

بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيمِ



دانشگاه سوادکوه

پردیس دانشگاهی
پایان نامه کارشناسی ارشد

امنیت تصاویر با استفاده از نهان نگاری در تجارت الکترونیک

از:

مرضیه میرزایی دودانگه

استاد راهنما:

دکتر اسداله شاه بهرامی

دکتر منوچهر نحوی

اسفند ۱۳۹۲

پردیس دانشگاهی
فناوری اطلاعات
تجارت الکترونیک

امنیت تصاویر با استفاده از نهان‌نگاری در تجارت الکترونیک

از:

مرضیه میرزایی دودانگه

استادان راهنما:

دکتر اسداله شاه بهرامی

دکتر منوچهر نحوی

اسفند ۱۳۹۲

تقدیم به:

همسر عزیز و صبورم که با بردباری و متانت، همواره حامی و پشتیبان من بوده است.

تقدیم به فرزندانم ، که صبورانه شرایط مرا تحمل کردند.

تشکر و قدردانی:

از اساتید راهنمای زحمتکش و صبورم، دکتر اسداله شاه بهرامی و دکتر
منوچهر نحوی که در طول یکسال گذشته، پاسخگویی بی دریغ، پشتوانه ای ارزنده
و تکیه گاه علمی وزین بودند، بی نهایت سپاسگزارم.
از درگاه ایزد بخشنده، برای آنها آروزی روزهای سرشار از سلامتی و موفقیت به
همراه بهترین ها را دارم.

فهرست مطالب

۱	فصل ۱: معرفی	۱
۲	۱-۱- مقدمه	۱-۱
۳	۲-۱- بیان مساله	۲-۱
۵	۳-۱- روش تحقیق	۳-۱
۵	۴-۱- سازماندهی پایان نامه	۴-۱
۶	فصل ۲: نهان نگاری دیجیتال	۶
۷	۱-۲- مقدمه	۱-۲
۸	۲-۲- تجارت الکترونیک	۲-۲
۱۰	۳-۲- پنهان سازی اطلاعات	۳-۲
۱۰	۴-۲- پنهان نگاری	۴-۲
۱۱	۵-۲- نهان نگاری	۵-۲
۱۲	۱-۵-۲- فاکتورهای اساسی نهان نگاری	۱-۵-۲
۱۲	۲-۵-۲- کاربردهای نهان نگاری	۲-۵-۲
۱۴	۳-۵-۲- طبقه بندی روش های نهان نگاری	۳-۵-۲
۱۴	۱-۳-۵-۲- نوع سند	۱-۳-۵-۲
۱۴	۲-۳-۵-۲- مشاهده پذیر و غیر قابل مشاهده پذیر بودن نهان نگاری	۲-۳-۵-۲
۱۴	۳-۳-۵-۲- مقاومت در برابر حملات	۳-۳-۵-۲
۱۵	۴-۳-۵-۲- استخراج نهان نگاره	۴-۳-۵-۲
۱۶	۵-۳-۵-۲- جاسازی نهان نگاره	۵-۳-۵-۲
۱۶	۱-۵-۳-۵-۲- پردازش های حوزه مکان	۱-۵-۳-۵-۲
۱۷	۲-۵-۳-۵-۲- پردازش های حوزه فرکانس	۲-۵-۳-۵-۲
۱۸	۶-۲- پردازش های حوزه فرکانس: تبدیل DCT	۶-۲
۲۰	۷-۲- پردازش های حوزه فرکانس: تبدیل DWT	۷-۲
۲۲	۱-۷-۲- ویژگی باندها در تبدیل DWT	۱-۷-۲
۲۴	۲-۷-۲- مزایا و معایب تبدیل DWT	۲-۷-۲
۲۵	۸-۲- حملات وارد بر الگوریتم های نهان نگاری	۸-۲
۲۶	۹-۲- معیارهای ارزیابی کیفیت الگوریتم های نهان نگاری دیجیتال	۹-۲
۲۷	۱۰-۲- نتیجه گیری	۱۰-۲
۲۹	فصل ۳: بررسی اجمالی الگوریتم های نهان نگاری	۲۹
۳۰	۱-۳- مقدمه	۱-۳
۳۰	۲-۳- الگوریتم های مطرح در حوزه DCT	۲-۳
۳۰	۱-۲-۳- الگوریتم Cox's	۱-۲-۳
۳۱	۲-۲-۳- الگوریتم Koch's	۲-۲-۳
۳۲	۳-۲-۳- الگوریتم ادریسی	۳-۲-۳
۳۳	۳-۳- الگوریتم های مطرح در حوزه DWT	۳-۳

