Presenting a New Method of Image Steganalysis Based on MLP Neural Network

S. Talati, R. Esfahani*

Abstract

The ever-increasing development of telecommunications has made secure transmission one of the most important issues today. Since there is a high hiding capacity in the image, the use of image encryption is much more common than other methods of encryption. This article uses the covert imaging technique with the wavelet transform method, and the results show that this method has high resistance. For the analysis of hidden images, an algorithmic wavelet transform method using matrix features (GLCM) and co-occurrence vectors (DCL) is presented. After checking these values in the original and cover images, the different features between these images are extracted and used to train the multilayer neural network (MLP). The classification stage has been performed using the layers of this neural network and the proposed algorithm has been tested for a database of 200 standard images (Casia-Iris). The detection accuracy of 90% of the hidden images in the proposed method shows the superiority of this hidden mining method over other methods.

Key Words: *Steganography, Steganalysis, Wavelet Transform, Co-occurrence Matrix, MLP Neural Network*

*Assistant Professor, Faculty of Computer and Commounication Engineering Department, Imam Hossein University, Tehran,Iran (resfahani@ihu.ac) - Writer-in-Charge

نشریه علمی پدافند غیرعامل

سال چهاردهم، شماره ۴، زمستان ۱۴۰۲، (پیاپی ۵۶): صص ۳۲-۲۱

علمی - پژوهشی

ارائه مدل جدید نهان‌کاوی هوشمند تصویر مبتنی‌بر شبکه‌عصبی MLP

سعید طلعتی[۱]، رضا اصفهانی[۲*]

تاریخ دریافت: ۱۴۰۲/۰۱/۱۱

تاریخ پذیرش: ۱۴۰۲/۰۴/۰۶

چکیده

پیشرفت روزافزون مخابرات، انتقال امن را به یکی از مهم‌ترین مسائل امروزه تبدیل کرده است. از آنجا که در تصویر ظرفیت پنهان شدن بالایی وجود دارد استفاده از پنهان‌نگاری تصویر نسبت به سایر روش‌های پنهان‌نگاری بسیار مرسوم‌تر است. در این مقاله از روش پنهان‌نگاری به روش تبدیل موجک استفاده‌شده که نتایج نشان می‌دهد این روش از مقاومت بالایی بهره می‌برد. و برای تحلیل تصاویر پنهان‌شده به روش تبدیل موجک الگوریتمی با استفاده از ویژگی‌های ماتریس (GLCM) و بردارهای هم‌رخدادی (DCL) ارائه‌شده است. پس از بررسی این مقادیر در تصاویر اصلی و کاور، ویژگی‌های متفاوت بین این تصاویر استخراج و برای آموزش شبکه عصبی چندلایه (MLP) استفاده می‌شوند. مرحله طبقه‌بندی با استفاده از لایه‌های این شبکه عصبی انجام‌شده و الگوریتم پیشنهادی برای پایگاه داده ۲۰۰ تصویر استاندارد (Casia-Iris) تست‌شده است. دقت آشکارسازی ٪۹۰ تصاویر پنهان‌شده‌در روش پیشنهادی برتری این روش نهان‌کاوی در برابر سایر روش‌ها را نشان می‌دهد.

کلیدواژه‌ها: پنهان‌نگاری، نهان‌کاوی، تبدیل موجک، ماتریس هم‌رخدادی، شبکه عصبی MLP

[۱] دانشجوی دکتری دانشگاه علوم و فنون هوایی شهید ستاری، تهران، ایران

[۲] استادیار دانشگاه جامع امام حسین(ع)، تهران، ایران(resfahani@ihu.ac.ir)- نویسنده مسئول

۱- مقدمه

پنهان‌نگاری[1] هنر و علم ارتباط پنهانی است که هدف آن پنهان کردن ارتباط به‌وسیله قرار دادن پیام در یک پوشانه (رسانه‌ای که این قابلیت را دارد تا اطلاعاتی را در آن پنهان کنیم مانند تصویر، صوت یا هر دیتای ممکن) است به‌گونه‌ای که کمترین تغییر قابل‌کشف را در آن ایجاد نماید و نتوان موجودیت پیام پنهان در رسانه را حتی به‌صورت احتمالی آشکار ساخت[۱]. در پنهان‌نگاری هدف مخفی کردن هرگونه نشانه‌ای از وجود پیام است[۲]. درواقع برتری پنهان‌نگاری در این است که می‌توان پیغامی را فرستاد بدون این‌که کسی بفهمد پیغامی فرستاده‌شده است[۳]. به علت آن‌که درک تصویری انسان از تغییرات در تصاویر محدود است، تصاویر یکی از مهم‌ترین رسانه‌های مورداستفاده در پنهان‌نگاری، به‌خصوص در اینترنت است الگوریتم‌های پنهان‌نگاری متعددی در حوزه‌های مکان و فرکانس برای ساختارهای مختلف تصاویر ارائه‌شده است. یکی از مهم‌ترین و متداول‌ترین روش‌های پنهان‌نگاری در تصاویر در حوزه مکان روش بیت کم‌ارزش و در حوزه فرکانس روش تبدیل موجک[2] است[۴].

در کنار گسترش روش‌های مختلف پنهان‌نگاری اطلاعات در تصاویر، روش‌های متنوعی نیز برای مقابله با آن تحت عنوان نهان‌کاوی ایجادشده است که هدف آن استفاده از ویژگی‌های تصاویر و الگوریتم‌های پردازشی برای کشف اطلاعات پنهان‌شده است. توانایی کشف پیام در تصویر تحت تأثیر فاکتورهای مختلفی قرار دارد که ازجمله می‌توان به طول پیام پنهان‌شده، درصد پنهان‌سازی اطلاعات، نوع پوشانه (صوت، تصویر و متن)، فرمت پوشانه انتخابی، روش جاسازی متن موردنظر در پوشانه اشاره کرد[۵]. طی سال‌های گذشته، هم‌زمان با پیشرفت روش‌های هوشمند، شاهد به‌کارگیری این روش‌ها در زمینه‌های مختلف هستیم. در همین رابطه روش‌هایی مانند: هوشمند بیزین[3]، منطق فازی[4]، شبکه عصبی[5] و الگوریتم ژنتیک[6] در تحلیل پنهان‌نگاری کاربرد دارند.

در ادامه ابتدا مشخصه‌های یک سیستم پنهان‌نگاری بیان می‌شود و پس از آن معیارهای متداول ارزیابی پنهان‌نگاری بررسی می‌شود سس پنهان‌نگاری با روش پیشنهادی تبدیل موجک تشریح شده و مزایا این روش شرح داد می‌شود. پس از آن نهان‌کاوی توضیح داده‌شده و به استخراج ویژگی‌های تصویر پرداخته می‌شود و در انتها تحلیل با استفاده از روش پیشنهادی شبکه عصبی چندلایه MLP ارائه و با سایر روش‌های پیشنهادی مقایسه و مزیت آن بیان خواهد شد.

[1] Steganography
[2] Wavelet transform
[3] Bayesian
[4] Fuzzy logic
[5] Neural Network(NN)
[6] Genetic algorithm

۲- مشخصه‌های یک سیستم پنهان‌نگاری

سه عامل مهم در پنهان‌نگاری که همیشه یک مصالحه[7] بین آن‌ها وجود دارد، عبارت‌اند از ظرفیت، مقاومت و شفافیت. بهینه‌سازی پارامترهای متقابل رقابتی است و به‌وضوح نمی‌تواند در یک‌زمان انجام شود.

