



دانشکده آموزشهای الکترونیکی

پایان نامه کارشناسی ارشد در رشته مهندسی فناوری اطلاعات (تجارت الکترونیکی)

ارائه روشی جهت واترمارک کردن اسناد بر مبنای رمزنگاری تصویری  
به منظور حفظ مالکیت معنوی اسناد تجاری

توسط:

سارا خداعی

استاد راهنما:

جناب آقای دکتر کورش زیارتی

خرداد ماه ۱۳۹۰



به نام خداوند بخشنده مهربان

به نام خدا

### اظہارنامہ

اینجانب سارا خداعی دانشجوی رشته‌ی مهندسی فناوری اطلاعات گرایش تجارت الکترونیکی دانشکده‌ی آموزشهای الکترونیکی اظہارمی کنم که این پایان نامہ حاصل پژوهش خودم بوده و در جاهایی که از منابع دیگران استفاده کرده‌ام، نشانی دقیق و مشخصات کامل آن را نوشته‌ام. همچنین اظہارمی کنم که تحقیق و موضوع پایان نامہ‌ام تکراری نیست و تعهد می‌نمایم که بدون مجوز دانشگاه دستاوردهای آن را منتشر ننموده و یا در اختیار غیر قرار ندهم. کلیه حقوق این اثر مطابق با آیین نامہ مالکیت فکری و معنوی متعلق به دانشگاه شیراز است.

نام و نام خانوادگی: سارا خداعی

تاریخ و امضا: ۹۰/۳/۱۷



به نام خدا

ارائه روشی جهت واترمارک کردن اسناد بر مبنای رمزنگاری تصویری به منظور حفظ مالکیت  
معنوی اسناد تجاری

به کوشش

سارا خداعی

پایان نامه

ارائه شده به تحصیلات تکمیلی دانشگاه شیراز به عنوان بخشی  
از فعالیت‌های تحصیلی لازم برای اخذ درجه کارشناسی ارشد

در رشته‌ی :

مهندسی فناوری اطلاعات (گرایش تجارت الکترونیکی)

از دانشگاه شیراز

شیراز

جمهوری اسلامی ایران

ارزیابی کمیته پایان نامه، بادرجه‌ی: عالی

دکتر کورش زیارتی، استادیار بخش مهندسی و علوم کامپیوتر (رئیس کمیته) . . . . .

دکتر سیده زهره عظیمی فر، استادیار بخش مهندسی و علوم کامپیوتر. . . . .

دکتر فرشاد تاجری پور، استادیار بخش مهندسی و علوم کامپیوتر. . . . .

خرداد ماه ۱۳۹۰

تقدیم به:

مادر فداکار

پدر دلسوز

و همسر عزیزم

که همواره و در همه حال پشتیبان و یار و یاور من بوده‌اند.

## سپاسگزاری

پیش از هر چیز خداوند متعال را به سبب تمام الطاف بیدریغش سپاسگزارم. همچنین از زحمات استاد راهنمای بزرگووارم، جناب آقای دکتر زیارتی که در این راه مرا یاری نمودند قدردانی می‌کنم. و همواره به خاطر می‌سپارم تلاش جناب آقای دکتر رهیده استاد محترم دانشگاه صنعتی شیراز را که بی‌شک در پیشبرد این پایان‌نامه، مرا بسیار یاری نمودند.

