طراحی و پـیاده سازی Digital Watermark جهت ارسال تصویر

مریم شاه پسند

موسسه آموزش عالی سجاد *M.shahpasand@gmail.com*

سید رضا کامل طباخ فریضی

دانشگاه آزاد- واحد تهران جنوب *Rezakamel@toosashena.com*

چکیده : با گسترش سیستمهای چند رسانه ای تحت شبکه شده ، احساس نیاز به امنیت اطلاعات ، حمایت از کپی رایت در رسانه های دیجیتالی مختلف مانند تصویر ، کلیپهای صوتی ، ویدئو شدت گرفته است و یکی از روشهای مناسب جهت رسیدن به این اهداف دیجیتال واترمارک می باشد که عبارتست از توانایی حمل اطلاعات همراه با رسانه مورد نظر جهت احراز هویت .

در این مقاله مروری بر تحقیقات انجام شده در راستای دیجیتال واترمارک[1] و انواع الگوریتمهای مختلف اعمال آن و کاربردهای آن صورت گرفته و نهایتا به بررسی پیاده سازی روشی در جهت اعمال این تکنولوژی در چهار مرحله بر اساس تمامی اصول تکنولوژی واترمارک از جمله حمایت از کپی رایت ، تشخیص جعلی یا اصل بودن تصویر،دستیابیهای کنترل شده و در پایان نحوه احراز هویت تصاویر واترمارک شده می پردازد .

واترمارکهای اعمال شده عبارتند از : ۱- واترمارک غیر قابل رویت با استفاده از *Checksum* ۲- واترمارک غیرقابل رویت با استفاده از الگوریتم تغییر در کم اهمیت ترین بیت ۳- واترمارک قابل رویت استفاده از روش برچسب گذاری اطلاعات ۴- واترمارک غیر قابل رویت با *Checksum* و استفاده از تابع درهم ساز. الگوی الگوریتمی این روش در پایان مقاله مشخص شده است.

واژه های کلیدی : احرازهویت ،تصویر، امنیت ،تابع در هم ساز، Digital Watermark

۱- مقدمه

گسترش سیستمهای چند رسانه ای، نیاز جهت حفاظت از کپی رایت رسانه های دیجیتالی مختلف مانند تصویر ، کلیپهای صوتی، ویدئو را بوجود آورد .حمایت کپی رایت شامل احراز هویت وشناسایی کپی های قانونی یک تصویر است .از روشهای حل این مشکل می توان به روشهای مختلف رمزنگاری اشاره نمود اما این روشها اگر چه مزایایی دارند اما دارای چندین عیب نیز می باشند از جمله می توان به گم شدن رمز عبور،تغییر محتویات در طول انتقال ،صرف زمان جهت رمز گشایی و برگردان داده نام برد که یکی از روشهای حل این مشکل ، اضافه کردن یک ساختار مرئی یا نامرئی به تصویر است که می توان آنها را مارک دار کرد که این روش *digital watermark* یا سایه گذاری دیجیتالی نامیده می شود . *watermark* عبارتست از توانایی حمل اطلاعات جهت احراز هویت یا کدهای احراز هویت یا علائم اختصاری ضروری جهت تفسیر تصویر . این توانایی جهت پیدا کردن کاربردی در برچسب گذاری تصویر ، انجام کپی رایت ، حفاظت از جعل کردن و دستیابی کنترل شده می باشد . (*watermark*) پردازش رمزگذاری مخفیانه اطلاعات کپی رایت در یک تصویر می باشد که این کار با تغییرات کوچک نشانه گذاری(مهرگذاشتن) در محتوای هر سلول تصویری صورت می گیرد.همانطور که گفته شد ، رمزگذاری محتویات را در طول انتقال داده از فرستنده به گیرنده محافظت می کند اما سایه گذاری دیجیتالی دسترسی به اطلاعات تصویر را

[1] . Digital watermark

محدود نمی کند. رمزگذاری محتویات را در طول انتقال داده از فرستنده به گیرنده محافظت می کند اما سایه گذاری دیجیتالی دسترسی به اطلاعات تصویر را محدود نمی کند.دیجیتال واترمارک در موارد زیادی کاربرد دارد که می توان به موارد زیر اشاره کرد :

۱- حفاظت از کپی رایت: امکان قرار دادن اطلاعات کپی رایت در محتوای فایل مانند نمایش اطلاعات درباره سازنده آن و انتشار اخطار درباره استفاده غیر مجاز.

