ششمین کنفرانس بین المللی انجمن رمز ایران
۱۵ و ۱۶ مهر ماه ۱۳۸۸، دانشگاه اصفهان
انجمن رمز ایران
دانشگاه اصفهان

ارائه یک روش واترمارکینگ جدید برای تصاویر در دامنه فرکانسی

عطیه زاهد[۱]، احمدرضا نقش نیلچی[۲]

[۱]کاشان، دانشگاه آزاد اسلامی واحد کاشان، گروه کامپیوتر[۱]
atiya.zahed@gmail.com
[۲] اصفهان، دانشگاه اصفهان، گروه مهندسی کامپیوتر[۲]
nilchi@yahoo.com

چکیده

در این مقاله، تعدادی از روشهای واترمارکینگ موجود، ازجنبه‌های مختلف مورد بررسی قرار گرفته‌اند. سپس یک روش جدید برای واترمارکینگ تصاویر با فرمت BMP ارائه شده است. این روش واترمارک را در دامنه فرکانسی تصویر با استفاده از تبدیل DCT جاسازی می‌کند و فرایند استخراج را بدون استفاده از تصویر اصلی انجام می‌دهد. این روش در برابر حملات JPEG و برش (Cropping) و تغییر اندازه (Scaling) مقاوم است.

واژه‌های کلیدی

واترمارکینگ، DCT، حمله JPEG، حمله برش، استخراج کور(Blind)

۱- مقدمه

امروزه با پیشرفت سریع تکنولوژی اطلاعات دیجیتالی، همه دارندگان کامپیوترهای خانگی در کامپیوتر خود، یک پردازشگر چند رسانه ای سریع، یک پهنای باند وسیع با قابلیت دسترسی به تمام دنیا وحافظه قابل جابجایی برای اطلاعات دیجیتالی را در اختیار دارند؛ به همین دلیل اطلاعات دیحیتالی 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 ازاین 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 انگیزهٔ خود را برای وارد کردن این محصولات در دنیای تجارت الکترونیک از دست خواهند داد[1]. در حال حاضراز 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.

امضای دیجیتالی با الگوبرداری از رمزنگاری (با استفاده از کلید عمومی و توابع درهم) ساخته شده است. دریافت کننده سند دیجیتالی ای که امضای دیجیتالی در آن به کار رفته است، در صورتی آن سند را معتبر خواهد دانست که به طریقی بتواند امضای دیجیتالی نهفته در سند را کشف کند. اما در صورتیکه کوچکترین تغییر تصادفی ویا عمدی در سند دیجیتالی که از امضای دیجیتالی برای حفاظت از حق کپی استفاده می کند، ایجاد شود، به گونه‌ای که باعث تغییر حتی یک بیت از سند شود، امکان بازیابی امضای دیجیتالی را برای دریافت کننده غیرممکن

خواهد کرد، در نتیجه اعتبار سند به سهولت از بین خواهد رفت [2].

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 می شود. این سیگنال می تواند 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 گونه ای غیر قابل تشخیص یا به اصطلاح نامرئی ، به فایل حاوی موسیقی دیجیتالی وصل می‌شد تا بتواند برای اثبات حق مالکیت به کار برود [26]. 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 [3] .

درطی دهه گذشته، روشهای مختلفی برای واترمارکینگ دیجیتالی ارائه شده است. این روشها را از نقطه نظرات گوناگون می‌توان دسته بندی کرد. از نقطه نظر نوع سندی که واترمارک می‌شود، چهارنوع سیستم واترمارکینگ وجود دارد: سیستم واترمارکینگ متن [4]، صوت [5]، تصویر [7,6] و ویدیو [9,8]. 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 [10] و روشهایی که دارای واترمارک نامرئی [11] می‌باشند. اگر سیستم‌های واترمارکینگ از جنبه مقاومت آنها دربرابر حملات مختلف تقسیم‌بندی شوند، سه دسته سیستم واترمارکینگ وجود دارد: سیستم‌های واترمارکینگ مقاوم [12]، سیستم‌های واترمارکینگ نیمه مقاوم [13] و سیستم‌های واترمارکینگ شکننده [14]. 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 [15] و واترمارک ازنوع تصویر [16]. 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 [17]، پردازش‌های دامنه فرکانسی [19,18]، پردازش‌های دامنه فشرده‌سازی [20] و پردازش‌های مرکب یا هیبرید [22,21].