## چکیده

# ارائه روشی جهت واترمارک کردن اسناد بر مبنای رمزنگاری تصویری به منظور حفظ مالکیت معنوی اسناد تجاری

به کوشش

سارا خداعی

با آغاز عصر اینترنت، داده‌های زیادی در سیستم‌های شبکه‌ای تبادل شده‌اند. فضای سایبر وجود روش‌های نسخه‌برداری و تکثیر، و در نتیجه نقض حقوق مالکیت فکری را تقویت کرده است. بنابراین، حفاظت از مالکیت صحیح و قانونی اطلاعات به یکی از موارد بسیار مهم در سال‌های اخیر مبدل گشته است. محققان تکنیک‌های زیادی از جمله واترمارک دیجیتالی را برای حفاظت از حقوق معنوی اسناد دیجیتال پیشنهاد کرده‌اند. در این روش واترمارک دیجیتالی در تصویر میزبان به منظور حفاظت از حق تالیف و بررسی صحت پنهان می‌گردد. جهت مشخص نمودن مالکیت حقیقی یک تصویر، واترمارک پنهان شده برای بررسی مالکیت استخراج می‌شود. در این رساله به ارائه روشی برای حفظ حق تالیف اسناد تجاری با استفاده از روش ترکیبی رمزنگاری تصویری و واترمارک دیجیتالی پرداخته می‌شود. رمزنگاری تصویری می‌تواند بدون هیچگونه عملیات رایانه‌ای رمزگشایی گردد، و یک روش کاملاً ایمن و ساده در پیاده سازی می‌باشد. رمزنگارنده برای به اشتراک گذاری یک سند سری بین  $n$  نفر، به هر یک از  $n$  استفاده کننده یک کاغذ شفاف حاوی تصویری خاص می‌دهد، و صرفاً تعداد  $k$  یا بیشتر از  $k$  نفر از آنها می‌توانند تصویر را با روی هم گذاشتن کاغذهای شفاف ببینند. روش رمزنگاری بصری در کنار واترمارک دیجیتالی میزان امنیت اسناد تجاری سری را افزایش می‌دهد و برخی نارسایی‌های روش‌های قبلی تصدیق هویت را برطرف می‌نماید.

کلمات کلیدی: رمزنگاری تصویری، واترمارک دیجیتالی، تبدیل موجک گسسته، تجزیه مقادیر منفرد، طرح رمزنگاری تصویری  $k$  از  $n$ .



## فهرست مطالب

صفحه	عنوان
۲	فصل اول مقدمه
۳	۱.۱ شروع و اوج گرفتن جرایم کامپیوتری
۵	۱.۲ اهمیت امنیت اطلاعات
۶	۱.۳ ایده اصلی تحقیق
۷	۱.۴ نگاهی کلی به فصول رساله
۸	فصل دوم مبانی نظری تحقیق
۹	۲.۱ حق تالیف
۱۰	۲.۲ معرفی رمزنگاری
۱۲	۲.۳ معرفی به اشتراک گذاری راز
۱۳	۲.۴ رمزنگاری تصویری
۱۴	۲.۵ واترمارکینگ دیجیتالی
۱۶	۲.۶ تبدیل موجک
۱۷	۲.۶.۱ تبدیل موجک گسسته (DWT)
۱۹	۲.۶.۲ تبدیل موجک‌ها آر
۲۰	۲.۷ تجزیه مقادیر منفرد
۲۰	۲.۷.۱ فرآیند تجزیه مقادیر منفرد
۲۲	۲.۷.۲ خصوصیات SVD
۲۲	۲.۸ نتیجه
۲۳	فصل سوم پیشینه تحقیق
۲۵	۳.۱ مدل اصلی رمزنگاری تصویری
۲۶	۳.۲ تعریف رمزنگاری تصویری $k$ از $n$
۲۷	۳.۳ راه حل‌های کارآمد برای $k$ و $n$ های کوچک
۳۰	۳.۴ یک طرح عمومی $K$ از $K$
۳۱	۳.۴.۱ ساختار اول

