ارائه یک روش واترمارکینگ ترکیبی جدید برای تصاویر در دامنه فرکانسی

عطیه زاهد[۱]، احمدرضا نقش نیلچی [۲]
۱- کارشناس ارشد و عضو هیات علمی دانشگاه آزاد اسلامی واحد کاشان، atiya.zahed@gmail.com
۲- استادیار، گروه مهندسی کامپیوتر دانشگاه اصفهان، nilchi@yahoo.com

چکیده

یکی از موضوع‌های مهم در عرصه تجارت الکترونیک، مسئله رعایت قانون حق‌کپی (Copyright) محصولات دیجیتالی است. واترمارکینگ دیجیتالی، یکی از روش‌هایی است که برای حل این مسئله ارائه شده است و نسبت به روش‌هایی مثل رمزنگاری و امضای دیجیتالی، که در حال حاضر برای رفع این مشکل استفاده می‌شوند، از امنیت بیشتری برخوردار است. در این مقاله، تعدادی از روش‌های واترمارکینگ موجود، ازجنبه‌های مختلف مورد بررسی قرار گرفته‌اند. سپس یک روش ترکیبی جدید برای واترمارکینگ تصاویر با فرمت BMP ارائه شده است. این روش واترمارک را در دامنه فرکانسی تصویر با استفاده از دو تبدیل DCT و DWT، جاسازی می‌کند و فرآیند استخراج را بدون استفاده از تصویر اصلی انجام می‌دهد. این روش در برابر حملات JPEG و برش (Cropping) و تغییر اندازه (Scaling) بسیار مقاوم است.

واژه‌های کلیدی

واترمارکینگ، DCT، DWT، حمله JPEG، حمله برش، حمله تغییر اندازه، استخراج کور(Blind)

۱–مقدمه

امروزه با پیشرفت سریع تکنولوژی اطلاعات دیجیتالی، همه دارندگان کامپیوترهای خانگی در کامپیوتر خود، یک پردازشگر چند رسانه‌ای سریع، یک پهنای باند وسیع با قابلیت دسترسی به تمام دنیا و حافظه قابل جابجایی برای اطلاعات دیجیتالی را در اختیار دارند. به همین دلیل اطلاعات دیجیتالی به سهولت در دسترس همگان قرار می‌گیرد و قابل توزیع است. این پیشرفت تکنولوژی اگرچه باعث سهولت بسیاری از کارها گشته، اما مانند دیگر مظاهر تکنولوژی، مشکلاتی را با خود به همراه داشته است. یکی از این مشکلات، توانایی دستکاری، کپی برداری و توزیع غیرقانونی اسناد دیجیتالی، توسط کاربرانی است که از این اسناد استفاده می‌کنند، و چنانچه مسائل امنیتی محصولات دیجیتالی از جمله اسناد چند رسانه‌ای دیجیتالی حل نشود، مالکان این محصولات انگیزه‌ی خود را برای وارد کردن این محصولات در دنیای تجارت الکترونیک از دست خواهند داد[۱]. در حال حاضر از دو روش استاندارد برای حفاظت ازحق کپی اسناد دیجیتالی استفاده می‌شود که عبارتند از: رمزنگاری و امضای دیجیتالی.

نقص بزرگ رمزنگاری، عدم حمایت آن از سندی است که در مرحله بعد از رمزگشایی قرار گرفته و قابل استفاده است. به عبارت بهتر، کاربر بعد از ارائه کلید معرف و رمزگشایی سند، می‌تواند هرنوع تغییری را در سند ایجاد کند و یا از روی آن هر تعداد که می‌خواهد، سند غیر مجاز کپی کند، به این ترتیب مالک سند نمی‌تواند حقوق خود را دنبال کند.

در صورتی که کوچکترین تغییر تصادفی و یا عمدی در سند دیجیتالی که از امضای دیجیتالی برای حفاظت از حق کپی استفاده می‌کند، ایجاد شود، به گونه‌ای که باعث تغییر حتی یک بیت از سند شود، امکان بازیابی امضای دیجیتالی را برای دریافت‌کننده غیرممکن خواهد کرد، در نتیجه اعتبار سند به سهولت از بین خواهد رفت [۲].

مطالعاتی که در این زمینه انجام شده است، نشان می‌دهد تنها راه حلی برای این مشکل مناسب است که بتواند اطلاعات امنیتی را به گونه‌ای به سند اصلی وصل کند که در طول عمر سند از آن جدا نشود و از سوی دیگر تا حد ممکن، این اطلاعات برای کاربر سند غیر قابل درک باشد. یکی از راه‌حل‌های مناسب برای این مسئله،

واترمارکینگ دیجیتالی است. در این روش سیگنال دیجیتالی به یک سند دیجیتالی وصل می‌شود و در تمام طول عمر سند به آن متصل است و برای حذف آن از سند، به سند آسیب جدی وارد می‌شود. این سیگنال می‌تواند شامل اطلاعاتی مثل حق کپی باشد.

واترمارکینگ دیجیتالی در سال ۱۹۵۴ توسط یکی از مهندسین شرکت موزاک (Muzac) بنام امیل همبروک (Emil Hembrook) ابداع شد. در این ابداع یک کد شناسایی به گونه‌ای غیر قابل تشخیص یا به اصطلاح نامرئی، به فایل حاوی موسیقی دیجیتالی وصل می‌شد تا بتواند برای اثبات حق مالکیت به کار برود[۲۶]. از آن زمان به بعد از واترمارکینگ دیجیتالی استفاده‌های فراوانی می‌شد، اما تا سال ۱۹۹۰ به عنوان یک موضوع تحقیقاتی با ارزش، توجه دانشمندان را به خود جلب نکرده بود. از اوایل دهه ۱۹۹۰، این موضوع به عنوان یک موضوع جذاب تحقیقاتی مورد توجه قرار گرفت و تا امروز نیز همچنان جذابیت و اهمیت خود را حفظ کرده است [۳].

درطی دهه گذشته، روش‌های مختلفی برای واترمارکینگ دیجیتالی ارائه شده است. این روش‌ها را از نقطه نظرات گوناگون می‌توان دسته‌بندی کرد. از نقطه نظر نوع سندی که واترمارک می‌شود، چهارنوع سیستم واترمارکینگ وجود دارد: سیستم واترمارکینگ متن [۴]، صوت [۵، ۶]، تصویر[۱۱-۷] و ویدیو [۱۵-۱۲]. از نقطه نظر مرئی بودن واترمارک درون سند، دو نوع روش وجود دارد: روش‌هایی که واترمارک در سند واترمارک شده قابل مشاهده و مرئی است [۱۶،۱۷] و روش‌هایی که دارای واترمارک نامرئی [۱۸،۱۹] می‌باشند. اگر سیستم‌های واترمارکینگ از جنبه مقاومت آنها در برابر حملات مختلف تقسیم‌بندی شوند، سه دسته سیستم واترمارکینگ وجود دارد: سیستم‌های واترمارکینگ مقاوم [۲۰،۲۱]، سیستم‌های واترمارکینگ نیمه مقاوم [۲۲] و سیستم‌های واترمارکینگ شکننده[۲۳].

از این دیدگاه که چه نوع داده‌ای به عنوان واترمارک به سند دیجیتالی وصل می‌شود، این سیستم‌ها به دو دسته تقسیم می‌شوند: واترمارک ازنوع اختلال[۲۴] و واترمارک ازنوع تصویر[۲۵]. از جنبه روش استخراج واترمارک، دو روش استخراج کور (نا آگاه) و استخراج بینا (آگاه) وجود دارد. و در نهایت مهم‌ترین دسته‌بندی مربوط به انواع روش‌های پردازشی (دامنه‌های جاسازی واترمارک) است. از این نظر، سیستم‌های واترمارکینگ به چهار دسته تقسیم می‌شوند: پردازش‌های دامنه مکانی [۲۶]، پردازش‌های دامنه فرکانسی [۲۹-۲۷]، پردازش‌های دامنه فشرده‌سازی [۳۰] و پردازش‌های مرکب یا هیبرید[۳۱-۳۴]. سیستم واترمارکینگی که در این مقاله ارائه می‌شود، یک سیستم واترمارکینگ نامرئی روی تصاویر است. این روش از یک تصویر باینری برای واترمارک استفاده می‌کند و واترمارک را در دامنه مرکب یا هیبرید، جاسازی می‌کند. فرآیند استخراج واترمارک در آن یک فرآیند استخراج کور است، و در برابر حملات JPEG و برش (Cropping) و تغییر اندازه (Scaling)، مقاوم است. در این مقاله، تلاش شده است که تحقیقات و روش‌های ارائه شده در زمینه واترمارکینگ از جنبه روش‌های پردازشی مختلف در اسناد چندرسانه‌ای، بررسی شوند.

