
بسم الله الرحمن الرحيم

دانشگاه اصفهان
دانشکده فنی و مهندسی
گروه مهندسی کامپیوتر

پایان‌نامه دکتری رشته کامپیوتر

واترمارکینگ تصویر در حوزه تبدیل پارامتریک اسلنت– هادامارد

استاد راهنما:
دکتر احمد رضا نقش نیلچی

پژوهشگر:
علی محمد لطیف

خرداد ۱۳۹۰

دانشگاه اصفهان
دانشکده فنی و مهندسی
گروه کامپیوتر

پایان‌نامه دکتری رشته کامپیوتر

آقای علی محمد لطیف

تحت عنوان

واترمارکینگ تصویر در حوزه‌ی تبدیل پارامتریک اسلنت– هادامارد

در تاریخ ۱۳۹۰/۳/۳۱ توسط هیأت داوران زیر بررسی و با درجه‌ی بسیار خوب به تصویب نهایی رسید.

۱- استاد راهنمای پایان‌نامه : دکتر احمدرضا نقش‌نیلچی با مرتبه‌ی علمی دانشیار امضا

۲- استاد داور داخل گروه : دکتر ناصر موحدی‌نیا با مرتبه‌ی علمی دانشیار امضا

۳- استاد داور داخل گروه : دکتر هومان نیک‌مهر با مرتبه‌ی علمی استادیار امضا

۴ - استاد داور خارج گروه : دکتر شادرخ سماوی با مرتبه‌ی علمی استاد امضا

۵ - استاد داور خارج گروه : دکتر منصور جم‌زاد با مرتبه‌ی علمی دانشیار امضا

امضای مدیر گروه

سپاسگزاری:

هرکه بر لوح جهان نقشی نیفزاید ز خویش

بیگمان چون نقش پا محو است در موج فنا (فریدون مشیری)

خداوند متعال را سپاس می گویم که در پرتو عنایات خاصه اش توفیق عطا فرمود تا در راهی که همواره ممدوح اولیای الهی بوده است، گام بردارم. درود بی پایان خود را به اندیشمندان و محققانی که مسیر علم و تحقیق را با راهنمایی ها و هدایت های خود همواره پر رونق نگاه داشته اند، تقدیم می دارم.

در طول دوران تحصیل از محضر اساتیدی بهره جسته ام که بدون راهنمایی های آن ها این مهم به انجام نمی رسید. لذا لازم می دانم بدین وسیله از زحمات و راهنمایی های استادگران قدر جناب آقای دکتر احمدرضا نقش نیلچی که همواره با بزرگواری تمام و صبر و حوصله بی نظیرشان در کلیه مراحل تحقیق و تدوین این پایان نامه، اینجانب را از راهنمایی های خردمندانه ی خویش بهره مند فرمودند، کمال تشکر و قدردانی را بنمایم.

در پایان از تمام سرورانی چون آقای دکتر امیر حسن منجمی، آقای دکتر ناصر موحدی نیا، آقای دکتر قاسم آقایی که با ایشان درس گذرانده ام قدردانی و تشکر می نمایم.

تقدیم به:

پدرم، رادمردی که دست کریمانه‌اش همیشه یاورم بوده و آتش هستی‌اش گرمابخش وجودم.

مادرم، که خاک پایش مرا تاجی است هدیه فرستاده از بهشت برین، هم او که دل نگرانی‌اش را می‌ستایم و ذره ذره وجودم مدیون اوست.

همسر و فرزندم محمد متین، که وجودشان دلیل دل گرمی من و همراهی‌شان نردبان موفقیت من بوده است.

چکیده:

رشد و توسعه‌ی محصولات دیجیتالی با مشکلاتی از قبیل کپی برداری غیرمجاز، توزیع غیرقانونی و جعل همراه بوده است. برای حل این مشکل، راه حل‌های متفاوتی از جمله رمزنگاری و واترمارکینگ پیشنهاد شده است که در سال-های اخیر، سیستم‌های واترمارکینگ مورد توجه فراوان قرار گرفته‌اند. در سیستم‌های واترمارکینگ دیجیتالی با درج یک علامت به نام واترمارک در محصول دیجیتالی از آن محصول محافظت می‌شود. در هر کاربرد، ویژگی‌های مخصوص به آن کاربرد مورد نیاز می‌باشد، اما داشتن شفافیت و مقاومت و ظرفیت در کاربردها مورد نیاز می‌باشد