۲- سندیت (بدون نقص) : قرار دادن اطلاعات مربوط به احراز هویت یا سندیت اطلاعات مانند استفاده از اطلاعات به عنوان رمز ورود و ذخیره کردن اطلاعات شخصی که مورد نیاز *e-comerce* است مشابه کلیدهای عمومی و خصوصی.

۳- ارتباط امن و غیر قابل رویت: در کاربردهایی که فایلها از طریق *attachment* های *E-mail* منتقل شده و یا محلهایی ذخیره می شوند که قابل دسترس عموم می باشند.

۴-بر چسب گذاری و حاشیه نویسی مخفی: مانند درج شماره شناسایی (*ID*) ، کلمات کلیدی برای جستجوی اطلاعات و خصوصیات فایل

۵- نمایش برچسب : در مواردی که کاربر مایل می باشد که نام صاحب یا سازنده توسط تمامی کاربران اعم از کاربران مجاز و غیرمجاز رویت شود .

۶- ایجاد شرایط دسترسی به تصویر : به کمک تکنیکهای واترمارک می توان افرادی را که می توانند تصاویر خاصی را رویت نمایند(مستقل از اینکه تصویر در اختیار چه کسانی است) محدود نمود.

۷- حفاظت از داده در مقابل نفوذگران شبکه: با ذخیره سازی اطلاعات بصورت واترمارک شده حتی اگر نفوذگران شبکه به اطلاعات دسترسی پیدا کنند امکان سوء استفاده از تصاویر و یا اطلاعات وجود ندارد.

۸- واتر مارک در تجارت : با گذشت زمان با توجه به اهمیت تجارت و گسترش رسانه های دیجیتالی ، تکنولوژی تجارت الکترونیک بوجود آمد و در این راستا تکنولوژی دیجیتال واتر مارک نیز گسترش یافت .

یک سیستم پرداخت الکترونیکی باید ویژگی هایی داشته باشد تا بشود آن را به گستردگی به کار برد. برخی از مهمترین این ویژگی ها عبارتند از: امنیت و قابل اطمینان بودن - قابلیت تغییر اندازه - اختفا - تطابق و تقابل انعطاف پذیری - قابلیت تبدیل - کارایی - سادگی کار - استفاده *offline* - باز بودن سیستم برای همگان .با توجه به خصوصیات یک سیستم تجارت الکترونیک در این راستا تلاش شده است تا از تمامی راه حلهای امنیتی که از جمله آن دیجیتال واترمارک می باشد ، استفاده شود . و با واترمارک کردن اسناد می توان آنها را در مقابل حملات و جعل سند محافظت کرد .

Digital watermarking یک تکنولوژی مناسب برای بر طرف کردن مشکلات امنیتی است که این مشکلات بوسیله روش های رمز نگاری رایج حل نمی شود. برای فراهم آوردن امنیت در یک فرایند چندرسانه ای نیاز به سه سطح امنیتی داریم: ارتباط مطمئن و امن – کنترل نحوه استفاده و دسترسی (کنترل چگونگی استفاده از فرایند) مدارک و ابزار لازم جهت پیگیری استفاده غیر قانونی. که این موارد مکملی برای حفاظت از کلیه قسمتهای بکار گرفته شده در یک فرایند تجارت چند رسانه ای می باشد و *Digital watermarking* مدارک لازم و قابلیت پیگیری برای کپی های غیرقانونی و همچنین توزیع اطلاعات چند رسانهای را فراهم می کند.

