
بسم الله الرحمن الرحيم

دانشگاه آزاد اسلامی

واحد تبریز

دانشکده فنی ومهندسی-گروه برق

پایان نامه برای دریافت درجه کارشناسی ارشد

گرایش: مهندسی برق- الکترونیک

عنوان:

ارائه یک روش واترمارکینگ کور براساس کوانتیزه کردن درخت ویولت

استادراهنما:

دکترسیامک حقی پور

استادمشاور:

دکتر بهزادمظفری

نگارش:

مسعودملکی

تابستان۱۳۸۹

تقدیم به

پدر مهربان

و

مادر دلسوزم

سپاسگزاری

هوالله الذی لا اله الا هوعالم الغیب والشهاده هوالرحمن الرحیم

اوست خدایی که غیراز او خدایی نیست که دانای نهان وآشکار عالم است وبخشنده ومهربان(در حق بندگان). سوره حشرآیه۲۲

آنکس را می ستایم که ستایش گویندگان تا آخرین حد مبالغه، وصف کمالش را کفایت نکندوروزی خوران از شمردن نعمت بی پایانش عاجزباشندوهرچه بکوشند یک از هزار آنرا سپاس نتوانند.برآستان شکوه وقدرت وعظمت وجلال تو پیشانی بندگی برخاک می نهم وبا تمام وجود شکرتو میگویم.

برخود واجب می دانم که از تمامی عزیزانی که در انجام این رساله یاریم کردند تقدیروتشکرکنم:

ازاستاد گرانقدرجناب آقای دکترسیامک حقی پور بخاطر راهنمایی های ارزنده در مسیرپیشبرداین رساله تشکروقدردانی مینمایم.

ازاستادگرامی جناب آقای دکتر بهزادمظفری به خاطرمساعدت ومشاورت های مفیدشان درانجام این رساله صمیمانه سپاسگزارم.

ازخانواده عزیزم که همواره با حمایت های بی دریغشان تکیه گاه شایسته ای برایم بوده اند و بی شک بدون یاری های ارزشمندشان هیچم مقدور نبود، قدردانی میکنم وزحمات آنان را ارج می نهم.

از دوست بسیار عزیزم جناب آقای مهندس وحیدپورگلزاری به خاطرکمکهای مفیدشان تشکروسپاسگزاری میکنم.

چکیده:

استفاده از رسانه های دیجیتالی به واسطه‌ی ذخیره‌سازی، انتقال و کاربری آسان در چند دهه‌ی اخیر رشد چشمگیری داشته است. اما ساختار چنین رسانه هایی همواره در معرض تهدید و تخطی از حقوق کپی رایت و حق مولف بوده است. در پانزده سال اخیر حفاظت از اطلاعات دیجیتالی به بحث مهمی در حوزه رسانه های دیجیتالی بدل شده است و تکنیک هایی که بتواند با اختصاص دادن اطلاعات مخفی در رسانه های دیجیتالی (مثلا اطلاعات مربوط به مولف یا حق کپی‌رایت) به حل این مشکلات بپردازد، روز به روز گسترش بیشتری یافته است. دراین میان تکنیکهای واترمارکینگ دیجیتال برای حفاظت از حق و حقوق چاپ سیگنالهای مدیا توسعه و پیشرفت کرده است. واترمارکینگ می تواند در حوزه های گسترده ای از اطلاعات نظیر صوت، تصویر ثابت وتصاویر ویدیوئی به کار رود.

فهرست مطالب

فهرست جدول ها

فهرست شکل ها

Abstract—this study has introduced watermark and applications of digital watermarking especially on digital images. We embed a watermark bit by comparing the significant difference with an average significant difference value, and the maximum coefficients are quantized. So there exists a large magnitude difference between the maximum coefficients and the second maximum coefficients after watermark embedding, which can be used for blind extracting watermark. As a result, the watermarked image looks lossless comparing with the original image. Moreover, by designing an adaptive threshold in the extracting process, our method can effectively resist common image processing attacks such as JPEG compression, media filtering, Gaussian noise, cropping, sharpening, and histogram equalization and so on, and it has a good transparency. Experimental results show that the watermarked image looks visually identical to the original, and the watermark can be effectively extracted even after either an unintentional image processing or intentional image attacks.

فصل اول

مقدمه ، هدف و پیشینه پژوهش

۱-۱- تاریخچه

دنیای دیجیتال سبب بروز تغییرات عمده ای در ارتباطات مابین انسان ها وپیشرفت تکنولوژی در برداشته است. زمانی که اولین کامپیوتر دیجیتال پای به عرصه ی وجود گذاشت هیچ کس فکر این مساله را نمی کرد که زمانی فرا خواهد رسید که بدون کامپیوتر زندگی برای بشر غیر قابل تصور خواهد بود. رشد و گسترش ارتباطات دیجیتال و ارزانی و فراگیر شدن آن مزید بر علت شد که بشر روی به جمع آوری و ذخیره اطلاعات به صورت داده های دیجیتالی آورد.چرا که اطلاعات دیجیتال[1] هم براحتی ذخیره میشوندوهم میتوان آنها را براحتی با کمک کامپیوتر پردازش کرد و از همه مهم تر اینکه می توان این اطلاعات را از طریق خطوط ارتباطی نوین علی الخصوص اینترنت به راحتی از نقطه ای از جهان به نقطه ای دیگر انتقال داد. اما همانطور که هیچ چیز در دنیای مهندسی دارای کیفیت مطلق نبوده این فاکتورهای مفید و حیاتی نقاط ضعفی نیز داشتند. یکی از مهمترین نقاط ضعف آنست که همانقدر که اطلاعات دیجیتال به راحتی ذخیره و پردازش می شوند و به راحتی انتقال پیدا می کنند، به همان اندازه هم اطلاعات صحیح راحت تر می توانند جای خود را در به اطلاعات نادرست دهند و سبب سردرگمی کسانی شوند که با این اطلاعات سروکار دارند. همچنین استفاده ی غیر مجاز و بدون اجازه از این اطلاعات نیز امری سهل الوصول خواهد بود. بدیهی است چنین مشکلاتی در سطح پروژه های عظیم تجاری، سیاسی، نظامی و ... غیر قابل گذشت خواهد بود و اندک مسامحه و کوتاهی درامنیت[2] اطلاعات سبب شکست های غیرقابل بخشش ،برای

[1] Digital information
[2] Security

صاحبان اینگونه پروژه ها خواهد شد. بنابراین متخصصان با توجه بـه مزیـت هـای فراوانـی کـه در دنیـای دیجیتال یافته بودند، به فکر ارائه راهکارهایی برای ایجاد امنیت اطلاعات در این دنیای جذاب افتادند.

در طول دو دهه ی گذشته راهکارهای فراوانی برای افزایش امنیت اطلاعات ارائه شده است.واترمارکینگ یکی از مهمترین این گونه راهکارهاست که توانسته است در پانزده سال اخیـر خـود را بـه عنـوان یکـی از مهمترین و پرکاربردترین شاخه های پردازش تصویر معرفی کند. به زبان سـاده واترمارکینـگ عبارتـست از قرار دادن یکسری اطـلاعـــات در لابه لای یک اثر دیجیتالی دیگر، به نحوی که این اطلاعات نـشاندهنده ی پیغامی برای مالکان و یا افراد مجاز اثر اصلی باشد.

واترمارکینگ بحث جدیدی نیست و این کار از دیرباز مورد توجه انسان قرار گرفتـه بـود امـا بـه نـوعی دیگر! در زمان های قدیم نیز برای اطمینان از اصلی بودن پیغامی که از جایی به جایی دیگر انتقال می یافـت و حاوی اطلاعات مهمی بود، به کمک مرکب های مخصوصی که اثـر آن بـر روی کاغـذ تنهـا در شـرایطی خاص مثلا قرار دادن در معرض حرارت آشکار می شد، نوشته و یا آرمی را قرار می دادند که بیـانگر اصـل بودن پیغام می بود. اولین واترمارکینگی که بر روی کاغذ انجام شده به سال ۱۲۸۲برمی گردد.این کـار بـرای اولین بار در ایتالیا صورت گرفت وچون این علامت ها شبیه تاثیر آب روی کاغذ بود از اواخـر قـرن ۱۸بـه بعدبه watermarkمعروف شد.علت قدیمی ترین واترمارک ها نامعلوم است.در زمان اخیر نیز برای اولین بار در ایالات متحده ی آمریکا برای چاپ اسکناس ۲۰ دلاری تصویررئیس جمهور آمریکا به کمـک مرکـب های مخصوص در پس زمینه ی اسکناس چاپ شده بود.

نظر و پیشنهاد پنهان کردن اطلاعات در روی کاغذ همانطور که گفته شد قدمت زیادی دارد.با این حال واترمارکینگ دیجیتال به نظر می رسد درسال ۱۹۹۳ برای اولین بار معرفی شد. زمانی که تیر کل ودوستان

شکل۱-۱ –تصویریک ۲۰دلاری آمریکا که تصویررییس جمهور در آن واترمارک شده

او دو تکنیک برای پنهان کردن اطلاعات و داده در تصویر نشان دادند . این دو روش بر اساس تغییر و تبدیل کم اهمیت ترین بیت (LSB) مقدارهای پیکسل کار می کرد.

واترمارکینگ دیجیتال یکی از تکنولوژی هایی است که به عنوان یک ابزار مناسب برای تعیین مبدا[۱]، خالق[۲] یک اثر، مالکیت[۳] پخش[٤] آن اثر، اجازه استفاده کننده ازآن اثر[٥] وغیره توسعه پیدا کرد. همچنین می توان از آن برای ردگیری آثاری که به طور غیرمجاز پخش شده است استفاده نمود. با توجه به موارد ذکر شده واترمارکینگ علاوه بر کاربردهای کلاسیک خود کاربردهای دیگری نیز یافته است. واترمارکینگ را می توان در حوزه هایی از قبیل نشر الکترونیکی[٦]، تبلیغات[۷]، سفارش کالاودریافت آن،گالری های تصویری[۸]، کتابخانه های دیجیتالی[۹]، روزنامه هاومجله های آنلاین، صوت وتصویر دیجیتالی[۱۰] و مخابرات محرمانه و...به کار برد.

[1] Source
[2] Creater
[3] Owner
[4] Distributor
[5] Athorized Consumer
[6] Electronic Publishing
[7] Advertising
[8] Picture Galleries
[9] Digital Libraries
[10] Digital Video and Audio

همچنین ازآن میتوان برای ردگیری[1] تصاویری که به صورت غیرمجاز پخش شده است استفاده کرد[۱۸].

۱-۲- علل اصلی پیدایش واترمارکینگ دیجیتال

امروزه اطلاعات از طریق شبکه جهانی اینترنت به طور گسترده و آسان در اختیار و دسترس کاربران قرار می گیرد. این شبکه های متصل به هم اجازه مراجعه متقابل بین پایگاههای داده را فراهم می کنند. ظهورمولتی مدیا اجازه کاربردهای مختلفی از فیلم، تصویر و صوت را فراهم می کند. به عنوان مثال در تجارت الکترونیکی یا آموزش از راه دوروغیره. امروزه صنعت برای اینکه صدا و تصویر و فیلم در حالت دیجیتالی در اختیار مشتریها قرار گیرد سرمایه گذاری می کند و همه کمپانیها و شرکت های تلویزیونی تصاویر آرشیوی خود را از حالت آنالوگی به صورت دیجیتالی برمی گردانند. این تغییرات و تحولات نظیر برگرداندن آثار سنتی مثل اسناد کاغذی یا همه ضبط شده های آنالوگی به صورت مدیای دیجیتای به این علت است که مزیتهای مدیای دیجیتال خیلی بیشتر از مدیای قدیمی و سنتی است. برخی از این مزیتها عبارتند از :

۱ – کیفیت سیگنالهای دیجیتال بیشتر از سیگنالهای آنالوگ نظیرشان است. دستگاهها و لوازم قدیمی وسنتی درگذر زمان از کیفیتشان کاسته می شود. داده آنالوگ برای دستیابی به کپی با کیفیت بالا به یک سیستم گران قیمت نیاز دارد درحالی که داده های دیجیتالی به آسانی کپی می شوند، بدون آنکه از کیفیتشان کاسته شود.

۲– اطلاعات و داده های دیجیتالی به آسانی می توانند روی شبکه ها منتقل شوند برای مثال در اینترنت امروزه حجم زیادی از داده های مولتی مدیا برای کاربران در سراسر جهان در دسترس می باشد واین گستردگی با نرخ رشد بیشتری همراه خواهد بود اگر دستیابی به سرویسهای مولتی مدیا نظیر تجارت الکترونیکی، آگهی ها، تلویزیونها، کتابخانه های دیجیتالی و .... افزایش پیدا کند.

[1] Tracking

۳ – کپی های دقیق یک داده دیجیتالی به آسانی ایجاد می شود. این کار خیلی مفید است، اما مشکلاتی را نیز برای صاحب داده با ارزش ،نظیر تصاویر دیجیتال گرانبها ایجاد می کند. یک کپی از یک داده دیجیتالی را نمی توان تشخیص داد وهمین طور اصل بودن آن را نیز نمی توان مشخص و مسجل کرد. اینکه مشخص کنیم کدام یک قطعه و داده اصلی و کدامیک کپی شده است کاری غیرممکن است واین از معایب سیستمهای دیجیتالی به شمار میرود.

٤– این امکان درداده دیجیتالی وجود داردکه اطلاعات وداده هایی را در آن پنهان کنیم به گونه ای که داده تغییر یافته با حس های انسانی غیرقابل تشخیص باشد.

یک فاکتور مهم که سبب کاهش رشد خدمات شبکه ای می شود بی میل شدن نویسندگان، ناشران و مهیاکنندگان داده های مولتی مدیا نسبت به پخش اسنادشان در محیط شبکه ها هستند. این به خاطر راحتی تکثیر داده دیجیتال اصلی وایجاد داده جدید که دقیقا شبیه اصلی است، می باشد.از طرفی این کار سبب ترغیب و تشویق به تخلف و تجاوز و سوء استفاده از اطلاعات می شود. سرقت و پخش اثرها ،از مشکلات ناشران می باشند.به همین خاطر خالقان وپخش کنندگان داده های دیجیتالی فعالانه دنبال راه حلی قابل اطمینان برای حل مشکلات مربوط به حفظ حق چاپ داده مولتی مدیای خود هستند. علاوه براین، پیشرفت آتی سیستمهای مولتی مدیای شبکه ای بویژه در شبکه های باز نظیر اینترنت مشروط به استفاده از روشهای موثر برای حفاظت از حق صاحبان اثر در مقابل کپی های غیرقانونی و تکثیرهای مجدد اسناد قرار گرفته در شبکه است. یکی از کارهایی که میتوان انجام دادو حقوق آنها را تضمین و از اموال آنها محافظت کردواترمارکینگ است.بدین ترتیب مهمترین واصلی ترین عامل پیدایش واترمارکینگ دیجیتال حفاظت از حق نشر و چاپ افراد صاحب اثرباشد.

۱-۳- تعریف واترمارکینگ دیجیتال

واترمارکینگ یعنی توانایی جاسازی یک پیام در یک داده دیجیتال بدون خراب کـردن مقـدار و ارزش آن اثر .به نظر می رسد واترمارکینگ دیجیتال یک روش خوب برای محافظت از حقوق صاحبان اثـر در مقابـل کپی برداری غیرمجاز باشد. واترمارکینگ دیجیتال چند مزیت دیگر نیز دارد. واترمارکینگ دیجیتال یک پیـام معلوم را در یک داده دیجیتالی به عنوان وسیله ای برای شناسایی صاحب حقیقـی داده جاسـازی مـی کنـد . یک تکنولوژی است که راهکارهایی برای امکان تجارت الکترونیک نظیردستیابی مشروط و مخصوص کاربر مجاز به خدمات ومنابع شبکه ها رافراهم می سازد. این مارک و آرم گذاری به صاحب اثـر ایـن اجـازه را می دهد که با ایمنی بیشتر اثر را برای دیدن یاشنیدن همه ارسال کند .این تکنیکها برای بسیاری از انواع داده های دیجیتال نظیر عکس ، فیلم ، صوت به کار می روند. واتر مارکینـگ دیجیتـال عبارتـست از قرارگـرفتن غیرمحسوس اطلاعات درون اطلاعاتی دیگر،بطوریکه به محافظت از آن داده با احراز هویت وحفظ حقـوق کپی رایت مالکین آن داده، می پردازد. به نحوی که تنها مالکین یا افراد صاحب صلاحیت توانـایی اسـتخراج وآشکارسازی اطلاعات درون میزبان را داشته باشندومعمولا بوسیله یک کلید سری این قابلیت بـه آنهـا داده می شود.یک واترمارک دیجیتال، یک سیگنال جاسازی شده ثابت و همیشگی در داخـل داده دیجیتـال نظیـر عکس ، فیلم ، صوت و متن است که می تواند به هر علتی از جمله ادعایی در مـورد اثـر بوسـیله عملیـات آماری و محاسبه ای آشکارسازی شده و استخراج گردد . واترمارک در داده میزبان به گونـه ای جدانـشدنی پنهان است و در برابر بسیاری از عملیاتها مقاوم می باشد. بنابراین بوسیله واترمارکینگ کار و اثر همیـشه در اختیار صاحب اثر است اما با یک علامت و آرم همیشگی. تکنیکهای واتر مارکینگ از استگانوگرافی به معنی پوشیده نوشتن منتج می شود.اما واترمارکینگ با استگانوگرافی وکریپتوگرافی متفاوت است.دربخش بعـد بـه این تفاوت ها اشاره ای مختصر خواهیم داشت.

۱-٤- تفاوت های واترمارکینگ با استگانوگرافی[1] وکریپتوگرافی[2]

در برخی موارد ممکن است به نظر برسد با رمزنگاری داده‌ها بتوان یک سطح امنیت مناسب برای آن‌ها فراهم ساخت، اما این شیوه عملاً موجب تحریک مهاجمان می‌شود. حتی پیش از این نیز مخفی کردن متن، بر رمز کردن آن ترجیح داده می‌شد. هرچند آغاز رمزنگاری مدرن را دوران درخشانی در اروپا می‌دانند، ولی در سال ١٦٤١ افرادی بودند که پنهان‌سازی داده را بر رمزنگاری ترجیح می‌داده‌اند. برتری‌های پنهان نمودن داده بر رمزنگاری در کاربردهای امروزی نیز آشکار است؛ برای روشنی بیشتر تصور کنید که سفارتخانه‌ی یک کشور خارجی قصد دارد پیامی را به یک جاسوس ناشناس ارسال کند، در چنین حالتی اگر پیام را به صورت رمز درآورد، منابع اطلاعاتی به راحتی به هویت جاسوس پی می‌برند. یکی از مهمترین شاخه‌های پنهان‌سازی، نهان‌نگاری می‌باشد. در حالی که هدف از رمزنگاری محافظت از داده می‌باشد، در نهان‌نگاری هدف به طور خاص مخفی کردن وجود آن‌هاست. در نهان‌نگاری داده، هدف ارسال یک پیام و اطلاعاتی تحت پوشش ارسال یک داده‌ی بی‌ضرر می‌باشد. در این جا هدف اصلی داده‌ای است که پنهان شده است و اطلاعات پوششی دارای اهمیت نمی‌باشد. برخلاف نهان‌نگاری در واترمارکینگ، داده‌ی گنجانده شده به دلیل اهمیت بالای سیگنال میزبان می‌باشد، که با اهداف متفاوتی نظیر حفظ حق نشر، درستی و تمامیت داده، ره‌گیری مسیر انتشار و ... انجام می‌شود. در واقع تفاوت اصلی این دو روش در سیگنال دارای ارزش می‌باشد که در نخستین مورد، پیام گنجانده شده و در دیگری خود میزبان است که دارای ارزش می‌باشد.استگانوگرافی علم مخابره کردن اطلاعات است به گونه ای که اطلاعات ارسالی پنهان باشند .