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 فرکانسی تصویر، جاسازی می‌کند. فرایند استخراج واترمارک در آن یک فرایند استخراج کور است، و در برابر حملات JPEG و برش (Cropping) و تغییر اندازه (Scaling)، مقاوم است.

به طور معمول DCT ،DFT و DWT، 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. سیستم-های واترمارکینگی که از دامنه DCT برای جاسازی واترمارک استفاده می‌کنند، نسبت به حملاتی مثل فشرده‌سازی‌های با اتلاف، از جمله JPEG وبرخی از حملات هندسی مثل برش مقاوم هستند. این سیستم‌ها با استفاده از DCT ، تصویر را به باندهای فرکانسی متفاوتی تفکیک می‌کنند وبه‌این ترتیب واترمارک را در باندهای فرکانسی میانی یک تصویر، جاسازی می‌کنند. روش ارائه شده در [23] یکی از روشهای به‌وجود آمده بر پایه DCT است، که در برابر حملات برش و Translation از مقاومت خوبی برخورداراست.

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 در حالیکه به کیفیت تصویر هم آسیبی نمی رساند.

روش‌هایی که براساس تبدیل DFT هستند نیز روش‌های مقاومی هستند. البته بدلیل اینکه اکثر فشرده‌سازی‌هایی که روی اسناد چندرسانه‌ای صورت می‌گیرند از DCT و DWTبهره 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 می شود، دامنه فشرده سازی 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 درآن غیرممکن می‌سازد.

در این مقاله سعی شده است که با استفاده از تبدیل DCT سیستم واترمارکینگ مقاومی طراحی شود. 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 تبدل DCT قرار می‌گیرد. واترمارک رمز شده نیز به طور جداگانه توسط الگوریتم جاسازی، در هر یک از این بخش‌ها، قرار می‌گیرد 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 می شود و دوباره بخشهای مختلف تصویر کنار یکدیگر قرار می گیرند و تصویر واترمارک شده را بوجود می آورند. تغییراتی که سیستم واترمارکینگ موجود روی تصویر بوجود می‌آورد، توسط چشم انسان غیر قابل رویت است.

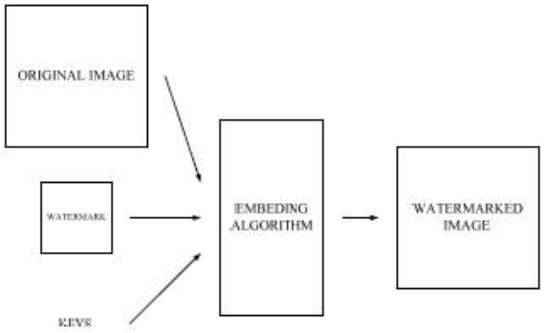
یکی از مزایای مهم این روش، استخراج کور واترمارک از تصویر واترمارک شده است. به‌این ترتیب برای استخراج واتر مارک در طول فرایند استخراج، نیازی به تصویر اصلی و مقایسه آن با تصویر واترمارک شده نیست. این مزیت باعث کمتر شدن بارمحاسباتی سیستم واترمارکینگ می‌شود. همچنین بدلیل کور بودن، می توان از این روش در واترمارکینگ ویدیویی استفاده کرد، زیرا حذف یا اضافه شدن فریم‌های ویدیو یا جابجایی آنها نمی‌تواند در فرایند استخراج مشکلی به وجود آورد.

