BER*	*Fa*	*PSNR*	*SSIM*	*NC*	*BER*	*Fa*
Baboon	۱۷/۵۴	۰/۷۹	۰/۸۴	۰/۰۸	۸۴	۳۱/۷۳	۰/۹۵	۰/۸۰	۰/۰۷	۲۰۴	۲۰/۵۰	۰/۸۲	۰/۹۲	۰/۰۳	۵
Barbara	۱۷/۸۸	۰/۸۴	۰/۹۰	۰/۰۴	۱۵	۳۳/۶۶	۰/۹۶	۰/۹۲	۰/۰۳	۴	۲۲/۸۷	۰/۸۵	۰/۹۱	۰/۰۱	۲
Lena	۱۹/۰۲	۰/۸۵	۰/۹۴	۰/۰۲	۰	۳۹/۴۲	۰/۹۶	۰/۹۳	۰/۰۳	۰	۲۵/۲۲	۰/۸۴	۰/۹۶	۰/۰۱	۰
Pepper	۲۰/۷۰	۰/۸۸	۰/۹۲	۰/۰۳	۱۴	۳۹/۰۷	۰/۹۶	۰/۹۴	۰/۰۲	۰	۲۵/۵۱	۰/۸۵	۰/۹۵	۰/۰۲	۰
Santiago	۱۵/۸۳	۰/۷۶	۰/۸۷	۰/۰۶	۴۴	۳۱/۶۰	۰/۹۶	۰/۸۹	۰/۰۵	۸	۱۹/۵۹	۰/۸۱	۰/۹۲	۰/۰۱	۱
Lake	۲۴/۵۱	۰/۸۵	۰/۹۱	۰/۰۳	۱۴	۳۷/۲۷	۰/۹۶	۰/۹۰	۰/۰۴	۳	۲۲/۳۵	۰/۸۳	۰/۹۲	۰/۰۳	۰
F16	۱۱/۷۵	۰/۵۰	۰/۸۹	۰/۰۴	۲۱	۳۹/۴۸	۰/۹۷	۰/۹۱	۰/۰۴	۰	۲۳/۵۵	۰/۸۶	۰/۹۴	۰/۰۲	۰
Elaine	۱۸/۲۶	۰/۷۹	۰/۹۴	۰/۰۲	۰	۳۷/۹۰	۰/۹۴	۰/۹۳	۰/۰۳	۰	۲۶/۷۶	۰/۸۵	۰/۹۷	۰/۰۱	۰

جدول ۴: مقایسه نشانه جاسازی و استخراج‌شده تحت حملات مختلف، بدون دستکاری (تصویر خاکستری)

حمله	نمک-فلفل چگالی ۰/۰۵					JPEG (۶۰)					JPEG (۵۰)				
تصویر	*PSNR*	*SSIM*	*NC*	*BER*	*Fa*	*PSNR*	*SSIM*	*NC*	*BER*	*Fa*	*PSNR*	*SSIM*	*NC*	*BER*	*Fa*
Baboon	۱۹/۶۱	۰/۶۰	۰/۶۹	۰/۱۵	۵۱	۳۷/۶۲	۰/۹۷	۰/۷۹	۰/۰۹	۷۴	۳۴/۷۴	۰/۹۶	۰/۵۶	/۲۱	۸۵۳
Barbara	۱۹/۴۰	۰/۴۸	۰/۷۲	۰/۱۳	۰	۳۹/۹۱	۰/۹۷	۰/۸۱	۰/۰۹	۸	۳۷/۸۴	۰/۹۵	۰/۶۵	۰/۱۷	۲۰۹
Lena	۱۹/۳۴	۰/۴۱	۰/۷۳	۰/۱۳	۰	۳۹/۳۲	۰/۹۵	۰/۸۴	۰/۰۷	۵	۳۷/۵۴	۰/۹۳	۰/۶۸	۰/۱۵	۵۴۴
Pepper	۱۹/۱۷	۰/۴۰	۰/۷۳	۰/۱۳	۰	۳۸/۵۸	۰/۹۴	۰/۸۴	۰/۰۷	۰	۳۶/۸۹	۰/۹۱	۰/۶۶	۰/۱۶	۴۱۲
Santiago	۱۹/۴۲	۰/۶۶	۰/۶۷	۰/۱۶	۴۹	۳۷/۴۲	۰/۹۸	۰/۷۵	۰/۱۲	۵	۳۴/۴۴	۰/۹۷	۰/۵۸	۰/۲۰	۵۲۸
Lake	۱۸/۹۷	۰/۴۹	۰/۶۹	۰/۱۵	۷۱	۳۸/۱۱	۰/۹۵	۰/۷۶	۰/۱۱	۴	۳۵/۹۹	۰/۹۳	۰/۵۹	۰/۲۰	۹۳۹
F16	۱۸/۸۲	۰/۴۳	۰/۷۲	۰/۱۳	۰	۴۱/۰۰	۰/۹۶	۰/۸۰	۰/۰۹	۳۱	۳۹/۱۳	۰/۹۵	۰/۶۲	۰/۱۸	۵۱۹
Elaine	۱۹/۴۴	۰/۴۱	۰/۷۲	۰/۱۳	۱۲	۳۷/۸۷	۰/۹۴	۰/۸۳	۰/۰۸	۰	۳۵/۶۴	۰/۹۰	۰/۶۸	۰/۱۵	۸۴

