دانشگاه صنعتی شیراز

دانشکده مهندسی برق و الکترونیک

پایان‌نامه کارشناسی‌ارشد مهندسی مخابرات-گرایش سیستم

نهان‌نگاری بدون اتلاف و نیمه‌شکننده‌ی تصاویر دیجیتال

بوسیله‌ی:

مینا باقری

استاد راهنما:

دکتر حبیب‌اله دانیالی

استاد مشاور:

دکتر محمّدصادق هل‌فروش

بهمن 1390

بسم الله الرحمن الرحيم

تقدیم به

پدر و مادر عزیزم به پاس زحمات بی دریغشان

سپاس‌گزاری

سپاس خدای را که هر چه هست از اوست و مرا یاری نمود تا قسمتی از عمر خود را در راه تحصیل علم و دانش سپری نمایم.

و با سپاس از استاد گرانقدر،جناب آقای دکتر حبیب‌اله دانیالی،که همواره راهنما و مشوق اینجانب در اتمام این پایان‌نامه بوده اند

و

با قدردانی از استاد مشاور جناب آقای دکتر هل‌فروش و سایر اساتید محترم گروه مخابرات

چکیده

نهان‌نگاری بدون اتلاف و نیمه‌شکننده‌ی تصاویر دیجیتال

با پیشرفت سریع تکنولوژی دیجیتال و استفاده‌ی گسترده از اینترنت، نهان‌نگاری دیجیتال به عنوان ابزار قدرتمندی در زمینه‌ی محافظت داده مورد استفاده قرار گرفته است. یک دسته‌ی مهم از روش‌های نهان‌نگاری که به نام نهان‌نگاری بدون اتلاف و نیمه‌شکننده شناخته می-شوند،برای رفع مشکل شکنندگی در الگوریتم‌های نهان‌نگاری بدون اتلاف مطرح شده‌اند.

هدف اصلی این پایان‌نامه ارائه‌ی الگوریتم‌هایی نیمه‌شکننده برای نهان‌نگاری بدون اتلاف به منظور بهبود نتایج وگسترش کاربرد نهان‌نگاری بدون اتلاف در زمینه‌ی سندیت تصویر است. بر این اساس سه الگوریتم نهان‌نگاری بدون اتلاف و نیمه‌شکننده پیشنهاد شده است. الگوریتم پیشنهادی اول، یک الگوریتم نهان‌نگاری تهی بر اساس ضرایب ویولت وماشین بردار پشتیبان است.در الگوریتم پیشنهادی دوم، نهان‌نگاری تهی به کمک ضرایب تجزیه‌ی مقادیر تکین در حوزه‌ی ویولت انجام شده است. و الگوریتم پیشنهادی سوم، نهان‌نگاری بر اساس انتخاب دو ناحیه‌ی مطلوب و غیرمطلوب از تصویر است. نهان‌نگاره ابتدا از ناحیه‌ی مطلوب تولید شده و سپس با روشی مقاوم و بدون‌اتلاف در ناحیه‌ی غیرمطلوب درج می‌شود.نتایج آزمایش‌ها نشان می‌دهد هر سه الگوریتم در عدم حضورحملات، بدون اتلاف هستند، یعنی قادر به استخراج دقیق نهان‌نگاره و بازیابی کامل تصویر میزبان هستند. در صورت وجود حملات محدود مانند فشرده‌سازی با ضریب کیفیت بالا نیز، استخراج صحیح نهان‌نگاره امکان‌پذیر است. هم‌چنین این الگوریتم‌ها شرایط بسیار مطلوبی برای بررسی سندیت تصاویر به خصوص برای کاربردهای پزشکی فراهم آورده‌اند.