۲-۱- شفافیت

پنهان‌پذیری[8] یا ادراک‌ناپذیری[9] با توجه به سیستم ادراکی[10] (شنیداری و دیداری) انسان مطرح می‌شود و عبارت است از میزان مصون ماندن از تغییری که در اثر درج اطلاعات در رسانه‌ی میزبان ازنظر ادراکی رخ می‌دهد [۶].

۲-۲- مقاومت

مقاومت یا پایداری[11] در برابر حملات عمدی و غیرعمدی مطرح بوده و بیان‌گر این است که الگوریتم استخراج تا چه حد توانایی بازیابی سیگنال اصلی را از روی سیگنال دریافتی (بعد از حمله) دارد [۶].

۲-۳- ظرفیت

ظرفیت[12] عبارت است از حداکثر مقدار داده قابل ذخیره‌سازی در حامل بدون آشکارسازی. گاهی از این مفهوم با عنوان بازده[13] نام‌برده می‌شود [۶].

۳- معیارهای متداول ارزیابی پنهان‌نگاری

به‌منظور ارزیابی منطقی عملکرد انواع روش‌های پنهان‌نگاری، نیاز به تعیین برخی معیار قابل‌پذیرش توسط اکثریت داریم. بنابراین قبل از بررسی روش‌های پنهان‌نگاری در فضاهای رنگ مختلف، معیارهای متداول مقایسهٔ روش‌های پنهان‌نگاری موردبررسی قرار داده‌شده است. سه نیازمندی متداولِ امنیت، ظرفیت و نامحسوس بودن؛ معیارهایی برای میزان عملکرد روش‌های پنهان‌نگاری استفاده شود.

[7] Trade off
[8] Visibility, Transparency or Fidelity
[9] Imperceptibility
[10] Subjective
[11] Robustness
[12] Capacity
[13] Payload

۳-۱- معیار میانگین مربعات خطا (MSE)

MSE معیاری برای محاسبه میانگین مربعات خطا است. این خطا به‌وسیله تفریقِ مقدارِ پیکسل از تصویر اصلی با تصویرِ پس از پنهان‌نگاری است.

رابطه (۱) برای محاسبه میانگینِ مربعات خطا در تصاویر رنگی است.

$$MSE = \frac{\sum_{(m,n)}(x(m,n) - y(m,n))^2}{N1 * N2} \quad (۱)$$

که در این رابطه $x(m,n)$ مقادیر پیکسل تصویر اصلی و $y(m,n)$ مقادیر پیکسل تصویر با پنهان‌نگاری و N1 و N2 مشخص‌کننده‌ی ارتفاع و عرضِ تصویر هستند[۷].

۳-۲- معیار سیگنال به نویز (SNR)

یکی از ویژگی‌های پنهان‌نگاری غیرقابل مشاهده بودن (نامحسوس بودن) است اما ازآنجاکه این معیار دقیق نیست باید معیاری تعریف شود تا توسط آن بتوان کارایی الگوریتم‌ها را در زمینه‌ی حفظ امنیت بسنجیم، که این معیار سیگنال به نویز (SNR) است که نشان‌دهنده میزان نویز اضافه‌شده به تصویر در اثر تعبیه اطلاعات در تصویر است. واحد این معیار دسی‌بل (db) است.

هرچه مقدار SNR بیشتر باشد تصویر حاوی پیام پنهان از کیفیت ظاهری بهتری برخوردار است. غالباً مقدار SNR بیش از ۳۵ دسی‌بل ازنظر درک نشدن تغییرات توسط انسان قابل‌قبول است. SNR به‌صورت ذیل محاسبه می‌شود[۷].

$$SNR = 10\,log\frac{\sum_{(m,n)} x^2(m,n)}{\sum_{(m,n)}(y(m,n) - x(m,n))^2} \quad (۲)$$

که در این رابطه $x(m,n)$ مقادیر پیکسل تصویر اصلی و $y(m,n)$ مقادیر پیکسل تصویر با پنهان‌نگاری است[۷].

۳-۳- معیار نرخ خطای بیت (BER)

از این معیار به‌منظور محاسبه خطای حاصل از تعبیه و بازیابی اطلاعات از تصویر استفاده می‌شود و به‌صورت درصد بیت‌های اشتباه استخراج‌شده از تصویر، نسبت به‌کل بیت‌های تعبیه‌شده در تصویر پوشش بیان می‌شود که این معیار از رابطه (۲) محاسبه می‌شود[۷].

$$BER = ((\sum_{i=1}^{l}(M(i) - M'(i))\text{^}2)/l\,) * 100 \quad (۳)$$

که M(i)، بیت i پیام تعبیه‌شده در تصویر و M′(i)، بیت i پیام استخراج‌شده است. همچنین L طول پیام یا تعداد کل بیت‌های تعبیه‌شده در تصویر است. بدیهی است هرچه مقدار BER کمتر باشد، روش بهتر و مطلوب‌تر است[۷].

۴- پنهان‌نگاری با استفاده از تبدیل موجک گسسته (DWT)

تبدیل موجک در ابتدای دهه ۱۹۸۰ معرفی گردید، از آن زمان تاکنون انواع متفاوتی از تبدیلات موجک توسعه‌یافته‌اند. مشهورترین نسخه این تبدیلات، تبدیل موجک گسسته[1] است که بهترین خواص فشرده‌سازی سیگنال را برای دسته بسیاری از سیگنال‌های دنیای واقعی همراه با جنبه‌های محاسباتی بسیار کارا دارد و به همین علت در زمینه‌های فشرده‌سازی تصویر، انتگرال‌گیری عددی و بازشناسی الگو بکار می‌رود.

با توجه به اینکه شبکیه چشم انسان تصاویر را به چندین کانال فرکانسی تقسیم می‌کند که پهنای باند هر یک از این کانال‌ها تقریباً یک اکتاو است؛ سیگنال‌های هر یک از این کانال‌ها در مغز به‌طور جداگانه پردازش می‌شوند. در تبدیل موجک نیز تصویر به باندهای فرکانسی تقریباً مساوی با مقیاس لگاریتمی تقسیم می‌گردد و به همین خاطر تغییرات ایجادشده در حوزه تبدیل موجک، برای چشم انسان کمتر قابل‌تشخیص است.

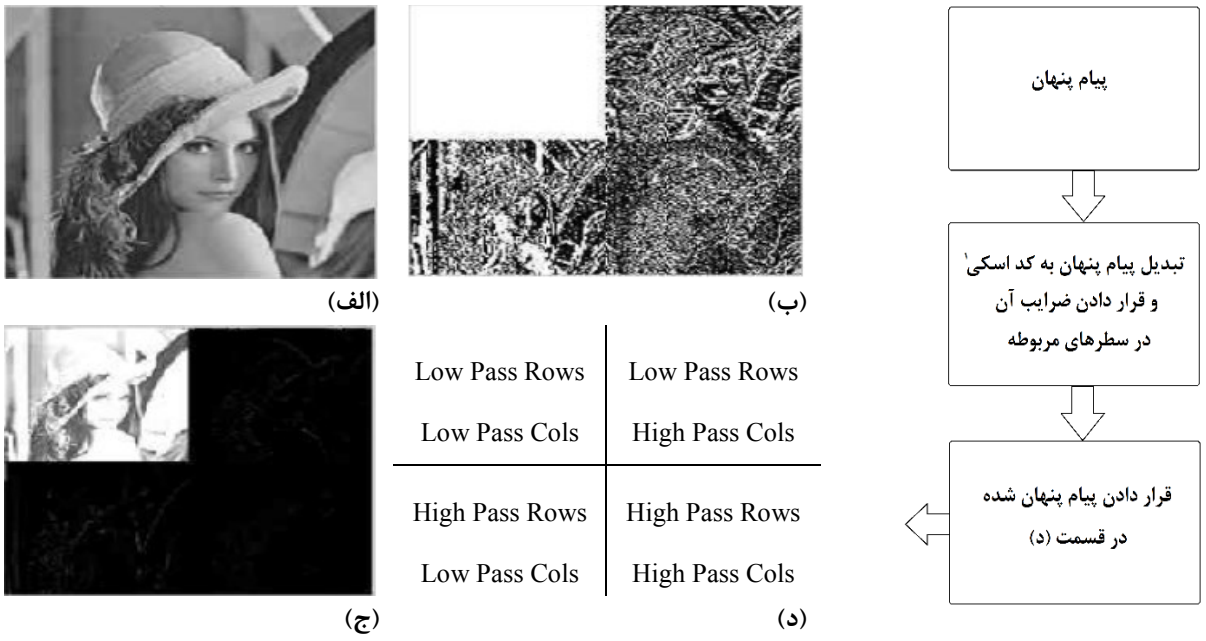
۴-۱- پنهان‌نگاری با استفاده از تبدیل موجک گسسته