جدول ۵: مقایسه نشانه جاسازی و استخراج‌شده تحت حملات مختلف، بدون دستکاری (تصویر رنگی)

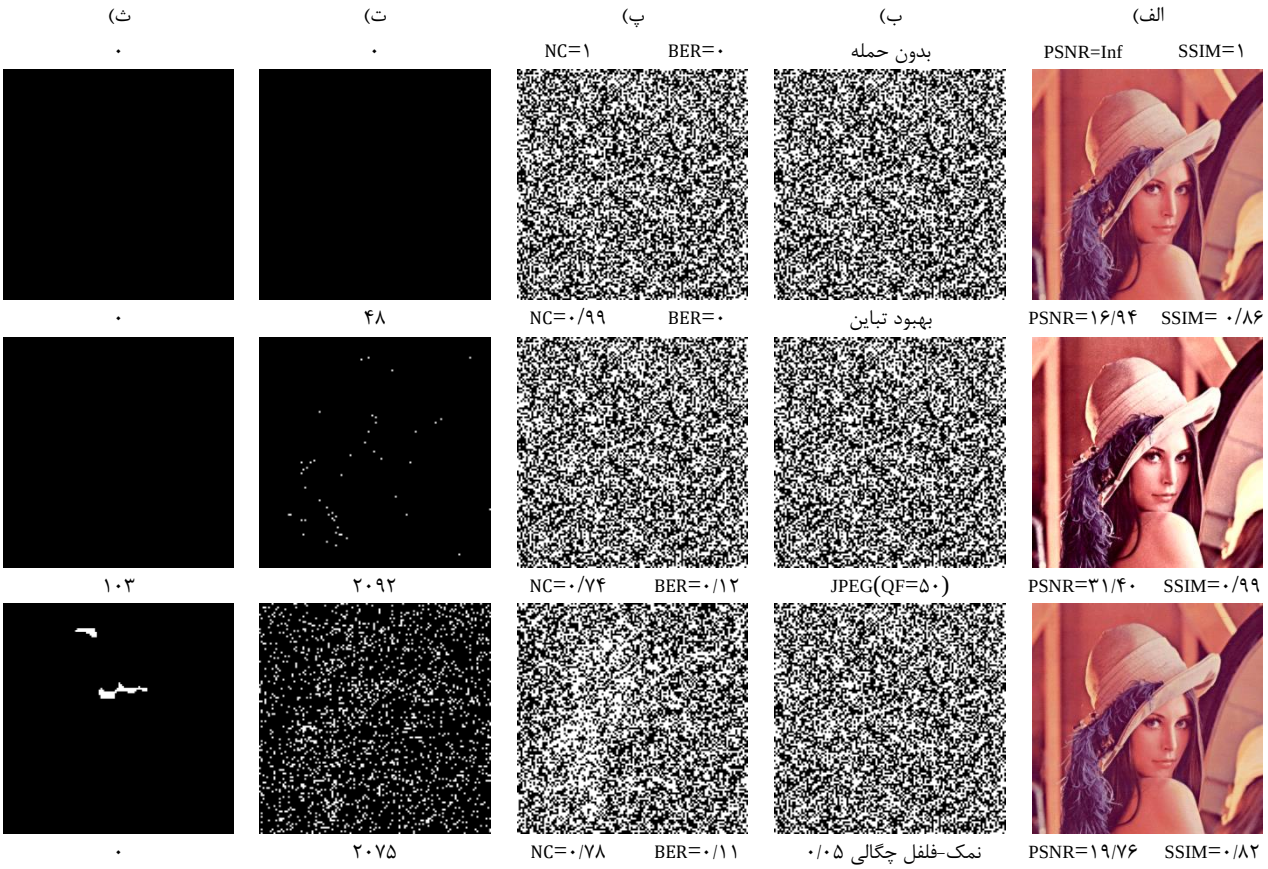
حمله	بهبود تباین					فیلتر گاوسی ۳×۳، $\sigma = ۰/۷$					تیزکردن با گاوسی $\sigma = ۵$				
تصویر	*PSNR*	*SSIM*	*NC*	*BER*	*Fa*	*PSNR*	*SSIM*	*NC*	*BER*	*Fa*	*PSNR*	*SSIM*	*NC*	*BER*	*Fa*
Baboon	۱۵/۷۱	۰/۷۶	۰/۸۵	۰/۰۶	۹۰	۳۰/۲۵	۰/۹۷	۰/۷۷	۰/۰۸	۹۹	۱۶/۱۹	۰/۷۵	۰/۸۵	۰/۰۷	۵۷
Barbara	۱۵/۷۸	۰/۷۷	۰/۹۲	۰/۰۳	۰	۳۲/۱۱	۰/۹۷	۰/۹۴	۰/۰۲	۱۶	۱۸/۱۵	۰/۷۹	۰/۹۴	۰/۰۲	۰
Lena	۱۶/۹۴	۰/۸۶	۰/۹۹	۰/۰۰	۰	۳۲/۶۵	۰/۹۸	۰/۹۴	۰/۰۲	۰	۲۰/۸۳	۰/۹۰	۰/۹۱	۰/۰۴	۰
Pepper	۱۷/۹۳	۰/۸۹	۰/۹۳	۰/۰۳	۰	۳۶/۷۶	۰/۹۹	۰/۹۴	۰/۰۳	۰	۲۰/۸۸	۰/۹۲	۰/۹۴	۰/۰۲	۰
Santiago	۱۴/۵۰	۰/۷۳	۰/۸۵	۰/۰۴	۱۰	۳۰/۱۷	۰/۹۷	۰/۷۵	۰/۰۷	۳۹	۱۵/۴۹	۰/۶۹	۰/۸۲	۰/۰۸	۰
Lake	۲۱/۳۲	۰/۸۷	۰/۸۶	۰/۰۶	۰	۳۷/۰۳	۰/۹۹	۰/۸۸	۰/۰۵	۱۲	۱۸/۳۵	۰/۷۹	۰/۸۸	۰/۰۳	۹
F16	۱۱/۲۶	۰/۴۷	۰/۸۵	۰/۰۵	۳۷	۳۷/۰۹	۰/۹۸	۰/۹۳	۰/۰۳	۰	۱۹/۵۰	۰/۷۳	۰/۹۲	۰/۰۳	۱۴