واترمارکینگ یک تکنیک وروشی است که برای یک تغییر غیرقابل مشاهده در مورد یک اثر دیجیتالی مهم بکار میرود.اما استگانوگرافی یک تکنیک وروشی است که برای یک تغییرغیر قابل کشف درمورد یک

[1] Steganography
[2] Cryptography

اثر دیجیتالی غیر مهم بکارمیرود.تفاوت دیگر در مورد نوع پیام جاسازی شده است.در واترمارکینگ پیام در مورد خود اثر است اما در استگانوگرافی پیام ارتباطی به میزبان ندارد. هدف استگانوگرافی پنهان کردن پیام اصلی در کنار پیامهای معمولی و بی ضرر است، به طوریکه آگاهی از وجود پیام سری ممکن نباشد .استگانوگرافی و واترمارکینگ هر دو متعلق به نوعی پنهان کاری اطلاعات هستند ولی منظور و هدف و شرایط دو تکنیک کاملا متفاوت است .برای مثال در واترمارکینگ، داده مهم، همان داده بیرونی است که قابل مشاهده نیزهست.داده داخلی، داده اضافی برای محافظت از داده بیرونی است و برای اثبات حقوق صاحب اثربه کارمی رود. در حالیکه در استگانوگرافی داده داخلی خیلی مهم است و داده بیرونی (همان ظرف شامل شونده پیامها) خیلی مهم نیست ودرواقع فقط اطلاعات اصلی و مهم را حمل می کند.بامرور چند واقعه تاریخی میتوانیم به تفاوتهای واترمارکینگ واستگانوگرافی بهتر پی ببریم.

در قبل از میلاد یکی از فرماندهان یونان طی جنگی سخت به اسارت خشایار شاه ایران در می آید.فرمانده اسیر شده غلامی داشت.سرغلام خود را تراشید وپیغام مهمی را خالکوبی کرد. بعد از اینکه موهای غلام به اندازه کافی رشد کرد اورا عازم یونان کرد. حال اگر پیام خالکوبی شده مضمونی چنین داشت "این غلام از آن فرمانده سپاه یونان است " در واقع یک واترمارکینگ صورت گرفته بود امادر صورتی که پیام اصلا به غلام مربوط نمی شد، یک استگانوگرافی صورت پذیرفته بود.

در سال ۱۹۸۱ برخی اسناد رسمی ومحرمانه دولت انگلیس در روزنامه ها انتشار یافت.مارگارت تاچر برای اینکه شخص منتشر کننده این اسناد را پیدا کند تمام اسناد ومدارک را برای هر وزیر خود بایک فونت وفاصله کلمات خاص طوریکه با چشم قابل شناسایی نباشد منتشر کرد.وبدین ترتیب یک واترمارک برای هر سند ایجاد کرد.

از طرفی واترمارکینگ شبیه کریپتوگرافی نیز نیست . واترمارکینگ از دستیابی به اطلاعات و داده ها

نمی خواهد جلوگیری کند . در حالی که در کریپتوگرافی *cryptography* هدف کلی ،ایجاد پیامهای غیر مفهوم است تا از دستیابی اشخاص غیر مجاز بتواند جلوگیری کند .یک واترمارک برای این طراحی می شود که برای همیشه در سیگنال میزبان ساکن شود و اگر صاحب اثر و کار دیجیتال مورد سوال و ادعایی قرار گرفت اطلاعات می تواند مشخصات صاحب اثر را به طور کامل استخراج کند .مهمترین هدف استگانوگرافی این است که قابل تشخیص نباشد ودشمن برای بدست آوردن پیام ابتدا باید محیط انتقال وپوشش را شناسایی کند وسپس در صورت امکان پیام را استخراج کند.لذا کریپتوگرافی هم در واترمارکینگ وهم در استگانوگرافی کاربرد دارد.معمولا در همه روشها پیام ابتدا رمز نگاری شده وسپس جاسازی می شود تا در صورت کشف نیز غیر قابل فهم باشدکه در مورد استگانوگرافی این کار با شدت بیشتری انجام می شود. حفاظت از حقوق چاپ و نشر داده مولتی مدیا بوسیله الگوریتمهای کریپتوگرافی برای تامین بیشتر امنیت و جلوگیری از دستیابی وغیرقابل خواندن کردن کار برای کاربران غیرمجاز کامل تر شده است. هرچند که سیستمهای رمزگذاری شده نیز مشکل را کاملا حل نکرده اند و وقتی رمزگذاری کشف شد هیچ کنترلی برای پخش و انتشار داده نیست . مفهوم واترمارکینگ زمانی معلوم می شود که مشکلات وابسته به کپی رایت افراد در مدیای دیجیتالی حل شود. واترمارکینگ برای شناسایی صاحب یا پخش کننده داده دیجیتال مورد استفاده قرار می گیرد . واترمارکینگ می تواند بمعنی فرایند رمزگذاری پنهان اطلاعات کپی رایت نیز تلقی گردد.بطوریکه امروزه این امکان وجود دارد که پیامهایی در داخل صوت،تصویر، فیلم تنها با در نظر گرفتن محدودیتهای سیستم های صوتی و بینایی انسان پنهان شوند.

بعد از ارائه ی مقدمه ای مختصر به ذکر خواص و تقسیم بندی های مختلف واترمارکینگ خواهیم پرداخت. با توجه به اینکه هیچ مساله ای در دنیای مهندسی دارای کیفیت مطلق نیست، واترمارکینگ نیز ضعف هایی را دربردارد که این ضعف ها درمقابل حمله هایی که به صورت عمدی و یا غیر عمدی قصد از

میان بردن و یا خراب کردن واترمارک را دارند، بروز می دهد. لذا جنگ دیرینه ای بین روشهای مختلف پنهان کردن وتشخیص اطلاعات همچنان ادامه دارد وهردو در ابتدای راه خود قرار دارند.در قسمتهای بعدمختصری راجع به این حملات و دسته بندی های آن نیز بحث خواهد شد.

۱-۵- خواص واترمارکینگ

به منظور ارائه ی راهکارهایی برای مقایسه ی روش ها والگوریتم های گوناگون واترمارکینگ، نیازمند تعریف معیارهایی مشخص برای اندازه گیری کارایی یک روش واترمارکینگ نسبت به روشی دیگر داریم. این معیارها را در این بخش به عنوان خواص واترمارکینگ معرفی می کنیم. در این بخش شرایط لازم برای یک سیستم واترمارکینگ موثر معرفی می شود. شرایط به کاربرد وابسته است. اما برخی از آنها برای کاربردهای عملی یکسان و رایج است. یکی از عوامل موثر در رقابت بین محققان این زمینه همین شرایط است. یک روش واترمارکینگ دوست دارد که مورد استفاده در مقیاس بزرگ و عمومی نظیر یک دادگاه قرار گیرد. هیچ کدام از تکنیکهای دیجیتال هنوز همه شرایط را ندارند. در حقیقت سه شرط اول زیر می توانند یک مثلث را شکل دهند. بهبود یکی از رأسهای مثلث روی دوتای دیگر تأثیر می گذارد. به طور کلی برای واترمارکینگ می توان سه خاصیت مهم را برشمرد که عبارتند از:امنیت رویت ومقاومت. در ادامه به توضیح هر کدام از این خواص خواهیم پرداخت.

۱-۵-۱-امنیت:

یک الگوریتم واترمارکینگ بر اساس این فرضیه و احتمال که حمله کنندگان احتمالی فرآیند جاسازی واترمارک را نمی دانند، نمی تواند بنا شود. شکنندگی برخی محصولات تجاری بر اساس این چنین فرضیه ای است. نکته این جاست که بوسیله ایجاد تکنیک خیلی مقاوم و الگوریتم جاسازی همگانی و آشکار، در حقیقت الگوریتمهای پیچیده را برای حمله کنندگان به واترمارک کاهش می دهیم. در برخی تکنیکها از

تصویر مارک نشده اصلی در فرآیند استخراج استفاده می کنند. آنها از یک کلید مخفی برای تولید واترمـارک برای کارهای سری استفاده می کنند.

۱-۵-۲- رویت:

منظور از رویت بدان معناست که تصویر اصلی و تصویر واترمارک شده از نظر دید انسان هیچ تفاوتی با هم نداشته باشند.

الف) حس نکردن و درک نکردن واترمارک:

محققان سعی دارند واترمارک را به صورتی که مورد توجه قرار نگیرد پنهان کنند. هرچند که این کار بادیگر شرایط نظیر مقاومت که یک شرط مهم در صورت حمله است، مقابله می کند.برای ایـن منظـور مشخـصات سیستم بصری انسان HVS برای تصاویر و مشخصات سیستم صوتی انسان HAS برای سیگنال صوتی باید بررسی شود و در نظر گرفته شودو یااز افراد زیادی بخواهیم که به تصاویر نگاه کرده و به ما بگویند که کدام تصویر از آنها اصلی است و کدام تصویر اضافاتی به همراه خود دارد.

ب) به صورت آماری غیر قابل مشاده بودن:

با توجه به اینکه دیدن یک احساس بشری است و قدرت دید انسان ها و مقدار توجه آنها به بخش های مختلف یک اثر بصری با یکدیگر متفاوت است، بهترین معیارتشخیص اینکه یـک تـصویر واترمـارک شـده است یا اصلی، استفاده از روش های آماری است.درضمن یک شخص متخلف نبایـد واترمـارک را بوسـیله روشهای آماری آشکارسازی کند. برای مثال در دسترس بودن کارهای دیجیتال با تعداد زیاد که بـا یـک کـد یکسان واترمارک شده اند، اجازه استخراج مارک جاسازی شده بوسیله کارهای آماری را می دهد. البته یـک راه حل برای این کار استفاده از یک واترمارک برای هر اثرو کار دیجیتالی است.

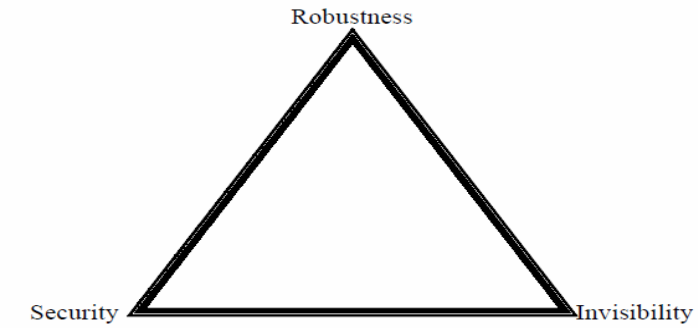
۱-۵-۳- مقاومت:

تصاویر دیجیتالی معمولا در معرض انـواع اعوجاجهـا و حملـه هـا نظیـر تـراکم و فـشردگی پـراتلاف، فیلترینگ، تغییر سایز، افزایش کنتراست، برشها، چرخشها و... قرار دارند. مارک باید حتی بعد از اینکه همـه این اعوجاجها رخ داد قابل آشکارسازی باشد.اگر واترمارک در قسمتهای مهم سیگنال تصویر جای داده شود مقاومت آن نیز در مقابل اعوجاجهای سیگنال بهتر خواهد بود. برای مثال یـک واترمـارک کـه در میـان داده های کم ارزش یک تصویر نهان است، در حالت فشردگی پر اتلاف ناجی و نجات دهنده نخواهد بود.علاوه بر اینها مقاومت کردن واترمارک در برابر دستکاریهای هندسی نظیر انتقال، تغییر سایز، چرخش یا برش هنوز یک مسئله مهم و مطرح است بویژه که این دستکاریهای هندسی خیلی معمول هستند. مقاومت بیانگر میـزان استقامت تصویر واترمارک در برابر حملات عمدی وغیرعمدی است، به نحوی که اطلاعات واترمارک حفظ شود. همانطور که در فصل اول بیان شد یکی از دلایل پیدایش الگوریتم های واترمارکینگ مقابله با اسـتفاده های غیر مجاز و تغییرات مجاز در اطلاعات دیجیتالی است. بنابراین به منظور کارایی این الگوریتم هـا مـی بایست قابلیت مقابله با حملات مختلف را در آنها لحاظ نمود. البته این بدان معنا نیست کـه یـک الگـوریتم زمانی کارا خواهد بود که در مقابل حملات مقاومت بیشتری داشته باشد، همانطور که در ادامه خواهـد آمـد در بعضی از کاربردها روش هایی مطرح شده اند که با کوچکترین تغییری در تصویر اطلاعات واترمـارک از میان خواهد رفت!

۱-۵-٤- ظرفیت:

منظور از ظرفیت میزان اطلاعات واترمارک است که ما می توانیم آن را در تصویر میزبان جاسازی کنیم. هر چه میزان این اطلاعات بیشتر باشد، قدرت مانور ما برای قرار دادن اطلاعات بیـشتر بنـا بـه کاربردهـای مختلف بیشتر خواهد بود. از طرف دیگر افزایش بیش از حد اطلاعات واترمارک سبب می شـود کـه میـزان

سطح روشنایی تصویر تغییرات بیشتری داشته باشد. این تغییرات در مواردی که قرار است تـصویر اصـلی و تصویر واترمارک شده از هم قابل تشخیص نباشد مناسب نیست.الگوریتم واترمارکینگ بایـد یـک تعـداد از بیتهای از پیش تعیین شده را در سیگنال میزبان جاسازی کند. این تعداد به کاربرد مورد نظر بستگی دارد هیچ



شکل ۱-۲- سه خاصیت مهم واترمارکینگ دیجیتال

قانونی برای این کار وجود ندارد. هرچند که در حالت تصویر حداقل ٤٠٠-۳۰۰ بیت باید در تصویرجاساز شود. به طور کلی تعداد بیتهایی که می تواند در داده مخفی شود محدود است.عاملی که میزان اطلاعات اضافه شونده را محدود می کند، طبیعت سیگنال اصلی والگوریتم به کار رفته برای جاسازی است.

۱-٦- رابطه ی خواص واترمارکینگ با یکدیگر:

همانطور که در بخش ظرفیت توضیح داده شد، خواص واترمارکینگ مفاهیمی مستقل نیستند و با افزایش و کاهش هر کدام از آنها می تواند بر روی خاصیتی دیگر اثر داشته باشد. بـه عنـوان مثـال افـزایش ظرفیـت واترمارکینگ سبب رویت پذیری بیشتر آن می شود و یا رویت پذیری واترمارک در تـصویر سـبب کـاهش مقاومت آن در مقابل حملات خواهد شد. بنابراین باید در طراحی یک الگوریتم در نظر داشت که کدام یـک از این خواص برای کاربرد مورد نظر ما کارایی بیشتری خواهد داشت تا به آن توجه بیشتری داشته باشیم.

نکته مورد توجه دیگر در زمینه ی خواص واترمارکینگ آنست که افزایش یا کاهش یک معیار به خـودی خود نشاندهنده ی مناسب بودن یا نامناسب بودن یک روش نیست. بلکه کاربرد مورد نظر مشخص می کنـد

که کدام خاصیت باید بیشتر باشد و کدام کمتر. مثلا در زمینه ی مقاومت در کاربردهایی که حفظ تصویر به طورکامل مورد نظر است، بهتر است که از روش های واترمارکینگ با مقاومت پایین استفاده کرد، چرا که هرگونه تغییری در تصویر سبب از میان رفتن واترمارک خواهد شد و گیرنده ی نهایی تصویر می تواند متوجه شود که تصویر اصلی است یا مورد تغییر قرار گرفته است.

۱-۷- نکاتی در مورد سیستم بینایی انسان

چشم انسان همانند یک فیلتر پایین گذر عمل می کند. به طوری که به تغییرات در فرکانس های پایین حساس است وبه راحتی آن را تشخیص می دهد. لذا در فشرده سازی معمولا فرکانس های بالا حذف می شوندوفرکانس های پایین تغییر کمی میکنند. سیستم بینایی انسان در نواحی از تصویر که روشنایی زیادویا کم باشد حساسیت کمتری نسبت به نویز از خود نشان می دهد. چشم انسان حساسیت کمتری نسبت به نویز در نواحی با بافت متراکم از خود نشان می دهد ودر این بین حساسیت بیشتری به نواحی نزدیک به لبه ها دارد.

۱-۸- طبقه بندی روش های واترمارکینگ

در این بخش به طبقه بندی روش های واترمارکینگ بر اساس خواص ذاتی این گونه الگوریتم ها میپردازیم. به طور کلی می توان از چند دیدگاه کلی به این الگوریتم ها نگاه کرد که بر این اساس روش های واترمارکینگ را به پنج دسته ی کلی تقسیم می کنیم:

۱-۸-۱- بینا ونابینا[1]

واترمارک ها را بر اساس نحوه استخراج شان دسته بندی می کنندکه شامل واترمارک های کور ونیمه کور وغیرکور بنابر بی نیاز بودن به داده های اولیه میزبان وعلامت، نیاز به تنها علامت ونیاز به داده میزبان به

[1] Noblind and Blind

ترتیب دسته بندی میشوند.چنانچه برای تشخیص واترمارک نهفته در تصویر اصلی بـه تـصویر میزبـان نیـاز باشد، الگوریتم مورد نظر در دسته ی بینـا و در صـورتی کـه بـه تـصویر اصـلی نیـازی نداشـته باشـیم، در دسته بندی نابینا قرار می گیرد. به طور کلی الگوریتم های بینا مقاوم تر از دسـته دیگـر هـستند، زیـرا بـرای تشخیص واترمارک می بایست تصویر اصلی در دسترس باشد، اما در بسیاری از کاربردها ما دسترسی به اثر اصلی نداریم و مجبوریم از روش نابینا استفاده کنیم.

۱-۸-۲- قابل مشاهده و غیر قابل مشاهده[1]

واترمارکینگ دیجیتال به دو بخش اصلی تقسیم می شود:واترمارک قابل مـشاهده و غیرقابـل مـشاهده.در صورتی که واترمارک نهفته شده در تصویر اصلی با چشم غیر مسلح قابل دیدن باشد قابل مشاهده و در غیر این صورت غیر قابل مشاهده نامیده می شود. فکر واندیشه ای که در پشت واترمارک قابل مـشاهده وجـود داردخیلی ساده است. این کار همانند مهرکردن یک برگه کاغذ است. به همین خاطر گاهی بـه آن مهـر زدن دیجیتالی نیز می گویند. برای مثال می توان به لوگو و آرم اضافه شده به گوشه تصویر تلویزیون کـه بوسـیله کانالهای تلویزیونی نظیر BBC ایجاد می شوداشاره کرد. یک روش قابل مشاهده ی خوب روشی است کـه افراد غیرمجاز قادر به از بین بردن و تغییر واترمارک نباشند. اما از آنجاییکه تغییر الگوهای قابـل مـشاهده در تصویر اصلی به سادگی صورت می گیرد ما همیشه باید این نکته را در نظر داشته باشیم کـه آیـا واترمـارک موجود اصلی است یا توسط افراد غیرمجاز مورد حمله قرار گرفته است.

