



دانشگاه 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 واترمارک در ضرایب تبدیل موجک گسسته با استفاده از روش همسایگی ضرایب پیشنهاد شده است. نتایج حاصل از این الگوریتم 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 الگوریتم 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

فصل اول .....	۱
مقدمه ای بر واترمارکینگ .....	۱
۱-۱-پنهان شدن اطلاعات ، استگانوگرافی ، واترمارکینگ .....	۴
۱-۲- تاریخچه واترمارکینگ .....	۷
۱-۳- اهمیت واترمارکینگ .....	۱۰
فصل دوم .....	۱۵
کاربردها و ویژگیهای واترمارکینگ .....	۱۵
۲-۱- کاربرد های واترمارکینگ .....	۱۶
۲-۱-۱- نظارت بر پخش .....	۱۷
۲-۱-۲- شناسایی مالک اثر .....	۱۹
۲-۱-۳- اثبات مالکیت .....	۲۱
۲-۱-۴- پیگیری تراکنش .....	۲۳
۲-۱-۵- تصدیق محتوا .....	۲۵
۲-۱-۶- کنترل کپی .....	۲۷
۲-۱-۸- بهبود میراث .....	۳۱
۲-۲- خصوصیات سیستم های واترمارکینگ .....	۳۲
۲-۲-۱- اثر بخشی درج .....	۳۳
۲-۲-۲- درستی .....	۳۳
۲-۲-۳- میزان داده ذخیره شده .....	۳۴
۲-۲-۴- استخراج آگاهانه یا کور .....	۳۵
۲-۲-۵- نرخ مثبت اشتباه .....	۳۶
۲-۲-۶- مقاومت .....	۳۷
۲-۲-۷- امنیت .....	۳۸
۲-۲-۸- رمز و کلیدهای واترمارک .....	۴۰
۲-۲-۹- دستکاری و واترمارکینگ چندگانه .....	۴۳
۲-۲-۱۰- هزینه .....	۴۳
فصل سوم .....	۴۵
آشوب و سیستمهای دینامیکی .....	۴۵
۳-۱- خلاصه های از علم دینامیک .....	۴۶
۳-۲- سیستمهای دینامیکی: .....	۴۸
۳-۲-۱- سیستمهای دینامیکی خطی .....	۴۸
۳-۲-۲- سیستمهای دینامیکی غیر خطی .....	۴۹

۵۰	۳-۳- معادلات دیفرانسیل
۵۲	۳-۴- فضای فاز
۵۴	۳-۵- نگاشتهای تکرار
۵۴	۳-۶- نگاشتهای خطی
۵۵	۳-۶-۱- نگاشت لورنتس
۵۵	۳-۶-۲- نگاشت تنت
۵۶	۳-۷- نگاشتهای غیرخطی
۵۶	۳-۷-۱- نگاشت لجستیک
۵۶	۳-۷-۲- نگاشت هنون
۵۶	۳-۸- سیستمهای دینامیکی غیرخطی
۵۷	۳-۸-۱- دوشاخه شدگی
۵۷	۳-۸-۲- دوشاخه شدگی زینی
۵۸	۳-۸-۳- دوشاخه شدگی گذار بحرانی
۵۹	۳-۸-۶- آشوب
۶۱	۳-۸-۷- جذب کنندهها
۶۲	۳-۸-۸- معادلات لورنتس
۶۵	۳-۸-۹- نمای لیپانوف
۶۷	۳-۸-۱۰- فراکتالها
۶۹	فصل چهارم
۶۹	الگوریتم های پیشنهادی
۷۱	۴-۱- سیستم های آشوبناک
۷۱	۴-۱-۱- نگاشت بیضوی ژاکوبی:
۷۲	۴-۱-۲- نگاشت غیر خطی تکه ای آشوبناک
۷۲	۴-۱-۳- نگاشت زوج شده آشوبناک
۷۳	۴-۱-۴- نگاشت کوانتومی
۷۳	۴-۲- چگونگی استفاده از نگاشت ها در واترمارکینگ
۷۴	۴-۲-۱- استفاده از نگاشت ها در رمزنگاری واترمارک
۷۴	۴-۲-۲- استفاده از نگاشت آشوبناک جهت تعیین محل درج و استخراج واترمارک در تصویر میزبان ..
۷۵	۴-۳- مدل اصلی سیستم واترمارکینگ پیشنهادی
۷۵	۴-۴- الگوریتم های پیشنهادی
۷۵	۴-۴-۱- الگوریتم اول : استفاده از تبدیل DCT و نگاشت های آشوبناک
۷۶	۴-۴-۱-۱- فرآیند رمزنگاری و رمزگشایی واترمارک
۷۷	۴-۴-۱-۲- فرآیند درج واترمارک
۷۹	۴-۴-۱-۳- فرآیند استخراج واترمارک