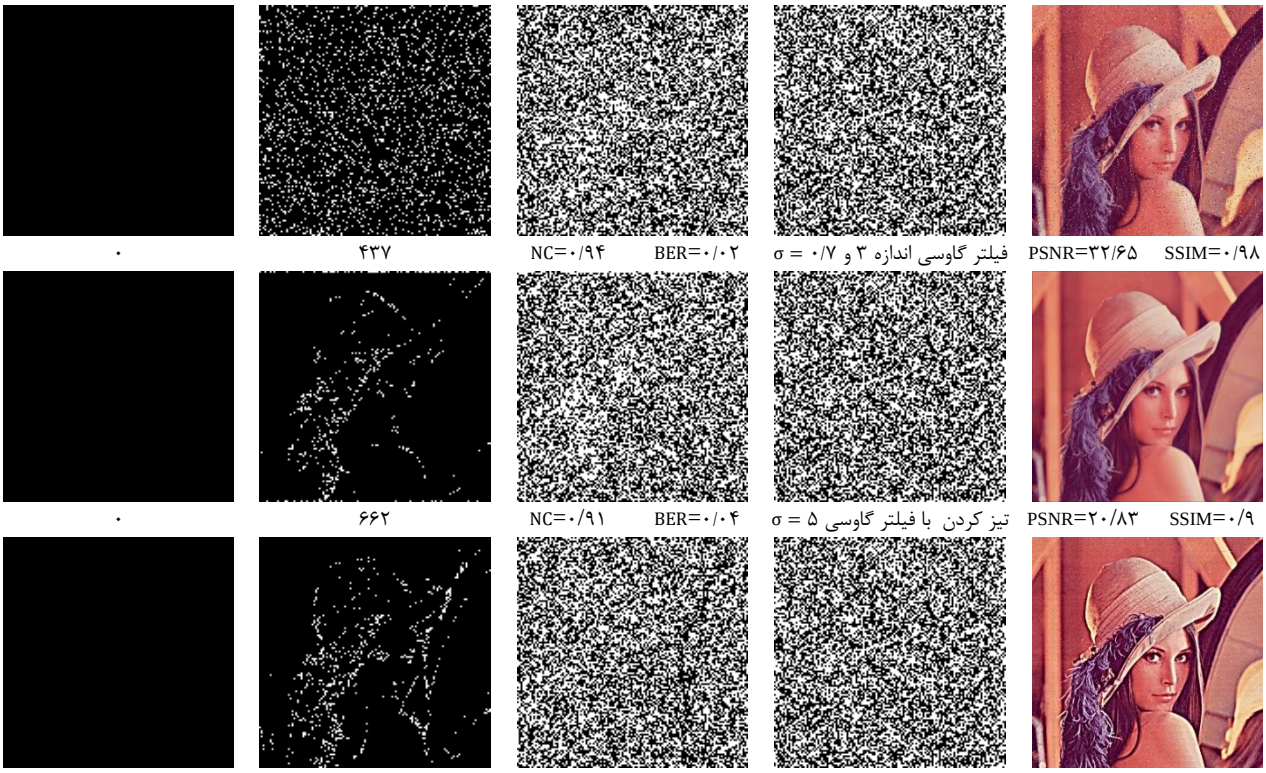
جدول ۶: مقایسه نشانه جاسازی و استخراج‌شده تحت حملات مختلف، بدون دستکاری (تصویر رنگی)