شفافیت و مقاومت و ظرفیت در اکثر سیستم‌های واترمارکینگ در تضاد با یکدیگر می‌باشند و دارا بودن هم‌زمان این سه ویژگی از نقاط برجسته‌ی تکنیک‌های واترمارکینگ می‌باشد. در تحقیقات اخیر تلاش‌های زیادی برای تامین توام این ویژگی‌ها، با تعیین محل درج واترمارک و تعیین قوت واترمارک، صورت گرفته است. نکته‌ی قابل توجه این است که در بعضی از این کاربردها، تامین هم‌زمان این ویژگی‌ها با داشتن دو درجه‌ی آزادی، یعنی محل درج واترمارک و قوت واترمارک، امکان‌پذیر نیست.

در این پایان‌نامه از یک روش حوزه‌ی فرکانس مبتنی بر تبدیل پارامتریک اسلنت- هادامارد برای واترمارکینگ تصاویر دیجیتالی استفاده می‌شود. وجه تمایز تبدیل پارامتریک اسلنت- هادامارد نسبت به دیگر تبدیل‌ها، وجود پارامترهای این تبدیل می‌باشد که با تغییر مناسب این پارامترها، می‌توان ویژگی‌های سیستم واترمارکینگ را به طور هم-زمان بهبود بخشید. در این تحقیق، از الگوریتم ژنتیک برای یافتن پارامترهای تبدیل جهت تامین هم‌زمان ویژگی‌های شفافیت و مقاومت و ظرفیت استفاده می‌شود. لازم به ذکر است در کاربردهای زمان حقیقی از این سیستم پیشنهادی، به دلیل زمان‌بر بودن الگوریتم ژنتیک استفاده نمی‌شود.

درج واترمارک در حوزه‌ی فرکانس بدون وابستگی به محتوای تصویر میزبان باعث کاهش شفافیت سیستم واترمارکینگ می‌شود. لذا در این تحقیق یک مدل جدید، برای درج واترمارک به گونه‌ای که وابسته به محتوای تصویر میزبان باشد، ارائه می‌شود. علاوه بر این، چون در اکثر سیستم‌های واترمارکینگ کاربر نهایی انسان می‌باشد، استفاده از ویژگی‌های سیستم بینایی انسان در طراحی سیستم واترمارکینگ، باعث افزایش کارایی سیستم واترمارکینگ می‌شود. لذا در سیستم واترمارکینگ پیشنهادی پس از درج واترمارک، به عنوان یک عمل پس‌پردازش، با استفاده از یک سیستم فازی مبتنی بر ویژگی‌های سیستم بینایی انسان، شفافیت سیستم واترمارکینگ بهبود داده می‌شود. نتایج حاصل از آزمایش‌ها نشان می‌دهد در اثر این عمل پس‌پردازش در کاربردهای تایید، کارآیی آشکارساز واترمارک اندکی کاهش می‌یابد که برای جبران کاهش کارآیی می‌توان قوت واترمارک را بدون کاهش شفافیت افزایش داد. همچنین نتایج آزمایش‌ها در کاربرد انتقال کد نشان می‌دهد این عمل پس‌پردازش تعداد بیت‌های صحیح استخراج شده را کاهش می‌دهد ولی نتایج نشان می‌دهد واترمارک استخراجی از نظر بصری قابل تشخیص می‌باشد.

در بخش ارزیابی، جای وجود یک سیستم رتبه‌بندی تکنیک‌های واترمارکینگ خالی است. بنابراین در این پایان-نامه، در بین روش‌های ارزیابی سیستم‌ها، از سیستم ارزیابی مبتنی بر آنتروپی جهت رتبه‌بندی تبدیل‌های مختلف در واترمارکینگ تصویر استفاده می‌شود که علاوه بر ارزیابی و مقایسه تکنیک‌های مختلف واترمارکینگ در حوزه تبدیل، می‌تواند در بهبود روش‌های موجود مورد استفاده قرار گیرد. نتایج حاصل از این رتبه‌بندی نشان می‌دهد تبدیل پارامتریک اسلنت- هادامارد با استفاده از پارامترهای محاسبه شده توسط الگوریتم ژنتیک از جایگاه ممتازی برخوردار است.

