

بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيمِ



دانشگاه اصفهان
دانشکده فنی و مهندسی
گروه مهندسی کامپیوتر

پایان نامه دکتری رشته کامپیوتر

واترمارکینگ تصویر در حوزه تبدیل پارامتریک اسلنت – هادامارد

استاد راهنما:
دکتر احمد رضا نقش نیلچی

پژوهشگر:
علی محمد لطیف

خرداد ۱۳۹۰

کلیه حقوق مادی مترتب بر نتایج
مطالعات، ابتکارات و نوآوری‌های
ناشی از تحقیق موضوع این پایان‌نامه
متعلق به دانشگاه اصفهان است.



دانشگاه اصفهان
دانشکده فنی و مهندسی
گروه کامپیوتر

پایان نامه 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 پایان نامه : 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

پاسکزاری:

هر که بر لوح جهان نقشی نیفزاید ز خویش

پیکان چون نقش پامحو است در موج فنا فزیدون شیری

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. در دینی پایان خود را به اندیشمندان و محققانی که مسیر علم و تحقیق را با راهبانی ها و هدایت های خود همواره پر رونق نگاه داشته اند، تقدیم می دارم.

در طول دوران تحصیل از محضرات ایتدی بهره جسته ام که بدون راهبانی های آن هاین مهم به انجام نمی رسید. لذا لازم می دانم بدین وسیله از زحمات و راهبانی های استاد گران قدر جناب آقای دکتر احمد رضا 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 راهبانی های خردمندانه ی خویش بهره مند فرمودند، کمال تشکر و قدردانی را بنمایم.

در پایان از تمام سرورانی چون آقای دکتر امیر حسن منجی، 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 دست‌گیرمانه‌اش همیشه یاورم بوده و آتش‌هستی‌اش گریبان‌بخش وجودم.
مادرم، که خاک‌پایش مراتاجی است، هدیه فرستاده از بهشت برین، هم‌او که دل‌نگران‌اش را می‌ستایم و ذره
ذره وجودم می‌یون اوست.

همسر و فرزندم محمد متین، که وجودشان دلیل دل‌گرمی من و همراهی‌شان زردبان 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، راه‌حل‌های متفاوتی از جمله رمزنگاری و واترمارکینگ پیشنهاد شده است که در سال‌های 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، کارایی آشکارساز واترمارک اندکی کاهش می‌یابد که برای جبران کاهش کارایی 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 پایان‌نامه، 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

صفحه	عنوان
۱	فصل اول : مقدمه و مبانی.....
۵	۱-۱ تاریخچه واترمارکینگ.....
۶	۲-۱ سیستم متداول واترمارکینگ دیجیتالی.....
۷	۳-۱ کاربردهای سیستم واترمارکینگ.....
۸	۱-۳-۱ محافظت از حق تالیف.....
۹	۲-۳-۱ تعیین هویت مالکیت.....
۹	۳-۳-۱ تصدیق داده.....
۹	۴-۳-۱ محافظت در مقابل جعل داده.....
۱۰	۵-۳-۱ محافظت از تکثیر غیرمجاز.....
۱۰	۶-۳-۱ آرشیوهای چندرسانه‌ای.....
۱۱	۷-۳-۱ پخش تلویزیون دیجیتالی.....
۱۱	۸-۳-۱ ردیابی.....
۱۲	۹-۳-۱ نظارت بر پخش.....
۱۲	۱۰-۳-۱ خودکارسازی فرآیندها.....
۱۲	۱۱-۳-۱ کنترل دستگاه.....
۱۳	۱۲-۳-۱ ارزیابی سیستم‌های انتقال داده.....
۱۳	۱۳-۳-۱ کاربرد پزشکی.....
۱۳	۴-۱ ویژگی‌های سیستم‌های واترمارکینگ.....
۱۴	۱-۴-۱ برگشت پذیر بودن.....
۱۴	۲-۴-۱ شفافیت.....
۱۵	۳-۴-۱ مقاومت.....
۱۵	۴-۴-۱ امنیت.....
۱۶	۵-۴-۱ ظرفیت.....
۱۶	۶-۴-۱ کم هزینه بودن.....
۱۷	۷-۴-۱ نوع سیگنال میزبان.....
۱۷	۸-۴-۱ نوع اطلاعات قابل درج.....

