پایان نامه دوره کارشناسی ارشد مهندسی برق مخابرات

واترمارکینگ تصویر با امنیت بالادر برابر حملات و بررسی امنیت با تئوری اطلاعات

هامرز هادی‌پور

استاد راهنما:

دکتر غزاله سربیشه‌ئی

اساتید دفاع:

دکتر احدی اخلاقی و دکتر اسدپور

پاییز ۹۱

به نام یزدان بخشاینده

این پایان نامه را با تمام وجود به مادر مهربان و پدر فداکار و خانواده عزیزم تقدیم می کنم شاید

قطره ای کوچک باشد در مقابل دریای بی کران زحماتشان.

تقدیر و تشکر :

با تشکر از سرکار خانم دکتر سربیشه‌ای که با وجود مشغله زیاد در تهیه این مطالب کمک بسیاری نمودند و اگر زحمات ایشان نبود هرگز این پروژه به نتیجه نمی‌رسید. همچنین از جناب دکتر احدی اخلاقی و جناب دکتر اسدپور که ارائه این پروژه را پذیرفتند سپاسگزارم.

چکیده :

با توجه به گسترش روز افزون ارتباطات در دنیای امروز ، ضرورت کنترل بهینه ارتباطات در محیط‌های گوناگون اداری ، چندرسانه ای ، فیزیکی ، دیجیتالی و امنیتی بیش از پیش روشن می‌شود. حفاظت از داده ها در مقابل کپی برداری و جعل از اهمیت بالایی برخوردار است به همین دلیل باید از راهکارهایی برای کنترل کپی کردن استفاده نمود .یکی از این راهکارها ، استفاده از تکنیک واتر مارکینگ می باشد.واتر مارکینگ به معنای پنهان کردن داده ها در تصاویر است به نحوی که با چشم قابل تشخیص نباشد و فقط افراد مجاز قادر به استخراج این داده ها باشند.

در این پایان نامه ابتدا با واترمارکینگ که یکی از مهمترین روش های مخفی کردن اطلاعات است آشنا می‌شویم و از اهداف و کاربردهای واترمارکینگ، دسته بندی آن وپارامترهای تاثیر گذار روی آن سخن می‌گوییم. همچنین به معرفی تئوری کدینگ و توضیحات مختصری از کدینگ BCH و Reed- Solomon می‌پردازیم.

در ادامه الگوریتمی مقاوم برای واترمارکینگ معرفی می‌کنیم که مبتنی بر SVD و DWT است و برای بهتر کردن مقاومت آن از کدینگ‌های تصحیح خطا استفاده می‌کنیم که در دو مرحله اعمال می‌شود و در نهایت برای اندازه گیری مقاومت یک الگوریتم با تئوری اطلاعات به معیاری برای مقاومت می‌رسیم که نتایج شبیه سازی، بالا بودن مقاومت الگوریتم پیشنهادی از نظر همبستگی و تئوری اطلاعات را نسبت به الگوریتم‌های پایه معرفی شده نشان می‌دهد.

فهرست مطالب

فصل چهارم:

فصل پنجم:

فهرست اشکال و جداول

فصل اول

مقدمه

رمز نگاری[1] و پنهان نگاری(متدهای پنهان سازی اطلاعات)هر کدام سیر تکاملی خود را از سالهای دور تاکنون پیموده اند. ردپای رمز کردن اطلاعات را اول بار می‌توان در حوالی سال ۱۹۰۰ پیش از میلاد جست ، که در آن زمان مصریان باستان از نوعی الفبای هیروگلیف نا متعارف درکتیبه‌های خطی خود استفاده می‌کردند.

در حدود ۵۰۰ سال قبل از میلاد ، یهودیان از الفبای" آتباش"که نوعی الفبای رمز وارونه است استفاده می‌کردند. در حدود سال ۵۰ تا ٦۰ قبل از میلاد جولیوس سزار از نوعی الفبای رمز برای مکاتبات حکومتی استفاده می‌کرد. یونانیان قدیم برای ارسال پیام‌های محرمانه خود اقدام به تراشیدن سر بردگان می‌کردند و با استفاده از سوزن وخال کوبی پیام محرمانه مورد نظرشان را روی پوست سر بردگان می‌نوشتند و بعد از مدتی که موی سرشان رشد کافی می‌کرد و کاملا روی پیام را می‌پوشاند، آنها را به سمت مقاصد مورد نظر می‌فرستاند و در آنجا هم با تراشیدن سرآنها به پیام مورد نظر می‌رسیدند درحالیکه خود بردگان از پیام نوشته شده بر روی سرشان مطلع نبودند.