۴-۴-۲- الگوریتم دوم: سیستم واترمارکینگ دیجیتال با استفاده از تبدیل موجک گسسته و سیستم های	
آشوبناک .....	۸۲
۴-۴-۲-۱- فرآیند رمزنگاری و رمزگشایی واترمارک .....	۸۲
۴-۴-۲-۲- فرآیند درج واترمارک .....	۸۲
۴-۴-۲-۳- فرآیند استخراج واترمارک .....	۸۴
۴-۴-۳- الگوریتم سوم: استفاده از تبدیل موجک گسسته و تجزیه مقدار منفرد در واترمارکینگ تصویر	
دیجیتال و امنیت واترمارک با استفاده از سیستم های آشوبناک .....	۸۶
۴-۴-۳-۱- فرآیند رمزنگاری و رمزگشایی واترمارک .....	۸۸
۴-۴-۳-۲- فرآیند درج واترمارک .....	۸۸
۴-۴-۳-۳- فرآیند استخراج واترمارک .....	۸۹
فصل پنجم .....	۹۳
۵-۱- تعاریف پایه .....	۹۴
۵-۱-۱- الگوریتم های پیشنهادی .....	۹۴
۵-۱-۲- تصویر اصلی یا پوشش .....	۹۴
۵-۱-۳- لوگوی واترمارک .....	۹۵
۵-۲- نتایج آزمایش ها .....	۹۶
۵-۲-۱- اثر بخشی درج .....	۹۶
۵-۲-۲- درستی .....	۹۸
۵-۲-۳- میزان داده ذخیره شده .....	۹۹
۵-۲-۴- استخراج آگاهانه یا کور .....	۱۰۰
۵-۲-۵- نرخ مثبت اشتباه .....	۱۰۰
۵-۲-۶- مقاومت .....	۱۰۰
۵-۲-۷- امنیت .....	۱۱۰
۵-۲-۷-۱- حذف غیرمجاز .....	۱۱۰
۵-۲-۷-۲- درج غیرمجاز .....	۱۱۰
۵-۲-۷-۳- استخراج غیرمجاز .....	۱۱۱
۵-۲-۸- کلید رمز و کلید واترمارک .....	۱۱۱
۵-۲-۸-۱- فضای کلید .....	۱۱۱
۵-۲-۸-۲- آزمون های آماری برای مولد اعداد تصادفی .....	۱۱۴
منابع و مآخذ .....	۱۲۳