کلمات کلیدی: نهان‌نگاری بدون‌اتلاف، نهان‌نگاری بدون‌اتلاف نیمه‌شکننده، نهان‌نگاری تهی، ناحیه مطلوب وغیرمطلوب، سندیت

فهرست مطالب

عنوان صفحه

فصل اول : مقدمه 1
1-1-زمینه و انگیزه پایان نامه 1
1-2-اهداف و اهمیت پایان نامه 2
1-3-ساختار پایان نامه 5
فصل دوم : نهان نگاری دیجیتال 6
2-1-مقدمه 6
2-2-معرفی نهان نگاری دیجیتال 6
2-3-موارد کاربرد نهان نگاری 9
2-3-1-شناسایی صاحب اثر 10
2-3-2-اثبات مالکیت 10
2-3-3-سندیت محتوا 11
2-3-4-پیگیری مسیر انتقال 12
2-3-5-دیده بانی پخش برنامه ها 12
2-3-6-کنترل نسخه برداری و دستگاه 13
2-4-خصوصیات سیستم های نهان نگاری دیجیتال 14
2-4-1-وفاداری به تصویر اصلی 14
2-4-2-ظرفیت 15
2-4-3-مقاومت، شکنندگی و نیمه شکنندگی 15
2-4-4-آشکارسازی کور یا غیرکور 17

2-4-5-امنیت 17
2-4-6-نرخ خطا 18
2-4-7-کلیدهای نهان نگاره 18
2-4-8-نهان نگاره ی چندگانه 19
2-5-نهان نگاری بدون اتلاف (برگشت پذیر) 20
2-6-نهان نگاری تهی 23
2-7-جمع بندی 25
فصل سوم : مروری بر روش های نهان نگاری بدون اتلاف و نیمه شکننده 26
3-1-مقدمه 26
3-2-هدف وضرورت روش های نهان نگاری بدون اتلاف نیمه شکننده 26
3-3-دسته بندی روش های نهان نگاری بدون اتلاف نیمه شکننده 28
3-3-1-روش های مبتنی بر جایگذاری نهان نگاره 28
3-3-2-روش های مبتنی بر نهان نگاری تهی 43
3-4-چالش های مطرح در نهان نگاری بدون اتلاف و نیمه شکننده 55
3-5-جمع بندی 57
فصل چهارم :الگوریتم های پیشنهادی 59
4-1-مقدمه 59
4-2-الگوریتم پیشنهادی اول: نهان نگاری تهی و نیمه شکننده بر اساس ضرایب ویولت و ماشین بردار پشتیبان 59
4-2-1-ماشین بردار پشتیبان (SVM) 61
4-2-2-استخراج ویژگی 64
4-2-3-آموزش SVM 65
4-2-4-استخراج نهان نگاره 67
4-2-5-نتایج پیاده سازی 67
4-2-6-نتیجه گیری 72

4-3-الگوریتم پیشنهادی دوم: نهان نگاری تهی و نیمه شکننده بر اساس تبدیل SVD در حوزه تبدیل ویولت.....73
4-3-1-تجزیه مقادیر منفرد (SVD).....74
4-3-2-فرآیند تولید نهان نگاره.....75
4-3-3-فرآیند استخراج نهان نگاره.....77
4-3-4-نتایج پیاده سازی.....77
4-3-5-نتیجه گیری.....85
4-4-الگوریتم پیشنهادی سوم: نهان نگاری تهی و نیمه شکننده بر اساس ROI و NROI.86
4-4-1-تولید نهان نگاره از ROI در فرستنده.....89
4-4-2-جایگذاری نهان نگاره در NROI در فرستنده.....89
4-4-3-استخراج نهان نگاره از ROI و NROI در گیرنده.....91
4-4-4-بازیابی تصویر اصلی.....92
4-4-5-نتایج پیاده سازی.....93
4-4-6-نتیجه گیری.....105
4-5-جمع بندی.....106
فصل پنجم : جمع بندی و پیشنهاد برای کارهای آینده.....109
فهرست منابع.....111

فهرست جداول

جدول3- 1- نتایج حاصل از الگوریتم [22] 31
جدول3- 2- PSNR، ظرفیت و سایز تصاویر شکل 3-3 32
جدول3- 3- نتایج کیفیت تصویر نهان نگاری شده و ظرفیت نهان نگاری الگوریتم [24] 40
جدول3- 4- میزان PSNR برای شش تصویر نهان نگاری شده بوسیله ی الگوریتم [25] 42
جدول3- 5- حملات استفاده شده برای الگوریتم [26] 45
جدول3- 6- نتایج آزمایش مقاومت الگوریتم [28] 49
جدول3- 7- بررسی نرخ NC دربرابر افزایش شدت فشرده سازی 51
جدول3- 8-PSNR برای تصویر نهان نگاری شده و نهان نگاره ی استخراجی در عدم حضور حملات 53