حمله	نمک-فلفل چگالی ۰/۰۵					JPEG (۶۰)					JPEG (۵۰)				
تصویر	*PSNR*	*SSIM*	*NC*	*BER*	*Fa*	*PSNR*	*SSIM*	*NC*	*BER*	*Fa*	*PSNR*	*SSIM*	*NC*	*BER*	*Fa*
Baboon	۱۹/۶۸	۰/۷۸	۰/۷۰	۰/۱۴	۰	۲۹/۶۷	۰/۹۶	۰/۷۹	۰/۱۰	۰	۲۸/۲۸	۰/۹۴	۰/۶۵	۰/۱۷	۲۴۹
Barbara	۱۹/۴۸	۰/۶۹	۰/۷۲	۰/۱۳	۰	۳۵/۲۴	۰/۹۸	۰/۸۹	۰/۰۵	۰	۳۳/۴۴	۰/۹۷	۰/۷۱	۰/۱۴	۱۱۸
Lena	۱۹/۷۶	۰/۸۲	۰/۷۸	۰/۱۱	۰	۳۳/۱۵	۰/۹۹	۰/۸۸	۰/۰۵	۰	۳۱/۴۰	۰/۹۹	۰/۷۴	۰/۱۲	۱۰۳
Pepper	۱۹/۶۳	۰/۸۳	۰/۷۲	۰/۱۳	۱۳	۳۲/۵۵	۰/۹۸	۰/۸۸	۰/۰۵	۰	۳۱/۴۰	۰/۹۸	۰/۷۰	۰/۱۴	۶۳
Santiago	۱۹/۳۶	۰/۷۳	۰/۶۹	۰/۱۵	۸۰	۳۰/۹۵	۰/۹۷	۰/۸۰	۰/۰۹	۰	۳۰/۸۳	۰/۹۶	۰/۶۶	۰/۱۶	۲۸۰
Lake	۱۹/۰۳	۰/۶۹	۰/۷۱	۰/۱۴	۱۵	۳۲/۵۰	۰/۹۶	۰/۸۳	۰/۰۸	۰	۳۱/۰۴	۰/۹۵	۰/۶۶	۰/۱۶	۲۵۲
F16	۱۸/۹۳	۰/۴۹	۰/۷۵	۰/۱۲	۰	۳۵/۶۱	۰/۹۵	۰/۸۵	۰/۰۷	۰	۳۴/۱۴	۰/۹۴	۰/۷۰	۰/۱۴	۵۰۸