۳۳	Xie's	الگوریتم	۱-۳-۳
۳۴	Xia's	الگوریتم	۲-۳-۳
۳۵	Wang's	الگوریتم	۳-۳-۳
۳۶	Tsun's	الگوریتم	۴-۳-۳
۳۶	Kim's	الگوریتم	۵-۳-۳
۳۸	Dugad's	الگوریتم	۶-۳-۳
۳۸	Nezhadarya's	الگوریتم	۷-۳-۳
۴۰		الگوریتم اکرمی	۸-۳-۳
۴۰		الگوریتم سهیلی	۹-۳-۳
۴۱		الگوریتم‌های ترکیبی	۴-۳
۴۱		تبدیل آرنولد	۱-۴-۳
۴۲	Fotopoulos	الگوریتم	۲-۴-۳
۴۲	Al-Haj	الگوریتم	۳-۴-۳
۴۳	Amirgholipour	الگوریتم	۴-۴-۳
43	Liu Ping Feng's	الگوریتم	۵-۴-۳
۴۳	Gunjal's	الگوریتم	۶-۴-۳
۴۴		مقایسه‌ی الگوریتم‌های مختلف نهان‌نگاری	۵-۳
۴۷		نتیجه‌گیری	۶-۳
۴۹		فصل ۴ بررسی الگوریتم پیشنهادی	
۵۰		مقدمه	۱-۴
۵۰		مشخصات تصاویر نهان‌نگاره	۲-۴
۵۲		تعداد سطوح تبدیل در DWT	۳-۴
۵۲		الگوریتم پیشنهادی	۴-۴
۵۳		الگوریتم جاسازی نهان‌نگاره	۱-۴-۴
۵۵		الگوریتم استخراج نهان‌نگاره	۲-۴-۴
۵۷		الگوریتم حداکثر نسبت ترکیب	۳-۴-۴
۵۸		بررسی مقاومت الگوریتم نهان‌نگاری پیشنهادی در برابر حملات مختلف	۵-۴
۶۰		مقاومت الگوریتم پیشنهادی در برابر حمله مات کردن	۱-۵-۴
۶۲		مقاومت الگوریتم پیشنهادی در برابر حمله نويز فلفل نمکی	۲-۵-۴
۶۳		مقاومت الگوریتم پیشنهادی در برابر حمله برش	۳-۵-۴
۶۴		مقاومت الگوریتم پیشنهادی در برابر حمله تغییر مقیاس	۴-۵-۴
۶۵		مقاومت الگوریتم پیشنهادی در برابر حمله چرخش	۵-۵-۴
۶۸		مقاومت الگوریتم پیشنهادی در برابر فشرده‌سازی JPEG	۶-۵-۴
۷۰		مقاومت الگوریتم پیشنهادی در برابر حمله‌ی فیلتر میانه	۷-۵-۴
۷۲		استفاده از الگوریتم حداکثر نسبت در نهان‌نگاری چندگانه	۶-۴
۸۲		جمع‌بندی نتایج شبیه‌سازی	۷-۴

۸۴ فصل ۵: جمع‌بندی و پیشنهاداتها
۸۵ ۱-۵ - مقدمه
۸۵ ۲-۵ - جمع‌بندی
۸۶ ۳-۵ - پیشنهادات
۸۷ منابع و مراجع

فهرست جداول

جدول ۲-۱- محدودیت‌های تجارت الکترونیک	۹
جدول ۳-۱- مقایسه الگوریتم‌های مختلف نهان‌نگاری	۴۵
جدول ۴-۱- لیست حملات انجام شده بر روی الگوریتم پیشنهادی	۵۱
جدول ۴-۲- نتایج بدست‌آمده قبل از وقوع حمله با سه سطح تبدیل در متد پیشنهادی.....	۶۰
جدول ۴-۳- نتایج بدست‌آمده قبل از وقوع حمله با دو سطح تبدیل در متد پیشنهادی	۶۰
جدول ۴-۴- نتایج تجربی بدست‌آمده بعد از وقوع حمله مات‌کردن	۶۱
جدول ۴-۵- نتایج تجربی بدست‌آمده بعد از وقوع حمله نويز فلغل نمکی	۶۲
جدول ۴-۶- نتایج تجربی بدست‌آمده بعد از وقوع حمله برش	۶۳
جدول ۴-۷- نتایج تجربی بدست‌آمده بعد از وقوع حمله تغییر مقیاس	۶۴
جدول ۴-۸- نتایج تجربی بدست‌آمده بعد از وقوع حمله فیلتر میانه	۷۱
جدول ۴-۹- نتایج بدست‌آمده قبل از وقوع حمله با جاسازی دو نهان‌نگاره با سه سطح تبدیل در متد پیشنهادی.....	۷۲
جدول ۴-۱۰- نتایج تجربی بدست‌آمده بعد از وقوع حمله مات‌کردن	۷۳
جدول ۴-۱۱- نتایج تجربی بدست‌آمده بعد از وقوع حمله نويز فلغل نمکی	۷۴
جدول ۴-۱۲- نتایج تجربی بدست‌آمده بعد از وقوع حمله برش	۷۵
جدول ۴-۱۳- نتایج تجربی بدست‌آمده بعد از وقوع حمله تغییر مقیاس	۷۶
جدول ۴-۱۴- نتایج تجربی بدست‌آمده بعد از وقوع حمله فیلتر میانه	۸۱