۱۷ ۹-۴-۱ نحوه‌ی استخراج واترمارک
۱۸ ۵-۱ سازگاری ویژگی‌های سیستم واترمارکینگ
۱۹ ۶-۱ حوزه‌ی درج واترمارک
۱۹ ۷-۱ ارزیابی سیستم‌های واترمارکینگ
صفحه	عنوان
۲۱ ۸-۱ ساختار پایان‌نامه
۲۳ ۹-۱ خلاصه
۲۴ فصل دوم: واترمارکینگ تصاویر دیجیتالی
۲۶ ۱-۲ فناوری‌های واترمارکینگ تصاویر دیجیتالی
۲۶ ۱-۱-۲ روش‌های حوزه‌ی مکان
۳۰ ۲-۱-۲ روش‌های حوزه‌ی فرکانس
۳۳ ۲-۲ تبدیل‌های تصویری
۳۳ ۱-۲-۲ تبدیل‌های متعامد ویکانی
۳۵ ۳-۲ واترمارکینگ در حوزه‌ی فرکانس
۳۵ ۱-۳-۲ واترمارکینگ در حوزه‌ی KLT
۳۵ ۲-۳-۲ واترمارکینگ در حوزه‌ی DFT
۳۷ ۳-۳-۲ واترمارکینگ در حوزه‌ی DCT
۳۹ ۴-۳-۲ واترمارکینگ در حوزه‌ی DWT
۴۰ ۵-۳-۲ واترمارکینگ در حوزه‌ی تبدیل هادامارد
۴۱ ۶-۳-۲ واترمارکینگ در حوزه‌ی تبدیل والش
۴۲ ۷-۳-۲ واترمارکینگ در حوزه‌ی تبدیل هار
۴۲ ۸-۳-۲ واترمارکینگ در حوزه‌ی تبدیل اسلنت
۴۳ ۴-۲ ارزیابی سیستم‌های واترمارکینگ
۴۳ ۱-۴-۲ ارزیابی بر اساس شفافیت
۴۷ ۲-۴-۲ ارزیابی بر اساس مقاومت
۵۰ ۳-۴-۲ ارزیابی بر اساس پیچیدگی الگوریتم
۵۰ ۴-۴-۲ ارزیابی بر اساس امنیت سیستم
۵۳ ۵-۲ خلاصه

۵۵	فصل سوم : واترمارکینگ تصاویر دیجیتالی مبتنی بر تبدیل پارامتریک اسلنت- هادامارد
۵۶	۱-۳ فشرده‌سازی انرژی تبدیلات تصویری.....
۵۸	۲-۳ تکرارپذیری.....
۶۱	۳-۳ واترمارکینگ در گروه تایید.....
۶۶	۴-۳ واترمارکینگ در گروه انتقال کد.....
۶۷	۵-۳ کاربرد الگوریتم ژنتیک در واترمارکینگ.....
۶۸	۶-۳ تعیین پارامترهای تبدیل پارامتریک اسلنت- هادامارد با استفاده از الگوریتم ژنتیک.....
۷۱	۷-۳ بهسازی شفافیت با استفاده از سیستم فازی.....

صفحه	عنوان
۷۳	۱-۷-۳ مشتق تصویر.....
۷۴	۲-۷-۳ مشتق فازی.....
۸۱	۸-۳ کارایی تبدیلهای مختلف در واترمارکینگ تصاویر.....
۸۴	۹-۳ خلاصه.....
۸۵	فصل چهارم : نتایج شبیه‌سازی.....
۸۶	۱-۴ فشرده‌سازی انرژی تبدیلهای مختلف.....
۸۷	۲-۴ باند میانی تبدیلهای مختلف.....
۹۱	۳-۴ تکرارپذیری.....
۹۴	۴-۴ محاسبه‌ی پارامترهای تبدیل پارامتریک اسلنت- هادامارد با استفاده از الگوریتم ژنتیک.....
۱۰۰	۵-۴ بهسازی شفافیت سیستم واترمارکینگ با استفاده از سیستم فازی.....
۱۰۹	۶-۴ مقایسه‌ی تبدیلهای مختلف در واترمارکینگ تصاویر.....
۱۲۱	۷-۴ خلاصه.....
۱۲۵	فصل پنجم : نتیجه‌گیری و پیشنهادات.....
۱۲۹	پیوست یک : تبدیلهای متعامد و یکانی.....
۱۴۰	پیوست دو : الگوریتم ژنتیک.....
۱۴۴	فهرست منابع.....