صفحه		عنوان
۳۱	ساختار دوم	۳.۴.۲
۳۲	طرح عمومی $k$ از $n$	۳.۴.۳
۳۳	توسعه	۳.۵
۳۵	نقایص طرح اولیه رمزنگاری بصری	۳.۶
۳۵	دیدگاه ریجمن و پربینیل	۳.۷
۳۶	روش سایه رنگ	۳.۸
۳۹	اصول اساسی رنگ	۳.۹
۴۰	چاپ تصاویر رنگی	۳.۱۰
۴۲	روش اول	۳.۱۰.۱
۴۶	روش دوم	۳.۱۰.۲
۴۹	روش سوم	۳.۱۰.۳
۵۱	روشی برای تولید سهم‌های معنی دار در رمزنگاری تصویری	۳.۱۱
۵۴	تبدیل سایه رنگ رنگی و استخراج پیکسل	۳.۱۱.۱
۵۵	رمزگذاری و رمز گشایی	۳.۱۱.۲
۶۰	پنهان کردن داده در رمزنگاری تصویری با اندازه ثابت تصویر	۳.۱۲
۶۱	VSS متداول	۳.۱۲.۱
۶۲	تصویر $VSS(2,2)$ با اندازه ثابت	۳.۱۲.۲
۶۴	پنهان کردن داده و رمز کردن تصویر محرمانه	۳.۱۲.۳
۶۵	استخراج داده و بازسازی تصویر محرمانه	۳.۱۲.۴
۶۷	رمزنگاری تصویری برای تصاویر خاکستری	۳.۱۳
۶۸	سایر روشها	۳.۱۴
۶۸	رمزنگاری تصویری برای ساختار دسترسی عمومی	۳.۱۴.۱
۶۹	آستانه بازگشتی رمزنگاری تصویری	۳.۱۴.۲
۶۹	رمزنگاری تصویری پیشرو	۳.۱۴.۳
۷۰	رمزنگاری تصویری افزایش منطقه ای	۳.۱۴.۴
۷۰	رمزنگاری تصویری مبتنی بر قطعه	۳.۱۴.۵
۷۱	به اشتراک گذاری چند سند سری	۳.۱۴.۶
۷۲	رمزنگاری بصری رنگی بدون تیرگی رنگ	۳.۱۴.۷
۷۲	رمزنگاری بصری بدون گستردگی پیکسل	۳.۱۴.۸

صفحه	عنوان
۷۲	موارد امنیتی ۳.۱۵
۷۴	تقلب کردن در یک VSC توسط یک MP ۳.۱۵.۱
۷۴	تقلب کردن در VCS توسط یک MO ۳.۱۵.۲
۷۵	تقلب در EVCS با استفاده از MP ۳.۱۵.۳
۷۶	الگوریتم محافظت از تقلب ۳.۱۵.۴
۷۷	واترمارک گذاری دیجیتالی ۳.۱۶
۷۸	واترمارک دیجیتالی و رمزنگاری تصویری ۳.۱۷
۸۲	فصل چهارم واترمارک گذاری دیجیتالی بر مبنای رمزنگاری تصویری
۸۴	واترمارک گذاری دیجیتالی بر مبنای رمزنگاری تصویری ۴.۱
۸۸	طرح رمزنگاری بصری استفاده شده ۴.۲
۹۱	واترمارک گذاری بر مبنای SVD ۴.۳
۹۲	طرح واترمارک گذاری DWT-SVD پیشنهادی ۴.۴
۹۳	معیارهای ارزیابی الگوریتمهای واترمارک گذاری ۴.۴.۱
۱۰۲	نتیجه ۴.۵
۱۰۳	فصل پنجم بررسی و تحلیل یافته‌های تحقیق
۱۰۴	واترمارک گذاری بر مبنای DWT-SVD ۵.۱
۱۰۷	نتایج حاصل از انواع حملات اعمال شده ۵.۲
۱۰۸	حمله هندسی: چیدن (CR) و چرخش (RO) ۵.۲.۱
۱۱۱	حمله‌های نویزی؛ نویز گوسی (GU) ۵.۲.۲
۱۱۲	حملات رفع نویز: فیلتر میانه (AF) ۵.۲.۳
۱۱۴	حملات فشردگی قالب: فشردگی JPEG ۵.۲.۴
	حملات پردازش تصویر: یکسان سازی هسیتوگرام (HE)، یکسان سازی تباین
۱۱۵	(CA) و تصحیح گاما (GC) ۵.۲.۵
۱۲۰	مقایسه با سایر روشها ۵.۳
۱۲۱	نتیجه ۵.۴
۱۲۳	فصل ششم نتیجه گیری و پیشنهادات
۱۲۳	آنالیز روش ۶.۱
۱۲۴	بررسی ضریب همبستگی ۶.۱.۱
۱۲۵	بررسی اوج نسبت سیگنال به نویز ۶.۱.۲

صفحه	عنوان
۱۲۷	۶.۱.۳ معیارهای کیفی روش واترماکگذاری دیجیتالی
۱۲۹	۶.۲ پیشنهادات آینده
۱۳۰	۶.۳ نتیجه
۱۳۲	مراجع
۱۴۳	چکیده به زبان انگلیسی

