دانشگاه پیام نور

دانشکده: فنی و مهندسی

گروه علمی: کامپیوتر و فناوری اطلاعات

واترمارکینگ تصاویر رنگی مبتنی بر تئوری آشوب در حوزهٔ فرکانس

نگارش: قاسم قاری‌زاده مقدم

استاد راهنما: جناب آقای دکتر مهدی جوانمرد

پایان نامه

برای دریافت کارشناسی ارشد

در رشته مهندسی کامپیوتر گرایش نرم‌افزار

بهمن ماه ۱۳۹۱

با سپاس فراوان از استاد گرانقدر جناب آقای دکتر مهدی جوانمرد که با راهنمایی‌های خود اینجانب را در طی تولید این رساله همواره مورد حمایت قرار دادند.

چکیده:

واترمارکینگ به معنای پنهان کردن نقش هایی در یک تصویر است به نحوی که با چشم قابل تشخیص نباشد و فقط افراد مجاز قادر به استخراج آن باشند، لذا واترمارکینگ یکی از روش‌های حفاظت اطلاعات محسوب می‌گردد. روش‌های گوناگونی برای واترمارکینگ تصاویر دیجیتال به کار گرفته شده تا با سرعت بالاتر، روش‌های امن تری را برای حفاظت از اطلاعات و استخراج واترمارک بدست آورد.

در این تحقیق ابتدا توضیحات و کلیاتی در مورد واترمارکینگ، تاریخچه آن ، انواع و کاربردهای آن، رمزنگاری و نهان نگاری و مقایسه آن با واترمارکینگ و همچنین نظریه آشوب و انواع توابع آشوبی و فوق آشوبی بیان شده است، سپس انواع مدل‌های تصاویر رنگی و روش‌های واترمارکینگ دیجیتال بر روی تصاویر مورد بررسی قرار گرفته و در پایان روشی نو مبتنی بر تئوری فوق آشوب برای واترمارکینگ تصاویر رنگی در حوزه فرکانس ارائه گردیده است و با بررسی نتایج و نتیجه گیری کلی از تحقیق صورت گرفته، پیشنهادات برای کار در آینده مطرح شده است.

فهرست مطالب

عنوان **صفحه**

فصل دوم: نظریه آشوب و توابع آن

فصل سوم: انواع تصاویر رنگی و روشهای واترمارکینگ دیجیتال

فهرست شکل ها

فهرست جدول ها

عنوان

فصل اول : واترمارکینگ

۱-۱: واترمارکینگ چیست؟

کلمه واترمارک به معنی فارسی نقش آبی است که به اصطلاح نشان دهنده ایجاد نقشی بر روی آب به صورت بی رنگ و شفاف است که معمولاً با چشم به صورت معمول قابل رویت نیست. واترمارکینگ نیز به معنای پنهان کردن نقش هایی در یک تصویر است به نحوی که با چشم قابل تشخیص نباشد و فقط افراد مجاز قادر به استخراج آن باشند.

با رشد فناوری دیجیتال طی دهه‌های گذشته، ارسال و ذخیره اسناد الکترونیکی افزایش یافته است و نسخه برداری از داده‌ها با سرعت بالا و هزینه‌ای اندک امکان پذیر شده است. بر این اساس استفاده از روشی برای حفاظت از این اسناد نیز مطرح گردید، که در نتیجه منجر به استفاده از سیستم‌های رمزنگاری شد. در سیستم‌های رمزنگاری قدیمی تنها دارنده کلید رمز می‌تواند به محتوای سند رمز شده دسترسی پیدا کند، ولی نقطه ضعف این سیستم این است که، پس از رمزگشایی داده‌ها امکان استفاده غیر مجاز از آنها نیز وجود خواهد داشت. همچنین ماهیت وجود رمز بر روی یک سند خود باعث ترقیب سارقان اطلاعات به استفاده از روشهایی برای دریافت رمز، رمزشکنی و استفاده غیر مجاز از محتوای آن خواهد شد. با توجه به این موضوع قرار دادن داده، به صورت نامحسوس، برای جلوگیری از استفاده غیر مجاز و حملات بداندیشانه، کارایی بهتری خواهند داشت. بر این اساس به جز واترمارکینک فیزیکی که در اسناد فیزیکی به کار می‌روند، واترمارکینگ دیجیتالی در تصاویر، صوت و ویدئو مطرح گردیده است.