اما واترمارکینگ غیرقابل مشاهده کمی پیچیده است. در بسیاری از موارد برای شناسایی حق چاپ داده، نظیر نام نویسنده، نام توزیع کننده و... مورد استفاده قرار می گیـرد. درمیـان تعـداد محققـانی کـه در حـوزه واترمارک های غیرقابل مشاهده کار کرده اند کمتر کسی پیدا می شود که برای واترمارک قابل مـشاهده نیـز

[1] Perceptible and Impeceptible

کار کرده باشد. واترمارکهای قابل مشاهده وغیرقابل مشاهده هردو برای دور کردن و بازداشتن از دزدی و سرقت به کار برده می شوند. اما هرکدام با روش های مربوط به خود این کار را انجام می دهند. برای اثبات حق صاحب اثر به صورت فوری وسریع واترمارک قابل مشاهده بسیار مفید است (Mintzer,Braudaway&Yeung 1997). مزیت اصلی آنها حذف ارزش تجاری اسناد بطور مجازی برای سازمان و متجاوزان است، بدون اینکه ارزش سند برای کارهای اصلی و مهم وقانونی از دست برود. اما واترمارکهای غیرقابل مشاهده در مرحله اول برای کمک برای بدست آوردن سارق و دزد است تا دلسردکردن سارق از دزدی (Mintzer 1997 , Swanson 1998).ازاین به بعد در بحثهایی که مطرح خواهند شد منظور از " واترمارک " همواره واترمارک غیرقابل مشاهده است مگر در جاهایی که علنا گفته شود. نکته مورد توجه آنست که در واترماکینگ های غیرقابل مشاهده واترمارک تنها به وسیله ی الگوریتم های خاص و به کمک کامپیوتر قابل بازیابی است.

۱-۸-۳- خصوصی و عمومی[1]

واترمارکینگ خصوصی نامیده می شود در صورتی که تنها افراد مجاز قادر به آشکارسازی و جاسازی واترمارک در تصویر میزبان باشند. به عنوان مثال تنها با داشتن یک کلید خصوصی می توان محل های قرار گیری واترمارک را در تصویر اصلی مشخص کرد و اقدام به بازیابی و یا تغییر آن نمود. در مقابل این الگوریتم ها روش های عمومی قرار دارند که محل قرار گیری واترمارک برای همه مشخص است. با توجه به نکات گفته شده روش های خصوصی از روش های عمومی مقاوم ترند. گونه ای دیگر از روش های عمومی که به روش های غیر مقارن معروفند نیز تعریف شده اند. در این گونه واترمارک برای همه قابل دسترسی است اما برای اطمینان از صحت واترمارک احتیاج به یک کلید عمومی و برای جایگذاری و یا از میان بردن واترمارک احتیاج به یک کلید خصوصی می باشد[۲۱].

[1] Private and Public

۱-۸-٤- مقاوم و شکننده[1]

همانطور که بیان گردید واترمارکینگ همواره در معرض حملات عمدی وغیر عمدی قرار دارد. درصورتی که واترمارک در مقابل حملات عمدی وغیر عمدی مقاوم باشد و از میان نرود و تغییر نکند مقاوم و در غیر این صورت شکننده نامیده می شود. البته دسته ای دیگر به نام نیمه شکننده نیز تعریف شده است که در چنین روش هایی واترمارک در مقابل حملات غیر عمدی نظیر عملیات پردازش تصویر مقاوم بوده ودر عوض در مقابل حملات غیر عمدی شکننده می باشد.در اثبات حق کپی رایت از نوع مقاوم استفاده می شودوبرای مواردی که می خواهیم از جزیی ترین تغییرات مطلع شویم به طور مثال در شناسایی تصاویر،از نوع شکننده استفاده می کنیم.در نوع سوم یک مقدار آستانه ای تعریف می شود که در صورتی که حمله از این حد بیشتر باشد واترمارکینگ شکسته می شود.

۱-۸-٥- حوزه مکانی و حوزه ی تبدیل[2]

در صورتی که روش های واترمارکینگ، اطلاعات واترمارکینگ را در میان مقادیر روشنایی تصویر میزبان قرار دهند در دسته بندی حوزه ی مکانی قرار می گیرند. در مقابل این روش ها روش هایی بر پایه ی حوزه ی تبدیل قرار دارند که در این گونه روش ها ابتدا با استفاده از یک تبدیل مثلا تبدیل فوریه اثردیجیتالی را به حوزه ی تبدیل برده و اطلاعات واترمارک را در لابلای تصویر تبدیل شده قرار داده و سپس تبدیل عکس می گیریم. روشن است که روش های بر مبنای حوزه ی مکانی دارای الگوریتم های ساده تری هستند و اطلاعات بیشتری قابل جاسازی کردن در تصویر اصلی است به طوری که در تصویر اصلی قابل تشخیص نباشد. در مقابل این مزایا چنین روش هایی مقاومت کمتری در برابر روش های بر پایه حوزه ی تبدیل دارند.دو گروه عمده از این روشها LSB-M(matching)و

[1] Robust and Fragile
[2] Spatial Domain and Transform Domain

LSB-F(flipping)هستند . در روشLSB-F داده مستقیما در بیت کم ارزش قرار داده می شود.اما در روش LSB-M در صورت عدم تطابق بیت کم ارز ش با داده مورد نظر ، مقدار پیکسل به صورت تصادفی یک واحد افزایش یا کاهش داده می شود. ظرفیت مناسب وعدم حساسیت چشم به تغییرات بیت کم ارزش از مزایای این دسته از روش هاست.البته روش هـای بـر مبنـای حـوزه تبـدیل دارای ظرفیـت پـایین تـر و پیچیدگی بیشتری هستند. روشهای مربوط به حوزه مکان استقامت کمتری در مقابل حملات حتی ساده ترین آنها دارند(انتقال چرخش وغیره).بنابراین اکثر پژوهشهای اخیربرروی حوزه تبدیل شامل تبدیل فوریه، تبدیل موجک، تبدیلDCT و...بوده است واین به این خاطر است که وقتـی از تـصویری تبـدیل معکـوس گرفتـه می شود، واترمارک به طور بی قاعده ای در طول تصویر پخش می شود، بنابر این خواندن واصلاح آن برای مهاجمان بسیار مشکل خواهد بود.روشهای جاسازی در حوزه مکان معمولا برای تصاویر BMPوروشـهای جاسازی در حوزه تبدیل برای تصاویر JPEGاستفاده می شود.

امروزه دسته ی دیگری از روش ها معرفی شده اند که قسمتی از الگوریتم جاسازی در حوزه ی مکـان و قسمتی دیگر در حوزه ی تبدیل صورت می گیرد. چنین روش هایی دارای تمام مزایاازقبیـل سـادگی روش، ظرفیت بالا و مقاومت بیشتر هستند.

۱-۹- کاربردهای واترمارکینگ دیجیتال

واترمارکینگ برای کارهای مختلفی مورد استفاده قرار می گیرد. همانطور که در بخش خواص واترمارکینگ گفته شد اولویت هر کدام از خواص واترمارکینگ بسته به کاربرد آن معین می شود. به همین دلیل در این بخش پنج دسته ی مهم از کاربردهای واترمارکینگ را بیان کرده و اولویت هر کدام از خواص واترمارکینگ را در آنها بررسی می کنیم.

۱-۹-۱-کاربردهای حفظ حق نشر[1]

یکی از مهمترین کاربردهای واترمارکینگ می باشد. در چنین کاربردهایی واترمارک هم می تواند شامل اطلاعاتی در رابطه با منبع و خالق اثر باشد و هم می تواند شامل اطلاعاتی درباره ی کاربر مجاز برای استفاده از تصویر باشد.با توجه به کاربرد ذکر شده چنین الگوریتم هایی می بایست تا آنجاییکه می توانند در مقابل حملات عمدی و غیر عمدی مقاوم بوده و اطلاعات واترمارک بدون تغییر حفظ شود. همچنین از نظر رویت نیز می بایست غیر قابل رویت باشد. از نظر ظرفیت محدودیت جدی وجود ندارد ولی هر چه ظرفیت بالاتر باشد بهتر است. ولی جنبه غیر قابل رویت بودن اهمیت بیشتری را دارد. از منظر دسته های طبقه بندی واترمارکینگ، روش ها می توانند بینا یا نابینا، حوزه زمانی یا حوزه ی تبدیل باشد. اما می بایست حتما رویت ناپذیر، خصوصی یا عمومی غیر متقارن و در نهایت مقاوم باشند.

کاربرد مهم دیگر در زمینه ی حفظ حق نشر، در تصاویر ویدئویی می باشد. از آنجاییکه امروزه قدرت پردازش کامپیوترها بالا آمده است، قابلیت استفاده از این روش ها در تصاویر ویدئویی نیز فراهم آمده است.

۱-۹-۲-کاربردهای تصدیق داده[2]

چون در راه انتقال اطلاعات ممکن است اطلاعات مورد حملات عمدی و یا غیر عمدی قرار گیرد و صحت اطلاعات در دسترس را مورد تردید قرار دهد از واترماکینگ برای تصدیق صحت استفاده می شود. روش کار بدین صورت است که اطلاعاتی به عنوان یک امضای دیجیتالی در میان داده های اصلی قرار داده می شود که نشاندهنده ی اصل بودن اثر می باشد. از نظر خواص در چنین کاربردهایی رویت پذیری چندان مساله ی مهمی نیست. مثلا امضای دیجیتال مورد نظر می تواند لوگوی مربوط به یک شرکت باشد که در

[1] Copyright Protection
[2] Data Authentication

پس زمینه ی صفحات قرار گرفته است. از نظر مقاومت هر چه واترمارک شکننده تر باشد بهتر است[۲۵]. چرا که ایجاد هر گونه تغییر در داده ی اصلی ممکن است سبب تغییرات گمراه کننده شود و اینجاست که شکننده بودن واترمارک سبب می شود که به ما نشان دهد که آیا داده های اصلی دستکاری شده است یا خیر. از نظر ظرفیت نیز هر چه ظرفیت بیشتر باشد قدرت انعطاف بیشتری خواهیم داشت. از منظر دسته های طبقه بندی واترمارکینگ، روش ها می توانند قابل مشاهده و یا غیرقابل مشاهده، حوزه ی زمانی و یا حوزه ی تبدیل باشند. اما می بایست حتما نابینا، خصوصی یا حداقل عمومی غیر متقارن بوده و ساختاری شکننده و در کاربردهای خاص نیمه شکننده باشند.

نکته مهم در چنین کاربردهایی آن است که قرار دادن اطلاعات امضا هر چند تاثیر اندکی را بر روی تصویر اصلی باقی می گذارد، اما در کاربردهایی نظیر تصاویر پزشکی و یا تصاویر نظامی حتی چنین تغییرات کوچکی نیز غیر قابل قبول خواهد بود.

۱-۹-۳-کاربردهای انگشت نگاری[1]

یکی از مهمترین شاخص های سیستم های تشخیص هویت استفاده از اثر انگشت می باشد. به همین دلیل حفاظت از دیتابیس های اثر انگشت افراد امری ضروری است. با استفاده از واترمارکینگ می توان در صورت توزیع غیر قانونی این اطلاعات منبع این سوءاستفاده را مشخص نمود. واترمارکینگ دیجیتال به منظور ردیابی مدرن سبب انتشار ساده و ارزان اثرهای دیجیتالی به صورت خیلی زیاد می شوند.در گذشته نیز تجاوز و دستبرد به اسناد دارای حق چاپ و تکثیر وجود داشت. اما اغلب بوسیله دستگاه فتوکپی و پخش آنها، این کار صورت می گرفت که کاری محدود و غیر عملی به حساب می رفت. به طور کلی واترمارکینگ دیجیتال این امکان را می دهد که هر عکس و تصویر یک مارک و آرم منحصر به فرد برای

[1] Fingerprinting

فروش داشته باشد (*finger printing*).اگر یک خریدار کپی غیر مجاز ایجاد کند از روی اثر کپی شـده، کپی کننده آشکار خواهد شد.

این دسته از کاربردهای واترمارکینگ را می توان زیر مجموعه ای از کاربرد های حفظ حق نشر دانـست، اگرچه در اینجا مساله حق مولف مطرح نیست اما هدف از واترمارکینگ قرار دادن اطلاعاتی مربوط به مالک داده ها و همچنین افراد مجاز به استفاده از اطلاعات می باشد. از نظر خواص واترمارکینگ در ایـن دسـته از کاربردها واترمارک رویت ناپذیر و مقاوم است و مانند کاربردهای قبلی ظرفیت بـالا قـدرت مـانور را بـرای ثبت اطلاعات واترمارک بالاتر می برد. از منظر دسته های طبقه بنـدی واترمارکینـگ، روش هـا مـی تواننـد حوزه ی زمانی یا حوزه ی تبدیلی باشند. اما می بایست حتما نابینا، رویـت ناپـذیر، خـصوصی یـا عمـومی نامتقارن و مقاوم باشند.

۱-۹-٤-کاربردهای کنترل کپی[1]

کپی برداری غیرقانونی از آثار هنری و استفاده از نسخه های کپی بـه جـای نـسخه هـای اصـل یکـی از مهمترین ضعف های استفاده از رسانه های دیجیتالی است. هر چند با استفاده از واترمارکینگ مـی تـوان بـه منبع انتشار غیرقانونی دست پیدا کرد، اما باز هم ضمانتی برای از میان رفتن ایـن گونـه سوءاسـتفاده هـا در مقیاس های کوچک و به صورت مستقل وجود ندارد. بنابراین استفاده از راهکاری سـخت افـزاری در ایـن میان امری ضروری به نظر می رسد؛ به طوری کـه هـیچ دسـتگاه ضـبط اطلاعـاتی اجـازه ی کپـی بـرداری غیرمجاز و هیچ دستگاه پخشی اجازه ی استفاده از نسخه های کپی را ندهد.

لابراتوار تحقیقاتی شرکت آی بی ام در توکیو[1] اولین بار در سال ۱۹۹٦ اقدام به ارائه راهکاری برای ایـن قفل سخت افزاری نمود. در این راهکار اطلاعات مربـوط بـه کنتـرل کپـی در میـان اطلاعـات اصـلی قـرار

[1] Copy Control

می گیرد و دستگاه ضبط و پخش تنها در صورت صحیح بودن ایـن اطلاعـات اقـدام بـه اجـرای دسـتورات کاربر می نمایند. البته هنوز راه درازی برای رسیدن به یک راهکار مناسب وجود دارد.

از نظر خواص واترمارکینگ در این دسته از کاربردها واترمارک رویت ناپـذیر و شـکننده اسـت و ماننـد کاربردهای قبلی ظرفیت بالا قدرت مانور را برای ثبت اطلاعات واترمارک بالاتر می برد. از منظر دسته هـای طبقه بندی واترمارکینگ، روش ها می توانند حوزه ی زمانی یا حوزه ی تبدیلی باشند. اما می بایست حتمـا نابینا، رویت ناپذیر، خصوصی یا عمومی نامتقارن و شکننده باشند.

۱-۹-۵-کاربردهای ارتباطات پنهانی[۲]

امنیت مخابرات در کاربردهایی نظیر کاربردهای نظامی مساله ی مهمی است. به دلیل ایمن نبـودن کانـال های ارتباطی اطلاعات می بایست به صـورت رمـز ارسـال شـوند. یکـی از راهکارهـای بـه رمـز درآوردن اطلاعات استفاده از واترمارکینگ است. در این جا تصویر میزبان برای گیرنده مهـم نبـوده و تنهـا اطلاعـات واترمارک است که مورد توجه قرار می گیرد. از نظر خواص واترمارک رویت ناپذیر و مقاوم بوده و ظرفیت می بایست بسیار بالا باشد. از منظر دسته بندی نیز، این روش ها می توانند بینا یا نابینـا، حـوزه ی زمـانی و یاحوزه ی تبدیلی باشند. اما می بایست حتما غیرقابل مشاهده، خصوصی و مقاوم باشند.

۱-۱۰- حملات و دسته بندی آنها

تاکنون الگوریتم های متعددی برای واترمارکینگ ارائه شده اند که هر کدام از این الگوریتم ها به منظـور برآوردن نیازهایی خاص طراحی شده اند. اما آنچه که برای ما یک الگوریتم را الگوریتمی کـارا معرفـی مـی کند، توانایی الگوریتم مذکور در برابر معیارهایی مشخص است که ایـن معیـار در واترمارکینـگ بـه عنـوان حملات شناخته می شود. واترمارک و حمله به واترمارک دوسوی یک سکه هـستند. هـدف هـر دوی آنهـا

[1] IBM Tokyo Research Laboratory(TRL)
[2] Cover communication

حفظ داده دیجیتال است. هدف واترمارک مقاومت در برابر حمله است ولی نـه بـه انـدازه ای کـه سـبب از دست دادن مقدار و ارزش داده حفاظت شده شود.از طرف دیگر هدف حملـه نیـز از بـین بـردن واترمـارک بدون از دست دادن مقدار و ارزش داده حفاظت شده است. حملات در واترمارکینگ انواع گوناگونی دارند، ولی به طور کلی می توان حملات را به دو دسته ی عمدی وغیر عمدی تقسیم نمود. در ایـن قـسمت بـه معرفی برخی حملات متداول میپردازیم. همان طور که گفته شد حملات انواع گوناگونی دارد. در بخش قبل حملات را به دو دسته ی عمدی و غیرعمدی تقسیم نمودیم. اما حملات را می توان به طـرق دیگـری نیـز تقسیم بندی نمود. در این بخش به بررسی حملات در سه دسته ی کلی می پردازیم.

۱-۱۰-۱-حملات پردازش تصویر[1]

حملات پردازش تصویر به چهار دسته ی فیلتر کردن، ریمدولاسیون، فشرده سازی جِی پِگ و فشرده سازی جِی پِگ ۲۰۰۰ تقسیم می شود.

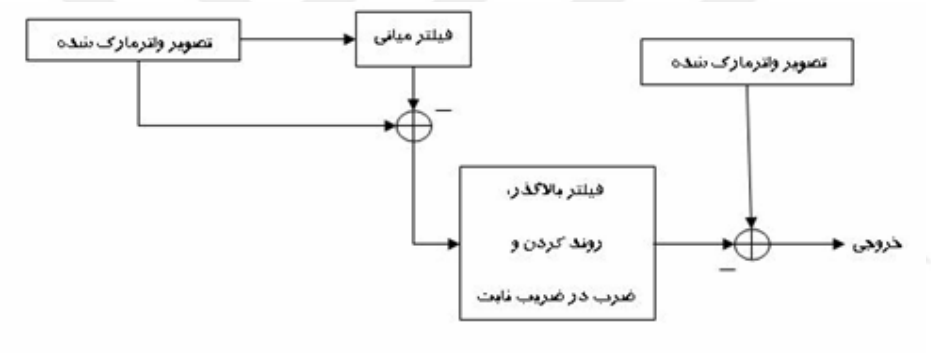
۱-۱۰-۱-۱- فیلتر کردن[2]

فیلتر کردن از آن دسته از عملگرهایی است که در حوزه ی فرکانس[3] عمل می کند. بدین معنا که ابتدا از تصویر تبدیل فوریه گرفته می شود، سپس تبدیل فوریه ی تصویر از فیلتر مورد نظر عبور داده می شود. فیلترها انواع گوناگونی دارند. مثلا اگر از فیلتر پایین گذر استفاده کنیم و از طرف دیگر اطلاعات واترمارک را در فرکانس های بالا بگنجانیم، بدیهی است که اطلاعات واترمارک را از دست خواهیم داد. به عبارت دیگر می توانیم بگوییم که فلان الگوریتم واترمارکینگ که واترمارک را در مولفه های فرکانس بالای تصویر قرار می دهد در برابر حملات ناشی از فیلتر پایین گذر مقاوم نیست.

