



دانشگاه پیام نور

دانشکده: فنی و مهندسی

گروه علمی: کامپیوتر و فناوری اطلاعات

واترمارکینگ تصاویر رنگی مبتنی بر تئوری آشوب در حوزه فرکانس

نگارش: قاسم قاریزاده مقدم

استاد راهنما: جناب آقای دکتر مهدی جوانمرد

پایان نامه

برای دریافت کارشناسی ارشد

در رشته مهندسی کامپیوتر گرایش نرم افزار

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 روش های حفاظت اطلاعات محسوب می گردد. روش های گوناگونی برای واترمارکینگ تصاویر دیجیتال به کار گرفته شده تا با سرعت بالاتر، روش های 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 مدل های تصاویر رنگی و روش های 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

صفحه	عنوان
	فصل اول: واتر مارکینگ
۲	۱-۱: واتر مارکینگ چیست؟
۲	۲-۱: ضرورت و اهداف واتر مارکینگ
۳	۳-۱: واتر مارک فیزیکی
۴	۴-۱: واتر مارک دیجیتال
۵	۵-۱: تعاریف مشابه و تفاوت‌ها
۵	۱-۵-۱: رمز نگاری
۵	۲-۵-۱: پنهان نگاری
۶	۳-۵-۱: تفاوت رمز نگاری و پنهان نگاری
۷	۴-۵-۱: واتر مارکینگ
۷	۶-۱: تفاوت‌های پنهان نگاری و واتر مارکینگ
۸	۷-۱: تاریخچه واتر مارکینگ
۱۰	۸-۱: مفاهیم و اصطلاحات متداول
۱۱	۹-۱: ویژگی‌های قابل تعریف در واتر مارک
۱۲	۱۰-۱: چهارچوب کاری واتر مارک
۱۴	۱۱-۱: کاربردهای عملی واتر مارکینگ
۱۷	۱۲-۱: پارامترهای ارزیابی واتر مارکینگ
۱۹	۱۳-۱: دامنه‌های جاسازی واتر مارک
۲۰	۱-۱۳-۱: دامنه‌ی مکانی
۲۱	۲-۱۳-۱: دامنه‌ی فرکانسی
۲۲	۱۴-۱: استفاده از واتر مارکینگ در ایران و سایر کشورها

## فصل دوم: نظریه آشوب و توابع آن

- ۲۴ ۱-۲ تعریف آشوب
- ۲۹ ۲-۲: خواص سیستم های آشوبی
- ۲۹ ۱-۲-۲: حساسیت به شرایط اولیه
- ۳۰ ۲-۲-۲: قطعیت
- ۳۰ ۳-۲-۲: عدم پیش بینی آماری
- ۳۱ ۳-۲: نمونه هایی از سیستم های آشوبی
- ۳۱ ۱-۳-۲: نگاشت
- ۳۱ ۲-۳-۲: نگاشت لجستیک
- ۳۴ ۳-۳-۲: نگاشت تنگ
- ۳۵ ۴-۳-۲: نگاشت نمایی
- ۳۶ ۵-۳-۲: نگاشت سینوسی
- ۳۶ ۶-۳-۲: نگاشت گاوسی
- ۳۶ ۷-۳-۲: نگاشت لورنز
- ۳۹ ۸-۳-۲: نگاشت آشوب چرخشی
- ۴۰ ۴-۲: نمونه هایی از سیستم های فوق آشوبی
- ۴۱ ۱-۴-۲: سیستم های فوق آشوبی چهاربعدی روسلر
- ۴۱ ۲-۴-۲: سیستم فوق آشوبی دستمال تاخوردده
- ۴۲ ۳-۴-۲: سیستم فوق آشوبی هنون
- ۴۳ ۴-۴-۲: سیستم های فوق آشوبی نه بعدی
- ۴۴ ۵-۴-۲: سیستم فوق آشوبی لورنز
- ۴۷ ۶-۴-۲: سیستم فوق آشوب چن
- ۴۸ ۷-۴-۲: سیستم فوق آشوبی لوو