## فهرست جدول‌ها

صفحه	عنوان و شماره
۵۳	جدول ۱-۳: جدول کدگذاری تصویر محرمانه (SCT) [۱۰]
۵۷	جدول ۲-۳: کدگذاری پوششی CCT [۱۰]
۸۰	جدول ۳-۳: مقایسه بین طرح‌های مختلف رمزنگاری بصری بر مبنای تعداد تصاویر سری، توسعه پیکسل، فرمت تصویر و نوع سهم ساخته شده [۱۰۸]
۹۴	جدول ۱-۴: مقایسه غیر قابل مشاهده بود (PSNR) بین روشهای T&L [۳۵]، E&G [۱۱۰]، و روش استفاده شده در طرح پیشنهادی [۱۱۳]
۹۵	جدول ۲-۴: مقایسه استحکام بین روشهای [۳۵]، [۱۱۰]، و روش استفاده شد پیشنهادی [۱۱۳]
۱۰۶	جدول ۱-۵: مقایسه بین مقدار عامل مقیاس و اوج نسبت سیگنال به نویز
۱۰۶	جدول ۲-۵: مقادیر ضریب همبستگی پیرسون واترمارک خارج شده از حملات مختلف [۱۱۳]
۱۰۹	جدول ۳-۵: نتایج حاصل از حمله چیدن بر روش استفاده شده
۱۱۰	جدول ۴-۵: نتایج حاصل از حمله چرخش
۱۱۲	جدول ۵-۵: نتایج حاصل از حمله نویز گوسی
۱۱۳	جدول ۶-۵: نتایج حاصل از حمله فیلتر میانه
۱۱۵	جدول ۷-۵: نتایج حاصل از حمله فشردگی JPEG
۱۱۶	جدول ۸-۵: نتایج حاصل از یکسان سازی هیستوگرام تصویر
۱۱۸	جدول ۹-۵: نتایج حاصل از یکسان سازی تباین تصویر
۱۱۹	جدول ۱۰-۵: نتایج حاصل از تصحیح گاما تصویر
۱۲۱	جدول ۱۱-۵: مقایسه PSNR بین روش پیشنهادی و سایر روشهای ترکیبی رمزنگاری تصویری و واترمارک گذاری دیجیتالی

## فهرست شکلها

صفحه	عنوان و شماره
۳	شکل ۱-۱: تعداد کاربران اینترنت بر اساس آمار بانک جهانی [۳]
۴	شکل ۱-۲: درصد هزینه‌های IT مصرف شده در بخش امنیت اطلاعات آمریکادر سالهای ۲۰۰۶ تا ۲۰۰۸ [۴]
۵	شکل ۱-۳: میانگین هزینه‌های مصرف شده در واکنش به جرائم کامپیوتری به ازای هر شرکت کننده در پژوهش [۴]
۶	شکل ۱-۴: میزان استفاده از تکنولوژی‌های امنیتی مختلف تا سال ۲۰۰۸ در آمریکا [۴]
۱۱	شکل ۲-۱: نمایش ساده رمزنگاری
۱۴	شکل ۲-۲: جدول طراحی شده توسط Naor و Shamir [۱۱۸]
۱۸	شکل ۲-۳: تصویر اصلی با استفاده از تبدیل موجک مقیاس ۲ به ۷ زیرباند تقسیم شده است [۱۵۳]
۲۰	شکل ۲-۴: الف) عملیات سطری تبدیل موجک گسسته‌ها آر دوبعدی؛ ب) عملیات ستونی از تبدیل موجک گسسته‌ها آر دوبعدی [۱۱۷]
۲۰	شکل ۲-۵: نمایش عاملگیری A به $USV^T$ [۸۷]
۲۸	شکل ۳-۱: نحوه قرارگیری زیرپیکسلها به ازای هر پیکسل در سهم‌های مسئله [۵] $VCS(2,2)$
۳۰	شکل ۳-۲: ماتریس‌های زیرپیکسل‌های بکار رفته در طرح [۵] $VCS(4,4)$
۳۴	شکل ۳-۳: توسعه طرح رمزنگاری بصری به سطح خاکستری [۵]
۳۴	شکل ۳-۴: در $VCS(2,2)$ ردیف بالا برای پیکسل سفید ردیف پایین برای پیکسل سیاه استفاده میشود [۵]
۳۷	شکل ۳-۵: الف) رنگ پیوسته؛ ب) سایه رنگ [۹۹]
۳۷	شکل ۳-۶: الف) رنگ پیوسته؛ ب) سایه رنگ [۹۹]
۳۸	شکل ۳-۷: طرح تقسیم و برهم نهی پیکسل‌های سفید و سیاه
۳۸	شکل ۳-۸: ساخت و برهم‌نهی رمزنگاری بصری سطح خاکستری. الف) سهم ۱؛ ب) سهم ۲؛ پ) سهم ۱+ سهم ۲ [۹۹]
۳۹	شکل ۳-۹: الف) مدل افزایشی؛ ب) مدل کاهششی [۹۹]
۴۱	شکل ۳-۱۰: چاپ تصاویر رنگی [۹۹]
۴۳	شکل ۳-۱۱: طرح اول از رمزنگاری رنگی [۹۹]
۴۵	شکل ۳-۱۲: چهار سهم تقسیم شده مجزا و نتیجه برهم نهی آنها. الف) سهم ۱ (آبی سایان)؛ ب) سهم ۲ (قرمز مگنت)؛ پ) سهم ۳ (زرد)؛ ت) ماسک؛ ث) تصویر حاصل از برهم‌نهی [۹۹]