۱-۲: ضرورت و اهداف واترمارکینگ

تا چندی پیش ژورنال‌های معتبر بین المللی، مقالات، متون علمی، داده‌های محرمانه ومکاتبات اداری، صرفاً به صورت فیزیکی و کاغذی وجود داشت و هریک در اختیار طیف محدودی از کاربران قرار می‌گرفت و به همان نسبت سوء استفاده از آنها با محدودیت و مشکلات بیشتری همراه بود، اما امروزه با پیشرفت تکنولوژی و ابداع کانال‌های ارتباطی گوناگون نظیر اینترنت و ارتباطات ماهواره‌ای و مخابراتی، انواع داده‌ها به آسانی و به نحو

بسیار گسترده در جهان مورد استفاده قرار می‌گیرند. این پیشرفت تکنولوژی اگرچه باعث سهولت بسیاری از کارها گشته، اما مانند دیگر مظاهر تکنولوژی، مشکلاتی را با خود به همراه داشته است. یکی از این مشکلات، توانایی دستکاری، کپی برداری و توزیع غیرقانونی اسناد دیجیتالی، توسط کاربرانی است که از این اسناد استفاده میکنند، و چنانچه مسائل امنیتی محصولات دیجیتالی از جمله اسناد چند رسانه‌ای دیجیتالی حل نشود، مالکان این محصولات انگیزه‌ی خود را برای وارد کردن این محصولات در دنیای تجارت الکترونیک از دست خواهند داد.

یکی از اهداف واترمارک جلوگیری از جعل اسناد و سوء استفاده از آنها است. به عبارتی وجود واترمارک در یک سند، اصل یا جعل بودن آن را برای ما مشخص و اثبات می‌کند. به طور خلاصه می‌توان گفت رعایت قانون حق کپی[1] اصلی ترین هدف واترمارکینگ می‌باشد. البته اهدافی دیگر نیز برای واترمارک قابل تعریف است، مانند شناسایی مالک سند، تعیین هویت محتوای مالک، اثر انگشت، شناسایی خریدار محتوا و ...

۱-۳: واترمارک فیزیکی

اگر بخواهیم واترمارک فیزیکی را به چیزی تشبیه کنیم، می‌توان گفت مانند شکل شناوری است که روی یک تکه کاغذ نازک در زیر نور دیده می‌شود. واترمارک نقشی است که علاوه بر طرح زمینه، به طور نامحسوس بر روی اسناد کاغذی چاپ می‌شود، و با کمک رنگ روشن تر و یا از راه در معرض نور قرار گرفتن قابل رؤیت می‌باشد. به عنوان یکی از قدیمی‌ترین نمونه‌های کاربرد واترمارگینگ می‌توان به چاپ اسکانس اشاره کرد. واترمارک باید به صورت شفاف و غیر قابل پاک شدن باشد. واترمارک باید به صورتی باشد که به هیچ عنوان نتوان از آن کپی برداری کرد. نسخه کپی شده نمی‌تواند داری واترمارک تصویر اصلی باشد. در این روش، سندیت و اصالت سند حفظ شده و با استفاده از هیچ دستگاهی اعم از کپی، اسکنر، و یا چاپگر و یا هیچ روشی دیگر امکان جعل وجود ندارد.[۱]