الگوریتم پنهان‌نگاری با استفاده از تبدیل موجک گسسته در تصویر به‌صورت زیر است:

- از تصویر حامل تبدیل موجک گرفته می‌شود.
- پیام سری به کد اسکی[2] و یک‌رشته از بیت‌های صفر و یک تبدیل می‌گردد.
- رشته بیتی در لابه‌لای ردیف‌های یکی از چهار جزء تبدیل موجک پنهان می‌گردد.

مراحل این روش در شکل (۱) آورده شده است.

[1] DWT= Descerete Wavelet Transform
[2] ASCII

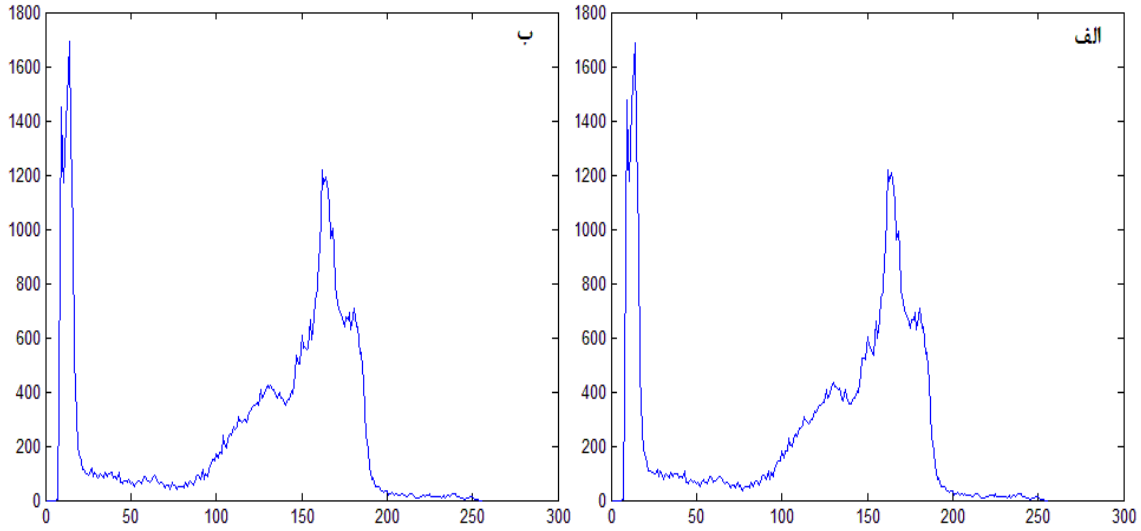


شکل(۱): مخفی کردن اطلاعات در تصویر به روش تبدیل موجک [۸]

۴-۱- تحلیل نتایج پنهان‌نگاری با استفاده از تبدیل موجک گسسته

شکل (۲) هیستوگرام‌های تصویر اصلی و تصویر با پنهان‌نگاری شده نشان می‌دهد. با دقت در مقایسه این هیستوگرام‌ها نتایج زیر حاصل می‌گردد:

هیستوگرام تصویر پنهان‌نگاری شده اختلاف بسیار کمی با هیستوگرام تصویر اصلی دارد. لذا پنهان‌نگاری با این روش مقاومت بسیار بالایی در مقابل تحلیل هیستوگرام دارد.



شکل (۲): هیستوگرام (الف: تصویر اصلی) و (ب: تصویر پنهان‌نگاری) در روش تبدیل موجک[۹]

تبدیل DWT یک تبدیل جدائی‌پذیر است، یک DWT دوبعدی را می‌توان با اعمال دو بار متوالی DWT یک‌بعدی، که ابتدا بر روی سطرها و سپس بر روی ستون‌های تصویر اعمال شود پیاده نمود.

پیاده‌سازی بانک فیلتر شناخته‌شده را می‌توان برای استفاده جهت محاسبه DWT دوبعدی بکار برد، که ساختار هرمی را نتیجه می‌دهد.

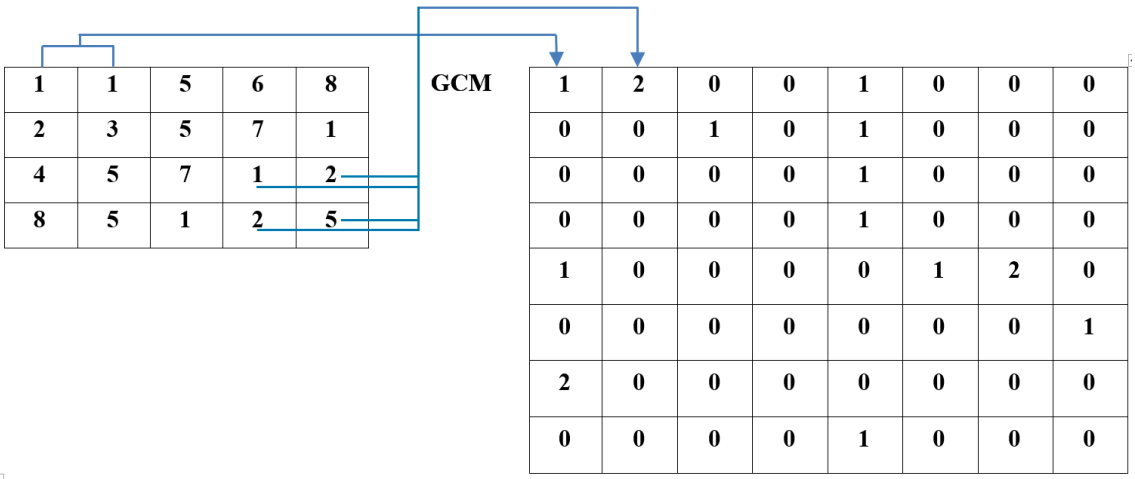
(ب) (الف)

شکل (۳): شکل (الف) تصویر اصلی ، شکل (ب) تصویر با پنهان‌نگاری

قسمت (الف) شکل (۳) تصویر اصلی و قسمت (ب) تصویر پنهان‌نگاری شده به روش تبدیل موجک را نشان می‌دهد. تبدیل موجک گسسته دارای مزایای زیادی است که این تبدیل را به روش برتر و روزآمد علم پنهان‌نگاری تبدیل نموده است.