کلمات کلیدی :

سیستم‌های واترمارکینگ دیجیتالی، شفافیت، مقاومت، الگوریتم ژنتیک، سیستم فازی، ارزیابی

فهرست مطالب

عنوان **صفحه**

عنوان **صفحه**

فهرست شکل‌ها

عنوان **صفحه**

عنوان **صفحه**

عنوان **صفحه**

فهرست جدول‌ها

فصل اول

مقدمه و مبانی

پیشرفت سریع علوم کامپیوتر، شبکه‌های کامپیوتری، ارتباطات و گسترش روزافزون کاربرد سیستم‌های چندرسانه‌ای دیجیتالی[1] باعث تغییرات فراوانی در زندگی بشر شده است. توسعه‌ی ابزارهای نرم‌افزاری و سخت‌افزاری فراوان، علاوه بر داشتن مزایا و استفاده‌های فراوان، مشکلاتی را برای محصول‌های دیجیتالی ایجاد کرده است.

امنیّت[2] و استفاده‌ی قانونی[3] از محصول‌های دیجیتالی، امری مهم و مورد توجّه اکثر هنرمندان و صاحبان آثار دیجیتالی است. آن‌ها علاقه‌مند هستند آثار هنری‌شان در مقابل تکثیرهای غیرمجاز محفوظ بماند و کلیه‌ی حقوق نشر و تکثیر متعلق به صاحبان آثار باقی بماند. برای حل این مشکل، دو مقوله‌ی «رمزنگاری»[4] و «واترمارکینگ»[5] پیشنهاد شده است.

رمزنگاری، یک روش عمومی حفاظت داده است که از طریق روش‌های ریاضی برگشت‌پذیر انجام می‌شود. در سیستم‌های حفاظتی مبتنی بر رمزنگاری، ابتدا داده با استفاده از الگوریتم‌های رمزنگاری، رمز می‌شود

---

[1] Digital Multimedia
[2] Security
[3] Legal
[4] Cryptography
[5] Watermarking

و سپس داده‌ی رمز شده، برای گیرنده ارسال می‌شود. در گیرنده، داده‌ی دریافت شده با استفاده از کلیدهای صحیح رمزگشایی می‌شود و در اختیار کاربر قرار داده می‌شود. بدیهی است برای افزایش امنیّت سیستم رمزنگاری، عملیات ریاضی با استفاده از کلیدهای[1] خاص و منحصر به فرد انجام می‌شود.

نکته‌ی مهم و قابل توجّه حفاظت داده با استفاده از سیستم‌های رمزنگاری، عدم کارایی کامل رمزنگاری در حفاظت داده است. در سیستم‌های رمزنگاری بعد از رمزگشایی داده، دیگر هیچ‌گونه حفاظتی بر روی داده صورت نمی‌گیرد و در این مرحله می‌توان از روی داده‌ی رمزگشایی شده، کپی غیر مجاز تولید کرد. علاوه بر این، می‌توان به راحتی داده‌ی رمزگشایی شده را جعل کرد.

یکی دیگر از مشکل‌های سیستم‌های رمزنگاری در تصویر این است که در بعضی از الگوریتم‌های رمزنگاری، ترتیب داده‌ی تصویر تغییر می‌کند که این باعث می‌شود داده‌ی رمز شده‌ی تصویر، برای کاربر دیگر به صورت تصویر ظاهر نگردد. با توجه به مشکلات معمولا از سیستم‌های رمزنگاری برای حفاظت داده به خصوص داده‌ی تصویر، کم‌تر استفاده می‌شوند.

برای داشتن یک ابزار قوی‌تر به‌گونه‌ای که همواره همراه داده باشد و بتواند از داده محافظت کند، واترمارکینگ پیشنهاد می‌شود. در یک سیستم واترمارکینگ با افزودن یک علامت انحصاری مربوط به مالک داده، به صورت مریی[2] و یا نامریی[3]، می‌توان از تغییر و جعل آن جلوگیری کرد. در دهه‌های اخیر به دلیل اهمیّت حفاظت داده‌ی دیجیتالی، در سطح جهانی تحقیق‌های فراوانی در زمینه‌ی مخفی‌سازی داده[4] صورت گرفته است. واترمارکینگ به عنوان یکی از زیرگروه‌های مخفی‌سازی داده در تصویرهای ساکن[5]، تصویرهای متحرک، و صوت[6] به صورت نظری و کاربردی گسترش قابل توجّهی داشته است.