## فهرست تصاویر

- شکل (۱-۱) اسکناس ۲۰ دلاری ۳
- شکل (۱-۳) تعداد مقالات چاپ شده توسط موسسه IEEE درباره واترمارکینگ و استگانوگرافی ۹
- شکل (۲-۲) مثالی از کد شناسایی یکتا که در پس زمینه متن حک شده است. ۲۳
- شکل (۲-۴) رابطه مابین رمزنگاری و کنترل کپی بر اساس واترمارک ۳۰
- شکل (۴-۱) پاندول چرخان. ۵۰
- شکل (۴-۲) مسیر در فضای فاز ۵۲
- شکل ۳-۳. نقاط ثابت به ازای مقادیر مختلف پارامتر  $R$  برای معادله  $\dot{x} = r + x^2$ . ۵۸
- شکل ۳-۴: نمودار دوشاخه شدگی برای معادله  $\dot{x} = r + x^2$ . ۵۸
- شکل ۳-۵: نقاط ثابت به ازای مقادیر مختلف پارامتر  $R$  برای معادله  $\dot{x} = r x - x^2$ . ۵۹
- شکل ۳-۶: نمودار دوشاخه شدگی برای معادله  $\dot{x} = r x - x^2$ . ۵۹
- شکل ۳-۱۲: نمونه‌های از جذب کننده عجیب در دو بعد. ۶۴
- شکل ۳-۱۳: نمونه‌های از جذب کننده عجیب در سه بعد. ۶۴
- شکل ۳-۱۴: انتخاب دو مسیر در فضای فاز با فاصله جدایی به اندازه  $\delta_0$ . ۶۵
- شکل ۳-۱۵: نمونه‌های از فراکتالها. ۶۸
- شکل ( ۴-۱ ) فرآیند درج واترمارک در مدل اصلی ۷۴
- شکل ( ۴-۲ ) فرآیند استخراج واترمارک در مدل اصلی ۷۶
- شکل (۴-۳) ضرایب حاصل از تبدیل کسینوسی گسسته دو بعدی و محل درج واترمارک ۷۷
- شکل (۴-۴) انواع همسایگی های بلوک های  $3 \times 3$  در ضرایب DCT ۷۸
- شکل (۴-۶) فلوجارت فرآیند استخراج واترمارک در الگوریتم اول ۸۱
- شکل (۴-۵) فلوجارت فرآیند درج واترمارک در الگوریتم اول ۸۱
- شکل (۴-۷) زیر باندهای حاصل از تبدیل موجک گسسته دوبعدی ۸۳

- شکل (۴-۱۰) تجزیه مقدار منفرد در یک بلوک ۴×۴ ۸۶
- شکل (۴-۹) فلوجارت فرآیند استخراج واترمارک در الگوریتم دوم ۸۷
- شکل (۴-۸) فلوجارت فرآیند درج واترمارک در الگوریتم دوم ۸۷
- شکل (۴-۱۱) فلوجارت فرآیند درج واترمارک در الگوریتم سوم ۹۱
- شکل (۴-۱۲) فلوجارت فرآیند استخراج واترمارک در الگوریتم سوم ۹۲
- شکل ۳-۵: لوگوی واترمارک ثابت برای تمام الگوریتم ها ( لوگوی USB ) ۹۵
- شکل ۲-۵: تصاویر مورد استفاده برای هر سه الگوریتم الف) تصویر HILL ب) تصویر BOAT ۹۵
- پ) تصویر PEPPERS ۹۵
- شکل ۱-۵: الف) تصویر FERDOWSI HALL (الگوریتم اول) ب) تصویر LENA (الگوریتم دوم) ۹۵
- پ) تصویر BARBARA (الگوریتم سوم) ۹۵
- شکل ۵-۵ : نتایج حاصل از الگوریتم دوم الف) تصویر اصلی (LENA) ب) تصویر واترمارک شده پ) لوگوی استخراج شده با مجموعه کلید صحیح ت) لوگوی استخراج شده با کلید ناصحیح ث) هیستوگرام تصویر اصلی ج) هیستوگرام تصویر واترمارک شده ۹۷
- شکل ۴-۵ : نتایج حاصل از الگوریتم اول الف) تصویر اصلی (FERDOWSI HALL) ب) تصویر واترمارک شده پ) لوگوی استخراج شده با مجموعه کلید صحیح ت) لوگوی استخراج شده با مجموع کلید ناصحیح ث) هیستوگرام تصویر اصلی ج) هیستوگرام تصویر واترمارک شده ۹۷
- شکل ۶-۵ : نتایج حاصل از الگوریتم سوم الف) تصویر اصلی (BARBARA) ب) تصویر واترمارک شده پ) لوگوی استخراج شده با مجموعه کلید صحیح ت) لوگوی استخراج شده با کلید ناصحیح ث) هیستوگرام تصویر اصلی ج) هیستوگرام تصویر واترمارک شده ۹۸
- شکل ۸-۵ : نتایج حاصل از استخراج واترمارک با الگوریتم اول در مقابل حملات الف) فشرده سازی JPEG (۰.۷۵) ب) نویز نمک و فلفل (۰.۱۰) پ) نویز گوسی (۰.۰۰۱) ت) یکسان کردن هیستوگرام ث) فیلتر میانه [۳×۳] ج) فیلتر پایین گذر [۳×۳] چ) تصحیح گاما (۰.۶۰) ح) مات کردن (۱۵°) خ) چرخش (۱°) د) برش (۰.۲۵) ذ) برش (۰.۵۰) ر) تیز کردن ز) مکمل کردن ۱۰۳