سیستم‌هایی که واترمارک را در دامنه مکانی اسناد مخفی می‌کنند، خود به سه روش تقسیم می‌شوند، که این سه روش به ترتیب عبارتند از: روش‌های مبتنی بر (Least Significant Bit) LBS [۲۶]، روش‌های مبتنی بر بلاک و روش‌های آماری و مبتنی بر ویژگی‌های تصویر[۱۱].

اگرچه میزان اطلاعاتی که می‌توان با استفاده از این روش‌ها در سند، مخفی کرد، نسبتاً زیاد است و انحرافاتی که در نتیجه جاسازی این اطلاعات بوجود می‌آید، بسیار کم است، اما در مجموع، روش‌های موجود در این زمینه در برابر حملات پردازش تصویر مثل فشرده سازی با اتلاف و بعضی حمله‌های هندسی مثل برش، بسیار ضعیف هستند و بیشتر در سیستم‌های واترمارکینگ شکننده و پنهان نگاری از این روش‌ها استفاده می‌شود[۲].

به طور معمول DCT (Discrete Cosine Transform)، DFT (Discrete Fourier Transform) و DWT (Discrete Wavelet Transform)، تبدیلاتی هستند که در سیستم‌های واترمارکینگی که پردازش را در دامنه فرکانسی انجام می‌دهند، بکار می‌روند. در این روش‌ها، واترمارک در تمام دامنه دیتای اصلی توزیع می‌شود.

سیستم‌های واترمارکینگی که از دامنه DCT برای جاسازی واترمارک استفاده می‌کنند، نسبت به حملاتی مثل فشرده‌سازی‌های با اتلاف، از جمله JPEG و برخی از حملات هندسی مثل برش مقاوم هستند. این سیستم‌ها با استفاده از DCT، تصویر را به باندهای فرکانسی متفاوتی تفکیک می‌کنند و به این ترتیب واترمارک را در باندهای فرکانسی میانی یک تصویر، جاسازی می‌کنند. روش ارائه شده در [۳۵] یکی از روش‌های به وجود آمده بر پایه DCT است، که در برابر حملات برش و Translation از مقاومت خوبی برخوردار است.

سیستم‌های واترمارکینگ در دامنه DWT، دارای مزایای زیادی هستند، که انطباق بیشتر آن با HVS (سیستم بینایی انسان) نسبت به دیگر دامنه‌های تبدیل، یکی از این مزایاست. این روش باعث می‌شود مقاومت واترمارک افزایش یابد درحالیکه به کیفیت تصویر هم آسیبی نمی‌رساند.

روش‌هایی که براساس تبدیل DFT هستند نیز روش‌های مقاومی هستند. البته بدلیل اینکه اکثر فشرده‌سازی‌هایی که روی اسناد چندرسانه‌ای صورت می‌گیرند از DCT وDWT بهره می‌برند، روش‌های مبتنی بر DFT کمتر مورد استفاده قرار می‌گیرند، زیرا هدف، سازگاری بیشتر سیستم‌های واترمارکینگ با این فشرده‌سازی‌هاست. دامنه دیگری که برای واترمارک کردن از آن استفاده می‌شود، دامنه فشرده‌سازی است. دامنه فشرده‌سازی نمی‌تواند دامنه قابل اعتمادی برای جاسازی واترمارک باشد. زیرا با تغییر نوع فشرده‌سازی یا فشرده‌سازی مجدد با پارامترهای متفاوت، سند دچار تغییراتی می‌گردد که کشف واترمارک را در آن غیرممکن می‌سازد. در روش هیبرید، برای جاسازی واترمارک، از ترکیبی از دامنه‌ها یا روش‌ها استفاده می‌شود.

در این مقاله سعی شده است که با استفاده از تبدیل‌های DCT و DWT، سیستم واترمارکینگ مقاومی طراحی شود تا سیستم واترمارکینگ حاصل، از مزایای هر دو روش بهره‌مند گردد. به این منظور، یک روش واترمارکینگ کور در دامنه فرکانسی ارائه شده که یک تصویر خاکستری (Gray Scale) را واترمارک می‌کند. الگوریتم مورد نظر یک تصویر باینری را درون یک تصویر خاکستری مخفی می‌کند. بدین منظور ابتدا تصویر باینری که همان واترمارک است، توسط کلیدی رمزگذاری می‌شود، این عمل سبب مقاوم‌ترشدن واترمارک در برابر شناسایی و حذف می‌شود. سپس تصویر اصلی به بخش‌های جداگانه‌ای تقسیم شده و هر بخش، جداگانه تحت یکی از تبدل‌های DCT یا DWT قرار می‌گیرد. واترمارک رمز شده نیز به طور جداگانه توسط الگوریتم جاسازی، در هر یک از این قسمت‌ها، مخفی می‌شود. استفاده از هر دو تبدیل DCT و DWT، باعث بهره‌وری از خواص هر دو تبدیل می‌شود و همچنین با این کار می‌توان نقاط ضعفی را که در یکی از این تبدیل‌ها وجود دارد با دیگری جبران نمود. بنابراین روش ارائه شده یک روش ترکیبی یا هیبرید (Hybrid) است.

در الگوریتم جاسازی از روابط بین ضرایب همسایه استفاده می‌شود و واترمارک در بین ضرایب میانی مخفی می‌شود. می‌توان برای مقاوم‌ترکردن واترمارک، ضرایب میانی را بر اساس اعداد تصادفی انتخاب کرد. پس از عملیات جاسازی عکس عملیات تبدیل انجام می‌شود و دوباره بخش‌های مختلف تصویر کنار یکدیگر قرار می‌گیرند و تصویر واترمارک شده را بوجود می‌آورند. تغییراتی که سیستم واترمارکینگ موجود روی تصویر بوجود می‌آورد، توسط چشم انسان غیر قابل رویت است. یکی از مزایای مهم این روش، استخراج کور واترمارک از تصویر واترمارک شده است. به این ترتیب برای استخراج واترمارک در طول فرآیند استخراج، نیازی به تصویر اصلی و مقایسه آن با تصویر واترمارک شده نیست. این مزیت باعث کمتر شدن بار محاسباتی سیستم واترمارکینگ می‌شود. همچنین بدلیل کور بودن، می‌توان از این روش در واترمارکینگ ویدیویی استفاده کرد، زیرا حذف یا اضافه شدن فریم‌های ویدیو یا جابجایی آنها نمی‌تواند در فرآیند استخراج مشکلی به وجود آورد.

در فرآیند استخراج، همانند فرآیند جاسازی، تصویر دریافتی به چندین بخش تقسیم شده و از هر بخش به طور جداگانه تبدیل DCT یا DWT گرفته می‌شود، آنگاه طبق روابط موجود بین ضرایب میانی با ضرایب همسایه، اطلاعات مخفی شده استخراج می‌شود. ضرایب میانی‌ای که مورد بررسی قرار می‌گیرند می‌توانند ضرایب ثابتی باشند یا اینکه توسط اعداد تصادفی انتخاب شوند.