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

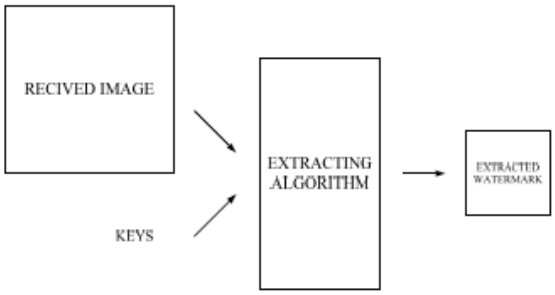
این مقاله دارای سه بخش دیگر است. در بخش دوم روش واترمارکینگ پیشنهادی به‌طورکامل توضیح داده شده است. در بخش سوم نتایجی که از پیاده سازی این روش بدست آمده و همچنین اثرحمله‌های مختلف در این روش مورد بررسی قرار گرفته‌اند و در فصل چهارم کارهای مهم انجام شده درتحقیق، باردیگربصورت خلاصه ذکرمی‌گردد ونتایج بدست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

۲- معرفی روش ارائه شده

روش ارائه شده در این مقاله به دو الگوریتم اصلی تقسیم می‌شود: الگوریتم جاسازی و الگوریتم استخراج. بلاک دیاگرام کلی روش در شکل‌های ۱ و ۲ نشان داده شده است.



شکل ۱ : بلاک دیاگرام کلی روش پیشنهادی برای جاسازی واترمارک



شکل ۲ : بلاک دیاگرام کلی روش پیشنهادی برای استخراج واتر مارک

۲-۱ الگوریتم جاسازی در دامنه فرکانسی با استفاده از تبدیل کسینوسی گسسته (DCT)

در ابتدا تصویر اصلی بنابر روشی خاص به چند قسمت تقسیم شده و در هر قسمت، طبق الگوریتم جاسازی، بخشی از واترمارک یا همه آن جاسازی می شود.

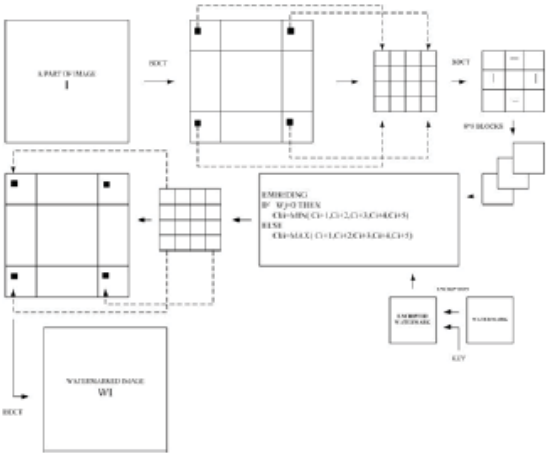
به این منظور بخش‌های جداگانه تصویر(I) به عنوان سندی که باید واترمارک شود و بخشی از واترمارک یا همه آن (W) به عنوان واترمارک وارد می‌شوند. I تحت تبدیل BDCT قرار می‌گیرد (تبدیل کسینوسی گسسته تحت بلاکهای ۸×۸). سپس با استفاده از اعداد تصادفی سودو یکی از ضرایب میانی بلاکهای ۸×۸، از ماتریس ضرایب حاصل (DI) انتخاب می‌شوند. با استفاده از این ضرایب انتخاب شده یک ماتریس کوچکتر که ابعادش نسبت به DI، ۱/۸ است، تشکیل می شود. که هر درایه آن یکی از ضرایب انتخابی از بلاکهای DI است و در جایگاه متناسب با بلاک متناظرش در DI قرار دارد. از این ماتریس (RDI) که خود ضرایب DCT یک ماتریس بزرگتر است، تبدیل کسینوسی گسسته تحت بلاکهای ۸×۸ گرفته می شود و

ماتریس DRDI بوجود می آید. اکنون در هر بلاک ۴ ضریب بر اساس [23] انتخاب و با استفاده از همسایگی آن با ضرایب اطرافش عملیات جاسازی طبق روابط زیر انجام می شود:

IF Wj=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، jامین بیت واترمارک مورد نظر و Cki، یکی از چهار ضریب انتخابی از بلاکهای ۸×۸ می باشد.