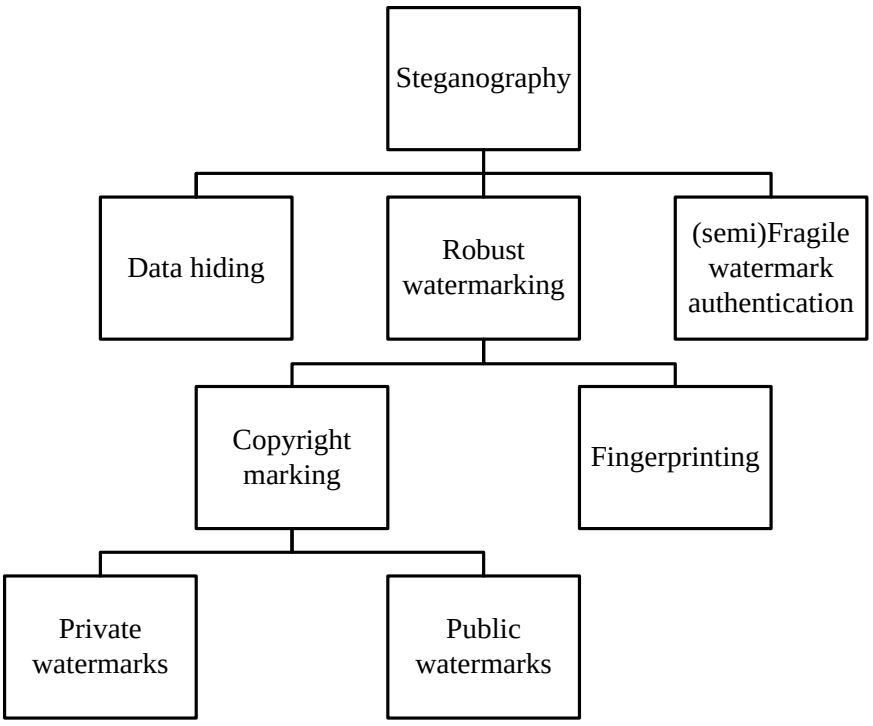
در سال‌های اخیر طبقه‌بندی‌های مختلفی برای مخفی‌سازی داده صورت گرفته است. طبقه‌بندی‌های موجود، با توجّه به اهداف وکاربردهای مخفی‌سازی داده صورت گرفته است. در این قسمت دو نوع طبقه‌بندی مختلف معرفی می‌شود.

---

[1] Keys
[2] Visible
[3] Invisible
[4] Data Hiding
[5] Still Image
[6] Audio

طبقه‌بندی اوّل توسط Vleeschouwer و همکاران وی، با توجّه به کاربرد مخفی‌سازی داده در سال ۲۰۰۲ میلادی پیشنهاد شد. این طبقه‌بندی در شکل ۱-۱ نمایش داده می‌شود[۱]. در این طبقه‌بندی Vleeschouwer واترمارکینگ را زیرگروه مخفی‌نگاری[۱] قرار داد.