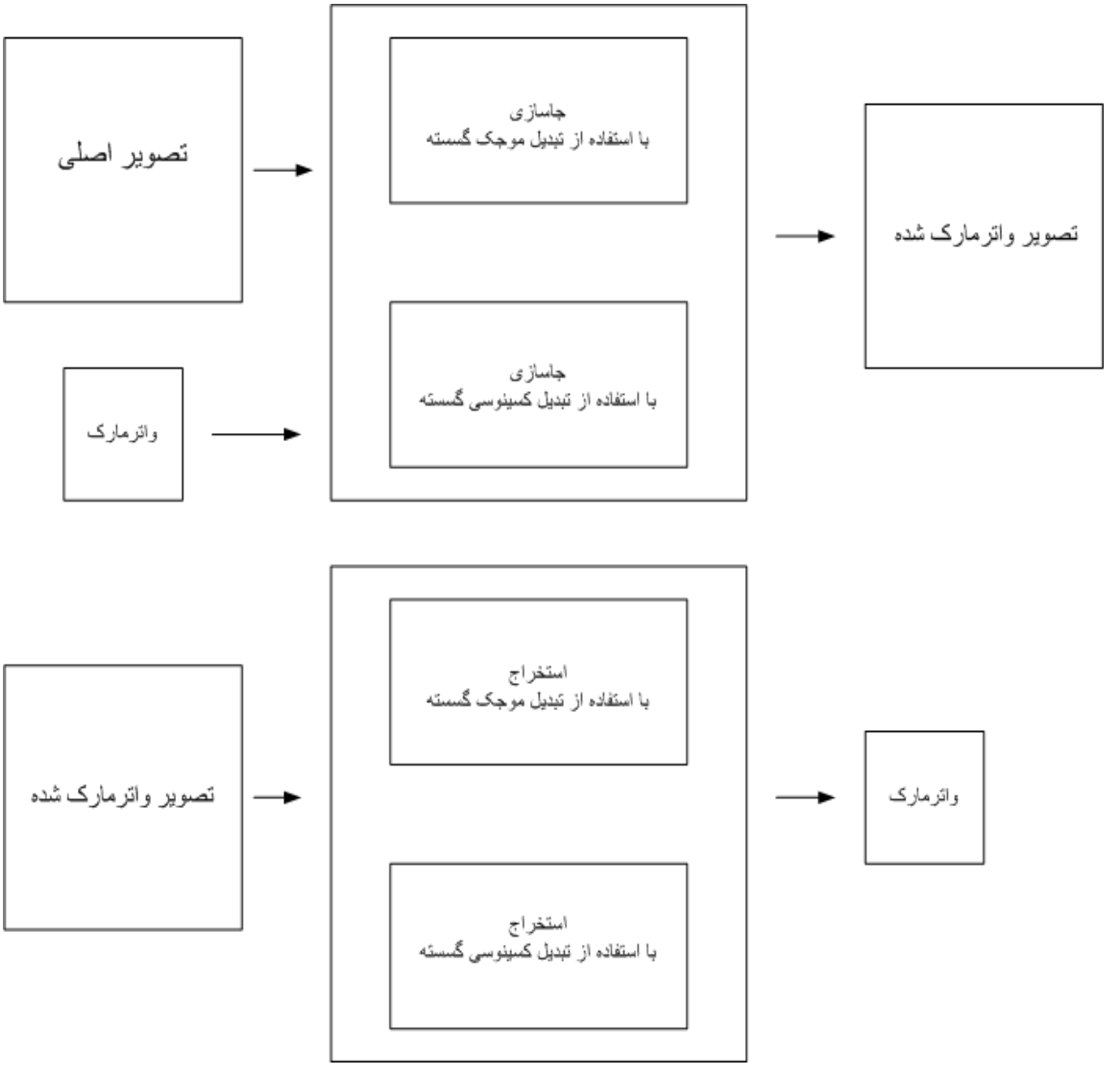
این مقاله دارای سه بخش دیگر است. در بخش دوم روش واترمارکینگ پیشنهادی به‌طورکامل توضیح داده شده است. در بخش سوم نتایجی که از پیاده سازی این روش بدست آمده و همچنین اثرحمله‌های مختلف در این روش مورد بررسی قرار گرفته‌اند و در فصل چهارم کارهای مهم انجام شده درتحقیق، بار دیگر به صورت خلاصه ذکرمی‌گردد و نتایج بدست آمده توضیح داده می‌شود. در پایان، نتیجه‌گیری و نکات مبهم و قابل پژوهش در آینده، ذکر می‌گردند.

۲ – معرفی روش ارائه شده

از آنجا که روش ارائه شده یک روش ترکیبی یا هیبرید می‌باشد، در فرآیند جاسازی از دو الگوریتم مختلف استفاده می‌شود. تصویر اصلی بنابر روشی خاص به چند قسمت تقسیم شده و در هر قسمت بخشی از واترمارک به یکی از دو روش موجود جاسازی می‌شود. یکی از این الگوریتم‌ها واترمارک مورد نظر که یک تصویر باینری می‌باشد، در دامنه فرکانسی تصویر با استفاده از تبدیل موجک گسسته و دیگری با استفاده از تبدیل کسینوسی گسسته، جاسازی می‌کند. شکل (۱) بلاک دیاگرام کلی این سیستم واترمارکینگ را نشان می‌دهد که شامل دو بخش جاسازی و استخراج است.

۲–۱– جاسازی در دامنه فرکانسی با استفاده از تبدیل موجک گسسته (DWT)

بخشی از تصویر (IO1) (صرفاً برای نام گذاری از حروف به اختصار استفاده می‌شود و این اختصارات معنای دیگری ندارند) به عنوان سندی که باید واترمارک شود و بخشی از واترمارک (W1) به‌عنوان واترمارک وارد می‌شوند، ورودی الگوریتم جاسازی هستند. در ابتدا تصویر ورودی به بلاک‌های ۶۴×۶۴ تقسیم می‌شود



شکل ۱ - بلاک دیاگرام کلی سیستم واترمارکینگ پیشنهادی

اگر هر یک از این بلاک‌ها BIO1 نامیده شوند، هر BIO1 در ۴ سطح تحت تبدیل موجک گسسته قرار می‌گیرند. برای جاسازی واترمارک از بین ناحیه‌های موجود در ماتریس ضرایب حاصل (VBIO1)، نواحی HL، LH انتخاب می‌کنیم. (LHi,HLi; i=1,2,3,4)(شکل(۲)). در هریک از این نواحی یک یا چند ضریب بر اساس اعداد شبه تصادفی و یا با استفاده از روش ارائه شده در [۳۵] انتخاب می‌شود. با توجه به بیت مورد نظر برای جاسازی عملیات زیر انجام می‌شود:

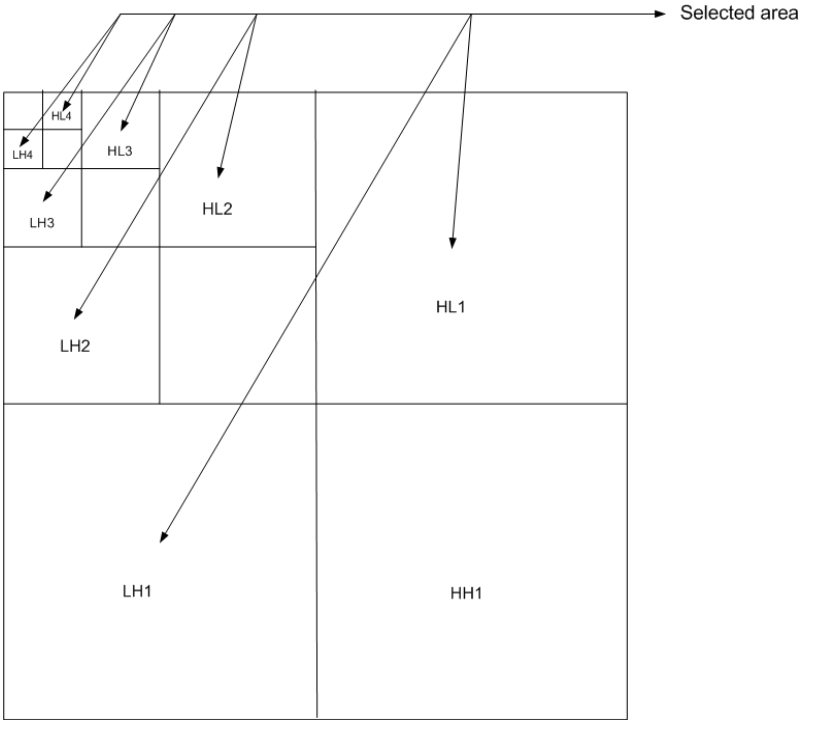
IF W1j=0 THEN

Cki=MIN(Ci+1,Ci+2,Ci+3,Ci+4,Ci+5)