۶- جمع بندی

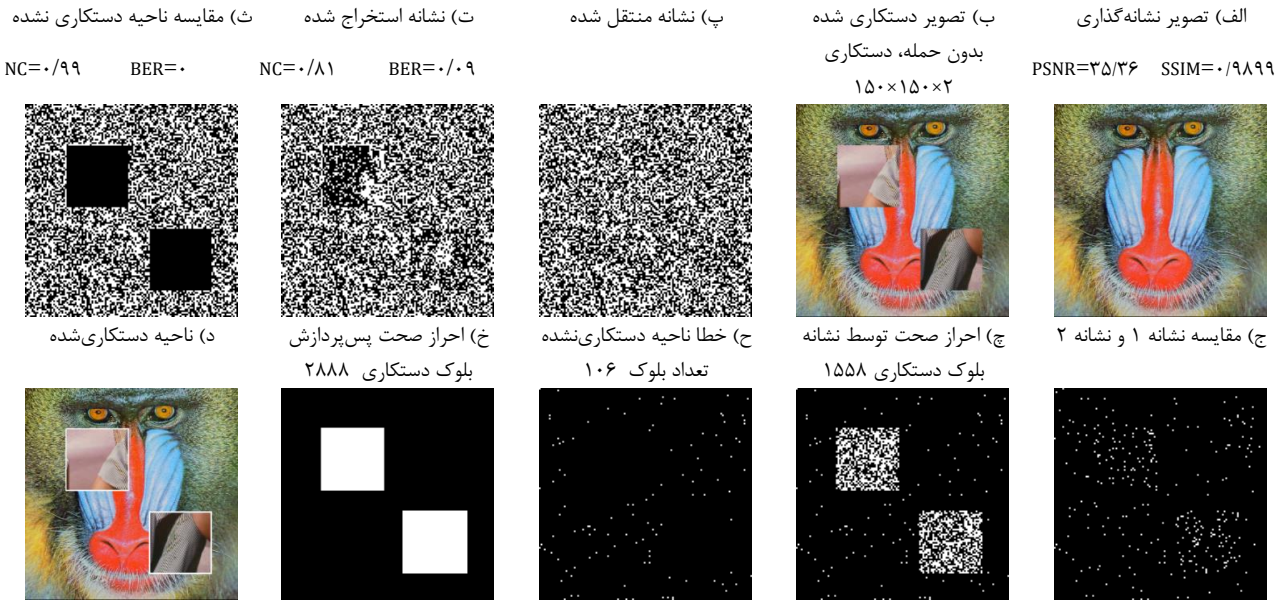
در این مقاله، روشی جدید جهت نشانه‌گذاری نیمه‌بینا و مقاوم در تصاویر رقمی جهت احراز صحت و تشخیص ناحیه دستکاری در تصاویر رنگی و خاکستری ارائه شد. در روش پیشنهادی اطلاعات نشانه در ضرایب فرکانس‌های بالا و به‌عبارتی لبه‌های افقی تبدیل موجک ترفیع صحیح تعبیه شده است و جهت استخراج از الگوریتم یادگیری ماشین، نزدیک‌ترین همسایه استفاده شده است. روش پیشنهادی با حفظ کیفیت تصویر نشانه‌گذاری‌شده، ضعف روش‌های دامنه مکان در برابر حملات فشرده‌سازی و عملیات پایه پردازش تصویر را رفع می‌کند و دقت بالایی در تشخیص ناحیه دستکاری در هنگام وقوع حمله فراهم می‌کند؛ به‌ویژه هنگامی که ناحیه دستکاری بزرگ است. این روش به‌دلیل، بهره‌گیری از تنها یک بیت برای شناسایی ناحیه دستکاری ۴×۴ و همچنین سه کلید مخفی برای استخراج و عدم نیاز به وجود تصویر اصلی، ایمن و کارا است. روش پیشنهادی در مقایسه با سایر روش‌های تشخیص دستکاری به‌دلیل کاهش نرخ اشتباه در شناسایی ناحیه تخریب در هنگام فشرده‌سازی با ضریب پایین و مقاومت بالا در برابر حملاتی مثل بهبود تباین، عملیات پایه پردازش تصویر برتری مطلق دارد؛ علاوه‌براین به‌دلیل استفاده از نشانه تصادفی، مقاومت در برابر حمله رونوشت مکان را فراهم کرده است.





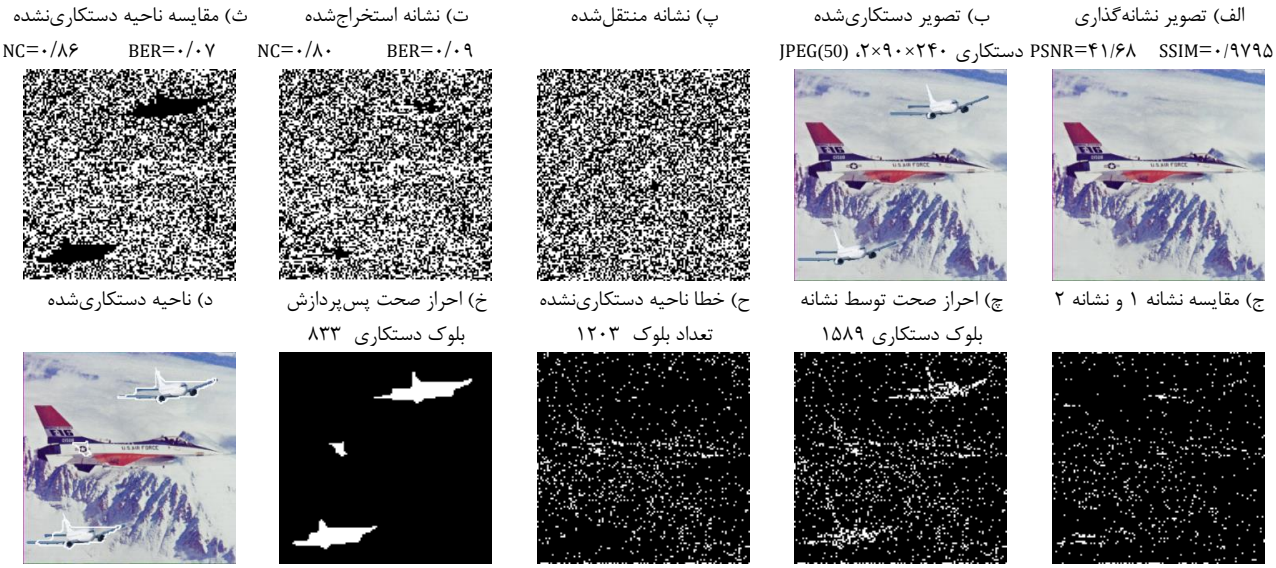
شکل ۹: مقاومت نشانه استخراج‌شده در برابر حملات مختلف