- شکل ۱۳-۳: طرح دوم از رمزنگاری تصویری رنگی [۹۹] ۴۷
- شکل ۱۴-۳: دو سهم شفاف و نتیجه حاصل از برهم نهی آنها: الف) سهم ۱؛ ب) سهم ۲؛ پ) تصویر برهم نهی. [۹۹] ۴۸
- شکل ۱۵-۳: تجزیه و بازسازی پیکسل رنگی [۹۹] ۵۰
- شکل ۱۶-۳: دوسهم شفاف و تاثیر برهم نهی آنها الف) سهم ۱؛ ب) سهم ۲؛ پ) تصویر برهم نهی شده [۹۹] ۵۱
- شکل ۱۷-۳: مرحله رمزگذاری در رمزنگاری تصویری با تصاویر با معنی [۱۰] ۵۲
- شکل ۱۸-۳: مرحله رمزگشایی در رمزنگاری تصویری با تصاویر با معنی [۱۰] ۵۳
- شکل ۱۹-۳: تجزیه تصویر رنگی در روش سایه رنگ [۱۰] ۵۴
- شکل ۲۰-۳: تصویر سایه رنگ رنگی [۱۰] ۵۵
- شکل ۲۱-۳: تصویر استخراج شده از روش سایه رنگ رنگی [۱۰] ۵۵
- شکل ۲۲-۳: توسعه پیکسل در رمزنگاری تصویری [۱۰] ۵۶
- شکل ۲۳-۳: تقسیم بلوک در رمزنگاری تصویری سایه رنگ رنگی [۱۰] ۵۶
- شکل ۲۴-۳: یک مثال از تولید سهمها [۱۰] ۵۸
- شکل ۲۵-۳: یک مثال از برهم نهی سهمهای ۱ و ۲ در سایه رنگ رنگی [۱۰] ۵۸
- شکل ۲۶-۳: تصاویر پوششی و تصویر محرمانه استفاده شده در روش رمزنگاری تصویری رنگی با تصاویر با معنی [۱۰] . ۵۹
- شکل ۲۷-۳: سهمهای تولید شده در رمزنگاری تصویری با تصاویر با معنی [۱۰] ۵۹
- شکل ۲۸-۳: تصویر حاصل از برهم نهی در رمزنگاری تصویری با سهمهای معنی دار [۱۰] ۶۰
- شکل ۲۹-۳: لغت رمز در VSS (۲,۲) متداول [۱۰۸] ۶۱
- شکل ۳۰-۳: مثال VSS (۲,۲) متداول؛ الف) تصویر محرمانه؛ ب) سهم ۱؛ پ) سهم ۲؛ ت) نتیجه برهم نهی سهمها [۶] ۶۲
- شکل ۳۱-۳: لغت رمز VSS (۲,۲) اندازه تصویر ثابت [۱۰۸] ۶۳
- شکل ۳۲-۳: روش رمزگذاری و رمزگشایی VSS (۲,۲) با اندازه تصویر ثابت [۱۰۸] ۶۳
- شکل ۳۳-۳: مثال روش VSS با اندازه تصویر ثابت. الف) تصویر محرمانه؛ ب) شفافیت T<sub>۱</sub>؛ پ) شفافیت T<sub>۲</sub>؛ ت) نتیجه برهم نهی T<sub>۱</sub>, T<sub>۲</sub> [۱۰۸] ۶۴
- شکل ۳۴-۳: پنهان کردن داده و قاعده کلی رمزنگاری با اندازه تصویر ثابت [۱۰۸] ۶۴
- شکل ۳۵-۳: نتایج آزمایش برای طرح پیشنهادی. الف) تصویر محرمانه؛ ب) واترمارک اصلی؛ پ) سهم T<sub>۱</sub>؛ ت) سهم T<sub>۲</sub>؛ ث) نتایج برهم نهی سهمها؛ ج) تصویر محرمانه بازسازی شده؛ چ) واترمارک استخراج شده [۱۰۸] ۶۶
- شکل ۳۶-۳: مراحل تقلب در رمزنگاری بصری [۱۱۵] ۷۳