جدول4- 1-مقایسه الگوریتم پیشنهادی و الگوریتم Kim [24] 69
جدول4- 2-نرخ خطای بیتی برای تصاویر تست تحت فشرده سازی JPEG با QF 100% تا 50% بدست آمده در الگوریتم پیشنهادی دوم 78
جدول4- 3- میزان BCR برای ضرایب مختلف انتخابی SVD برای تصویر Lena 80
جدول4- 4-نتایج برای تصویر Lena نهان نگاری شده با ROI اندازه نصف کل تصویر و تحت حمله ی فشرده سازی JPEG 95
جدول4- 5-BER برای تصویر نهان نگاری شده با ROI سه چهارم کل تصویر وضرایب مختلف SVD، تحت حمله ی فشرده سازی 97
جدول4- 6- بررسی تأثیر ضرایب SVD مختلف بر میزان عدد نسبت (نسبت تعداد نهان نگاره های یک به تعداد کل بیت های نهان نگاره) 102

فهرست شکل‌ها

شکل2- 1-شمای کلی یک سیستم نهان نگاری عمومی..... 7
شکل2- 2-طبقه بندی روش های نهان نگاری برگشت پذیر بر مبنای مقاومت..... 21
شکل3- 1-الگوی استفاده شده در [22و23] برای محاسبه پارامتر α..... 29
شکل3- 2-بلوک دیاگرام مراحل جای گذاری نهان نگاره در الگوریتم [22]..... 30
شکل3- 3-تصاویر اصلی و تصاویر نهان نگاری شده در الگوریتم [22]..... 33
شکل3- 4-هیستوگرام α،هیستوگرام α بعد از ایجاد فواصل خالی و هیستوگرام α پس از جایگذاری نهان نگاره در تصویر Lena برای الگوریتم [23]..... 34
شکل3- 5-نمودار نرخ بیت خطا (BER) در برابر افزایش ضریب کیفیت فشرده سازی JPEG برای تصاویر تست a تا h..... 35
شکل3- 6-نمودار تغییرات PSNR در برابر افزایش سطوح جایگذاری..... 36
شکل3- 7-فلوچارت الگوریتم نهان نگاری ارائه شده در [24]..... 37
شکل3- 8-توزیع مقادیر اختلاف مرکز ثقل ها الف: بلوک 8×8 وب: بلوک 16×16..... 38
شکل3- 9-الف: نهان نگاری بیت یک و ب: نهان نگاری بیت صفر در الگوریتم [24]..... 39
شکل3- 10-نمودار نرخ بیت صحیح در برابر حملات مختلف برای الگوریتم [26]..... 44
شکل3- 11-نمودار نرخ تشابه در حضور الف: نویز، ب: فشرده سازی و ج: فیلترینگ برای الگوریتم [27]..... 46
شکل3- 12-الگوی نگاشت ضرایب و یولت برای الگوریتم [28]..... 47
شکل3- 13-تصویر تحت حمله و نهان نگاره ی استخراجی برای حملات: الف-فشرده سازی با ضریب کیفیت 20%، ب: قطع و ج: چرخش..... 50
شکل3- 14-دیاگرام شبکه عصبی استفاده شده در [30]..... 52

شکل4-1-بلوک دیاگرام الگوریتم نهان نگاری پیشنهادی بر اساس تبدیل ویولت و SVM..... 60
شکل4- 2-ابرسطح با حداکثر مرزِ جداکننده به همراه مرزهای جداکننده برای کلاس بندی نمونه داده های مربوط به دو کلاس متفاوت..... 61
شکل4- 3-نحوه ساخت ابرسطح جداکننده بین دو کلاس داده در فضای دو بعدی..... 62
شکل4-4-استخراج ویژگی در حوزه تبدیل ویولت..... 65