فهرست اشکال

- شکل ۱-۲ - طبقه‌بندی پنهان‌سازی اطلاعات ۱۰
- شکل ۲-۲ - بلوک دیاگرام جاسازی پنهان‌نگاری در حوزه فرکانس ۱۷
- شکل ۳-۲ - بلوک دیاگرام روند تشخیص داده پنهان‌شده ۱۷
- شکل ۴-۲ - مجموعه ضرایب DCT در یک بلوک 4×4 ۱۹
- شکل ۵-۲ - تجزیه زیر باندها با استفاده از DWT دو بعدی با سه سطح تبدیل ۲۱
- شکل ۶-۲ - استاندارد DWT دو بعدی با دو سطح تبدیل ۲۲
- شکل ۷-۲ - (a) یک نمونه تصویر شامل تمام جزئیات، (b) یک مرحله تبدیل ویولت تصویر و ۴ زیرباند ایجاد شده ۲۴
- شکل ۱-۳ - نحوه جاسازی پنهان‌نگاره در الگوریتم Cox ۳۱
- شکل ۲-۳ - روند جاسازی پنهان‌نگاره در الگوریتم ادریسی ۳۳
- شکل ۳-۳ - ساختار درج کردن پنهان‌نگاره ۳۴
- شکل ۴-۳ - درج اطلاعات پنهان‌نگاری در بزرگترین ضرایب موجک سطح دوم تجزیه DWT ۳۵
- شکل ۵-۳ - فلوچارت درج اطلاعات پنهان‌نگاری در الگوریتم Kim ۳۷
- شکل ۶-۳ - تصویرسازی فیلد گرادیان در ۵ سطح، بدست آمده از ۵ سطح تجزیه DWT ۳۹
- شکل ۷-۳ - ساختار الگوریتم Ali Al-Haj ۴۲
- شکل ۱-۴ - (a) تصویر اصلی پنهان‌نگاره؛ (b) نمونه‌ای از تصاویر برای ارزیابی الگوریتم پیشنهادی ۵۱
- شکل ۲-۴ - مجموعه ضرایب انتخاب شده از ۲ سطح تبدیل DWT برای جاسازی پنهان‌نگاره ۵۳
- شکل ۳-۴ - مجموعه ضرایب انتخاب شده از ۳ سطح تبدیل DWT برای جاسازی پنهان‌نگاره ۵۴
- شکل ۴-۴ - محل جاسازی ۴ پنهان‌نگاره در تصویر اصلی. مجموع هر ۴ شکل یکسان، نشان‌دهنده یک پنهان‌نگاره درج شده 32×32 بیتی، در تصویر ۵۵
- شکل ۵-۴ - فرایند جاسازی پنهان‌نگاره در الگوریتم پیشنهادی ۵۵
- شکل ۶-۴ - فرایند استخراج پنهان‌نگاره در الگوریتم پیشنهادی ۵۶
- شکل ۷-۴ - انتخاب یک بیت از چهار بیت، توسط الگوریتم حداکثر نسبت ۵۸
- شکل ۸-۴ - استخراج یک پنهان‌نگاره از بین ۴ پنهان‌نگاره استخراجی با الگوریتم حداکثر نسبت ۵۸
- شکل ۹-۴ - تصاویر پنهان‌نگاری شده توسط الگوریتم پیشنهادی ۵۹

فهرست نمودارها

نمودار ۴-۱-	مقایسه‌ای از تمام زوایای مورد نظر بین سه الگوریتم مطرح بر روی تصویر peppers	۶۶
نمودار ۴-۲-	مقایسه‌ای از تمام زوایای مورد نظر بین سه الگوریتم مطرح بر روی تصویر Baboon	۶۶
نمودار ۴-۳-	مقایسه‌ای از تمام زوایای مورد نظر بین سه الگوریتم مطرح بر روی تصویر Lena	۶۷
نمودار ۴-۴-	مقایسه‌ای از تمام زوایای مورد نظر بین سه الگوریتم مطرح بر روی تصویر Barbara	۶۷
نمودار ۴-۵-	مقایسه‌ی مقاومت الگوریتم پیشنهادی و دو الگوریتم دیگر در برابر حمله فشرده‌سازی JPEG بر روی تصویر peppers	۶۸
نمودار ۴-۶-	مقایسه‌ی مقاومت الگوریتم پیشنهادی و دو الگوریتم دیگر در برابر حمله فشرده‌سازی JPEG بر روی تصویر Baboon	۶۹
نمودار ۴-۷-	مقایسه‌ی مقاومت الگوریتم پیشنهادی و دو الگوریتم دیگر در برابر حمله فشرده‌سازی JPEG بر روی تصویر Lena	۶۹
نمودار ۴-۸-	مقایسه‌ی مقاومت الگوریتم پیشنهادی و دو الگوریتم دیگر در برابر حمله فشرده‌سازی JPEG بر روی تصویر Barbara	۷۰
نمودار ۴-۹-	مقایسه‌ای از تمام زوایای چرخش بین الگوریتم پیشنهادی با جاسازی دو نهان‌نگاره و دو الگوریتم مطرح دیگر بر روی تصویر Barbara	۷۷
نمودار ۴-۱۰-	مقایسه‌ای از تمام زوایای چرخش بین الگوریتم پیشنهادی با جاسازی دو نهان‌نگاره و دو الگوریتم مطرح دیگر بر روی تصویر Baboon	۷۷
نمودار ۴-۱۱-	مقایسه‌ای از تمام زوایای چرخش بین الگوریتم پیشنهادی با جاسازی دو نهان‌نگاره و دو الگوریتم مطرح دیگر بر روی تصویر peppers	۷۸
نمودار ۴-۱۲-	مقایسه‌ای از تمام زوایای چرخش بین الگوریتم پیشنهادی با جاسازی دو نهان‌نگاره و دو الگوریتم مطرح دیگر بر روی تصویر Lena	۷۸
نمودار ۴-۱۳-	مقایسه‌ی مقاومت الگوریتم پیشنهادی با جاسازی دو نهان‌نگاره و دو الگوریتم دیگر در برابر حمله فشرده‌سازی JPEG بر روی تصویر Barbara	۷۹
نمودار ۴-۱۴-	مقایسه‌ی مقاومت الگوریتم پیشنهادی با جاسازی دو نهان‌نگاره و دو الگوریتم دیگر در برابر حمله فشرده‌سازی JPEG بر روی تصویر Baboon	۷۹
نمودار ۴-۱۵-	مقایسه‌ی مقاومت الگوریتم پیشنهادی با جاسازی دو نهان‌نگاره و دو الگوریتم دیگر در برابر حمله فشرده‌سازی JPEG بر روی تصویر peppers	۸۰
نمودار ۴-۱۶-	مقایسه‌ی مقاومت الگوریتم پیشنهادی با جاسازی دو نهان‌نگاره و دو الگوریتم دیگر در برابر حمله فشرده‌سازی JPEG بر روی تصویر Lena	۸۰