فصل سوم: انواع تصاویر رنگی و روشهای واترمارکینگ دیجیتال

۵۳	۱-۳ مدل رنگ RGB
۵۵	۲-۳ مدل رنگ CMY
۵۶	۳-۳ مدل رنگ YIQ
۵۷	۴-۳ مدل رنگ HIS
۶۱	۵-۳ تبدیل رنگها از RGB به HIS
۶۲	۶-۳ تبدیل رنگها از HSI به RGB
۶۴	۷-۳: واترمارکینگ خالص
۶۵	۸-۳: واترمارکینگ با کلید مخفی
۶۵	۹-۳: واترمارکینگ با کلید عمومی
۶۶	۱۰-۳: واترمارکینگ در تصاویر رنگی
۶۶	۱-۱۰-۳: واترمارکینگ در تصاویر رنگی بر اساس سیستم بصری انسان
۶۷	۲-۱۰-۳: واترمارکینگ تصاویر رنگی با استفاده از MWT
۶۷	۳-۱۰-۳: واترمارکینگ تصاویر رنگی با استفاده از فضای YST
۶۷	۱۱-۳: واترمارکینگ تصویر با تبدیل با دامنه فرکانسی
۶۸	۱-۱۱-۳: واترمارکینگ بازگشت پذیر وفقی بر اساس تبدیل طول موج
۶۸	۲-۱۱-۳: واترمارکینگ بر اساس DCT و DHT
۶۹	۳-۱۱-۳: واترمارکینگ بر اساس DCT و Cort
۶۹	۴-۱۱-۳: واترمارکینگ بر اساس DCT و طیف گسترده
۷۰	۵-۱۱-۳: روش بازیابی بر روی واترمارکهای دیجیتال
۷۰	۶-۱۱-۳: روش واترمارکینگ بر اساس CT, SVD
۷۰	۱۲-۳: روش های واترمارکینگ مبتنی بر سلولار اتوماتا
۷۱	۱-۱۲-۳: واترمارکینگ تصاویر رنگی با اتوماتای سلولی و دنباله ی رندوم p-seudo
۷۱	۲-۱۲-۳: یک روش واترمارکینگ بر اساس تبدیل با سلولار اتوماتا

- ۷۲ ۳-۱۲-۳: واترمارکینگ بر اساس اسکرمبل تصویر با سلولار اتوماتای فوق آشوبی
- ۷۲ ۳-۱۳: روشهای واترمارکینگ با قدرت مقابله در مقابل حملات هندسی
- ۷۲ ۳-۱۳-۱: واترمارکینگ تصویر مستقل از تغییرات هندسی بر اساس ACR
- ۷۳ ۳-۱۳-۲: یک تکنیک بهینه سازی موثر برای واترمارکینگ دیجیتال
- ۷۳ ۳-۱۳-۳: واترمارکینگ بر مبنای نرمال سازی تصویر و کدهای فرکتالی
- ۷۳ ۳-۱۳-۴: واترمارکینگ صفر بر اساس تئوری تشدید وفقی فازی
- ۷۴ ۳-۱۴: روش های واترمارکینگ مبتنی بر آشوب
- ۷۴ ۳-۱۴-۱: الگوریتم واترمارکینگ وفقی تصویر بر اساس رمزنگاری آشوبی و DCT
- ۷۵ ۳-۱۴-۲: یک روش واترمارکینگ بر اساس دو نگاشت آشوبی
- ۷۵ ۳-۱۴-۳: واترمارکینگ تصویر بر اساس نگاشت آشوبی PLCM
- ۷۶ ۳-۱۴-۴: تکنولوژی واترمارکینگ بر اساس جاذب آشوبی لورنز
- ۷۶ ۳-۱۴-۵: الگوریتم واترمارکینگ برای محافظت حق کپی تصویر
- ۷۷ ۳-۱۴-۶: یک روش رمزنگاری امن دیگر برای جاسازی واترمارک
- ۷۸ ۳-۱۵: سایر موارد
- ۷۸ ۳-۱۵-۱: واترمارکینگ مبتنی بر تغییر یافته ی مربع جادویی
- ۷۸ ۳-۱۵-۲: واترمارکینگ دو دامنه ای
- ۷۹ ۳-۱۵-۵: واترمارکینگ دوتایی بر اساس تبدیل فوریه فرکتالی
- فصل چهارم: روش پیشنهادی
- ۸۱ ۴-۱: ویژگی های الگوریتم واترمارکینگ پیشنهادی
- ۸۲ ۴-۲: جاسازی واترمارک در تصویر میزبان
- ۸۲ ۴-۲-۱: ایجاد دنباله ی فوق آشوبی لورنز برای درهم آمیختن تصویر واترمارک
- ۸۳ ۴-۲-۲: اعمال پردازش های لازم بر روی هر یک از دنباله های فوق آشوبی
- ۸۳ ۴-۲-۳: مقیاس گذاری خروجی چهارم و یا همان کلید خارجی
- ۸۳ ۴-۲-۴: تغییر ترتیب سه ورودی اول با توجه به کلید خارجی