فهرست شکل‌ها

صفحه	عنوان
۳	شکل ۱-۱: طبقه‌بندی مخفی‌سازی داده توسط Vleeschouwer.....
۴	شکل ۱-۲: طبقه‌بندی مخفی‌سازی داده توسط Cheddad.....
۶	شکل ۱-۳: سیستم عمومی واترمارکینگ.....
۲۷	شکل ۱-۲: تصویر کشتی.....
۲۷	شکل ۲-۲: آرم دانشگاه اصفهان.....
۲۷	شکل ۲-۳: تصاویر واترمارک شده در بیت کم‌ارزش تا بیت پرارزش.....
۲۸	شکل ۲-۴: تصاویر مربوط به فقط بیت هفت تا فقط بیت صفر تصویر کشتی.....
۲۹	شکل ۲-۵: فلوجارت درج یک رشته اعداد شبه تصادفی در تصویر.....
۳۸	شکل ۲-۶: ضرایب تبدیل DCT برای بلوک 8×8
۴۸	شکل ۲-۷: فلوجارت ارزیابی مقاومت سیستم واترمارکینگ.....
۵۲	شکل ۲-۸: منحنی ROC در حالت آشکارسازی تصادفی.....
۵۲	شکل ۲-۹: منحنی ROC سه سیستم مختلف.....
۵۸	شکل ۳-۱: فشرده‌سازی انرژی تصویر کشتی برای تبدیل گسسته کسینوسی.....
۶۲	شکل ۳-۲: باند میانی تبدیل اسلنت.....
۶۲	شکل ۳-۳: ماسک باند میانی در حوزه‌ی تبدیل فوریه.....
۶۴	شکل ۳-۴: تابع توزیع عمومی گوسین به ازای مقادیر مختلف c
۶۸	شکل ۳-۵: فلوجارت الگوریتم ژنتیک برای انتخاب پارامترهای تبدیل پارامتریک اسلنت- هادامارد.....
۷۲	شکل ۳-۶: مدل جدید برای درج واترمارک با استفاده از سیستم فازی.....
۷۳	شکل ۳-۷: همسایگی 3×3 اطراف پیکسل مرکزی.....
۷۴	شکل ۳-۸: مشتق اصلی و مشتق‌های نسبی در جهت شمال غربی.....
۷۶	شکل ۳-۹: یک سیستم فازی.....
۷۶	شکل ۳-۱۰: تابع عضویت برای مشتق‌های اصلی و نسبی.....
۷۷	شکل ۳-۱۱: تابع عضویت مشتق فازی.....
۷۹	شکل ۳-۱۲: غیرفازی‌کننده به روش نقطه مرکزی.....
۸۸	شکل ۴-۱: فشرده‌سازی انرژی تبدیل‌های DCT، Slant و Hadamard.....
۸۸	شکل ۴-۲: فشرده‌سازی انرژی تبدیل‌های DCT، Haar و Walsh.....
۸۹	شکل ۴-۳: فشرده‌سازی انرژی تبدیل‌های DCT، Multiple-betas Slant و Multiple-betas Slant.....

- شکل ۴-۴ : تصویر باند فرکانسی میانی تبدیل گسسته فوریه..... ۸۹
- شکل ۵-۴ : باند فرکانسی میانی تبدیل های مختلف..... ۹۰
- شکل ۶-۴ : باند فرکانسی میانی تبدیل پارامتریک اسلنت هادامارد به ازای دو مجموعه پارامترهای متفاوت..... ۹۱