پس از عمل جاسازی، ماتریس ضرایب DRDI تبدیل به WDRDI خواهد شد. از WDRDI تبدیل کسینوسی گسسته معکوس تحت بلاکهای ۸×۸ می‌گیریم. سپس هر عنصر از این ماتریس را که یکی از ضرایب میانی بلاک متناظرش در DI است را به جایگاه خود باز می گردانیم تا بدین ترتیب ماتریس WDI بدست آید. اکنون از ماتریس حاصل تبدیل کسینوسی گسسته معکوس می گیریم تا WI حاصل شود. WI یک تصویر واترمارک شده می باشد. شکل ۳ بلاک دیاگرام جاسازی را نمایش می‌دهد :



شکل ۳: بلاک دیگرام جاسازی در دامنه فرکانسی با استفاده از DCT

۲-۲ فرایند استخراج

روشی که در این مقاله ارائه شده، یک روش کور است، بنابر این در فرایند استخراج نیازی به تصویر اصلی واترمارک شده نیست و تنها اطلاعات مورد نیاز برای فرایند استخراج از تصویر دریافت شده، 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 جداگانه توسط الگوریتم استخراج، مورد بررسی قرار می‌گیرد.

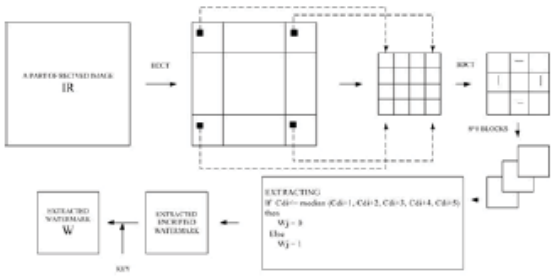
در این قسمت هم تا حدودی، اعمال انجام شده در فرایند جاسازی انجام می شود. پس از دریافت بخش مورد نظر بنام Ir ، از آن تحت بلاکهای ۸×۸ تبدیل DCT گرفته می شود و بدین ترتیب BDIr حاصل می‌شود. از هر بلاک ۸×۸ یک یا چند ضریب، بر طبق همان روندی که در مرحله جاسازی انتخاب شده بود، انتخاب می‌شود (اگر از اعداد تصادفی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

سپس از کنارهم قرار دادن ضرایب متناظر از بلاکهای ۸×۸، ماتریس کوچکتری تولید می‌شود به گونه ای 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 [23] انتخاب و بر اساس رابطه آن با ضرایب همجوارش، واترمارک رمز شده استخراج می شود:

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

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

پس از استخراج کامل، W با استفاده از کلید مخصوص رمزنگاری، رمزگشایی شده و به این ترتیب، بخش دیگری از واترمارک در دسترس است. بلاک دیاگرام شکل ۴ روند استخراج در دامنه فرکانسی با استفاده از تبدیل کسینوسی گسسته (DCT) را نمایش می دهد.



شکل ۴: بلاک دیاگرام روند استخراج در دامنه فرکانسی با استفاده از DCT

از ترکیب Wهای استخراج شده Weکه واترمارک اولیه است، حاصل می‌شود.

۳- پیاده‌سازی و نتایج حاصل

برای پیاده‌سازی این روش، از نرم‌افزار 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 به‌کار گرفته شد. این روش به گونه‌ای پیاده‌سازی شد که تصویر واترمارک را، چهار بار در چهار قسمت تصویر اصلی جاسازی می‌کرد. نتایج، در ادامه شرح داده می شود. شکل ۵ شامل: الف، تصویر اصلی (لنا)، تصویر واترمارک و ب، تصویرواترمارک شده و تصویر واترمارک استخراج شده است (الف تصاویر سمت راست و ب، تصاویر سمت چپ است).