[1] Image Processing Attack
[2] Filtering
[3] Frequently Domain

۱-۱۰-۱-۲- ریمدولاسیون[1]

این حمله برای اولین بار توسط لانگلار بیان شد. ساختار این حمله بدین صور است که ابتدا تصویر واترمارک شده از یک فیلتر میانی[2] عبور داده می شود، حاصل از تصویر واترمارک شده کم می شود. تصویر حاصل را به عنوان یک پیشگویی از واترمارک در نظر گرفته می شود. واترمارک پیشگویی شده پس از عبور از یک فیلتر بالاگذر و روند شدن، در یک ضریب ثابت ضرب شده و از تصویر واترمارک شده کم می شود. در بلوک دیاگرام(۱-۳) مراحل ذکر شده، آمده است.



شکل(۱-۳):بلوک دیاگرام حمله ریمدولاسیون

۱-۱۰-۱-۳- فشرده سازی جِی پِگ[3]

فشرده سازی جِی پِگ یکی از متداول ترین روش های فشرده سازی است که در سال ۱۹۸٦ تولید و در سال ۱۹۹۲ انتشار یافت و موسسه بین المللی استاندراد این روش را در سال ۱۹۹٤ پذیرفت. فشرده سازی جِی پِگ قادر است سایز تصویر را به ۵٪ مقدار معمول آن کاهش دهد و این امر به کمک صفر کردن ضرایب کم ارزش تبدیل کسینوسی گسسته صورت می پذیرد.

۱-۱۰-۱-٤- فشرده سازی جِی پِگ ۲۰۰۰

[1] Remodulation
[2] Median Filter
[3] JPEG(Joint Photographic Expert Group)

کمیته ی جِی پِگ به منظور حل مشکلات بلوک بلوک شدن ناشی از استفاده از تبدیل کسینوسی، روش دیگری را بنیان نهاد که بر اساس تبدیل موجک[1] عمل می نمود و با وجود ارائه نرخ فشرده سازی بالاتر اثرات بلور شدن[2] و بلوک شدن را ندارد و در کاربردهای پزشکی، صنعتی و استفاده در اینترنت به کار می رود.

۱-۱۰-۲- حملات تبدیلات هندسی[3]

حملات تبدیلات هندسی انواع گوناگونی دارد که دراینجا به نُه مورد از آنها اشاره می شود.

۱-۱۰-۲-۱- مقیاس گذاری[4]

همانطور که از نام این اثر نیز پیداست این حمله ناشی از تغییر سایز تصویر می باشد. به عنوان مثال با نصف کردن طول تصویر و رساندن عرض تصویر به یک سوم مقدار اصلی آن و انجام دادن عمل عکس به کمک الگوریتم های درونیابی، سایز تصویر به همان اندازه ی اصلی خواهد بود، اما بدیهی است که به دلیل تقریب های درونیابی مقادیر پیکسل ها تغییر خواهد نمود.

۱-۱۰-۲-۲- چرخش[5]

رابطه ی چرخش برای هر پیکسل در رابطه زیر آمده است. با توجه به آنکه مقادیر پیکسل ها باید مقدار صحیح داشته باشد، بعد از عمل چرخش مقادیر پیکسل ها را می بایست روند نمود. بنابراین با انجام یک چرخش ۳۰ درجه ای در جهت عقربه های ساعت و سپس انجام یک چرخش ۳۰ درجه ای بر خلاف جهت عقربه های ساعت، مقادیر پیکسل ها با مقادیر اولیه متفاوت خواهد بود.

---

[1] Wavelet
[2] Blurring
[3] Geometric Transform Attacks
[4] Scaling
[5] Rotation

$$[X'Y'] = [X\ Y]\begin{bmatrix} Cos\theta & Sin\theta \\ -Sin\theta & Cos\theta \end{bmatrix} \quad (۱-۱)$$

۱-۱۰-۲-۳- بریدن[1]

بریدن سبب می شود که بخشی از اطاعات مربوط به واترمارک از میان رود. در چنین مواردی برای تشخیص واترمارک می توان قسمت های بریده شده از تصویر واترمارک شده را با معادل واترمارک نشده ی آن جانشین نمود.

۱-۱۰-۲-٤- تبدیلات خطی[2]

رابطه ی کلی تغییر مقادیر پیکسل ها به کمک تبدیلات خطی به صورت رابطه زیر می باشد. اثر منفی این تبدیلات در روند کردن نهایی مقادیر پیکسل ها می باشد.

$$[X'\ Y'] = [X\ Y]\begin{bmatrix} T_{11} & T_{12} \\ T_{21} & T_{22} \end{bmatrix} \quad (۲-۱)$$

۱-۱۰-۲-٥-خمش[3]

این حمله اولین بار توسط پتیکلاس مطرح شد و شامل مجموعه ای از اعمال تبدیلات غیرخطی، درونیابی، افزودن نویز وفشرده سازی بر روی تصویر می باشد.

۱-۱۰-۲-٦-پیچش[4]

بیان کننده ایجاد تغییرات موج گونه بر روی تصویر می باشد.

۱-۱۰-۲-۷-تصویر سه بعدی[5]

به طور کلی در تصاویر سه بعدی خطوط موازی در بی نهایت به هم می رسند و اندازه ی اشیا بر اساس

[1] Clipping
[2] Linear Transform
[3] Bending
[4] Petitocolas
[5] Prespictive Projection

میزان فاصله ی آنها از مرکز تصویر کوجکتر می شود. این حمله بیانگر اعمال چنین تغییراتی در تصویر می باشد.

۱-۱۰-۲-۸-ترکیب تصاویر[1]

این حمله برای اولین بار توسط هولیمن معرفی شد. ترکیب تصاویر به معنای استفاده از چندین تصویر واترمارک شده و ترکیب بخش هایی از هر تصویر و تشکیل یک تصویر جدید با توجه به محل قرارگیری آنها در تصاویر اولیه می باشد.

۱-۱۰-۲-۹-استفاده از الگو[2]

استفاده از الگوها یکی از روش های مدرن واترمارکینگ است. اساس این روش ها بر مبنای واترمارکینگ در حوزه ی فرکانس می باشد. در اینگونه روش ها بعد از گرفتن تبدیل از تصویر اصلی با استفاده از الگویی خاص واترمارک را در داخل مولفه های تصویر قرار می دهند. می توان با استفاده از الگوهای از پیش تعیین شده، واترمارک گنجانده شده در چنین تصاویری را استخراج نمود.

۱-۱۰-۳- حملات رمزگذاری[3]

چنین حملاتی مشابه حملاتی هستند که در رمزنگاری با آنها روبرو هستیم. تنها تفاوت در اینجا مقصود حمله کننده است. حملات رمز گذاری سعی در کشف کلید های عمومی وخصوصی جاسازی واترمارک را دارند.

[1] Collage
[2] Template
[3] Cryptography Attack

فصل دوم

روش تحقیق

۲-۱- مراحل واترمارکینگ:

هر چند که واترمارکینگ را می توان در حوزه های گوناگون اطلاعات دیجیتال به کاربرد، اما دراین رساله توجه خود را به واترمارکینگ بر روی تصاویر دیجیتال معطوف می نماییم. دو مرحله اساسی در فرآیندواترمارکینگ قابل بحث است:

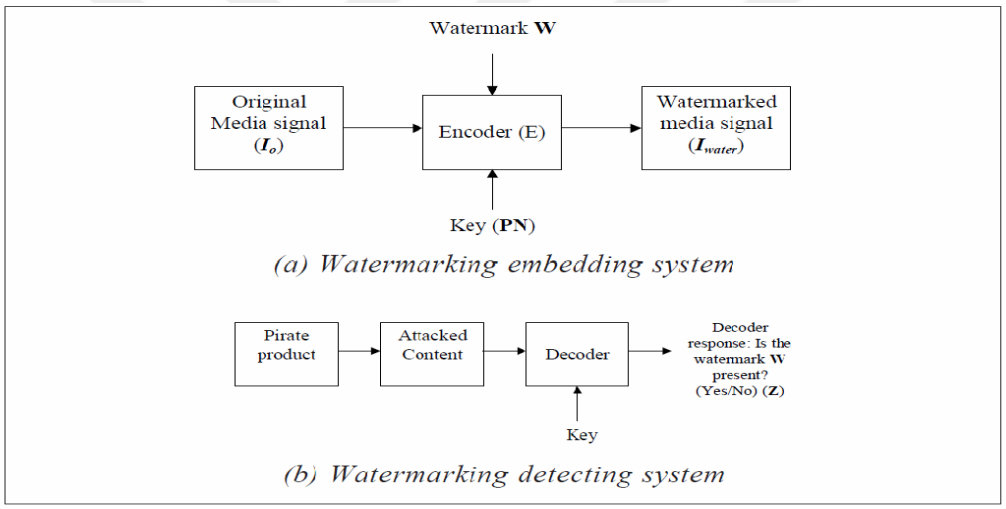
۱-قراردادن[۱] واترمارک[۲] در تصویرمیزبان(جاسازی واترمارک[۳])

۲-استخراج واترمارک[٤]

در مرحله ی اول واترمارک مورد نظر را در تصویر مورد نظر قرار می دهیم. این واترمارک هم می تواند در پس زمینه ی تصویر میزبان قابل رویت باشد و هم می تواند به گونه ای مخفی قرار گیرد که سیستم بینایی انسان[۵] قادر به تشخیص نباشد. یک تصویر بدون دیده شدن واترمارک و از دست دادن کیفیت وبدون بستگی داشتن به نوع فرمت تصویر،براحتی می تواند مارک شود.برای مثال یک تصویر bitmap (BMP) می تواند با فشرده شدن به تصویر JPEG تبدیل شود. نتیجه، یک تصویری است که مقداری فضای داخلی از دست داده ولی نمی توان از تصویر اصلی متمایزش کرد. معمولا یک فشرده سازی JPEG تا سطح ۷۰٪ به گونه ای است که از دید سیستم بینایی انسان پوشیده می ماند. همین خصوصیت تصاویر دیجیتال است

[1] Embedding
[2] Watermark
[3] Watermarking Embedding
[4] Watermarking Extraction
[5] Human Visual System(HVS)

که اجازه جاسازی و تعبیه داده اضافی را در تصویر فراهم می کند که کیفیت تصویر تغییر نکند. پیام در فضای مجازی بی استفاده وخالی تصویر مخفی می شود و در زیر آستانه حس بینایی انسان باقی می ماند. در مرحله ی بعدی که در واقع می توان آن را فرآیند آشکارسازی نیز نامید، واترمارک مورد نظر از داخل تصویر میزبان استخراج می شود. البته این استخراج به معنای بازیابی کلیه ی اطلاعات واترمارک نیست. گاهی تشخیص اینکه تصویر مورد نظر دارای اطلاعاتی غیر از اطلاعات اصلی خود تصویر است، برای مقصود ما کافی خواهد بود.



شکل(۲-۱)فرآیند واترمارکینگ

فرآیند عملیات جاسازی و آشکار سازی به شرح زیر انجام می گیرد:

I_{orig} را سیگنال مولتی مدیای اصلی (یک تصویر – یک صوت یا یک ویدیو) قبل از واترمارکینگ تعریف می کنیم. W را واترمارکی که صاحب حق و چاپ و نشر دوست دارد در اثرش جاسازی شود تعریف می کنیم و I_{water} را سیگنال واترمارکی شده تعیین می کنیم.

بلوک دیاگرام شکل(۲-۱) شمای کلی فرایند واترمارکینگ را نشان می دهد. واترمارک W که رمزگذاری نیزشده داخل I_{orig} با استفاده از تابع جاسازی E، جاسازی شده است. تابع جاسازی تغییرات کوچکی در

I_{orig} با توجه به W ایجاد می کند. برای مثال اگر:

$$E(I_{orig}, W) = I_{water} \qquad (۱-۲)$$

$$W = (W_1, W_2, ...)$$

عملیات جاسازی ممکن است شامل جمع یا منها کردن یک مقدار کم α از هر پیکسل یا نمونه از I_{orig} باشد. درمرحله دوم از یک سیستم واترمارکینگ، تابع آشکارساز D با استفاده از W و گاهی I_{orig} یک W' از سیگنال R استخراج می کند.

$$D(R, I_{orig}) = W' \qquad (۲-۲)$$

سیگنال R همان سیگنال I'_{water} است و می توان گفت یک صورت (ورژن) از I_{water} که برای از بین بردن واترمارک آن تلاش شده است وبه اصطلاح مورد حمله قرارگرفته است. سیگنال R ممکن است یک سیگنال بی ربط و ناوابسته نیز باشد. سری W' استخراج شده با W مقایسه می شود تا تعیین گردد که R واترمارک شده است یا نه. مقایسه معمولا بر اساس یک ضریب همبستگی و یک آستانه به ترتیب λ_0, P صورت می گیرد. این دو برای ایجاد یک تقسیم باینری Z که آیا سیگنال واترمارک شده یا نه استفاده می شود. برای چک کردن همسانی و شباهت W , W' ضریب همبستگی بین آنها می تواند بر اساس رابطه زیر محاسبه شود:

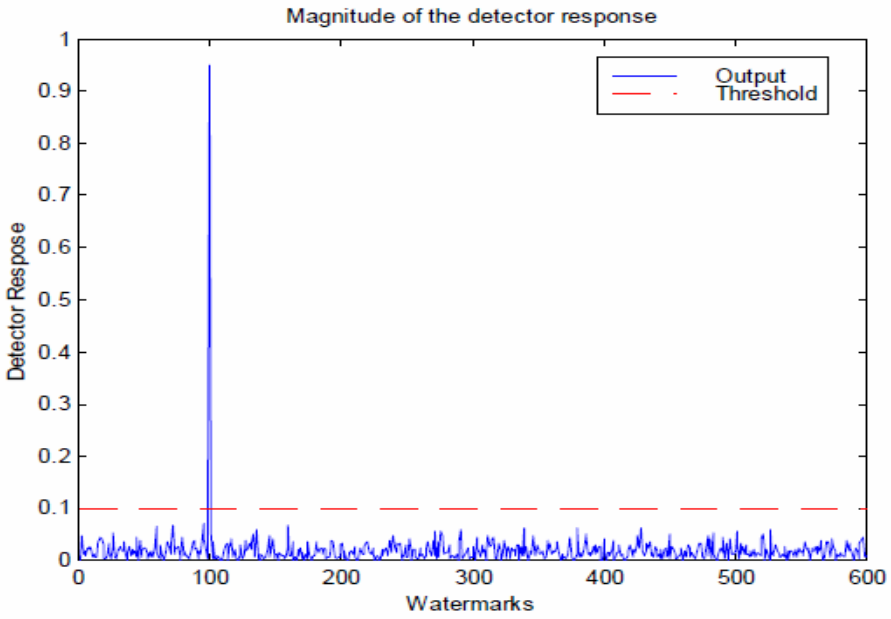
$$P = (W, W') = \frac{W.W'}{\sqrt{W'.W'}} \qquad (۳-۲)$$

که همان ضرب اسکالر بین این دو بردار W , W' است.

اما تابع تصمیم گیری برابر است با:

$$Z(W', W) = \begin{cases} 1 & P \geq \lambda_0 \\ 0 & otherwise \end{cases} \qquad (٤-۲)$$

که p مقدار همبستگی و λ_0 آستانه است.مقدار یک در این رابطه نشان دهنده این است که آشکار سازی واترمارک صورت گرفته و صفر یعنی آشکارسازی صورت نگرفته است. به عبارت دیگر اگر W , W' به قدر کفایت وابسته باشند (بزرگتر از λ_0) محقق می شود که سیگنال R شامل واترمارک است و حق صاحب اثر سیگنال تأیید می شود. در غیر اینصورت صاحب واترمارک w هیچ حق و حقوقی روی سیگنال R ندارد.شکل (۲-۲) آستانه آشکارسازی ۶۰۰ سری واترمارک تصادفی مطالعه شده را نشان می دهد که فقط یکی از واترمارکها بطور معنی دار خروجی همبستگی بالایی نسبت به بقیه دارد.



شکل(۲-۲):استخراج بیت واترمارک ازمیان ۶۰۰ بیت

یک مثال برای واترمارکینگ:

با یک مثال ساده فرآیند اساسی واترمارکینگ را دراینجا مطرح می کنیم. در تصویر میزبان، اولین بلوک تصویر درختان ۸×۸ پیکسل در شکل ۵ دیده می شود. تبدیل گسسته کسینوسی *DCT* به کار برده شده است.

شکل(۲-۳):تصویزدرختان بهمراه اولین بلوک ۸*۸

$$B_1 = \begin{bmatrix} 0.7232 & 0.8245 & 0.6599 & 0.7232 & 0.6003 & 0.6122 & 0.6122 & 0.5880 \\ 0.7745 & 0.7745 & 0.7745 & 0.7025 & 0.7745 & 0.7025 & 0.7745 & 0.7025 \\ 0.7745 & 0.7745 & 0.7025 & 0.7745 & 0.7745 & 0.7025 & 0.7025 & 0.7025 \\ 0.7025 & 0.7025 & 0.7025 & 0.7025 & 0.7025 & 0.7745 & 0.7025 & 0.7025 \\ 0.7745 & 0.7025 & 0.7745 & 0.7025 & 0.7025 & 0.7025 & 0.7025 & 0.7025 \\ 0.7025 & 0.7025 & 0.7025 & 0.7745 & 0.7025 & 0.7745 & 0.7025 & 0.7025 \\ 0.7025 & 0.7745 & 0.7025 & 0.7025 & 0.7745 & 0.7025 & 0.7745 & 0.7025 \\ 0.7025 & 0.7025 & 0.7745 & 0.7745 & 0.7745 & 0.7025 & 0.7025 & 0.7025 \end{bmatrix}$$

با *DCT* گرفتن از *B1* داریم:

$$DCT(B_1) = \begin{bmatrix} 5.7656 & 0.1162 & -0.0379 & 0.0161 & -0.0093 & -0.0032 & -0.0472 & -0.0070 \\ -0.0526 & 0.1157 & 0.0645 & 0.0104 & -0.0137 & -0.0114 & -0.0415 & -0.0336 \\ -0.0354 & 0.0739 & -0.0136 & -0.0410 & -0.0081 & -0.0187 & -0.0871 & 0.0063 \\ -0.0953 & 0.0436 & 0.0379 & -0.0090 & -0.0394 & 0.0182 & -0.0031 & -0.0589 \\ -0.1066 & 0.0500 & 0.0034 & -0.0355 & -0.0093 & 0.0147 & 0.0526 & -0.0278 \\ -0.0790 & -0.0064 & 0.0088 & 0.0240 & -0.0200 & -0.0361 & -0.0586 & -0.0731 \\ -0.0422 & 0.0366 & -0.0460 & -0.0150 & 0.0518 & 0.0141 & 0.0105 & -0.0980 \\ 0.0025 & 0.0697 & 0.0327 & -0.0140 & 0.0286 & -0.0084 & -0.0422 & 0.0329 \end{bmatrix}$$

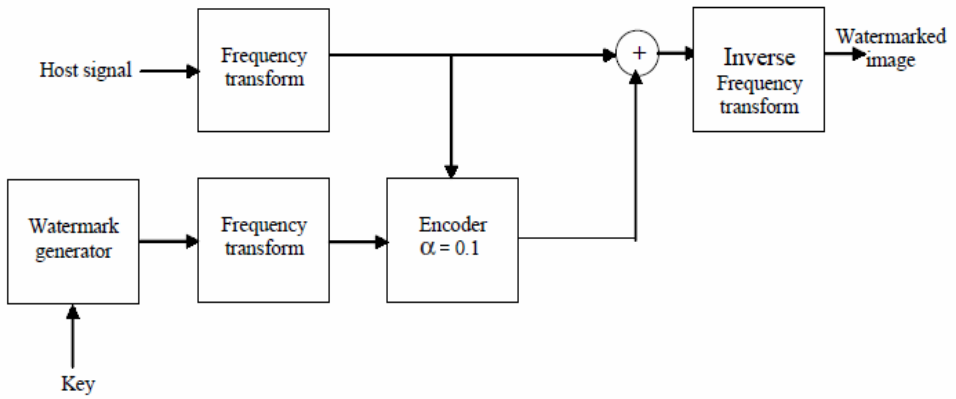
در *DCT(B1)* بیشترین انرژی روی مقدار *DC* متمرکز شده است(۵/۷۶۵۶ = ضریب DC).