صفحه

عنوان

- شکل ۷-۴ : منحنی ROC تبدیل پارامتریک اسلنت- هادامارد جهت تکرارپذیری..... ۹۱
- شکل ۸-۴ : واترمارک استخراج شده به ازای پارامترهای مختلف تبدیل پارامتریک اسلنت- هادامارد..... ۹۲
- شکل ۹-۴ : منحنی تغییرات آشکارساز به ازای پارامترهای مختلف..... ۹۳
- شکل ۱۰-۴ : سطح زیر منحنی ROC برای حمله ی فشرده سازی JPEG..... ۹۴
- شکل ۱۱-۴ : نمودار تغییرات مقدار برازندگی بهترین کروموزوم و متوسط مقادیر برازندگی طی نسل های متوالی..... ۹۶
- شکل ۱۲-۴ : تصاویر واترمارک شده با استفاده از پارامترهای محاسبه شده توسط الگوریتم ژنتیک.. ۹۷
- شکل ۱۳-۴ : نمودار تغییرات مقدار برازندگی بهترین کروموزوم و متوسط مقادیر برازندگی طی نسل های متوالی برای تصویر Lena..... ۹۸
- شکل ۱۴-۴ : نمودار تغییرات مقدار برازندگی بهترین کروموزوم و متوسط مقادیر برازندگی طی نسل های متوالی برای تصویر Baboon..... ۱۰۰
- شکل ۱۵-۴ : واترمارک استخراج شده بعد از حمله های مختلف..... ۱۰۰
- شکل ۱۶-۴ : نتایج ماسک Barni و ماسک فازی..... ۱۰۱
- شکل ۱۷-۴ : تصویر واترمارک شده و آشکارساز واترمارک برای تصویر دوربین..... ۱۰۲
- شکل ۱۸-۴ : تصاویر واترمارک شده با الگوریتم پیشنهادی و مورد حمله قرار گرفته به همراه آشکارسازی..... ۱۰۷
- شکل ۱۹-۴ : واترمارک های استخراج شده پس از حمله های متداول..... ۱۰۸
- شکل ۲۰-۴ : هیستوگرام ضرایب تبدیل تصویر کشتی..... ۱۱۱
- شکل ۲۱-۴ : تصاویر مختلف میزبان..... ۱۱۴
- شکل ۲۲-۴ : منحنی PSNR برای تصاویر مختلف..... ۱۱۵
- شکل ۲۳-۴ : منحنی BCR تصاویر مختلف در مقابل حمله ی فیلتر عدد میانه با سایز ۳×۳..... ۱۱۶
- شکل ۲۴-۴ : منحنی BCR تصاویر مختلف در مقابل حمله ی فیلتر میانگین با سایز ۳×۳..... ۱۱۶
- شکل ۲۵-۴ : منحنی BCR تصاویر مختلف در مقابل حمله ی فیلتر پایین گذر باترورث مرتبه دوم..... ۱۱۷
- شکل ۲۶-۴ : منحنی BCR تصاویر مختلف در مقابل حمله ی فیلتر بالاگذر باترورث مرتبه دوم..... ۱۱۷
- شکل ۲۷-۴ : منحنی BCR تصاویر مختلف در مقابل حمله ی متعادل سازی هیستوگرام..... ۱۱۸

۱۱۹	شکل ۴-۲۸ : منحنی BCR تصاویر مختلف در مقابل حمله‌ی فشرده‌سازی JPEG با ضریب کیفیت/۸۰
۱۱۹	شکل ۴-۲۹ : منحنی BCR تصاویر مختلف در مقابل حمله‌ی نویز گوسی با میانگین صفر و انحراف۰/۰۱ معیار
۱۲۰	شکل ۴-۳۰ : منحنی BCR تصاویر مختلف در مقابل حمله‌ی تغییر سایز با اندازه دو.....
۱۲۱	شکل ۴-۳۱ : منحنی BCR تصاویر مختلف در مقابل حمله‌ی چرخش.....
۱۲۲	شکل ۴-۳۲ : منحنی BCR تصاویر مختلف در مقابل حمله‌ی برش با مرکز (۱۲۸ و ۱۲۸) با شعاع۱۰۰

صفحه

عنوان

۱۲۳	شکل ۴-۳۳ : منحنی BCR تصاویر مختلف در مقابل حمله‌ی تصحیح گاما با پارامتر ۱/۵.....
۱۲۳	شکل ۴-۳۴ : منحنی BCR تصاویر مختلف در مقابل حمله‌ی تنظیم سطوح خاکستری در بازه[۰/۲-۰/۸]
۱۲۴	شکل ۴-۳۵ : منحنی BCR تصاویر مختلف در مقابل حمله‌ی هافتون.....