۸۴	۴-۲-۵: مقیاس گذاری سه خروجی اول با توجه به سایز تصویر
۸۴	۴-۲-۶: ترکیب دنباله‌های فوق آشوبی
۸۶	۴-۲-۷: تولید ماتریس جابجایی
۸۶	۴-۲-۷-۱: مقدار دهی اولیه ماتریس A
۸۶	۴-۲-۷-۲: کامل کردن ماتریس A
۹۱	۴-۲-۷-۳: تکرار ماتریس H که قبلاً در ماتریس A تکرار شده است
۹۲	۴-۲-۷-۴: تکرار از ماتریس A در ماتریس H
۹۳	۴-۲-۸: نحوه ی مشخص کردن مقادیر تکراری
۹۴	۴-۲-۹: انتخاب مدل رنگ تصویر میزبان برای درج واترمارک
۹۴	۴-۲-۱۰: تبدیل فرکانسی تصویر میزبان به روش DWT
۹۷	۴-۲-۱۱: مشخص کردن مکان درج واترمارک در تصویر میزبان
۹۹	۴-۳: استخراج واترمارک
	فصل پنجم: تحلیل روش پیشنهادی و نتیجه گیری
۱۰۲	۵-۱: ارزیابی تأثیرگذاری
۱۰۴	۵-۲: زمان نگاشت واترمارک
۱۰۴	۵-۳: ارزیابی مقاومت در برابر حملات
۱۰۵	۵-۳-۱: حملات غیر هندسی
۱۰۷	۵-۳-۲: حملات هندسی
۱۰۸	۵-۴: نتیجه گیری
۱۰۸	۵-۵: پیشنهادات برای تحقیقات آینده
۱۱۰	منابع و مراجع:



## فهرست شکل ها

صفحه	عنوان
۶	شکل ۱-۱: فرآیند رمزنگاری
۶	شکل ۲-۱: فرآیند پنهان نگاری
۷	شکل ۳-۱: فرآیند واترمارکینگ
۱۳	شکل ۴-۱: درج واترمارک
۱۳	شکل ۵-۱: استخراج واترمارک
۱۴	شکل ۶-۱: آشکارسازی واترمارک
۳۰	شکل ۱-۲: حساسیت شدید به تغییرات اندک شرایط اولیه در سیستم های آشوبی
۳۲	شکل ۲-۲: رفتار آشوبی نگاشت لاجستیک
۳۲	شکل ۳-۲: مسیر فضای حالت نگاشت لاجستیک
۳۳	شکل ۴-۲: نگاشت لاجستیک با توجه به مقادیر مختلف $r$
۳۵	شکل ۵-۲: رفتار آشوبی سیستم تنت در بازه زمانی
۳۵	شکل ۶-۲: مسیر فضای حالت نگاشت تنت
۳۷	شکل ۷-۲: تصویر جاذب سیستم در فضای فاز $(X-Y)$
۳۷	شکل ۸-۲: تصویر جاذب سیستم در فضای فاز $(X-Z)$
۳۷	شکل ۹-۲: تصویر جاذب سیستم در فضای فاز $(Y-Z)$
۳۷	شکل ۱۰-۲: تصویر جاذب سیستم در فضای فاز $(X-Y-Z)$
۳۸	شکل ۱۱-۲: پاسخ زمانی متغیرهای حالت سیستم آشوبناک لورنز
۳۹	شکل ۱۲-۲: مسیر فضای حالت (الف: یک سیستم تصادفی ، ب: یک سیستم آشوبی)
۴۲	شکل ۱۳-۲: سیستم فوق آشوب دستمال تاخوردده
۴۴	شکل ۱۴-۲: نمایی از سیستم فوق آشوبی ۹ بعدی