1. Copy Right

۱-٤: واترمارک دیجیتال

در قرن فعلی که به قرن ارتباطات موسوم است، به دلیل گسترش روز افزون ارتباطات جهانی و ابداع کانال‌های ارتباطی گوناگون نظیر شبکه اینترنت وارتباطات ماهواره‌ای و مخابراتی، اطلاعات به راحتی در اختیار طیف گسترده‌ای از مردم در سرتاسر دنیا قرار می‌گیرد. با ورود فن‌آوری‌های دیجیتال به نظام‌های اداری سرتاسر دنیا و به زندگی عموم مردم، اسناد و اطلاعات به سرعت پخش شده و در معرض دسترس افراد مختلف خواهد بود. همچنین با پیشرفت روزافزون حاصل شده نظام‌های اداری فاقد کاغذ گسترش یافته است. از این رو بسیار از اسناد به صورت دیجیتالی تهیه شده و عرضه می‌گردد. این اسناد می‌توانند در قالب های گوناگون مانند: متن، کتابهای الکترونیکی، تصاویر ساکن، تصاویر متحرک، فیلم، پایگاه های داده، نرم افزارها، بازی‌های کامپیوتری یا انواع دیگر باشند. ماهیت دیجیتالی داده ایجاب می‌کند که ایجاد، تغییر، به روزرسانی، اصلاحات، اشتراک‌گذاری، ذخیره سازی و انتشار آنها آسان‌تر و سریع‌تر از قبل باشد. از این رو دسترسی و تبادل آزاد اطلاعات، می‌تواند به همان نسبت امکان سوء استفاده از آن را بالاتر ببرد. بنابراین اهمیت و ضرورت پنهان‌سازی محتوای اطلاعات در اینجا روشن می‌شود.[۲]

دانشمندان در سطوح پیشرفته‌تر دانش کامپیوتر بر آن هستند تا در این زمینه، چاره‌اندیشی کنند. از جمله شاخه‌های مهم دانش کامپیوتر در این زمینه، شاخه‌ی هوش مصنوعی و زیر مجموعه‌ی پردازش تصویر می‌باشد. در این شاخه حفاظت از داده‌ها در مقابل کپی‌برداری 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 واترمارکینگ دیجیتال می‌باشد. همانطور که اشاره کردیم، واترمارکینگ به معنای پنهان کردن داده یا نقشی در سند اصلی است به نحوی که با چشم قابل تشخیص نباشد و فقط افراد مجاز قادر به استخراج آن باشند.[۳]

۱-۵: تعاریف مشابه و تفاوت‌ها

واترمارکینگ دیجیتال رابطه بسیار نزدیکی با رمزنگاری و پنهان‌نگاری داده دارد، که با توجه به کاربردهایی که دارند در موارد گوناگون مورد استفاده قرار می‌گیرند. در ادامه به توضیح مختصری در این زمینه می‌پردازیم:

۱-۵-۱: رمزنگاری

به رمز کردن محتوای یک پیام، رمز نگاری یا در اصطلاح کریپتوگرافی[1] گفته می‌شود و عبارت است از بهم ریختگی اطلاعات به طوری که برای کسی قابل فهم نباشد. فن‌آوری رمزنگاری، امکان مشاهده، مطالعه و تفسیر پیام‌های ارسالی توسط افراد غیرمجاز را سلب می‌نماید. در این رابطه از الگوریتم‌های پیشرفته‌ی ریاضی به منظور رمز نمودن پیام‌ها و ضمائم مربوطه، استفاده می‌شود. کلمه کریپتوگرافی از ریشه یونانی کریپتو به معنای رمز گرفته شده است. به فرآیند رمز نگاری اصطلاحا فرآیند Encryption و به فرآیند رمزگشایی، Decryption گفته می‌شود. برای اینکه رمزگشایی امکان پذیر باشد گردد، فرستنده پیام حتما باید کلید رمزگشایی را برای گیرنده ارسال کند. این کلید نبایستی در اختیار موجودیت دیگری غیر از گیرنده قرار گیرد. رمزنگاری به طور ذاتی انگیزه خرابکاری را برای یافتن الگوریتم‌ها و راه‌های رمز شکنی بالا می‌برد.