فهرست جدول‌ها

صفحه	عنوان
۷۵	جدول ۱-۳ : مشتق‌های اصلی و نسبی
۸۰	جدول ۲-۳ : قوانین فازی
۹۵	جدول ۱-۴ : محدوده تغییرات پارامترهای تبدیل پارامتریک اسلنت- هادامارد
۹۸	جدول ۲-۴ : پارامترهای محاسبه شده توسط الگوریتم ژنتیک و نتایج آزمایش‌ها با این پارامترها
۱۱۰	جدول ۳-۴ : مقاومت و شفافیت تبدیل‌های مختلف برای ارزیابی سیستم واترمارکینگ مبتنی بر آنروپی
۱۱۲	جدول ۴-۴ : نتایج معیار ارزیابی برای تبدیل‌های مختلف
۱۱۳	جدول ۵-۴ : نتایج ارزیابی تبدیل‌های مختلف برای واترمارکینگ تصاویر

فصل اول

مقدمه و مبانی

پیشرفت سریع علوم کامپیوتر، شبکه‌های کامپیوتری، ارتباطات و گسترش روزافزون کاربرد سیستم‌های چندرسانه‌ای دیجیتال^۱ 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 دیجیتال ایجاد کرده است.

امنیت^۲ و استفاده‌ی قانونی^۳ از محصول‌های دیجیتال، امری مهم و مورد توجه اکثر هنرمندان و صاحبان آثار دیجیتال است. آن‌ها علاقه‌مند هستند آثار هنری‌شان در مقابل تکثیرهای غیرمجاز محفوظ بماند و کلیه حقوق نشر و تکثیر متعلق به صاحبان آثار باقی بماند. برای حل این مشکل، دو مقوله‌ی «رمزنگاری»^۴ و «واترمارکینگ»^۵ 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 امنیت سیستم رمزنگاری، عملیات ریاضی با استفاده از کلیدهای^۱ خاص و منحصر به فرد انجام می‌شود.

نکته‌ی مهم و قابل توجه 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 معمولاً از سیستم‌های رمزنگاری برای حفاظت داده به خصوص داده‌ی تصویر، کم‌تر استفاده می‌شوند.

برای داشتن یک ابزار قوی‌تر به گونه‌ای 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 مریبی^۲ و یا نامریبی^۳، می‌توان از تغییر و جعل آن جلوگیری کرد. در دهه‌های اخیر به دلیل اهمیت حفاظت داده‌ی دیجیتالی، در سطح جهانی تحقیق‌های فراوانی در زمینه‌ی مخفی‌سازی داده^۴ صورت گرفته است. واترمارکینگ به عنوان یکی از زیرگروه‌های مخفی‌سازی داده در تصویرهای ساکن^۵، تصویرهای متحرک، و صوت^۶ به صورت نظری و کاربردی گسترش قابل توجهی داشته است.