شکل4- 5-انتساب نهان نگاره به ماتریس ویژگی استخراج شده از تصویر میزبان 66
شکل4- 6-ارزیابی مقاومت الگوریتم پیشنهادی اول، استخراج نهان نگاره از تصاویر تست..... 68
شکل4- 7-مقایسه ی تغییرات BCR در مقابل حمله ی فشرده سازی برای الگوریتم پیشنهادی با الگوریتم [24]..... 69
شکل4- 8-نتایج تأثیر اندازه ی بلوک ماتریس ویژگی بر نهان نگاره ی استخراجی 70
شکل4- 9-مقایسه ی الگوریتم پیشنهادی و الگوریتم [26]..... 71
شکل4- 10-فرآیند تولید نهان نگاره 75
شکل4- 11-نمودار BCR بدست آمده در فشرده سازی JPEG با QF های مختلف برای تصاویر تست..... 79
شکل4- 12-نمودار BCR برای ضرایب مختلف SVD از بلوکهای 8×8..... 81
شکل4- 13-نمودار BCR برای ضرایب مختلف SVD - الف: ضرایب 2 تا 5 از بلوکهای 8×8 در مقایسه با متوسط آن ها و ب: ضرایب 2 تا 12 از بلوک های 16×16 در مقایسه با متوسط آن ها..... 82
شکل4- 14- نمودار مقایسه مقادیر BCR برای الگوریتم پیشنهادی و الگوریتم[26] برای تصویر Lena 83
شکل4- 15-الف:تصویر Lena مخدوش شده، ب: تصویر Lena فشرده شده با QF= %98، ج: محل وقوع خطا آشکار شده برای الف ود: محل وقوع خطاآشکار شده برای ب 84
شکل4- 16-مقایسه ی الگوریتم پیشنهادی اول ودوم..... 85
شکل4- 17-فلوچارت درج و استخراج نهان نگاره برای الگوریتم پیشنهادی سوم..... 88
شکل4- 18-ROI برای تصویر Lena با سایز نصف کل تصویر 93
شکل4- 19-نمودار BER برای تصویر Lena نهان نگاری شده با ROI اندازه نصف کل تصویر و تحت حمله ی فشرده سازی JPEG..... 95
شکل4-20-ROI برای تصویر Lena با اندازه ی سه چهارم کل تصویر 97
شکل4-21-BER برای تصویر نهان نگاری شده Lena با اندازه ی ROI سه چهارم کل تصویر و ضرایب مختلف SVD، تحت حمله ی فشرده سازیJPEG..... 98
شکل4- 22-تصاویر تست برای بررسی تأثیر ضرایب SVD بر میزان BER برای الگوریتم پیشنهادی..... 99
شکل4-23- تأثیر ضرایب مختلف SVD بر میزان BER..... 101
شکل4-24-تأثیر ضرایب وزن دار k_1 و k_2 بر میزان BER برای تصویر Lena و تحت حمله ی فشرده سازی..... 103
شکل4- 25- تصاویر پزشکی استفاده شده و ROI در آنها برای بررسی نتایج الگوریتم پیشنهادی سوم..... 104

شکل4- 26-تأثیر ضریب وزن دار k_2 بر میزان BER برای تصاویر پزشکی و حمله ی فشرده سازی JPEG 104

فهرست علائم اختصاری

BCR	Bit Correct Rate
BER	Bit Error Rate
bpp	bit per pixel
DCT	Discrete Cosine Transform
DWT	Digital Wavelet Transform
HVS	Human Vision System
IDWT	Integer Digital Wavelet Transform
NC	Normalized Correlation
NROI	Non Region of Interest
PSNR	Peak Signal to Noise Ratio
QF	Quality Factor
ROI	Region of Interest
SVD	Singular Value Decomposition
SVM	Support Vector Machine