۱-۵-۲:پنهان نگاری

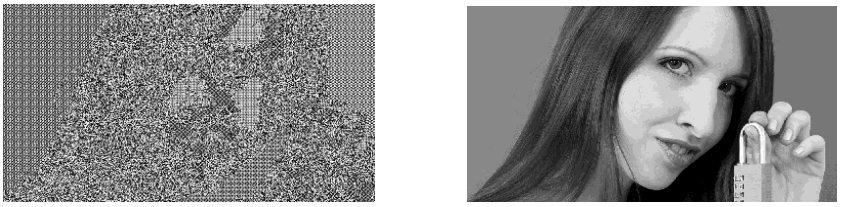
پنهان‌نگاری یا استگانوگرافی[2] هنر برقراری ارتباطات پنهانی است و هدف آن پنهان کردن ارتباطات به وسیله قرار دادن پیام در یک رسانه پوششی است به گونه‌ای که کمترین تغییر قابل کشف را در آن ایجاد نماید و نتوان موجودیت پیام پنهان در رسانه را حتی به صورت احتمالی آشکار ساخت. این کلمه از ریشه‌ی یونانی استگانو

1. Cryptography
2. Steganography

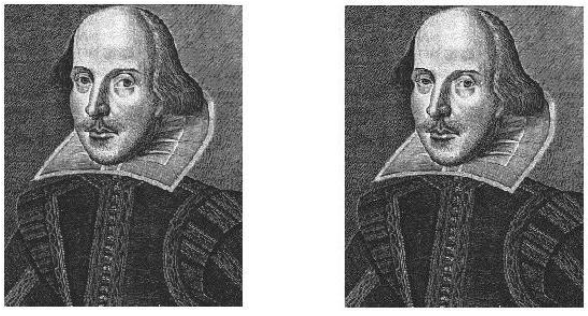
به معنی پنهان گرفته شده است. در استگانوگرافی تلاش می‌شود وجود پیام رمز قابل تشخیص نباشد. در نتیجه با این کار، امکان نفوذ نفوذگران کاهش می‌یابد.[٤و٥]

۱-۵-۳:تفاوت رمز نگاری و پنهان نگاری

یک تفاوت مهم رمزنگاری و پنهان‌نگاری در آن است که پنهان نگاری حتما به میزبانی یک محیط ثانویه تک رسانه یا چند رسانه انجام پذیر است. وجه برتری ذاتی پنهان نگاری در آن است که از آنجا که وجود پیام رمز، از منظر عموم مخفی می‌گردد، به همان نسبت تلاشها و انگیزه‌های رمز شکنی فروکش می‌کند. نکته مهم آن است که نباید پنهان نگاری را به عنوان جایگزین برای رمزنگاری تصور کرد. بلکه پنهان نگاری مکمل مناسبی برای رمزنگاری به شمار می‌رود. برای بالا بردن ضریب اطمینان، می‌توان از رمزنگاری و پنهان نگاری به‌صورت ترکیبی و هم‌زمان استفاده کرد. شکل ۱-۱ یک تصویر با فرآیند رمزنگاری و شکل ۱-۲ تصویری با فرآیند پنهان نگاری را نمایش میدهد.



شکل ۱-۱: فرآیند رمزنگاری

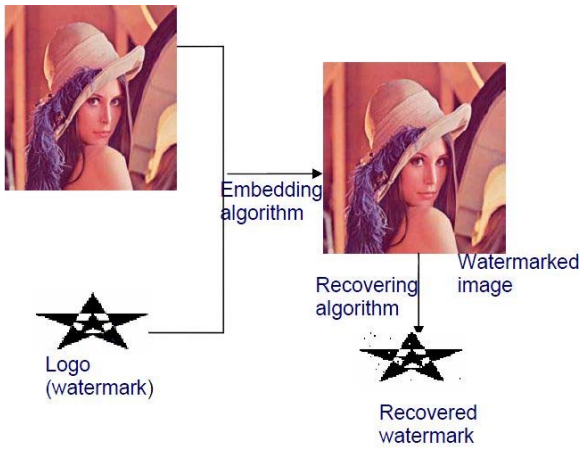


شکل ۱-۲: فرآیند پنهان نگاری

همان طور که در شکل۱-۲ مشاهده می شود از لحاظ ظاهری این دو شکل با هم تفاوتی ندارند. اما در تصویرسمت راست متن هایی مخفی شده است. [۵]