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

¹ Keys

² Visible

³ Invisible

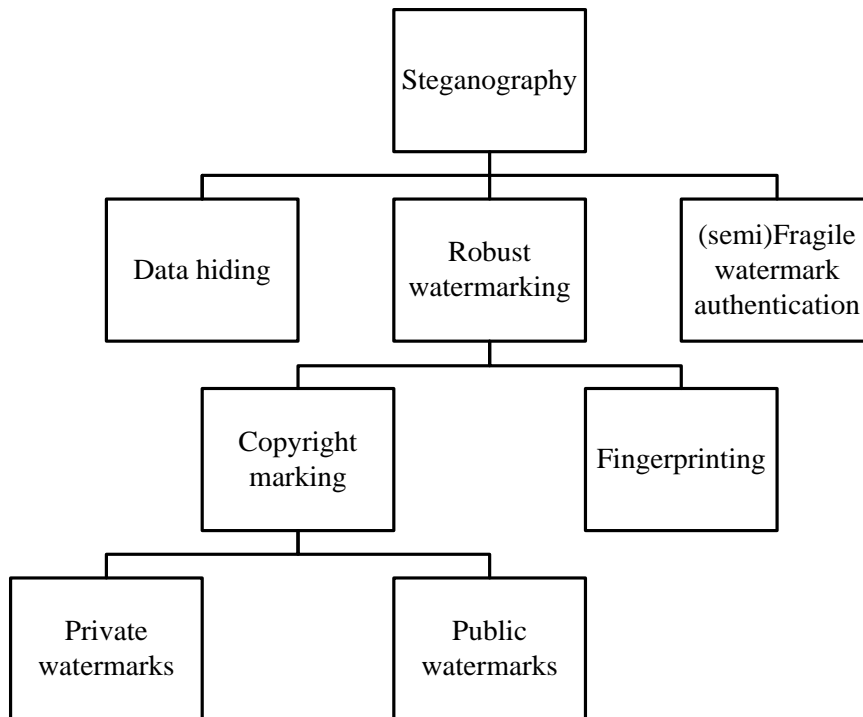
⁴ Data Hiding

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 و اترمارکینگ 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]

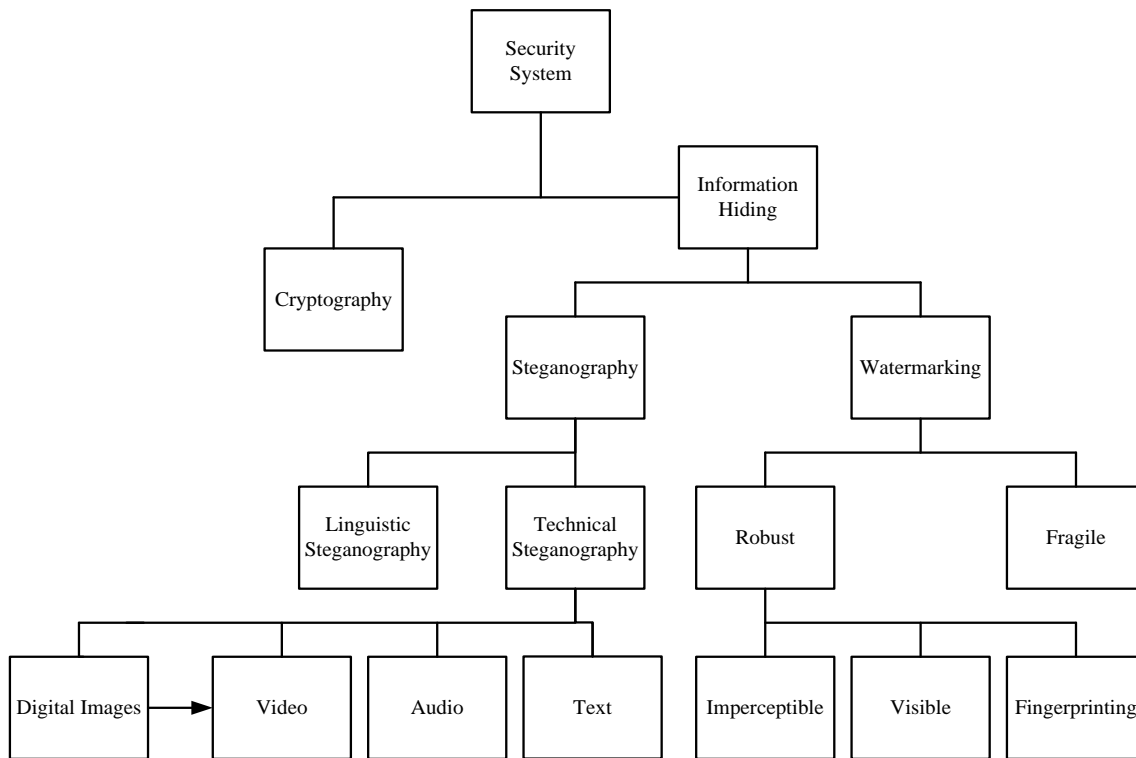
¹ Steganography

² Covered

³ Writing

⁴ tattooed

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



شکل ۲-۱: 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^۱ از اهمیت ویژه‌ای برخوردار است و برای حفظ اصالت و جلوگیری از جعل و تکثیر غیرمجاز آن با سیگنال دیگری به نام واترمارک^۲ نشانه‌گذاری می‌شود. در واترمارکینگ، سیگنال واترمارک یک سیگنال معمولی است و از بین رفتن آن زیاد مهم نیست و فقط سالم ماندن سیگنال میزبان اهمیت دارد. اما در مخفی‌نگاری، پیامی که در سیگنال میزبان مخفی می‌شود، مهم است.

¹ Host
² Watermark