- شکل ۳-۳۷: تقلب در یک رمزنگاری بصری با روش MP [۱۱۵] ۷۴
- شکل ۳-۳۸: تقلب در رمزنگاری بصری با روش MO [۱۱۵] ۷۵
- شکل ۳-۳۹: تقلب در EVCS با استفاده از MP [۱۱۵] ۷۵
- شکل ۴-۱: طرح واترمارک گذاری دیجیتالی بر مبنای رمزنگاری تصویری ۸۵
- شکل ۴-۲: انتخاب زیرپیکسلها در رمزنگاری تصویری (۲و۲؛ الف) پیکسل اصلی؛ (ب) زیرپیکسلهای تولید شده؛ (پ) نتیجه برهم نهی زیرپیکسلها ۸۹
- شکل ۴-۳: الگوریتم مرحله رمزگذاری در رمزنگاری بصری (۲،۲) ۹۰
- شکل ۴-۴: الگوریتم مرحله رمزگشایی در رمزنگاری بصری (۲،۲) ۹۰
- شکل ۴-۵: (الف) تصویر اصلی، (ب) سهم یک؛ (پ) سهم دو؛ (ت) برهم نهی سهم یک و دو ۹۱
- شکل ۴-۶: واترمارک خارج شده بدست آمده از طریق روشهای [۱۱۰]، [۳۵]، و روش استفاده شده [۱۱۳] پس از اعمال حملات متفاوت CR(الف-پ)، RO(ت-ج)، GN(چ-خ)، AF(د-ر)، JPEG(ز-س) HE(ش-ض)، CA(ط-ع)، GC(غ-ض) [۱۱۳] ۹۵
- شکل ۴-۷: نمودار مراحل پنهان سازی واترمارک ۹۸
- شکل ۴-۸: الگوریتم پنهان سازی واترمارک ۹۹
- شکل ۴-۹: نمودار مراحل خارج سازی واترمارک ۱۰۰
- شکل ۴-۱۰: الگوریتم خارج سازی واترمارک ۱۰۱
- شکل ۴-۱۱: (الف) تصویر اصلی؛ (ب) تصویر واترمارک؛ (پ) تصویر واترمارک شده؛ (ت) واترمارک خارج شده ۱۰۲
- شکل ۵-۱: (الف) تصویر پوششی؛ (ب) واترمارک؛ (پ) تصویر واترمارک شده [۳۶] ۱۰۶
- شکل ۵-۲: نمونه ای از حمله چیدن؛ (الف) ۲۵ درصد بالای تصویر (مناطق روشن)؛ (ب) ۲۵ درصد پایین تصویر (مناطق تیره تر) ۱۰۹
- شکل ۵-۳: نمونه ای از حمله چرخش با زاویه ۴۵ درجه . ۱۱۱
- شکل ۵-۴: (الف) تصویر اصلی؛ (ب) تصویر نویزی با میزان واریانس نویز ۱۰۰؛ ۱۱۲
- شکل ۵-۵: اعمال عملیات فیلتر میانه بر تصویر به میزان ۱۰۰٪؛ ۱۱۴
- شکل ۵-۶: تصویر قبل و پس از فشردگی JPEG ۱۱۵
- شکل ۵-۷: یکسان سازی هیستوگرام تصویر الف به میزان ۱۰۰ در روشن کردن مناطق تیره؛ (ب) به میزان ۲۰۰ در تیره کردن مناطق روشن ۱۱۷
- شکل ۵-۸: یکسان سازی تباین تصویر به میزان ۷۰- ۱۱۹
- شکل ۵-۹: تصحیح گاما تصویر با اندازه ۱۲۰