امروزه با پیشرفت تکنولوژی و با توجه به گستردگی ارتباطات کامپیوتری و سهولت انتقال و توزیع و پخش اطلاعات دیجیتال و توسعه فن‌آوری اطلاعات و بوجود آمدن شبکه‌های گسترده دیجیتالی مانند اینترنت هر روزه بر تعداد استفاده‌کنندگان از این محصولات دیجیتالی افزوده می‌شود. از جمله محصولات دیجیتال، تصاویر دیجیتال است. استفاده از تصاویر دیجیتال در کاربردهای علمی و تجاری بسیار مرسوم بوده و همچنان رو به افزایش است. از کارهای هنری مشهور، اسناد رسمی و اسناد تجاری گرفته تا چک‌های بانکی و تصاویر پزشکی همگی می‌توانند به صورت دیجیتال مورد استفاده قرار گیرند. امروزه تجارت الکترونیکی از خطرات امنیتی رنج می‌برد، کپی برداری نامحدود از محصولات دیجیتال، به راحتی و بدون افت کیفیت باعث شده تا راهکارهایی برای حفظ محصولات ارائه شود، تا حقوق مادی تولیدکنندگان این محصولات به خطر نیفتد. نهان‌نگاری روشی برای حفاظت از محصولات دیجیتالی است.

نهان‌نگاری فرایند قراردادن الگوهای از پیش تعریف شده در داده‌های چند رسانه‌ای به منظور حفاظت از آنها است. قرار دادن این الگوها باید بگونه‌ای باشد که کاهش کیفیت حداقل بوده و همچنین غیرقابل مشاهده باشد. الگوریتم‌های نهان‌نگاری مختلفی در حوزه‌های مختلف ارائه شده است. روش‌های حوزه مکان، روش‌های حوزه فرکانس و روش‌های ترکیبی از این جمله هستند. به منظور مقاومت بیشتر نهان‌نگاره در برابر حملات عمومی پردازش تصویر، از الگوریتم‌های ترکیبی استفاده می‌شود. در الگوریتم پیشنهادی، از ترکیب DWT و DCT با روش تکرار نهان‌نگاره در زیرباندهای مختلف تصویر استفاده شده است و برای اولین بار از الگوریتم حداکثر نسبت (MRC) برای استخراج نهان‌نگاره استفاده کرده است. این الگوریتم شامل دو مرحله است: در مرحله اول، یک نهان‌نگاره با الگوی تکرار شونده در زیرباندهای مختلف جاسازی می‌شود. در مرحله دوم، نهان‌نگاره از بین نهان‌نگاره‌های جاسازی شده با استفاده از الگوریتم حداکثر نسبت استخراج می‌شود. در این الگوریتم حتی می‌توان بجای استفاده از یک نهان‌نگاره از دو نوع مختلف نهان‌نگاره با خاصیت تکرار در زیرباندهای مختلف استفاده کرد و در هنگام استخراج به راحتی توسط الگوریتم حداکثر نسبت این نهان‌نگاره‌ها را استخراج نمود. هدف از قرار دادن یک نهان‌نگاره به دفعات در زیرباندهای مختلف یک تصویر، افزایش مقاومت است. منطقی که در پشت این ایده نهفته است این است که اگر نهان‌نگاره، در تمامی زیرباندهای فرکانس بالا، پایین و میانی یک تصویر جاسازی شود، باعث مقاومت بیشتر در برابر گروه گسترده‌تری از حملات می‌شود. یکی دیگر از مزایای این روش، استخراج کور نهان‌نگاره از تصویر نهان‌نگاری شده است. به این ترتیب برای استخراج نهان‌نگاره در طول فرایند استخراج، نیاز به تصویر اصلی و مقایسه آن با تصویر نهان‌نگاری شده نیست. این مزیت باعث کاهش بار محاسباتی سیستم نهان‌نگاری می‌شود.