۵- نهان‌کاوی

در کنار گسترش روش‌های مختلف پنهان‌نگاری اطلاعات در تصاویر، روش‌های متنوعی نیز برای مقابله با آن تحت عنوان نهان‌کاوی[۱۰] ایجاد شده است که هدف آن استفاده از ویژگی‌های تصاویر و الگوریتم‌های پردازشی برای کشف اطلاعات پنهان‌شده است. توانایی کشف پیام در تصویر تحت تأثیر فاکتورهای مختلفی قرار دارد که ازجمله می‌توان به طول پیام پنهان‌شده، درصد پنهان‌سازی اطلاعات، نوع پوشانه (صوت، تصویر و متن)، فرمت پوشانه انتخابی، روش جاسازی متن موردنظر در پوشانه اشاره کرد. معمولاً نهان‌کاوی برای رسیدن به دو هدف صورت می‌گیرد یک، پیدا کردن و دوم نابودی پیام‌های جاسازی‌شده است. پیدا کردن پیام‌ها که بسیار مفیدتر از نابودی آن است می‌تواند به دودسته کلی تقسیم شود، عکس‌ها و متن‌ها. باوجود روش‌های بسیار زیاد، پیدا کردن یک پیام مخفی‌شده در حجم عظیمی از متن‌ها که جابجا می‌شوند کار بسیار دشوار و تقریباً غیرممکن است.



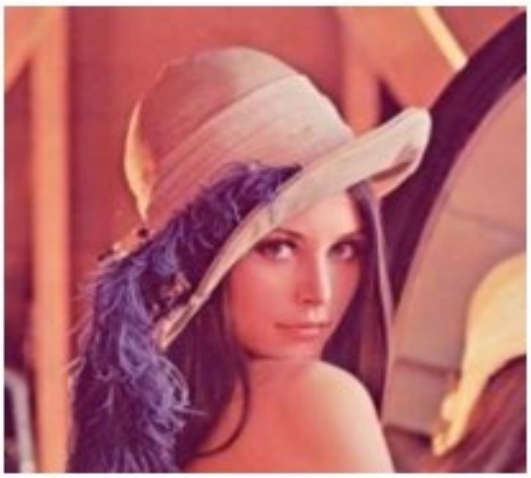
1	1	5	6	8
2	3	5	7	1
4	5	7	1	2
8	5	1	2	5

1	2	0	0	1	0	0	0
0	0	1	0	1	0	0	0
0	0	0	0	1	0	0	0
0	0	0	0	1	0	0	0
1	0	0	0	0	1	2	0
0	0	0	0	0	0	0	1
2	0	0	0	0	0	0	0
0	0	0	0	1	0	0	0

شکل (۴): ماتریس هم‌رخدادی(GLCM)[۱۱].

با توجه به این‌که پنهان‌نگاری و جاسازی اطلاعات در تصویر باعث ایجاد تغییرات در مقادیر پیکسل‌های تصویر و به‌تبع آن در مقادیر ماتریس GLCM می‌گردد، در این مقاله از این تغییرات برای استخراج ویژگی‌هایی که در تصاویر پوشانه یا گنجانه متفاوت باشد، استفاده‌شده است. همبستگی مقادیر میان پیکسل‌های مجاور در یک تصویر به حدی زیاد است که اگر لبه‌ها را در یک تصویر حذف کنیم، تفاوت مقدار یک پیکسل با پیکسل‌های مجاورش کم و یا صفر می‌شود. درنتیجه با توجه به همبستگی

شدید میان پیکسل‌های مجاور در تصاویر، مقادیر قطر اصلی ماتریس GLCM موردبررسی قرار داده خواهد شد. بدین منظور ابتدا از تصویر پوشانه (لنا) استفاده می‌شود، GLCM محاسبه و مجموع مقادیر روی قطر اصلی آن حساب خواهد شد. سپس به روش تبدیل موجک، اطلاعاتی را در تصویر لنا مخفی کرده و این تصویر را "imagesteg1" می‌نامیم. درنهایت مجدداً اطلاعاتی را در "imagesteg1" ذخیره کرده و تصویر "imagesteg2" محاسبه می‌شود. از "imagesteg2" نیز GLCM گرفته می‌شود و مجموع مقادیر روی قطر اصلی آن محاسبه می‌شود. در مرحله بعد تفاوت مجموع مقادیر قطر اصلی دو تصویر لنا و "imagesteg1"و همچنین دو تصویر "imagesteg1" و "imagesteg2"را محاسبه خواهد شد. برای تصویر استاندارد لنا که در شکل (۵) آمده است، این مقادیر محاسبه و در جدول (۱) ذکرشده است.



شکل (۵): تصویر لنا

جدول (۱): نتیجه ویژگی‌های استخراج‌شده از ماتریس GLCM تصویر لنا

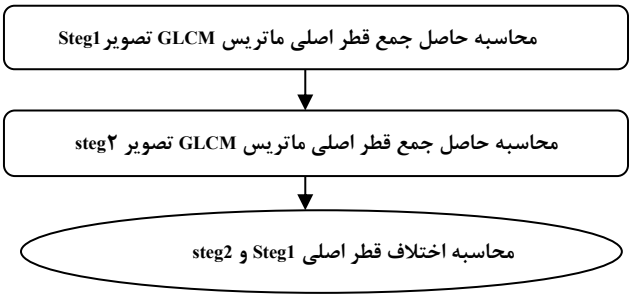
مجموع مقادیر قطر اصلی برای تصویر لنا	۳۷۵۲۹
مجموع مقادیر قطر اصلی برای تصویر "imagesteg1"	۳۲۴۷۵
مجموع مقادیر قطر اصلی برای تصویر "imagesteg2"	۳۲۰۳۰
(ویژگی ۱) تفاوت مجموع مقادیر قطر اصلی در دو تصویر لنا و "imagesteg1"	۵۰۵۴
(ویژگی ۲) تفاوت مجموع مقادیر قطر اصلی در دو تصویر "imagesteg1" و "imagesteg2"	۴۴۵

چون طیف رنگ تصویر در نقاط مختلف تصویر متغیر است، بهتر است تصویر به بخش‌های کوچک‌تر تقسیم شود. ازاین‌رو هر تصویر به تصویرهایی با ابعاد "۶۴×۶۴" تقسیم‌شده (یک تصویر "۲۵۶×۲۵۶"به ۱۶ تصویر"۶۴×۶۴" تبدیل‌شده و ویژگی‌های هر تصویر"۶۴×۶۴" استخراج‌شده). در پایان ویژگی‌های استخراج‌شده برای هر تصویر، میانگین ویژگی‌های به‌دست‌آمده از هر بخش است. نتایج این تغییر برای تصویر لنا در جدول (۲) نشان داده شده است.

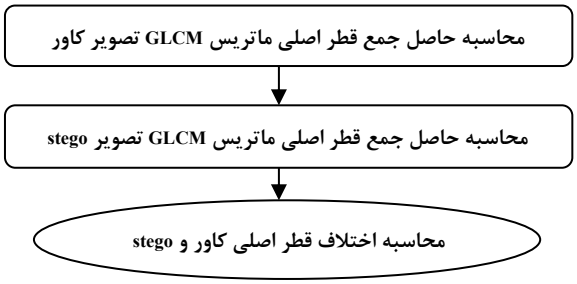
جدول(۲): نتیجه ویژگی‌های استخراج‌شده از ماتریس GLCM تصویر لنا بعد از میانگین‌گیری

مجموع مقادیر قطر اصلی برای تصویر لنا	۷۸۱۳/۵۷۱
مجموع مقادیر قطر اصلی برای تصویر "imagesteg1"	۵۱۸/۲۳۸۴
مجموع مقادیر قطر اصلی برای تصویر "imagesteg2"	۵۱۶/۴۳۸۴
(ویژگی ۱) تفاوت مجموع مقادیر قطر اصلی در دو تصویر لنا و "imagesteg1"	۵۳/۵۴۲۹
(ویژگی ۲) تفاوت مجموع مقادیر قطر اصلی در دو تصویر "imagesteg1" و "imagesteg2"	۱/۸

الگوریتم ویژگی‌های ۱ و ۲ در قسمت (الف و ب شکل(۶)) بیان‌شده است.