صفحه نشانه‌های اختصاری

DWT= Discrete Wavelet Transform	تبدیل موجک گسسته
DWT-SVD= Discret Wavelet Transform-Singular Value Decomposition	الگوریتم تبدیل موجک گسسته و تجزیه مقادیر منفرد
PSNR= Peak Signal to Noise Ratio	پیک نسبت سیگنال به نویز
SVD= Singular Value Decomposition	تجزیه مقادیر منفرد
VCS(k,n) = Visual Cryptography Schema (k,n)	طرح رمزنگاری تصویری/بصری/مصور k از n

# فصل اول

## مقدمه

## مقدمه

به نظر میرسد اخلاق حرفه ای و تجاری در سالهای اخیر، زمانیکه بر مبادلات چندملیتی و محلهای دادرسی و دادگاهی اعمال می‌شود، به موضوعی سیال و متغیر مبدل گشته است. همانگونه که در گذشته‌ی غرب گاهی قانون‌های رسمی به منظور توسعه در بخش‌های مختلف زیر پا گذاشته می‌شد، امروزه نیز شاهد موارد مشابهی هستیم که اندیشه بارز نمودن خود را در دنیای جدید کسب و کار الکترونیکی دارد. به نظر میرسد توجه به ظرافت‌های اخلاقی به واسطه مسائل فرعی در حال از بین رفتن است. در حالیکه اینترنت دیگر یک موجود تازه متولد شده نیست، اما همچنان صنعتی است که دوران کودکی خود را پشت سر میگذارد و مانند هر کودکی، اولین قدمهای آن آزمایشی و نامطمئن می‌باشد. اشتباهات رخ می‌دهد، سقوطها بسیار است و به نظر میرسد جهان بی‌مرز و بسیار گسترده شده است. کمپانی‌هایی که در این تکنولوژی جدید بوجود می‌آیند بر روی فرصتها و توانایی‌ها تمرکز می‌کنند؛ به ناچار آنها نسبت به کسب و کارهای شهرت یافته، با ظرائف حقوقی و اخلاقی مورد توجه قرار میگیرند. با این وجود تصمیماتی که آنها میگیرند و فعالیتهایی که انجام می‌دهند تاثیر شگرفی بر دنیای اطراف آنها دارد.

علاوه بر این، مهمترین و قیمتی‌ترین حقوق دارایی با در نظر گرفتن اینترنت، دارایی‌های فکری<sup>۱</sup> است: نشان تجاری<sup>۲</sup>، حق تالیف<sup>۳</sup> و حق اختراع<sup>۴</sup>. دولتها مدتهاست که این حقوق را شناخته اند. قانون مالکیت معنوی<sup>۵</sup> در بسیاری از کشورها تصویب شده است. بسیاری از کشورها معاهده‌ی حق مالکیت بین المللی را امضا نموده اند [۱]. آنهایی که در قلمرو حقوقی این معاهده به کسب و کار می‌پردازند می‌دانند که باید به این قانون پایبند بوده یا و هزینه‌های ناشی از آن را پرداخت نمایند.