۹- پایگاه داده ها و واتر مارک: یکی از مهمترین اطلاعاتی که در شبکه های مختلف بخصوص اینترنت روزانه با حجم زیادی در حال انتقال می‌باشد، اطلاعات پایگاه داده ای و جداول اطلاعاتی می‌باشد که حفاظت آنها به خصوص در مواردی که این اطلاعات، اطلاعات مالی می باشند از اهمیت خاصی برخوردار است. یکی از روشهایی که در این زمینه می‌تواند موثر واقع شود دیجیتال واتر مارک است. اعمال واترمارک در بانکهای اطلاعاتی به دو صورت امکان پذیر است : ۱- اضافه کردن اطلاعات به کل فایل با توجه به روشهای موجود برای واترمارک . ۲- اضافه کردن اطلاعات به هر رکورد داده یا به رکوردهای خاص

۱۰- کاربرد واترمارک در سیستم عامل: یکی دیگر از کاربردهای *Watermark* استفاده از این تکنیک در ساختار سیستم عاملها می باشد. با اعمال *Watermark* در قسمتهای مختلف سیستم عامل از قبیل نحوه ذخیره سازی سیستم فایلها می توان به سیستم عامل منحصر به فردی رسید که قابلیتهای خاص داشته باشد، همچنین می توان برای احراز هویت کاربران

نیز از این روشها استفاده کرد. در این گونه کاربردهـا *Watermark* بـصورت یـک *component* در داخـل سیـستم عامـل نـصب می شود.

۱۱- کاربردهای غیر تصویری واتر مارک: واترمارک در صوت نیز می تواند به دو صورت قابل شـنیدن و غیـر قابـل شـنیدن اعمال شود. همچنین در تصاویر متحرک نیز می توان از واترمـارک اسـتفاده کـرد، ایـن روش مـی توانـد در محیطهـای فعـال (متحرک) مانند ویدئو نیز اجرا شود.

۱۲- واترمارک در امضای کور : کور کردن امضای دیجیتال براحتی توسط روشهای مختلف در واترمارکهای غیر قابل رویـت امکانپذیر است.

این مقاله شامل بررسی الگوریتمهای مختلف اعمال واترمارک و بررسی پیاده سازی روشی امن در جهـت اعمـال دیجیتـال واترمارک روی تصویر می باشد . بگونه ای که احراز هویت کاملا صحیح صورت گیرد.

[۱۷،۱۳،۱۱،۹،۸،۶،۵،۴،۳،۲،۱]

۲- الگوریتمهای مختلف اعمال دیجیتال واترمارک

۲-۱- تغییر کم اهمیت ترین بیت [1] :

اکثر روشهای معمول و اخیر در اعمال واترمارک تغییر در کم اهمیت ترین بیت (*LSB*) می باشد البته در ایـن روش فـرض می شود داده ای که در کم اهمیت ترین بیت (*LSB*) موجود است فاقد معنی و اهمیت می باشد . در راستای الگـوریتم تغییـر در *LSB* روشهای مختلفی موجود است که تفاوت آنها به دو صورت ظاهر می شود : ۱- نوع تغییرات اعمال شـده در *LSB* ۲- نحوه تعیین بایتهایی که قرار است *LSB* آنها تغییر کند. هر دو مورد فوق می توانند با قرارهـای قبلـی یـا بـر اسـاس یکـسری قوانین ریاضی خاص و یا به صورت تصادفی تعیین گردند.لازم به ذکر است بین الگوریتمهای موجوددر اعمال واترمـارک ، روش تغییر در *LSB* از نظر امنیتی جزء مطمئن ترین روشها محسوب می شود.

۲-۲- برچسب گذری اطلاعات:

این روش در مورد رسانه های دیجیتالی چون تصویر و ویدئو به کار مـی رود و عبارتـست از افـزودن برچـسب بـه صـورت الگوهای کوچک هندسی. این روش برای داده های صوتی قابل اعمال نیست زیرا در مقابل اعوجاجهای هندسی معمول از جمله بریدن مقاوم نمی باشد . در این الگوریتمهای نیز روشهای مختلفی ایجاد شده که دارای پایه و اساس یکسان می باشد و تفـاوت آنها در نحوه و تعیین محل و برچسب گذاری می باشد.

۲-۳- قرار دادن نویزهای تدریجی [2] :

در این روش اطلاعاتی که قرار است صورت تکنولوژی واترمارک به تصویر اضافه شود در قالب نویز اعمال می شـود کـه در این راستا نیز روشهای زیادی وجود دارد که مربوط نحوه اضافه نمودن نویز و مقدار آن می باشد از معمـولترین روشـها در ایـن الگو می توان اضافه کردن نویز به *LSB* ها به صورت تصادفی را نام برد.