در جنگ آمریکا، نیروهای انگلستان و آمریکا هر دو، از نوعی جوهرهای نامرئی برای رمز گذاری استفاده کردند. استفاده از جوهرهای نامرئی با استفاده از آبلیمو، آب پیاز، مخلوط شیر و سرکه یک از روشهای بسیار رایج در مخفی نویسی بود. به طوریکه با این جوهرها در بین سطرهای یک نامه معمولی، پیام‌های خود را می‌نوشتند و سپس ارسال می‌کردند. وگیرنده‌ها برای آشکار سازی به حرارت دادن نامه می‌پرداختند. واترمارکینگ نیز بعنوان یک تکنیک در فرآیند پنهان نگاری امروز مورد توجه واقع شده است.

واترمارکینگ شاخه‌ای از فرآیند پنهان نگاری[2] محسوب می‌شود که نخستین بار در سال ۱۹۹٦ معرفی شد. تکنولوژی واترمارکینگ دیجیتال به کاربرها اجازه می‌دهد تا اطلاعات را در محتویات دیجیتال مانند متن، تصویر ثابت، ویدئو و صوت وارد کنند. این اطلاعات وارد شده معمولا غیر قابل مشاهده (نامرئی) است که بعدا می‌تواند تشخیص داده شود و یا استخراج گردد. الگوریتم‌های واترمارکینگ، به منظور درج اطلاعات سیگنال پیام در داخل داده میزبان، تغییرات کوچکی را بر اساس سیگنال پیام در داده میزبان، ایجاد می‌کنند، به نحوی که با چشم انسان قابل مشاهده نباشد. به اطلاعات وارد شده واترمارک[3] گفته می‌شود.

واترمارکینگ بعنوان یک روش در حفاظت کپی رایت و جلوگیری از تکثیر غیر قانونی اطلاعات، روش مناسبی محسوب می‌شود. روش‌های واترمارکینگ در حوزه مکان و در حوزه فرکانس کار می‌کنند. حوزه مکان ظرفیت بالا و مقاومت پایین تری دارد در حالی که حوزه فرکانس مقاومت بیشتری دارد.

در سال‌های اخیر، با توسعه سریع MMS و سایر تجارت‌های دیجیتالی، استفاده غیر قانونی از تصاویر دیجیتال و حملات از قبل بیشتر و جدی‌تر شده است. حفاظت از محتوای چند رسانه‌ای اخیرا به یک مسئله مهم به دلیل انتقال از فن‌آوری-های آنالوگ به دیجیتال تبدیل شده است. با این حال ، رسانه‌های دیجیتال نیز باعث ایجاد فرصت‌های گسترده برای

[1] cryptography
[2] steganography
[3] watermark

دزدی از داده‌های دارای کپی رایت می‌شود. بنابراین بسیار مهم است که راه و وسیله‌ای برای تشخیص نقض کپی رایت و کنترل دسترسی به رسانه‌های دیجیتال موجود باشد.

هر الگوریتم واترمارکینگ دیجیتال دارای ویژگی های مختلفی از مانند مشاهده ناپذیری , امنیت و نیرومندی می باشد که تلاش واترمارکر در جهت ایجاد میزان مناسبی از هر یک از این ویژگیها با توجه به نوع کاربرد الگوریتم واترمارکینگ می باشد. همچنین مقاوم کردن داده‌های واترمارک در مقابل حملات مختلف از اهمیت بسیاری برخوردار است و امروزه تلاش‌های زیادی برای بدست آوردن مقدار عددی برای امنیت داده‌های واترمارک انجام می‌شود.

در این پروژه ما تلاش داریم تا الگوریتم مقاومی در برابر حملات مختلف برای واترمارکینگ ارائه کنیم و با توجه به تئوری اطلاعات معیاری هم برای امنیت الگوریتم بدست آوریم.