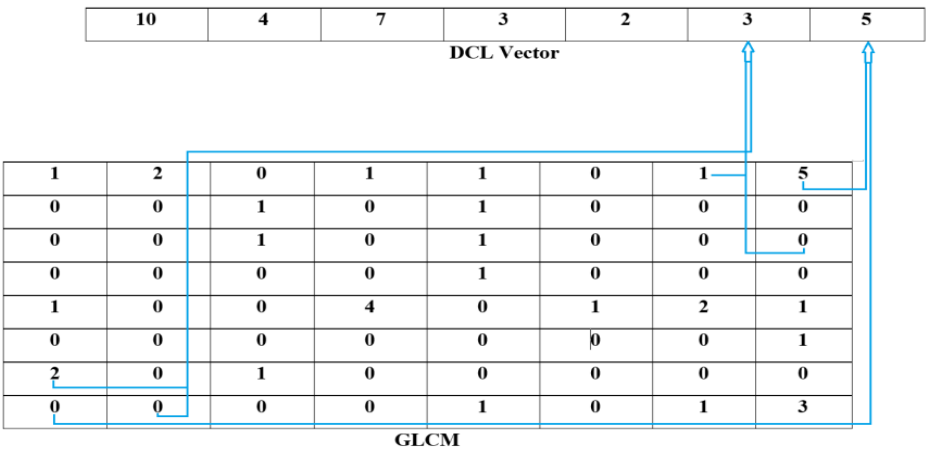


شکل (۶)الف: استخراج ویژگی ۱ از ماتریس GLCM

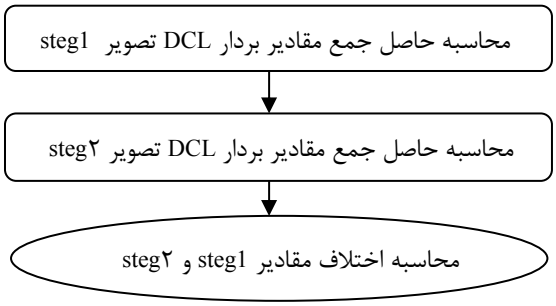


شکل(۶)ب: استخراج ویژگی ۲ از ماتریس GLCM

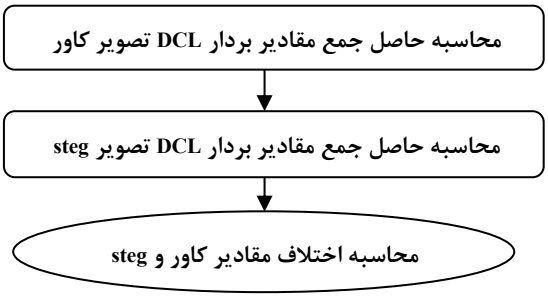
تصاویر متعددی از طیف رنگ متفاوت و حوزه ویژگی‌هایی که استخراج‌شده، ساخته‌شده که بسیار گسترده و متعدد می‌باشند. برخی از ویژگی‌های استخراج‌شده کوچک هستند درحالی‌که برخی دیگر بسیار زیاد هستند. محدوده گسترده و متعدد، جداسازی تصویر کاور از تصویر stego را دشوار می‌سازد. برای حل این مشکل دو ویژگی جدید از تصاویر به‌عنوان عامل‌های آشکارسازی با استفاده از بردارهای هم‌رخدادی (DCL) استخراج گردیده است. در مرحله قبل ویژگی‌ها از ماتریس GLCM استخراج‌شده بودند بردار DCL از ماتریس هم‌رخدادی حاصل می‌گردد، به‌عنوان‌مثال یک بردار (۷×۱) تعداد رخداد ۷ ویژگی مؤثر میزان تفاوت بین سطوح خاکستری پیکسل‌های همسایه در تصویر را معلوم می‌کنند. شکل (۷) استخراج هفت ویژگی مؤثر از ماتریس هم‌رخدادی را نشان می‌دهد. درواقع در این روش ماتریس‌های هم‌رخدادی جایگزین ماتریس تصویر شده است و قدر مطلق تفاضل سطر و ستون ماتریس‌های هم‌رخدادی، شماره ستون بردارDCL را می‌سازد. ارزش هریک از درایه‌های بردار هم‌رخدادی برابر مجموع درایه‌هایی از ماتریس‌های هم‌رخدادی است که قدر مطلق تفاضل سطر و ستون آن‌ها برابر موقعیت مکانی ستون آن درایه است. درایه اول بردار هم‌رخدادی مربوط به مجموع مقادیر درایه‌هایی از ماتریس‌های هم‌رخدادی است که تفاوت سطر و ستون آن‌ها برابر ۱ است. درایه دوم بردار DCL مربوط به مجموع درایه‌هایی از ماتریس‌های هم‌رخدادی است که قدر مطلق تفاضل سطر و ستون آن‌ها برابر ۲ است. به همین ترتیب ۷ سطح تغییر بین سطر و ستون درایه‌های ماتریس هم‌رخدادی دلیل ایجاد درایه هفتم بردار DCL بوده است.



شکل (۷): تشکیل بردارDCL از ماتریس هم‌رخدادی استخراج ویژگی ۲ از ماتریس GLCM



شکل (۸): استخراج ویژگی ۳ از بردار DCL



شکل (۹): استخراج ویژگی ۴ از بردار DCL

معادله (۱) نحوه تشکیل بردار DCL آورده شده است.

$$DCL(k) = \sum_{i,j} GLCM(i,j), if\, i-j = k \; and \; k = 1,2,\dots,7 \quad (۴)$$

در این روش، ارزش عددی هر پیکسل و پیکسل همسایه‌اش اساس کار نیست، در این روش میزان واحد تغییر بین هر پیکسل و پیکسل همسایه‌اش حائز اهمیت است. به همین ترتیب دو ویژگی دیگر (ویژگی ۳ ، ویژگی ۴) از تصاویر اصلی و با پنهان‌نگاری استخراج گردید (شکل‌های ۸ و ۹). درنتیجه بعد از محاسبه ویژگی‌های ۱و۲ در تصویر لنا، بردار DCL را محاسبه کرده و مجموع مقادیر بردار به دست می‌آید.

سپس به روش تبدیل موجک، اطلاعاتی در تصویر لنا مخفی‌شده و این تصویر"imagesteg1" نامیده می‌شود. درنهایت مجدداً اطلاعاتی در "imagesteg1" ذخیره می‌شود و تصویر "imagesteg2" ساخته می‌شود. در "imagesteg2" نیز بردار DCL به‌دست‌آمده و مجموع مقادیر این بردار محاسبه می‌شود. در مرحله بعد تفاوت مجموع مقادیر دو تصویر لنا و "imagesteg1" و همچنین دو تصویر "imagesteg1" و "imagesteg2" برای تصویر استاندارد شکل (۱۰) محاسبه می‌گردد.