۲-۴- روشهای آماری:

---

1 . least significant Bit Modification

2 . Quantigation Noise Emtedding

در این الگو اطلاعات قالب واترمارک بر اساس فرمولهای آماری موجود و یا بر اساس آمارگیری از کل پیکسلها در تصاویر انجام و به تصویر اعمال می شود و به همین دلیل در این الگو نیز. روشهای مختلفی وجود دارد و معمولترین آنها انتخاب n جفت تصادفی می باشد که شامل b_i ها و a_i ها می باشد و از روشنایی a_i ها کاسته و به b_i ها افزوده شد، و از نظر آماری روشنایی کل تصویر تغییر نکرده و اطلاعات واترمارک بر اساس شماره پیکسلهای b_i, a_i و محتویات آنها تعیین می گردد . یکی از مهمترین نقایص این روش عدم مقاومت در برابر تبدیلات هندسی می باشد.

۲-۵- استفاده از *checksum* :

در این روش الگو برای ایجاد *check sum* اغلب هفت بیت با ارزش در هر بایت مد نظر است که در این روش اگر امنیت در مقابل زمان بسیار قابل توجه باشد . از تابع *SHA1* به عنوان *Checksum* استفاده می شود و بگونه ای که فایل مورد نظر در تابع در هم ساز قرار گرفته و خروجی آن که یک ۲۰ بایتی منحصر به فرد می باشد . در حالتی که زمان اهمیت بسیار زیادی دارد از روشهای ساده تری که به صورت قراردادی است استفاده می شود که البته هیچکدام مانند *SHA1* استاندارد نیستند.

۲-۶- روشهای ترکیبی:

در این روش محققین با بررسی هدف و کاربرد مورد نظر روشها و الگوریتمهای موجود را با هم ترکیب یا آنها را تغییر می دهند و یا روشی دیگر ابداع می کند و بطور کلی امروزه برای کاربردهای خاصی از واترمارک خاصی استفاده می کنند.
[۱۴،۸،۷،۶،۴] .

۳- نحوه پیاده سازی

اعمال واترمارک باید بگونه ای باشد که نه تنها تمامی خصوصیات واترمارک را در بر داشته باشد بلکه اهداف کاربر را نیز شامل شود. در این راستا روشی ارائه شده که واترمارک به دو صورت قابل رویت و غیر قابل رویت روی تصویر قرار گرفته و تا حد امکان کلیه خصوصیات مورد نظر کاربران را فراهم کند و اعمال آن به صورت زیر می باشد.