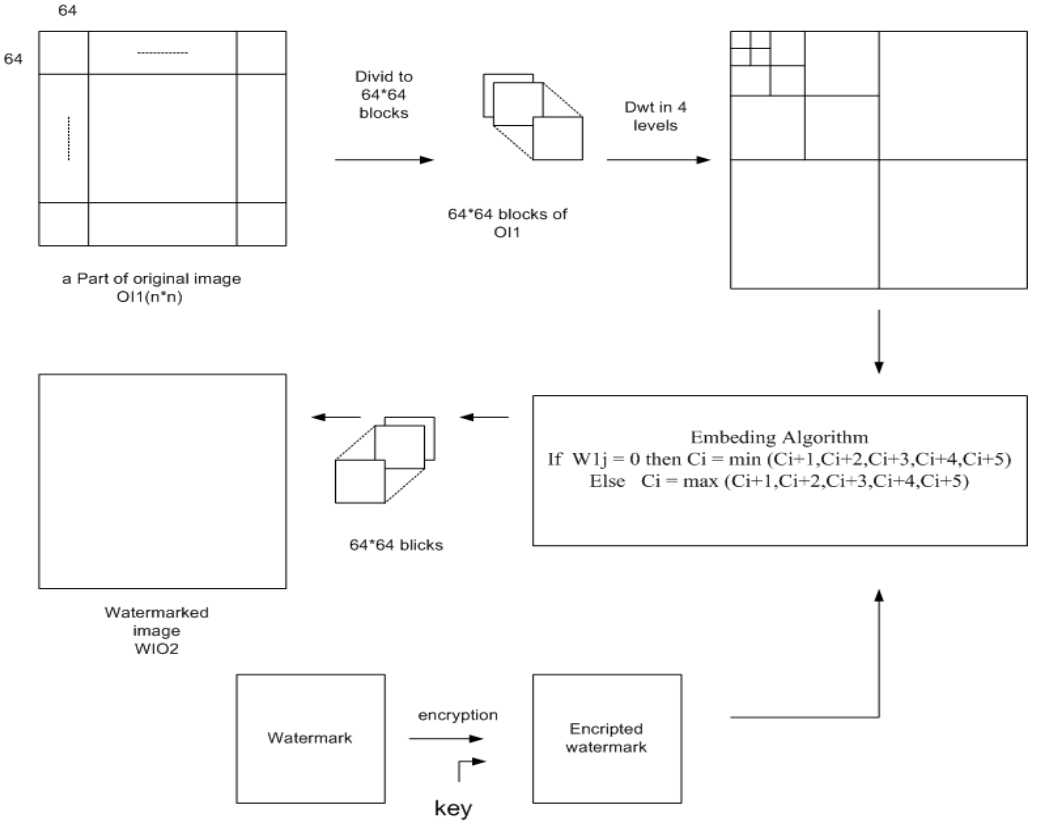
ELSE

Cki=MAX(Ci+1,Ci+2,Ci+3,Ci+4,Ci+5)

که Wj، j امین بیت واترمارک و Ck، k امین ضریب انتخاب شده برای جاسازی می‌باشد. پس از جاسازی واترمارک در ماتریس ضرایب VBIO1 این ماتریس در چهار سطح تحت تبدیل معکوس موجک گسسته (IDWT) قرار می‌گیرد. پس از انجام کلیه این مراحل روی بلاک‌های ۶۴×۶۴ آنها به ترتیب اولیه کنار هم قرار می‌گیرند، که حاصل تصویر واترمارک شده‌ای به نام WIO1 خواهد بود. شکل(۳) بلاک دیاگرام الگوریتم را به طور کامل نمایش می‌دهد.



شکل ۲ - نواحی انتخابی برای جاسازی



شکل ۳ - بلاک دیاگرام جاسازی در دامنه فرکانسی با استفاده از تبدیل DWT

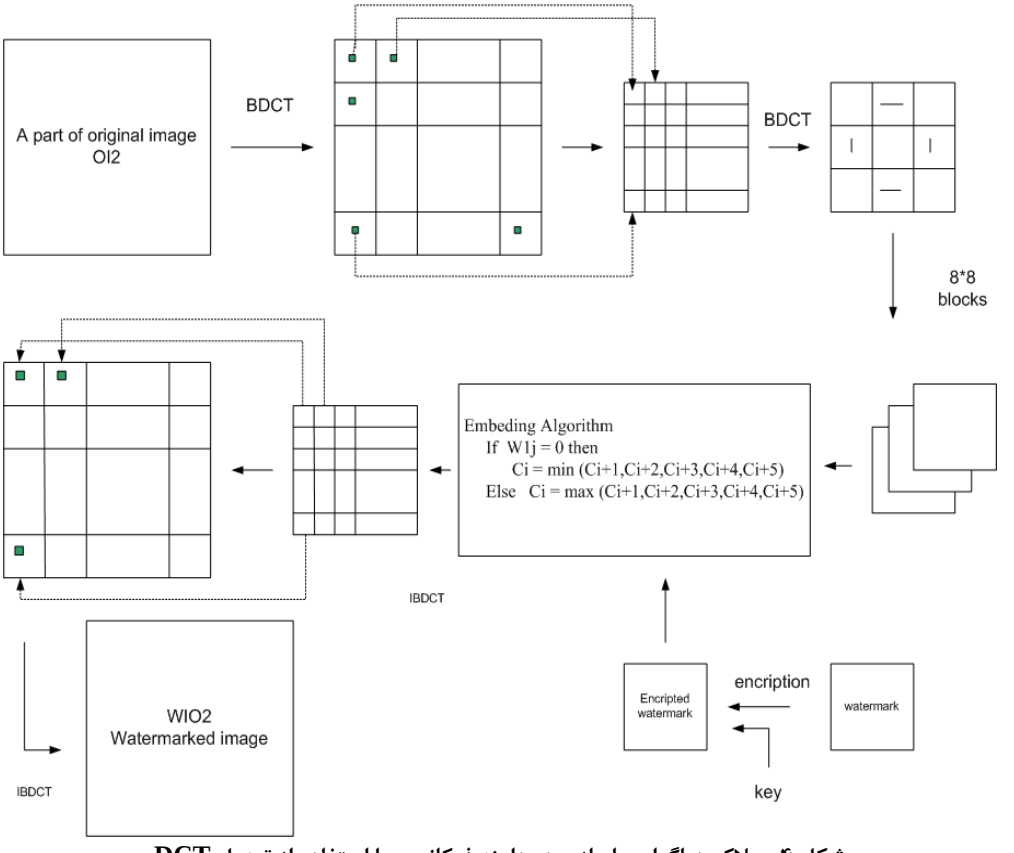
۲-۲- الگوریتم جاسازی در دامنه فرکانسی با استفاده از تبدیل کسینوسی گسسته (DCT)

در این قسمت بخشی از تصویر (IO2) به عنوان سندی که باید واترمارک شود و بخشی از واترمارک (W2) به عنوان واترمارک وارد می‌شوند. IO2 تحت تبدیل BDCT قرار می‌گیرد (تبدیل کسینوسی گسسته تحت بلاک‌های ۸×۸). سپس با استفاده از اعداد تصادفی سودو، یکی از ضرایب میانی بلاک‌های ۸×۸، از ماتریس ضرایب حاصل(DIO2) انتخاب می‌شوند. با استفاده از این ضرایب انتخاب شده، یک ماتریس کوچکتر که ابعادش نسبت به DIO2، ۱/۸ است، تشکیل می‌شود. که هر درایه آن یکی از ضرایب انتخابی از بلاک‌های DIO2 است و در جایگاه متناسب با بلاک متناظرش در DIO2 قرار دارد. از این ماتریس (RDIO2) که خود ضرایب DCT یک ماتریس بزرگتر است، تبدیل کسینوسی گسسته تحت بلاک‌های ۸×۸ گرفته می‌شود و ماتریس DRDIO2 بوجود می‌آید. اکنون در هر بلاک ۴ ضریب بر اساس [۳۵] انتخاب و با استفاده از همسایگی آن با ضرایب اطرافش عملیات جاسازی طبق روابط زیر انجام می‌شود:

```
IF   W2j=0 THEN
   Cki=MIN(Ci+1,Ci+2,Ci+3,Ci+4,Ci+5)
ELSE
   Cki=MAX(Ci+1,Ci+2,Ci+3,Ci+4,Ci+5)
```

که W2j، j امین بیت واترمارک مورد نظر و Cki، یکی از چهار ضریب انتخابی از بلاک‌های ۸×۸ می‌باشد.