فصل اول : مقدمه

1-1- زمینه و انگیزه پایان‌نامه

در دهه‌های اخیر ذخیره‌ی اطلاعات و داده‌ها مانند انواع اسناد و مدارک، تصاویر، ویدئوها وآهنگ‌ها به قالب دیجیتال بسیار رایج شده است. برای بسیاری افراد انتقال فایل‌های دیجیتال از طریق اینترنت یک امر روزمره محسوب می‌شود. با پیشرفت سریع تکنولوژی دیجیتال و استفاده گسترده از اینترنت زندگی روز به روز آسان‌تر شده است، اما همراه با این سهولت، مشکلاتی جدی نیز به وجود آمده است. همان‌طور که می‌دانیم با توجه به ماهیت داده‌ی دیجیتال، ساختن نسخه‌های بدون اتلاف از نسخه اصلی با محدودیت خاصی مواجه نیست. سهولت و کیفیت بالا در نسخه‌برداری رسانه‌ی دیجیتال نسبت به آنچه که برای داده آنالوگ امکان‌پذیر بود، صاحبان صنایع را نگران نسخه‌برداری‌های غیرمجاز کرده است. علاوه بر این با گسترش استفاده از اینترنت، داده راحت‌تر و بیشتر از گذشته از طریق اینترنت انتقال می‌یابد و انتقالات حساس داده در اینترنت به‌راحتی به‌وسیله هکرهای ناشناس مختل می‌شود. بنابراین نهان‌نگاری و رمزنگاری داده معمولاً برای محافظت از اطلاعات و جلوگیری از بازیابی آن‌ها در طی انتقال از یک کانال غیرامن مورد استفاده قرار می‌گیرد. رمزنگاری یک روش رایج برای محافظت از فاش شدن اطلاعات مهم است، اما از آنجایی که در رمزنگاری با یک‌بار دی‌کد شدن داده، امکان محافظت از آن بطور کامل از بین می‌رود، رمزنگاری بطور کامل پاسخگوی نیاز مبحث محافظت از اطلاعات نیست. نهان‌نگاری با خصوصیات ویژه مربوط به خود، راه‌حلی مناسب برای این مشکل فراهم کرده‌است[1-3].

نهان‌نگاری جایگذاری یک سیگنال پیام[1] در یک سیگنال میزبان[2]می‌باشد، به‌نحوی که تنها جایگذاری‌کننده و افراد ذیصلاح توانایی استخراج آن را داشته باشند. به سیگنال پیام نهان‌نگاره گفته می‌شود و پس از انجام چنین عملیاتی سیگنال میزبان، سیگنال نهان‌نگاری شده خواهد بود.امروزه با توجه به ضرورت موجود برای فعالیت در زمینه‌ی محافظت از حق چاپ، اثبات

[1] Message
[2] Host

مالکیت و تشخیص دستخوردگی برای داده‌ی دیجیتال، نهان‌نگاری بسیار رواج پیدا کرده است[4].

در یک سیستم نهان‌نگاری تصاویر دیجیتال، نهان‌نگاره می‌تواند دربردارنده اطلاعاتی در مورد تصویر، شامل عنوان تصویر، محل تصویربرداری و یا امضای صاحب اثر باشد. در حالی‌که جایگذاری نهان‌نگاره ارزش عملی تصویر را افزایش می‌دهد، بطور اجتناب ناپذیری در کیفیت بصری تصویر اعوجاج ایجاد می‌کند. برای ما مطلوب‌تر است که تا حد امکان این اعوجاج کمتر باشد، اما سایر نیازمندی‌ها از جمله مقاومت و ظرفیت نهان‌نگاری در تعارض با این مسئله است. در حالی‌که مدل‌های سیستم بصری انسان (HVS[1]) برای بررسی اثرات ناشی از جایگذاری نهان‌نگاره در تصویر مورد استفاده قرار می‌گیرند تا از عدم درک اعوجاج ایجاد شده توسط سیستم بینایی انسان مطمئن شوند، کاربردهایی وجود دارند که در آن‌ها هیچ گونه اعوجاجی در تصویر بازیابی‌شده نسبت به تصویر اصلی قابل قبول نیست. در این حالت می‌باید پروسه استخراج نهان‌نگاره و بازیابی تصویر اصلی بدون هیچ خطایی صورت گیرد. مثال رایج این مورد، تصاویر پزشکی است که در آن‌ها حتی تغییرات کوچک به‌دلایل قانونی مورد قبول نیست. مثال دیگر ملاحظات قانونی و آنالیز تصاویر نظامی در شرایط ویژه‌ای است که در آن شرایط وجود اعوجاج غیرقابل پذیرش است. نهان‌نگاری بدون اتلاف داده به‌عنوان روشی مناسب برای نهان-نگاری داده برای مشتریانی است که هیچ‌گونه افت کیفیتی را در برابر نهان‌نگاری نمی‌پذیرند. در این روش‌ها داده‌ی نهان‌نگاری‌شده پس از استخراج نهان‌نگاره بدون هیچ تغییری به همان حالت اصلی داده‌ی میزبان بازگردانده می‌شود [5-7].