شکل ۵ :

الف- تصویر اصلی و واترمارک اصلی

ب- تصویر واترمارک شده و واتر مارک استخراج شده

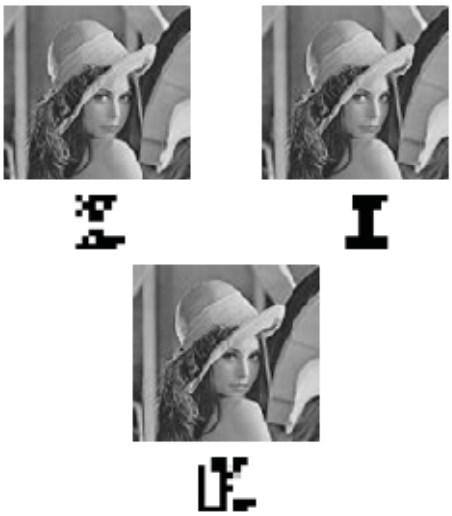
همانطور که مشاهده می‌شود، بین تصویر اصلی و تصویر واترمارک شده از نظر ظاهری، تفاوتی وجود ندارد. نسبت سیگنال به نویز PSNR(Peak Signal to Noise Ratio) بین تصویر اصلی و تصویر واترمارک شده برابر۴۵/۴۶۷۷dB اندازه‌گیری شده است. برای تخمین شباهت واترمارک استخراج شده و واترمارک اصلی از فرمول NCC(Normalized Cross Correlation) استفاده شده است. به این ترتیب شباهت بین واترمارک اصلی و واترمارک استخراج شده برابر ۱/۰ اندازه گیری شد.

بعد از این مرحله، اثرات حملات jpeg و برش، تغییر اندازه 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 ۶ 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. پس از انجام ازمایشات مختلف، این نتیجه حاصل شد که با حذف۷۵% از تصویر واترمارک شده، واترمارک، با NCC=0.9429 قابل بازیابی می‌باشد. در شکل ۷ این نتایج نشان داده شده است.

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

فاکتور کیفیت فشرده‌سازی(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



شکل ۶ : (از راست به چپ) :

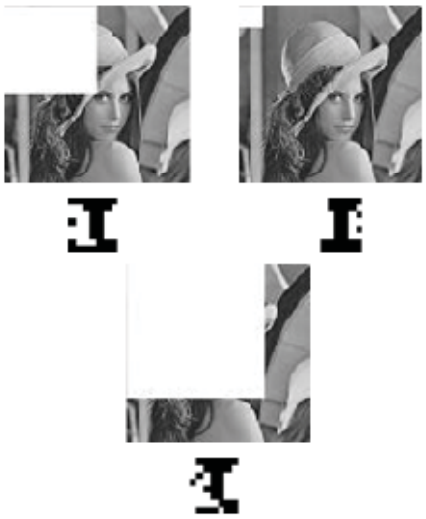
الف- تصویر فشرده شده با QF=90 و واترمارک استخراج شده

ب- تصویر فشرده شده با QF=50 و واترمارک استخراج شده

ج- تصویر فشرده شده با QF=25 و واترمارک استخراج شده

در حمله تغییر اندازه، تغییرات به گونه‌ای انجام می‌شود که ابعاد تصویر را دچار تغییر می‌کند و هیچ گونه 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 می شوند، بسیار مقاوم است و این تغییرات، در استخراج واترمارک خللی وارد نمی کند. اما تغییرات مقیاسی که باعث کوچکتر شدن تصویر می شود، باعث

از بین رفتن واترمارک نهفته در تصویر می گردد. 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 قابل مشاهده و بررسی است.



شکل ۷ : (از راست به چپ) :

الف- تصویر برش خورده با درصد ۱۲.۵ و واترمارک استخراج شده

ب- تصویر برش خورده با درصد ۲۵ و واترمارک استخراج شده

ج- تصویر برش خورده با درصد ۷۵ و واترمارک استخراج شده

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	۴۶۱*۴۶۱	۰/۹۹۲۸
%۸۰	۴۱۰*۴۱۰	۰/۹۸۹۱
%۷۰	۳۵۸*۳۵۸	۰/۹۲۹۲
%۶۰	۳۰۷*۳۰۷	۰/۸۸۴۱
%۵۰	۲۵۶*۲۵۶	۰/۶۲۵۰
%۴۰	۲۰۵*۲۰۵	۰/۵۱۰۹
%۱۱۰	۵۶۳*۵۶۳	/۸۰۹۶
%۱۲۰	۶۱۴*۶۱۴	۱/۰
%۲۰۰	۱۰۲۴*۱۰۲۴	۱/۰
%۳۰۰	۱۵۳۶*۱۵۳۶	۱/۰
%۵۰۰	۲۵۶۰*۲۵۶۰	۱/۰