پس از عمل جاسازی، ماتریس ضرایب DRDIO2 تبدیل به WDRDIO2 خواهد شد. از WDRDIO2 تبدیل کسینوسی گسسته معکوس تحت بلاک‌های ۸×۸ می‌گیریم. سپس هر عنصر از این ماتریس را که یکی از ضرایب میانی بلاک متناظرش در DIO2 است را به جایگاه خود باز می‌گردانیم تا بدین ترتیب ماتریس WDIO2 بدست آید. اکنون از ماتریس حاصل تبدیل کسینوسی گسسته معکوس می‌گیریم تا WIO2 حاصل شود. WIO2 یک تصویر واترمارک شده می‌باشـــد. شکل (۴) بلاک دیاگرام جاسازی را نمایش می‌دهد :



شکل ۴ - بلاک دیاگرام جاسازی در دامنه فرکانسی با استفاده از تبدیل DCT

۲-۳ – فرآیند استخراج

روشی که در این مقاله ارائه شده، یک روش کور (Blind) است، بنابراین در فرآیند استخراج نیازی به تصویر اصلی واترمارک شده نیست و تنها اطلاعات مورد نیاز برای فرآیند استخراج از تصویر دریافت‌شده، کلیدهایی است که برای رمزنگاری واترمارک و انتخاب بخش‌های تصویر اصلی برای واترمارکینگ به کار می‌رود. براساس رمزی که بین فرستنده و گیرنده وجود دارد، نحوه تقسیم‌بندی تصویر برای جاسازی واترمارک مشخص شده، و هر بخش توسط یکی از الگوریتم‌های استخراج، مورد بررسی قرار می‌گیرد.

۲-۳-۱ – الگوریتم استخراج دردامنه فرکانسی با استفاده از تبدیل DWT

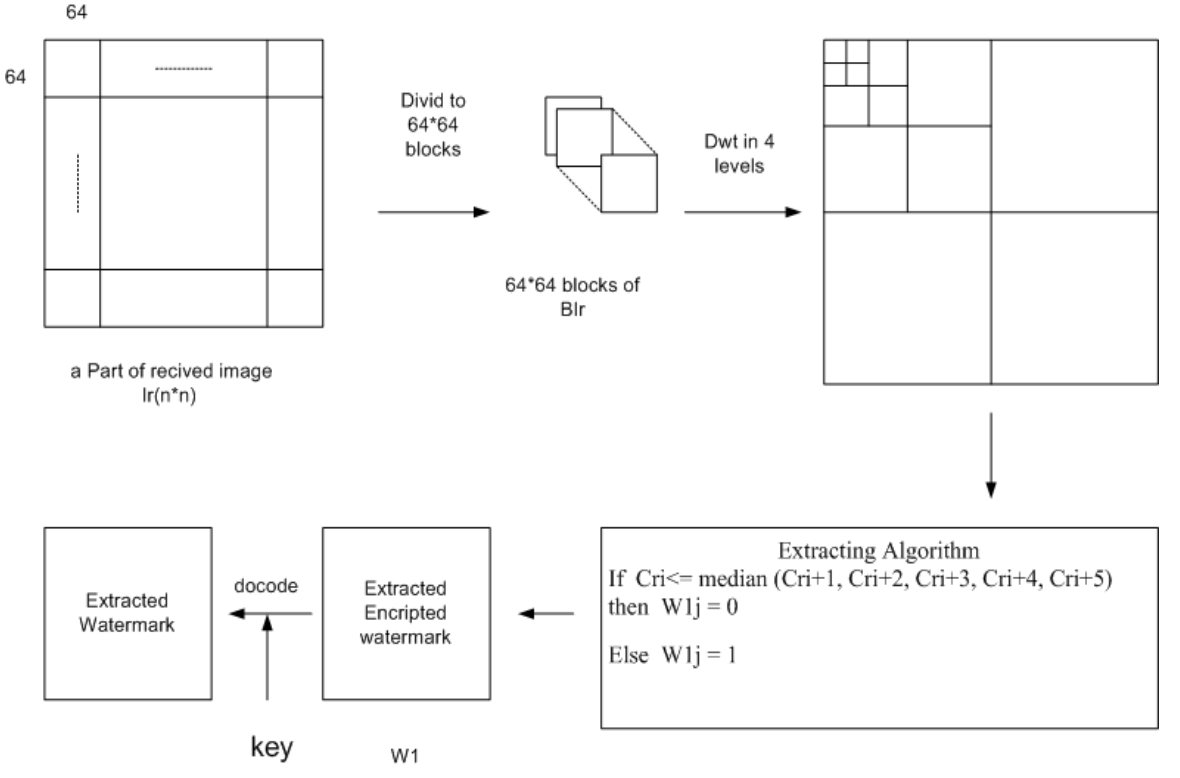
بخشی از تصویر دریافتی که در این قسمت مورد بررسی قرار می‌گیرد، Ir نام دارد. در ابتدا Ir ، به بلاک‌های ۶۴×۶۴ تقسیم‌شده و روی هر بلاک (BIr) به طور جداگانه اعمال زیر را انجام می‌شود :

BIr در چهار سطح تحت تبدیل موجک گسسته قرار می‌گیرد. در نواحی HL و LH از هر سطح (HLi,LHi ; i=1,2,3,4) یک‌سری از ضرایب (Cri) انتخاب می‌شوند. این انتخاب با استفاده از اعداد تصادفی سودو خواهد بود که نقطه شروع آن، یکی از کلیدهای بین فرستنده و گیرنده است. سپس با توجه به رابطه بین ضریب انتخابی و همسایگانش، داده جاسازی شده، تشخیص داده می‌شود :

If Cri<= median (Cri+1, Cri+2, Cri+3, Cri+4, Cri+5)
then W1j = 0
Else W1j = 1

W1j، j امین بیت استخراج شده و Cri، r امین ضریب انتخاب شده است.

پس از استخراج کامل، W1 با استفاده از کلید مخصوص رمزنگاری، رمزگشایی شده و بدین ترتیب، بخشی از اترمارک استخراج می‌شود. در شکل(۵) بلاک دیاگرام فرآیند استخراج در دامنه فرکانسی با استفاده از تبدیل موجک گسسته (DWT) نمایش داده شده است.