در فصل ۱ تاریخچه‌ای از علم واترمارکینگ ارائه شده و انواع تکنیک‌ها، خواص و کاربردهای واترمارکینگ به ویژه واترمارکینگ تصویر در فصل ۲ آمده است. در فصل ۳ با تئوری کدینگ و کدینگ‌های استفاده شده در این پروژه آشنا خواهیم شد. سپس در فصل ۴ و۵ به الگوریتم پیشنهادی ونتایج شبیه سازی و محاسبه مقداری برای امنیت الگوریتم می-پردازیم.

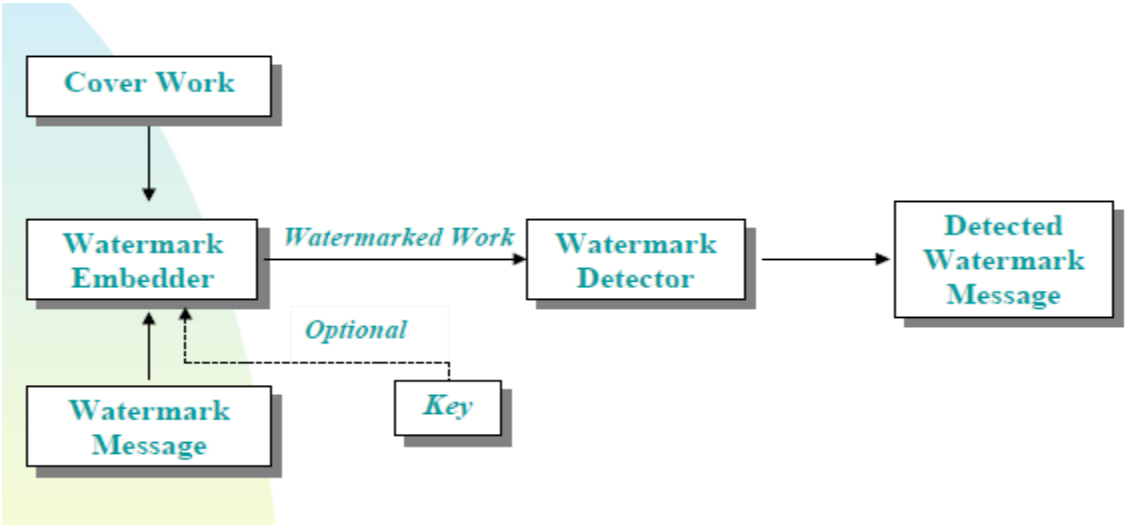
فصل دوم

واترمارکینگ دیجیتال

در این بخش ابتدا واترمارکینگ و کاربردهای آن، انواع تقسیم بندی آن و معیارهای مهم برای الگوریتم‌های واترمارکینگ بررسی می‌شود سپس انواع روش‌های جاساز کردن واترمارک در داده‌های مختلف را معرفی می‌کنیم و در هر روش به طور خلاصه تکنیک‌های مختلف و پرکاربرد نیز بیان می‌شود.

۲-۱ الگوی عمومی واترمارکینگ:

شکل ۲-۱ حالت عمومی واترمارکینگ را که تمام الگوریتم‌ها استفاده می‌کنند نمایش می‌دهد.



شکل ۲-۱: الگوی عمومی واترمارکینگ

۲-۲ اهداف و کاربردهای واترمارکینگ[۱و۲]:

واترمارکینگ دارای کاربردهای متفاوتی می‌باشد که در اینجا به اختصار به برخی از این کاربردها اشاره می‌شود.

حفظ کپی رایت[1]

افزایش سرعت اینترنت و پیشرفت در زمینهٔ تکنیکهای فشرده سازی با عث شده تا استفاده از محصولات چندرسانه‌ای در این بستر رونق چشمگیری پیدا کند. امروزه منابع دیجیتال براحتی توسط افراد مختلف در اینترنت به اشتراک گذاشته می‌شوند و این مطلب باعث نگرانی تولیدکنندگان آثار چندرسانه ای شده است معمول ترین روش برای حفظ امنیت در نقل و انتقال تصاویر دیجیتال درج کردن یک امضای دیجیتال در تصویر اصلی به منظور اثبات و اعلان مالکیت تصویر برای صاحب اصلی آن است.

