دانشگاه سیستان و بلوچستان
تحصیلات تکمیلی

پایان نامه کارشناسی ارشد در رشته مهندسی برق- مخابرات

عنوان:

بهبود امنیت و قدرت واترمارکینگ تصاویر دیجیتال در مقابل حملات هندسی و غیرهندسی

اساتید راهنما:

دکتر شهرام مهنا

دکتر فرحناز مهنا

استاد مشاور:

دکتر مهدی رضایی

تحقیق و نگارش:

ژیلا ایوبی

۱۳۹۰

تقدیم به پدر بزرگوار، سخاوتمند و شجاعم که هر چه دارم بعد از خداوندگار متعال از اوست.

تقدیم به مادر مهربان و دلسوزم که دعایش همواره در حقم مستجاب و گره گشای مشکلاتم بوده و هست.

تقدیم به برادرم پیمان، که برادری را در حق من تمام و کمال به اتمام رساند و همواره یار و یاور من بود.

تقدیم به سرزمین مادری ام آذربایجان

و

تقدیم ویژه به زاهدان عزیزم که باب دوستیهای ماندگار زیادی را برای من مفتوح کرد.

سپاسگزاری

حمد و سپاس سزاوار خداوندی است عز و جل که زبان از مدح و حمد ایشان عاجز است. خداوندی که توفیق نوشیدن جرعه ای از دریای علم را نصیب این حقیر سعید کرد. سلام و صلوات بر صفی عالمین محمد مصطفی و سلام بر علی دروازه شهر علم

سپاس از تمامی آموزگاران دوران تحصیلم از ابتدا تا به حال که همیشه مستفیض از محضر ایشان بودم.

تقدیر و تشکر از آقای دکتر شهرام مهنا و خانم دکتر فرحناز مهنا که راهنمایی این پروژه بر عهده ایشان بود.

تشکر از آقای دکتر مهدی رضایی استاد مشاور عزیزم.

و سپاس ویژه از اساتید دانشگاه سیستان و بلوچستان که شاگردی از محضر ایشان همواره باعث افتخار من خواهد بود.

چکیده:

در این پروژه روشی جدیدی برای واترمارکینگ کور تصاویر دیجیتال بر اساس استفاده از نگاشت های آشوبناک در حوزه تبدیل پیشنهاد شده است. هدف اصلی این پروژه بالا بردن امنیت فرآیند درج و استخراج واترمارک و بهبود فرآیند استخراج در مقابل حملات هندسی و غیر هندسی رایج است. به همین منظور در طی دوره تحقیق و بررسی روشهای مختلفی بر روی ایده اصلی انجام پذیرفت و نتیجه حاصل سه الگوریتم متنوع است که هر کدام نسبت به الگوریتم های قبلی دارای پیشرفت هایی است. در الگوریتم اول از یک نگاشت آشوبناک برای رمز نگاری واترمارک و از نگاشتی دیگر برای درج و استخراج واتر مارک در ضرایب تبدیل موجک گسسته با استفاده از روش همسایگی صرایب پیشتهاد شده است. نتایج حاصل از این اگوریتم نشان داد که فضای امنیتی کلید رمز نگاری و کلید واترمارک به طول 10^{112} و مقاومت الگوریتم در مقابل حملات هندسی و غیر هندسی در بعضی از موارد چشمگیر نبوده است. به همین دلیل الگوریتم دوم با همان فرآیند و تنها با تغییر در نگاشت های آشوبناک و در حوزه تبدیل کسینوسی گسسته انجام شد که نسبت به اگوریتم اول دارای نتایج بهتری بوده است. فضای کلید امنیتی برای این الگوریتم 10^{126} و تنها ضعف آن در حملات چرخش و مات کردن تصویر واترمارک شده، بوده است. در الگوریتم سوم مطالعات جدی تری انجام پذیرفت که حاصل آن تغییر اساسی در فرآیند درج و استخراج بود که از روش هیبرید مبتنی بر تجزیه مقدار منفرد در حوزه تبدیل موجک گسسته انجام پذیرفت و همچنین از نگاشت های آشوبناک بهتری نسبت به دو الگوریتم قبل استفاده شده است. حاصل استفاده از الگوریتم سوم فضای کلید امنیتی به طول 10^{154} است و تنها حمله ناامید کننده، حمله چرخش بوده است. البته در این حمله نیز واترمارک از بین نرفته و با اندکی تغییر و جستجو واترمارک قابل استخراج است که این موضوع هدف مطالعات آینده خواهد بود.