شکل ۵- بلاک دیاگرام استخراج در دامنه فرکانسی با استفاده از تبدیل DWT

۲-۳-۲ - الگوریتم استخراج در دامنه فرکانسی با استفاده از تبدیل DCT

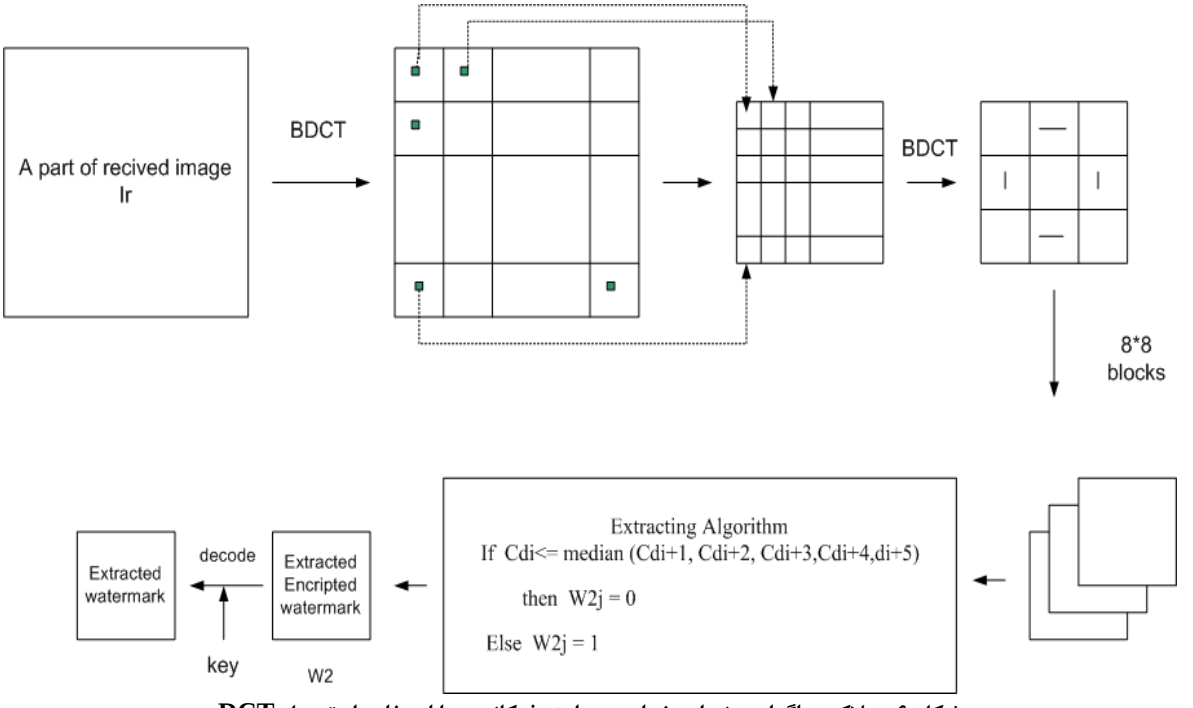
در این قسمت هم تاحدودی، اعمال انجام شده در فرآیند جاسازی انجام می‌شود. پس از دریافت بخش مورد نظر بنام Ir، از آن تحت بلاک‌های ۸×۸ تبدیل DCT گرفته می‌شود و بدین ترتیب BDIrحاصل می‌شود. از هر بلاک ۸×۸ یک یا چند ضریب، بر طبق همان روندی که در مرحله جاسازی انتخاب شده بود، انتخاب می‌شود (اگر از اعداد تصادفی سودو استفاده شده، اکنون نیز همان اعداد استفاده می‌شوند و اگر ضرایب ثابتی انتخاب شده بودند، دوباره همان ضرایب انتخاب می‌شوند.)

سپس از کنارهم قرار دادن ضرایب متناظر از بلاک‌های ۸×۸، ماتریس کوچکتری تولید می‌شود به گونه‌ای که هر عنصر از این ماتریس، عضوی از یک بلاک ۸×۸ است و متناظر با جایگاه بلاک خودش قرار گرفته است. ابعاد ماتریس حاصل برابر ۱/۸ ماتریس BDIr است ؛ می‌توان نام آن را RBDIr گذاشت. از RBDIr تحت بلاک‌های ۸×۸ تبدیل DCT گرفته می‌شود. اکنون ضرایب حاصله از هر بلاک طبق [۳۵] انتخاب و بر اساس رابطه آن با ضرایب همجوارش، واترمارک رمز شده استخراج می‌شود:

```
If  Cdi<= median (Cdi+1, Cdi+2, Cdi+3, Cdi+4, Cdi+5)
then
    W2j = 0
 Else
    W2j = 1
```

W2j ، j امین بیت استخراج شده و Cdi، d امین ضریب انتخاب شده است.

پس از استخراج کامل، W2 با استفاده از کلید مخصوص رمزنگاری، رمز گشایی شده و به این ترتیب، بخش دیگری از واترمارک در دسترس است. بلاک دیاگرام شکل (۶) روند استخراج در دامنه فرکانسی با استفاده از تبدیل کسینوسی گسسته (DCT) را نمایش می‌دهد. از ترکیب W1 وW2، We که واترمارک استخراج شده است، حاصل می‌شود.



شکل ۶ - بلاک دیاگرام روند استخراج در دامنه فرکانسی با استفاده از تبدیل DCT

۳- پیاده سازی و نتایج حاصل

برای پیاده‌سازی این روش، از نرم افزار MATLAB 2007 استفاده شد. تصاویر خاکستری (Gray Scale) با ابعاد ۵۱۲×۵۱۲ به عنوان تصویر اصلی و یک تصویر باینری با ابعاد ۸×۸ به عنوان تصویر واترمارک به‌کارگرفته شد. این روش به‌گونه‌ای پیاده‌سازی شد که تصویر واترمارک را، چهار بار در چهار قسمت تصویر اصلی جاسازی می‌کرد. نتایج، در ادامه شرح داده می‌شود.

شکل(۷) شامل: الف، تصویر اصلی لنا (Lena) ، تصویر واترمارک و ب، تصویرواترمارک شده لنا و تصویر واترمارک استخراج شده است (الف تصاویر سمت راست و ب، تصاویر سمت چپ است).

شکل ۷- الف- تصویر اصلی و واترمارک اصلی
ب- تصویر واترمارک شده و واتر مارک استخراج شده

همانطور که مشاهده می‌شود، بین تصویر اصلی و تصویر واترمارک شده از نظر ظاهری، تفاوتی وجود ندارد. نسبت سیگنال به نویز PSNR(Peak Signal to Noise Ratio) بین تصویر اصلی و تصویر واترمارک شده برابر ۴۵,۴۶۷۷ اندازه‌گیری شده است. برای تخمین شباهت واترمارک استخراج شده و واترمارک اصلی از فرمول NCC(Normalized Cross Correlation) استفاده شده است. به این ترتیب شباهت بین واترمارک اصلی و واترمارک استخراج شده برابر ۱,۰ اندازه‌گیری شد.

بعد از این مرحله، اثرات حملات jpeg و برش، تغییر سایز و چرخش، روی تصویر واترمارک شده، بررسی شد. ابتدا حمله jpeg مورد بررسی قرار گرفت. تصویر واترمارک شده، توسط فاکتورهای کیفیت (QF) متفاوت بررسی شد. نتایج بدست آمده در جدول (۱) و در شکل (۸) نمایش داده شده اند.

نتایج نشان می‌دهد که این روش برابر حمله JPEG، مقاومت قابل قبولی دارد. از آنجا که تصویر اصلی به چهار قسمت تقسیم شده و هر قسمت هم توسط الگوریتم جداگانه‌ای واترمارک شده است، در نتیجه می‌توان پیش‌بینی کرد که این روش در برابر حمله برش مقاومت زیادی داشته باشد. زیرا هر قسمتی از واترمارک استخراج شده که توسط حمله برش از بین رفته است، می‌تواند توسط واترمارک‌های استخراج شده در قسمت‌های دیگر بازیابی شود.

جدول ۱ - نتایج اثر فشرده سازی JPEG با QFهای متفاوت بر روی واترمارک استخراج شده

فاکتور کیفیت فشرده سازی(QF)	NCC	PSNR
۹۵	۱,۰	۴۱,۳۲۹۱
۹۰	۱,۰	۴۰,۵۰۳۶
۸۵	۰,۹۴۲۹	۳۸,۲۳۳۰
۷۵	۰,۹۴۲۹	۳۶,۹۰۷۸
۵۰	۰,۹۱۴۳	۳۵,۱۴۱۱
۲۵	۰,۷۷۱۴	۳۳,۲۰۸۲

(الف) (ب)

(ج)

شکل ۸ - الف- تصویر فشرده شده با QF=90 و واترمارک استخراج شده
ب- تصویر فشرده‌شده با QF=50 و واترمارک استخراج شده
ج- تصویر فشرده‌شده با QF=25 و واترمارک استخراج شده

پس از انجام آزمایشات مختلف، این نتیجه حاصل شد که با حذف ۷۵٪ از تصویر واترمارک شده، واترمارک، با NCC=0.9429 قابل بازیابی می‌باشد. در شکل (۹) این نتایج نشان داده شده است.