محافظت از کپی برداری[2]

به معنای مقابله با تکثیر و نظیر مقابله با تکثیر غیرقانونی تولیدات نرم افزاری، فیلم، موسیقی، انیمیشن، تصویر، کتب الکترونیک، نشریات و... می‌باشد.

صحت داده[3]

واترمارک برای شناسایی تغییرات اعمال شده در پوشش رسانه مورد استفاده قرار می‌گیرد. نویسنده دارای یک کلید منحصر به فرد در ارتباط با محتوا است و می‌تواند درستی آن محتوا را با استخراج واترمارک تایید کند. به عنوان مثال: چک کردن برای عکس تقلبی گذرنامه

ارتباطات رمزی و محرمانه[4]

نظیر استفاده در ارگانهای نظامی و انتظامی، تامین امنیت ملی کشورها، استفاده در اهداف جاسوسی، استفاده در جنگها برای مخابره اخبار و آگاهی از وضعیت دشمن، خرابکاری، عملیات بمب گذاری.

[1] Copyright protection
[2] Copy protection
[3] Data authentication
[4] Concealed communication

کاربرد های متفرقه واترمارک

می‌توان به فرآیندچاپ اسکناس، صدور اوراق هویت، صدور اوراق بهادار، صدور اسناد تجاری، بررسی اسناد دادگاهی و حفاظت از آنها، کاربرد در پزشکی قانونی، کاربرد درآموزش الکترونیک، کاربرد در علامت گذاری و...

۲-۳ انواع واترمارک:

۲-۳-۱ دسته بندی از نظر قابلیت ادراک:

- مرئی/شنیدنی[۱]

واترمارک بوسیله حس بینایی یا شنوایی انسان قابل تشخیص است.

- نامرئی/غیر قابل شنیدن[۲]

واترمارک توسط سیستم بینایی یا شنوایی انسان قابل تشخیص نیست.

۲-۳-۲ دسته بندی ازجنبه مقاومت :

- شکننده[۳]

تغییر محتوای فایل میزبان به و اترمارک صدمه می‌زند یا حتی آن را از بین می‌برد.

- نیمه شکننده[٤]

در مقابل بعضی حملات شکننده و بعضی حملات مقاوم است.

- مقاوم[٥]

تغییر محتوای فایل میزبان به واترمارک خدشه‌ای وارد نمی‌سازد .

۲-۳-۳ دسته بندی ازجنبه داده مورد نیاز برای استخراج :

- کور[٦]

[1] Visible/audible
[2] Invisible/inaudible
[3] fragile
[4] Semi-fragile
[5] robust
[6] blind

- آگاه(بینا) [1]

۲-۳-٤ دسته بندی از جنبه نوع سندی که واترمارک می‌شود[2] :

- متن
- صوت
- تصویر
- ویدیو

۲-۳-۵ دسته بندی از نظر روش پردازش[3] :

- فضایی(مکانی)
- طیفی(فرکانسی)
- ترکیبی (هیبرید)

۲-۴ پارامترهای تاثیر گذار در واترمارکینگ[۳،۲] :

- **مقاومت**

مفهوم مقاومت این است که واترمارک بتواند پس از عملیات معمول رسانه‌ای از قبیل فیلتر کردن، فشرده سازی با اتلاف، تصحیح رنگ، و یا تشخیص دادن هندسی آشکارسازی شود. هیچ کس قادر به حذف، تغییر و یا آسیب واترمارک بدون کلید مخفی نباشد. این پارامتر هر چقدر بالاتر باشد نشانه آن است که میزان تخریب و اثرپذیری واترمارک در اثر تغییرات در فایل میزبان کمتر است.

- **شفافیت دید**

محتوای واترمارک شده دارای کیفیت معقول همانند محتویات اصلی است. این پارامتر مشخص می‌نماید که حداکثرمجاز اثرگذاری واترمارک در فایل میزبان (برای آنکه شناسایی نشود) چقدر است.

[1] informed
[2] Inserted media
[3] Processing method

- **ظرفیت**

میزان واترمارکی که می‌تواند وارد یا استخراج شود. این پارامتر حداکثر حجم ممکن که میزبان برای واترمارک قادراست فراهم کند مشخص می‌کند.