شکل (۱۰): تصویر home (Image، imagesteg1، imagesteg2)

مقادیر DCL تصاویر لنا، "imagesteg1"و "imagesteg2"برای تصویر "home" محاسبه و در جدول(۳) ذکرشده است.

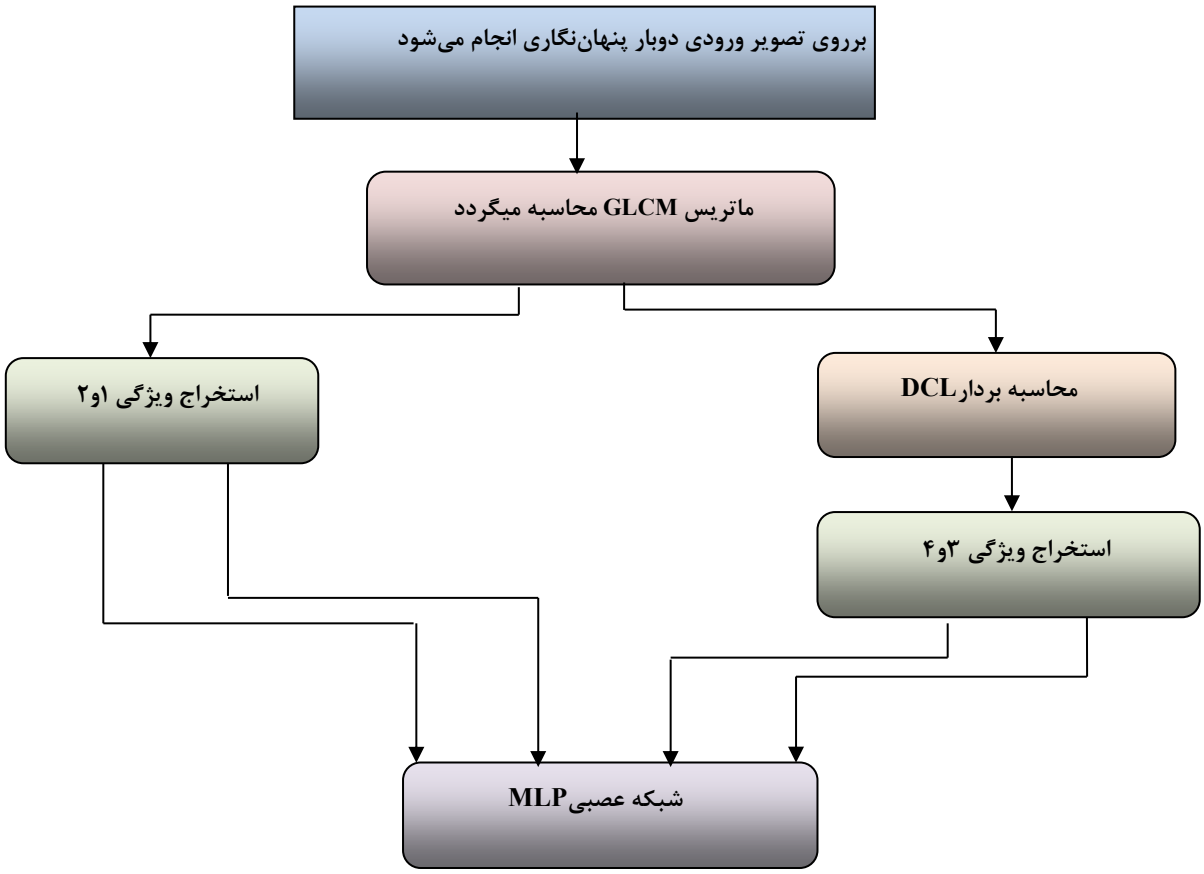
جدول (۳): نتیجه ویژگی‌های استخراج‌شده از بردار DCL

مجموع مقادیر قطر اصلی برای تصویر لنا	۳۵۶/۱۹
مجموع مقادیر قطر اصلی برای تصویر "imagesteg1"	۵۲۷/۸۶
مجموع مقادیر قطر اصلی برای تصویر "imagesteg2"	۵۳۰/۱۵
(ویژگی ۱) تفاوت مجموع مقادیر در دو تصویر لنا و "imagesteg1"	۱۷۱/۶۷
(ویژگی ۲) تفاوت مجموع مقادیر در دو تصویر "imagesteg1" و "imagesteg2"	۲/۲۹

به‌این‌ترتیب عامل آشکارسازی از تصویر کاور ویژگی ۳ و عامل آشکارسازی از تصویر با پنهان‌نگاری ویژگی ۴ انتخاب گردید. بنابراین اگر ویژگی ۳ بزرگ باشد آنگاه انتظار داریم که اختلاف بین "تصویر کاور و تصویر imagesteg1" بزرگ باشد و اگر این عامل کوچک باشد، آنگاه انتظار داریم که اختلاف بین "تصویر کاور و تصویر imagesteg1" کوچک خواهد بود. همچنین اگر ویژگی ۴ بزرگ باشد آنگاه انتظار داریم که اختلاف بین "تصویر imagesteg1 و تصویر imagesteg2" بزرگ باشد و اگر این عامل کوچک باشد، آنگاه اختلاف بین "تصویر imagesteg1و تصویرimagesteg2" کوچک خواهد بود.

عامل‌های آشکارسازی برای ۲۰۰ تصویر (۱۰۰تصویر کاور و ۱۰۰تصویر با پنهان‌نگاری) محاسبه گردید.

درنهایت می‌توان الگوریتم تشخیص تصاویر پنهان‌نگاری شده به روش تبدیل موجک را به‌صورت شکل (۱۱) بیان نمود.

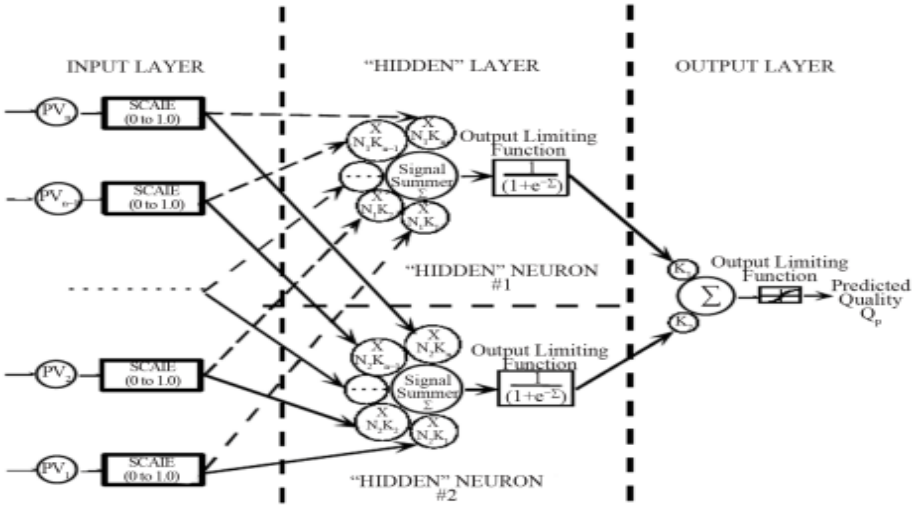


شکل (۱۱): الگوریتم تشخیص تصویر پنهان‌نگاری شده

۶- تحلیل با استفاده از شبکه عصبی چندلایه MLP

در شبکه عصبی نرون‌ها به‌صورت طبیعی به روش خاصی اتصال می‌یابند تا یک شبکه عصبی را تشکیل دهند نحوه اتصال نرون‌ها می‌تواند به‌گونه‌ای باشد که شبکه تک لایه یا چندلایه باشد. شبکه‌های چندلایه از یک‌لایه ورودی، یک‌لایه خروجی و یک یا چندلایه بین آن‌ها (لایه پنهان) که مستقیماً به داده‌های ورودی و نتایج خروجی متصل نیستند تشکیل یافته‌اند[۱۲].