(الف) (ب)

(ج)

شکل ۹ - الف- تصویر برش‌خورده با درصد ۱۲.۵ و واترمارک استخراج شده
ب- تصویر برش‌خورده با درصد ۲۵ و واترمارک استخراج شده
ج- تصویر برش‌خورده با درصد ۷۵ و واترمارک استخراج شده

در حمله تغییر اندازه، تغییرات به گونه‌ای انجام می‌شود که ابعاد تصویر را دچار تغییر می‌کند و هیچ‌گونه سطر یا ستونی از تصویر حذف نمی‌شود. با توجه به نتایج حاصل از تغییر مقیاس‌های متفاوت روی تصاویر واترمارک شده بر اساس روش مورد نظر، آشکار است که این روش در برابر تغییر مقیاس‌هایی که منجر به بزرگتر شدن تصویر می‌شوند، بسیار مقاوم است و این تغییرات، در استخراج واترمارک خللی وارد نمی‌کند. اما تغییرات مقیاسی که باعث کوچکتر شدن تصویر می‌شود، باعث از بین رفتن واترمارک نهفته در تصویر می‌گردد. برای تغییرات کمتر از ۵۰٪، واترمارک استخراج شده نسبت به واترمارک اولیه، دچار تغییرات زیادی گشته است. نتایج بدست آمده از اثر حمله تغییر مقیاس در جدول (۲) و شکل (۱۰) قابل مشاهده و بررسی است.

جدول ۲ - نتایج حاصل از واتر مارک استخراج شده پس از حمله تغییر مقیاس با درجات مختلف

تغییر مقیاس نسبت به تصویر اولیه	ابعاد تصویر تغییر یافته	NCC واترمارک استخراج شده
٪۹۰	۴۶۱۴۶۱	۰/۹۹۲۸
٪۸۰	۴۱۰۴۱۰	۰/۹۸۹۱
٪۷۰	۳۵۸۳۵۸	۰/۹۲۹۲
٪۶۰	۳۰۷۳۰۷	۰/۸۸۴۱
٪۵۰	۲۵۶۲۵۶	۰/۶۲۵۰
٪۴۰	۲۰۵۲۰۵	۰/۵۱۰۹
٪۱۱۰	۵۶۳۵۶۳	۰/۸۰۹۶
٪۱۲۰	۶۱۴۶۱۴	۱/۰
٪۲۰۰	۱۰۲۴۱۰۲۴	۱/۰
٪۳۰۰	۱۵۳۶۱۵۳۶	۱/۰
٪۵۰۰	۲۵۶۰۲۵۶۰	۱/۰

شکل ۱۰- الف- واترمارک جاسازی شده وتصویر اصلی

شکل ۱۰- ب- واترمارک استخراج شده از تصویر تغییر مقیاس یافته با درصد ۷۰

شکل ۱۰- ج- واترمارک استخراج شده از تصویر تغییر مقیاس یافته با درصد ۵۰

شکل ۱۰- د- واترمارک استخراج شده از تصویر تغییر مقیاس یافته با درصد ۱۱۰

شکل ۱۰- ه- واترمارک استخراج شده از تصویر تغییر مقیاس یافته با درصد ۳۰۰

برای بررسی اثر حمله چرخش، تصاویر واترمارک شده حول مرکز تصویر و تحت زوایای مختلفی چرخانده می‌شود. تصاویر شکل (۱۱)، نشان دهنده اثرات این حمله روی تصویر واترمارک شده و واترمارک استخراج شده است. تصویر الف نسبت به تصویر اصلی، یک درجه در جهت عقربه‌های ساعت و تصویر ب، یک درجه خلاف جهت عقربه‌های ساعت چرخیده است. واترمارک‌های استخراج شده از نظر دیداری نسبت به واترمارک اصلی بسیار متفاوت هستند. این امر نشان می‌دهد که روش ارائه شده در برابر حمله چرخش (Rotation)، مقاومتی ندارد و واترمارک استخراج شده از تصویری که دچار این حمله گشته است، قابل مقایسه با واترمارک اصلی نیست.

(الف) (ب)

شکل ۱۱ - الف- تصویر با یک درجه چرخش به راست و واترمارک استخراج شده از آن
ب- تصویر با یک درجه چرخش به راست و واترمارک استخراج شده از آن

پس از بررسی اثر حمله‌های متفاوت بر روی واترمارک استخراج شده از تصاویری که توسط الگوریتم پیشنهادی، واترمارک شده‌اند، نتایج حاصل، با نتایج همین حمله‌ها در خروجی الگوریتم‌های دیگر مقایسه شدند. به این منظور، روش‌های ارائه شده در [۷] که روشی مبتنی بر تبدیل موجک گسسته است، روش ارائه شده در [۳۵] که روشی مبتنی بر تبدیل کسینوسی گسسته است و روش ارائه شده در [۲۶] که روشی مبتنی بر LBS است، برای مقایسه با روش پیشنهادی در این مقاله انتخاب شدند. سپس ده تصویر استاندارد پردازش تصویر، تحت هر یک از این روش‌ها واترمارک شدند. پس از انجام حمله‌های مورد نظر، سعی شد که از هر یک از این تصاویر واترمارک شده طبق همان روش به کار رفته، واترمارک استخراج شود. اگر عملیات استخراج به درستی انجام می‌گرفت، امتیاز یک، در غیر این‌صورت، امتیاز صفر برای روش مورد نظر، منظور می‌شد. در جدول (۳) نتایج کامل این مقایسات، نشان داده شده است.

جدول ۳- نتایج حاصل از مقایسه روش‌های مختلف

حمله / روش	فشرده سازی با اتلاف	تغییرمقیاس	برش	چرخش
روش [۲۶]	۲	۲	۵	۱
روش [۳۵]	۹	۶	۶	۶
روش [۷]	۷	۶	۷	۸
روش پیشنهادی	۱۰	۵	۹	۱

همانطور که از نتایج حاصل پیداست، روش ارائه شده در این مقاله، در برابر حملات فشرده‌سازی با اتلاف و برش از سه روش دیگر مقاوم‌تر است، اما در برابر حمله‌های تغییر مقیاس و چرخش، نسبت به روش‌های مبتنی بر تبدیل موجک گسسته و تبدیل کسینوسی گسسته، مقاومت کمتری دارد.

۴- نتیجه‌گیری

در این مقاله روش‌های مختلف واترمارکینگ دیجیتالی در تصاویر مورد مطالعه و بررسی قرار گرفت. با توجه به اینکه در واترمارکینگ دیجیتالی، حجم اطلاعات جاسازی شده نسبت به پارامترهای دیگری مثل مقاومت، نامرئی بودن، نوع استخراج و... اهمیت بالایی ندارد، و از طرفی فضای فرکانسی تصویر نیز می‌تواند در برآورده کردن نیازهای اصلی، موثرتر باشد، روش ارائه شده از فضای فرکانسی استفاده می‌کند و یک روش واترمارکینگ ترکیبی جدید در تصاویر Bitmap، ارائه می‌شود. طبق این روش، یک تصویر به قسمت‌هایی تقسیم می‌شود و هر قسمت توسط یکی از تبدیل‌های DCT یا DWT به فضای فرکانسی برده می‌شود و با توجه به اینکه هر قسمت تحت چه تبدیلی قرار گرفته است، الگوریتم جاسازی روی آن انجام می‌شود، سپس عکس تبدیل‌های مذکور صورت گرفته و قسمت‌های مختلف تصویر به فضای پیکسلی برگردانده می‌شوند و آنگاه کنار یکدیگر قرار می‌گیرند.

بلاک دیاگرام‌های واترمارکینگ و استخراج، در شکل‌های(۲ و ۳ و ۴ و ۵) نشان داده‌شده‌اند. در این روش، استخراج بدون نیاز به تصویر اصلی صورت می‌گیرد. نتایج نشان می‌دهد که این روش در برابر حملات JPEG، تغییر اندازه و برش، مقاومت خوبی دارد. لازم به ذکر است که می‌توان با استفاده از راهکارهای موثری مثل اســـتفاده از الگوریتم‌های ژنتیک، همچنین استفاده از شبکه‌های عصبی در بهبود فرآیند جاسازی و استخراج این روش استفاده کرد تا این روش بتواند در برابر حملات دیگر نیز مقاوم شود.