- **امنیت**

این پارامتر تا حدودی شبیه به مقاومت است و تعیین می‌کند که فایل میزبان تا چه میزان وجود واترمارک را می‌تواند مخفی نگه دارد. امنیت به معنای این است که واترمارک وارد شده نمی‌تواند حذف شود.

- **پیچیدگی**[1]

پیچیدگی به عنوان تلاش و زمان مورد نیاز برای وارد کردن و بازیابی واترمارک شرح داده شده است.

۲-۵ مقایسه روش‌های واترمارکینگ :

- حوزه مکان: شفافیت نسبتا زیاد، ظرفیت بالا، پیچیدگی کمتر، ولی مقاومت کمتری دارند.
- حوزه فرکانس: ظرفیت این حوزه بستگی به ویژگی‌های ظاهری تصویر و تنوع رنگ به کار رفته در آن دارند مقاومت این تبدیل‌ها نسبت به حوزه مکان بیشتر است. ولی پیچیدگی زمانی زیادی دارند.

۲-۶ روش‌های واترمارکینگ:

۲-۶-۱ واترمارکینگ متن[2]

این روش در محافظت از مدارک الکترونیکی و مدارک کاغذی که به صورت الکترونیکی کپی و توزیع می-شوند کاربرد دارد. ولی یکی از مشکلات این است که باید هر کپی به صورت جداگانه نشانه گذاری شود .

تکنیک‌ها :

- روش‌های فاصله باز: فاصله گذاری داخل جمله، فاصله‌های پایان خط، فاصله گذاری داخل کلمه
- روش‌های ترکیبی[3]
- روش‌های معنایی

[1] complexity
[2] Text-based watermarking
[3] Syntactic methods

۲-۶-۲ واترمارکینگ تصویر

از خصوصیاتی که این تکنیک باید داشته باشد این است که برای اینکه مانع دید تصویر اصلی نشود باید نامرئی باشد. برای اینکه شناسایی و پاک نشود باید به طور آماری نامرئی باشد. استخراج واترمارک از تصویر، ساده باشد در غیراین صورت روند آشکارسازی به زمان محاسبه بیشتری نیاز دارد.

تکنیک ها :

بیت با کمترین ارزش[۱]

تکنیک‌های بر مبنی همبستگی[۲]

تکنیک‌های طیف گسترده[۳]

تکنیک‌های حوزه تبدیل[٤]

- تبدیل ویولت[٥]
- تبدیل کسینوسی گسسته (DCT)[٦]

۲-۶-۳ واترمارکینگ صوت

تولید فایل صوتی بدون قابلیت دستکاری، فراهم کردن درجه‌های دسترسی مختلف، مناسب کردن سیگنال صوتی برای نیازهای مختلف کاربران از کاربردهای این تکنیک است. از خصوصیات این تکنیک این است که واترمارک به طور ادراکی غیر قابل شنیدن است، به طوری که هیچ تنزل کیفیت ادراکی در فایل صوتی اتفاق نمی‌افتد.

۲-۶-۴ واترمارکینگ ویدیو

[1] Least significant bit
[2] Correlation-based techniques
[3] Spread spectrum techniques
[4] Transform domain techniques
[5] Wavelet watermarking techniques
[6] Discrete cosine transform

۲-۷ حملات واترمارکینگ[۲،٤،٥] :

واترمارک دیجیتال به عنوان رمز نگاری داده قابلیت و یا درجه امنیت یکسان ندارد. این کار نه ازمشاهده و یا گوش دادن محتوا، و نه از دسترسی به آن محتوا جلوگیری می‌کند. بنابراین، واترمارکینگ دیجیتال از حملات هکرها مصون نیست. تقسیم بندی های مختلفی برای حملات وجود دارد:

- حملات غیر عمدی[۱]: برش دادن[۲]، فشرده سازی، نویز جمع شونده
- حملات عمدی[۳]: حملات تبانی[٤]، حمله‌های جعل[٥]، حمله‌های تحریف[٦]
- حملات حذف کننده[۷]: فیلتر متوسط گیر،میانه، گوسی

[1] Unintentional attacks
[2] cropping
[3] Intentional attacks
[4] Collusion attacks
[5] Forgery attacks
[6] Distortive attacks
[7] Removal attacks