کلمات کلیدی: واترمارکینگ دیجیتال ، حفاظت از حق کپی ، امنیت ، استحکام ، حملات هندسی و غیر هندسی

فهرست مطالب

فهرست تصاویر

فصل اول

مقدمه ای بر واترمارکینگ

مقدمه و تعاریف

اگر یک اسکناس ۲۰ دلاری روبروی نور قرار گیرد، گوشه اسکناس تصویر پرزیدنت اندرو جکسون دیده می شود. اگر به گوشه تصویر اندرو جکسون نگاه کنید خواهید دید که تصویر دیگری به صورت واترمارک[1] در آن تکرار شده است. این واترمارک مستقیما در طول فرایند ساخت کاغذ در آن پنهان شده است، بنابراین جعل آن کار بسیار مشکلی است. برای خنثی کردن این روش و برای جعل آن، جاعل ها اسکناس ۲۰ دلاری را می شستند و بر روی همان کاغذ اسکناس ۱۰۰ دلاری چاپ میکردند.

واترمارک روی اسکناس ۲۰ دلاری درست مانند واترمارک های امروزی است و دارای دو مشخصه می باشد که مربوط به موضوع پایان نامه فعلی است.

اول اینکه واترمارک از دید طبیعی پنهان است و فقط زمانی قابل مشاهده است که حاصل یک فرآیند مشاهده خاص باشد (مثلا در حالت نگه داشتن اسکناس رو به نور) علاوه بر کاغذ، واتر مارک را می توان به اشیاء فیزیکی دیگر و سیگنال های الکتریکی اعمال کرد. به عنوان مثال واترمارک بر روی پارچه، بر چسب پوشاک، بسته بندی محصولات و وسایل فیزیکی می تواند با رنگ ها و جو هر های خاصی به کار رود [۱، ۲].

بازنمایی الکترونیکی موسیقی و تصاویر و ویدیو انواع متداولی از سیگنال ها هستند که می توانند واترمارک شوند. مثالی را در نظر بگیرید که شامل واترمارک غیر محسوس باشد ولی اساسا متفاوت از سایر معانی است. یک جاسوس به نام آلیس نیازمند یک ارتباط خیلی مهم با مافوق خود است. آلیس در حال نوشتن نامه ای است تا تعطیلات آخر هفته خود را شرح دهد. بعد از نوشتن نامه جوهر قلمش را با شیر جایگزین می کند و یک پیغام خیلی محرمانه مابین خطوطی که با جوهر نوشته شده می نویسد. وقتی که شیر خشک شد، این پیغام محرمانه برای چشم انسان غیر قابل مشاهده است. وقتی که کاغذ بر روی شمع قرار می گیرد پیام محرمانه قابل مشاهده می شود. این یک مثال ساده ای از استگانوگرافی[2] است.

---

[1] Watermark
[2] Steganography

شکل (۱-۱) اسکناس ۲۰ دلاری

بر عکس واترمارکینگ در استگانوگرافی، پیام پنهان شده نامربوط به محتوای نامه است که فقط به عنوان تله یا پوششی برای پنهان سازی محرمانه برای فرستادن نامه هاست. واترمارکینگ به عنوان عملی برای غیر قابل مشاهده سازی یک اثر متفاوت و برای درج یک پیام در آن اثر تعریف می شود. استگانوگرافی به عنوان عملی برای غیر قابل کشف سازی یک اثر متفاوت و برای درج یک پیام محرمانه تعریف می شود.

اگر چه اهداف واترمارکینگ و استگانوگرافی کاملا متفاوت است ولی هر دو برنامه برخی از عناصر خود را در سطوح بالاتر به اشتراک می گذارند.