واترمارک یک سری حقیقی *pseudo-random* است که از یک منبع تصادفی ویک مقداراصلی(کلید)سرچشمه گرفته است.

$$W = \begin{bmatrix} 1.6505 & 0.2759 & -0.8579 & -1.6130 & -1.0693 & 0.2259 & -0.4570 & 0.7167 \\ 0.7922 & -0.6320 & 0.8350 & -0.3888 & 0.4993 & 0.2174 & -1.6095 & -0.9269 \\ 0.7319 & 0.7000 & 1.6191 & -0.0870 & 0.7859 & 0.1870 & -0.3633 & 2.5061 \\ 0.9424 & 0.8966 & -0.0246 & -1.4165 & 0.5422 & 0.1539 & -1.1958 & 0.0374 \\ 0.2059 & 1.8204 & 0.5224 & -0.9099 & -1.6061 & -0.7764 & -0.8054 & -1.0894 \\ -0.1303 & -0.3008 & 1.6732 & -1.1281 & -0.3946 & 0.8294 & -0.0007 & -0.7952 \\ 0.0509 & -1.7409 & 1.1233 & 0.3541 & 0.1994 & -0.0855 & 0.1278 & -0.6312 \\ -0.1033 & -1.7087 & 0.5532 & 0.2068 & 2.5359 & 1.7004 & -0.6811 & -0.7771 \end{bmatrix}$$

با DCT گرفتن از w داریم:

$$DCT(W) = \begin{bmatrix} 0.2390 & 1.5861 & 0.1714 & 0.7187 & -0.3163 & -1.0925 & 2.6675 & 1.3164 \\ 0.1255 & 0.8694 & 2.8606 & -0.2411 & 0.6162 & -1.1665 & -0.1335 & -0.8266 \\ 0.0217 & -1.4093 & -1.3448 & 1.3837 & 1.3513 & 1.0022 & 0.8743 & 0.3735 \\ -1.7482 & 0.8337 & 1.5394 & -0.0076 & -1.7946 & 1.1027 & -0.4434 & -0.5771 \\ -0.7653 & 0.5313 & 0.9799 & 1.2930 & -0.0309 & -0.9858 & -0.9079 & -0.8152 \\ 0.4222 & -0.9041 & 1.2626 & -0.0979 & 0.6200 & 0.1858 & -0.1021 & 0.1452 \\ 1.4724 & -1.1217 & 0.7449 & -0.2921 & -0.3144 & -0.7244 & 0.4119 & 0.0535 \\ 0.4453 & 0.0380 & 0.9942 & -1.5048 & 0.0656 & 0.4169 & -0.7046 & -0.5278 \end{bmatrix}$$



شکل(۲-۴):بلوک دیاگرام فرایندواترمارکینگ

B_1 بوسیله w واترمارک شده است این کار در بلوک دیاگرام نشان داده شده است که براساس رابطه زیر است:

$$f_w = f + \alpha . w . f \qquad (۵-۲)$$

که f ضرایب DCT سیگنال میزبان B_1 و w ضرایب DCT سیگنال واترمارک و انرژی واترمارکینگ که برابر $\alpha = 0/1$ است. مقدار DC سیگنال میزبان تغییر نمی کند. این کار به خاطر کمتر کردن اعوجاج تصویر واترمارک شده است.بنابراین مقدار DC واترمارک نشده باقی می ماند. معادله فوق را به صورت فرمت ماتریس نیز می توان نوشت:

$$DCT(B_{1W}) = \begin{cases} DCT(B_1) + \alpha \cdot DCT(W) \cdot DCT(B_1) & for\ all\ \text{coefficient}\ except\ DC\ value \\ DCT(B_1) & for\ DC\ value \end{cases}$$

توجه کنید که مقدار DC تصویر واترمارک شده برابر همان مقدار واترمارک شده در حالت DCT نیز است.

برای تشکیل و ایجاد تصویر واترمارک شده، معکوس DCT آرایه دو بعدی بالا محاسبه می شود.

$$DCT(B_{1w}) = \begin{bmatrix} 5.7656 & 0.1346 & -0.0386 & 0.0172 & -0.0090 & -0.0028 & -0.0598 & -0.0079 \\ -0.0532 & 0.1258 & 0.0830 & 0.0101 & -0.0145 & -0.0101 & -0.0409 & -0.0308 \\ -0.0355 & 0.0635 & -0.0117 & -0.0467 & -0.0092 & -0.0206 & -0.0947 & 0.0066 \\ -0.0786 & 0.0472 & 0.0438 & -0.0090 & -0.0323 & 0.0202 & -0.0029 & -0.0555 \\ -0.0984 & 0.0527 & 0.0037 & -0.0400 & -0.0092 & 0.0132 & 0.0478 & -0.0255 \\ -0.0823 & -0.0058 & 0.0099 & 0.0238 & -0.0212 & -0.0368 & -0.0580 & -0.0742 \\ -0.0485 & 0.0325 & -0.0494 & -0.0146 & 0.0502 & 0.0131 & 0.0109 & -0.0985 \\ 0.0026 & 0.0700 & 0.0360 & -0.0119 & 0.0288 & -0.0088 & -0.0392 & 0.0312 \end{bmatrix}$$

$$B_{1w} = \begin{bmatrix} 0.7331 & 0.8361 & 0.6609 & 0.7228 & 0.5991 & 0.6026 & 0.6175 & 0.5922 \\ 0.7818 & 0.7809 & 0.7735 & 0.7011 & 0.7712 & 0.6955 & 0.7755 & 0.6998 \\ 0.7734 & 0.7746 & 0.6973 & 0.7682 & 0.7663 & 0.7002 & 0.6956 & 0.6920 \\ 0.7064 & 0.7093 & 0.7045 & 0.7037 & 0.7013 & 0.7692 & 0.6986 & 0.6933 \\ 0.7872 & 0.7100 & 0.7789 & 0.7081 & 0.7067 & 0.7012 & 0.7013 & 0.6996 \\ 0.7051 & 0.7032 & 0.7026 & 0.7801 & 0.7078 & 0.7741 & 0.7015 & 0.6978 \\ 0.7017 & 0.7765 & 0.7002 & 0.7067 & 0.7765 & 0.7026 & 0.7736 & 0.6992 \\ 0.6877 & 0.7048 & 0.7712 & 0.7800 & 0.7793 & 0.7001 & 0.7044 & 0.6974 \end{bmatrix}$$

براحتی می توانیم B_{1W} , B_1 را مقایسه کرده و تغییرات جزئی را که سبب واترمارک شده اندرا ببینیم.

۲-۲- بررسی چند الگوریتم نابینای متداول واترمارکینگ

همانطور که گفته شد یک سیستم واترمارکینگ از دو قسمت قرار دادن واترمارک و استخراج واترمارک تشکیل شده است. در هر کدام از روش های زیر نحوه ی عمل این دو قسمت شرح داده شده است. در روش های ارائه شده c_o به معنای تصویر اصلی و c_w به معنای تصویر واترمارک شده می باشد.

۲-۲-۱-روش اول: واترمارکینگ نابینا و آشکارسازی به کمک ضرایب همبستگی[1]

در این روش ابتدا یک الگوی ثابت (w_r) برای جاسازی در نظر گرفته می شود. با فرض یک بیتی بودن پیغام واترمارک، ضریبی از w_r به عنوان بیت یک و ضریبی از $-w_r$ به عنوان بیت صفر در نظر گرفته می شود. بنابه توضیحات داده شده رابطه ی(۲-٦) قابل بیان است.

$$w_m = \begin{cases} w_r & if\ m = 1 \\ -w_r & if\ m = 0 \end{cases} \qquad (٦-٢)$$

$$w_a = \alpha w_m$$

$$c_w = c_o + w_a$$

ضریب α در اینجا با مقاومت و رویت پذیری داد و ستد[2] دارد. در این روش آشکارسازی با فرض آنکه تنها نویز گوسی در سیستم موجود است، به کمک ضرایب همبستگی صورت می گیرد. وظیفه ی آشکارساز[3] در اینجا تشخیص وجود الگوی w_r در تصویر می باشد. بدین منظور همبستگی میان تصویر دریافت شده و الگوی w_r محاسبه می شود:

$$corr\ (c, w_r) = \frac{1}{N} c.w_r = \frac{1}{N} \sum_{x,y} c[x, y] w_r[x, y] \qquad (۷-۲)$$

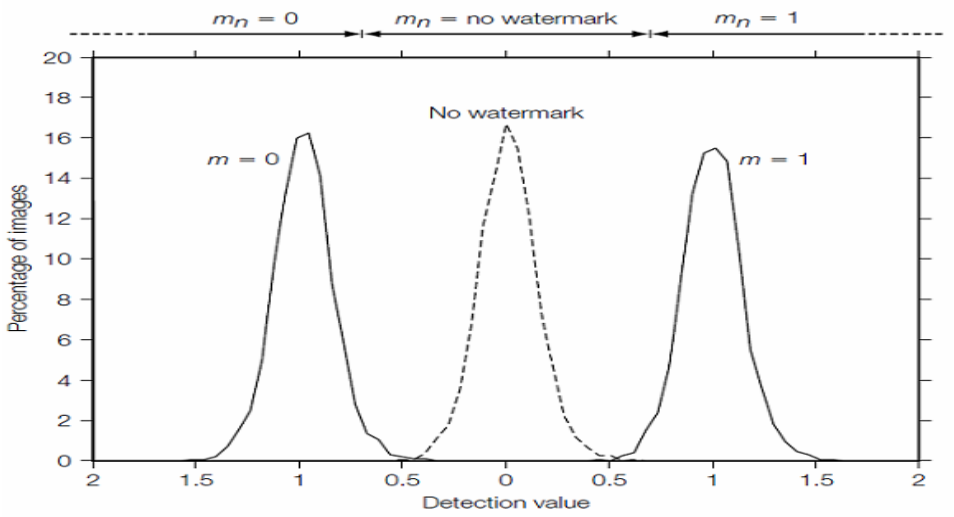
در رابطه ی(۲-۷) N به اندازه ی تعداد پیکسل های تصویر بوده و سیگما بر روی کل پیکسل ها نظیر

[1] corrolation
[2] Trade of
[3] Detector

به نظیرمحاسبه می شود. با توجه به آنکه $c = c_o + w_a + \eta$ که η نویز گوسی می باشد، عبارت همبستگی رابطه ی(۲-۷) به سه زیر عبارت تقسیم می شود که حاصل همبستگی میان c_o و η با w_r مقدار کوچکی است. بنابراین تنها عامل موثر در این رابطه همبستگی میان ترم های w_a با w_r خواهد بود که با توجه به آنکه بیت یک یا صفر بوده باشد، مقدار این همبستگی مثبت یا منفی خواهد شد. بنابراین اگر حاصل رابطه (۲-۷) مقداری بزرگ و مثبت باشد، واترمارک برابر با یک، اگر مقداری بزرگ و منفی باشد، واترمارک برابر با صفر ودر نهایت اگر مقداری کوچک باشد، نشاندهنده ی عدم وجود واترمارک خواهد بود. میزان سنجش واحد بزرگ بودن یا کوچک بودن حاصل همبستگی توسط یک مقدار آستانه بیان می شود. با توجه به نکات بیان شده بیت واترمارک را می توان با استفاده از رابطه ی(۲-۸) بدست آورد.

$$m_n = \begin{cases} 1 & if\ cor(c, w_r) > \tau \\ no\ watermark & if\ -\tau \le cor(c, w_r) \le \tau \\ 0 & if\ cor(c, w_r) < -\tau \end{cases} \qquad (۲-۸)$$

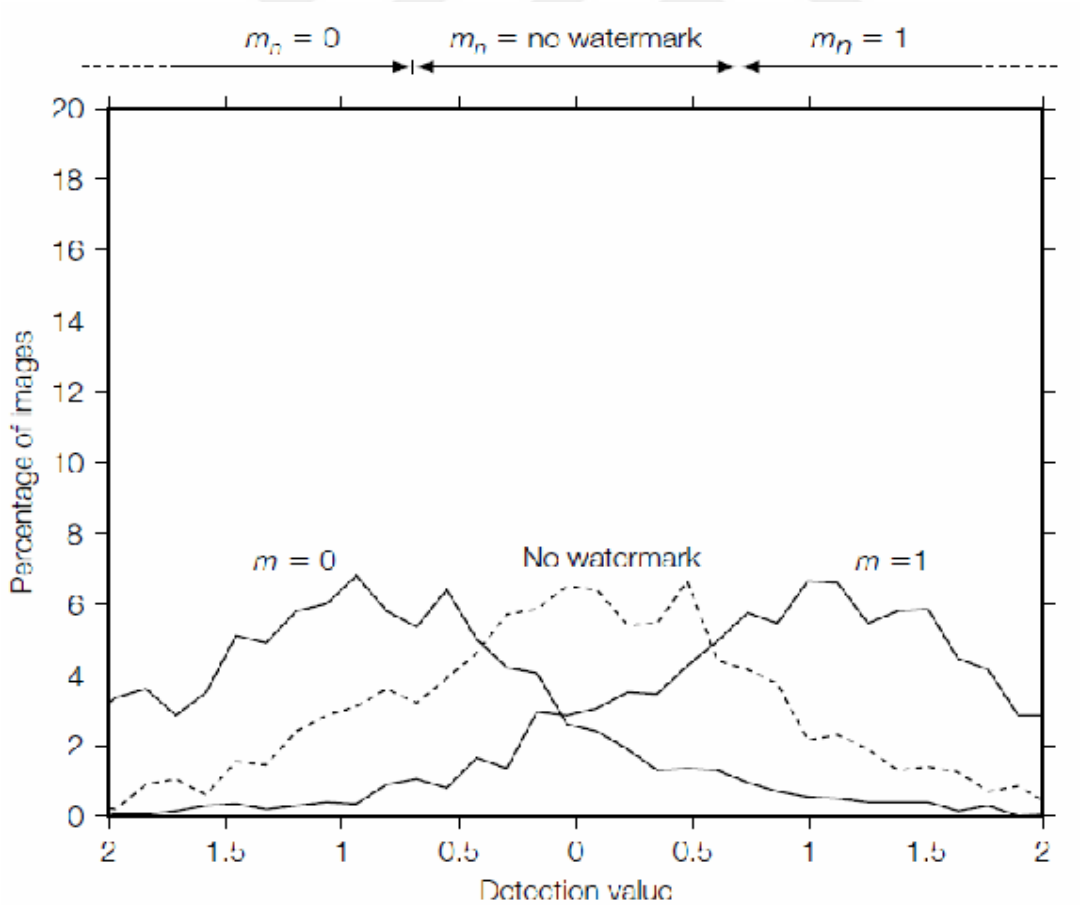
در شکل (۲-۵)توزیع مربوط به همبستگی ۲۰۰۰تصویر واترمارک نشده،واترمارک شده با صفر وواترمارک



شکل(۲-۵):توزیع مقادیر همبستگی برای ۲۰۰۰ تصویر در روش آشکارسازی اول[۲۲]

شده با ۱ نشان داده شده است.

انتخاب مقدار آستانه نقش مهمی در آشکارسازی صحیح دارد به طوریکه هر چه این مقدار کوچکتر باشد، احتمال آنکه تصویری بدون واترمارک، واترمارک شده تشخیص داده شود بیشتر است. نکته مهم دیگر در این روش انتخاب الگوی اولیه ی w_r است که نقش مهمی در کارایی روش دارد. به عنوان مثال اگر این الگو تنها حاوی مولفه های فرکانس پایین باشد، کارایی روش تاحد زیادی کاهش می یابد زیرا تصاویر نیز دارای مولفه های فرکانس پایین بزرگتری هستند و مقدار همبستگی دست خوش تغییر می شود. به عبارت دیگر سه منحنی توزیع نشان داده شده درشکل () با هم همپوشانی بیشتری خواهند داشت و تعداد تشخیص



شکل(۲-۶): اثر انتخاب نامناسب الگوی اولیه در توزیع هبستگی در روش اول[۲۲]

های درست آشکارساز کاهش می یابد. درشکل (۲-٦)نمونه ای از توزیع نامناسب ناشی از انتخاب الگوی اولیه ی اشتباه نشان داده شده است.از طرف دیگر چشم انسان نیز به مولفه های فرکانس پایین حساسیت بسشتری داشته و در نتیجه میزان رویت پذیری واترمارک افزایش می یابدودر نهایت اینکه این روش زمانی جوابی درخور توجه به ما می دهد که تصویر و نویز اضافه شونده دارای توزیع گوسی باشند.

۲-۲-۲- روش دوم: واترمارکینگ نابینا با ضریب اصلاح شده

همانطور که درشکل (۲-٦) دیده شد، در مواردی که حتی الگوی اولیه مناسب است، باز هم ممکن است منحنی های واترمارک یک و صفر با منحنی بدون واترمارک به دلیل اضافه شدن نویز همپوشانی داشته باشند و در نتیجه با انتخاب هر مقدار آستانه ای نتوان بازدهی را به صددرصد رساند. در اینجا روشی برای حل این ضعف ارائه می شود. در این روش با تعیین یک مقدار مناسب برای ضریب α ،کارایی روش را بالا می بریم.با فرض عدم وجود نویز مقدار همبستگی در آشکارساز برابر است با رابطه (۲-۹).