شکل ۷-۵: تصویر واترمارک شده حاصل از الگوریتم اول در مقابل حملات الف) فشرده سازی JPEG (۷۵٪) ب) نویز نمک و فلفل (۱۰٪) پ) نویز گوسی (۰،۰۰۱) ت) یکسان کردن هیستوگرام ث) فیلتر میانه [۳×۳] ج) فیلتر پایین گذر [۳×۳] چ) تصحیح گاما (۰،۶) ح) مات کردن (۱۵°) خ) چرخش (۱°) د) برش (۲۵٪) ز) تیزکردن (۵۰٪) ر) تیزکردن ز) مکمل کردن ۱۰۳

شکل ۹-۵: تصویر واترمارک شده حاصل از الگوریتم دوم در مقابل حملات الف) فشرده سازی JPEG (۷۵٪) ب) نویز نمک و فلفل (۱۰٪) پ) نویز گوسی (۰،۰۰۱) ت) یکسان کردن هیستوگرام ث) فیلتر میانه [۳×۳] ج) فیلتر پایین گذر [۳×۳] چ) تصحیح گاما (۰،۶) ح) مات کردن (۱۵°) خ) چرخش (۱°) د) برش (۲۵٪) ز) تیزکردن (۵۰٪) ر) تیزکردن ز) مکمل کردن ۱۰۴

شکل ۱۰-۵: نتایج حاصل از استخراج واترمارک با الگوریتم دوم در مقابل حملات الف) فشرده سازی JPEG (۷۵٪) ب) نویز نمک و فلفل (۱۰٪) پ) نویز گوسی (۰،۰۰۱) ت) یکسان کردن هیستوگرام ث) فیلتر میانه [۳×۳] ج) فیلتر پایین گذر [۳×۳] چ) تصحیح گاما (۰،۶) ح) مات کردن (۱۵°) خ) چرخش (۱°) د) برش (۲۵٪) ز) تیزکردن (۵۰٪) ر) تیزکردن ز) مکمل کردن ۱۰۴

شکل ۱۲-۵: نتایج حاصل از استخراج واترمارک با الگوریتم سوم در مقابل حملات الف) فشرده سازی JPEG (۷۵٪) ب) نویز نمک و فلفل (۱۰٪) پ) نویز گوسی (۰،۰۰۱) ت) یکسان کردن هیستوگرام ث) فیلتر میانه [۳×۳] ج) فیلتر پایین گذر [۳×۳] چ) تصحیح گاما (۰،۶) ح) مات کردن (۱۵°) خ) چرخش (۱°) د) برش (۲۵٪) ز) تیزکردن (۵۰٪) ر) تیزکردن ز) مکمل کردن ۱۰۵

شکل ۱۱-۵: تصویر واترمارک شده حاصل از الگوریتم سوم در مقابل حملات الف) فشرده سازی JPEG (۷۵٪) ب) نویز نمک و فلفل (۱۰٪) پ) نویز گوسی (۰،۰۰۱) ت) یکسان کردن هیستوگرام ث) فیلتر میانه [۳×۳] ج) فیلتر پایین گذر [۳×۳] چ) تصحیح گاما (۰،۶) ح) مات کردن (۱۵°) خ) چرخش (۱°) د) برش (۲۵٪) ز) تیزکردن (۵۰٪) ر) تیزکردن ز) مکمل کردن ۱۰۵