هر دو سیستم شامل یک درج کننده[۳] ویک استخراج کننده[۴] است. درج کننده دو ورودی می گیرد، یکی داده ایی است که می خواهیم درج شود (به عنوان مثال، واترمارک یا پیام محرمانه) و دیگری اثرپوششی[۵] است که می خواهیم در آن داده را درج کند. خروجی درج کننده معمولا منتقل یا ضبط می شود. پس از آن اثر واترمارک شده به عنوان ورودی استخراج کننده مطرح می شود. بیشتر استخراج کننده ها سعی می کنند تعیین کنند آیا داده در اثر وجود دارد یا نه و اگر وجود دارد خروجی پیام رمزگشایی شود.

در اواخر سال۱۹۹۰ میلادی سر و صدای زیادی در مورد سیستم های دیجیتالی برای تنوع محتوای واترمارکینگ بوجود آمد. تمرکز اصلی روی تصویر، صدا و ویدیو بود. اما محتوایی چون تصاویر باینری [۳]، متن [۴،

[3] Embedder
[4] Extractor
[5] Cover work

۵، ۶]، خطوط نقاشی [۷]، مدل های سه بعدی [۸، ۹، ۱۰]، پارامترهای انیمیشن [۱۱]، کدهای اجرایی [۱۲] و مدارهای مختلط [۱۳، ۱۴] نیز واترمارک شده اند.

علاقه به استگانوگرافی بعد از حملات تروریستی ۱۱ سپتامبر به میزان قابل توجهی افزایش یافت. وقتی که معلوم شد که تروریست ها برای پنهان سازی ارتباط خود به احتمال زیاد از اولین متد استگانوگرافی استفاده کرده اند و روی شایع ترین نوع مخفی کردن به نام جاسازی روی بیت های کم ارزش [۱۵، ۱۶] در تصاویر نگاشت بیتی تمرکز کرده اند. بعدها تلاش قابل توجهی روی رایج ترین فرمت تصاویر مانند JPEG [۱۷، ۱۸] و فایل های صوتی [۱۹] نیز انجام شد. روش های دقیق برای تشخیص پیام های پنهان شده موجب تحقیق بیشتر برای فایل های چند رسانه ای در استگانوگرافی شد [۲۰، ۲۱].

۱-۱-پنهان شدن اطلاعات ، استگانوگرافی ، واترمارکینگ

پنهان شدن اطلاعات[6]، استگانوگرافی و واترمارکینگ هر سه زمینه های مرتبط و نزدیک بهم هستند که شامل هم پوشانی و اشتراک در تکنیک هستند. با این همه تفاوت های اساسی در طراحی تکنیک ها با هم دارند. در این قسمت درباره این تفاوت ها بحث و گفتگو خواهد شد.

پنهان‌شدن اطلاعات (یا پنهان کردن داده ها) اصطلاحی کلی است که یک دامنه‌ی وسیع از مسایلی فراتر از پنهان سازی پیام در محتوی را شامل می شود. اصطلاح پنهان سازی در اینجا اشاره به غیر قابل مشاهده کردن (همانند واتر مارک) یا نگه داشتن و حفظ اطلاعات سری را دارد. بعضی از نمونه‌های تحقیقاتی در این زمینه ممکن است در کنفرانس‌های بین المللی پنهان‌سازی اطلاعات که شامل مقالاتی در موضوعاتی مانند محافظت شبکه از کاربران ناشناس [۲۲] و حفظ بخش هایی از پایگاه داده های سری از کاربران غیر مجاز یافت می شود [۲۳].

مخترع کلمه استگانوگرافی تریتمیوس است که نویسنده اولین کتابهای رمزنگاری، پلی گرافیا و استگانوگرافیا. اصطلاح فنی استگانوگرافیا از کلمه یونانی استگانو مشتق شده است که به معنی تحت پوشش و گرافیا به معنی نوشتن است. استگانوگرافی هنر پنهان کردن اطلاعات است.

---

[6] Information Hiding

جدول (۱-۱) چهار گروه بندی از مخفی کردن اطلاعات. هرگروه با یک مثال در متن توضیح داده شده است.