۵- مراجع

[1] J. Lee, S. Jung, "**A survey of watermarking techniques applied to multimedia**", Proceedings of 2001 IEEE International Symposium on Industrial Electronics (ISIE2001), Vol. 1, pp. 272-277, 2001.

[2] S. Katzenbeisser, F. Petitcolas(Eds), "**Information hiding techniques for steganography and digital watermarking",** Artech House Books, 2000.

[3] J. Cox, M. Miller, "**The first 50 years of electronic watermarking**", 2001 IEEE Forth Workshop on Multimedia Signal Processing, pp. 225-230, 2002.

[4] Y. Kim, K. Moon, Oh I., "**A text watermarking algorithm based on word classification and inter-word space statistics**", Proceedings of Seventh International Conference on Document Analysis and Recognition 2003, pp. 775 -779, 2003.

[5] D. Kirovski, H. Malvar, "**Robust spread-spectrum audio watermarking**", Proceedings of IEEE International Conference on Acoustics, Speech, and Signal Processing, 2001, Vol. 3, pp. 1345-1348, 2001.

[6] S. Foo, T. Yeo and D. Huang , "**An adaptive audio watermarking system**" Proceedings of IEEE Region 10 International Conference on Electrical and Electronic Technology 2001, Vol. 2, pp. 509-513, 2001.

[7] H. Inoue, A. Miyazaki and T. Katsura," **An Image Watermarking Method Based on the Wavelet Transform**", 1999 International Conference on Image Processing, 1999. ICIP 99. Vol. 1, pp. 296 – 300, 1999.

[8] C. Lu, H. Yuan and M. Liao, "**Multipurpose Watermarking for Image Authentication and Protection**", IEEE Transactions on Image Processing, Vol. 10, Issue. 10, pp. 1579-1592, 2001.

[9] A. Herrigel, J. Ruanaidh, "**Secure Copyright Protection Techniques for Digital Images**", Workshop on Information Hiding, LNCS, Springer Verlag, 2003.

[10] M. Buckley, M. Ramos, S. Hemami and S. Wicker, "**Perceptually-based robust image transmission over wire less channels**", Proceedings of 2000 International Conference on Image Processing, Vol. 2, pp. 128-131, 2000.

[11] R. Wolfgang, E. Delp, "**A watermark for digital images**", Proceedings of International Conference on Images Processing, pp. 219-222, 1996.

[12] N. Checcacci, M. Barni, F. Bartolini and S. Basagni, "**Robust video watermarking for wireless multimedia communications**", Proceedings of IEEE Wireless Communications and Networking Confernce 2000, WCNC. 2000, Vol. 3, pp. 1530-1535, 2000.

[13] F. Hartung, B. Girod, "**Watermarking of Uncompressed and Compressed Video**", IEEE Transactions of Signal Processing, Vol. 66, No. 3 (Special issue on Watermarking), pp. 283-301, 1998.

[14] C. Lu, M. Liao, "**Video object-based watermarking: a rotation and flipping resilient scheme**", Proceedings of 2001 International Conference on Image Processing, Vol. 2, pp. 483-486, 2001.

[15] R. Wolfgang, C. Podilchuk and E. Delp, "**Perceptual Watermarks for Digital Images and Video**", Proceedings of the SPIE/IS and T International Conference on Security and Watermarking of Multimedia Contents, Vol. 3657, pp. 40- 51, 1999.

[16] M. Swanson, B. Zhu and A. Tewfik, "**Transparent robust image watermarking**" Proceedings of International Conference on Image Processing, 1996, Vol. 3, pp. 211-214, 1996.

[17] M. Swanson, B. Zhu, B. Chau and A. Tewfik, "**Object-Based Transparent Video Watermarking**", Proceedings of IEEE Signal Processing Society 1997 Workshop on Multimedia Signal Processing, Princeton, New Jersey, USA, Jun. 23-25, 1997.

[18] T. Furon, P. Duhamel, "**Robustness of asymmetric watermarking technique**", Proceedings of International Conference on Image Processing 2000, Vol. 3, pp. 21-24, 2000.

[19] R. Lancini, F. Mapelli and S. Tubaro, "**A robust video watermarking technique in the spatial domain**", Processing and Multimedia Communications, 4th EURASIP-IEEE Region 8 International Symposium on Video/Image VIProm- Com, pp. 251-256, 2002.

[20] M. Ramkumar, A. Akansu, "**Robust Protocols for Proving Ownership of Image**" IEEE Transactions on Multimedia ,Vol. 6, Num. 2 , PP. 22-27, 2004.

[21] P. Lee, M. Chen, "**Robust error concealment algorithm for video decoder**", IEEE Transactions on Consumer Electronics, Vol. 45, Issue. 3, pp. 851 -859, 1999.

[22] D. He, Q. Sun and Q. Tian, "**A semi-fragile object based video authentication system** "Proceedings of the 2003 International

Symposium on Circuits and Systems ISCAS '03, Vol. 3, pp. 814-817, 2003.

[23] J. Fridrich, M. Goljan and A. Baldoza, "**New fragile authentication watermark for images**", Proceedings of 2000 International Conference on Image Processing, Vol. 1, pp. 446-449, 2000.

[24] N. Merhav, "**On random coding error exponents of watermarking systems**" IEEE Transactions on Information Theory, Vol. 46 Issue. 2, pp. 420-430, 2000.

[25] C. Hsu, J. Wu, "**Hidden Digital Watermarks In Images**", IEEE Transactions on Image Processing, Vol. 8, No. 1, 1999.

[26] N. Memon, "**Analysis of LSB based image steganography techniques Chandramouli**" , Proceedings of 2001 International Conference on Image, Vol. 3. pp. 1019-1022, 2001.

[27] G. Langelaar, I. Setyawan and R. Lagendijk, "**Watermarking Digital Image and Video Data**", IEEE Signal Processing Magazine, Vol 17, pp. 20-43, 2000.

[28] F. Duan, I. King, L. Xu and L. Chan, "**Intra-block algorithm for digital watermarking**", Proceedings of IEEE 14th International Conference on Pattern Recognition (ICPR'98), Vol. 2, pp. 1589-1591, 1998.

[29] B. Verma, S. Jain, "**A New Color Image Watermarkig Scheme**", SpringerLink Date , Vol. 245, pp. 497-504, 2007.

[30] R. Sunil, M. Petriu, "**An Adaptive Compressed MPEG2 Video Watermarking Scheme**", IEEE Transactions on Instrumentation and Measurement, Vol. 54, pp. 54-58, 2005.

[31] Y. Wang, A. Pearmain, "**Blind MPEG2 Video Watermarking Robust Against Geometric Attacks: A Set of Approaches in DCT Domain**", IEEE Transactions on Image Processing, Vol. 15, No. 6, 2006.

[32] X. Zhu, Z. Tang, "**A Novel Multibit Watermarking Scheme Combining Spread Spectrum and Quantization**" , IWDW 2006, LNCS 4283, Springer-Verlag Berlin Heidelberg 2006, pp. 111- 122, 2006.

[33] P. W. Chan, M. R. Lyu and R. T. Chin, "**A Novel Scheme for Hybrid Digital VideoWatermarking: Approach, Evaluation and Experimentation**", IEEE Transactions on Circuits and Systems for Video Technology, Vol. 15, Issue 12, pp. 1638 – 1649, 2005.

[34] J. Fridrich, "**A hybrid watermark for tamper detection in digital images**", Proceedings of the fifth International Symposium on Signal Processing and Its Applications, ISSPA '99, Vol. 1, pp. 301-304, 1999.

[35] F. Duan, I. King, L. Xu and L. Chan, "**Intra-block maxmin algorithm for embedding robust digital watermark into images**", Proceedings of the IAPR International Workshop on Multimedia Information Analysis and Retrieval, MINAR' 98, Lecture Notes in Computer Science, Berlin Heidelberg, Germany, Springer-Verlag, Vol. 1464, pp. 255-264, 1998.