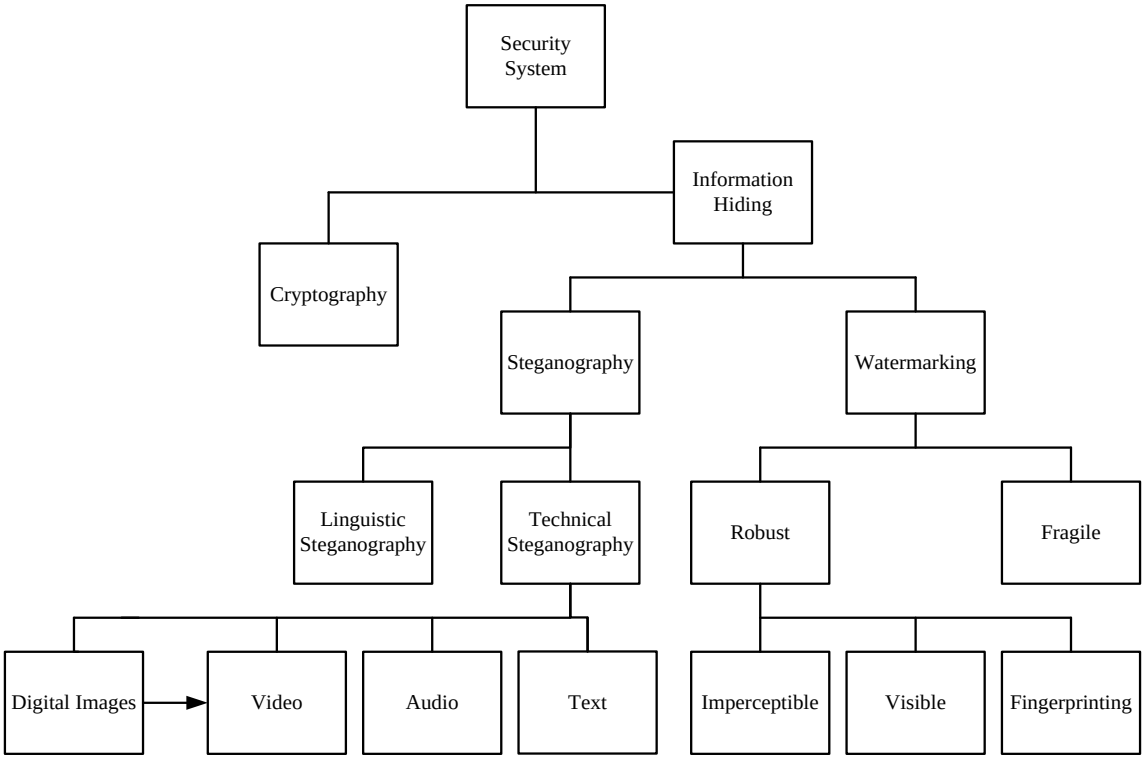
مخفی‌نگاری از دو کلمه یونانی Steganos به معنی پوشیده[۲] و Graphia به معنی نوشتن[۳] تشکیل شده است. یکی از ابتدایی‌ترین استفاده‌های مخفی‌نگاری، توسط Herodotus مورخ یونانی، حدود ۴۰۰ سال قبل از میلاد به ثبت رسیده است. هنگامی که حاکم یونان Histiaeus به دست داریوش زندانی شده بود، او باید پیامی را به صورت مخفیانه به برادر خوانده‌اش در Miletus می‌فرستاد. به همین منظور، وی موی سر غلامش را تراشید و پیام را روی سر او خال‌کوبی[۴] کرد. بعد از مدتی، موی سر غلام رشد کرد و پیام در بین موهای غلام مخفی شد. سپس Histiaeus غلام را به سوی برادر خوانده‌اش فرستاد. در مقصد برادر خوانده‌ی حاکم یونان، پس از تراشیدن موی سر غلام، پیام ارسالی را مشاهده کرد[۲]



شکل ۱-۱ : طبقه‌بندی مخفی‌سازی داده توسط Vleeschouwer[۱]

[1] Steganography
[2] Covered
[3] Writing
[4] tattooed

طبقه‌بندی دوّم بر اساس امنیت سیستم توسط Cheddad و همکاران او در سال ۲۰۰۹ میلادی مطابق شکل ۱-۲ ارائه شد[۳]. همان طور که ملاحظه می‌شود این طبقه‌بندی با جزئیات بیش‌تر و کامل‌تری، نسبت به طبقه‌بندی قبلی است. موضوع قابل توجّه در این طبقه‌بندی‌های ارائه شده این است که واترمارکینگ با مخفی‌نگاری و مخفی‌سازی داده ارتباط نزدیکی دارد.



شکل ۱-۲ : طبقه‌بندی مخفی‌سازی داده توسط Cheddad[۳]

واترمارکینگ، مخفی‌نگاری و مخفی‌سازی داده دارای هم‌پوشانی بوده و مفاهیم زیادی بین آن‌ها مشترک می‌باشد. لازم به ذکر است این سه موضوع دارای تفاوت‌هایی نیز می‌باشند. بیش‌ترین تفاوت مخفی‌نگاری و واترمارکینگ در اهداف آن‌ها است. در واترمارکینگ، سیگنال میزبان[1] از اهمیّت ویژه‌ای برخوردار است و برای حفظ اصالت و جلوگیری از جعل و تکثیر غیرمجاز آن با سیگنال دیگری به نام واترمارک[2] نشانه‌گذاری می‌شود. در واترمارکینگ، سیگنال واترمارک یک سیگنال معمولی است و از بین رفتن آن زیاد مهم نیست و فقط سالم ماندن سیگنال میزبان اهمیّت دارد. اما در مخفی‌نگاری، پیامی که در سیگنال میزبان مخفی می‌شود، مهم است.

[1] Host
[2] Watermark