واحدهای لایه ورودی صرفاً وظیفه توزیع مقادیر ورودی را به لایه بعد بر عهده‌دارند. و هیچ‌گونه تأثیری بر روی سیگنال‌های ورودی ندارند. به‌همین دلیل در شمارش تعداد لایه‌ها به‌حساب نیامده‌اند. شبکه شامل یک‌لایه خروجی است که پاسخ سیگنال‌های ورودی را ارائه می‌دهد. که تعداد نرون‌ها در لایه ورودی و لایه خروجی برابر با تعداد ورودی‌ها و خروجی‌ها است و لایه یا لایه‌های پنهان وظیفه ارتباط دادن لایه ورودی به لایه خروجی را بر عهده‌دارند[۱۳]. شبکه با داشتن این لایه‌های پنهان قادر می‌گردد که روابط غیرخطی را از داده‌های ارائه‌شده به شبکه استخراج کند. شکل (۱۲) شبکه عصبی چندلایه MLP را نشان می‌دهد.



شکل (۱۲): شبکه عصبی چندلایه MLP

در این مقاله از شبکه عصبی چندلایه (MLP) به‌عنوان تحلیل‌کننده استفاده‌شده است. شبکه عصبی چندلایه یک مولد شبکه عصبی مصنوعی با تغذیه مستقیم است که دسته‌های داده‌های ورودی را روی دسته خروجی مناسب ترسیم می‌کند. شبکه مورد آزمایش دارای ۴ لایه است که یک‌لایه ورودی، دولایه پنهان و یک‌لایه خروجی دارد. تعداد نرون‌های لایه ورودی۴ است که برابر با تعداد ویژگی‌ها است و تعداد درون‌های لایه خروجی ۱ است که مشخص می‌کند که آیا تصویر با پنهان‌نگاری است یا خیر؛ ویژگی‌ها برای ۱۰۰ تصویر اولیه به دست آورده شده و از ۷۵ تصویر به‌عنوان ورودی (آموزش) شبکه عصبی ۴ لایه استفاده گردید و از ۲۵ تصویر به‌عنوان تست استفاده شد.

در جدول (۴) به مقایسه دقت آشکارسازی روش پیشنهادی و مقایسه آن با سایر روش‌ها پرداخته‌شده است.

جدول (۴): مقایسه دقت آشکارسازی روش پیشنهادی با سایر روش‌ها

روش	میزان تشخیص روش پیشنهادی
Steganalysis of DWT Based Steganography Technique for SD and HD Videos[14]	۵۶/۶٪
Unsupervised Steganalysis Based on Artificial Training Sets [16]	٪۷۸
Steganalysis based on steganography pattern discovery [17]	٪۷۹
New steganalysis method using glcm and neural network [18]	٪۸۰
Particle Swarm Optimization based feature selection with novel fitness function for image steganalysis [20]	۸۲/۶۲٪
Steganalysis: breaking highly unde- tectable steganography [21]	٪۸۵
Compact image steganalysis for LSB-matching steganography [22]	۸۷/۲٪
روش پیشنهادی	٪۹۰

۷- نتیجه‌گیری

هم‌زمان با پیشرفت پنهان‌سازی اطلاعات، علم تحلیل پنهان‌سازی نیز به‌سرعت در حال پیشرفت است و هرروز روش‌های جدیدتری به وجود می‌آیند. این روش‌ها اهداف گوناگونی همچون تشخیص وجود پیام و یا تشخیص و آشکارسازی پیام و در مراحل بالاتر تشخیص، آشکارسازی و حذف و جایگزینی پیام را دنبال می‌کنند. در این مقاله از روش پنهان‌سازی اطلاعات در سیگنال‌های تصویر، به روش تبدیل موجک الگوریتمی استفاده‌شده که نتایج نشان از مقاومت بالای این روش می‌داد.

برای تحلیل تصاویر پنهان‌نگاری شده به روش تبدیل موجک الگوریتمی با استفاده از ویژگی‌های ماتریس GLCM و بردارهای هم‌رخدادیDCL برخی از مقادیر در تصاویر کاور و اصلی ارائه شد و ویژگی‌هایی که بین این تصاویر متفاوت هستند استخراج گردید. ویژگی‌ها برای آموزش شبکه عصبی استفاده شد و مرحله طبقه‌بندی با استفاده از لایه‌های شبکه عصبی چندلایه (MLP) انجام شد.

الگوریتم پیشنهادی برای پایگاه داده ۲۰۰ تصویر استاندارد (Casia-Iris) تست شد و نتایج جدول (۴) نشان‌دهنده مزیت این روش نسبت به سایر روش‌های بررسی‌شده است؛ چراکه دقت روش پیشنهادی ۹۰٪ آشکارسازی تصاویر با پنهان‌نگاری بوده که بالاتر از بیشترین مقدار دقت در مقالات (۸۷/۲٪) است.

۸- مراجع

[1] De Rosal Ignatius Moses Setiadi, “Digital image steganography survey and investigation (goal, assessment, method, development, and dataset)” Signal Processing, vol. 206, May 2023.

[2] Pratap Chandra Mandal, Imon Mukherjee, Goutam Paul, B. N. Chatter “Digital image steganography: A literature survey” Information Sciences vol. 609, pp. 1451-1488, September 2022.

[3] B. F. Alatiyyat and N. C, ”Survey on Image Steganography Techniques” 2nd International Conference on Computing and Information Technology (ICCIT), Tabuk, Saudi Arabia, 2022, pp. 57-64, doi: 10.1109/ICCIT52419.2022.9711651.

[4] Saeid Fazli, Maryam Zolfaghari-Nejad, “A New Steganalysis Method for Steganographic Images on DWT Domain” International Journal of Science and Engineering Investigations, March 2012, Vol. 1.

[5]Trivikram Muralidharan, “The infinite race between steganography and steganalysis in images”, Signal Processing, vol. 201, December 2022.

[6] S. Talati and P. Etezadifar, “Providing an Optimal Way to Increase the Security of Data Transfer using Watermarking in Digital Audio Signals” Majlesi Journal of Telecommunication Devices, 9(1), pp. 35-46, 2020.

[7] S. Talati, P. EtezadiFar, M. R. Hassani Ahangar, and M. Molazade, “Investigation of Steganography Methods in Audio Standard Coders: LPC, CELP, MELP” Majlesi Journal of Telecommunication Devices, 12(1), pp. 7-15, 2023, doi: 10.30486/mjtd.2022.695928.

[8] I. R. Farah, I. B. Ismail, and M. B. Ahmed, "A Watermarking System Using the Wavelet Technique for Satellite Images", Word Academy of Science, Engineering and Technology, vol. 17, Dec. 2006. ISSN 1307-6884.

[9] C. Rafael Gonzalez, “Digital Image Processing using Matlab”, Pearson Prentice Hall, 2004.

[10] Bo Yang and Beixing Deng, “Steganography in Gray Images Using Wavelet”, Department of Electronic Engineering, Tsinghua University, Beijing, China, 2005.

[11] S. Ghanbari, “New Steganalysis Method using GlCM and Neural Network” International Journal of Computer Applications, March 2012.