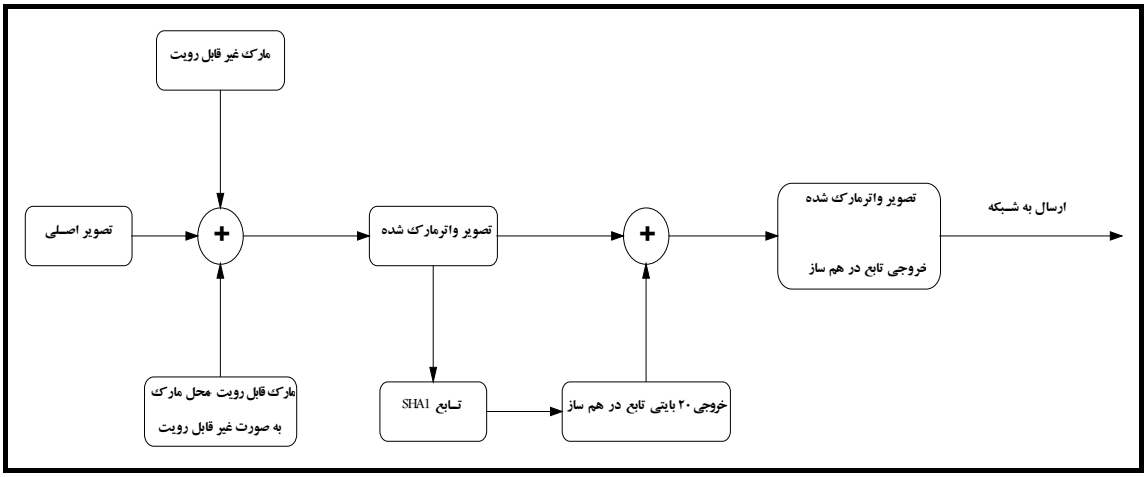
ابتدا فایل تصویر که در قالب بیت مپ می باشد خوانده می شود با توجه به آن می توان سایز تصویر (طول و عرض)، تعداد کل پیکسلها، تعداد بیاتها در هر پیکسل را مشخص کرد، و هدر فایلهای بیت مپ ۵۴ بایت است که ۲۰ بایت پایانی آن مورد استفاده قرار نمی گیرد، به عبارتی دیگر با تغییر محتویات آنها تصویر کوچکترین تغییری نمی کند که می توان در این ۲۰ بایت اطلاعات *Checksum* را قرار داد اما از آنجایی که با تغییر قالب هدر به کلی تغییر می کند نمی توان *checksum* اصلی که همان تابع در هم ساز تصویر است را در این ۲۰ بایت قرار داد بنابراین یک سری حسابی که جمله اول و قدر نسبت می تواند یک مقدار مشخص و قراردادی باشد و یا اینکه به صورت تصادفی انتخاب و برای چک کردن آن از سمت گیرنده از کلید عمومی و خصوصی استفاده کرد . این نوع واترمراک به صورت غیر قابل رویت [1] می باشدزیرا در حالت عادی و توسط کاربران غیر مجاز قابل درک و رویت نمی باشد . در سمت گیرنده در راستای احراز هویت تصویر با داشتن جمله اول و قدر نسبت سری، صحت آن ، چک می شود و در صورت درستی دیگر و اترمارکهای اعمال شده بررسی می شود.

فایل تصویر موجود همانطور که گفته شد دارای یک واترمارک قابل رویت است که صاحب یا به عبارتی فرستنده تصویر را مشخص می کند و برای تمامی افراد (مجاز و غیر مجاز) قابل رویت است . محل این واترمارک که توسط مالک تعیین می گردد و در تصویر با استفاده از الگوریتم تغییر در *LSB* قرار می گیرد . که محل آن با استفاده از قدر نسبت سری موجود در هدر مشخص می شود . در سمت گیرنده در ادامه احراز هویت تصویر ، ابتدا گیرنده مارک قابل رویت تصویر را بررسی و اگر مربوط

[1] . invisible

به گیرنده باشد فایل را خوانده و محل آن را با محل واقعی تصویر مقایسه می کند. در صورتی که هر دو یکسان باشند ، بایتهای حاصل اطلاعات مربوط به محل فایل تغییری نکرده اند.

در پایان اصلی ترین واترمارک که به صورت *check sum* و بر اساس تابع در هم سازی ایجاد می شود و در تصویر اعمال می شود و همانطور که مشخص است تابع در هم ساز یک به یک بوده و با کوچترین تغییری ، تغییر می کند. ابتدا بر اساس مشخصات فیزیکی موجود رنگ مارک قابل رویت را مشخص کرده سپس با رنگ بدست آمده تصویر در محل مورد نظر کاربر واترمارک شده و فایل تصویر بدون در نظر گرفتن هدر در تابع در هم ساز قرار می گیرد . این تابع ۲۰ بایت خروجی دارد که از آن، رنگ مارک نهایی تعیین می گردد و تصویر با رنگ جدید واترمارک شده البته واترمارکهای قبلی که گفته شده همزمان در تصویر اعمال می شود و در پایان خروجی تابع در هم ساز در انتهای فایل اضافه و تصویر آماده ارسال می باشد. در سمت گیرنده نیز اگر بر اساس سه مارک اولیه احراز هویت، صحیح صورت گرفت، بر طبق الگوریتم رنگ مارک اولیه با توجه به مشخصات فیزیکی تصویر به دست آمده و تصویر آن رنگ واترمارک شده، در تابع در هم ساز قرار می گیرد اگر ۲۰بایت خروجی این تابع، ۲۰ بایت پایانی تصویر برابر باشد، تصویر بدون کوچکترین تغییر و کاملا صحیح از فرستنده مورد نظر دریافت شده است.[۱۶،۱۵،۱۲،۱۴]