کلید واژه: نهان‌نگاری، الگوریتم حداکثر نسبت، DWT, DCT

فصل اول

معرفی

از ابتدای تاریخ بشریت، انسانها علاقمند بوده‌اند که با برجا گذاشتن نام و نشانی بر روی آثار خود، آفریننده این آثار را مشخص نمایند. شاید مواردی از این علاقه را بتوان بر روی نقاشی‌ها و سفال‌های بجا مانده از دوران باستان پیدا کرد. امروزه نیز با پیشرفت تکنولوژی و با توجه به گستردگی ارتباطات کامپیوتری و سهولت انتقال و توزیع و پخش اطلاعات دیجیتال و توسعه فن‌آوری اطلاعات و بوجود آمدن شبکه‌های گسترده دیجیتالی مانند اینترنت هر روزه بر تعداد استفاده‌کنندگان از این محصولات دیجیتالی افزوده می‌شود. از جمله محصولات دیجیتال، تصاویر دیجیتال هستند. استفاده از تصاویر دیجیتال در کاربردهای علمی و تجاری بسیار مرسوم است و همچنان رو به افزایش است. از کارهای هنری مشهور، اسناد رسمی و اسناد تجاری گرفته تا چک‌های بانکی و تصاویر پزشکی همگی می‌توانند به صورت دیجیتال مورد استفاده قرار گیرند. تجارت الکترونیکی با تمام فوایدی که دارد از خطرات امنیتی رنج می‌برد، کپی‌برداری نامحدود از محصولات دیجیتال، به راحتی و بدون افت کیفیت باعث شده تا راهکارهایی برای حفظ محصولات ارائه شود، تا حقوق مادی تولیدکنندگان این محصولات به خطر نیفتد.

در سالهای اخیر پنهان‌سازی داده^۱ به عنوان ابزاری مناسب جهت حفاظت از داده‌های دیجیتال مورد توجه قرار گرفته است. برای پنهان‌سازی داده روشهای سخت‌افزاری و نرم‌افزاری وجود دارد، اما آنچه در این پایان‌نامه مورد بررسی قرار گرفته است، روشهای نرم‌افزاری پنهان‌سازی داده است. روشهای مختلفی برای پنهان‌سازی داده نرم‌افزاری از قبیل، پنهان‌نگاری^۲، نهان‌نگاری^۳، کانال‌های پوششی^۴، گمنامی^۵ [۳۴] وجود دارد. در این پایان‌نامه به بررسی نهان‌نگاری دیجیتال پرداخته و روش‌های آن بررسی می‌شود.

نهان‌نگاری اطلاعات یکی از روش‌های پنهان‌سازی داده است، که در دهه اخیر به یکی از زمینه‌های تحقیقاتی بسیار مهم در حوزه پردازش تصویر و سیگنال، تبدیل شده است، و مطالعه و پژوهش‌های بسیار زیادی در این زمینه انجام شده است. به طور خلاصه می‌توان گفت، نهان‌نگاری به معنی پنهان کردن یک داده در داخل داده چندرسانه‌ای مانند ویدیو، متن، تصویر، صدا است بطوریکه که با چشم قابل مشاهده نبوده و فقط افرادی که مجاز هستند با انجام یکسری پردازش‌ها قادر به استخراج آن باشند. همچنین داده پنهان‌شده در اثر تکنیک‌های پردازش تصویر از بین نرود [۱۲، ۱۳]. امروزه از نهان‌نگاری دیجیتال به طور گسترده‌ای استفاده می‌شود، یکی از کاربردهای آن در تجارت الکترونیکی است.

¹ Data Hiding

² Steganography

³ Watermarking

⁴ Covert Channels

⁵ Anonymity

تولید کنندگان محصولات چندرسانه‌ای که آثار خود بر روی بستری مانند اینترنت منتشر می‌کنند، تا از طریق این بستر محصولات خود را تبلیغ کرده و به فروش آثار خود اقدام نمایند، باید این اطمینان را داشته باشند که محصولاتشان از تغییر، کپی‌های غیر مجاز مصون می‌ماند و همچنین خریدار نیز باید این اطمینان را داشته باشد که محصولی را که خریداری کرده‌اند محصول اورژینال بوده و دارای کیفیت خوبی است.

پس می‌توان گفت روش‌های نهان‌نگاری باید به طور موثر از فرایندهایی که از کپی‌های غیرمجاز پشتیبانی می‌کنند محافظت شود، این در صورتی امکان دارد که روش‌های نهان‌نگاری خاصی اعمال شود. در حقیقت روش‌هایی که فرایند حفاظت از کپی‌های غیرمجاز را پشتیبانی می‌کنند باید [۱]:

- موثر و کارآمد باشد.
 - طراحی آن باید بگونه‌ای باشد که رسیدگی کاملی به حساب حقوق خریداران و فروشندگان داشته باشد.
 - از مکانیزم‌های مناسب برای حفاظت از حریم خصوصی خریدار در معاملات وب سایت‌ها استفاده کنند.
 - اطلاعات محرمانه را به گونه‌ای در داده‌ها چندرسانه‌ای قرار دهد که امکان سوء استفاده از آن کم باشد. یعنی نتوان به راحتی آن را استخراج کرد، دستکاری و تغییر داد.
 - به خریداران در معاملات اینترنتی، بدون اینکه نیاز به عملیات امنیتی پیچیده‌ای داشته باشند، کمک کنند.
- نهان‌نگاری به عنوان یک راهکار مطرح است، به طوری که تولیدکنندگان این آثار (مانند تصویر) به استناد به این داده نهان-نگاره^۱، می‌توانند آثار خود را حفظ نمایند، و مراجع تصمیم‌گیری و قضایی با استناد به داده نهان‌نگاره می‌توانند مالکیت صاحب اثر را اثبات نمایند. الگوریتم‌های مختلفی برای نهان‌نگاری مطرح شده ولی با توجه به اهمیت موضوع، تحقیقات همچنان ادامه دارد، و تلاش می‌شود الگوریتم‌های کارا تر که در برابر گروه گسترده‌تری از حملات مقاوم هستند، ارایه شود.
- این فصل به این صورت سازماندهی شده است. در بخش ۱-۲ به بیان مساله پرداخته می‌شود. روش تحقیق مساله در بخش ۱-۳ ارائه شده است. مروری کلی بر ساختار پایان نامه در بخش ۱-۴ بیان می‌گردد.

۲-۱ بیان مساله

همان‌طور که عنوان شد یکی از روش‌هایی که برای حفاظت از اطلاعات از جمله تصویر در برابر کپی‌رایت مطرح است، نهان‌نگاری است. برای انجام نهان‌نگاری روش‌های مختلفی در حوزه‌های مختلف وجود دارد، از جمله این روش‌ها: روش‌های حوزه مکان^۲، روش‌های حوزه فرکانس^۳ و روش‌های ترکیبی^۱ است.

¹ Watermark

² Spatial Domain

³ Frequency Domain

الگوریتم‌های مختلفی در حوزه مکان برای نهان‌نگاری ارائه شده است. روش‌های حوزه مکان در مقایسه با دیگر روش‌ها، زمان پیاده‌سازی کوتاه‌تر، سرعت اجرای بیشتر، نیاز سخت‌افزاری کمتری دارند اما در برابر تکنیک‌های پردازش تصویر، بسیار ضعیف عمل می‌کنند، بعنوان مثال یک برش ساده از تصویر ممکن است داده‌ی نهان‌نگاره را از بین ببرد [۱۳، ۲۸]. روش‌های حوزه فرکانس معمولاً پیچیدگی زمانی زیادی دارند، همچنین ظرفیت بیشتری برای جاسازی نهان‌نگاره دارند و در برابر تکنیک‌های پردازش تصویر، مقاوم‌تر عمل می‌کنند. حوزه‌های فرکانسی که امروزه رایج هستند عبارتند از: تبدیل فوریه گسسته (DFT^2)، تبدیل کسینوسی گسسته (DCT^3) و تبدیل موجک گسسته (DWT^4) [۱۳، ۱۲]. اکثر الگوریتم‌هایی که در حوزه فرکانس ارائه شده در حوزه تبدیل DCT و DWT هستند، البته امروزه به‌خاطر رواج استانداردهایی مانند JPEG2000 و MPEG4 تبدیل DWT کاربرد بیشتری دارد و الگوریتم‌های زیادی در این حوزه معرفی شده است. به منظور مقاومت بیشتر نهان‌نگاره در برابر حملات عمومی پردازش تصویر می‌توان از الگوریتم‌های ترکیبی که می‌تواند ترکیبی از تبدیل کسینوسی (DCT) و تبدیل موجک (DWT) باشد، استفاده نمود، در این روش‌ها به منظور بهبود عملکرد روش‌های نهان‌نگاری تصاویر دیجیتال بر مبنای DWT از روش‌های مبتنی بر DCT نیز استفاده می‌گردد. به‌عبارت دیگر از ترکیب DCT و DWT برای نهان‌نگاری تصاویر دیجیتال استفاده می‌گردد. دلیل اصلی استفاده از هر دو روش این است که بدین وسیله می‌توان اشکالات موجود در هر روش را کم‌رنگ‌تر کرد، بطوریکه بتوان روش نهان‌نگاری موثرتری را بدست آورد [۳۱].

همانطور که عنوان شد، الگوریتم‌های مختلفی با استفاده از DCT و DWT و یا ترکیب این دو پیشنهاد شده است و حملات بسیاری روی این الگوریتم‌ها صورت گرفته است. مقاومت در برابر حملات مهم‌ترین ویژگی این الگوریتم‌ها محسوب می‌گردد. پس حمله‌ای موفق است که بتواند نهان‌نگاره را بدون آسیب رساندن به تصویر اصلی، شناسایی، استخراج یا حذف نماید. هدف در این پایان‌نامه ارایه الگوریتمی کارا و مقاوم در حوزه ترکیب می‌باشد که دارای مقاومت بیشتر در برابر گروه گسترده‌تری از حملات پردازش تصویر است. لازم به ذکر است که عدم شفافیت نهان‌نگاره جزو ملزومات محسوب شده و ویژگی مهمی است. برای ارزیابی عدم شفافیت نهان‌نگاره در الگوریتم‌ها از معیار نرخ پیک سیگنال به نویز ($PSNR^5$) استفاده کرده و برای بررسی مقاومت و مقایسه تفاوت نهان‌نگاره اصلی و نهان‌نگاره استخراج شده از معیار میانگین خطای مطلق (MAE^6) استفاده می‌شود.