شکل ۱۴-۵: نمودار مقایسه BER در سه الگوریتم پیشنهادی بر اساس تصویر BOAT ۱۰۹

شکل ۱۳-۵: نمودار مقایسه BER در سه الگوریتم پیشنهادی بر اساس تصویر HILL ۱۰۹

شکل ۱۵-۵ : نمودار دوشاخگی نگاشت های (الف) نگاشت بیضوی ژاکوبی (ب و پ) نگاشت زوج شده (ث و ج)

۱۱۲

نگاشت کوانتومی (چ) نگاشت غیر خطی تکه ای

## 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<sup>۱</sup> در آن تکرار شده است. این واترمارک مستقیماً 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 (مثلاً 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 جوهر 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 اساساً 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<sup>۲</sup> است.

---

<sup>1</sup> Watermark

<sup>2</sup> 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 یک پیام در آن اثر تعریف می شود. استگانوگرافی به عنوان عملی برای غیر قابل کشف سازی یک اثر متفاوت و برای 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<sup>۳</sup> و یک استخراج کننده<sup>۴</sup> 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<sup>۵</sup> 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 سال ۱۹۹۰ 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]،

---

<sup>3</sup> Embedder  
<sup>4</sup> Extractor  
<sup>5</sup> 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 ، 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.

پنهان شدن اطلاعات ( یا پنهان کردن داده ها) اصطلاحی کلی است که یک دامنه ی 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 نمونه های تحقیقاتی در این زمینه ممکن است در کنفرانس های بین المللی پنهان سازی 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.

---

<sup>6</sup> Information Hiding

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

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

استگنوگرافی در داستان کهن از هرودوت نقل شده است [۲۴]. که طبق دستور او یکی از بردگانش همراه اربابش هیستایوس با یک پیغام محرمانه که روی سر برده خالکوبی شده بود به شهر میلِتوس در یونان فرستاده می شود. بعد از خالکوبی و گذشت مدت زمانی موهای برده رشد می کند و پیغام را مخفی می کند. پس از عزیمت آنها به میلِتوس، 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 می کند. در این سناریو، پیام دارای ارزش اولیه برای هیستایوس بوده و برده فقط حامل پیغام بوده است. می توان از این مثال برای برجسته کردن تفاوت بین واترمارکینگ و استگنوگرافی استفاده کرد. فرض شود که پیغام روی سر برده قابل دید نباشد، این برده به هیستایوس 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 هیستایوس می تواند سر برده را بتراشد و مالکیتش را ثابت کند. در این سناریو برده (اثر پوششی) دارای ارزش اولیه برای هیستایوس 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 استگنوگرافی تقسیم شود که در آن وجود پیام به صورت مخفی نگه داشته می شود. در سیستم های غیر استگنوگرافی 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 استگنوگرافی 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 می‌دهد. پیمان SALT\_II به هر دو کشور اجازه می‌دهد تا تعداد زیادی انبار موشکی داشته باشند، اما باید تعداد موشک‌ها محدود باشد. برای بررسی تعهدات این پیمان، هر یک از کشورها می‌توانند 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 می‌توان 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 هشدار است که این تصاویر را نمی‌توان بازسازی کرد. باید دانست که واترمارک نامرئی درج شده در هر تصویر مانع سرقت می‌شود.

۴- درج اطلاعات آشکار به انتقال اطلاعات کمی شناخته شده به اثر اشاره دارد. در جایی که اطلاعات پنهان شده با سیگنال‌هایی 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 می‌شد [۲۷]. کد غیرقابل شنیدن در زمان پخش و پنهان بود. اما واترمارک

نیست، زیرا پیام با محتوای پخش غیر مرتبط بود. ضمناً، آن مثالی برای استگنوگرافی 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. می توان 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