شکل ۱- الگوی الگوریتم اعمال دیجیتال واترمارک

۴- نتیجه گیری و پیشنهاد :

واتر مارک نه تنها می تواند از کپی رایت حمایت کند و براحتی رسانه های دیجیتالی را از اصل آنها تشخیص دهد بلکه میتوان در کنار رمزگذاریها وبا پوشش معایب آنها یک سیستم امن ایجاد کند . واترمارک خود می تواند به عنوان ابزاری در جهت حمله استفاده شودکه می توان به روشهای زیر اشاره کرد :

۱-تغییرات محلی : در این نوع حملات ، کدهایی که در تصویر به صورت مارک قرار گرفته است ، تغییر داده می شود .۲- مرتب سازی مجدد : در این روش کدها از طریق تعداد زیادی از قطعه کدهای مستقل مجددا مرتب شده و نهایتا این روش الگوهای مختلف را بوجود می آورد .۳- اضافه کردن کد :در این روش تعدادی کد به تصویر اضافه شده که البته این قطعه کدها باعث غیرقابل رویت شدن تصویر می شوند . ۴- غیر کامپایل شدن کد :در این روش با تغییر هدر فایل ،تصویر در برنامه مورد نظر غیرقابل کامپایل شدن می شود .۵- فشرده سازی کد : در این روش با استفاده از الگوریتمهای فشرده سازی ،تصویر فشرده و سپس در بایتهای باقیمانده ،کدهای ضد فشرده سازی گذاشته می شود یعنی امکان بازکردن تصویر نمی باشد .

همچنین در ادامه این کار می توان به بررسی روشی پرداخت که در تبدیل قالب تصاویر اطلاعات واترمارک تغییر نکند.

۵- مراجع :

1) Cox, J. Kilian, F. T. Leighton, and T. Shamoon, "Secure spread spectrumwatermarking for multimedia," IEEE Trans. Image Processing, Dec. 1997.

2) F. M. Boland, J. J. K. Ó Ruanaidh and C. Dautzenberg, "Watermarking digital images for copyright protection," Proceedings of the International Conference on Image Processing and its Applications , July

3) F.mintzer,G.Braudaway,and M.M yeung,"Effective and ineffective digital watermark",in proceeding of ICIP,(Santa Barbara,CA),October 1997.

4) F.Y.Duan,I.King-A short summery of Digital Watermarking Techniques for multimedia Data

5) Funda Ergun, Joe Kilian, and Ravi Kumar. A note on the limits of collusion resistant watermarks. In Jacques Stern, editor, Advances in Cryptology – EUROCRYPT'99, volume 1592 of Lecture Notes in Computer Science.Springer-Verlag, 1999.

6) gordon w.braudaway.protecting publicly available image with an invisible image watermark in proceedings,1997 IEEE international conference on image processing ,santa barbara ,CA,USA,Oct.1997

7) http://www.watermarkingworld.org

8) http://www.watermarkrs.com

9) Jian Zeho , Applying Digial Watermark techniques to online multimedia commerce

10) M. D. Swanson, M. Kobayshi, and A. H. Tewfik, "Multimedia dataembedding and watermarking technologies," Proc. IEEE, June 1998.

11) M.M.yeung and F.Mintzer,"An invisible watermarking technique for image verification",in proceedings of ICIP,(Santa Babara,CA),October 1997.

12) Man Young Rhee – Internet Security

13) P. Wolfgang and E. Delp, "A watermark for digital images," in Proc.IEEE Int. Conf. Image Processing, Lausanne, Switzerland, Sept. 1996

14) ping wah wong.A public key watermark for image verification and Authentication

15) R. Venkatesan and M. H. Jakubowski, "Image hashing," DIMACS Conf. on Intellectual Property Protection, Piscataway,NJ (USA), Apr. 2000

16) R. Venkatesan, S.-M. Koon, M. H. Jakubowski, and P. Moulin - ROBUST IMAGE HASHING

17) W. Stallings, Cryptography and Network Security, Prentice Hall, New W. Bender, D. Gruhl, N. Morimoto, and A. Lu, "Techniques for Data Hiding," IBM System, no. 3–4, February 1996.