[12] S. Talati and M. R. Hassani Ahangar, “Analysis, Simulation and Optimization of LVQ Neural Network Algorithm and Comparison with SOM”, Majlesi Journal of Telecommunication Devices, 9(1), pp. 17-22, 2020.

[13] Talati, S., and M. R. Hasani Ahangar. “Radar data processing using a combination of principal component analysis methods and self-organizing and digitized neural networks of the learning vector.” Electronic and Cyber Defense 9.2 (2021): 1-7.

[14] M. Dalal and M. Juneja, “Steganalysis of DWT Based Steganography Technique for SD and HD Videos”. Wireless Pers Commun 128, pp. 2441–2452, 2023.

[16] D. Lerch-Hostalot and D. Megías, “Unsupervised Steganalysis Based on Artificial Training Sets.” Engineering Applications of Artificial Intelligence, vol. 50, pp. 45-59 2016. https://doi.org/10.1016/j.engappai.2015.12.013.

[17] H. Sajedi, “Steganalysis based on steganography pattern discovery,” Journal of Information Security and Applications, vol. 30, pp. 3–14, 2016.

[18] S. Ghanbari, “New steganalysis method using glcm and neural network,” International Journal of Computer Applications; vol. 42(7), pp. 46–50, 2012.

[20] Rostami V, Khiavi AS. “Particle Swarm Optimization based feature selection with novel fitness function for image steganalysis”. In: Artificial intelligence and robotics, 2016. p. 109–14.

[21] (HUGO), “Steganalysis: breaking highly unde-tectable steganography,” Lecture notes in computer science (including subseries on lecture notes in artificial intelligence lecture notes in bioinfor- matics (LNCS)), vol. 6958, pp. 71–84, 2011.

[22] O. Juarez-Sandoval, “Compact image steganalysis for LSB-matching steganography”. In: Proceedings-2017 5th international work- shop on biometrics and forensics, (IWBF 2017), pp. 1–6, 2017.

[23] S. Talati, A. Rahmati, and H. Heidari, “Investigating the Effect of Voltage Controlled Oscillator Delay on the Stability of Phase Lock Loops”, MJTD, vol. 8, no. 2, pp. 57-61, 2019.

[24] S. Talati and M. R. Hassani Ahangar, “Combining Principal Component Analysis Methods and Self-Organized and Vector Learning Neural Networks for Radar Data”, Majlesi Journal of Telecommunication Devices, vol. 9(2), pp. 65-69, 2020.

[25] M. R. Hassani Ahangar, S. Talati, A. Rahmati, and H. Heidari, “The Use of Electronic Warfare and Information Signaling in Network-based Warfare”. Majlesi Journal of Telecommunication Devices, vol. 9(2), pp. 93-97, 2020.

[26] M. Aslinezhad, O. Mahmoudi, and S. Talati, “Blind Detection of Channel Parameters Using Combination of the Gaussian Elimination and Interleaving,” Majlesi Journal of Mechatronic Systems, vol. 9(4), pp. 59-67, 2020.

[27] S. Talati and A. Amjadi, “Design and Simulation of a Novel Photonic Crystal Fiber with a Low Dispersion Coefficient in the Terahertz Band”. Majlesi Journal of Mechatronic Systems, vol. 9(2), pp. 23-28, 2020.

[28] S. Talati, S. M. Alavi, and H. Akbarzade, “Investigating the Ambiguity of Ghosts in Radar and Examining the Diagnosis and Ways to Deal with it,” Majlesi Journal of Mechatronic Systems, vol. 10(2), 2021.

[29] P. Etezadifar and S. Talati, “Analysis and Investigation of Disturbance in Radar Systems Using New Techniques of Electronic Attack,” Majlesi Journal of Telecommunication Devices, 10(2), pp. 55-59, 2021.

[30] S. Talati, B. Ebadi, and H. Akbarzade “Determining of the fault location in distribution systems in presence of distributed generation resources using the original post phasors,” QUID 2017, pp. 1806-1812, Special Issue No.1- ISSN: 1692-343X, Medellin-Colombia. April 2017.

[31] S.Talati and S. M. Alavi "Radar Systems Deception using Cross-eye Technique," Majlesi Journal of Mechatronic Systems, vol. 9(3), pp. 19-21, 2020.
[32] S.Talati, M. Akbari Thani, and M. R.Hassani Ahangar, "Detection of Radar Targets Using GMDH Deep Neural Network", Radar Journal, vol. 8 (1), pp. 65-74, 2020.
[33] S.Talati, R. Abdollahi, V. Soltaninia, and M. Ayat, "A New Emitter Localization Technique Using Airborne Direction Finder Sensor," Majlesi Journal of Mechatronic Systems, vol. 10(4), pp. 5-16, 2021.
[34] H. Akbarzade, S. M. Alavi, and S. Talati, "Investigating the Ambiguity of Ghosts in Radar and Examining the Diagnosis and Ways to Deal with it," Majlesi Journal of Mechatronic Systems, vol. 10.2, pp. 17-20, 2021.
[35] S. M. Hashemi, S. Barati, S. Talati, and H. Noori, "A genetic algorithm approach to optimal placement of switching and protective equipment on a distribution network." J. Eng. Appl. Sci. vol. 11, pp. 1395-1400, 2016.
[36] O. Sharifi-Tehrani and S. Talati, "PPU Adaptive LMS Algorithm, a Hardware-Efficient Approach; a Review on", Majlesi Journal of Mechatronic Systems, vol. 6, no. 1, Jun. 2017.
[37] S. Hashemi, & M. Abyari, Sh. Barati, S.Tahmasebi, and S. Talati, "A proposed method to controller parameter soft tuning as accommodation FTC after unknown input observer FDI," Journal of Engineering and Applied Sciences, vol. 11, pp. 2818-2829, 2016.
[38] S. Talati, et al., "Analysis and Evaluation of Increasing the Throughput of Processors by Eliminating the Lobe's Disorder," Majlesi Journal of Telecommunication Devices 10.3, pp. 119-123, 2021.
[39] S. Talati, S. M. Ghazali, M. R. Hassani Ahangar, and S. M. Alavi, "Analysis and Evaluation of Increasing the Throughput of Processors by Eliminating the Lobe's Disorder'," Majlesi Journal of Telecommunication Devices, vol. 10(3), pp. 119-123, 2021. doi: 10.52547/mjtd.10.3.119
[40] S. Talati, A. Rahmati, and H. Heidari, "Investigating the Effect of Voltage Controlled Oscillator Delay on the Stability of Phase Lock Loops", MJTD, vol. 8, no. 2, pp. 57-61, May 2019.
[41] S. Talati and P. EtezadiFar, "Electronic attack on radar systems using noise interference," Majlesi Journal of Mechatronic Systems 10.3, pp. 7-11, 2021.
[42] S. M. Ghazali, J. Mazloum, and Y. Baleghid, "Modified binary salp swarm algorithm in EEG signal classification for epilepsy seizure detection," Biomedical Signal Processing and Control, vol. 78, September 2022, 103858.
[43] S. Talati, S. M.Ghazali, V. R. SoltaniNia, "Design and construct full invisible band metamaterial-based coating with layer-by-layer structure in the microwave range from 8 to 10 GHz," Journal of Physics D: Applied Physics, vol. 56, no. 17, 2023. DOI 10.1088/1361-6463/acb8c7.
[44] M. R. Hasani Ahangar and M. Mohammadi, "Evaluation of Efficient Factors on Quality of Service in Routing Protocols," Passive Defense Quarterly, no. 3, vol. 3, 2012.