¹ Hybrid Domain

² Discrete Fourier Transform (DFT)

³ Discrete Cosine Transform (DCT)

⁴ Discrete Wavelet Transform (DWT)

⁵ Peak Signal To Noise Ratio

⁶ Mean Absolute Error

۳-۱ روش تحقیق

همان طور که ذکر شد روش‌های مختلفی برای نهان‌نگاری در حوزه‌های مختلف وجود دارد، که بنا به کاربرد و نوع داده و همچنین نوع پردازش بکار رفته در آن، از این روش‌ها استفاده می‌شود. کارهای انجام شده در این پایان‌نامه شامل مراحل زیر است:

- ۱- بررسی نقش نهان‌نگاری در تجارت الکترونیک و لزوم استفاده آن.
- ۲- بررسی الگوریتم‌های حوزه مکان، حوزه فرکانس و ترکیبی و چند الگوریتم در حوزه DWT, DCT و ترکیبی مورد بررسی قرار می‌گیرد.
- ۳- انواع حملات صورت گرفته در نهان‌نگاری، مانند حملات حذف، حملات هندسی مورد بررسی قرار می‌گیرد.
- ۴- یک الگوریتم نهان‌نگاری ترکیبی پیشنهاد شده است که در حوزه DWT و DCT بوده و یک نهان‌نگاره با الگوی تکرار شونده، در زیرباندهای مختلف جاسازی می‌شود. در این الگوریتم برای استخراج نهان‌نگاره از روش حداکثر نسبت (MRC^1) استفاده شده است. این الگوریتم شامل دو مرحله است: در مرحله اول، چندین نهان‌نگاره یکسان در زیرباندهای مختلف جاسازی می‌شود. در مرحله دو، یک نهان‌نگاره از بین نهان‌نگاره‌های جاسازی شده در زیرباندهای مختلف با استفاده از الگوریتم حداکثر نسبت استخراج می‌شود. برای بررسی کارایی و مقاومت این الگوریتم، از دو الگوریتم مطرح شده ترکیبی استفاده می‌گردد تا مقاومت الگوریتم پیشنهادی در برابر حملات نسبت به دو الگوریتم مشابه در این حوزه مقایسه گردد. نتایج حاصل از پیاده‌سازی این سه الگوریتم که با برنامه MATLAB نوشته شده است، ارائه شده و در نهایت نتایج شبیه‌سازی ارائه می‌گردد.

۴-۱ سازماندهی پایان‌نامه

فصل‌بندی این پایان‌نامه به این شرح است. در فصل دو اطلاعات اصلی در بحث نهان‌نگاری و ملزومات آن مورد بررسی قرار می‌گیرد و همچنین کاربردهای نهان‌نگاری دیجیتال، طبقه‌بندی الگوریتم‌های نهان‌نگاری، با ذکر جزئیات آنها بررسی می‌گردد. حملات وارد بر الگوریتم‌ها مورد بررسی قرار می‌گیرد. در فصل سوم چند الگوریتم مختلف نهان‌نگاری در حوزه DWT, DCT و ترکیبی مورد بحث قرار می‌گیرد. در فصل چهارم یک الگوریتم جدید ترکیبی ارائه می‌گردد و مقاومت این الگوریتم در برابر حملات نسبت به دو الگوریتم مشابه در این حوزه مورد ارزیابی قرار می‌گیرد. در فصل پنجم جمع‌بندی و پیشنهادات بیان می‌گردد.

¹Maximum Ratio Combining (MRC)

فصل دوم

نهان نگاری دیجیتال

نهان‌نگاری دیجیتالی در سال ۱۹۵۴ توسط یکی از مهندسين شرکت موزاک (Muzac) بنام امیل همبروک (Emil Hembrook) ابداع شد. در این ابداع یک کد شناسایی به گونه‌ای غیرقابل تشخیص یا به اصطلاح نامرئی، به فایل حاوی موسیقی دیجیتالی وصل می‌شد تا برای اثبات حق مالکیت به کار برود. از آن زمان به بعد از نهان‌نگاری دیجیتالی استفاده-های فراوانی می‌شد، اما تا سال ۱۹۹۰ به عنوان یک موضوع تحقیقاتی با ارزش، توجه دانشمندان را به خود جلب نکرده بود. از اوایل دهه ۱۹۹۰، این موضوع به عنوان یک موضوع جذاب تحقیقاتی مورد توجه قرار گرفت [۶]، اما نهان‌نگاری تصاویر دیجیتال بطور عمده از حدود سال‌های ۱۹۹۵ و ۱۹۹۶ مورد توجه قرار گرفت [۵] و در طی این مدت الگوریتم‌های فراوانی با کاربردهای متنوع در این زمینه طراحی و منتشر شد.