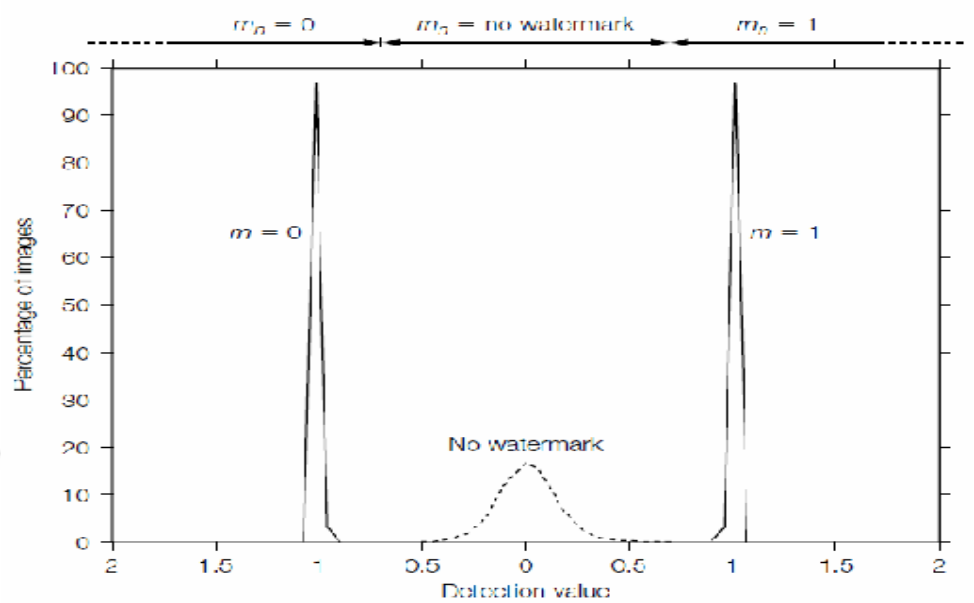
$$corr\ (c, w_m) = \frac{1}{N}(c_o.w_m + w_a.w_m), \qquad (۹-۲)$$

$$w_a = \alpha\ w_m\ ,\ \ w_m = \pm w_r$$

حال فرض می کنیم که می خواهیم مقدار همبستگی در آشکارساز به اندازه ی β از مقدار سطح آستانه بزرگتر باشد. با جایگزین کردن مقدار $\tau+\beta$ در طرف چپ رابطه ی(۲-۹) می توان یک مقدار مناسب برای α تعیین نمود که این مقدار از رابطه ی(۲-۱۰) بدست می آید.

$$\alpha = \frac{N(\tau+\beta) - c_o.w_m}{w_m.w_m} \qquad (۱۰-۲)$$

بقیه روش مانند قبل است. درشکل(۲-۷) توزیع نمونه برای همبستگی به ازای در نظر گرفتن $\tau+\beta=1$ مشاهده می شود.ملاحظه می شود که نسبت به روش اول همپوشانی توزیع ها با یکدیگر به خوبی ازمیان رفته است.



شکل(۲-۷): توزیع همبستگی برای ۲۰۰۰ تصویر با استفاده از ضریب اصلاح شده در روش دوم **[۲۲]**

۲-۲-۳-روش سوم: واترمارکینگ نابینا بر مبنای ساختار بلوکی

این روش همان روش اول با اعمال پاره ای تغییرات جزئی در سیستم جاسازی کننده و سیستم آشکارکننده است. در سیستم جاسازی کننده الگوی ثابت (w_r) بدون توجه به سایز تصویر به صورت یک بلوک ۸*۸ درنظر گرفته می شود. برای جاسازی این یک و یا صفر در هر تصویر، تصویر میزبان را نیز به بلوک های غیر همپوشان ۸*۸ تقسیم نموده و الگوی واترمارک را به هر کدام از بلوک ها مطابق روش اول اضافه می کنیم.

$$c_w(x, y) = c_o(x, y) + w_a(x \bmod 8, y \bmod 8) \qquad (۲-۱۱)$$

a mod b همان باقیمانده ی تقسیم a بر b می باشد. قسمت آشکارساز از دو بخش تشکیل شده است. در قسمت اول می بایست تصویر را به یک بلوک ۸*۸ تبدیل کنیم و در قسمت دوم میزان شباهت این بلوک را با الگوی w_r پیدا می کنیم. در قسمت دوم به جای استفاده از همبستگی دو سیگنال از کسینوس

زاویه ی بین دو سیگنال که مقدار متوسط آنها حذف شده است استفاده می کنیم. این کار دو فایده دارد. اول آنکه با حذف مقدار متوسط از سیگنال، مقادیر ثابتی که به همه ی پیکسل ها اضافه شده و اثری در تشخیص ندارند حذف می شوند، و دوم اینکه با نرمالیزه نمودن ضرب داخلی دو سیگنال (تقسیم کردن بر اندازه های دو سیگنال) و بدست آوردن کسینوس زاویه ی بین دو سیگنال اثر ضرب شدن سیگنال اولیه در یک مقدار ثابت از بین می رود. روابط سیستم آشکارساز به مطابق با رابطه ی(۲-۱۱) است. ادامه ی روند آشکار سازی مانند روش اول و استفاده از مقدار آستانه و مطابق رابطه ی زیر است:

$$v(i,j)=\frac{1}{B}\sum_{x=0}^{w/8}\sum_{y=0}^{h/8}c(8x+i,8y+j)$$

$$corrc(v,w_r)=\frac{(v-\bar{v}).(w_r-\overline{w_r})}{\sqrt{\left|v-\bar{v}\right\|w_r-\overline{w_r}\right|}} \qquad (۱۲-۲)$$

این روش نسبت به روش اول مزایا و معایبی دارد. از نظر سادگی آشکارساز روش اخیر ساده تر است، زیرا برخلاف روش اول به تعداد اندازه ی تصویر نیاز به ضرب کننده نداریم و تنها به ٦٤ ضرب کننده نیاز داریم. همچنین این رو ش نسبت به روش اول مقاوم تر است. اما مشکل این روش در انتخاب الگوی اولیه است که می بایست در انتخاب آن دقت بیشتری صورت گیرد. می توان ضریب α در این روش را مانند روش دوم اصلاح نمود که البته این کار به بهای پیچیده تر شدن سیستم تمام می شود.

۲-۲-٤- روش چهارم: واترمارکینگ نابینا با استفاده از روش تقسیم کد[1]

در روش هایی که تاکنون مورد بررسی قرار گرفتند، در هر تصویر تنها یک بیت واترمارک جاسازی می شد. در روش جاری قصد ما قرار دادن بیش از یک بیت اطلاعات و به طور خاص قرار دادن هشت بیت واترمارک می باشد. چنانچه در روش اول نشان داده شد برای جاسازی دو سمبل داده از یک الگو استفاده شد که برای یکی از سمبل ها آن الگو و برای دیگری همان الگو با علامت منفی واترمارک می گردید. دلیل

[1] Code Division

استفاده از یک الگوی واحد برای نشان دادن یک سمبل ایجاد فاصله ی فضایی حداکثر مابین دو سمبل است که برابر با ۱۸۰ درجه خواهد بود. برای جاسازی اطلاعات شامل بیش از دو سمبل مطابق با روند قبلی می بایست برای هر سمبل یک الگوی واحد را در نظر گرفت و سعی نمود که زاویه ی فضایی هر سمبل با سمبل دیگر تا جای ممکن زیاد باشد. اما این کار در هنگام آشکارسازی در زمانی که تعداد سمبل ها زیاد شود کمی دشوار خواهد بود. به عنوان مثال اگر بخواهیم ٦٥٥٣٦ سمبل را واترمارک کنیم، می بایست در آشکارساز به همین مقدار عمل همبستگی گیری و مقایسه را انجام دهیم. در حالی که این تعداد سمبل معادل یکی داده ی ١٦ بیتی است که نمی توان این حجم از داده را در دنیای امروز حجمی بالا نامید. بنابراین برای حل این مشکل از روش تقسیم کد استفاده می کنیم.

روش تقسیم کد

فرض کنید که یک رشته پیام با طول هشت داشته باشیم و سیستم دارای چهار سمبل مجزا باشد. در این صورت چنین رشته ای می تواند $8^4 = 65536$ پیغام مجزا را ایجاد نماید. برای تشخیص دادن چنین پیغامی در هر یک از هشت سمبل رشته ی مورد نظر به چهار مقایسه برای تشخیص چهار سمبل نیاز داریم. در نتیجه برای تشخیص ٦٥٥٣٦ پیغام مجزای موردنظر تنها ۳۲ عمل مقایسه لازم است. این ایده مبنای استفاده ما برای جاسازی نمودن یک دیتای هشت بیتی در تصویر میزبان می باشد.

شرح روش

با توجه به توضیحات ذکر شده برای جاسازی یک دیتا به طول هشت بیت، به جای یک الگو در روش های قبل هشت الگوی مستقل را در نظر می گیریم و با توجه به اینکه در هرکدام از این هشت بیت مقدار ۱ یا ۰ برای جاسازی مورد نظر باشد، الگوی مورد نظر با توجه به درایه ی مربوطه و یا منفی آن به تصویرمیزبان اضافه می شود. به عنوان مثال اگر هشت الگوی مورد نظر را با w_{ri} (i=1 to 8) نشان دهیم و

خواهان جاسازی رشته بیت ۱۰۱۱۰۰۰۱ در تصویر اصلی باشیم، تصویر واترمارک شده به صورت رابطه ی() خواهد بود.

$$c_w = c_o + w_{r1} - w_{r2} + w_{r3} + w_{r4} - w_{r5} - w_{r6} - w_{r7} + w_{r8} \qquad (۱۳-۲)$$

در قسمت آشکارساز میزان شباهت تصویر واترمارک شده با هرکدام از الگوهای w_{ri} (i=1 to 8) محاسبه شده و با توجه به علامت بدست آمده برای هر کدام از مقایسه ها مقدار صفر و یا یک برای آن درایه تشخیص داده می شود. با توجه به موارد بیان شده در صورتی که تصویر مورد مقایسه واترمارک هم نشده باشد، مقداری تصادفی به عنوان واترمارک گزارش می شود که یکی از ضعف های این روش است.

۲-۲-۵- روش پنجم: واترمارکینگ کد شبکه ای[1] وآشکارسازی به کمک الگوریتم ویتربی[2]

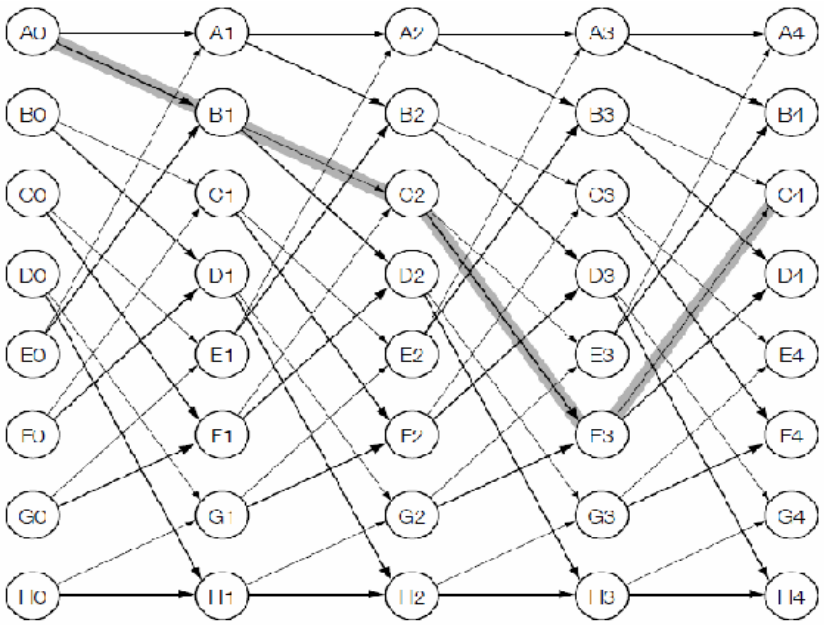
مهمترین ضعف استفاده از سیستم هایی نظیر سیستم روش قبل شبیه شدن بیش از اندازه ی رشته کدهای طولانی است که تنها در چند بیت با هم اختلاف دارند و این امر امکان وقوع خطا را در آشکارسازی افزایش می دهد. برای حل این مشکل نظیر راهکارهایی که در مخابرات دیجیتال استفاده می شود، روش کد کردن منبع مورد توجه قرار می گیرد. کد کردن منبع به طور کلی به معنای اضافه کردن اطلاعاتی به رشته بیت های ارسالی است که امکان خطایابی را در گیرنده فراهم آورند. ساده ترین کدکننده ی منبع افزودن بیت توازن[3] به اطلاعات است. از دیگر روش های کد کردن می توان کد گذاری همینگ[4] و کد بی سی اچ[5] رانام برد. هر کدام از روش های کدگذاری در از بین بردن خطاهایی خاص کاربرد دارند. مثلا خطاهای تصادفی به وسیله ی کد همینگ راحتتر آشکار می شوند و خطاهای پخشی که در آن خطا در گروهی از

[1] Trellis
[2] Viterbi
[3] Parity
[4] Hamming Code
[5] BCH Code

سمبل های پشت سرهم روی می دهد به کمک کد بی سی اچ بهتر آشکار می شوند. در روش جاری از کدگذاری شبکه ای برای رمزکردن و از الگوریتم ویتربی برای رمزگشایی استفاده می شود. در ادامه روش کد گذاری شبکه ای و الگوریتم ویتربی به طور خلاصه توضیح داده خواهد شد.

۲-۲-۵-۱-کدگذاری شبکه ای

این روش با ماشین حالت قابل نشان دادن است. بدین ترتیب که برای شروع تولید کد یک حالت اولیه رادرنظر می گیریم. برای کد کردن یک رشته بیت از اطلاعات ابتدا بیت اول را مورد توجه قرار می دهیم. با توجه به ساختار ماشین حالت در نظر گرفته شده به ازای بیت یک و صفر دو نوع انتقال حالت می توان داشت. هر انتقال میان حالات معادل تولید یک رشته بیت است. درشکل(۲-۸) این انتقال حالات برای تولید رشته بیت ۱۰۱۰و با در نظر داشتن هشت حالت مجزا نشان داده شده است. بنابراین در این روش به جای انتقال مستقیم بیت مورد نظر سمبل متناظر با انتقال میان حالات در هر مرحله ارسال می شود.



شکل(۲-۸):رشته بیت ماشین حالت برای تولید رشته بیت ۱۰۱۰ در کدگذاری شبکه ای [۲۲]

۲-۲-۵-۲-الگوریتم ویتربی

این الگوریتم بر مبنای یافتن شبیه ترین مسیر به مسیر اصلی پایه گذاری شده است. برای این منظور از همان روش یافتن همبستگی مابین الگوی مسیر و الگوهای مرجع نظیر آنچه در روش های قبل استفاده شد، بهره می گیریم. برای این منظور ابتدا به ازای هر حالت اولیه یک متغیر برای ایفای نقش انباره انتخاب می کنیم. در صورتی که احتمال قرار گرفتن در هر یک از حالات اولیه برابر باشد، مقدار اولیه برای تمام متغیرهای حالات برابر صفر خواهد بود. برای یافتن بهترین مسیر برای گذر از حالت صفر به حالت یک از رابطه ی استفاده می کنیم.

$$z(i) = \max(z(i) + v.w_{ij})$$
$$i \in \{A0, B0, C0, D0, E0, F0, G0, H0\}$$
$$j \in \{A1, B1, C1, D1, E1, F1, G1, H1\} \qquad (۱۴-۲)$$

با توجه به رابطه ی به ازای هر حالت اولیه میزان همبستگی بردار ورودی و الگوهای مرجع محاسبه شده و مقدار ماکزیمم در انباره ی z قرار داده می شود. در این مرحله هر کدام از z ها مقدار بزرگتری را داشت مسیر مورد نظر در مرحله ی اول خواهد بود. همین روش را برای مراحل بعدی ادامه می دهیم تا مسیر نهایی رابیابیم.

شرح روش

با توجه به الگوریتم های بیان شده، برای واترمارکینگ به روش مورد نظر، به ازای هر مسیر یک الگوی مرجع تعریف می کنیم که با الگوهای دیگر وابستگی نداشته باشد. برای واترمارک کردن هر رشته بیت دلخواه، با توجه به ماشین حالت تعریف شده، الگوهای مرجع متناسب با هر مسیر را به الگوی واترمارک اضافه کرده و با تصویر اصلی جمع می کنیم. در قسمت آشکارساز نیز با توجه به الگوریتم ویتربی، مسیر

مورد نظر را بازیابی می نماییم. نکته مورد توجه در این روش آنست که همانند روش قبل تصاویری که واترمارک نشده اند نیز در قسمت آشکارساز باعث تولید رشته بیتی تصادفی خواهند شد.

۲-۲-٦- روش ششم: واترمارکینگ کد شبکه ای با توانایی تشخیص تصاویر واترمارک نشده

یکی از ضعف های دو روش اخیر بیان شده عدم توانایی تشخیص تصاویر واترمارک نشده با تصاویر واترمارک شده می باشد. به منظور حل این مشکل سه راه حل وجود دارد که درادامه می آید.

۲-۲-٦-۱- افزایش پیغام های غیر معتبر با استفاده از افزایش طول پیغام

ساده ترین روش تشخیص پیغام های تصادفی افزایش تعداد پیغام ها به کمک افزایش طول پیغام و در نتیجه افزودن تعداد پیغام های نامعتبر می باشد. در اینصورت تنها تعداد محدودی از کل پیغام های ممکن برای ارسال توسط فرستنده معتبر بوده و احتمال معتبر بودن پیغام های تصادفی کاهش می یابد. ب عنوان مثال به جای گنجاندن یک واترمارک شانزده بیتی، یک واترمارک بیست و پنج بیتی را جاسازی می کنیم که نه بیت اضافی حاص مجموع هشت بیت اول و دوم واترمارک اصلی است. بدین ترتیب از هر ۵۱۲ پیغام، تنها یک پیغام معتبر خواهد بود.

۲-۲-٦-۲- استفاده از سطح آستانه برای تشخیص هر سمبل

همانطور که در دو روش اول مشاهده شد، مقدار همبستگی هر الگو با تصویر مورد نظر با یک مقدار آستانه مقایسه می گردید و تنها در صورتی که همبستگی مابین دو سیگنال از مقداری معین بالاتر می رفت، الگوی مذکور در تصویر مورد نظر آشکار می گشت. البته در استفاده از همبستگی باید دقت کرد که فقط می توان از رابطه ی برای محاسبه استفاده نمود. استفاده از کسینوس زاویه بین دو سیگنال هر جند اثرات مثبت بیشتر دارد، اما در مواقعی که پیغام مورد نظر مانند دو روش اخیر شامل بیش از یک الگو باشند، دچار مشکل

خواهد شد. این مشکل در بخش بعد توضیح داده خواهد شد. بنابه نکات بیان شده، در این روش تشخیص پیغام های تصادفی، اعتبار هر سمبل به طور جداگانه و بدون توجه به دیگر سمبل ها صورت می پذیرد.

۲-۲-٦-۳- استفاده از سطح آستانه برای تشخیص هر پیغام

مشکل استفاده از کسینوس زاویه دو سیگنال در تشخیص پیغام های شامل بیش از یک سمبل در این نکته نهفته است که زاویه بین دو سیگنال به صورت یک زاویه ی فضایی تعریف می شود که این زاویه مقداری بین صفر تا ۳٦۰ درجه دارد. با افزایش تعداد سمبل های یک پیغام به منظور بازشناسی واحد هر پیغام، ۳٦۰ درجه باید بین تعداد پیغام های ممکن تقسیم شود و با افزایش تعداد پیغام ها سهم هر پیغام از این زاویه ی فضایی کوچکتر خواهد شد. به همین دلیل برای تعیین مقدار آستانه در روش هایی که از مقدار

$$corr1 = \frac{v_1.w_1}{|v_1||w_1|} = \frac{v_o.w_1 + w_1.w_1}{|v_o + w_1||w_1|} \qquad (۱۵-۲)$$

$$corr2 = \frac{v_2.w_1}{|v_2||w_1|} = \frac{v_o.w_1 + w_1.w_1}{|v_o + w_1 + w_2||w_1|} \qquad (۱٦-۲)$$

زاویه ی بین دو سیگنال استفاده می کنند، باید به طول پیغام نیز توجه داشت. چرا که با افزایش طول پیغام مقدار آستانه باید کوچکتر انتخاب شود. نکات بیان شده از منظری دیگر نیز قابل بررسی است. فرض کنید که بردارهای v_1 و v_2 به ترتیب شامل پیغام های $v_o + w_1$ و $v_o + w_1 + w_2$ باشد. استفاده از روش کسینوس زاویه برای تشخیص الگوی w_1 به صورت رابطه ی خواهد بود.