---

<sup>1</sup> Intellectual Property

<sup>2</sup> Trade Mark

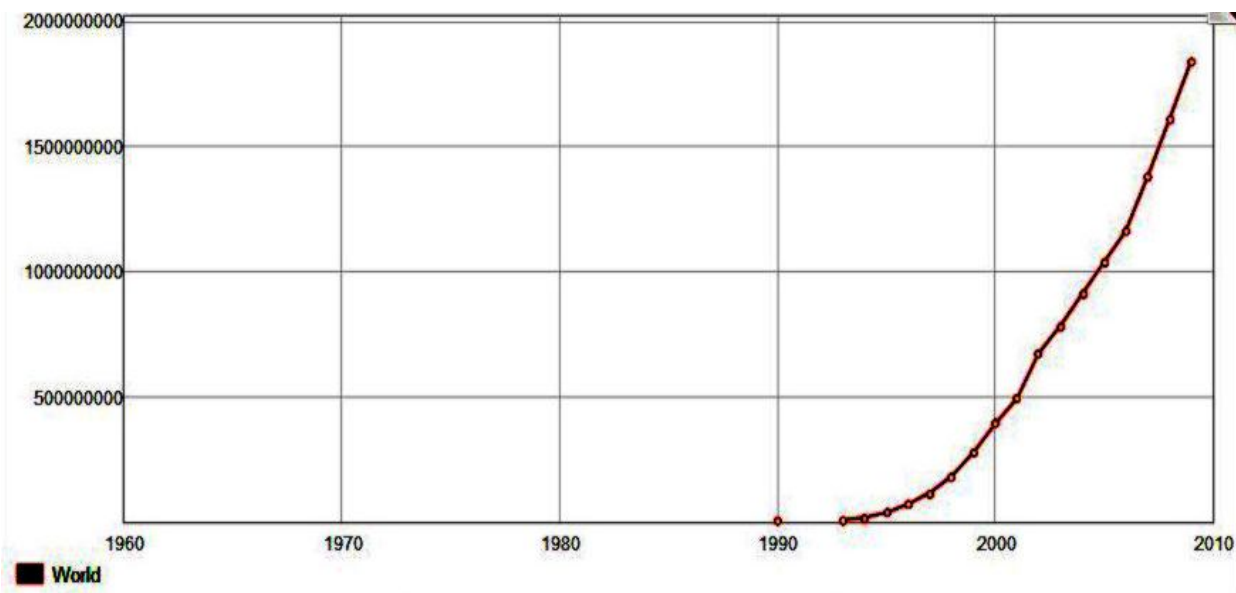
<sup>3</sup> Copyright

<sup>4</sup> Patent

<sup>5</sup> intellectual property right

## ۱.۱ شروع و اوج گرفتن جرایم کامپیوتری

در طول سه دهه گذشته سیستم‌های کامپیوتری از حالت سیستم‌های منفرد وایزوله main frame به شبکه‌های پیچیده ارتباطی و باز تغییر کردند. نتیجه یکپارچگی سیستم‌های محاسباتی و شبکه‌ها، باعث انقلاب ارتباطی شد که تمامی جنبه‌های زندگی انسانها را تحت تأثیر قرارداد. اینترنت یک شبه جهان گستر با دسترسی آزاد و احتمالاً برجسته‌ترین جنبه این انقلاب می‌باشد که توانست امکان ارتباط موثر و ارزان مردم سراسر جهان را با همدیگر، برقرار سازد. همچنین باعث ایجاد فرصت‌های جدید برای اشخاصی و گروه‌های مختلف از جمله دولتمردان، تجار، سازمانها، و موسسات آموزشی گردید. تحقیقات اخیر نشان می‌دهد، تعداد کاربران اینترنت شبکه جهان گستر از ۱۶ میلیون نفر در پایان سال ۱۹۹۵ به حدود دو میلیارد نفر در سال ۲۰۱۰ رسیده است [۳]. شکل ۱-۱ این آمار را به صورت نموداری نشان می‌دهد.



شکل ۱-۱: تعداد کاربران اینترنت بر اساس آمار بانک جهانی [۳]

با افزایش میزان وابستگی به کامپیوتر در تمام سطوح زندگی انسانها، اطلاعات حساس بیشتری با استفاده از کامپیوتر و شبکه‌های کامپیوتری به صورت روزانه ذخیره و ارسال می‌گردد. این انقلاب، در عین حال تهدیدها و جرایم کامپیوتری جدیدی که شامل افزایش شمار حمله‌های کامپیوتری و شکستن حریم است به