	پیام مستقل از اثر پوششی	پیام وابسته به اثر پوششی
حضور مخفی	واترمارکینگ پوششی(مثال ۱)	استگانوگرافی(مثال ۲)
حضور قابل شناسایی	واترمارکینگ آشکار(مثال ۳)	ارتباط درج شده آشکار(مثال ۴)

استگانوگرافی در داستان کهن از هرودوت نقل شده است [۲۴]. که طبق دستور او یکی از بردگانش همراه اربابش هیستاییوس با یک پیغام محرمانه که روی سر برده خالکوبی شده بود به شهر میلتوس در یونان فرستاده می شود. بعد از خالکوبی و گذشت مدت زمانی موهای برده رشد می‌کند و پیغام را مخفی می‌کند. پس از عزیمت آنها به میلتوس، به محض ورود سرش تراشیده می شود و پیغام برای آریستاگوراس نایب السلطنه شهر فاش می شود. پیام دریافتی، حاکم آنجا را برای شورش علیه پادشاه ایران تشویق می‌کند. در این سناریو، پیام دارای ارزش اولیه برای هیستاییوس بوده و برده فقط حامل پیغام بوده است. می‌توان از این مثال برای برجسته کردن تفاوت بین واترمارکینگ و استگانوگرافی استفاده کرد. فرض شود که پیغام روی سر برده قابل دید نباشد، این برده به هیستاییوس تعلق دارد که در این پیغام برده (اثر پوششی) تعریف از واترمارکینگ را برآورده می کند.

ممکن است دلیل این مخفی کاری فقط برای تزیین باشد، بهر حال اگر شخص دیگری ادعا کند که برده مال اوست هیستاییوس می تواند سر برده را بتراشد و مالکیتش را ثابت کند. در این سناریو برده (اثر پوششی) دارای ارزش اولیه برای هیستاییوس است و پیغام اطلاعات مفید را در مورد اثر پوششی فراهم می سازد.

سیستم ها برای درج پیام ها در اثرها می توانند به دو نوع سیستم واتر مارکینگ تقسیم شوند. که در یکی, پیام ارتباط با اثر پوششی دارد، و در سیستم های غیر واترمارکینگ، هر پیامی اثر پوششی غیر مرتبط دارد. آن همچنین می تواند به طور مستقل به سیستم های استگانوگرافی تقسیم شود که در آن وجود پیام به صورت مخفی نگه داشته می شود. در سیستم های غیر استگانوگرافی وجود پیام لازم نیست که مخفی باشد.

این نتایج مربوط به چهار دسته از سیستم های پنهان سازی اطلاعات می باشد که در جدول ۱-۱ خلاصه سازی شده است.

یک مثال از هر چهار دسته به روشن شدن تعاریف موجود در جدول کمک می کند.

۱- در سال ۱۹۸۱ عکسی از اسناد محرمانه کابینه بریتانیا در روزنامه‌ها چاپ شد. شایعه این بود که برای تعیین منبع افشای اطلاعات، مارگارت تاچر به ترتیب کپی اسناد را بین وزیران توزیع کرده بود. در هر نسخه فاصله کلمات متفاوت بود که برای رمز کردن هویت شخص دریافت کننده مورد استفاده قرار گرفته بود. به این ترتیب منبع افشاگری میتوانست شناسایی شود [۲۵]. این مثالی برای واترمارکینگ پنهان است. اطلاعات کدگذاری شده واترمارکینگ پنهان شده بودند و مربوط به هر یک از دریافت کننده های کپی اسناد بودند و وزرا از وجود آن بی اطلاع بودند تا منبع افشا قابل شناسایی باشد.

۲- احتمال درج داده نامربوط به اثر پوششی در استگانوگرافی همیشه یک نگرانی برای ارتش بوده است. سیمونز توضیحات جالب خود را در کانال‌های مخفی ارائه می‌کند [۲۶]. در آن مسایل تاییدیه پیمان SALT_II را که ما بین آمریکا و اتحاد جماهیر شوروی است را مورد بحث فنی قرار می دهد.

پیمان SALT_II به هر دو کشور اجازه می دهد تا تعداد زیادی انبار موشکی داشته باشند، اما باید تعداد موشک ها محدود باشد. برای بررسی تعهدات این پیمان، هر یک از کشورها می توانند حسگرهایی را در انبارهای کشور دیگر نصب کنند. هر حسگر باید به کشور دیگر بگوید که آن انبار پر شده یا نه و نه چیز دیگری. نگرانی این کشورها این بود که کشورهای متبوع ممکن است حسگر را برای برقراری ارتباط و اطلاعات بیشتری مورد استفاده قرار دهند، برای مثال تعیین محل انبارها یا پنهان سازی اطلاعات در پیام های قانونی.