- شکل ۲-۱۵: نماهایی از سیستم فوق آشوبی لورنز ۴۴
- شکل ۲-۱۶: رفتار فوق آشوبی لورنز ۴۵
- شکل ۲-۱۷: رفتار آشوبی لورنز ۴۶
- شکل ۲-۱۸: رفتار متناوب سیستم لورنز ۴۶
- شکل ۲-۱۹: سیستم فوق آشوب چن ۴۸
- شکل ۲-۲۰: رفتار دینامیکی سیستم فوق آشوب لوو به ازای مقادیر مختلف **d** ۵۰
- شکل ۲-۲۱: منحنی های جذب سیستم فوق آشوب لوو ۵۰
- شکل ۳-۱: مکعب رنگی RGB ۵۳
- شکل ۳-۲: مکعب رنگی ۲۴ بیتی ۵۴
- شکل ۳-۳: روابط ادراکی بین مدل های رنگ RGB و HIS ۵۹
- شکل ۳-۴: پرده ی رنگ و اشباع در مدل رنگ HSI ۶۰
- شکل ۳-۵: مدل رنگ HSI مبتنی بر صفحات مثلثی و دایره ای ۶۰
- شکل ۳-۶: ضریب فرکانسی با استفاده از تابع Cort ۶۹
- شکل ۴-۱: ترکیب دنباله فوق آشوبی ۸۵
- شکل ۴-۲: ماتریس H ۸۵
- شکل ۴-۳: ماتریس اولیه ی A ۸۷
- شکل ۴-۴: ماتریس کامل A بعد از پایان برنامه ۸۷
- شکل ۴-۵: نحوه ی کامل کردن ماتریس A ۸۸
- شکل ۴-۶: تکرار در ماتریس H ۸۹
- شکل ۴-۷: نحوه ی تشخیص تکراری بودن یک مقدار ۸۹
- شکل ۴-۸: نحوه ی برخورد با تکرار در ماتریس H ۹۰
- شکل ۴-۹: تکرار شماره ی ۲ ۹۱
- شکل ۴-۱۰: تکرار شماره ۳ ۹۲
- شکل ۴-۱۱: پیدا کردن یک سطر خاص ۹۳

- شکل ۴-۱۲: واترمارک اصلی و رمز شده ۹۴
- شکل ۴-۱۳: تجزیه دو سطحی تصویر ۹۶
- شکل ۴-۱۴: تصویر میزبان تجزیه شده با تبدیل DWT ۹۷
- شکل ۴-۱۵: تصویر اصلی و واترمارک شده ۹۸
- شکل ۴-۱۶: مراحل جاسازی واترمارک در تصویر میزبان ۹۸
- شکل ۴-۱۷: واترمارک اصلی و واترمارک استخراج شده ۱۰۰
- شکل ۵-۱: تصویر میزبان اصلی ۱۰۲
- شکل ۵-۲: تصویر لوگوی واترمارک ۱۰۲
- شکل ۵-۳: تصویر واترمارک شده ۱۰۲
- شکل ۵-۴: تصویر میزبان اصلی ۱۰۲
- شکل ۵-۵: اختلاف تصویر اصلی و واترمارک شده ۱۰۲
- شکل ۵-۶: هیستوگرام تصویر اصلی و واترمارک شده ۱۰۳
- شکل ۵-۷: لوگوی استخراج شده با کلید درست ۱۰۳
- شکل ۵-۸: لوگوی استخراج شده با کلید نادرست ۱۰۳