الف) تصویر نشانه‌گذاری ب) نشانه منتقل‌شده پ) نشانه استخراج‌شده ت) احراز صحت به کمک نشانه ث) احراز صحت پس‌پردازش

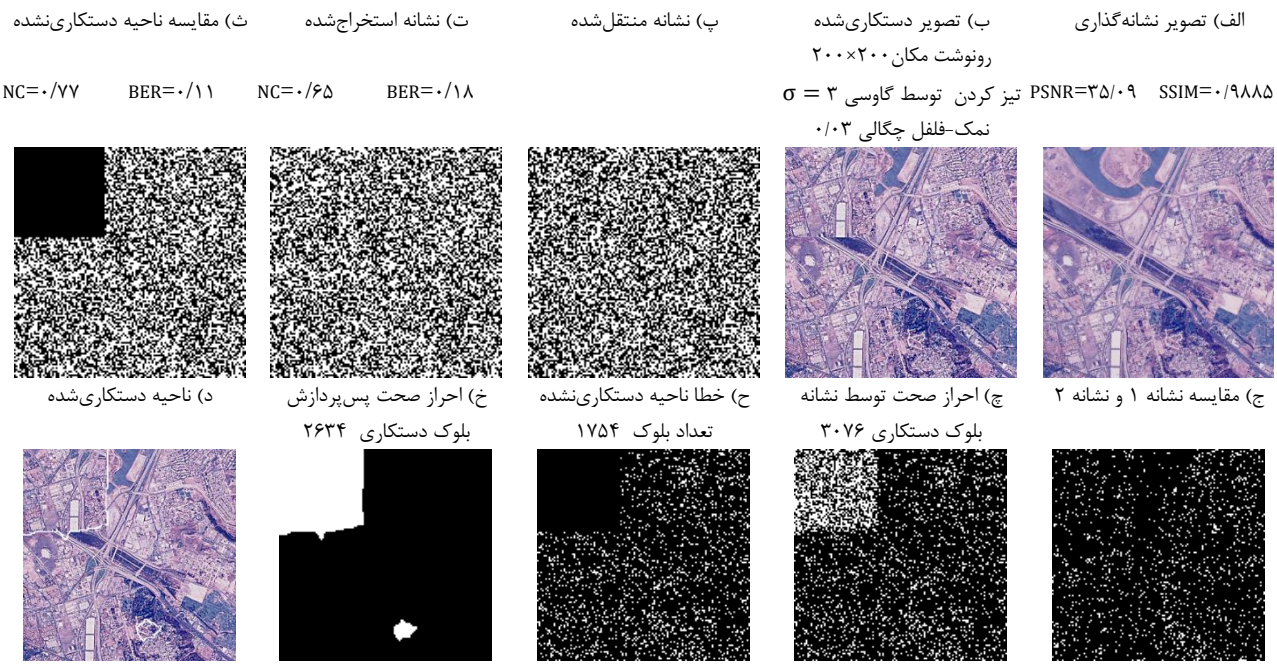


شکل ۱۰: نتایج نشانه‌گذاری، تشخیص و احراز صحت، تصویر *Baboon*

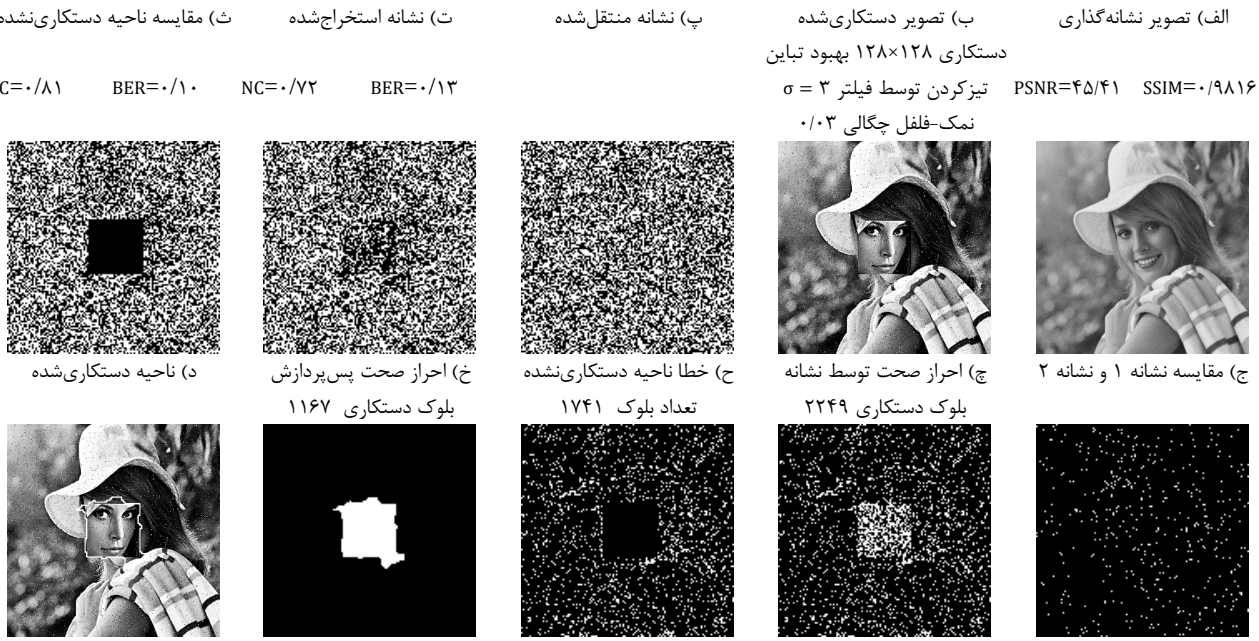
شکل ۱۱: نتایج نشانه‌گذاری، تشخیص و احراز صحت، تصویر *Lena*