۱-۵-٤: واترمارکینگ

واترمارکینگ دیجیتال شاخه‌ای از فرآیند پنهان‌نگاری محسوب می‌شود که برای اولین بار در سال ۱۹۹٦ معرفی شد. واترمارک در صوت، ویدئو و تصویر کاربرد دارد که در این تحقیق، واترمارک‌های مبتنی بر تصویر مورد نظر هستند. واترمارکینگ به عنوان یک روش در حفاظت از حق کپی و جلوگیری از تکثیر (کپی‌برداری) غیر قانونی اطلاعات، روش مناسبی محسوب می‌شود. در شکل ۱-۳ یک فرآیند واترمارکینگ مشاهده می شود.



شکل ۱-۳: فرآیند واترمارکینگ

۱-٦:تفاوت‌های پنهان‌نگاری و واترمارکینگ

در پنهان‌نگاری به طور خاص مخفی کردن وجود داده‌ها و ارسال اطلاعات تحت پوشش یک داده‌ی دیگر مورد نظر می‌باشد و هدف اصلی، داده‌ای است که پنهان شده است و اطلاعات پوششی دارای اهمیت نمی‌باشد.

برخلاف نهان‌نگاری، در واترمارکینگ گنجاندن داده به دلیل اهمیت بالای سیگنال میزبان می‌باشد، که با اهداف متفاوتی از پنهان نگاری نظیر حفظ حق نشر، درستی و تمامیت داده، ره گیری مسیر انتشار و ... انجام می‌شود. در واقع تفاوت اصلی این دو روش در سیگنال دارای ارزش می باشد که در نخستین مورد، پیام گنجانده شده دارای ارزش است و در دیگری خود میزبان است که دارای ارزش می‌باشد.

۱-۷:تاریخچه واترمارکینگ

با نگاهی تاریخی بر ماجرای واترمارکینگ و پنهان نگاری در می‌یابیم که پنهان‌سازی اطلاعات، قدمتی دیرینه دارد. البته روش‌های پنهان نگاری در قدیم، بسیار ابتدایی و متفاوت و گاه عجیب بوده‌اند. در این قسمت مروری بر وقایع بر جسته در این زمینه خواهیم داشت.

تاریخچه رمز کردن اطلاعات برای نخستین بار به حوالی سال ۱۹۰۰ پیش از میلاد بر می‌گردد، که در آن زمان مصریان باستان از نوعی الفبای هیروگلیف نامتعارف در کتیبه‌های 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 می کرد. طبق روایات هرودوت – مورخ یونانی – فرمانروای یونانی به نام هیستیائوس برای رساندن فرمان شورش علیه ایرانیان، پیغام محرمانه خود را بر سر تراشیده یکی از بردگان معتمد خود خالکوبی کرد. هرودوت همچنین نقل می‌کند که دمراتوس پیام هشدار حمله دشمن را بر قرصهایی چوبی می نوشت و به مخاطب می‌رساند.

سیر تکاملی رمز کردن اطلاعات همچنان ادامه یافت. ردپای رمز کردن داده در اروپای قرون وسطی نیز دیده می‌شود. استگانوگرافی در قرن ۱۵ و ١٦ توسعه یافت. به دلیل اینکه اکثر نویسندگان کتاب‌ها از ایجاد تفرقه بین احزاب و فرقه‌های می‌ترسیدند نام خود را در میان کتاب مخفی می‌کردند. رساله‌هایی نیز در این زمینه نوشته شده بودکه از میان آنها می‌توان به کتاب بی شاپ ژان ویکینز[1] اشاره کرد که روش‌هایی را از کدکردن پیغام‌ها در موزیک تا جوهرهای نامرئی پیشنهاد داد. همچنین او اولین طرح‌ها را در رمز گشایی با استفاده از تناوب

1. Bishop Gohn Wikins