در حالی‌که نیاز به نهان‌نگاری بدون اتلاف در موارد فوق احساس می‌شود، کاربردهایی مانند حفظ حق چاپ برای صاحبان اثر وجود دارند که در آن‌ها نیازمند به روش‌های نهان‌نگاری مقاوم هستیم. در روش‌های نهان‌نگاری مقاوم با توجه به تکنینک به‌کار گرفته شده برای جایگذاری نهان‌نگاره در سیگنال میزبان، حتی در صورت عدم حضور حملات، بازیابی تصویر اصلی از تصویر نهان‌نگاری شده در گیرنده امکان‌پذیر نخواهد بود. در چنین حالتی به نظر می-رسد که داشتن امکان حفظ حق چاپ در مواردی که نیازمند نهان‌نگاری بدون اتلاف هستیم، مسئله‌ای چالش برانگیز است.

2-1- اهداف و اهمیت پایان‌نامه

روش‌های نهان‌نگاری بدون اتلاف (برگشت‌پذیر) بسیاری در گذشته به‌عنوان تکنیک‌های رایج و قدرتمند برای محافظت از حق‌چاپ رسانه‌های حساس مورد مطالعه قرار گرفته‌اند. اما این

[1]Human vision system

روش‌ها در محیط‌های با اتلاف برای انتقال پیام نهان‌نگاری شده به‌شدت شکننده هستند و در نتیجه برای کاربردهای دنیای واقعی مقاوم نیستند[12]. به بیان دیگر یک تغییر کوچک در داده‌ی نهان‌نگاری شده مانند فشرده‌سازی، امکان بازیابی صحیح نهان‌نگاره را غیرممکن می‌کند. این مسئله‌ی اساسی اخیراً با روش‌های جدید نهان‌نگاری بدون‌اتلاف، مرسوم به نهان‌نگاری بدون‌اتلاف نیمه‌شکننده مرتفع شده است که برای کاربردهای محافظت از حق‌چاپ و سندیت قانونی محتوا بیشتر مورد توجه قرار گرفته‌اند.

وظایف کلیدی تمام الگوریتم‌های بدون‌اتلاف نیمه‌شکننده طراحی الگوریتمی برای نهان-نگاری بدون‌اتلاف است که مسئله برگشت‌پذیری را در حالتی که داده‌ی نهان‌نگاری شده دستخوش هیچ تغییری نمی‌شود، برآورده کند و علاوه بر این چگونگی ساخت یا انتخاب ویژگی‌هایی بدون‌تغییر در برابر حملات، برای داشتن مکانیزمی مقاوم را تأمین کند. هدف اصلی روش‌های بدون اتلاف نیمه‌شکننده حساس بودن در برابر حملاتی است که محتوای داده‌ی اصلی را تغییر می‌دهند (مانند برش یا تغییر سایز تصویر) و در مقابل مقاومت در برابر حملات غیرعمد و غیرقابل اجتناب (مانند فشرده‌سازی محدود JPEG) است. در دنیای واقعی تصاویر در فرآیند انتقال حداقل از پردازش‌های غیرعمد که سعی در تخریب محتوا ندارند، مصون نیستند و همین امر روش‌های نهان‌نگاری برگشت‌پذیر نیمه‌شکننده را بسیار کاربردی‌تر از روش‌های شکننده کرده‌است [13]. به‌عنوان مثال در کاربردهای نهان‌نگاری بدون‌اتلاف برای تصاویر پزشکی، وجود حملات خفیف و محدودی مانند فشرده‌سازی با ضریب کیفیت بالا نیز منجر به از دست رفتن نهان‌نگاره می‌شود به‌طوری‌که در اغلب موارد استخراج حتی یک بیت از نهان-نگاره با اطمینان صورت نخواهد گرفت. با کمک روش‌هایی موسوم به نهان‌نگاری بدون اتلاف نیمه‌شکننده این امکان فراهم می‌شود که نهان‌نگاره در برابر چنین حملات محدودی مقاوم شده و حتی در کاربردهایی مانند تصاویر پزشکی که مصون از وجود حملات غیرقابل اجتنابی مانند فشرده‌سازی نیستد، نهان‌نگاره به درستی قابل استخراج باشد.