۳- مثالی از واترمارک آشکار (واترمارک قابل مشاهده) را می توان در وب سایت موزه آرمیتاژ دید. موزه تعداد زیادی از کپی های دیجیتال با کیفیت بالا از مجموعه های معروف را در وب سایت خود ارائه کرده است. برای شناسایی آرمیتاژ به عنوان صاحب اثر هر تصویر واترمارک شده یک پیغام در پایین هر صفحه وب وجود دارد که حاوی هشداری است که این تصاویر را نمی توان بازسازی کرد. باید دانست که واترمارک نامریی درج شده در هر تصویر مانع سرقت می شود.

۴- درج اطلاعات آشکار به انتقال اطلاعات کمکی شناخته شده به اثر اشاره دارد. در جایی که اطلاعات پنهان شده با سیگنال هایی که در آن درج شده اند غیر مرتبط است. در اواخر سال ۱۹۴۰ در رادیو درج کد زمانی در فرکانس مشخص کاری مرسوم بود (برای مثال در ۸۰Hz) و این کد زمانی در فاصله های زمانی متناوب در هر ۱۵ دقیقه درج می شد [۲۷]. کد غیرقابل شنیدن در زمان پخش و پنهان بود. اما واترمارک

نیست، زیرا پیام با محتوای پخش غیر مرتبط بود. ضمنا، آن مثالی برای استگانوگرافی هم نیست، زیرا وجود یک کد زمانی درج شده معین و شناخته شده هم نیست.

با تمایز بین داده های درج شده می توان ارتباط بین اثر پوششی و داده پنهان شده را فهمید. می‌توان برنامه های مختلف و الزامات روش های پنهان کردن داده ها را پیش بینی کرد. با این حال، تکنیک واقعی ممکن است خیلی مشابه باشد و یا در برخی موارد یکسان باشد. اگر چه این پروژه روی تکنیک های واترمارکینگ تمرکز دارد ولی بیشتر این تکنیک ها قابل اجرا در پنهان سازی اطلاعات در حوزه های دیگر هستند.

۲-۱- تاریخچه واترمارکینگ

هنر ساخت کاغذ هزار سال زودتر در چین بوجود آمد، اما کاغذ واترمارک شده در سال ۱۲۸۲ در ایتالیا ظاهر شد. مارک ها با افزودن سیم نازک به قالب های کاغذ درست می شدند. جایی که سیم وجود دارد، کاغذ آن کمی نازک تر و شفاف تر خواهد بود. هدف و معنای اولین واترمارکینگ مشخص نیست، اما ممکن است مانند توابع عملی برای شناسایی مدل هایی که صفحات کاغذ ساخته شده اند باشد، یا برای شناسایی علایم تجاری سازنده کاغذ استفاده شده است.

در قرن هجدهم، واترمارک روی کاغذ های ساخته شده در اروپا و آمریکا به کار گرفته شده بود و به عنوان علامت تجاری مورد استفاده قرار گرفته بود و نیز تاریخ تولید کاغذ و نشان دهنده اندازه صفحات اصلی است، در این زمان بود که استفاده از واترمارک به عنوان پول و سایر اسناد شروع شد. اصطلاح واترمارک به نظر می رسد در پایان قرن هجدهم ابداع شده باشد و ممکن است اصطلاح واترمارک از اصطلاح آلمانی مشتق شده باشد [۲۸] (گر چه ممکن است که کلمه آلمانی از کلمه انگلیسی گرفته شده باشد [۲۹]) که در واقع یک اسم بی مسمی است. در اینجا آب در ایجاد مارک هیچ نقشی و اهمیتی ندارد و احتمال داده می شود که علایمی شبیه اثرات آب روی کاغذ باشد.

در سال ۱۹۵۴ امیل همبروگ از شرکت موزاک برای واترمارک آثار موسیقی, ثبت اختراع کرد که یک فن آوری دیجیتال بود. یک کد شناسایی بطور متناوب بوسیله یک فیلتر خیلی باریک متمرکز در پهنای باند ۱kHz به