## فهرست جدول ها

	عنوان
۱۹	جدول ۱-۱: مقایسه‌ی دامنه‌ی فرکانسی و مکانی
۳۳	جدول ۱-۲: ماهیت رفتار سیستم به ازای مقادیر مختلف I
۸۴	جدول ۱-۴: ترتیب خروجی ها بر اساس کلید خارجی
۱۰۴	جدول ۱-۵: زمان اجرای دنباله فوق آشوبی
۱۰۷	جدول ۲-۵: نتایج حمله به تصویر واترمارک شده

# 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 دهه های گذشته، ارسال و ذخیره اسناد الکترونیکی افزایش یافته است و نسخه برداری از داده ها با سرعت بالا و هزینه ای 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 سیستم های رمزنگاری شد. در سیستم های رمزنگاری قدیمی تنها دارنده کلید رمز می تواند به محتوای سند رمز شده دسترسی پیدا کند، ولی نقطه ضعف این سیستم این است که، پس از رمزگشایی داده ها 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 واترمارکینگ فیزیکی که در اسناد فیزیکی به کار می روند، واترمارکینگ دیجیتالی در تصاویر، صوت و ویدئو مطرح گردیده است.

## ۱-۲: ضرورت و اهداف واترمارکینگ

تا چندی پیش ژورنال های معتبر بین المللی، مقالات، متون علمی، داده های محرمانه و مکاتبات اداری، صرفاً به صورت فیزیکی و کاغذی وجود داشت و هریک در اختیار طیف محدودی از کاربران قرار می گرفت و به همان نسبت سوء استفاده از آنها با محدودیت و مشکلات بیشتری همراه بود، اما امروزه با پیشرفت تکنولوژی و ابداع کانال های ارتباطی گوناگون نظیر اینترنت و ارتباطات ماهواره ای و مخبراتی، انواع داده ها 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<sup>۱</sup> اصلی‌ترین 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 واترمارکینگ 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

## ۱-۴: 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 و ارتباطات 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 قالب‌های گوناگون مانند: متن، کتابهای الکترونیکی، تصاویر ساکن، تصاویر متحرک، فیلم، پایگاه‌های 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، رمزنگاری یا در اصطلاح کریپتوگرافی<sup>۱</sup> 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 ضمامم مربوطه، استفاده می‌شود. کلمه کریپتوگرافی از ریشه یونانی کریپتو به معنای رمز گرفته شده است. به فرآیند رمزنگاری اصطلاحاً 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: پنهان‌نگاری

پنهان‌نگاری یا استگانوگرافی<sup>۲</sup> 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

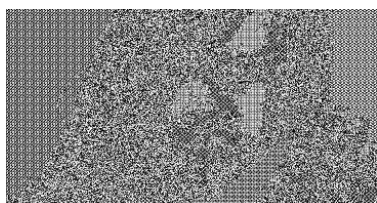
---

1. Cryptography  
2. Steganography

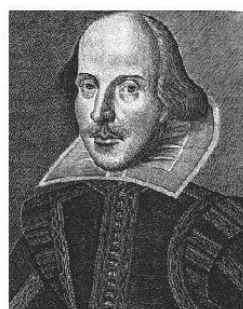
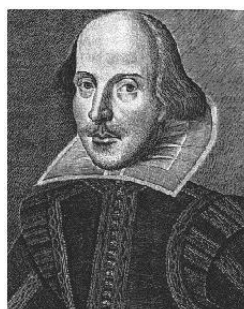
به معنی پنهان گرفته شده است. در استگانوگرافی تلاش می‌شود وجود پیام رمز قابل تشخیص نباشد. در نتیجه با این کار، امکان نفوذ نفوذگران کاهش می‌یابد. [۴ و ۵]

### ۱-۵-۳: تفاوت رمز نگاری و پنهان نگاری

یک تفاوت مهم رمزنگاری و پنهان‌نگاری در آن است که پنهان‌نگاری حتماً به میزبانی یک محیط ثانویه تک رسانه یا چند رسانه انجام پذیر است. وجه برتری ذاتی پنهان‌نگاری 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 پنهان‌نگاری را به عنوان جایگزین برای رمزنگاری تصور کرد. بلکه پنهان‌نگاری مکمل مناسبی برای رمزنگاری به شمار می‌رود. برای بالا بردن ضریب اطمینان، می‌توان از رمزنگاری و پنهان‌نگاری به صورت ترکیبی و هم‌زمان استفاده کرد. شکل ۱-۱ یک تصویر با فرآیند رمزنگاری و شکل ۲-۱ تصویری با فرآیند پنهان‌نگاری را نمایش می‌دهد.