برای بررسی اثر حمله چرخش، تصاویر واترمارک شده حول مرکز تصویر و تحت زوایای مختلفی چرخانده می شود. تصاویر شکل ۸، 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 متفاوتند. این امر نشان می دهد 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.

شکل ۸: (از راست به چپ)

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

ب- تصویر با یک درجه چرخش به چپ و واترمارک استخراج شده از آن

پس از بررسی اثر حمله‌های مختلف بر روی واترمارک استخراج شده از تصاویری که توسط الگوریتم پیشنهادی، واتر مارک شدند، نتایج بدست آمده با نتایج حاصل از اثر همین حمله‌ها در خروجی الگوریتم‌های دیگر مقایسه شدند. به این منظور، روش‌های ارائه شده در [24] که روشی مبتنی بر تبدیل موجک گسسته است و روش ارائه شده در [23] که روشی مبتنی بر تبدیل کسینوسی گسسته است و روش ارائه شده در [27] که روشی در دامنه مکانی 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 برای هریک از این تصاویر واترمارک شده طبق همان روش به کار رفته، عمل استخراج واترمارک انجام بگیرد. اگر در عملیات استخراج، واترمارک به درستی حاصل می شد، امتیاز یک و در غیر اینصورت، امتیاز صفر برای روش مورد نظر، اضافه می‌شد. در جدول ۳ نتایج کامل این مقایسات نشان داده شده است.

همانگونه که از نتایج حاصل پیداست، روش ارائه شده در این مقاله، در برابر حمله‌های فشرده‌سازی با اتلاف و برش از سه روش دیگر مقاوم تر است، اما در برابر حمله‌های تغییر مقیاس و چرخش، نسبت به روش‌های مبتنی بر تبدیل موجک گسسته و تبدیل کسینوسی گسسته [23]، مقاومت کمتری دارد.

جدول ۳ : نتایج حاصل از مقایسه روش‌های مختلف

حمله روش	فشرده‌سازی با اتلاف	تغییر مقیاس	برش	چرخش
روش[۱۷]	۲	۲	۵	۱
روش[۲۳]	۹	۶	۶	۶
روش[۲۴]	۷	۶	۷	۸
روش پیشنهادی در این مقاله	۱۰	۵	۸	۰

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 می کند و یک روش واترمارکینگ ترکیبی جدید در تصاویربا فرمت Bitmap، ارائه می شود. 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 کناریکدیگر قرار می‌گیرند.

بلاک دیاگرام‌های واترمارکینگ و استخراج، در شکل‌های ۳و۴ 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 استفاده از الگوریتم‌های ژنتیک، همچنین استفاده از شبکه‌های عصبی در بهبود فرایند جاسازی و استخراج این روش استفاده کرد تا این روش بتواند در برابر حملات دیگر نیز مقاوم شود.

مراجع

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

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

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

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

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

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

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

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

[9] Wolfgang R., Podilchuk C., Delp E., 1999, "*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.

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

[11] Lancini R., Mapelli F., Tubaro S., 2002, "*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.

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

[13] He D., Sun Q. , Tian Q., 2003, "*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.

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

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

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

[17] Memon N., 2001, "*Analysis of LSB based image steganography techniques Chandramouli*" ,

Proceedings 2001 International Conference on Image, Vol. 3. pp. 1019-1022.

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

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

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

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

[22] Chan P.W., Lyu M.R. , Chin R.T., 2005, "*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.

[23] Duan F., King I., Xu L., Chan L., 1998, "*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, 1998. Springer- Verlag, Vol. 1464, pp. 255-264.

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