نهان‌نگاری به دو صورت سخت‌افزاری و نرم‌افزاری قابل پیاده‌سازی است، اما آنچه در این پایان‌نامه مد نظر است، پیاده‌سازی نرم‌افزاری آن است. نهان‌نگاری نرم‌افزاری به معنای پنهان‌سازی داده، در داخل داده‌های چندرسانه‌ای همانند: تصویر، متن، صوت و ویدئو میزبان است، نهان‌نگاری دیجیتالی در تصویر، روشی است که یک قطعه از اطلاعات در تصویر گنجانده می‌شود بطوریکه این داده‌ها غیرقابل رویت باشند و امکان حذف آنها نیز توسط کاربران غیرمجاز وجود نداشته باشد، و در هنگام لزوم استخراج شود. اطلاعاتی که در تصویر گنجانده شده است نهان‌نگاره نام دارد. این اطلاعات می‌تواند شامل اطلاعاتی مرتبط با تصویر یا صاحب تصویر باشد که صاحب حقیقی و حقوقی تصویر است، یا حتی این اطلاعات نامربوط به اثر یا صاحب اثر باشد. در واقع روشهای نهان‌نگاری، تصویر اصلی را به تصویر نهان‌نگاری شده تبدیل می‌کنند. یکی از کاربردهای اصلی نهان‌نگاری کنترل حق تکثیر^۱ و تایید هویت^۲ داده دیجیتالی است [۴، ۵].

در تجارت الکترونیک حفاظت از اطلاعات بسیار حائز اهمیت است، و صاحبان اثر به دنبال شیوه‌هایی برای حفاظت از آثار خود هستند. نهان‌نگاری دیجیتال این امکان را فراهم کرده است که صاحبان آثار دیجیتال با خاطری آسوده اطلاعات خود را در اینترنت منتشر نمایند بدون اینکه نگران این باشند که آثار آنها مورد سوء استفاده قرار گیرد. حال سوال این است که کدام یک از الگوریتم‌های نهان‌نگاری برای این امر مناسب است.

سازماندهی مطالب در این فصل به این شرح است. در بخش ۲-۲ تجارت الکترونیک و اهمیت، مزایا و معایب آن بررسی می‌شود. در بخش ۲-۳، ۲-۴ و ۲-۵ پنهان‌سازی اطلاعات، پنهان‌نگاری و نهان‌نگاری مورد بحث قرار خواهد گرفت. در بخش ۲-۶ و ۲-۷ الگوریتم‌های نهان‌نگاری حوزه فرکانس بررسی می‌شود. در بخش ۲-۸ حملات وارد بر الگوریتم‌های نهان‌نگاری بررسی

¹ Copyright Protection

² Authentication

می‌شود و سرانجام در بخش ۲-۹ معیارهای ارزیابی الگوریتم‌های نهان‌نگاری دیجیتال مورد بحث قرار گرفته و نتیجه‌گیری از مطالب این فصل در بخش ۲-۱۰ آورده شده است.

۲-۲ تجارت الکترونیک

در یک تعریف ساده، تجارت الکترونیکی را می‌توان انجام هرگونه امور تجاری و بازرگانی به صورت روی خط^۱ و از طریق شبکه جهانی اینترنت بیان کرد. این تکنیک در سال‌های اخیر در بستر اینترنت رشد فزاینده‌ای داشته است. این امر می‌تواند شامل خرید و فروش عمده یا خرده‌ی کالاهای فیزیکی و غیر فیزیکی (نظیر اتومبیل و یا نرم‌افزارهای کامپیوتری)، ارائه سرویس‌های مختلف به مشتریان (نظیر مشاوره‌های پزشکی یا حقوقی) و دیگر موارد تجاری (هم چون تبادل کالا به کالا و راه‌اندازی مناقصات و مزایادات) باشند [۲].

هدف از به کارگیری تجارت الکترونیک، گسترش روش‌های قدیمی تجارت نیست، بلکه ارائه روش جدید در انجام امور بازرگانی محسوب می‌شود. به واسطه این روش جدید، فروشندگان قادرند که محصولات و خدمات خود را به شکل تمام وقت به تمام خریداران در سراسر جهان مستقل از مرزهای جغرافیایی و ملیت‌ها عرضه کنند. بسیاری از مردم، تجارت الکترونیک را منحصر به خرید و فروش از طریق شبکه اینترنت می‌دانند، در حالی که این امر فقط بخش کوچکی از تجارت الکترونیک را تشکیل می‌دهد و این مفهوم اکنون گستره وسیعی از جنبه‌های مختلف تجاری و اقتصادی را دربرگرفته است. به سادگی می‌توان هرگونه تراکنش مالی، تجاری بین موسسات و افراد مختلف را در حیطه تجارت الکترونیک گنجانند. بر مبنای تعریفی که کنسرسیوم صنعت Commercenet از تجارت الکترونیک ارائه می‌دهد، این نوع تجارت عبارت است از "استفاده از کامپیوتر-های یک یا چند شبکه برای ایجاد و انتقال اطلاعات تجارت که بیشتر با خرید و فروش اطلاعات، کالا و خدمات از طریق اینترنت مرتبط است." رسالت تجارت الکترونیک فقط ارتباط نیست بلکه پی‌ریزی و تقویت روابط تجاری است. تجارت الکترونیک در حال تغییر روش‌های تجارت خرید و حتی تغییر نحوه تفکر ماست. پس تعریف جامع‌تر از تجارت الکترونیک عبارت است از: "تبادل اطلاعات تجاری و فروش اطلاعات، خدمات و کالا با استفاده از شبکه جهانی اینترنت" [۳].

تجارت الکترونیک دارای مزایای بی‌شماری برای سازمان‌ها، تک تک مشتریان و حتی جامعه است [۲].

- جهانی شدن
- کاهش هزینه‌های تبلیغات برای شرکتها و به دلیل عدم حضور واسطه
- بهبود زنجیره تامین
- سرعت عرضه در بازار

¹ Online