شکل ۱-۱: فرآیند رمزنگاری

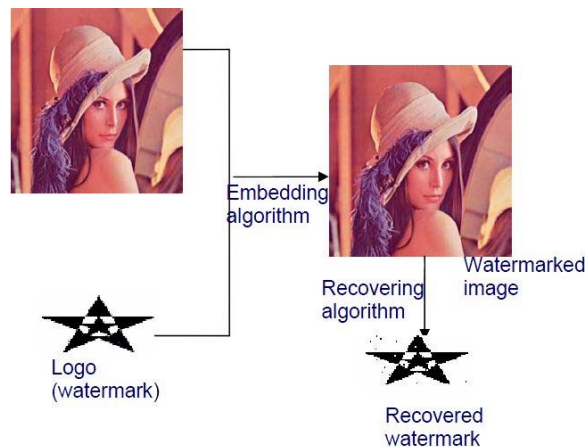


شکل ۲-۱: فرآیند پنهان‌نگاری

همان طور که در شکل ۱-۲ مشاهده می شود از لحاظ ظاهری این دو شکل با هم تفاوتی ندارند. اما در تصویر سمت راست متن هایی مخفی شده است. [۵]

### ۱-۵-۴: واترمارکینگ

واترمارکینگ دیجیتال شاخه ای از فرآیند پنهان نگاری محسوب می شود که برای اولین بار در سال ۱۹۹۶ معرفی شد. واترمارک در صوت، ویدئو و تصویر کاربرد دارد که در این تحقیق، واترمارک های مبتنی بر تصویر مورد نظر هستند. واترمارکینگ به عنوان یک روش در حفاظت از حق کپی و جلوگیری از تکثیر (کپی برداری) غیر قانونی اطلاعات، روش مناسبی محسوب می شود. در شکل ۱-۳ یک فرآیند واترمارکینگ مشاهده می شود.



شکل ۱-۳: فرآیند واترمارکینگ

### ۱-۶: تفاوت های پنهان نگاری و واترمارکینگ

در پنهان نگاری به طور خاص مخفی کردن وجود داده ها و ارسال اطلاعات تحت پوشش یک داده ی دیگر مورد نظر می باشد و هدف اصلی، داده ای است که پنهان شده است و اطلاعات پوششی دارای اهمیت نمی باشد.

برخلاف نهمان‌نگاری، در واترمارکینگ گنجاندن داده به دلیل اهمیت بالای سیگنال میزبان می‌باشد، که با اهداف متفاوتی از پنهان‌نگاری نظیر حفظ حق نشر، درستی و تمامیت داده، ره‌گیری مسیر انتشار و ... انجام می‌شود. در واقع تفاوت اصلی این دو روش در سیگنال دارای ارزش می‌باشد 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 پنهان‌نگاری در می‌یابیم که پنهان‌سازی اطلاعات، قدمتی دیرینه دارد. البته روش‌های پنهان‌نگاری در قدیم، بسیار ابتدایی و متفاوت و گاه عجیب بوده‌اند. در این قسمت مروری بر وقایع برجسته 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 ۶۰ قبل از میلاد، جولوس سزار از نوعی الفبای رمز برای مکاتبات حکومتی استفاده می‌کرد. طبق روایات هرودوت - مورخ یونانی - فرمانروای یونانی به نام هیستیاثوس 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 می‌نوشت 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 ۱۶ 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 بود که از میان آنها می‌توان به کتاب بی‌شاپ ژان ویکینز<sup>۱</sup> اشاره کرد که روش‌هایی را از کد کردن پیغام‌ها در موزیک تا جوهرهای نامرئی پیشنهاد داد. همچنین او اولین طرح‌ها را در رمز گشایی با استفاده از تناوب

---

1. Bishop Gohn Wikins