در عبارت مربوط به $corr2$ حاصلضرب $w_1.w_2$ به دلیل عمود بودن الگوها حذف شده است. با توجه به مقادیر $corr1$ و $corr2$ مشاهده می شود با اینکه هر دو سیگنال حاوی الگوی w_1 هستند، اما $corr2$ به دلیل همراه داشتن الگوی w_2 مقداری کوچکتر دارد.

به منظور حل مشکل ذکر شده با توجه به طول پیغام آشکار شده و مقایسه مقدار آستانه متناسب با طول پیغام معتبر بودن پیغام را تشخیص داد.

۲-۳- معرفی تبدیل ویولت

۲-۳-۱-تاریخچه

تبدیل ویولت در ابتدای دهه۱۹۸۰ توسط مورلت ودوستانش معرفی شد ودر ارزیابی داده های زلزله بکار رفت. تبدیل ویولت برخلاف تبدیل فوریه ، که تابع های آن سینوسی می باشد، برپایه موج های کوچک که ویولت نامیده می شوندبنا شده است.ویولتها یا همان موجک ها با فرکانسی متغییر وطول محدود می باشند.این تبدیل به ما اجازه می دهد که یک صفحه موزیک معادل برای یک تصویر فراهم کنیم، که نه تنها مشخص می کند که چه نتی یعنی چه فرکانسی نواخته شده است بلکه زمان نواخته شدن آن را نیز مشخص می کند.به بیان دیگر تبدیل فوریه متداول فقط اطلاعات فرکانسی را فراهم می کند در حالی که اطلاعات زمانی از دست رفته است.اما تبدیل موجک هم اطلاعات زمانی وهم اطلاعات فرکانسی را در اختیار می گذارد.به عبارت دیگر تبدیل فوریه همانند یک منشور که نور را به چند رنگ می شکند تبدیل فوریه نیز سیگنال را به فرکانس های مختلف می شکافد.در سیگنال های ایستا همه فرکانس ها در همه زمانها رخ می دهد بنابراین تبدیل فوریه می تواند بسیار مفید واقع شود.اما برای سیگنال های غیر ایستا به هیچ وجه کارایی ندارد. برای سیگنال های غیر ایستا میتوان از تبدیل ویولت استفاده کرد.برای اعمال تبدیل موجک بر تصاویر ،باید از تبدیل موجک دو بعدی استفاده کنیم.بدین منظور تبدیل یک بعدی را بر سطرهاوستون های آرایه تصویراعمال می کنیم تا از ترکیب مولفه های این دو تبدیل، تبدیل دو بعدی بدست آید.این فرایندر شکل صفحه بعد آورده شده است.دراین نمودار تصویر اولیه در راستایXیعنی سطرها از یک فیلتر پایین گذر ویک فیلتر بالا گذرعبور داده شده ونمونه برداری کاهشی صورت گرفته است.این مرحله دو تصویر

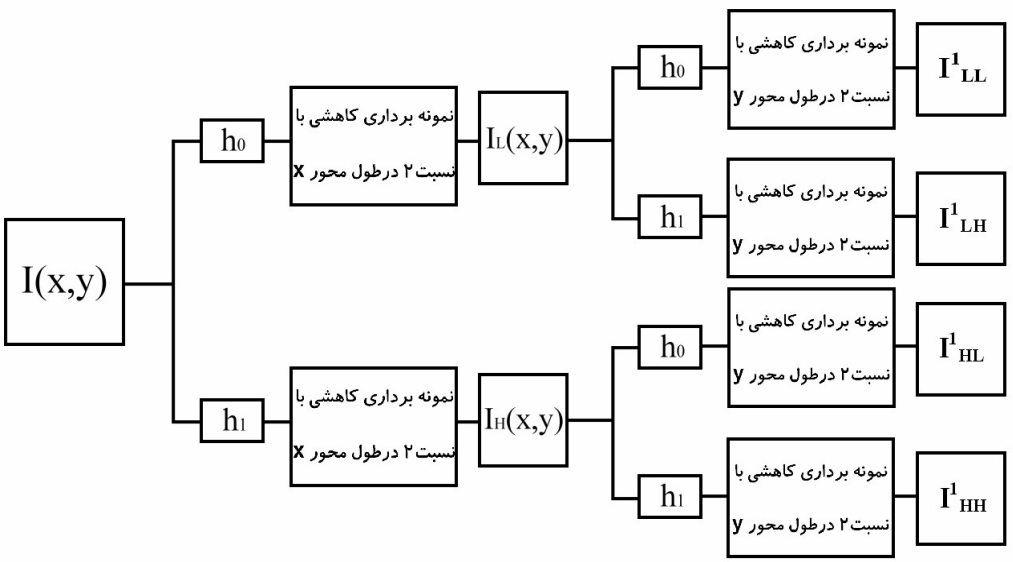
حاصل می کند که یکی شامل فرکانس های پایین تصویر $I^{L}(x,y)$ ودیگری شامل فرکانس های بالای تصویر $I^{H}(x,y)$ است.در مرحله بعدی هریک از این دو تصویر در راستای yیعنی ستون ها از یک فیلتر پایین گذر ویک فیلتر بالاگذر عبور داده شده ونمونه برداری کاهشی میشود.در نتیجه چهار تصویر حاصل می شودکه عبارتند از:

مولفه I^{1}_{LL} متناظربا مولفه فرکانس پایین تصویردر هردو جهت.

مولفه I^{1}_{LH} شامل جزییات افقی تصویر است.

مولفه I^{1}_{HL} شامل جزییات عمودی تصویر است.

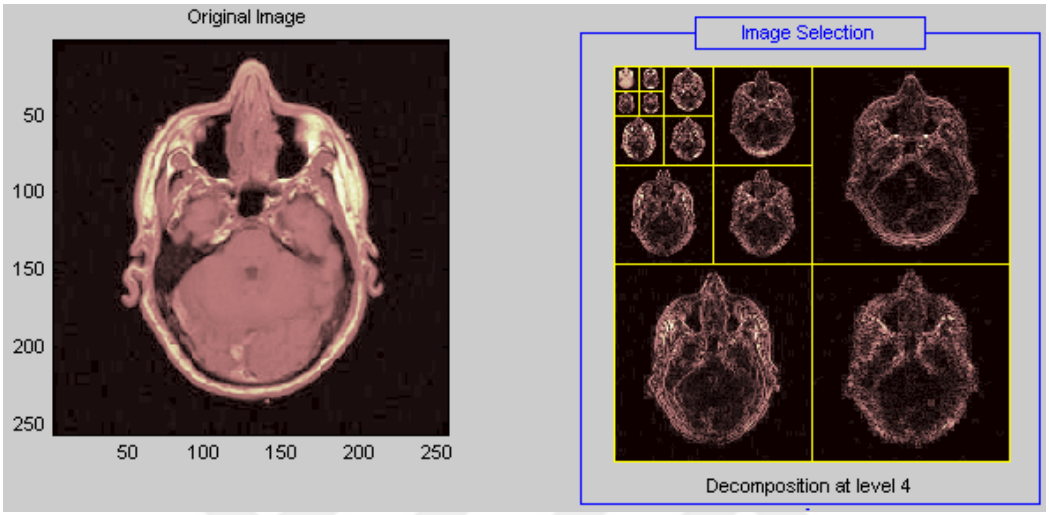
مولفه I^{1}_{HH} شامل جزییات قطری تصویر است.



شکل(۲-۹):فیلترهای تبدیل ویولت

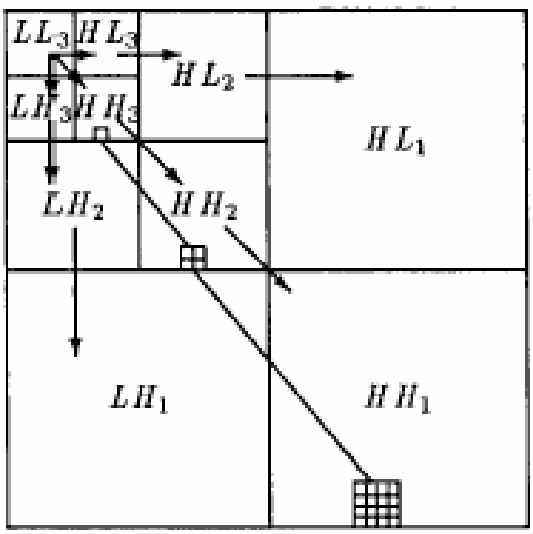
همانطور که در تصویر (۲-۱۰) نیز دیده می شود تصویر تشدید مغناطیسی سر بعداز هربار تجزیه موجک به چهار آرایه به ابعاد نصف آرایه تقریب قبل از خود به زیرباندهای جزییات وتقریب جدید تبدیل می شود وبرای تجزیه بیشتر دوباره زیرباند تقریب به چهار زیرباند تجزیه می شود.

این کار در شکل زیر ٤بار اتفاق افتاده است.



شکل(۲-۱۰):تجزیه تصویرباتبدیل ویولت دو بعدی

بعداز اعمال تبدیل ویولت برروی یک تصویر یا یک سیگنال می توان آنرا به خاطر زیر نمونه های اعمال شده به صورت درخت هایی نمایش داد. بدین ترتیب که یک ضریب در زیربانـدهای پایین باچهار یا١٦یا٦٤و...ضریب از زیربانـدهای بالا همبستگی دارد.این همبستگی یک نمودار درختی را بین ضرایب تشکیل می دهد.این درخت هادر شکل زیر نشان داده شده است.



شکل(۲-۱۱):درخت های ویولت در سه جهت

۲-۳-۲- مزایا ومعایب تبدیل ویولت:

در بین تکنیک های واترمارکینگ در حوزه تبدیل ، روش های واترمارکینگ در حوزه تبدیل موجک گسسته(DWT)معروفیت بیشتری را در بین تبدیل های دیگر بدست آورده است.به این علت است که تبدیل موجک گسسته دارای خواصی نظیر محلی سازی مکان- فرکانس ، نمایش مالتی رزولوشن، مدلسازی از سیستم بینایی انسان(HVS) وپیچیدگی محاسبات خطی است.بااستفاده از سیستم بینایی انسان میدانیم که چشم نسبت به نویز در زیرباندهای با رزولوشن بالا حساسیت کمتری نشان می دهد.این مزایا به ما اجازه میدهدکه واترمارک های با انرژی زیادرا درناحیه هایی قرار دهیم که سیستم بینایی انسان به آن حساسیت کمتری دارد.مانند ضرایب جزییات.تعبیه کردن واترمارک در این نواحی باعث افزایش مقاومت می شود وکمترین صدمه به کیفیت وتصویر وارد می شود.

برای غلبه بر ضعف های موجک تبدیل کرولت(Curvelet) پیشنهاد شد.بعد از چندی برای غلبه بر معایب این تبدیل هم تبدیل دیگری بنام تبدیل کانتورلت معرفی گردید.

۲-٤- معرفی شبیه سازی صورت گرفته

درچندین روش بکاررفته واترمارکینگ [۱و۲و۳و۱۱] از دو گروه ضریب به نمایندگی از بیت ۰ واترمارک وبیت ۱ واترمارک استفاده شده است. براین اساس تنها یک گروه از ضرایب در هر بار کوانتیزه می شود. ونگ و لین [۲] یک طرح واترمارکینگ کور برمبنای تبدیل موجک پیشنهاد دادندکه شبیه به[۳]بود. در این کارضرایب ویولت تصویر میزبان به صورت درخت ویولت جدا می شد وهر بیت واترمارک بااستفاده از دو درخت جاسازی می شد.یکی از دو درخت باتوجه به ضریب کوانتیزه می شد وبدین ترتیب تفاوت عددی بزرگی بین درخت کوانتیزه شده ودرخت کوانتیزه نشده به نمایش گذاشته می شد.این تفاوت بعدا برای

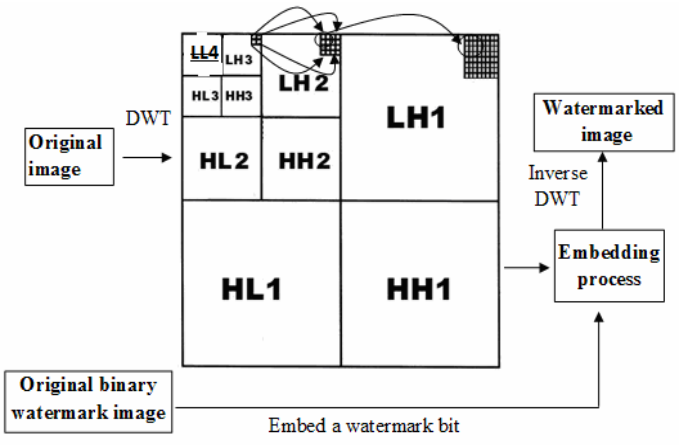
استخراج واترمارک مورد استفاده می شد.لی ودوستانش[۱] مدل ونگ و لین را با اضافه کردن سیستم بینایی انسان جهت مقاوم تر کردن در برابر حمله های هندسی بهبود بخشیدند.لین ودوستانش [۱۱] بوسیله استفاده کردن از چهار درخت برای جاسازی بیت های واترمارک این روش را نیز بهتر کردند.در این روش نیز یکی ازچهار درخت براساس مقدار بیت باینری واترمارک کوانتیزه می شد. پنگ و دوستانش[٤]یک روش کوانتیزه کردن درخت ویولت بر اساس بیت های واترمارک ارائه کردند.در این روش نیز اختلاف معناداری بین بیت ۰ جاسازی شده وبیت ۱ جاسازی شده ایجاد می شد که بعدا در استخراج واترمارک به کار گرفته می شد.نحوه انتخاب درخت ها نیز توسط یک کلید مخفی صورت می گرفت.آنها از دوریشه برای جاسازی استفاده کردند.

در این رساله ما یک روش واترمارکینگ کور براساس کوانتیزه کردن درخت ویولت ارایه می کنیم. در تحقیقات قبلی محقق شد که واترمارک جاسازی شده در ضرایب مهم، مقاوم است.موضوع مهم در آشکارسازی کور استفاده ازروشی است که واترمارک را به همان روشی که جاگرفته استخراج کند[۹و۱۲و۱۳].دراینجا ما یک روش واتر مارکینگ که بیت واترمارک رادر ضرایب ویولت ماکسیمم ودومین ماکسیمم در هر درخت جاسازی میکند، پیشنهاد می کنیم.روش پیشنهاد شده از[٤-۱]متفاوت می باشد. آنهااز دو درخت یا دو بلوک برای جاسازی بیت واترمارک استفاده می کنند.ما واترمارک را بوسیله ایجاد اختلاف دردامنه(اندازه) بین دو ضریب بزرگتر ویولت در یک درخت ویولت جاسازی می کنیم.برای انتخاب درخت ها ازیک کلید مخفی استفاده میکنیم.برای استخراج یک مقدارآستانه تطبیقی طراحی می شود. اگراختلاف بین دو ضریب، بزرگ تر از مقدار آستانه تطبیقی باشد یک بیت ۱واترمارک استخراج می شودودرغیر این صورت یک بیت ۰ واترمارک استخراج می شود.

نتایج تجربی نشان میدهد که روش پیشنهادی در برابر انواع حمله های مختلف مقاومت خوبی دارد.

۲-٤-۱- واترمارکینگ بوسیله کوانتیزه کردن درختهای ویولت

یک تصویر میزبان در اندازه n در n بوسیله تبدیل ویولت گسسته سه سطحی تبدیل به ضرایب ویولت می شود.دریک تجزیه سه سطحی ما ده باند فرکانسی داریم که در شکل ۱ نشان داده شده است.یک رابطه پدر وفرزندی این زیرشاخه هارا مثل یک درخت ویولت بهم متصل کند[۲]. بعد از تبدیل ویولت سه سطحی برای یک تصویرn در n ،ما ۳زیرباندLH3 ,HL3,HH3رابه عنوان ریشه هاخواهیم داشت ولذا $3*(n/2^3 * n/2^3)$درخت در سه جهت میتوانیم داشته باشیم.سطح تفکیک بالا(نظیرسطح۳در شکل ۱)ضرایب خیلی مهمتری نسبت به یک سطح تفکیک پایینتر(نظیرسطح۲درشکل ۱)رادارد.همانطورکه دیده می شود،وقتیn= ۵۱۲ است ۲۱ ضریب برای یک درخت ویولت ازیک شاخهLH3تاLH1 همانند رابطه پدر وفرزندی ساخته میشود. در روش پیشنهادی، ما تنها به دو ضریب بزرگتردر هر درخت نیاز داریم. همان طور که در شکل ۱نشان داده شده است یک ضریب ازLH3و٤ضریب از همان موقعیت در همان مکان فضایی در LH2انتخاب شده است.البته ما درخت ها را براساس یک کلید مخفی انتخاب می کنیم.این کلید بر اساس یک هسته تابع شبه تصادفی ایجاد میشود.ماز این هسته به عنوان کلید مخفی در فرایند استخراج استفاده می کنیم.



شکل(۲-۱۲):درخت های ویولت

۲-٤-۲- پیش پردازش

بایک DWT سه سطحی همانطور که در شکل ۱نشان داده شده ما ۱۰ باند فرکانسی داریم.یک زیرباند بالاتر خیلی مهمتراز یک زیر باند پایین تر است.استفاده از زیرباند LL3به عنوان یک ریشه برای جاسازی واترمارک مناسب نیست.چرا کهLL3 یک زیرباند فرکانس پایین بوده وشامل اطلاعات مهم درمورد تصویر است وتغییردر آن براحتی باعث اعوجاج درتصویر می شود.جاسازی واترمارک درزیر باندHH3هم مناسب نیست چراکه این زیرباند نیز براحتی میتواند با یک فشردگی بااتلاف حذف شود.

زیرباندLH3بسیار مهمتراززیرباندHL3است[۱۰]. بنابراین برای انتخاب ریشه جهت جاسازی، زیرباند LH3مقدمتر از HL3 است.در این مقاله یک تصویر واترمارک باینری Wدر اندازه Nw بیت جاسازی می شود. هربیت واترمارک را با۰و۱نشان میدهیم وNw انتخابی ما بازیرباندها همپوشانی ندارد.

۲-٤-۳- جاسازی واتر مارک

تصویرواترمارک ۳۲*٦٤ میباشد.ما LH3,LH2را به دو تکه مساوی تقسیم می کنیم.بوسیله یک کلید شبه تصادفی جاسازی واترمارک را در دو تکه بالایی وپایینی زیر باند ها انجام میدهیم.ابتدا درخت ها را انتخاب نموده وسپس میانگین تفاضل maxو secرا در تمامی درخت ها بروش زیر محاسبه میکنیم:

$$\varepsilon = \left\lfloor \frac{1}{N} \sum_{i=1}^{N} (\max_i - \sec_i) \right\rfloor \qquad (۱۷-۲)$$

که در این رابطه ε میانگین اختلاف ضرایب ماکس ودومین ماکس در درخت های انتخابی میباشد.Nتعداد بیت های واتر مارک است.$\lfloor \rfloor$علامت جزصحیح است.