شکل ۱۲: نتایج نشانه‌گذاری، تشخیص و احراز صحت، تصویر *F16*



شکل ۱۳: نتایج نشانه‌گذاری، تشخیص و احراز صحت، تصویر *Santiago*



شکل ۱۴: نتایج نشانه‌گذاری، تشخیص و احراز صحت، تصویر *Elaine*

بر اساس مزیت‌های که در بالا اشاره شد، روش ارائه‌شده، روشی مؤثر، ایمن و کارآمد برای تشخیص نواحی دستکاری در تصاویر رنگی و خاکستری می‌باشد.

کارهای آینده- با وجود ویژگی‌ها و توانایی‌های مثبت روش پیشنهادی، ازجمله مقاومت در برابر حملات فشرده‌سازی، نویز نمک-فلفل، بهبود تباین، فیلتر گاوسی، تیزکردن، رونوشت مکان و سایر عملیات پایه پردازش تصویر، متأسفانه روش پیشنهادی در برابر حملات هندسی شکننده است. مطالعات بعدی اختصاص به بهبود مقاومت روش در مقابل حملات هندسی و توانایی بازسازی ناحیه دستکاری‌شده دارد.

مراجع

[1] Kushwah, V. R. Singh, S. Tiwari and M. Gautam, “A review study on digital watermarking techniques,” *Futuristic Trends in Engineering, Science, Humanities*, and Technology FTESHT, vol. 16, no. 166, 2016.

[۲] بهروز بلوریان حقیقی، امیرحسین طاهری‌نیا، «روش واترمارکینگ نیمه‌شکننده مبتنی بر تبدیل کسینوس گسسته جهت تشخیص و بازسازی دستکاری در تصویر»، *مجله پردازش سیگنال پیشرفته دانشگاه تبریز*، جلد ۱، شماره ۱، صفحات ۳۵-۴۶، ۱۳۹۵.

[3] S. Prabhishek and R. S. Chadha, “A survey of digital watermarking techniques, applications and attacks,” *Internation-al Journal of Engineering and Innovative Technology (IJEIT)*, no. 9, 2013.

[4] C. S. Hsu and S. F. Tu, “Image tamper detection and recovery using adaptive embedding rules,” *Measurement*, vol. 88, 2016.

[5] C. S. Hsu and S. F. Tu, “Probability-based tampering detection scheme for digital images”, *Opt Commun.*, vol. 283, no. 9, 2010.

[6] Q. Song and H. Zhang, “Image tamper detection and recovery using dual watermark,” *6th International Conference on Wireless Communications Networking and Mobile Computing (WiCOM)*, Chengdu, 2010.

[7] C. C. Chang, K. N. Chen, Z. H. Wang, M. C. Li, “A quadratic-residue-based fragile watermarking scheme,” *in Proc. Of the 2009 ISECS Int. Conf. On Computing, Communication, Control, and Management*, Sanya, pp. 512–515, China, 2009.

[8] D. Zhang, Z. Pan and H. Li, “A contour based semi fragile image watermarking algorithm in DWT domain,” *in Proc. of the Second Int. Workshop on Education Technology and Computer Science*, Wuhan, China, pp. 228–231, vol. 3, 2010.

[9] P. L. Lin, C. K. Hsieh and P. W. Huang, “A hierarchical digital watermarking method for image tamper detection and recovery,” *Pattern Recognition*, vol. 38, no. 12, 2005.

[10] T. Y. Lee and S. D. Lin. “Dual watermark for image tamper detection and recovery,” *Pattern recognition*, vol. 41, no. 11, 2008.

[11] S. Shivani, D. Singh and S. Agarwal, “Dct based approach for tampered image detection and recovery using block wise fragile watermarking,” *Pattern Recognition and Image Analysis*, Springer, pp. 640–647, 2013.

[12] D. Singh, S. Shivani and S. Agarwal, “Quantization-based fragile watermarking using block-wise authentication and pixel-wise recovery scheme for tampered image,” *Int. J. Image Graph*, vol. 13, no. 2, 2013.