الگوریتم‌های نهان‌نگاری بدون‌اتلاف نیمه‌شکننده (مقاوم) موجود به دو دسته کلی تقسیم می‌شوند. در دسته اول نهان‌نگاره در فرستنده در داده‌ی میزبان جایگذاری شده و سپس در گیرنده، نهان‌نگاره استخراج و داده‌ی اصلی بازیابی می‌شود. در واقع این دسته از روش‌ها وابسته به جایگذاری و استخراج نهان‌نگاره هستند. دسته دوم از روش‌ها که با عنوان روش‌های نهان-نگاری تهی شناخته می‌شوند، نهان‌نگاره را در داده‌ی میزبان جایگذاری نمی‌کنند، بلکه ویژگی-های اساسی از داده میزبان استخراج کرده و آن‌ها را به نحو مناسبی به نهان‌نگاره منتسب می-کنند.

در روش‌های نهان‌نگاری که نهان‌نگاره با تغییر داده‌ی اصلی جایگذاری می‌شود، (مانند روش‌های مبتنی برتغییر کم ارزش‌ترین بیت)، اگر تعداد زیادی از ضرایب متناظر تصویر در حوزه فرکانس و یا پیکسل‌های تصویر تغییر کنند، غیرقابل مشاهده بودن عملیات نهان‌نگاری

میسر نمی‌شود و چنانچه تعداد این ضرایب تغییر یافته کم باشد، مقاومت روش مختل می‌شود. اما از آنجایی که روش‌های نهان‌نگاری تهی، نهان‌نگاره را با استفاده از ویژگی‌های داده‌ی میزبان می‌سازند و محتوای داده‌ی اصلی را تغییر نمی‌دهند، پاسخگوی تعارض ذاتی میان مقاومت الگوریتم نهان‌نگاری و کیفیت داده‌ی نهان‌نگاری‌شده هستند. روش‌های موجود نهان‌نگاری تهی اگرچه بدون اتلاف هستند، اغلب کاملاً مقاوم و یا کاملاً شکننده هستند و در هر زمنیه با توجه به نیاز مقاومت و یا نیاز شکنندگی به تولید نهان‌نگاره پرداخته‌اند، اما توجه به خصوصیت نیمه-شکنندگی در روش‌های نهان‌نگاری تهی مورد بررسی قرار نگرفته است.در واقع ما به الگوریتمی برای نهان‌نگاری تصاویر دیجیتال نیاز داریم که علاوه بر تهی بودن توانایی شناخت شدت حملات وارده را نیز داشته باشد. به بیان دیگر الگوریتم قادر باشد با توجه به نهان‌نگاره‌ی استخراجی حمله خفیف و شدید را تشخیص دهد. در این حالت می‌باید نهان‌نگاره تولید شده از تصویر اصلی این خصوصیت را داشته باشد که چنانچه حملات وارد شده به تصویر محدود و غیر قابل اجتناب هستند، نهان‌نگاره در گیرنده بدون خطا و یا تقریباً بدون خطا استخراج شود و سندیت تصویر دریافتی محرز شود و چنانچه حملات شدت یافته و سعی در مخدوش کردن محتوای تصویر اصلی داشته باشند، خطای موجود در استخراج نهان‌نگاره از تصویر دریافتی در گیرنده نسبت به حالت قبل به طرز معناداری افزایش یابد و بدین‌وسیله سندیت تصویر دریافتی تایید نگردد. در این پایان‌نامه سعی شده است که به این نیاز، که نهان‌نگاری بدون اتلاف نیمه-شکننده تصاویر دیجیتیال به کمک الگوریتم‌های نهان‌نگاری تهی است، پاسخ داده شود.