باتوجه به[٤] میدانیم که ضرایب مثبت در برابرحملات مختلف بسیار مقاومتر از ضرایب منفی هستند.لذا تمام ضرایب ماکسیمم منفی را در درخت های انتخابی صفر میکنیم. برای جاسازی یک بیت ۱واترمارک به

روش زیر عمل می کنیم.با توجه به کلیدمخفی درخت مورد نظر انتخاب شده واینکه درخت از قسمت فوقانی است یا از قسمت تحتانی براساس بیتهای ۰ و۱کلید مخفی بدست می آیدو جاسازی بروش زیر صورت می گیرد:

اگر $\Delta i \geq Max(\varepsilon, T)$ (۱۸-۲)

آنگاه $max_i^{new} = max\ i$

اگر $\Delta i < Max(\varepsilon, T)$ و $max\ i$عضوریشه باشد

آنگاه $max_i^{new} = maxi + \beta$

اگر $\Delta i < Max(\varepsilon, T)$ و $max\ i$عضوریشه نباشد

آنگاه $max_i^{new} = maxi + \beta * \gamma$

که در روابط فوق $\Delta i = maxi - seci$ درهر درخت انتخابی میباشد.

maxi و seci به ترتیب ماکسیمم ودومین ماکسیمم در هر درخت انتخابی میباشند و max_i^{new} ضربب ماکسیمم جدید وبه روز شده در درخت انتخاب شده است.باتوجه به اینکه ضرایب فرکانس پایین تر مقاومتر از فرکانس بالا هستند، در صورتی که ضریب ماکسیمم از ریشه باشد فقط به اندازه βضریب را افزایش می دهیم. در حالیکه اگر ضریب ماکسیمم از ریشه نباشد میتوانیم به اندازه $\beta * \gamma$افزایش ایجاد کنیم.بدین تر تیب ما از ایجاد اختلاف بیشتر بین دو تصویر اصلی وتصویر واترمارک شده جلوگیری میکنیم. اما ما بااستفاده از یک پارامتر دیگری بنام T کاهش اختلاف بین این دو تصویر را تضمین میکنیم واز ایجاد اعوجاج بیشتر جلوگیری می کنیم.در نتایج عملی بدست آمده مشخص شده است که برخی تصاویرε کوچکی دارند که باعث می شود اختلاف بین ضرایب ماکس و دومین ماکس فاحش نباشد.با استفاده از این پارامتر مقاومت در برابر حملات را افزایش میدهیم.

برای جاسازی بیت ۰ واتر مارک نیز در صورتی که ضریب ماکس دوم منفی باشد ابتدا آنرا صفر کرده و به این صورت عمل میکنیم:

اگر $seci < 0$ آنگاه $max_i^{new} = 0$ و $sec_i^{new} = 0$ (۱۹-۲)

اگر $seci > 0$ آنگاه $max_i^{new} = sec_i^{new}$

که sec_i^{new} دومین ضریب ماکس جدید در iامین درخت انتخابی است.

۲-٤-٤- طراحی دکودر

در روش پیشنهاد شده هیچکدام از تصاویر اصلی و واترمارک اصلی برای فرایند استخراج مورد نیاز نمیباشد. لذاروش پیشنهادی یک روش کور است. در طول فرایند جاسازی ،جاسازی بیت ۱واترمارک بوسیله اضافه کردن یک مقدار β(یا βدر γ) به ضریب ویولت ماکسیمم محلی در درخت ویولت وجاسازی بیت۰ بوسیله$maxi=seci$ بود.بنابراین اگر یک بیت ۰واترمارک در درخت ویولت جاسازی شده، اختلاف محلی بین دو ضریب بزرگتر نزدیک صفر خواهد بود.در غیر این صورت اگر بیت ۱واترمارک دردرخت ویولت جاسازی شده این اختلاف محلی بین دو ضریب بزرگتر ،بیشترازβ خواهد بود.برای استخراج صحیح بیت واتر مارک ما مقدار yرابصورت زیر تعریف می کنیم:

$$y = \left\lfloor \frac{1}{N * \alpha} \sum_{j=1}^{N*\alpha} \varphi_j \right\rfloor \qquad (۲۰-۲)$$

که تابع φ مرتب شده تفاضل ضرایب ماکس در همه درختهای انتخابی به صورت صعودی می باشد. αپارامتر مقیاس است و$۱ \leq \alpha > ۰$. αبرای تعیینy مهم است و برای تعیین اینکه مشخص کنیم که چند در صد از اختلاف های ضرایب در φ میتواند مورد استفاده برای میانگین واقع شود استفاده می شود. بزرگی α منجربه بزرگی yخواهد بود. فرض کنید همه بیت های واتر مارک جاسازی شده برابر ۱ باشد.این

یعنی اینکه تفاوت بین ضرایب ویولت ماکسیمم وضرایب ویولت ماکسیمم دوم برای هر درخت ویولت جاسازی شده بزرگتر از β است.مقدار α بایدبرای اجتناب از خطای احتمالی استخراج کوچک قرار داده شود. از طرف دیگر اگرهمه بیتهای واترمارک جاسازی شده ۰ هستندمقدار α باید تاجای امکان بزرگ انتخاب شود.بنابراین α برای استخراج واترمارک بسیارمهم است.

۲-٤-٥- استخراج واترمارک

پیرو روابط٤و٥ استخراج واترمارک بسیار آسان خواهد بود.ابتدا بوسیله هسته ای که همان کلید مخفی نام دارد درخت های تغییر یافته را مشخص میکنیم.اگر اختلاف ضرایب ماکس محلی بزرگتر یا برابرyباشد، باتوجه به اینکه $0<y\leq\beta$ ، آنگاه بیت واترمارک جاسازی شده برابر ۱میتواند باشد.درغیراین صورت بیت واترمارک جاسازی شده ۰است. بیت واترمارک براساس رابطه زیر استخراج می شود:

اگر $maxi-seci>y$

آنگاه بیت واترمارک=۱ (۲-۲۱)

درغیراینصورت بیت واترمارک=۰.

فصل سوم

نتیجه گیری و بحث

۳-۱- نتایج عملی

تمامی پیش پردازش ها وپردازش ها و حملات در نرم افزار matlab7.8 صورت گرفته است. برای اینکه بتوانیم نتایج بدست آمده را با کارهای قبلی مقایسه کنیم روش [٤]وروش پیشنهادی را در روی یک تصویر مشترک اجرا کردیم.برای این کار از تصویر لنا که کارهای قبلی نیز برروی آن انجام شده استفاده می کنیم. تصویر لنا وواترمارک باینری در شکل(۳-۱) نشان داده شده است.شکل (۳-۲) تصویر واترمارک شده ونتیجه استخراج شده را نشان می دهد. همانطور که مشاهده می شود بین تصویر اصلی وتصویر واترمارک شده از نظر ظاهری تفاوتی وجود ندارد.

برای اینکه به میزان شباهت تصویراصلی به تصویر واترمارک شده پی ببریم از رابطه زیر استفاده میکنیم:

$$PSNR = 10\log_{10}\left[\frac{255*255}{\frac{1}{H*W}\sum_{x=0}^{H-1}\sum_{y=0}^{w-1}\left[A(x,y)-A'(x,y)\right]^2}\right] \qquad (۱-۳)$$

که دراین رابطه H وW به ترتیب طول وعرض تصویر اصلی هستندوA و ′Aمکان پیکسل های دو تصویراصلی وواترمارک شده می باشند.این رابطه در واقع نرخ پیک سیگنال به نویز برای ارزیابی بین کیفیت تصویر واترمارک شده وتصویر اصلی را بیان می کند.بعداز استخراج واترمارک ضریب همبستگی نرمالیزه شده برای استفاده در قضاوت برای وجود واترمارک محاسبه میشود.

روش پیشنهاد شده PSNR(Peak Signal to Noise Ratio)بسیار مطلوب تری نسبت به روش

[٤]دارد. مقدار ضریبNCC(Normalized Cross Correlation)بصورت زیر محاسبه می شود:

$$NC=\frac{1}{w_i * w_j}\sum_{i=0}^{w_i-1}\sum_{j=0}^{w_w-1} w(i,j)*w'(i,j) \qquad (۲-۳)$$

که درآنwh و ww طول وعرض واترمارک هستند(w(i,j و w'(i,j) بترتیب مقدار مختصات درواترمارک اصلی و واتر مارک استخراج شده هستند.دراینجا اگر بیت واترمارک برابر یک باشدw(i,j) برابر۱قرار داده میشود.در غیراین صورت ۱- خواهدبود. w'(i,j) هم به همین شکل جاگذاری می شود.بنابراین مقدارعبارت

شکل(۳-۱): تصویر اصلی لنا در اندازه ۵۱۲*۵۱۲ وتصویراصلی واترمارک باینری در اندازه ۳۲*۶۴

شکل(۳-۲): تصویر واترمارک شده لنا با PSNR=42/17 وواترمارک باینری استخراج شده باNC=1.

w(i,j) ×w'(i,j)برابر ۱یا۱- است.بدین ترتیب شباهت بین واترمارک اصلی وواترمارک استخراج شده برابر۱ اندازه گیری شد.

برای انجام شبیه سازی ما پارامترهارا بدین صورت قرار میدهیم. T=۱۰ پارامترمقیاس, $\beta = 20, \alpha = 0.7$.در ادامه هم حمله های هندسی وهم غیر هندسی را در نظر میگیریم.حمله های غیر هندسی شامل فشردگی JPEGوفیلترینگ پایین گذرویکسان سازی هیستوگرام است.در مورد حمله های چرخشی علامت (+) در جهت حرکت عقربه های ساعت وعلامت(-) حرکت در خلاف عقربه های ساعت می باشد.از جدول(۳-۱) دیده می شود که روش پیشنهاد شده در مقایسه با روش پنگ[٤]در یک شرایط مشابه بسیار خوب عمل کند.درضمن نرخ سیگنال به نویز ما بسیار مطلوب تر از روش های قبلی می باشد.همچنین در جدول زیرواترمارک های استخراج شده بعد از حملات مختلف نیز آورده شده است. همانگونه که مشخص است

NC / حملات	lien[۱۱] psnr=۴۱،۵۴	Peng[۴] Psnr=۳۷،۳۷	روش پیشنهادی Psnr=۴۲،۱۷	واترمارک استخراج شده بعداز حمله در رروش پیشنهادی
Median filter3*3	۰،۷۹	۰،۷۳	۰،۷۸	
Gaussian filter	۰،۸۴	۰،۸۱	۰،۹۴	
Jpeg(Qf=10)	۰،۱۷	۰،۶۰	۰،۶۳	
Jpeg(Qf=20)	۰،۶۱	۰،۸۱	۰،۸۶	
Jpeg(Qf=30)	۰،۷۹	۰،۸۹	۰،۹۵	
Jpeg(Qf=50)	۰،۸۹	۰،۹۷	۰،۹۹	
Jpeg(Qf=70)	۰،۹۷	۰،۹۹	۱	
Scaling 256*256	۰،۷۹	۰،۷۶	۰،۸۳	
Rotation(degree:0.25)	۰،۱۶	۰،۸۲	۰،۸۷	
Rotation(degree:1)	۰،۰۷	۰،۸۱	۰،۸۷	
Rotation(degree:-0.25)	۰،۱۰	۰،۸۲	۰،۸۸	
Rotation(degree:-1)	۰،۱۶	۰،۸۱	۰،۸۷	
Histogram equalization	NA	۰،۸۵	۰،۹۱	

جدول(۳-۱): مقایسه روش پیشنهادی با روش های قبلی

تقریبا در تمامی حملات واتر مارک براحتی قابل تشخیص میباشد.

۳-۲- نتیجه گیری

در این رساله ما واترمارکینگ دیجیتال را معرفی کرده وخواص وکاربردهاووانواع آن رابررسی کردیم وسپس یک روش واتر مارکینگ کور براساس کوانتیزه کردن درخت های ویولت با یک سری کلید شبه تصادفی ارائه کردیم. ما یک بیت واترمارک را بوسیله کوانتیزه کردن ضریب ویولت ماکسیمم در یک درخت ویولت جاسازی می کنیم.درخت ها براساس یک کلیدمخفی انتخاب میشوند. درخت ها به اندازه کافی کوانتیزه می شوند تا یک اختلاف بقدر کفایت بزرگ، بین بیت ۱ وبیت ۰ واترمارک دیده شود. در طول استخراج یک مقدار آستانه ای تطبیقی طراحی می شود.دامنه تفاضل درهردرخت انتخاب شده ویولت، با یک مقدار آستانه تطبیقی مقایسه می شود.در این روش بدون نیاز به تصویر اصلی وواترمارک عمل استخراج واترمارک را انجام دادیم.علاوه بر این با طراحی مقدار آستانه ای تطبیقی در فرایند استخراج ، روش ما در برابر حمله های معمولی نظیر فیلترینگ میانی،فیلترینگ میانگین گیری مقاومتر می شود.مقادیرنسبت سیگنال به نویز بدست آمده غیرقابل رویت بودن مارک در تصویروقدرت بدون تغییرماندن مارک پس از استخراج در الگوریتم ارائه شده را نشان میدهد. روش ارائه شده می تواند قابلیت های مهم واترمارکینگ شامل غیر قابل رویت بودن، استحکام،کوربودن رابرآورده می کند.

مراجع

[1] E. Li, H. Liang, and X. Niu,"An integer wavelet based multiple logo-watermarking scheme," presented at Proc. IEEE WCICA, 2006 of Conference.

[2] S. H. Wang and Y. P. Lin, "Wavelet tree quantization for copyright protection watermarking," IEEE Trans. Image Processing, vol. 13, pp. 154-165, Feb. 2004.

[3] G. C. Langelaar and R. L. Lagendijk, "Optimal differential energy watermarking of DCT encoded images and video," IEEE Trans.Image Processing, vol. 10, pp. 148-158, Jan.2001.

[4] P. Liu and Z Ding , "A blind image watermarking scheme based on wavelet tree quntization" ,"IEEE, pp.218-222, 2009

[5] Wong P.W, " A Public Key Watermark for Image Verification and Authentication [Conference] In Proc. IEEE Int. Conf. Image Processing. - Chicago : [s.n.], 1998.

[6] J. R. Hernandez, M. Amado, and F. Perez-Gonzalez, "DCT-domain watermarking techniques for still images: detectorperformance analysis and a new structure,"IEEE Trans. Image Processing, vol. 9, pp. 55-68, Jan. 2000.

[7] L. Sin-Joo and J. Sung-Hwan, "A survey of watermarking techniques applied to multimedia," in Proc. IEEE ISIE 2001, pp.272-277

[8] H. J. Wang and C. C. J. Ko,"High fidelity image compression with multithreshold wavelet coding (MTWC)," presented at SPIE's Annual Meeting-Application of Digital Image Processing XX, San Diego, 1997 of Conference.

[9] M. Hsieh, D. Tseng, and Y. Huang, "Hiding digital watermarks using multiresolution wavelet transform," IEEE Trans. Ind. Electron., vol. 48, pp. 875-882, Oct. 2001.

[10] J. M. Shapiro, "Embedded image coding using zerotrees of wavelet coefficients," IEEE Trans. Signal Processing. [see also IEEE Trans. Acoust., Speech, Signal Processing], vol. 41, pp. 3445-3462, Dec. 1993.

[11] B. K. Lien and W. H. Lin,"A watermarking method based on maximum distance wavelet tree quantization," presented at 19th Conf.Computer.

[12] I. J. Cox, J. Kilian, F. T. Leighton, and T.Shamoon, "Secure spread spectrum watermarking for multimedia," IEEE Trans.Image Processing, vol. 6, pp. 1673-1687, Dec.1997.

[13] H. J. Wang, P. C. Su, and C. C. J. Kuo,"Wavelet-based digital image watermarking,"Optics Express, vol. 3, pp. 491-496, Dec. 1998

[14] N. Nikolaidis and I. Pitas, "Robust image watermarking in the spatial domain," Signal Processing, vol. 66, pp. 385-403, 1998.

[15]Barni M.,et al. " A DCT-Domain System for Robust Image Watermarking [Journal] **,"** Signal Processing. - 1998. - 66. - p. 357.

[16]Berghel H., and L. O'Gorman" Protecting Ownership Rights through Digital Watermarking [Journal] **,"** IEEE Computer Mag. . - 1996. - 29. - p. 101.

[17]Caronni G" Assuring Ownership Rights for Digital Images [Conference] **,"**In Proc. Reliable IT Systems. – Germany : Viewveg, 1995.

[18]Celik M. U., et al. " Hierarchical Watermarking for Secure Image Authentication with localization [Journal] IEEE Trans. Image Processing. - 2002. - 11. - p. 585.

[19]Cox I. J., et al. " Secure Spread Spectrum Watermarking for Images Audio and Video [Conference] **,"**In Proc. IEEE Int. Conf. on Image Processing. - Lausanne, Switzerland : IEEE, 1996.

[20]Cox I. J., et al. " Secure Spread Spectrum Watermarking for Multimedia [Journal] **,"** IEEE Trans. Image Processing. - 1997. - 6. - p. 1673.

[21]Deguillaume F., S. Voloshynovskiy, and T. Pun. " Secure Hybrid Robust Watermarking Resistant against Tampering and Copy Attack [Journal] **,"** Signal Processing. - 2003. - 83. - p. 2133.

[22]Ingemar J. Cox Matthew Miller, Jeffrey Bloom, Jessica Fridrich, Ton Kalker Digital Watermarking and Steganography [Book]. - [s.l.] : Morgan Kaufmann, 2007. - 2end Edition : p. 624.

[23]Lin S. D., and S.-F. Chen. " A Robust DCT-Based Watermarking for Copyright Protection [Journal] **,"** IEEE Trans. Consumer Electronics. - 2000. - 46. - p. 415.

[24]Nikolaidis N., and I. Pitas. " Robust Image Watermarking in the spatial Domain [Journal] **,"** Signal Processing. - 1998. - 66. - p. 385.

[25]Pitas I., and T.Kaskalis Applying Signatures on Digital Images [Conference] **,"** In Proc. IEEE Workshop on Nonlinear Signal and Image Processing. - Neos Marmaras, Greece : [s.n.], 1995. - p. 460.

[26]Sun Q., and S.-F. Chang. " Semifragile Image Authentication Using Generic Wavelet Domain Features and ECC [Conference] **,"** In Proc. IEEE Int. Conf. on Image Processing. - 2002.

[27]Swanson M. D., B. Zhu, and A. H. Tewfik. Transparent Robust Image Watermarking [Conference] In Proc. IEEE Int. Conf. on Image Processing. - Lausanne, Switzerland : IEEE, 1996.

[28]Wolfgang R., and E. Delp A Watermarking Technique for Digital Imagery:Further Studies [Conference] In Proc. Int . Conf. Imaging Science, Systems and Technology. - Las Vegas, NV : [s.n.], 1997.

Islamic Azad University
Tabriz Branch

Faculty of Engineering- Department of Electronic

Thesis «M.Sc »
On Electronic

Subject:

A Blind Watermarking Based On Quantization of Wavelet Trees

Thesis Advisor:
Siamak haghipour(Ph.d)

Consulting Advisor:
Behzad Mozaffary(Ph.d)

By:
Masoud Maleki

Summer 2010