[13] Z. Qian, G. Feng, X. Zhang and S. Wang, “Image self-embedding with high-quality restoration capability,” *Digital Signal Process.*, vol. 21, no. 2, 2011.

[14] C. Dong, Y. W. Chen, J. Li and Y. Bai, “Zero watermarking for medical images based on DFT and LFSR,” *Computer Science and Automation Engineering (CSAE)*, 2012 IEEE International Conference on, vol. 1, 2012.

[15] Q. Qin, W. Wang, S. Chen, D. Chen and W. Fu, “Research of digital semi-fragile watermarking of remote sensing image based on wavelet analysis,” *in Proc. IEEE International Symposium on Geo science and Remote Sensing, Anchorage*, Alaska, USA, pp. 2542–2545, 2004.

[16] C.M. Wu, Y.C. Hu, K.Y. Liu and J.C. Chuang, “A novel active image authentication scheme for block truncation

coding," *Int. J. Signal Process. Image Process. Pattern Recogn*, vol. 7, no. 5, 2014.

[17] W. C. Wu and Z. W. Lin, "An image content protection and tampering localization scheme using singular values," *International Scientific Conference on Engineering and Applied Sciences*, Okinawa Japan, pp. 238–247, July 2015.

[18] L. Laouamer, M. AlShaikhb, L. Nana and A. Chrisitine Pascu, "Robust watermarking scheme and tamper detection based on threshold versus intensity," *Journal of Innovation in Digital Ecosystems*, vol. 2, no. 1, 2015.

[19] A. Phadikar, P. Maity and M. Mandal, "Novel wavelet-based QIM data hiding technique for tamper detection and correction of digital images," *Journal of Visual Communication and Image Representation*, vol.23, no. 12, 2012.

[20] S. Dadkhah, A. A. Manafb, Y. Horic, A. E. Hassaniend and S. Sadeghie, "An effective svd-based image tampering detection and self-recovery using active watermarking," *Signal Processing Image Communication*, vol. 29, no. 10, 2014.

[21] Y. Zheng, R. Wang and J. LI, "Nonlinear wavelet and bp neural networks adaptive lifting scheme," *IEEE International Conference on Apperceiving Computing and Intelligence Analysis (ICACIA)*, pp. 316–319, 2010.

[22] C. S. Hsu and S. F. Tu, "Image tamper detection and recovery using adaptive embedding rules," *Measurement*, vol. 88, 2016.

[23] D. Singh and K. Singh, "Effective self-embe-dding watermarking scheme for image tampered detection and localization with recovery capability," *Journal of Visual Communication and Image Representation*, vol. 38, 2016.

[24] X. Tong, Y. Liu, M. Zhang and Y. Chen, "A novel chaos-based fragile watermarking for image tampering detection and self-recovery," *Signal Processing: Image Communication*, vol. 28, no. 3, 2013.

[25] M. J. Barani, M. Yousefi and P. Ayubi, "A secure watermark embedding approach based on chaotic map for image tamper detection," *7th Conference on Information and Knowledge Technology (IKT)*, 2015.

[26] O. Benrhouma, H. Hermassi and S. Belghith, "Tamper detection and self-recovery scheme by dwt watermarking," *Nonlinear Dynamics*, vol. 79, no.3, 2014.

[۲۷] رضا خدایی، محمدعلی بالافر، «اثربخشی بسط پرس‌وجو مبتنی بر خوشه‌بندی اسناد شبه‌بازخورد با الگوریتم K-NN»، *مجله مهندسی برق دانشگاه تبریز*، جلد ۴۶، شماره ۱، صفحات ۱۴۳-۱۵۱، ۱۳۹۵.

[۲۸] وحیده منعمی‌زاده، جواد حمیدزاده، «جستجوی k نزدیک‌ترین همسایه تقریبی با روش ترکیب خطی»، *مجله مهندسی برق دانشگاه تبریز*، جلد ۴۷، شماره ۲، ۱۳۹۶.

[29] R. P. Singh, N. Dabas, V. Chaudhary and Nagendra, "Online sequential extreme learning machine for watermarking in dwt domain", *Neurocomputing*, vol. 174, 2016.

[30] A. Mishra, A. Goel, R. Singh and G. Chetty, "A novel image watermarking using extreme learning machine," *International Joint Conference on Neural Networks (IJCNN)*, pp. 1–6, 2012.

زیرنویس‌ها

[1] Robust
[2] Fragile
[3] Semi-Fragile
[4] Data Payload
[5] Non-Blind
[6] Blind
[7] Semi-Blind
[8] Contrast
[9] Image Splicing
[10] Copy-Move
[11] Halftone
[12] Chaotic Map
[13] Logistic Map
[14] Cross Map
[15] Luminance
[16] Kurtosis
[17] Skewness
[18] Entropy
[19] Normalized Correlation
[20] Bit Error Ratio