در الگوریتم‌هایی که در این پایان‌نامه پیشنهاد شده چند مسئله مورد بررسی قرار گرفته است:

1- از آنجایی که الگوریتم‌های نهان‌نگاری تهی با توجه به نیاز شرح داده شده، نسبت به روش‌هایی که با جایگذاری نهان‌نگاره در تصویر میزبان سروکار دارند، مناسب‌تر بوده و کیفیت تصویر را به هیچ‌عنوان مختل نمی‌کنند، الگوریتم‌های پیشنهادی همگی از دسته روش‌های نهان‌نگاری تهی هستند.
2- در الگوریتم‌های پیشنهادی مسئله‌ی اصلی انتخاب ویژگی‌هایی است که به خوبی پاسخگوی نیاز نیمه‌شکنندگی باشند. این ویژگی‌ها از تصویر میزبان استخراج شده و به نهان‌نگاره منتسب می‌شوند. بنابراین می‌باید به‌گونه‌ای طراحی شوند که در برابر حملات خفیف و محدود مقاوم و در برابر حملات شدیدتر شکننده باشند.
3- مسئله‌ی مهم دیگر که در الگوریتم‌های پیشنهادی مورد توجه قرار می‌گیرد، امکان بررسی سندیت تصویر دریافتی در گیرنده است. این الگوریتم‌ها می‌باید به صورتی طراحی شوند که با توجه به میزان خطا در نهان‌نگاره‌ی استخراجی امکان بررسی سندیت تصویر نیز وجود داشته باشد.

4- اگرچه در تمامی الگوریتم‌های نهان‌نگاری تهی وجود حجم سربار داده علاوه بر داده‌ی نهان‌نگاری شده مسئله‌ای غیرقابل اجتناب است، اما در این الگوریتم‌ها به میزان داده‌ی سربار ناشی از نهان‌نگاری تهی تصویر نیز توجه می‌شود و سعی بر آن است تا از حجم آن تا حد امکان کاسته شده و یا به کلی رفع شود.

3-1- ساختار پایان‌نامه

باقیمانده این پایان‌نامه بصورت زیر سازماندهی شده است. در فصل دوم به بیان مقدمات لازم در زمینه‌ی نهان‌نگاری دیجیتال، بیان خصوصیات سیستم‌های نهان‌نگاری، موارد کاربرد آن، نهان-نگاری بدون اتلاف و بدون اتلاف نیمه شکننده و نهایتاً نهان‌نگاری تهی پرداخته خواهد شد.

در فصل سوم مروری بر روش‌های نهان‌نگاری بدون اتلاف نیمه شکننده خواهیم داشت. این روش‌ها در دو گروه مجزا مورد بررسی قرار می‌گیرند و در هر دسته چند مورد از تکنیک‌های شاخص موجود با ذکر جزئیات شرح داده می‌شوند.

در فصل چهارم به شرح الگوریتم‌های پیشنهادی برای نهان‌نگاری بدون اتلاف نیمه‌شکننده خواهیم پرداخت. این الگوریتم‌ها بر اساس نهان‌نگاری تهی و تبدیل ویولت و ماشین بردار پشتیبان (SVM[1])، نهان‌نگاری تهی بر اساس ضرایب تجزیه مقادیر منفرد (SVD[2]) و نهان-نگاری تهی بر اساس ROI[3] (ناحیه‌ی مطلوب) و NROI[4] (ناحیه‌ی غیرمطلوب) هستند. برای هر کدام از این روش‌ها مراحل الگوریتم گام به گام و با ذکر جزئیات توضیح داده شده و نتایج شبیه‌سازی و مقایسه نتایج با سایر روش‌های مشابه موجود ارائه شده است.

نهایتاً فصل پنجم به نتیجه‌گیری و ارائه‌ی پیشنهاداتی برای ادامه کار اختصاص یافته است.

[1] Support vector machine
[2] Singular value decomposition
[3] Region of interest
[4] Non region of interest